
HACKING
KYBER
NETICKÁ
KRIMI
NALITA
nejen o hackingu, crackingu,
virech a trojských koních bez tajemství
Václav Jirovský
GRADA

Kybernetická kriminalita

nejen o hackingu, crackingu, virech a trojských koních bez tajemství

Václav Jirovský

Vydala Grada Publishing, a.s.
U Průhonu 22, Praha 7
jako svou 3070. publikaci

Odpovědný redaktor Martin Kysela
Návrh vnitřního layoutu Miroslav Lochman
Sazba Petra Tesárková
Návrh a grafická úprava obálky Petra Tesárková
Počet stran 288
První vydání, Praha 2007

Vytiskly Tiskárny Havlíčův Brod, a.s.
Husova ulice 1881, Havlíčkův Brod

ISBN 978-80-247-1561-2

Obsah

Předmluva

„Chci, aby lidé slyšeli mé potvrzení, že počítač je nová mocná metafora, která nám pomáhá porozumět mnoha aspektům světa, ale že také zotročuje mysli těch, kteří jiné metafory nemají a nemají ani jiné zdroje, na které by se mohli odvolat". Takto jasné stanovisko pronesené Josephem Weizenbaumem na jeho přednášce v Obecním domě v květnu 2002 zcela jasně odráželo změnu jeho životního postoje. Proměna spolutvůrce prvních počítačů, autora učících se programů, profesora informatiky na MIT a počítačového disidenta, který se hluboce zamýšlí nad úlohou technologií na tomto světě, odrážela mimo jiné i vojenské zneužívání počítačových technologií. I když jeho historka o agentech požadujících po MIT vytvoření počítačového modelu prezidenta Spojených států, který by za prezidenta rozhodoval v případě jeho nedostupnosti způsobené např. atomovým útokem, byla až na pokraji science fiction, přeci jen zanechala hluboce hlodající pochybnost.

Otázka vlivu počítačových systémů a informatizace společnosti spolu s fenoménem bezpečnosti počítačových systémů se stává velmi populárním tématem. Konají se konference na téma bezpečnosti, publikují se nejrůznější osvědčené postupy, kterak zabezpečit počítačovou a komunikační infrastrukturu před napadením, doporučují se stále nové programy nebo zařízení pro ochranu systémů. Existují desítky firem, které za přesně specifikovanou částku „dodají bezpečnostní řešení" a na internetu kolují stovky návodů jak ta

či ona bezpečnostní opatření obejít. Slovo „bezpečnost" se stalo módou a „bezpečnostní řešení" produktem kalkulujícím se strachem z neznáma, podobně jako pojišťovací agenti, přesvědčující obyvatele oázy o nutnosti pojistit se proti povodni.

konecma

Byla to asi právě ta neustále skloňovaná „bezpečnost", která mne vedla k docela obyčejné otázce: jak vlastně fungují mechanizmy útoků, proti kterým se chceme bránit. Jak pracují mechanizmy hrozeb? Co je skryto za „nebezpečností" virtuálního světa? Domnívám se, že nezbytnost analýzy obecných charakteristik takových útoků je zřejmá. Většina bezpečnostních řešení staví spíše na popisech realizovaných útoků než na jejich rozboru, na vyčlenění společných rysů a hledání obecných vlastností. A bez toho nelze stanovit obecná a fungující pravidla ochrany i před útoky, které dosud nebyly realizovány.

Kybernalita neboli kybernetická kriminalita má své místo ve virtuálním prostoru datových a telekomunikačních sítí. Studium kybernality zakládá nový interdisciplinární obor zabývající se nelegálními a škodlivými aktivitami v počítačovém prostoru, které jsou založeny na použití nebo zneužití počítačové technologie. Prezentace souvislostí dění v kyberprostoru a v reálném světě připomíná poněkud známou filmovou trilogii Matrix. Avšak text této knihy není Matrix, i když by to někdy tak mohlo vypadat. Je to reálná součást našeho každodenního života, kdy nás technologie posunula do nové dimenze, do dimenze kyberprostoru. A ať chceme nebo nechceme, budeme se muset v této „páté dimenzi" naučit žít.

Václav Jirovský

Praha 2007

Poděkování

Na tomto místě bych rád poděkoval všem, kteří mne k sepsání této knihy inspirovali, nebo mi pomohli cennou radou. Studium kybernality je interdisciplinární záležitostí a vyžaduje široký rozsah znalostí jak z oblasti společenských věd, tak i věd technických. A proto jsem vděčen všem odborníkům, kteří v debatách vyslovili svůj názor, a tím mi pomohli upravit mé vlastní nazírání na některé speciální otázky.

V tomto smyslu bych chtěl především vyjádřit svůj dík JUDr. Tomáši Gřivnovi, Ph.D. z katedry trestního práva Právnické fakulty Univerzity Karlovy, který věnoval čas opravám mých nepřesných formulací z jeho oboru a Prof. RNDr. Jaroslavu Pokornému, CSc. z Matematicko-fyzikální fakulty Univerzity Karlovy, jenž mi umožnil předmět Kybernalita přednášet v rámci výuky informatiky. Za cenné připomínky děkuji rovněž Ing. Robertu Malému.

Mé poděkování v neposlední řadě náleží i mým studentům předmětu Kybernalita, jejichž postřehy z prostředí, ve kterém se denně pohybují, mi byly zdrojem řady zajímavých informací a námětů.

Václav Jirovský

1.

Vznik kyberprostoru

Když v roce 1968 došlo k prvnímu síťovému propojení mezi čtyřmi univerzitními počítači a ke vzniku zárodku sítě ARPANET, nikdo nepředpokládal obrovský rozvoj síťových technologií propojujících miliony uzlů. V době návrhu dnes nejrozšířenějšího protokolu TCP/IP nepředpokládali jeho tvůrci tak obrovský rozmach internetu, a tak na bezpečnostní charakteristiky sítí a protokolů nebyl kladen takový důraz jako dnes. Nicméně technologie pokročily dopředu rychleji než bylo očekáváno a slabiny těchto technologií se staly cílem nelegálních aktivit probíhajících v počítačových sítích.

Abychom pochopili současný vztah společnosti a technologií, je třeba si uvědomit, že rychlost, se kterou se rozvíjely počítačové a komunikační technologie, byla mimo veškeré běžné praktiky a společnost, zvyklá na relativně pomalý technický rozvoj, reagovala se zpožděním. Výpočetní technika a telekomunikace absolvovaly devadesát procent své historie během druhé poloviny minulého století, a tak při tomto překotném vývoji není divu, že lidská společnost, která přetavovala zvyky, morálku a etiku do podoby zákonů a pravidel po staletí, začala za postupem technologií zaostávat.

Vývoj lidské společnosti je doprovázen neustálou interakcí jedinců a komunit, a jsou to právě tyto interakce, které posunují vývoj individua i společnosti vpřed. Historicky tyto interakce

existovaly vždy v objektivně vnímatelném fyzickém prostředí a jejich aktéry byli opět objektivně vnímatelní jedinci nebo skupiny. Tedy k interakcím docházelo vždy na fyzické úrovni. Hra malých dětí na zemanském dvorci byla součástí jejich výchovy a růstu, zdokonalovala jejich vnímání světa a vytvářela nezbytný percepční aparát. Komunikace jedince byla tedy vždy doprovázena fyzickým vjemem, kdy posluchač vnímal nejenom řeč protistrany, ale i její pohyby, postavení nebo fyzické rysy. Mezilidská komunikace tak sestávala ze dvou vzájemně vyrovnaných a propojených složek – verbální komunikace a mimoverbální komunikace, neboli řeči těla.

konecma

Se zdokonalováním verbální komunikace a vytvářením nových prostředků vyjadřování ustupovala mimoverbální komunikace do pozadí a objevovaly se první příznaky přesunu lidského vnímání do virtuálního prostoru. S trochou přehánění by se dalo říci, že to byly dva vynálezy, které posunuly život člověka do virtuálního prostoru. Objev a používání knihtisku, který zpřístupnil písemná sdělení širším masám, byl začátkem takového přesunu. Zatímco do té doby veškeré dění probíhalo na fyzické úrovni jednání jedince, knižní vydání romantického románu přesunulo jeho čtenáře do vysněného světa a osobnosti hrdinů ponechalo jeho představivosti. A tak jedinec, oddělený od společnosti, mohl trávit příjemné chvíle v kruhu svých imaginárních hrdinů, aniž by se svým okolím jakkoli komunikoval. Z hlediska přenosu to však byl jednosměrný tok informací od autora imaginace ke čtenáři, který stimuloval jeho představy pouze v jeho uzavřeném virtuálním světě.

Významnou změnu přinesla výpočetní technika a internet. Interaktivita, u knižních virtuálních postav dosud nedostupná, se stala podstatou počítačové komunikace, totální ztráta mimoverbálního vnímání[1], možnost vytváření nesmrtelných virtuálních jedinců, snadnost přechodu mezi komunitami a potlačená potřeba kompromisů vedly k vytvoření nového „kybernetického" světa, který se pro mnohé stal snesitelnější a příjemnější nežli svět reálný. Kyberprostor, jak jej budeme nadále nazývat, se stal pátou dimenzí života společnosti se všemi rysy, které dennodenní společenské aktivity přinášejí. A podobně jako náš reálný svět i kyberprostor nabývá všech společenských atributů – politických, obchodních, emocionálních, kultovních nebo náboženských. Nalezneme zde kyberprofesionály stejně jako kyberzelenáče, kybersportovce i kyberlenochy, kybermoralisty stejně jako kyberzločince.

Do kyberprostoru se přenáší všechny rysy současné společnosti, ale život v kyberprostoru si formuluje svoje vlastní pravidla, která se často vymykají přirozenému řádu, ve kterém lidské společenství žilo po staletí. Chce-li tato společnost v kyberprostoru přežít, nic jiného je nezbývá, než stará pravidla chování přizpůsobit, nová vytvořit a naučit se v tomto pátém rozměru života společnosti existovat. Tento způsob existence však přináší i jistá nová nebo modifikovaná nebezpečí, nové nebo modifikované formy chování, se kterými se musíme vypořádat, naučit se je akceptovat nebo najít způsoby, jak jim čelit.

Studium kybernetické kriminality – kybernality zahrnuje řadu nových pohledů na jedince i společnost, resp. na jejich projekce do kyberprostoru. Je nutno si uvědomit, že veškeré dosud známé nelegální aktivity probíhaly ve fyzickém prostoru, kde každý z aktérů byl lehce popsatelný a postižitelný. Tak tomu není v kyberprostoru, kde se setkáváme pouze s projekcemi pachatelů, s jejich virtuálním obrazem, který může být od skutečných rysů pachatele na hony vzdálen. A s tím se stávající metody vyšetřování a chápání trestných činů jenom obtížně vyrovnávají. Současné chápání „kybernetického" trestného činu, kterému chybí klasické atributy, se zatím velmi opatrně formuje. Standardizované metody policejního vyšetřování selhávají při „honění duchů" v kyberprostoru, justice tápe ve formulacích trestního zákona. Ohraničení jurisdikcí, rychlost provedení trestného činu a zahlazení stop, to všechno jsou oblasti, kde je dnešní legislativa teprve na počátku.

[1] Někdy se setkáme s tvrzením, že mimoverbální komunikaci představují v kyberprostoru emotikony nebo způsob psaní textu. Tyto výrazové prostředky však již existovaly dávno před jejich rozšířením do světa elektronické komunikace a jsou pouhou nedokonalou náhražkou mimoverbální komunikace.

Studium kybernality vychází z chápání a popisů technologií a možností, které tyto technologie dávají člověku. I když v prvním přiblížení je to zejména informatika a telekomunikace, které jsou základními technologiemi při vytváření kyberprostoru, můžeme najít některé specifické vědy, již tento proces významně ovlivňují[2]. Do studia kybernality však zasahují významně i společenské vědy, zejména sociologie, psychologie a právní věda. V následujících kapitolách uvidíme, jak právě v těchto oblastech dochází k velmi významným zjištěním, souvisejícím se změnami lidského chování a jeho projekcí do právního řádu.

1.1 Chápání kyberprostoru

„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky... Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v mysli, shluky a souhvězdí dat. Jako světla města,...". Tak popisuje kyberprostor William Gibson ve své knize „Neuromancer" [G01]. I když se tento termín poprvé objevil v roce 1982 jeho povídce „Burning Chrome" [G02], do širšího povědomí pronikl právě s románem „Neuromancer".

Gibsonem popisovaný kyberprostor, nazvaný „matrix", je možné navštívit po přímém napojení mozku k počítači prostřednictvím elektrod a lze se v něm pohybovat bez rušivého vlivu technologického zprostředkování. Představa bezprostředního spojení člověka s technologií je zde fikcí, nicméně právě fikce je prostředí, v němž Gibson rozpoutává svou imaginaci. Termín kyberprostor přešel později od významného představitele kyberpunku do běžného užívání a objevily se i jeho přesnější a vědečtější definice, např. [F01]. John Barlow, zakladatel Electronic Frontier Foundation, považuje za kyberprostor existující počítačové sítě a vlastně veškeré telekomunikační sítě[3]. Zcela zřejmým příkladem kyberprostoru mohou být systémy virtuální reality a další druhy virtuálních a počítačem simulovaných prostředí. V neposlední řadě jsou to i různé počítačové hry a zejména internet.

Než se budeme dále věnovat kyberprostoru, podívejme se do historie vzniku kybernetiky a informatických oborů. Norbert Wiener, zakladatel kybernetiky pro ni v roce 1947 vytvořil název odvozený z řeckého slova χυβερνητης, jež znamená „kormidelník". Kybernetiku pak definoval jako „vědu o řízení a komunikaci v živých organismech a strojích" a stejného názvu použil v titulu své knihy [W01]. Dalším důležitým základem bylo formulování kvantitativního a pravděpodobnostního pojetí informace, s nímž přišel ke konci čtyřicátých let Claude Shannon. Shannonovo pojetí oproštovalo informaci od jejího hmotného i symbolického kontextu. Umožnilo kvantifikovat procesy, které do té doby byly chápány pouze intuitivně a svým způsobem přispělo i k rozvoji nových technologií a vynálezů. Poslední objev, který patří do magické trojice pramenů moderních technologií patří Johnu Bardeenovi, Williamu Shockleymu, and Walteru Brattainovi, vědcům z Bellových laboratoří na Murray Hill, kteří zkonstruovali první polovodičovou součástku – tranzistor[4]. Tím začal závod technologií o prostor a čas, období miniaturizace a mikrominiaturizace.

Souvislosti vývoje technologií a společnosti popisuje španělský sociolog, působící jako emeritní profesor na univerzitě v Berkeley, Manuel Castells, který hovoří o „novém technologickém paradigmatu" [C01]. Jeho myšlenkový proud sleduje řada jeho kolegů, kteří považují vývoj technologií, jejich masové uplatnění, urychlované využitím nových materiálů a procesů, za

[2] Abych nezabíhal příliš daleko, stačí si jen uvědomit úzkou provázanost technologií a ekonomiky, abychom pochopili, že např. ekonomické nástroje podpořené technologiemi mohou významně podporovat některé mocenské zásahy.

[3] Podle Barlowa se v kyberprostoru nalézáte např. když telefonujete.

[4] Za svůj objev byli v roce 1956 oceněni Nobelovou cenou za fyziku.

jeden z určujících proudů vývoje myšlení a chování současné společnosti. V této souvislosti jsou často předpokládány významné společenské změny, např. profesor historie na newyorské universitě Mark Poster se domnívá, že nastává „druhý věk médií", kdy elektronická média vyvolají hluboké transformace kulturní identity a subjektivity, jenž povedou k odklonu od profilu moderního rozumného a stabilního občana. Tento trend dokonce srovnává se vznikem městské kupecké kultury ve středověku [P01].

Proměna technologií, prudký nástup informatiky a mikroelektroniky, biotechnologie a genetické inženýrství, to všechno stimulovalo i nové proudy v umění. Gibson a ostatní autoři kyberpunkové literatury zkusili domyslet některé z trendů současné kultury, v níž technologie hrají primární roli a přemíra různých informací i životních stylů „v důsledku vede ke konci sociálna jako významného referenčního bodu" [F02]. Při vytváření takového pohledu na kulturu měly nemalý podíl právě různé městské subkultury, včetně punku. Součástí Gibsonových románů a povídek jsou subkultury, které stále vzbuzují představu určitého vyloučení ze společnosti a technologii používají ke svým vlastním účelům. Přitom si jednotlivé prvky technologie přizpůsobí a obdaří je novým významem, což je manipulace reality připisovaná zejména punkovému hnutí. V Neuromancerovi vystupuje „Panther Moderns", technologicky velmi vyspělá subkultura mladých, v níž hlavní roli sehrává změna „image" zahrnující využití mikroelektronických implantátů a biokosmetických úprav vzhledu. Nově získaným zjevem dráždí hlavního protagonistu, počítačového maniaka Casea. V kyberpunku se vyskytují i subkultury protestující, např. Zionité v Neuromancerovi, skupina vykazující známky rastafariánství[5] a považující kyberprostor dat za „Babylón". Jinou skupinou jsou LoTekové[6] z povídky 'Johny Mnemonic', kteří si vytvářejí alternativní životní prostor nad městem.

Kyberpunk ovšem nezobrazuje pouze všezahrnující, vysoce estetizovaný a technologizovaný svět, proti němuž nelze revoltovat. Naopak, k punkovým rysům lze počítat i protest či alespoň pobuřující, znepokojující rebelii prostřednictvím označování vlastního těla a jeho vzhledu. Někteří autoři [M01] nacházejí v kyberpunku množství aktivit zaměřených proti „Korporaci", a lze říci, že kyberpunková snaha rebelovat proti centralizované moci a nadnárodním „zadržovatelům informací" je předznamenáním generace bytostně s technologií spjaté – generace hackerů a crackerů na Internetu.

[5] Rastafariánství je kultovní směr úzce spjatý s reggae a marihuanou. Jeho vyznavači se vnějškově vyznačují účesem z dlouhých zacuchaných copánků – dreadlocks a oblečením v barvách červená-žlutá-zelená. Rozmohlo se zejména na Jamajce, kde žije asi 100.000 rastafariánů. Rastafariánství v 70. letech proslavil především reggae zpěvák Bob Marley.

[6] Pravděpodobně vytvořeno od „low technology" jako výraz opozice vůči „hi-tech".

2.

Pět problémů kybernality

Kybernetickou kriminalitou, neboli **kybernalitou**, rozumíme takovou činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti. Tato kriminalita může být namířena přímo proti počítačům, jejich hardwaru, softwaru, datům, sítím apod., nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízení jsou prostředím, v němž se taková činnost odehrává. Obtížnost sledování projevů kybernality spočívá v tom, že se odehrávají v prostředí, jenž je objektivně pouze velmi obtížně vnímatelné. Dění v tomto prostředí můžeme pozorovat pouze pomocí strojů a přístrojů, které nám přístup do kyberprostoru umožní. Útočník, nebo pachatel pracuje v globálním prostředí, může se v kyberprostoru velmi rychle a nepozorovatelně pohybovat, měnit identity nebo i mizet. Může vytvářet, předstírat nebo realizovat různé hrozby a vždy bude o krok napřed. Může využívat variability předpisů v různých jurisdikcích nebo nedostatků ve vyšetřovacím procesu.

Studium kybernality je velmi široká mezioborová disciplína a nevztahuje se jen na úzký okruh trestných nebo nemorálních činů. Podobně, jako třeba organizovaná kriminalita nebo násilná trestná činnost, zahrnuje i kybernalita mnoho různorodých oblastí, které se mohou vzájemně prolínat. Proto není snadné ji jednoduše a jednoznačně kategorizovat a možných kriterií pro její klasifikaci najdeme celou řadu. Můžeme např. vycházet z dělení podle role,

jakou hraje výpočetní technika při páchání trestné činnosti nebo způsobu, kterým se projeví vzniklá škoda, podle motivu pachatele nebo podle jeho vztahu k poškozenému apod.

Všechny skupiny kriminálních činů, ať už v běžném životě nebo v kyberprostoru, jsou společensky nebezpečné a představují pro společnost hrozby. Latentní nebezpečí kybernetických hrozeb spočívá zejména v tom, že jejich aktivity nejsou viditelné a konečné důsledky nejsou s průběhem páchaného trestného činu viditelně spjaty.

2.1 Problém první – hrozby

Informační systémy jsou používány nejenom pro správu informací a práci s nimi, ale i pro řízení a správu jiných systémů. Součástí každého informačního systému je nejenom hardware, software a vlastní data, ale také lidé, kteří informační systémy provozují a spravují. Z hlediska bezpečnosti mají informační systémy zpravidla zajišťovat utajení chráněných dat, jejich dosažitelnost pro autorizované subjekty a jejich integritu. Dalšími prvky bezpečnosti může být třeba nepopiratelnost provedené operace s daty nebo vzniku datové či programové jednotky, její autentičnost nebo pseudonymita[1] či anonymita autora.

Proti informačnímu systému může být veden útok, jehož důsledky v případě úspěchu závisejí na povaze tohoto systému. Výsledný efekt útoku se může v lepším případě projevit jako drobné nepříjemnosti působené uživatelům, v horším případě může dojít i k velkým finančním ztrátám nebo výpadkům životně důležitých funkcí společnosti. V praxi může porušení dostupnosti znamenat například krátkodobý výpadek webové stránky, nemožnost dostat se ke schránce elektronické pošty, ale i výpadek dodávky elektrického proudu v postižené oblasti nebo zasažení jiného energetického zdroje. Ztráta utajení umožní útočníkovi číst vaší elektronickou poštu, seznam vašich kontaktů nebo čísla bankovních účtů. Porušení integrity se neobejde bez ztráty nebo náročného obnovování poškozených dat a pokud systém autorizuje útočníka k podání platebního příkazu cizím jménem, může oběť přijít i o významnou finanční částku. Podaří-li se útočníkovi nepozorovaný průnik do systému a následující modifikace samotného informačního systému, může ho nepozorovaně zneužívat dlouhou dobu.

Pravděpodobnost úspěšného útoku lze snížit lepší ochranou systému, ale každá ochrana znamená vynaložení finanční částky bez okamžitě viditelného efektu. Žádný informační systém není absolutně bezpečný a při návrhu ochrany informačního systému je nutno si uvědomit, že cena chráněných objektů také nemusí být stejná pro vlastníka informace a pro útočníka. Zvyšování zabezpečení bez znalosti ceny chráněných aktiv[2] může být od určité úrovně výš ekonomicky neúnosné. Proto je nutno pochopit význam rizik a hrozeb v souvislosti s chráněnými informacemi a informačními systémy.

Pod označením **hrozba** můžeme chápat cokoliv, co nějakým způsobem může vést k nežádoucí změně informace, chování systému nebo ovlivnit jeho parametrů. Sem je možno zahrnout osoby, prostředky, události nebo i myšlenky, které představují nějaké potenciální narušení důvěrnosti, integrity, dostupnosti nebo legálnosti použití systému. **Útok** je faktickou realizací hrozby. **Ochranou** pak rozumíme veškeré fyzické mechanismy, definované politiky nebo procesy, které mají sloužit k ochraně systému nebo obecně majetku před hrozbou nebo útokem. Každá ochrana se však vyznačuje zranitelností, což jsou většinou slabá místa ochrany nebo její úplná absence.

[1] Pseudonymita je chápána jako schopnost dokázat souhlasnou totožnost původu datových nebo jiných informačních jednotek bez odhalení skutečné totožnosti jejího autora.

[2] Chráněná aktiva mohou být nejenom fyzické předměty, ale i např. know-how nebo informace o těchto aktivech, popř. informace k informacím o aktivech vedoucí.

Velmi důležitým momentem je již zmíněné **riziko**, jehož míru můžeme vztáhnout k hodnotě chráněného majetku v případě, že dojde k úspěšnému útoku ve zranitelném místě systému. Riziko bude vysoké, když hodnota chráněného majetku je vysoká a existuje velká pravděpodobnost úspěšného útoku. Naopak, riziko bude malé, pokud hodnota chráněného majetku bude nízká nebo bude malá pravděpodobnost úspěšného útoku. Metody vyhodnocení rizik jsou pokryty analýzou rizik, která obvykle předchází formulaci bezpečnostní politiky, a jejím výsledkem jsou kvantifikace nákladů na opatření pro ochranu ve vztahu k hodnotě chráněného majetku.

Hrozby mohou být klasifikovány jako **úmyslné**, tedy např. průnik útočníka do systému, a **neúmyslné**, kdy ohrožení systému vzniká chybou operátora, uživatele nebo samotného systému[3]. Úmyslné hrozby můžeme dále rozdělit na hrozby **pasivní** a hrozby **aktivní**. Příkladem pasivní hrozby je monitorování provozu, při kterém je zjišťován obsah předávaných informací, aniž by byl měněn. Útok, což je vlastně realizace aktivní hrozby, zahrnuje změnu přenášené informace, např. částky při finanční transakci. K uskutečnění hrozby přitom nemusí nutně docházet jenom při komunikaci mezi dvěma subjekty prostřednictvím sítě, může to být i změna informace na médiu, které je součástí napadeného systému.

2.1.1 Taxonomie hrozby

Nedá se říci, že by v současné době existovala nějaká univerzální taxonomie hrozeb, neboť jejich existence a význam se mění podle prostředí ve kterém ohrožený proces probíhá. Abychom však byli schopni popsat roli bezpečnostních prvků systémů v počítačové síti a zejména veškeré entity s hrozbou spojené, pokusme se shrnout některé základní rysy hrozeb do tří velkých skupin – základní hrozby, aktivační hrozby a podkladové hrozby.

Základní hrozby

Můžeme rozeznat čtyři skupiny **základních hrozeb**, které odrážejí čtyři hlediska bezpečnosti informačního systému:

- ✓ **Únik informace**, neboli případ, kdy informace důvěrného charakteru je prozrazena neautorizovanému subjektu nebo je jím odhalena. Únik informace pak může vést k přímým útokům se značným dopadem.
- ✓ **Narušení integrity** zahrnuje porušení konzistence dat, kdy může dojít k vytvoření nových dat či změně nebo vymazání stávajících dat neautorizovaným subjektem.
- ✓ **Potlačení služby**, ke kterému dochází v případě, kdy je úmyslně bráněno přístupu legitimního subjektu k informacím nebo jiným systémovým zdrojům. Příkladem jsou známé útoky DoS[4], kdy úmyslné vytvoření vysoké zátěže zdroje nelegitimními a jalovým žádostmi vede k neúspěšným pokusům o přístup legitimních subjektů.
- ✓ **Nelegitimní použití** znamená, že zdroj je používán neautorizovaným subjektem nebo neadekvátním způsobem. Příkladem může být průnik do systému a používání placených služeb aniž by docházelo k faktickému vyúčtování a zaplacení služby.

[3] Na tomto místě je nutno upozornit, že pojem úmyslnosti a neúmyslnosti je nutno chápat spíše ve smyslu sémantickém než čistě ve smyslu trestního zákona, i když obě pojetí mají velmi blízko.

[4] DoS – Denial of Service, způsob útoku v distribuovaném informačním systému, kdy jsou přenosové kanály zahlceny záplavou jalových informací generovaných útočníkem, což v důsledku vede k nedostupnosti informačních zdrojů.

Aktivační hrozby

Význam aktivačních hrozeb spočívá v tom, že jejich realizace vede k bezprostřednímu vytvoření základní hrozby, a tak i k přímému ohrožení bezpečnostních parametrů systému. Odtud také plyne jejich název neboť aktivují základní hrozby. Jejich rozdělení je následující:

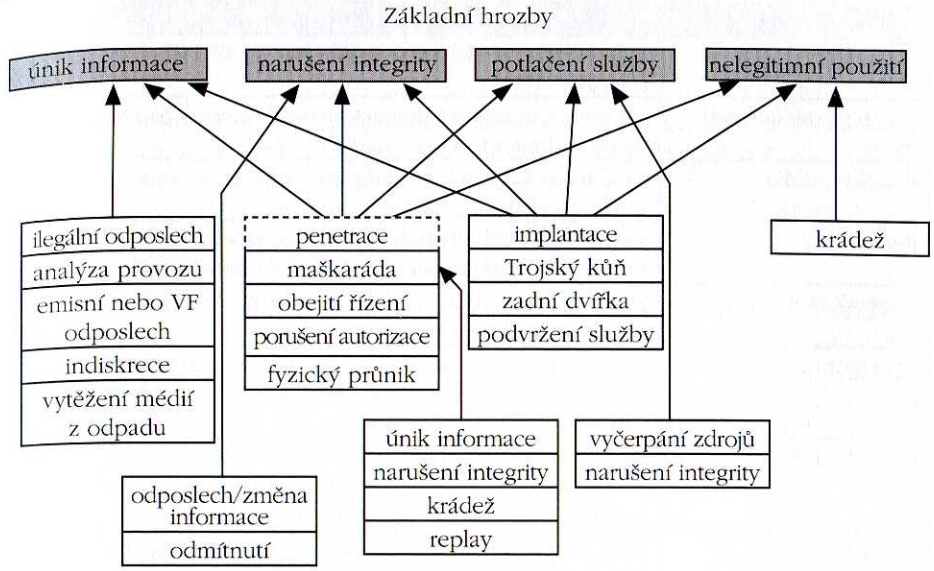
konec ma

- ✓ Penetrační hrozby:
  - ✓ ***Maškaráda*** – *případ, kdy se jedna entita (osoba nebo systém) vydává za jinou entitu. Toto je jeden z nejběžnějších způsobů narušení bezpečnostního perimetru systému, např. „login" perimetru. Neautorizovaná entita v tomto případě „přesvědčí" příslušný ochranný systém o tom, že je odpovídající autorizovaná entita a tak využívá všech práv a privilegií oné fiktivní autorizované entity. Hackeři používají maškarádu velmi často a slaví tak nejeden úspěch.*
  - ✓ ***Obejití řízení*** – *v tomto případě útočník využije systémové nebo bezpečnostní slabiny k získání neautorizovaných práv nebo privilegií.*
  - ✓ ***Narušení autorizace*** *spočívá ve zneužití autorizovaného přístupu ke zdroji pro neautorizované účely. Takový útok musí být veden zevnitř systému uživatelem, který má k danému zdroji přístup a nejedná se ani tak o selhání systémové jako o selhání personální.*
- ✓ Implantační hrozby:
  - ✓ ***Trojský kůň*** *je historicky nejběžnějším případem vložené hrozby, kdy software obsahuje neviditelnou nebo při běžném provozu nepozorovatelnou část, která po spuštění naruší bezpečnostní prvky systému. Příkladem může být např. program, který podporuje běžnou činnost uživatele, např. textový editor, ale přitom umožňuje uložení informací o aktivitách uživatele, např. text, který uživatel napsal, ukládá do skryté části systému, odkud mohou být tyto informace vyzdviženy autorem trojského koně. Existuje celá řada programů, které, staženy z internetu, poskytují jednoduché služby. Přitom však implantují „trojského koně", který odesílá informace o aktivitách uživatele na předem stanovenou internetovou adresu.*
  - ✓ ***Zadní vrátka*** *je část systémového software, která umožňuje při poskytnutí specifického datového řetězce na svůj vstup, obejít nástroje bezpečnostní politiky systému. Příkladem může být systém přihlašování uživatelů (login), kdy pro specifický identifikátor uživatele jsou vynechány všechny běžné kontroly hesel.*

Implantační hrozby jsou obvykle probouzeny autory až po nějaké době, kdy implantovaná součást software ležela v systému již dostatečně dlouho a případný „implantátor" je mimo podezření nebo dosah.

Podkladové hrozby

Analyzujeme-li základní a aktivační hrozby v nějakém systémovém prostředí, můžeme identifikovat některé hrozby, které mohou vést k realizaci i několika základních hrozeb. Např. budeme-li uvažovat o úniku informací, jako o základní hrozbě, pak můžeme najít několik hrozeb, které mohou vést k realizaci úniku informace – tajný odposlech, analýza komunikačního provozu nebo indiskrece zaměstnance. Takovým hrozbám, které jsou pokladem pro realizaci až několika základních hrozeb říkáme podkladové hrozby. Vztah mezi základními hrozbami a podkladovými hrozbami ukazuje obr. 2.1, popis jednotlivých hrozeb je v tab. 2.1.



Obr. 2.1: *Vztah základních a podkladových hrozeb*

Skutečnost takových hrozeb dokazuje např. statistika doložená v [N01], která vychází z více než 3.000 případů zneužití počítačového systému. Mezi nejčastější hrozby patří, seřazeno od nejvyšší četnosti výskytu, porušení autorizace, maškaráda, obejití řízení, Trojský kůň, zadní vrátka a vytěžování odpadových médií.

Hrozba	Popis
Porušení autorizace	Osoba, která je autorizována k použití zdroje pro jistý účel jej použije k jinému, neautorizovanému účelu.
Obejití řízení	Útočník využije bezpečnostních mezer v systému nebo jeho slabin.
Potlačení služby	Omezení legitimního přístupu k informacím nebo jiným zdrojům v síti.
Nezákonný odposlech	Informace je získávána monitorováním přenosového kanálu.
Emisní nebo VF odposlech	Informace je extrahována z vysokofrekvenčního vyzařování nebo emisí či jiných elektromagnetických jevů, ke kterým dochází při provozu elektronického zařízení.
Nelegitimní použití	Zdroj je používán neautorizovanou osobou nebo neautorizovaným způsobem.
Indiskrece	Autorizovaná osoba prozradí důvěrnou informaci neautorizované osobě z neopatrnosti nebo za úplatu.
Únik informace	Získání důvěrné informace neautorizovanou osobou nebo systémem.
Narušení integrity	Konzistence dat je narušena jejich neautorizovaným vytvořením, úpravou nebo vymazáním.
Změna dat při přenosu	Přenášená data jsou během přenosu informačním kanálem změněna, odstraněna nebo zcela vyměněna.

konecma

Hrozba	Popis
Maškaráda	Jedna entita (osoba nebo systém) se představuje jako jiná entita.
Vytěžení odpadových médií	Informace je získávána z magnetických nebo papírových médií, vyhozených do odpadu.
Fyzický průnik	Útočník získá kontrolu na systémem proniknutím k jeho ovládacím prvkům.
Replay	Zachycená kopie legitimní transakce je využita pro opětovný přenos s nelegitimním úmyslem.
Popření skutečnosti	Strana zúčastněná ve vzájemné komunikaci později popře, že k takové komunikaci došlo.
Vyčerpání zdrojů	Jistý zdroj, např. port, je úmyslně natolik zatížen, že je znemožněno používání služby, která je na něj vázána, řádnými uživateli.
Podvržení služby	Podvržený systém nebo systémová komponenta, které se vůči uživatelovi chovají jako běžná součást systému, slouží k získání citlivých informací od důvěřivého uživatele.
Krádež	Kritický prvek bezpečnostního systému (např. přístupová karta) nebo veškerá citlivá informace jsou zcizeny.
Analýza provozu	Informace je neautorizovanou entitou získána pomocí sledování provozu a výběrem podstatných jeho částí.
Zadní vrátka	Do systému je zabudována vlastnost nebo vložena součást, která při jisté konstelaci vstupních dat umožní obejít bezpečnostní mechanismy.
Trojský kůň	Software obsahuje zdánlivě nevinnou nebo neviditelnou část kódu, který – pakliže je spuštěn – ohrozí bezpečnost uživatele.

Tab. 2.1: *Typické hrozby*

I když se zdá, že výčet v tabulce není úplný, zahrnuje všechny známé způsoby útoku, nezahrnuje však jejich metody. To znamená, že např. viry nebo červi současně patří do kategorie „obejití řízení" a „maškarády" a jsou jen realizací této kombinované formy útoku. Na druhou stranu, některé z uvedených útoků mohou vyžadovat další podpůrné informace, např. maškaráda předpokládá buď indiskreci či jiný způsob získání hesla.

2.1.2 Charakter hrozby a její cíl

Charakter hrozby i cíl hrozby jsou dány motivací a zkušenostmi pachatele. Jsou spolu úzce svázány a lze očekávat, že volba typu hrozby bude adekvátní jejímu cíli. Při uvažování proti komu nebo kam může být hrozba směrována není možno předpokládat nějakou loajalitu vůči státu nebo národu. Již svým globálním charakterem je kybernetická hrozba oddělena od reálného prostředí a teritoriálního pojetí, a tedy jsou narušeny i vazby na konkrétní národnostní vědomí nebo na obavy z dopadu „státní" ruky zákona.

Je zřejmé, že hrozba může mít dva základní stavy:

- ✓ zastrašovací moment, kdy potenciální hrozba formulovaná útočníkem není dokonána a k dosažení kýženého efektu u cíle má samotné vyjádření hrozby postačující efekt,
- ✓ realizace hrozby, kdy se útočník nespokojí s formulací hrozby vůči cíli a hrozbu uskuteční, nebo se ani s formulací hrozby neobtěžuje a provede ji bez předběžného ohlášení.

Základní vlastnost hrozby snadno přejít do fáze, kdy je schopna zasáhnout cíl, narušit ho nebo jej i zničit, je evidentní. U kybernetické hrozby je to zejména její „mystický" ráz, kdy útočník využívá virtuální povahy a složitosti kyberprostoru, umocněné v mnoha případech neznalostí nebo neinformovaností napadeného. Kybernetickou hrozbu je obtížné bez specifických znalostí a možností vysledovat, zadržet nebo ovládnout. Přitom se může jednat i o hrozbu, kterou útočník není ani schopen uskutečnit[5].

Cíl a charakter hrozby je ve velké míře dán motivem pachatele nebo útočníka a variabilita motivací je značná. Mezi časté autory hrozeb patří zejména extrémistické etnické nebo náboženské skupiny. Hrozby mohou být určeny lokálnímu cíli, ale často mívají transnacionální charakter zejména tam, kde jsou jejich autory globální skupiny. Tyto aktivity nemají nějaké specifické zaměření a lze je nalézt ve všech sférách – bezpečnostních, náboženských, obchodních apod.

2.2 Problém druhý – legislativa

Jedním ze základních problémů legislativy v oblasti kybernetických trestných činů je vlastní definice kybernality, která se neustále mění s vývojem technologií a změnami charakteru informačních systémů. Obecně je však možno pod pojmem kybernetická kriminalita chápat páchání trestné činnosti, v níž je aktivní složkou informační technologie jako souhrn technického a programového vybavení včetně dat. V mezinárodním společenství se pro tento typ kriminality ustálily pojmy „Cyber-Crime" nebo „high-tech crime".

V oblasti trestního práva došlo k jistým pokusům o vymezení, kdy se jako kybernalita nechápe taková trestná činnost, která je zaměřená na techniku jako objekt zájmu pachatele majetkového trestného činu (například krádež počítače). Přesto často dochází k situacím, kdy je výpočetní a jiná technika objektem zájmu ryze „kybernetického" trestného činu, ale současné poškození této techniky vede k souběhu s majetkovým trestným činem.

Platné právní normy nejsou schopny tyto nové zločiny zcela jasně a taxativně vyjmenovat a proto je většina soudních řízení spjata s legislativní vágností. Jediným možným řešením za současného stavu je použití institutu přípustné analogie – tedy aplikace právních norem postihující delikty s podobnými charakteristikami. Míra přípustnosti, tak jak ji chápe trestní zákon, je však velmi omezená, a tak některé analogie není možno s ohledem na přesnost vyjádření v zákoně použít.

Budeme-li se zabývat pohledem na situaci ve světě, pak zjistíme, že některé státy nemají v této oblasti zákony žádné nebo se existující zákony výrazně liší v jednotlivých jurisdikcích. Činnost, která je v jedné zemi trestná, nemusí být v druhé zemi vůbec zahrnuta do legislativy nebo může být legální. Při globálním rozměru kybernality se pro řešení vzniklé škody nedostává potřebných nástrojů. Navíc, mimo nedostatek zákonných norem, existuje nedostatek zákonných precedentů nebo judikátů.

Zdálo by se, že státy, které zákony pro oblast kybernality, jsou na tom jsou lépe. Ale ani to není pravdou. Vzhledem k obtížnosti definice kybernetického trestného činu, jeho nejasně definovaných mezí a obtížnosti v jeho dokazování, dochází často k beztrestnosti jinak zřejmě

[5] Případ, kdy útočník vyhrožuje např. vymazáním důležitých souborů ještě neznamená, že je toho schopen. K tomu, aby takovou hrozbu mohl uskutečnit musí nejdříve do systému proniknout a získat potřebná práva. A to není lehká úloha. Záleží nyní na tom, jak dokáže ohrožovaná strana vyhodnotit potenciál útočníka v poměru ke svým bezpečnostním opatřením a stavu ochrany svého systému.

nelegitimního chování pachatelů. Existují rozsáhlé mezinárodní aktivity, které se snaží o bližší specifikaci kybernetických trestných činů a o koordinaci mezi jednotlivými státy. Tyto aktivity sice vedly k návrhu mezinárodní smlouvy [E14], avšak celý proces je velmi pomalý.

konecma

Mezi rozhodující činitele ovlivňující legislativní proces lze zařadit vlastní vůli zákonodárců daný stav změnit, jejich odpovídající vzdělání a schopnost porozumět problému a v neposlední řadě též rychlost legislativního procesu. Pro jednoduchost ignorujme první faktor a předpokládejme, že zákonodárné sbory mají vůli situaci řešit. Zbylé dva faktory si zaslouží podrobnější rozbor.

Předpoklad, že mezi jmenovanými činiteli existuje skutečný odborník na problematiku kybernality, je velmi optimistický, avšak tento fakt sám o sobě nemusí být překážkou. Dle liberálně pojaté teorie má být stát jen tvůrcem pravidel a rozhodčím, dohlížejícím na jejich dodržování. Samotná pravidla hry si však mají zvolit její účastníci, tedy občané a firmy. Aby vše fungovalo správně, musíme se smířit s faktem, že odborníci, kteří působí jako poradci zákonodárců na všech úrovních, budou reprezentovat výše uvedené skupiny. Otazníkem ovšem je, zda tito poradci skutečně budou hájit obecné zájmy, nebo zájmy vybrané zájmové skupiny. Totéž samozřejmě platí o politicích, kteří v konečné fázi zákony schvalují.

Rychlost legislativního procesu nelze téměř žádným způsobem ovlivnit. Obsah zákonných norem mohou odborní poradci jistým způsobem korigovat, ale rychlost samotného procesu je plně v rukou politiků. O legislativním procesu každého státu lze tvrdit, že by měl být rychlejší a nemá tedy cenu si jeho průběh idealizovat. Je asi rozumnější současný stav přijmout a spokojit se s ním. Co jistě stojí za zlepšení je kvalita navrhovaných zákonů. Schválení každého nového zákona trvá dlouhou dobu, a proto každá chyba, nedokonalost či vyložená hloupost ve schválené normě bolí několikanásobně. Jednou když musíte podle těchto nedokonalostí jednat, podruhé vzhledem k potřebě tuto normu novelizovat a potřetí, když je nutno znovu absolvovat vyčerpávající schvalovací postup.

Snad největším nepřítelem kvalitních zákonů v České republice je možnost poslaneckých návrhů úprav do zákona, které jsou často prosazovány lobbisty prostřednictví některého poslance. Příprava zákona je velmi odborná záležitost, a proto by „amatéři", jimiž poslanci ve velké míře jsou, neměli mít možnost zákon v detailech měnit. Moudré se jeví ustanovení prvorepublikového parlamentu, který mohl předložený zákon pouze jako celek schválit nebo jako celek odmítnout. Tak byla zajištěna smysluplnost zákona a jeho potřebná odborná úroveň.

Onu reálnost a vztah ke skutečným problémům by měly zajistit konzultace s odbornými poradci z praxe – v oblasti právních norem týkajících se kybernality by toto mělo být naprostou samozřejmostí. Budou-li tedy zákonodárci schvalovat skutečně kvalitní zákony, není ona rychlost legislativního procesu natolik bolestná a omezující. Sníží-li se počet nutných novelizací, bude právní stav přehlednější pro občany i firmy a zákonodárcům bude umožněno pracovat na nových normách namísto novelizace stávajících, nedokonalých.

2.3 Problém třetí – policie a justice

Kybernalita, jako trestná činnost, je páchána s použitím velmi specifických technologických nástrojů a specializovaných znalostí. K jejímu odhalení a prokázání je tedy opět třeba velmi speciálních nástrojů, znalostí a postupů. A to je právě jeden z hlavních problémů policie a justice – nedostatek vysoce kvalifikovaných pracovníků, kteří by byli schopni zvládnout problematiku kybernality nejenom po stránce technologické, ale i po stránce právní a po-

[6] Abychom byli objektivní, snahy o přizpůsobení struktury policie stále rostoucímu počtu technologicky založených nebo podporovaných trestných činů existují, nicméně je to proces dlouhodobý a finančně náročný – viz např. [H09] .

licejní praxe[6]. Mimo to, policie se musí vyrovnat i s tím, že klasické vyšetřovací metody selhávají. Je to zejména dáno odlišným charakterem stop v kyberprostoru, jejich trvanlivostí a použitelností v důkazním řízením.

Zatímco stopy klasického trestného činu je možno zajistit ještě několik hodin nebo dnů po činu[7], v případě kybernality je zajištění stop otázkou minut. Trestný čin se odehrává ve složitém technologickém prostředí, jehož stav se každou sekundou mění. Navíc, toto prostředí podléhá rychlému technologickému vývoji, a tak spektrum kybernetických trestných činů podléhá technologickým trendům, velmi rychle se rozvíjí a modifikuje. Současná rychlost vyšetřovacího procesu neodpovídá technologickým trendům.

Obdobným problémem jako policie trpí i justice. Přestože je většina projevů kybernality trestná, není vždy snadné takovou činnost odhalit, dokázat a pachatele odsoudit. Kromě běžných problémů nepomáhá jistě soudnímu řízení ani fakt, že soudci jsou specialisty na právo, nikoliv na informační technologie, takže v odborných případech musí využívat soudní znalce a spoléhat na ně. Nedostatek kvalifikovaného soudního personálu a soudců, kteří by byli schopni orientace ve složité struktuře kyberzločinu, nepřispívá ke kvalitě soudního řízení v případech, kdy je projednáván kybernetický trestný čin. K tomu přispívá i nedostatek kvalitních znalců a znaleckých ústavů schopných provést i elementární forenzní zkoumání zabaveného počítače nebo jiné, řádně dokumentované důkazní postupy[8]. Pomalost procesních postupů může vést i ke ztrátě důkazů, které bezprostředně po spáchání trestného činu existovaly, avšak dlouhé administrativní řízení neumožnilo jejich řádné zajištění. Pomalost soudního procesu je tak jedním z největších problémů patřících do třetí skupiny.

Na tomto místě je vhodné vzpomenout i skutečnost související s posuzováním obsahu internetu. Často je internet prezentován jako „nejdemokratičtější médium". I když, dotaženo do úrovně definic, je těžko si pod tímto označením představit původní záměr autora tohoto výroku, můžeme jej pro tento okamžik chápat tak, že vyjádření jakékoliv myšlenky nebo názoru na internetových stránkách není nijak kontrolováno nebo omezováno politickými či mocenskými strukturami[9]. Nicméně, pokud nebudeme zaměňovat demokracii s anarchií, pak je nutno si uvědomit, že existují jisté meze svobody projevu, které by měly stanovit jaký obsah je ještě svobodným projevem a jaký již ne [H01]. Právě toto rozhodnutí je často zásadním pro posuzování stránek s tzv. extremistickým obsahem.

Základním hlediskem pro posouzení je omezení práva na svobodu projevu, jenž je zaručeno jen do té míry, aby nepoškozovalo práva ostatních. Při posuzování trestných činů souvisejících s překročením mezí svobody projevu je nutno si uvědomit, že se nemůže jednat o nedbalostní trestný čin. K naplnění jeho skutkové podstaty je vždy nutný úmysl pachatele. Z toho lze usoudit, že trestně odpovědný za takové trestné činy je ten, kdo podobné projevy veřejně publikuje, nikoliv správce nebo vlastník serveru, kde se takový projev objeví[10].

[7] Samozřejmě záleží na prostředí, ve kterém se trestný čin stal a na charakteru zajišťované stopy.

[8] Je nutno si uvědomit, že nesmírně stoupá množství počítačů předložených k forenzní analýze. Dnes téměř při každé domovní prohlídce je zabaven počítač, někdy i několik počítačů. Při kapacitě magnetických médií současných personálních počítačů je důkladná forenzní analýza počítače časově náročným úkolem, a tak formulace zadání pro znalce: „Najděte něco související s případem ...", je zcela nepostačující.

[9] To není zcela pravdivé. Existují země s poměrně přísně regulovaným a sledovaným obsahem internetových stránek, které je doplněno řízením a monitorováním přístupu uživatelů k internetovým adresám mimo sledované teritorium.

[10] Tedy pokud nebyl tento text vložen na webové stránky umístěné na serveru s jeho vědomím nebo pokud o tom prokazatelně musel vědět. Nicméně tato beztrestnost trvá do okamžiku, kdy se o takovém stavu dozví a má možnost zjednat nápravu.

2.3.1 Praxe v České republice

V českých novinách a na internetu je často používán termín "softwarová policie", tedy policejního útvaru specializovaného na vyhledávání a vyšetřování trestných činů souvisejících s porušováním autorských práv[11]. Softwarová policie však ve skutečnosti neexistovala a zkoumání kybernetické trestné činnosti se na počátku 90. let omezovalo pouze na znalecká zkoumání v Kriminalistickém ústavu Praha. V roce 1998 vzniklo pod patronací Policejního prezidia PČR a Úřadu služby kriminální policie a vyšetřování (ÚSKPV) oddělení informační kriminality, které bylo operační a vyšetřovací složkou. Náplní práce oddělení bylo zpočátku softwarové pirátství, ale postupně byla tato problematika přenesena na základní útvary služby kriminální policie a uvedený policejní útvar plní spíše koordinační a informační funkci.

Na začátku roku 2006 došlo ke změně struktury a vzniklo nové pojetí oddělení informační kriminality. Předpokládá se vytvoření specializovaných míst operativních detektivů na útvarech s republikovou působností a současně na jednotlivých krajských správách PČR. Jako první vzniklo 1. května 2005 pracoviště na PČR, Správě hl. m. Prahy [A01]. Oddělení informační kriminality má za úkol odhalovat, vyšetřovat a monitorovat trestnou činnost, zajišťovat důkazní materiály na Internetu a zajišťovat servisní činnost a podporu útvarům kriminální policie. Běžný postup je takový, že oddělení předává své poznatky dále k šetření podle věcné a místní příslušnosti. Pouze v náročných případech provádí tento útvar vyšetřování sám.

Hlavní zaměření oddělení informační kriminality je softwarové pirátství a kriminalita na internetu. Z policejních statistik však vyplývá, že policie není v odhalování nelegálního šíření programů moc úspěšná [A01]. Pokles počtu odhalených případů z 1.688 v roce 2001 na 418 případů v roce 2004 prudce kontrastuje s výroční zprávou Business Software Alliance pro rok 2004, která konstatuje nárůst podílu nelegálně držených programů v České republice na 41% oproti 40% v roce 2003 [B01]. Mimo softwarového pirátství se oddělení informační kriminality zabývá zejména:

- ✓ sledováním zakázané pornografie, zvláště pak odhalováním organizovaných skupin, které na internetu distribuují pedofilní či zoofilní materiály,
- ✓ extremistickými projevy, monitorováním stránek s fašistickým, ekoradikalistickým a podobným obsahem,
- ✓ zneužíváním platebních a obchodních systémů a vyšetřováním podvodných případů v obchodně platební činnosti,
- ✓ vyšetřováním pomluv, výhrůžek a šíření poplašných zpráv na internetu[12].

Samotní policisté přiznávají, že jejich vybavení i možnosti pokulhávají nejen za lidmi, kteří páchají trestnou činnost, ale i za jejich západoevropskými kolegy. Přesto se policie může pochlubit určitými úspěchy, jako je například v roce 2004 odhalení ostravského mladíka, který elektronickou poštou vyhrožoval bombovým útokem. Policie však bude vždy o několik kroků pozadu za nelegálními činnostmi na internetu, pokud nedojde k výraznému zákonnému omezení svobod občanů. Zdá se však, že trend nastoupený v posledních letech povede k odhalování alespoň těch nejzávažnějších deliktů.

[11] Jedná se o trestný čin podle §152 Trestního zákona, kde skutková podstata je definována jako neoprávněný zásah do zákonem chráněných práv k autorskému dílu, kam patří i programové dílo v jakékoli podobě, nebo databáze.

[12] V březnu roku 2005 padl první trest za tyto trestné činy. Petr Partyk byl nepodmíněně odsouzen k trestu odnětí svobody za pomluvu obecního úředníka na veřejném diskusním fóru.

Naše justice je úspěšná především při odsuzování pachatelů, kteří porušují autorský zákon. Česká odnož organizace BSA[13] uvádí na svých internetových stránkách několik desítek obvinění či odsouzení občanů a firem, kteří tento zákon porušili. Nicméně většina těchto rozsudků se týká relativně nepatrných delikventů (viz. [B01]), tedy pachatelů, kteří způsobily softwarovým firmám škody v řádu desítky tisíc korun. Soudy jsou však ve většině případů závislé na tom, co jim předloží policie, což také do značné míry způsobuje jejich malou úspěšnost v případech, kde jde o jiný typ počítačové kriminality[14].

2.4 Problém čtvrtý – společnost

Vnímání počítačové kriminality společností je zatíženo nehmotným charakterem produktů a bezprostřední neviditelností následků trestného činu. Zatímco krádež počítače, tedy fyzického hardwaru, je vnímána jako běžný trestný čin, u věcí, které nemají hmotnou podstatu, se veřejné mínění přesouvá na druhou stranu barikády. Pachatel, který převede několik milionů z účtu svého zaměstnavatele na účet vlastní, je posuzován jinak, než kdyby přišel do banky s pistolí a peníze si vzal násilím. Společnost ho spíše považuje za šikovného a mazaného podvodníčka.

Tento stav je způsoben tzv. fenoménem zločinu „bílých límečků"[15], jenž je páchán úředníky, programátory, funkcionáři společností, a jenž se i přesto, že je společensky velmi nebezpečný a způsobuje značné finanční ztráty, odlišuje od klasické představy zločinu s jeho násilnou fyzickou podstatou. Softwarové pirátství je společností vnímáno ještě benevolentněji. Velká část občanů, kteří vlastní počítač, na něm má nainstalováno i nelegální programové vybavení a nepovažuje to za porušení zákona. Vždyť software není žádná hmotná věc a navíc jsou poškozovány firmy, které „mají peněz dost". Alarmující jsou výsledky nezávislého průzkumu společnosti Ipsos Public Affairs [E01], provedeného mezi 1 500 profesionály, z něhož vyplývá, že ačkoliv si 90 % z nich myslí, že softwarová kriminalita je „riziko, které si žádná firma nemůže dovolit podstoupit", tak 23 % jich přiznává, že některý software v jejich organizaci není licencován.

K obecně laxnímu postoji veřejnosti vede i značná neúspěšnost při vyšetřování a trestání kybernality. Tabulka 2.2 uvádí porovnání běžné ozbrojené bankovní loupeže s kybernetickým zločinem obdobného charakteru a vychází z dlouhodobých statistik amerického úřadu pro vyšetřování – FBI. Je evidentní, že kybernetický útok vede, pokud se podaří, k daleko většímu zisku pro pachatele. Pachatel zároveň neriskuje fyzické zranění a pravděpodobnost, že bude dopaden a odsouzen je minimální.

[13] Business Software Alliance (BSA) je organizace, která se podle svého vyjádření zabývá „prosazováním bezpečného a legálního digitálního světa". Vznikla v roce 1998 a působí v desítkách zemí světa.

[14] Případy postihu podle §152 TZ, t.j. porušování autorských práv, jsou nejjednoduššími případy kybernality, a to jak v hledání důkazních materiálů a prostředků, tak i ve sféře soudního projednávání. Při „marketingové kampani" prováděné BSA a držiteli autorských práv není divu, že se jedná o nejvíce zdůrazňovanou oblast kybernetické kriminality.

[15] Viz zejména [S01] a [P03].

konecma

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	pachatel riskuje, že bude zraněn nebo zabit	bez rizika fyzického zranění
Zisk	průměrně 3 až 5 tisíc USD	od 50 až do 500 tisíc USD
Pravděpodobnost dopadení	dopadeno 50 až 60 % útočníků	dopadeno cca 10 % útočníků
Pravděpodobnost odsouzení	odsouzeno 95 % dopadených útočníků	z dopadených útočníků dojde k soudnímu projednávání pouze u 15 % útočníků a z nich je skutečně odsouzeno jenom 50 %
Trest	průměrně 5 až 6 let, pokud pachatel někoho nezranil	průměrně 2 až 4 roky

Tab. 2.2: *Porovnání následků klasického a kybernetického trestného činu*

Základním aspektem ovlivňujícím stav kybernality je informatická vzdělanost a vybavenost společnosti. Krajními hypotetickými příklady jsou extrémní stavy společností, z nichž první intenzivně používá informatiku, avšak nevěnuje dostatečnou pozornost bezpečnosti a kybernetické ochraně. Druhá nepoužívá informatické technologie vůbec. Je zřejmé, že první uvedená společnost bude rájem pro kybernalitu, zatímco druhá bude z tohoto hlediska zcela bezpečná. Všechny reálné společnosti se však nacházejí někde uprostřed mezi těmito hypotetickými stavy a mezi paradoxní zjištění patří, že informovanost o bezpečnosti a možných útocích v takové společnosti nezáleží na stupni jejího hospodářského vývoje, ale je ve všech státech na relativně stejné úrovni.

Důvodem k tomuto zjištění je sama existence kybernetického prostoru a jeho charakter. Informace o útocích, a nezřídka i útoky samotné, se šíří v celém prostoru s nesmírnou rychlostí a sdílení informací o možných hrozbách a provedených útocích je relativně velmi jednoduché. Diferencujícím faktorem je v tomto případě legislativní připravenost společnosti a následující schopnost implementace legislativy represivními a justičními složkami. A zde se zdá být nemožné dojít k celosvětově srovnatelnému stavu. Hlavním důvodem je existence různých právních systémů, rozdílné chápání morálky a trestu dané historickým a kulturním vývojem jednotlivých národů a celá řada dalších omezujících vlivů.

Ke změně postoje veřejnosti ke kybernalitě je nezbytné obecné zvýšení počítačové gramotnosti a zlepšení informovanosti společnosti v této oblasti. Je nutno vysvětlovat, jak kybernalita vypadá, jaké má důsledky, jak je možno ji zjistit a jak ji lze trestat.

2.5 Problém pátý – chápání bezpečnosti

Většina běžných uživatelů důvěřuje počítačům a jejich výstupům možná více, než by bylo vhodné, a neuvědomuje si zcela otázku bezpečnosti. Některé společnosti si prostřednictvím nešifrovaných, prostých e-mailů posílají vyhrazené interní informace, které by je ani nenapadlo napsat třeba na korespondenční lístek. Uživatelé často volí příliš jednoduchá, snadno zapamatovatelná a snadno odhalitelná přístupová hesla k informačním systémům. Velké důvěře se těší i informační zdroje a programy volně dostupné prostřednictvím Internetu. Ty jsou zpravidla k dispozici pouze ve zkompilované podobě, takže uživatel nemá možnost včas zjistit, zda program opravdu dělá to, co je u něj napsáno. A navíc, uživatel zpravidla nemá vůbec zájem takové ověřování provádět.

Někdy až neuvěřitelná víra v pravdivost textů šířených e-mailem vede k šíření počítačových virů a červů, k jejichž aktivaci je třeba netriviální spolupráce[16], a hoaxů – nepravdivých poplašných zpráv[17]. Pravděpodobnou příčinou je nízká úroveň znalostí a zkušeností běžných uživatelů, z nichž mnozí umí právě tolik, aby mohli vykonávat na počítači svou práci, ale rizika s ní spojená si neuvědomují. Ve falešném pocitu bezpečnosti se utvrzují tím, že se zatím „ještě nikdy nic nestalo". Jsou tak zbytečně vystaveni hrozbě kybernetických útoků, ale například i ztráty vlastních dat, pokud např. stejným způsobem přistupují k jejich zálohování.

A pokud se „něco stane", nejčastěji to svádějí uživatelé na chybu v nekvalitním, děravém softwaru nebo ve špatném, nefunkčním antivirovém programu a nejsou ochotni přiznat souvislost bezpečnostního incidentu s vlastním chováním. Navíc, v případě většího incidentu, poškozená strana si zpravidla na útočníkovi nic nevezme, a to ani v případě, když se ho podaří najít a odsoudit. Jak bylo uvedeno v předcházející kapitole, alespoň částečným řešením této situace je vzdělání běžných uživatelů, počínaje výukou na základní škole a konče proškolováním na pracovišti. U velkých firem pak správce informačního systému musí najít tu optimální bezpečnostní konfiguraci systému, aby dovolil uživatelům pouze a právě jenom tolik, aby mohli dělat svojí práci.

Bezpečnost informačního systému je často chápána jako mezní technologický problém s jasně definovanými okrajovými podmínkami. To však v reálném světě neplatí. Konstrukce bezpečnostních prvků v ryze teoretické rovině vždy probíhá v ideálních matematických podmínkách. Poměrně složitými způsoby se dokazují síly šifer a jejich neprolomitelnost, a to vždy za předpokladu, že nepřítel nemá k dispozici extrémní výpočetní výkon. Matematici celého světa konstruují teoreticky velmi obtížné a, za současných podmínek, neřešitelné úlohy, které mají zajistit dostatečnou úroveň bezpečnosti. Bohužel, při následné implementaci těchto ryze teoretických mechanismů se objevují efekty, se kterými se při matematickém návrhu nepočítalo.

Učebnicovým příkladem těchto vedlejších efektů jsou tzv. postranní kanály. Vliv těchto postranních kanálů byl pozorován při pokusech o prolomení teoreticky velmi silných matematických šifer. Obvykle se při konstrukci šifry určí matematický postup a dokáže jeho dostatečná složitost, a to bez uvažování další implementace. A právě při implementaci vstupují do celého procesu např. hardwarové prvky a jejich fyzikální vlastnosti nebo vlastnosti přenášených zpráv. Experimentálně bylo např. zjištěno, že hardwarové jednotky, určené pro výpočet šifer, při své činnosti vyzařují jisté spektrum, které velmi silně koreluje s použitými klíči. Analýzou tohoto spektra bylo možné některé, ve své době bezpečné šifry, velmi rychle prolomit. Takové vedlejší fyzikální efekty se samozřejmě vymykají všem teoretickým modelům, se kterými matematici počítali.

Význam šifrování a utajování přenášených zpráv se často přeceňuje. I když se to zdá neuvěřitelné, tak např. pro policejní odposlechy tvoří obsah hovoru jen asi padesát procent vlastní zpravodajské informace. Žádné šifrování obsahu neskryje informaci o tom kdo volal, kdy volal a komu volal. Stejné je to i na internetu. Odeslaný mail můžeme šifrovat, ale odesilatele a adresáta není možné ukrýt[18].

[16] Typickým příkladem je pokyn „Rozbalte přiložený zip soubor a klikněte na dokument.exe". Přes jeho evidentně podezřelý význam je až příliš mnoho uživatelů, kteří uposlechnou.

[17] Mezi nejzajímavější hoaxy patří výzva „Najdete-li v adresáři WINDOWS soubor setdebug.exe, okamžitě ho smažte". Uživatel, který se poleká a uposlechne se jistě nepotáže s dobrou.

[18] Existují systémy umožňující anonymizované předávání zpráv, např. tzv. „Turtle Network", avšak zatím se v širší míře neprosadily.

3.

Kyberprostor a společnost

V úvodní kapitole jsme se snažili popsat vznik kyberprostoru jako nového fenoménu moderní společnosti. Role, kterou kyberprostor hraje, se od dob prvních představ posunula a současný internet s miliony připojených klientů a severů začal představu kyberprostoru realizovat.

Mezi základní vlastnosti kyberprostoru patří globální pokrytí, což je zcela evidentně u internetu splněno. Celková penetrace internetu se sice liší v jednotlivých oblastech světa, jak ukazuje tabulka. 3.1, ale dopady na chování společnosti jsou celosvětové.

konecma

Oblast	Počet obyvatel (odhad 2006)	Počet obyvatel v % celkové populace	Používání internetu (absolutně k červnu 2006)	Penetrace Internetu	Podíl na celkovém používání v %	Nárůst v letech 2000-2005
Afrika	915210928	14,1 %	23649000	2,6 %	2,3 %	423,9 %
Asie	3667774066	56,4 %	380400713	10,4 %	36,5 %	232,8 %
Evropa	807289020	12,4 %	294101844	36,4 %	28,2 %	179,8 %
Střední východ	190084161	2,9 %	18203500	9,6 %	1,7 %	454,2 %
Severní Amerika	331473276	5,1 %	227470713	68,6 %	21,8 %	110,4%
Jižní Amerika/ Karibské ostrovy	553908632	8,5 %	79962809	14,7 %	7,8 %	350,5 %
Oceánie / Austrálie	33956977	0,5 %	17872707	52,6 %	1,7 %	134,6 %
Svět celkem	6499697060	100,0 %	1043104886	16,0 %	100,0 %	189,0 %

Tab. 3.1: *Penetrace internetu*

Další důležitou vlastností kyberprostoru je jeho decentralizovanost. V internetu, se kterým se snažíme kyberprostor ztotožnit, také neexistuje žádná centrální autorita, která by o jeho existenci či neexistenci rozhodovala, či ho nějakým způsobem řídila. Fungování internetu je dáno dohodou jeho uživatelů a správců, kteří se svým jednáním přizpůsobují majoritní většině. Dochází tak k tomu, že je splněn další požadavek na kyberprostor – je řízen pouze svými uživateli.

Z povahy jeho řízení a používání plyne i otevřenost internetu, což patří rovněž mezi důležité vlastnosti kyberprostoru. Každý, kdo splní předepsaná kritéria se může připojit k internetu a tak se přesunout do kybernetického světa. I když toto připojení je poněkud jednodušší než popisuje Gibson[1], přesto je možno se v něm volně pohybovat, korespondovat s ostatními uživateli kyberprostoru, navazovat známosti nebo i jej zneužívat.

Otevřenost kyberprostoru vede k tomu, že se v něm vyskytuje nesmírné množství informací. Každý uživatel může v kyberprostoru uložit a prezentovat libovolné informace. Tyto informace nemohou být žádným způsobem redigovány, upravovány nebo cenzurovány, a tak se kyberprostor časem stává „smetištěm" informací, na kterém je možno najít všechno, ale určení významu nalezené informace se stává kruciálním problémem. Problém nalezení potřebné informace se v kyberprostoru přerodil do nové, daleko složitější, formy – problému evaluace nalezeného množství informací, vybrání správných resp. pravdivých informací a jejich odpovídající vyhodnocení.

Otevřenost kyberprostoru, potažmo internetu, spolu s jeho interaktivitou, vede k domněnce, že kyberprostor je nejdemokratičtějším uskupením. Spíše by se však dalo hovořit o rozsáhlé anarchii v chování populace kyberprostoru která, nebýt omezována přísnými technologickými pravidly užívání, by kyberprostor již dávno zlikvidovala a učinila nepotřebným[2].

[1] Gibsonovo připojení ke kyberprostoru je realizováno přímým napojením mozku pomocí elektrod bez rušivého vlivu technologického zprostředkování [N02].

[2] Každý, kdo internet používá si určitě všiml, jak vhodným prostředím je pro různé grafomany, exhibicionisty, šiřitele dogmatických náboženství a další fanatiky.

Mimo všechny vlastnosti spojené s existencí kyberprostoru však internet poskytuje, alespoň zdánlivě, i vlastnosti, které nepatří mezi vlastnosti kyberprostoru, nicméně jsou důležitým ovlivňujícím prvkem vzniku nelegálních aktivit. Mezi první patří poměrně neprůhledné prostředí, které je dáno technologickou složitostí internetu a jenž v žádném případě neusnadňuje roli složkám, pověřeným dozorem nad dodržováním zákona. Toto technologické „příšeří" vzbuzuje mnohdy falešný dojem anonymity, kdy se pachatel cítí velmi bezpečný, vzdálen od místa činu a znám jenom svou fiktivní elektronickou identitou.

Druhou důležitou vlastností je **deteritorializace** aktivit na internetu. Jedním z důležitých rysů kyberprostoru je jeho globálnost a stejně tak internet vytváří spojité prostředí, nerozdělené hranicemi mezi státy nebo kontinenty. A tak aktivity, ať již legální nebo nelegální se jenom obtížně lokalizují na příslušné teritorium, na území pod stejnou státní správou nebo jurisdikcí. Možná přítomnost kdekoli, rychlý přesun mezi místy tisíce kilometrů vzdálenými, to všechno dává legálním i nelegálním aktivitám v kyberprostoru zcela jiný ráz a možnosti.

Právě možnost existence v kyberprostoru, v kterékoli jeho části v libovolném čase, je jedním ze stimulů pro vytváření různých názorově jednotných skupin a virtuálních komunit. Kyberprostor umožňuje jejich komunikaci, prezentaci a koordinaci, vede až ke vzniku subkultur. Zároveň však vytváří prostředí pro sváření a souboje subkultur, které se mohu zpětně promítnout do dění v reálném světě nebo toto dění odrážet.

Soustředíme-li náš zájem na jedince, pak překvapivě zjistíme, že mnozí z nás nepotřebují nutně reálně naplnit své ambice, uspokojí se s pouhou jejich virtuální podobou. Rozdíl mezi virtuálním a reálným prožitkem je stejný jako rozdíl mezi reálným a symbolickým jednáním. K tomu, abychom uvolnili svoji agresi vůči jinému člověku, stačí často pouhé symbolické zničení nepřítele a obdobně mnoha lidem stačí pouhá symbolická realizace jejich snu. Symbolický prožitek sice nemůže nabídnout plný prožitek skutečnosti, ale také minimalizuje případná rizika. V kyberprostoru se nemůže fyzickému jedinci nic stát, a tak může např. vystupovat na různých diskusních nebo chatových serverech v různých rolích, měnit svůj věk i pohlaví, a uskutečňovat vlastní představu o sobě [H02].

3.1 Populace kyberprostoru

S rozvojem technologií globální komunikace, zejména internetu, se vytváří nový prostor pro realizaci jedince i nová dimenze pro socializaci. Zkušenosti, které jedinec získává během pobytu v kyberprostoru samozřejmě ovlivňují jeho psychiku, sociální chování, zvyklosti a přístup k hodnotám. Nové druhy pocitů jedince, které zakouší po zapnutí počítače a připojení k síti, jsou psychology často přirovnávány ke známým pocitům a zkušenostem z reálného světa, např. prohlížení webových stránek je přirovnáváno k pocitům, které jedinec zažívá při cestování, k pobytu v jiné zemi [S06].

Vliv technologií na současnou společnost je nesporný. Nesporný je i vliv na psychiku jednotlivce, na vytváření specifických virtuálních společenství a komunit, na zcela jiný pohled a přístup k sociálnímu chování. Nová dimenze zkušeností se pak promítá do reálného života a vnitřní střet osobnosti kyberprostoru s osobností žijící v reálném prostoru je u každého jedince nevyhnutelný. Moderní sociologie a psychologie se těmto jevům začínají věnovat, avšak k reálným a použitelným závěrům je ještě daleko.

3.2 Netholismus a netománie

konecma

Zatímco ve Spojených státech je závislost na internetu a internetové erotice oblíbeným mediálním strašákem, v Evropě se na příznaky podobných problémů s užíváním internetu poukazuje jen zřídka. Nicméně situace není ani v Evropě příliš příznivá. Ve vedlejším Německu výzkumy prokázaly, že zhruba každý dvacátý uživatel internetu se na něm stává závislým, ve Švédsku[3] je takto závislých osob asi 40 tisíc, což je asi 0,6 % uživatelů internetu. Podle zdravotnických průzkumů v Rakousku je u našich jižních sousedů 30 tisíc osob závislých na internetu (rovněž asi 0,6 %). Je to o jednu třetinu více závislých než na heroinu.

Je už skutečností, že po určité době se používání internetu projeví na lidské psychice. Závisí to zejména na způsobu komunikace a obsahu informací, které na internetu vyhledává. Vyhledávání virtuální komunikace a virtuálních vztahů je většinou reakcí na neuspokojivé osobní zázemí uživatele. Problematické reálné osobní vztahy vytvářejí pocity frustrace a existuje nebezpečí, že začne dávat přednost virtuálním vztahům, u nichž získá pocit většího porozumění a obohacení života. Internetový svět se stane nakonec pro uživatele natolik atraktivní, že bude ochoten obětovat svůj skutečný svět a degradovat ho na uspokojení nejzákladnějších fyziologických potřeb. K základním příznakům patologického užívání internetu patří neustálé myšlenky na připojení k internetu, snížená sebekontrola při jeho používání nebo neschopnost přerušit práci s internetem. Potřeba útěku z „krutého" reálného světa do jednoduššího světa virtuálního, kde nejsou vyžadovány žádné kompromisy a kde se může projevovat, jak se mu zlíbí, se nakonec může projevit až v totálním rozštěpení osobnosti. Nešťastný a nespokojený člověk toužící po jednoduchém světě, ve kterém by mohl realizovat své sny dostává příležitost v přívětivém prostředí kyberprostoru, avšak za cenu svého totálního pohlcení[4].

Firma Websense [W02] tvrdí, že 25 % zaměstnanců, kteří jsou k internetu připojeni, sami cítí, že jsou na internetu závislí. Existence závislosti je živena tím, že firmy vlastně své zaměstnance naučí za internetem sedět dlouhé hodiny a redukuje jejich práci na zaznamenávání údajů do počítače. Tam, kde se dříve odehrávala telefonická nebo přímá komunikace s kolegy nebo se zákazníky, se dnes vypisují maily. Firmy stále více zavádějí informační systémy, ekonomické systémy, CRM[5] a další systémy. To sice zvyšuje produktivitu firmy, ale vede to k odosobnění práce a v důsledku to znamená jenom zadávání údajů do počítače a komunikaci s displejem a klávesnicí. Není potom divu, že zaměstnanec hledá rozptýlení tak, jak je zvyklý vyhledávat informace – z počítače a na internetu. Naučil se tu být doma a zpohodlněl.

Studie výše uvedené firmy uvádí, že průměrný americký kancelářský zaměstnanec dnes tráví více než celý jeden pracovní den v týdnu činností na internetu, která nesouvisí s jeho prací – brouzdáním po webech, osobními maily, chatem a pod. Ukazuje se, že mezi nejčastější nepracovní činnosti na internetu patří prohlížení zboží a nakupování v e-shopech, čtení zpravodajství a časopisů, erotika, pornografie a gambling. Intenzivní používání internetu v práci potvrzují i další výzkumy. Téměř 70 % veškerého provozu na erotických serverech je v pracovních hodinách mezi devátou ranní a pátou odpolední, více než 60 % všech internetových nákupů je prováděno z pracoviště atd. Přestože se firmy snaží tuto činnost svých zaměstnanců omezit, vždy se najde nějaká možnost, jak tato omezení obejít.

[3] Švédsko má největší penetraci internetu v zemích EU (74,9 %). Za ním je v tabulce z roku 2006 Dánsko (69,4 %) následované Holandskem (65,9 %) a Anglií (62,9 %). Česká republika je s penetrací 49,9 % na dvanáctém místě v EU.

[4] Závislost na internetu se dá přirovnat k závislosti na drogách jenom částečně. Závislost na internetu je vždy zejména psychická, i když některé zdroje uvádějí i závislost fyzickou.

[5] CRM – Customer Relationship Management – způsob, kterým firmy řídí svůj vztah se zákazníky za pomoci informačních technologií.

Závislost na internetu lze obecně vymezit přítomností následujících symptomů:

- ✓ **Přikládání důležitosti** – internetová aktivita se stává nejdůležitější v životě, dominuje myšlení, pocitům, chování. A pokud se právě své závislosti závislý nevěnuje, přemýšlí alespoň, kdy se oné činnosti bude věnovat příště.
- ✓ **Změna nálady** – pokud závislý jedinec není připojen k internetu a neprovádí svoji oblíbenou činnost, na níž je závislý, není schopen se řádně soustředit.
- ✓ **Zvyšování prahového efektu** – pocit libosti z provádění oblíbené činnosti na internetu vyžaduje stále větší „dávky", hry musí být hrány déle, komunikace musí být emocionálně vypjatější apod., aby došlo k uspokojení závislosti.
- ✓ **Abstinenční příznaky** – po přerušení práce s internetem se dostavují nepříjemné psychické, či fyzické pocity.
- ✓ **Konflikt s okolím** – vlivem abstinence nebo narušením virtuálního světa reálnými problémy dochází ke konfliktu mezi závislým jedincem a okolním světem – rodinou, kolegy v práci, problémy ve škole apod.
- ✓ **Recidiva** – recidivami rozumíme opětovné návraty do dřívějších stavů libosti vyvolaných činností, na níž je jedinec závislý, tzn. že se při dalším kontaktu s předmětem závislostí dostane do již jednou zažívaného stavu podstatně rychleji než při kontaktu prvním.

V uvedených případech je nutno rozlišovat mezi fyzickou a psychickou závislostí. Při psychické závislosti pociťuje jedinec neodolatelnou touhu po stavu (pocitech), které mu prostředí internetu přináší. Závislost na internetu je zřejmě psychická, a tak bychom se mohli mylně domnívat, že se zde vůbec fyzické příznaky nedostavují. Nicméně i v případě psychické závislosti dochází k rozvoji četných psychických i fyzických symptomů, jakými jsou např. snížená schopnost normálně fungovat v běžném každodenním životě a fyzické příznaky – např. bolesti hlavy, žaludeční vředy apod.

Mezi jedinci závislými na internetu lze vysledovat oblíbenost některých online aplikací. Tento profil se od nezávislých lidí značně odlišuje – viz tabulka 3.2 [N03]:

Aplikace	Internetově závislí	Internetově nezávislí
Chatovací místnosti	35 %	7 %
MUD[6]	28 %	5 %
News	15 %	10 %
e-mail	13 %	30 %
WWW	7 %	25 %
Ostatní informační kanály (gopher, ftp, atd.)	2 %	24 %

Tab. 3.2: *Oblíbenost aplikací pro internetové závislé a nezávislé jedince*

Psychiatři znají diagnózu chorobného hráčství na automatech. Jedná se o dobře prozkoumané onemocnění, s jasně rozpoznatelnými symptomy, zřejmými důsledky i propracovanou metodikou léčení. Jinak je tomu ovšem u internetové nebo obecně počítačové závislosti.

[6] MUD (Multi-User Dungeons) – forma internetové komunikace kombinovaná s hrou - postavy mají své charakteristické role, možnost boje, používání zbraní apod.

Nejenže na toto téma nebylo ještě zpracováno dostatečné množství odborných studií, ale dosud nebyl navržen žádný vyhovující obecný popis závislosti. Navíc, stávající studie se často rozcházejí i v základních údajích, jako např. kolik hodin týdně by měl průměrný „nemocný" u internetu strávit.

konecma

Studie mezi uživateli internetu ukázala na průměrný výsledek 19 hodin týdně, průzkum mezi studenty na univerzitě v Austinu v Texasu doložil, že „závislí" stráví připojeni průměrně 11 hodin týdně, jeden menší odborný test označil jako „patologické uživatele" už i ty, kteří dosáhli 8,5 hodiny týdně. [C02]. Mezi rekordmany bude jistě patřit žena, uváděná ve studii prováděné studenty Matematicko-fyzikální fakulty Univerzity Karlovy mezi uživateli českého chatu. Snaha nalézt porozumění pro své problémy dovedla tuto ženu do virtuálního světa internetu, kde trávila v chatovacích místnostech až 114 hodin týdně [K05].

Nicméně existuje alespoň základní charakteristika závislosti, či nadměrného užívání internetu, kterou uvádí psycholog z Harvardské univerzity Maressa Hecht Orzack [C03]:

- ✓ používání počítače pro potěšení, uspokojení nebo ulehčení od stresu,
- ✓ pocit podrážděnosti, ztráta ovládání nebo deprese při odluce od internetu,
- ✓ stále se zvyšující objem finančních prostředků utrácených za hardwarové a softwarové vybavení, časopisy a další související aktivity,
- ✓ zanedbávání práce, školy, rodiny a ostatních závazků,
- ✓ lhaní o době strávené u počítače,
- ✓ riskování ztráty kariérních možností, vzdělání nebo osobních vztahů,
- ✓ opakované selhávání při snaze ovládnout se při užívání počítače,
- ✓ vynechávání jídla, stres, bolesti v kříži, vyschlé oči, bolesti hlavy a nedostatek či poruchy spánku.

Další autoři např. [S02] doplňují toto schéma některými jinými symptomy jako:

- ✓ velké a náhlé změny v životním stylu umožňující trávit více času na internetu,
- ✓ odmítání trávit více času offline,
- ✓ nutkavé myšlenky o tom, co se na internetu děje v době offline,
- ✓ fantastické sny o internetu,
- ✓ celkové snížení fyzické aktivity,
- ✓ snižování socializace s následkem ztráty mnoha přátel.

Výčet samozřejmě nemusí být úplný, vždy však jde o nějakou změnu osobnosti. Případy netomanie nebo netholismu, což jsou označení pro tyto závislosti, jimiž je nazvala současná lékařská věda, jsou a budou častější s tím, jak se život společnosti bude do internetu – kyberprostoru, přesouvat. Již dnes je zřejmé, že celá řada aktivit společnosti je na internetu závislá – na internetu obchodujeme, objednáváme jízdenky a letenky, čteme denní tisk apod. Firma, které nemá svůj internetový server v podstatě neexistuje. Přechod do kyberprostoru, na který lidská psychika není zcela připravena, bude doprovázen právě takovými závislostmi, které jsme výše popsali.

I když jsem uváděl, že internetové závislosti jsou zejména psychického rázu, jejich dopad může být nesmírně silný. Rozpad osobnosti končící Jekyll-Hyde syndromem, kdy jedinec žije současně v obou světech, kybernetickém a reálném, aniž by tyto své existence dokázal propojit, postupný přechod do virtuálního světa spojený s rezignací na okolní reálný svět, to jsou důsledky internetových závislostí. Propadnutí virtuálním internetovým vztahům ztráta schopnosti odolávat „krutosti" reálného světa pak dožene některé jedince i sebevražedným pokusům. V dopise na rozloučenou, který zanechal člověk, jehož internetová závislost a zklamání v reálném i virtuálním světě dohnala ke skoku z Nuselského mostu se píše: „Internet je katalyzátor. Nevyrábí vaši náladu, ale zesiluje ji. Jste-li šťastni, prožíváte na internetu ještě nádhernější chvilky. E-mail od milované osoby vám rozbuší srdce spolehlivěji než elektrický šok. Jste-li v depresi, budete na internetu cítit ještě větší tíhu, větší bezmoc, větší závist. Možná ji přese všechno unesete. Každému se to ale nepodaří... "

3.3 Chat a chataři

Chat je snad nejoblíbenějším způsobem komunikace skupiny lidí na internetu. Nejedná se o nic jiného , než o sérii důmyslných webových stránek, kde se návštěvníci zaregistrují a pak mohou navštěvovat virtuální místnosti, kde se odehrávají často bouřlivé diskuse. Pro zobrazení stránek není vyžadováno žádné nestandardní softwarové vybavení, postačí webový prohlížeč, který je dnes součástí snad každého počítače.

Na chat se může dostat každý, kdo se dostane k počítači s internetem a anonymita uživatelů chatu jim umožňuje vytvářet virtuální postavy reprezentující jejich identitu. Samotné diskuse se odehrávají v tzv. místnostech, což je pouze logické rozčlenění uživatelů podle tématu diskuze. Místnosti mohou odpovídat geografické poloze chatujících, různým koníčkům, sportům, oblíbené jsou místnosti určené k seznamování apod. Uživatelé si pak vyměňují textové zprávy případně doplněné o ikonky vyjadřující nějaké nálady, emoce apod., a to jak skrytě mezi konkrétními uživateli tak i veřejně, kdy jsou texty viditelné pro všechny návštěvníky místnosti.

Chat bývá součástí např. webového portálu a provozovatelé jej doplňují o řadu dalších služeb např. posílání zpráv ostatním v době jejich nepřítomnosti, využívání mailových služeb, prezentaci dalších informací o chatující osobě, vedení seznamů virtuálních přátel či nepřátel apod. Tyto služby však mají vliv spíše na oblíbenost jednotlivých chatů, než na oblibu samotného chatování. Mezi nejvýznamnější chatovací servery v českém jazyce patří **www.xchat.cz**, **lide.seznam.cz** a **www.xko.cz**, kde se návštěvnost pohybuje v řádech desetitisíců uživatelů denně.

Místnosti chatu lze rozdělit na stálé a dočasné. Dočasnou místnost si může založit každý, stálé místnosti jsou vytvářeny správci systému. Často dochází ke změně místnosti dočasné na stálou na popud uživatelů, kteří se v dočasné místnosti často vyskytují. Takto vzniklá komunita rozhoduje o pravidlech dané místnosti, může spravovat webové stránky s informacemi o místnosti, organizovat srazy, volit stálé správce místnosti apod.

Správci jsou uživatelé chatu, kteří mají v místnosti větší práva než ostatní, mají dohlížet na dodržování pravidel místnosti a „zlobivé" návštěvníky varovat nebo rovnou vyhodit z místnosti. Najdou se případy, kdy komunita dané místnosti k ní má silný citový vztah. Navštěvují výlučně svoji místnost, citlivě vnímají dění v ní, vedou bouřlivé diskuse, co by se mělo změnit, kdo by měl být správcem, kdy zorganizovat sraz a podobně.

Chování uživatelů se v různých místnostech liší a záleží na názvu a tedy návštěvnících dané místnosti, zda se povedou spíše soukromé rozhovory, nebo půjde o otevřené diskuse. Taxonomii chatovacích místností můžeme vytvořit např. podle následujícího vzoru:

- ✓ Malé soukromé místnosti – do 10 uživatelů, vzájemně se všichni dobře znají, v některých případech i z reálného života, a vedou soukromé uzavřené rozhovory. Není snadné ani nějak atraktivní se do takovýchto místností dostat a zapojit se do rozhovorů. Celá místnost se vyprazdňuje téměř okamžitě po domluvě účastníků.

- ✓ Malé veřejné místnosti – do 10 uživatelů, kteří se většinou rovněž dobře znají, avšak oproti předchozí skupině existuje značný rozdíl v jejich přístupu k nově příchozím – vítají je a aktivně zapojují do rozhovorů. Většinou jde o společensky citlivější jedince, kterým nevyhovuje větší množství komunikujících nebo jiné rušivé prvky na obrazovce. Místnosti jsou atraktivní např. pro uzavřenější či plaché jedince.
- ✓ Středně velké místnosti – do 30 uživatelů; často jde o místnost věnovanou jednoznačnému tématu – městu, místu, sportu, koníčku, žánru hudby, odbornému tématu, či nějakému současnému fenoménu (např. televiznímu seriálu). Diskuse na dané téma jsou většinou veřejné, když někdo někoho něčím pozitivně či negativně zaujme, přechází na soukromé rozhovory. V těchto místnostech se vyskytuje velké procento náhodných návštěvníků, ale základ tvoří pravidelní návštěvníci většinou posedlí daným tématem.
- ✓ Velké anonymní místnosti jsou většinou místnosti věnované seznamování, flirtování, sexu apod., kde naprostá většina rozhovorů je soukromých ve dvojicích a na obrazovce se objevují jen nově příchozí nebo žádosti o konverzaci. Neexistuje žádný kolektivní duch či atmosféra, přesto že jde o místnosti s největším počtem návštěvníků. Dlouhodobé opakované návštěvy stejných lidí nejsou časté s výjimkou virtuálních exhibicionistů, kterým takové prostředí vyhovuje. Místnosti lákají jedince, oblibující lechtivější témata nebo neustálé změny chatujících.
- ✓ Velké kolektivní místnosti, kde se schází velké množství lidí. Tyto místnosti nemívají společné téma rozhovorů a jsou nazývány velmi obecně, např. „Pokec". Vyskytuje se zde část stálých návštěvníků, tvořících základ komunity místnosti, což jsou často velmi společenské, vstřícné, otevřené osobnosti. Značné množství uživatelů takových místností je pravděpodobně náhodné, přilákáno obecným názvem a velkou návštěvností odpovídající pestrosti probíraných témat a atraktivitě místnosti.

Mezi návštěvníky chatu můžeme nalézt několik význačných skupiny, které se liší svými psychologicko-sociálními rysy, jenž v převážné míře určují jejich chování na chatu a motivaci. Významnou část návštěvníků chatů tvoří pubertální či dospívající mládež, která hledá jinou formu zábavy. Často se vydávají za nějaký svůj vzor, idol, nebo o nich hovoří.[7] Často se stydí za svůj nízký věk, a tak ho neuvádí nebo se ostaršují, čímž se mohou pohybovat mezi dospělými a vstupovat do diskuzí, které by v reálném životě byly pro ně obtížně přístupné. Jindy se tito uživatelé baví výhradně se svými vrstevníky o svých záležitostech (např. místnost pro „dvanácti až šestnáctileté").

Pozoruhodnou a poměrně velkou skupinu návštěvníků chatu tvoří fanatici nějakého tématu. Ti navštěvují výhradně místnosti zaměřené na předmět jejich zájmu, kde se potkávají se stejně fanatickými jedinci a tráví čas nikdy nekončící diskuzí o předmětu svého zájmu. Příkladem takové skupiny jsou místnosti zaměřené na nějaká náboženská témata, idoly populární hudby apod.

Převážná většina chatařů začala navštěvovat chat v době, kdy jim vznikl nějaký problém např. v rodině, s partnerem, ve společnosti, po úmrtí někoho blízkého nebo mají nějaké zdravotní problémy. Vzhledem k charakteru chatu, kdy jedinec vlastně vstupuje do virtuální komunity a rychle se stává jejím členem, je častou příčinou k první návštěvě chatu pocit osamělosti nebo touha vyzkoušet nový způsob seznámení. Někteří, například uzavření nebo starší lidé, se mohou na chatu snáze projevovat a seznamovat se s lidmi, neboť jim to činí menší potíže než ve skutečném životě. Chataři této skupiny jsou poměrně hovorní, neboť se potřebují vypovídat o svých potížích někomu, kdo je vyslechne, pochopí a často tak hledají společenskou podporu, kterou třeba právě ztratili[8]. Protože na chatu není nutno vyhledávat kompromisy[9], je vždy možné odejít do prostředí, které s problémy jedince bude sympatizovat a bude třeba nabízet i řešení[10].

Významná skupina návštěvníků chatu jsou „chataři z nudy". Navštěvují chat ve své pracovní době, pokud se příliš nudí, jejich práce je nebaví, nebo mají před sebou úkol, problém, který právě nehodlají či se obávají řešit. Útěk k takové zábavě je často nasnadě, když jde např. o noční službu na vrátnici nebo recepci, kde většinu času zaměstnanec tráví čekáním na nějakou událost. Pokud mají k dispozici trvalé připojení k internetu, mohou trávit na chatu téměř celou pracovní dobu s oknem minimalizovaným do ikony a otevíraným ve chvíli, kdy se nikdo nedívá. Tito lidé, pokud jsou na chatu hodně často, si mohou tvořit i „chatovací kariéru", být na chatu známý, oblíbený, ucházet se o post stálého správce apod.[11]

Způsob chování a života internetově závislých chatařů je poměrně stereotypní. Noci tráví na chatu, den v práci, pokud nemohou chatovat, částečně prospí a odpoledne dělají jen to nejnutnější, aby se co nejrychleji mohli dostat zpátky do svého virtuálního domova. Kromě nedostatku spánku si na nějaké zdravotní či psychické problémy většinou nestěžují, pokud tento stereotyp není narušen např. nutnost zůstat v práci déle, výpadek proudu, pád chatovacího serveru apod. Na chatu tráví hodně času, láká je především zábava a podpora virtuální společnosti, jenž tvoří jejich náhradní rodinné prostředí. Většina z nich připouští, že díky chatování přichází o řadu možností v reálném světě. Na chatu jsou však proto, že nemají nic lepšího.

Patrně vlivem pocitu anonymity prostředí a bezpečnosti se lidé na chatu chovají často dost odlišně od chování v reálném světě. Často rozebírají témata, o nichž by se běžně zdráhali mluvit, styděli se, dochází k dezinhibici, jednání končící až virtuálním exhibicionizmem[12]. Charakteristickým projevem je substituce společenské role a statusu, kdy jedinec vystupuje v roli někoho jiného, a je vnímán pouze podle vlastního popisu své virtuální identity. Odlišnosti od reálné osobnosti se většinou soustřeďují na věk, pohlaví, osobní fotografii apod.

Avšak nemusí se jednat jen o fyzické atributy. K „vlastní tvorbě" dochází i v chování internetové osobnosti, která se na internetu „rodí" a její tvůrce se postupně s novou rolí úplně ztotožňuje. Není neobvyklé, že někteří uživatelé chatu mohou mít dokonce takových virtuálních identit více a používají ji podle svého momentálního rozpoložení nebo podle účelu návštěvy chatu. Často je tvorba nového projekcí vlastních ideálů, potřeb či tužeb, a to zejména u osob trpícími pocity méněcennosti, jedinců obtížně přijímaných nebo nepřijímaných společností. I když jim jejich „virtuální osobnost" zdánlivě pomáhá v jejich psychickém problému, může na druhé straně takové chování vyvolávat neustále se prohlubující depresivní stavy, zejména při přechodech do reálného světa, pocity úzkosti, neklidu nebo obav.

---

7 Chataři vystupují na chatu pod svoji přezdívkou – „nickem". Tento nick do jisté míry charakterizuje osobu chataře a často slouží i k vyvolání reakce ostatních návštěvníků chatu.

8 Při analýze chatů prováděné studenty MFF UK byla např. nalezena žena, která trávila chatováním až 115 hodin týdně. Příčinou jejího chování byly problémy v rodině, příležitost a nuda v práci, omezení pohybu po zranění. Mezi lidmi na chatu se cítila dobře, se svými reálnými problémy se mohla podělit s partou dobrých virtuálních přátel. Na chatu tak získávala podporu virtuální společností v řešení svých problémů.

9 To je typický rys virtuální komunity a kyberprostoru vůbec. Absence nutnosti kompromisů vede k vytváření velmi kompaktních komunit úzce tematicky zaměřených.

10 Sem můžeme zařadit i motivaci vycházející z odluky od jazyka, kultury nebo společnosti při dlouhodobém studijním či pracovním pobytu v zahraničí.

11 Zajímavá je z tohoto hlediska statistika počtu návštěvníků chatu v průběhu dne. Obvykle je největší nárůst mezi osmou a desátou hodinou, kdy začíná pracovní doba. S malými odchylkami se počet návštěvníků udržuje až téměř do půlnoci, pak klesá a nejmenší je mezi třetí a šestou hodinou ranní.

12 To je zřejmé zejména na sexuálně orientovaných chatech.

3.3.1 Rozvraceči

I do těch nejuzavřenějších místností chatu čas od času vnikne někdo, kdo způsobí rozvrat, chaos a zkázu. Existují jedinci a skupiny, jejichž cílem pobytu na chatu je vnést rozkol mezi účastníky rozhovoru a získat vládu nad místností. Mnohdy takový rozkolník vystupuje ze začátku skromně a pomocí několika souvislých rozhovorů se nejprve stane právoplatným členem, možná i správcem místnosti. Po získání důvěry nebo správcovství obrátí hovor ve změť nesmyslů a celou místnost totálně rozloží.

Ideologii takového chování, pokud je možné ji nalézt, lze vysledovat v tzv. AntiXChatu, který vznikl jako reakce na nepřehlednou a doposud uspokojivě nevysvětlenou komerční přeměnou XChatu[13]. Když se k této změně přidalo občasné bezohledné a panovačné chování správců místností, několik lidí se rozhodlo pro partizánský boj s cílem znepříjemňovat život správcům. Někteří pak svoji taktiku rozšířili na „omezené" uživatele chatu[14], mezi které zařadili většinu „fanaticky" laděných místností. Prostředkem těchto skupin není technologie[15], ale pouze jejich komunikační schopnosti a základní znalosti chování chatujících jedinců.

Zajímavým rysem je snaha ukázat, že existuje i jiná mentalita než ta většinová, což ostatně je velmi často opakované stanovisko v prostředí internetu. Asi právě proto, že kyberprostor dal možnost k volnému vyjadřování jedinců, bez jakékoli cenzury nebo omezení, uvedený názor je často prezentován v nejrůznějších virtuálních komunitách. Tento obecný rys vede k tomu. že rozvraceč nejedná na základě společných tezí, ať už sociálních, náboženských nebo morálních a svým jednáním se snaží vyburcovat uživatele k přemýšlení o správnosti a odůvodnění platných postupů. Většina uživatelů si to neuvědomí a reaguje nepřátelsky nebo útěkem, a tak přispívá k rozvracečově sebeuspokojení.

Samotné rozhovory s rozvracečem mohou mít nejrůznější formu. Při získávání důvěry hovoří většinu času smysluplně a rozumně a pokud se vydává za obyčejného uživatele, není jej možné odlišit. Při agresivní strategii používají velmi hrubé odpovědi, což oběť natolik zmate, že umožní rozvraceči další verbální útok.

Takový přístup je nejzřetelnější ve flirtovacích místnostech. Rozvraceč nechá konverzaci rozvíjet a po nějaké době zchladí oběť studenou sprchou. Hovor v těchto místnostech bývá o ne zcela běžných erotických fantaziích a jejich otevřené sdílení dává rozvraceči mocnou převahu nad obětí, která nebude schopna ani ve virtuálním světě zajít tak daleko. Často rozvraceči mají bohaté znalosti a zkušenosti z chatu a správně odhadnou totožnost oběti, což potom zneužijí k jejímu zesměšnění. Jiným způsobem jak oběť zmást je použití „kytiček" a podobných emotikonů, což v praxi vypadá tak, že je rozvraceč použije v rozhovoru na naprosto nesouvisející téma a pak na něm tvrdošíjně trvá. S tím souvisí i přesvědčování o změny příslušnosti ve virtuální komunitě – rozvraceč zvolí neobvyklou barvu písma a začne přesvědčovat ostatní chataře aby si také změnili barvu písma, a tak se k němu přidali.

Rozvraceči si vybírají místnosti, kde již jejich název svědčí o stádnosti nebo konvenčnosti v jednání (např. místnost „Harry Potter") nebo kde existuje prostor pro přetvářku a klam (např. místnost „Bezva flirtík"). Pokud se rozvraceč rozhodne pro agresivní strategii, jeho chování v místnosti může skončit dvěma způsoby: buď uživatel odchází pro slabé nervy či je znechucen, nebo je vyhoštěn přistižený obtěžující rozvraceč. Prvním rozhodnutím pro úspěšného agresivního rozvraceče je volba „nicku", který se liší podle místnosti, na kterou hodlá zaútočit a podle pohlaví, které chce prezentovat. Pokud na provokaci nickem nikdo nezareaguje, snaží se rozvraceč vyprovokovat někoho v místnosti k reakci. Nejsnazší způsob je vybrat vhodnou přezdívku, většinou z hlediska rozvraceče nehloupější, a začít přímo šeptat – tedy začít komunikaci ve dvojici, aniž by byl nějaký text zobrazován na společné obrazovce viditelné všem chatařům v místnosti. Během šeptání je druhá strana ironizována, urážena pro své přesvědčení a zesměšňována parodováním svého nicku. Pokud oběť odpovídá ostřeji než je běžný konverzační průměr, vrací rozvraceč nadávky a urážky ve velmi posílené formě nebo naopak odpovídá velmi asertivně.

Základní princip práce rozvracečů spočívá v prvotní provokaci a navázání kontaktu. Následovně se odehrává komunikační souboj pouze s jediným rozvracečem, který musí sám stíhat reagovat na všechny konflikty, které vyvolal a zpravidla nemá naději na podporu od ostatních v místnosti. Mírou úspěšnosti rozvraceče je získání vlády nad místností. V případě, kdy jeden rozvraceč používá v místnosti dva nicky, nebo spolupracují dva rozvraceči na bázi „zlý" a „dobrý", pak běžní chataři nemají proti takovému postupu šanci. Chování rozvracečů připomíná politická jednání, kdy nikdo není tím, kým se zdá být a kdy konečným cílem je moc a právo v rukou rozvraceče.

[13] www.xchat.cz

[14] Jedním ze základní myšlenek AntiXChat skupin je velký nesouhlas s organizovaností a jistou primitivností vedených hovorů. Pokud bylo možno vést s některými z nich rozhovor, nejčastější odpověď na otázku proč to dělají byla, že „chtějí znetvořit mozky lidí, že kecají takový bláboly." I když další komentář byl ve smyslu jestli to vůbec ještě jde, nijak to předcházející tvrzení neovlivnilo.

[15] Technologické prostředky se v tomto případě pohybují od psaní komunikujících skriptů – robotů až op tzv. tapetování, což je vyplňování obrazovky chytu nějakou ASCII grafikou tak, aby zabrala co nejvíce místa a znesnadnila komunikaci chatujících.

3.4 Pařani

Pařani jsou hráči internetových her. Možná by se dalo mluvit o gamblingové závislosti u her typu „single-player", kdy každý hráč hraje sám za sebe proti nepřátelům nebo nástrahám ovládaných počítačem. Nicméně, na rozdíl od gamblingu, zde není ona nepatrná naděje zisku finanční částky, a tak má jednotvárná hra většinou jasný konec, kdy hráč znuděný jednotvárností zvládne všechny nástrahy a s hrou skončí.

Pro internet, resp. počítačové sítě jsou typické dvě skupiny her:

- ✓ Hry typu „multiplayer", kdy spolu hrají spolu jednotlivci nebo teamy hráčů prostřednictvím sítě LAN nebo internetu. Hry jsou tím atraktivnější, čím více hráčů se jí účastní a mají obvykle přitažlivou grafiku i herní atmosféru. Často se jedná o strategické nebo závodní hry, avšak drtivou většinu představují hry akční, kdy jednotliví hráči po sobě vzájemně střílí. Hry se pak liší jen detaily, např. formou, prostředím, zbraněmi, záludnostmi scénáře apod. Součástí těchto her jsou diskuze nebo blogy, kde se hodnotí jednotliví hráči a průběh hry. Hraní těchto her je často provázeno hlučnými projevy – zvuků ze hry, emocionálními projevy hráčů jako hlasité výkřiky, nadávky, tlučením do blízké zdi apod. Velmi oblíbené jsou tyto hry ve známém úzce lokalizovaném prostředí jako jsou studentské koleje, počítačové laboratoře apod. K „pařanské kultuře" pak patří turnaje v počítačových hrách[16], kdy jde vše stranou kvůli domluvenému zápasu, po výhře následuje obrovské nadšení, po prohře obrovské zklamání provázené mírnou agresivitou nebo naopak depresí.
- ✓ Internetové hry, které se hrají prostřednictvím webového prohlížeče. Internetová hra tedy není tak expresivní jako hry typu multiplayer na sítích LAN, je často ochuzena o zvuky a věrnou prostorovou grafiku. Hraní se povětšinou skládá z prohlížení a vyplňování různých formulářů a sledování změn. I když by se mohl tento typ her zdát poměrně nudný, přináší hráčům nový sociální kontakt sepjatý se stejným

[16] Je zajímavé, jak organizátoři těchto her věnují množství času pro zajištění všeho potřebného na bázi dobrovolnosti, neboť takové turnaje nejsou dotovány nějakými cenami nebo sponzory. Někteří obětavci dokonce nabízí vlastní počítače pro zřízení hráčských vyhrazených serverů jenom proto, aby se turnaj uskutečnil.

zájmem na výhře své „aliance". Hráči jsou z daleko většího teritoria a pokud není hra v nějakém málo běžném jazyce, třeba češtině, kde se zapojují jen hráči jazyka znalí, může se jednat o opravdu globální záležitost. Během hry hráči vytváří skupiny, úmluvy, teamy nebo aliance, mohou spolu komunikovat, navzájem soupeřit nebo si pomáhat. Základem však zůstává kolektivní snaha něčeho dosáhnout[17]. Cíle hry jsou různé, většinou se jedná o hry strategické, obchodní nebo válečné. U tohoto typu her má významnou roli organizátor hry, který určuje pravidla hry během jejího průběhu, čímž dostává řadu prostředků pro manipulaci s hráči, udržení hráčů online, připojení v určitou dobu, nebo připuštění hráčů do hry apod.

Doba strávená při hraní her a aktivitách souvisejících s hraním se u jednotlivých hráčů značně liší a pohybuje se většinou mezi 3 až 14 hodinami denně. Zajímavá je vytrvalost hráčů, kteří zapínají počítač ihned po probuzení a s krátkými přestávkami, jenž omezují na minimální možnou míru, pokračují až do pozdních nočních hodin bez zjevné známky únavy. Skalní hráči mnohdy nedbají o svůj zevnějšek, a tak jak k počítači po probuzení usedli zůstávají většinu dne.

Hráč většinou zaujímá určitou polohu, upřeně zahleděn do svého monitoru, na hlavě sluchátka a mikrofon pro dorozumívání se spoluhráči a omezuje komunikaci s okolím jen na nezbytně nutnou míru. Pokud se podaří, většinou po delší době a pod nátlakem, odpoutat hráče od jeho virtuálního světa, většinou zmaten tápe v realitě, hledá a přemýšlí nad elementárními úkony. Snaha odpoutat hráče od hraní nečekaně nemá velkou šanci na úspěch. Lze říci, že hraní internetových nebo síťových her vyvolává závislosti podobné gamblingu a chování hráčů při nuceném přerušení hry vykazuje příznaky až abstinenčního syndromu.

Jedna ze semestrálních prací studentů MFF UK popisuje zajímavý pokus učiněný na skupině „pařanů" hrajících internetovou hru na kolejích MFF UK. Autor práce změnil směrovací tabulky na počítačích „pařanů" a server provozující jejich oblíbenou internetovou hru přesměroval na svůj lokální webový server, kde byla zřízena jednoduchá chybová stránka o nedostupnosti služby. Stejná úprava byla provedena i na některých počítačích v blízkém okolí se souhlasem jejich majitelů. Po prvním zalogování hráčů nastal zmatek, místo jejich oblíbených formulářů a tabulek na ně čekala pouze černobílá nic neříkající chybová zpráva. Hráči byli naprosto zmateni, neboť to byla jediná služba, která jim přestala z ničeho nic fungovat, ale služba pro ně nesmírně důležitá. Začali průzkumem okolí, zkoušeli i počítače spolubydlících a sousedů, ale bez úspěchu. Hledali text oné chybové zprávy v internetových vyhledávačích, psali dotazy do herních internetových fór, diskutovali s ostatními „pařany". Neúspěch ve znovuuvedení hry do provozu vyvolal zdrcení, hráči tápali a nevěděli, jak nastalou situaci řešit. Chybové hlášení na přesměrovaném serveru se každý den mírně měnilo, až se postupně začalo blížit k výsměchu. Každá změna mezi hráči vyvolala prudkou diskusi a debatu nad tím, co se asi děje. Teprve po necelém týdnu se situace náhle vyřešila, když jeden z hráčů kliknul na odkaz na stránce s onou chybovou zprávou, kde už řadu dní byla informace o příčině jejich obtíží s pozdravy. Hráči byli zcela nečekaným vysvětlením situace zaskočeni, jiní se zdáli být popuzeni, když zjistili, že o příčině jejich obtíží vědělo široké okolí.

Chování hráčů v době, kdy nehrají se jedinec od jedince liší. Zatímco někteří mají další, pro ně důležitou činnost, které rádi věnují čas, jiní takové činnosti nemají, nebo je postupně odbourávají. Velmi často se projevuje abstinenční syndrom, kdy hráč trpí nutkavou potřebou se rychle vrátit ke své hře, neboť má obavy o to, co se bez něj děje, je neklidný, nedočkavý nebo podrážděný. Předmětem společenské konverzace je pouze hra, probírají se aktuální herní situace, řeší možné přístupy nebo strategie apod. Každá snaha odvést hovor jinam vede buď k ukončení hovoru nebo k návratu k původnímu tématu – hře. Hráče není snadné zaujmout jiným tématem a když se to podaří, není to na dlouho.

Příčin internetového „pařanství" může být celá řada a u každého jedince se mohou různit. Nicméně, většinou se jedná o podobné podněty jako v případě chatařů – znuděnost hráčů okolím, které je jimi vnímáno jako nudné a stereotypní. Hraní jim přináší zábavu, zdánlivou duševní zátěž a poskytuje jednoduché vnější podněty v přívětivém prostředí kyberprostoru. Oproti jiným zájmům, které mohou být např. i fyzicky náročné, jim stačí daleko méně – stáhnout a spustit novou hru, připojit se na nějaký server. Hry bývají často velmi atraktivní, vždy se snaží něčím upoutat, zaujmout a přinutit hráče hrát ji co nejdéle. Uspokojení společenských potřeb při komunikaci je zdánlivé. Komunikace probíhá převážně s ostatními hráči, na stejná jednotvárná témata a hráči jsou o řadu sociálních prožitků ochuzeni, aniž by si to uvědomovali[18].

Hráči internetových a síťových her mezi sebou vytváří vlastní virtuální komunity a lze mezi nimi najít řadu rysů a příznaků internetové a hráčské závislosti. Většinou se jedná o mladé lidi a je tedy naděje, že si časem svoji závislost uvědomí, od virtuálního světa se odpoutají a podniknou opatření ke zvýšení kvality svého společenského života. Podlehnutí „pařanství" v sobě nese záludnost všech podobných závislostí, včetně rozpadu osobnosti.

[17] Někteří zdatnější hráči využívají svých odborných znalostí při tvorbě jednoduchých skriptů, které sledují stav internetové hry a důležité informace jim zasílají formou SMS na jejich mobilní telefon. Pak můžete daleko od počítačů a internetu zpozorovat internetového hráče, jenž začne zběsile a hystericky vykřikovat zdánlivě nesmyslné věty o vlastním napadení nebo zničení, nebo naopak po příchodu SMS propadá sangvinickému veselí a snaží se o ně podělit s nic nechápajícím okolím.

[18] Šokující je případ popisovaný v jedné semestrální práci na MFF UK, kdy „pařana" navštívila ve školní počítačové laboratoři jeho přítelkyně. Poté, co se pozdravili, dostala sluchátka, byl jí puštěn film a po dvou hodinách se ve stejném duchu rozloučili.

4.

Hackeři a crackeři

Téma hackingu a crackingu je velmi kontroverzní a nebezpečné, neboť cokoli v dané oblasti řeknete, to bude jednou částí dotčené komunity oceněno, zatímco jiná její část autora zatratí. Většina z nás si pod pojmem „hacker" představí unuděného, shrbeného teenagera s umaštěnými vlasy a mnoha dioptriemi, nabourávajícího se po nocích do řídících počítačů raketového centra Pentagonu. Kriminálníka, který ze všech počítačů na světě krade informace a prodává je za miliony dolarů. Nebezpečného jedince, který ohrožuje celosvětový mír a když jej ukáží záběry televizních kamer, jak je odváděn tajnými agenty v poutech, obyčejný člověk si oddychne. Alespoň takový je obraz hackera, jak jej v nás vytvořila média. Skutečnost je ale jiná.

4.1 Historie hackingu

Pojmenování „hacker" a termín „hacking" vznikl zhruba v padesátých letech minulého století v komunitě radioamatérů, kde se jím označoval šikovný, technicky nadaný jedinec, schopný hledat nová zapojení a metody ke zlepšení výkonu a dosahu svého vysílače. Termín „hacking" byl převzat z angloamerického žargonu jezdců na koních, kde se jím

označovala nenucená vyjížďka bez nějakého zřejmého cíle. Následovně, ještě v časech před masovým příchodem počítačů, zdomácněl na MIT, kde „hack" označovalo jednoduchý, často neuhlazený, ale efektní způsob řešení problému. Posléze přešel do studentského slangu a „hackem" se označovalo spáchaní nějaké nepřístojnosti studenty MIT. Provinilec byl, a tato tradice stále trvá, nazýván „hackerem"[1].

konecma

Hacking v dnešním slova smyslu se dostává do povědomí na přelomu šedesátých a sedmdesátých let, kdy skupinka technologických nadšenců využívala nedokonalost telefonní sítě na uskutečňování nezpoplatněných dálkových telefonních hovorů. Jedním z otců tohoto nápadu byl John Draper, známý v hackerském světě jako „Captian Crunch". Základem mechanizmu oklamání telefonní sítě AT&T byl tón o kmitočtu 2600 Hz, kterým se řídilo přepínání dálkových hovorů[2]. Tento tón generoval pomocí dětské píšťalky, která byla přiložena k balení cereálií „Cap'n Crunch". Tak vznikl první hackerský nástroj[3] – blue-box, krabička, která umožňovala telefonovat zadarmo[4].

První hackerské pokusy se tedy odehrávaly v dálkové komunikační síti firmy AT&T a tato specializovaná skupina hackerů byla označována jako „phreakers". Phreakers sami sebe označovali za technicky založenou skupinu pokračovatelů hnutí hippies, které v šedesátých letech minulého století významně ovlivnilo tehdější ekonomicky aktivní vrtsvu obyvatel USA i ve světě. Svoji činnost obhajovali tím, že několikahodinové rozhovory uskutečňují zejména v noci, kdy je síť stejně nevytížená a nedělají to za peníze. Phreakeři organizovali velké telefonní seance, kdy bylo do diskuze zapojeno až několik desítek účastníků z celých Spojených států. Naučili se přeprogramovat ústředny z pouličního telefonního automatu a změnit čísla uživatelů. Postupně se však obrátilo veřejné mínění proti nim a do celé věci se vložila FBI. Potenciální možnost ohrožení systému tísňového volání 911 vedla k velkému zátahu na phreakery a postavení celého phreakerského hnutí mimo zákon.

Skutečný rozvoj hackingu se začíná projevovat až v osmdesátých letech, kdy se širšího uplatnění dostává technologii BBS – Bulletin Board System. BBS byly počítače umožňující vzdálené připojení a umožňujícímu uživateli čerpat informace z databáze uložené na počítači pomocí standardizovaných dotazů. Vznikly první hackerské skupiny, které spolu komunikovaly, vyměňovaly si informace o zjištěných heslech počítačů, přístupových kódech a nástrojích. První hackerské pokusy se soustředily na hádání hesel nebo jejich „lámání", tedy techniky, které spoléhají více na důvtipnost hackera než na speciální programy.

S nástupem webových technologií a prvním vydáním Netscape Navigatoru se začínají objevovat první speciální hackerské nástroje, označované jako „easy-to-use". Hacking se začíná měnit s nárůstem obejmu informací dostupných na počítačových sítích a do světa hackerů začínají vstupovat i lidé bez potřebného vzdělání a vědomostí – „script-kiddies", „lammers" a „loosers"[5], zaměřující svoje úsilí do nebezpečných oblastí – viz tabulka 4.1. Vznikají hackerské weby, kde volně stáhnout programy využívající bezpečnostní díry v systémech, jsou instalovány první „back-doors", utajené vstupy do systému pomocí kterých je možno systém vzdáleně a skrytě ovládat. Mezi první rozšířené back-doors patří „Back Orifice" vyvinutý skupinou „Cult of the Death Cow" pro operační systémy Windows 95 a Windows 98, který se dostal na síť v roce 1998. Avšak již od poloviny devadesátých let minulého století začínají hackeři používat sofistikované nástroje pro předběžnou diagnostiku sítí a automatizaci útoků.

Rok	Událost
1983	Počítač s kódovým označením WOPR (součást vojenského systému s označením BURGR) interpretoval hackerské vniknutí jako odpálení nepřátelské nukleární rakety. Následkem toho byla uvedena část armády do stavu vysoké pohotovosti.
1988	Morrisův „Worm" se vymknul kontrole a napadl na 6 000 počítačů. Dostal tak řadu univerzitních a vládních počítačů mimo provoz.
1988	Národní banka v Chicagu se stává obětí počítačového podvodu za 70 milionů dolarů.
1995	Ruští hackeři převedli 10 milionů dolarů z Citibank na svá konta.
1996	Hackeři napadli webové stránky významných amerických institucí – CIA, Air Force a Ministerstva spravedlnosti
1996	U.S. General Acounting Office zveřejnil zprávu, že došlo k 250 000 útoků na počítače ministerstva obrany, z toho 65 % bylo úspěšných.
1999	Prezident Clinton podepsal nárůst výdajů o 1,46 miliardy dolarů na zvýšení bezpečnosti vládních počítačů.
1999	Skupina hackerů vydírá anglickou vládu – ovládla britský vojenský satelit a za předání kontroly požadují nemalou částku.
2000	Jeden z největších DDoS útoků postihl servery eBay, Yahoo, Amazon a další; ztráty jdou do desítek milionů dolarů.
2000	Jsou ukradeny zdrojové kódy Windows a Microsoft Office.
2001	Byl proveden útok na DNS servery. I když se podařilo zjistit útok téměř okamžitě, odstranění následků trvalo dva dny. Po celou dobu byly nepřístupné stránky firmy Microsoft.
2002	Microsoft přerušuje vývoj systému Windows, osm tisíc programátorů je vyškoleno pro oblast bezpečnosti.

Tab. 4.1: *Přehled významných útoků na přelomu století*

Každá generace hackerské komunity vyrůstala v jiných podmínkách počítačového světa, měla jiná pravidla a byla jinak přijímána společností. Skuteční experti, kteří si snad jako jediní zaslouží označení hacker, byli původci většiny nosných myšlenek na kterých dnes stojí téměř celá oblast informačních technologií. I když jde o historii sedmdesátých let minulého století, kdy se dnešní podoba informačních technologií rodila, tehdejší hackeři byli studenti, soustředění kolem výpočetních center jednotlivých univerzit. Mít právo používat titul hacker byla v té době čest, neboť to znamenalo, že jste skutečný odborník. Značná část těchto hackerů se postupem doby stala řediteli úspěšných společností působících na trhu informačních technologií a do této kategorie spadají i takové osobnosti jako Bill Gates nebo o něco mladší Linus Torvalds. Přesto, že každý z nich nyní reprezentuje odlišnou ideologii vývoje a trendů v informatice, oběma jsou společné rozsáhlé znalosti a úsilí namířené konstruktivním směrem. Tato generace, dnes označovaná jako „stará garda", vyrůstala v jiné době. Jejich hackerské aktivity nešly mimo rámec univerzity a neškodily širokému okruhu osob, protože to technicky ani nebylo možné. Na akademické půdě se jejich hackerské výstřelky daly tolerovat, neboť byly, až na pár výjimek, také „akademické".

[1] Jiný historický pramen uvádí, že slovo „hacking" bylo převzato od skupiny železničních modelářů, kteří modifikovali koleje, výhybky a mašinky tak, aby jezdily rychleji, lépe nebo prostě odlišně.

[2] Tehdejší ústředny měly spojený signalizační a hlasové kanály, takže veškerá signalizace pro řízení ústředny byla přenášena ve stejném pásmu, jako hovor. U dnešních ústředen jsou tyto cesty odděleny.

[3] Správněji „phreakerský" nástroj, neboť tato skupina hackerů se označuje jako „phreakeři".

[4] Pro zajímavost, do okruhu Johna Drapera a „výrobců" blue-boxu patřili i Steve Wozniak a Steve Jobs, zakladatelé firmy Apple.

[5] Těmito názvy jsou označovány jedinci, kterými hackerská komunita pohrdá – viz další text.

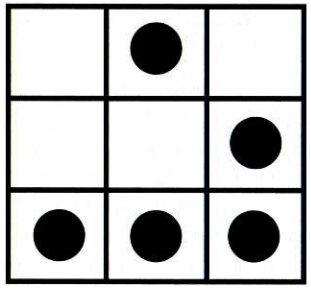
Novodobí hackeři patří do mnohem problematičtější skupiny. Stále sice převyšují své okolí odbornými znalostmi, avšak působí ve zcela jiném prostředí. Není to už tolerantní akademická půda, která poskytovala „staré gardě" vše, co potřebovali – akademickou svobodu, myšlenkovou volnost a technické vybavení, ale celosvětová počítačová síť, využívaná komerčními subjekty pečlivě střežícími své zájmy. To také mění náhled na hackery. Přesto, že jejich aktivity stále vyžadují vysoký stupeň odbornosti, stále častěji je na ně nahlíženo jako na osoby, které škodí. Tato změna pohledu je důsledkem aktivit komerčních firem, neboť jedním ze základů hackerské činnosti je odhalování nedostatků komerčních projektů, což u postižených projektů a firem snižuje dosažitelný zisk.

konec ma

Přes veškeré a někdy oprávněné výhrady, však nelze hackerům upřít znalosti a schopnosti, pomocí nichž vyvíjejí silný tlak na zlepšování bezpečnosti sítí a kvality programů. Možná je způsob vynucování nápravy, který zvolili, nekorektní a v některých případech i nezákonný a připomíná filmové příklady braní zákona do vlastních rukou. Nicméně nikdo nemůže popřít, že bez hackerů a jejich veřejných útoků bychom dnes neměli k dispozici mnoho service packů a bezpečnostních záplat. Naše počítače by byly mnohem otevřenější, méně chráněné a snadno zranitelné. A nevznikl by ani tržní segment bezpečnostních technologií, který je nemalým zdrojem příjmů pro mnohé technologicky vyspělé firmy.

Kolem hackerů, kteří něco umí, není nutno dělat zbytečný rozruch. Je to období růstu, které nutně musí ve životě překonat a později, jak se potvrdilo u „staré gardy", převedou své aktivity na legální platformu prospěšnou společnosti. Stanou se z nich bezpečnostní odborníci, nebo se uchytí u firem zabývajících se počítačovou bezpečností, pokud takovou firmu sami nezaloží. Tento trend již lze pozorovat u některých hackerských serverů, ze kterých se pomalu stávají servery komerční, transformují se a nabízejí produkty související s počítačovou bezpečností.

Je pravdou, že někdy tento přechod z „puberty" a cesta k dopívání je narušena stykem s kriminálním podsvětím, které v hackerských znalostech spatřuje nové pole svých aktivit. Pokud hacker neodolá a dá se na cestu vedoucí do pekel, stává se většinou členem skupin organizovaného zločinu působících nejčastěji v oblasti porušování autorských práv. Hackerské schopnosti však kriminální podhoubí využívá i při volbě a přizpůsobení používaných technologií pro komunikaci, předávání zpráv, sledování aktivit vytypovaných cílů. V tomto okamžiku však hacker přestává být hackerem a stává se jedním z členů kriminálního podsvětí.



Obr. 4.1: *Hackerský emblém*

4.2 Definice hackera

Definovat hackera v dnešní době, kdy pohled na hackerství je médii značně zkreslen, není jednoduché. Podle internetového souboru „Jargon File: The New Hackers Dictionary" je hacker člověk, kterého baví zkoumat detaily programovatelných systémů a hledat metody, jak je vylepšit. Další rysy v uvedeném souboru zahrnují:

- ✓ člověka, který s nadšením programuje, dokonce je programováním posedlý, a nebo dává přednost praktickému programování před teoretickými úvahami o programování,
- ✓ jedince, který vyniká v rychlém programování nebo je expertem ve využívání konkrétního programu,
- ✓ osobu, která dokáže ocenit „hack value", tedy hodnotu ztvárněného technologického řešení, nebo
- ✓ obecně osobu, která je expertem nebo nadšencem v daném vědním oboru (podle toho se může vyskytovat třeba hacker v biologii).

Pojem hacker může též označovat příslušnost ke globální komunitě v kyberprostoru nebo obecně na síti. V tom případě však označená osoba veřejně deklaruje svůj souhlas s dodržováním některé z verzí hackerské etiky. Jako příklad nesprávné definice je v tomto souboru zmíněna obecně rozšířená představa zlomyslného jedince, který odposlouchává informace nebo se snaží prolomit jejich ochranné prvky. Odtud pocházejí pojmenování jako „password hacker" nebo „network hacker". Správný termín pro tento případ je však „cracker" [N04].

Policejní definice uvedená v [R01] definuje hackera jako osobu, která proniká do chráněných systémů, přičemž jejím cílem je prokázat vlastní kvality bez toho, aby měli zájem na získání nebo zničení informací v systému obsažených. Za nejdůležitější je překonání ochranné bariéry, což je považováno za zábavu, dobrodružství či „sportovní nadšení", a to bez nároku na veřejné uznání. Hackerům stačí uspokojení z toho, když se o jejich činu hovoří alespoň ve vlastní komunitě. Hacking je jejich koníčkem, u počítače dokáží vysedávat dlouhé hodiny a získaná data nebo programy využívají pouze pro svoji potřebu nebo pro potřebu svých přátel.

Sami hackeři se většinou vidí jako uživatelé velmi dobře vybavení technologickými znalostmi, které zpravidla získali samostudiem. Uspokojení nacházejí v objevování skrytých detailů informačních a telekomunikačních systémů, především v oblasti jejich bezpečnosti a zranitelnosti. Milují praktické, rychlé a sofistikované programování, nikoliv však přehledné a uspořádané. Jsou to lidé s kreativním myšlením, kteří se nedají přimět ke stereotypní práci s počítačem [H03].

Nejhorší představu o hackerovi však prezentují média. Představují ho jako kriminální individuum nabourávající se do cizího informačního systému bez ohledu na důvod nebo cíl takové činnosti. Podle médií je hacker člověk, který ničí internetové stránky, snaží se narušit informační systémy nebo získat choulostivé osobní údaje jiných uživatelů. Tato představa, vyvěrající spíše z novinářské nevědomosti a touze po senzaci, než ze skutečného hackerského světa, však vytvořila neblahou představu hackera v myslích prostých lidí. Média zcela zkreslila úlohu hackerů ve vývoji informačních technologií, představila je jako zloděje a vetřelce. Zapomněla, že vždy jde o velmi inteligentní osobnosti, které se snaží dokazovat dennodenně svoji zručnost v oboru, jehož kouzlu podlehli. Jedním z kréd hackerů je víra, že by informace měli být přístupné pro každého, a proto bojují proti jejich vlastnění.

4.3 Hackeři v kyberprostoru

konecma

I když jsou hackeři spíše uzavření a nevynikají komunikativními schopnostmi, tvoří své vlastní komunity, v nichž se cítí dobře. Specifika jejich sociálního chování, kam patří mimo jiné silný individualismus a téměř neschopnost pracovat v týmu, jsou často jejich zaměstnavateli přehlížena pro jejich mimořádné znalosti technologií a pracovní zaujetí při řešení vzniklých technických problémů.

Hacker neuznává mocenské autority[6], firemní hierarchií pohrdá, obléká se především pro své pohodlí, tak aby se cítil sám dobře. Pokud je součástí hackerské komunity žena – hackerka, používá pouze nenápadný make-up nebo jej nepoužívá vůbec a své chování přizpůsobuje majoritní mužské části komunity. Peníze znamenají pro hackery tolik, jako pocit respektu ostatních členů hackerské komunity, jejich obdiv a uznání. V jejich jídelníčku se často vyskytují méně běžná a zejména orientální jídla a pijí ohromná množství čaje, i když se vyskytují výjimky pijící srovnatelné množství kávy. Pro hackerskou komunitu je typický způsob zápisu textů a používání vlastního žargonu obvykle úzce souvisejícího se specifickým suchým humorem.

4.3.1 Morální hodnoty hackerské komunity

Základním vyznáním hackerů je svoboda jedince, nicméně jsou ochotni i pomáhat druhým. Elektronický svět, v němž pohybují, je pro ně plný výzev a problémů čekajících na vyřešení. Hacker neřeší žádný problém vícekrát a k vyřešenému problému se nevrací. Morální povinností hackera je sdílení získaných informací a know-how.

Svět hackerů je založen na principu dobré reputace. Nový člen získá svoji pozici v komunitě až potom, co prokáže nejen svoje schopnosti a dovednosti, ale i ochotu sdílet své znalosti s ostatními členy komunity a podílet se na ideálech komunity. Hacker nebere, ale dává; věnuje svůj čas, svoji kreativitu a výsledky svých experimentů ve prospěch vyřešení problému. Existují dva základní principy hackerské etiky, které jsou mezi hackery široce, i když ne obecně, přijímány:

- ✓ Prvním principem je víra, že sdílení informací je správné a dobré a je etickou povinnosti hackerů dělit se o své poznatky psaním open-source kódů a usnadňováním přístupu k informacím a počítačovým zdrojům v maximální možné míře.
- ✓ Druhým principem je přesvědčení, že „nabourávání" do systémů pro pobavení a získání zkušeností je eticky v pořádku, pokud nedojde k vandalismu, zcizení nebo narušení informací či porušení jejich utajeni.

Většina hackerů se hlásí k hackerským principům v prvním uvedeném významu a naplňuje jej psaním a zveřejňováním open-source programů. Někteří rozšiřují tento trend a prosazují myšlenku, že všechny informace by měly být volně dostupné a jakákoliv legislativní kontrola patentovými nebo autorskými zákony je špatná.

Smysl druhého principu je v hackerské komunitě různě vnímán i vykládán. Někteří chápou jakýkoliv akt pronikání do cizího systému za neetický, zatímco druzí považují průnik do cizího systému, který nezanechá žádné škody a pokud možno ani stopy, za vrchol hackerské etiky. Tento princip pak rozšiřují na dva kroky:

- ✓ nabourání systému,
- ✓ kontaktování správce mailem (nejlépe ze superuživatelského konta nabouraného systému) a vysvětlení, jak k nabourání došlo, kde je bezpečnostní „díra" a jak ji „zalepit".

Budiž řečeno ke cti hackerské komunity, že téměř všichni hackeři se aktivně podílejí na šíření a sdílení technických a programátorských triků, počítačových zdrojových kódů. V populaci kyberprostoru jsou kyberpredátory, kteří se snaží o zajištění jeho čistoty a průhlednosti.

Hackerská pravidla a etika byly během času shrnuty do základní hackerského patera, které bylo později rozšířeno na sedm pravidel:

1. Přístup k počítačové technologii je pro všechny bez rozdílu a zdarma.
2. Všechny informace zdarma.
3. Nedůvěřujeme vládě a obecně mocenským autoritám, podporujeme decentralizaci.
4. Hackeři mají být posuzováni podle jejich dovedností jinými hackery a ne nějakou formální organizací nebo jinými nerelevantními kritérii.
5. Na počítači je možné vytvořit i umění a krásu.
6. Počítače mohou změnit život k lepšímu.
7. Hacker nikdy nepoškodí systém.
8. Hacker se nikdy neprolamuje do státních počítačů

O hackerské etice je možno psát dlouho a stavět názory jednoho hackera proti druhému. V komunitě silných individualit se množství názorů na jedno téma nevyhneme. Nicméně posedlost technologiemi, síla myšlení a protest proti nechápajícímu světu, který dal vznik nové kultuře, může dokreslit citát z hořkého pohledu hackera s přezdívkou The Mentor, který ve svém hackerském manifest uveřejněném krátce po jeho uvěznění píše [M02]: „Ano, jsem zločinec. Mým zločinem je zvědavost, jeho podstatou je posuzování lidí podle toho co říkají a co si myslí, nikoliv podle toho jak vypadají. Můj zločin spočívá v tom, že jsem chytřejší než vy, což mi nikdy neodpustíte..."

4.3.2 Hackerský jazyk a humor

Jedním ze znaků hackerské komunity je specifický jazyk, kterým se vyjadřuje. Protože většina komunikace je písemná, texty jsou předány po počítačové síti, specifika hackerského jazyka spočívá v úpravách grafického vzhledu běžných slov, slangovém zápisu, ale i specifickém žargonu.

Specifický hackerský humor vyžaduje alespoň základní technické znalosti z výpočetní techniky, aby byl správně pochopen. Projevy tohoto humoru můžeme zaznamenat nejenom ve slovních hříčkách a příbězích, ale i ve vážných dokumentech nebo technickém řešení problémů.

Jeden z členů „staré gardy" Donald E. Knuth vytvořil textový editor pod názvem TeX, který je dodnes často používán pro přípravu technicky orientovaných text, podobně jako běžný kancelářský Microsoft Word. Po dokončení TeXu vypsal odměnu za nalezení chyb v programu. I když několik chyb bylo nalezeno, není známo, že by si někdo odměnu vybral. Je to projevem hackerské etiky, a těžko by někdo jiný než brilantní programátor chybu našel, že nepreferuje finanční odměnu. Pro skutečného hackera je větší ctí pocit, že tu chybu našel a že mu je Donald E. Knuth něco dlužen.

[6] Takto jednoznačné tvrzení s použitím termínu „autorita" je ale zkreslující. Neuznávání autorit v hackerské komunitě se vztahuje na autority státní, firemní nebo podobné mocenské hierarchie. Jedná se tedy o autoritu v řídící hierarchii nikoliv o autoritu odbornou. Uznávání „odborné autority", oceňující odborné schopnosti, patří naopak k základům hackerské filosofie a sami hackeři touží po tom, aby se uznávanými odbornými autoritami stali.

Jiným příkladem hackerského humoru je specifikace RFC1149. Jedná se o jeden z dokumentů, kde jsou popsány protokoly a funkce v síti internet[7] a zabývá se přenosem zpráv pomocí poštovních holubů. Přenos podle tohoto dokumentu byl skutečně otestovaný v roce 2001 v Norsku. Data byla vytisknuta na tiskárně a uložena do pouzdra, které nesl poštovní holub. Jakmile poštovní holub dosáhl cíle, data byla z pouzdra vyjmuta, založena do snímače OCR písma, digitalizována a předána příslušné vrstvě protokolu podle specifikace. Parametr „round-trip time", který ukazuje na dobu nutnou k doručení zprávy příjemci a přijetí potvrzení o jejím úspěšném doručení odesílatelem, byl v tomto případě změřen a dosahoval jeden a půl hodiny[8].

konec na

S typicky hackerským řešením svého problému přišel jeden ruský administrátor počítače, který byl umístěn ve vzdálené lokalitě. Systém tohoto počítače poměrně často zkolaboval a počítač se „zasekl". To znamenalo, aby administrátor cestoval více než hodinu přes celou Moskvu, na místě počítač restartoval a vrátil se zpět. Tedy aktivita, zabírající téměř půl pracovního dne, navíc jistě ne příliš pohodlná. Celý problém vyřešil s použitím vyřazené starého počítače s CD mechanikou, na kterém nainstaloval jenom nejnutnější části operačního systému Linux a démona pro vzdálené ovládání a vhodně jej umístil proti nespolehlivému serveru. Ve chvíli, kdy vzdálený server zkolaboval, přihlásil se k tomuto „servisnímu počítači" a vydal příkaz „eject". V reakci na tento příkaz se vysunula CD mechanika a hranou stlačila tlačítko reset na nespolehlivém serveru. Ten se restartoval a administrátor ušetřil několik hodin nepříjemného cestování.

4.3.3 Typy hackerů

I když jsme se snažili osobnost hackera v předcházejících kapitolách poněkud ozřejmit a postavit ji do lepšího světla, než jak jej vnímá pod tlakem médií společnost, je nutno uznat, že v hackerské komunitě, stejně jako v každé jiné společnosti existují různé typy osobností. Pokusy o vytvoření typologie hackera většinou selhávají, ale pokusme se alespoň vyznačit skupiny, které mají společné zájmy a vyznačující se podobným charakterem.

Prvním rozlišovacím prvkem je důvod k aktivitě hackera. Z předcházejících kapitol víme, že základním motivem hackera je přijetí výzvy k souboji s technologickým problémem, nikoliv zisk, který z jeho vyřešení plyne. Toto hledisko nám umožní rozlišit dvě základní skupiny:

- ✓ hackery, které jsme již dostatečně popsali v předcházejících kapitolách a
- ✓ crackery, jejichž prvotním cílem je zneužití hackerských metod, většinou pro finanční zisk; do této skupiny je však možno zařadit i individua zneužívající internet a technologie pro vandalismus, teroristické aktivity, finanční podvody a další nelegální činnosti.

Toto hrubé dělení je často spojováno s tzv. kloboukovým dělením[9], kde aktéři jsou rozdělováni do tří skupin, v podstatě podle stejného klíče jako v předcházejícím:

- ✓ „White hats" neboli „bílé klobouky" jsou typičtí hackeři, uznávající hackerskou etiku a často jsou zaměstnáváni firmami zabývajícími se bezpečností systémů. Najmutí hackeři provádějí útoky podobné jako kdyby chtěli napadnout systém, ale činí to s vědomím a na žádost majitele, s cílem najít bezpečnostní slabiny systému. Můžeme se setkat s označením těchto skupin jako „tiger-team" nebo „sneakers".
- ✓ „Black hats", čili „černé klobouky", vyvíjejí podobnou činnost jako „white hats", avšak s cílem systém napadnout a prolomením ochranných prvků získat nějaké výhody pro sebe nebo pro svého zaměstnavatele, kterým je obvykle nějaká nelegální organizace. Jedním z nejznámějších označení těchto skupin je „H4H", neboli „Hackers for Hire", a její členové nabízí své služby jiným kriminálním, teroristickým nebo extremistickým skupinám. Rovněž se z této skupiny rekrutují hackeři sloužící průmyslové špionáži mezi velkými konkurenty. Takový „spřízněný" hacker se nechá najmout do počítačového centra konkurenta, kde shromažďuje důvěrné informace a přes nenápadnou internetovou adresu je směruje svému skutečnému zaměstnavateli.
- ✓ „Grey hats" se pohybují na pomezí obou skupin, jak již jejich název „šedé klobouky" napovídá. Tato skupina byla zřejmě vytvořena proto, že předcházející skupiny spolu na mnoha místech interferují a rozdíl je jenom v přístupu k problému. Zároveň slouží jako doplňující prvek v taxonomii a obvykle je přechodovým stadiem rodícího se hackera, který nemá ujasněn svůj budoucí úkol.

Samostatná skupina hackerů, která se nijak s předcházejícími nespojuje, označuje sama sebe za skupinu „brilantních programátorů". Jedná se o velmi respektovanou skupinu s hlubokými znalostmi o systémech a jejich bezpečnostních barierách. Nicméně jsou to stále hackeři, nadšenci programující bez jakéhokoli plánování, což jim na druhou stranu poskytuje výhodu měnit libovolně specifikace během práce na projektu. Firma dodávající software a zaměstnávající takového hackera je z něj často nešťastná. Nejen, že volně přizpůsobuje specifikace „k obrazu svému", ale k jeho programům často neexistuje žádná dokumentace, neboť on se v programu vyjadřuje svým přirozeným jazykem, a tedy je všechno jasné a dokumentace není třeba. Přesto, že tato skupina programátorů je velmi produktivní, její zaměstnávání v týmu je obtížné, a tak často končí jako „jednomužné" firmy nebo programování se svou obživou vůbec nespojují.

Ve skupině „brilantních programátorů" můžeme najít dvě podskupiny odlišující se svým přístupem k řešení problému:

- ✓ „Guru", hacker, který má dlouholeté zkušenosti a vyzná se v předloženém problému do detailů. Tyto své zkušenosti zúročí při řešení a dokáže zvolit správný postup vedoucí k řešení.
- ✓ „Wizard" neboli čaroděj, jehož chování při řešení problému vychází z konkrétních excelentních znalostí detailů specifického problému a dokáže ho vyřešit způsobem, který je ostatním téměř nepochopitelný. Nebezpečí „čarodějského" řešení problému spočívá v tom, že nemusí nutně fungovat ve všech okrajových stavech.

Některé prameny rovněž dělí hackery podle toho s čím přicházejí do styku při hackingu. Taková taxonomie rozeznává domácí hackery, kteří zneužívají možností daných jejich zaměstnáním a pozicí ve firmě, a vnější hackery, jenž jsou rozlišení možnostmi a zkušenostmi na „super-hackers" a „professional hackers".

Vyjdeme-li z předcházejících úvah a shrneme-li základní charakteristiky, můžeme dojít k typologii zahrnující nejvýznamnější skupiny hackerů:

[7] RFC – Request for Comment je řada dokumentů, které popisují technické a organizační standardy sítě internet (původně ARPANET). Tato řada dokumentů se vydává od roku 1969 a obsahuje podrobné technické údajů o propojování počítačů, protokolech, procedurách, programech a konceptech. Součástí RFC jsou i záznamy o jednáních odborných skupin, ale někdy, a to je tento případ, i humorné konstrukce obvykle vydávané 1. dubna.

[8] Pro méně technicky orientovaného čtenáře – obvykle se tento čas v síti internet pohybuje v řádu jednotek až desítek tisícin sekundy.

[9] Toto dělení je odvozeno od klobouků hlavních hrdinů ve westernech. Obvykle kladný hrdina míval světlý nebo bílý klobouk, zatímco záporný hrdina se vyznačoval tmavou, nejčastěji černou barvou klobouku.

- ✓ Kriminální hackeři neboli crackeři – jejich motivací je zisk za každou cenu, cíle zahrnují většinou servery velkých firem nebo institucí a často se jedná o organizované a izolované skupiny spojené s kriminálním podsvětím. Do této skupiny můžeme zařadit i hackery najímané korporacemi s cílem provádět průmyslovou a obchodní špionáž u konkurence.
- ✓ Profesionální hackeři, které je možno rozdělit podle předcházející kloboukové typologie na „White Hats", „Grey Hats" a „Black Hats".
- ✓ Nespokojení zaměstnanci tvoří jednu z nejnebezpečnějších skupin hackerských aktivit a jsou podrobně pospány ve zvláštní kapitole.
- ✓ Ideologičtí hackeři patří k fanaticky zaměřeným skupinám internetových aktivistů, kteří používají internetu k šíření a prosazování svých politických nebo ideologických cílů. Jejich aktivity obvykle souvisí s nějakou významnou událostí ve světové politice nebo ekonomice. Často se označují jako „haktivisté" a bývají zahrnování do kyberteroristických skupin.
- ✓ Script-kiddies (lammers, loosers) jsou nejmladší skupinou hackerů, která si však označení „hacker" ani nezaslouží. Proti takovému „házení do jednoho pytle" protestují nejenom příslušníci „staré gardy" a ex-hackeři, ale i řada počítačových specialistů. Problém spočívá v tom, že se jedná o skupinu s minimálními technologickými znalostmi, která využívá nástrojů a informací hackerské komunity[10] aniž by byla schopna docenit jejich dopady a následky. I když se zdá, že aktivity script-kiddies budou neplodné, případný neuvědomělý zásah může být o to více zničující. Skript-kiddies nevytvářejí vlastní programy, jen stáhnou z internetu hotový nástroj a ten použijí pro své zviditelnění. Bohužel, mnoho lidí, zejména novinářů, kteří se k problematice hackerů vyjadřují, vůbec neví o čem je řeč, a tak bez zaváhání označí např. tvůrce viru „VBS/OnTheFly-Kournikova" za hackera. Přitom téměř celý virus je shodný s kódem, který produkuje volně dostupný generátor virů. Do stejné skupiny patří i tvůrci DoS útoků, kterými se sice podaří vytvořit kritickou situaci na internetu, avšak vzhledem k minimálnímu přínos pro odhalování chyb v programech a relativně malou potřebnou technickou erudici útočníka, je takový útok pod úroveň každého hackera.
- ✓ Nevyužití dospělí hackeři jsou původní skript-kiddies, kteří nenašli odpovídající uplatnění a touží po uznání v hackerské komunitě. Jedná se o tu smutnější součást hackerské komunity, která není nijak výrazná.

4.3.4 Osobnosti hackingu

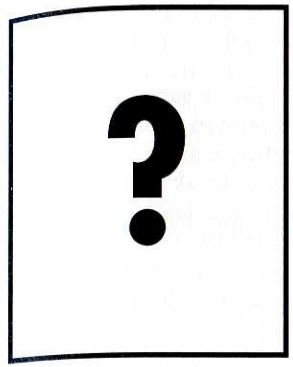
Jako každá lidská aktivita, má i hacking svoje významné osobnosti a skupiny. Mnozí hackeři, kteří se proslavili svými kousky, si buď si odpykávají trest nebo založili firmu specializující se na ochranu a bezpečnost počítačových systémů. Obvykle se řadí do skupiny označované jako 3lit3 – „Elite". Mezi ně patří např. Kevin Mitnick, Vladimír Levin[11] nebo John Barlow[12].

[10] Nezapomeňme podotknout, že hackeři se o informace dělí a neskrývají je.

[11] Spolupracoval s odnoží ruské mafie a skupina hackerů pod jeho vedením pronikla do počítačové sítě Citybank odkud převedla částku převyšující 3,7 milionu dolarů na jiné účty. Levin byl v roce 1995 zatčen při své cestě do Londýna. Následovně byl odsouzen ke třem letům vězení a pokutě 240 000 USD.

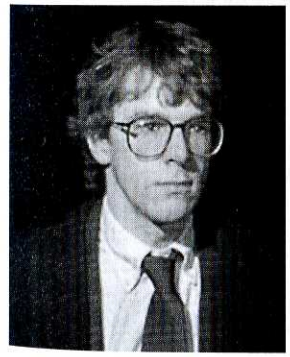
[12] Jméno Johna Barlowa, textaře skupiny Garteful Dead, je spojováno s kolapsem sítě AT&T v roce 1990 a se zveřejněním přísně tajného dokumentu, který popisoval funkci linky tísňového volání 911. Jemu osobně se však nikdy nic neprokázalo. John Barlow je zakladatelem nadace EFF (Electronic Froniter Foundation), která dodnes sleduje ochranu občanských práv v „kyberprostoru".

Mezi 3lit3 jsou jak White Hats, tak i Black Hats. Přibližme si alespoň některé z nich, jejichž vztah k hackerskému světu se liší, ačkoliv jsou všichni za hackery označováni.



Markus Hass

Psal se rok 1986 a astronom Cliff Stolle, který na částečný úvazek spravoval počítačovou síť Berkeleyské univerzity řešil zdánlivě nepatrný problém. Počítačový systém berkeleyské univerzity byl sledován dvěma nezávislými programy, které identifikovaly připojeného uživatele, určovaly dobu jeho práce a připravovaly podklady pro účtování spotřebovaného strojového času. Účetní zjistili rozdíl mezi výsledky práce obou programů a nebyli schopni jej vysvětlit a tak bylo na něm, aby našel chybu, neboť „za to mohl počítač"[13]. Jediný rozdíl mezi účetními programy byl v tom, že jeden z nich sledoval uživatele podle uživatelského jména zatímco druhý podle čísla účtu, které bylo přiděleno legitimním uživatelům, a ti ho museli zadávat vždy při vstupu do systému[14]. Cliff zjistil, že někdo se vloupal do systému a vytvořil si vlastní uživatelské jméno „Hunter", avšak nevěděl o druhém programu, a tak zapomněl vytvořit odpovídající číslo účtu. Když o svém zjištění informoval policii a uvedl škodu 75 centů, ti se mu vysmáli a případ neřešili. Cliff Stolle však vystopoval s pomocí telekomunikačních firem útočníka až v německém Hannoveru a identifikoval ho jako Markuse Hasse, jednoho ze tří členů hackerské skupiny „Hannover Hackers". Tato skupina byla placena sovětskou KGB a pokoušela se o prolamování do počítačů a získávání tajných informací. Celý případ byl odložen jako špionáž, avšak v historii hackingu zůstal zaznamenán jako první případ zjištěného prolomení ochranných prvků systému.



Robert Tappan Morris

Otec Roberta T. Morrise, Bob Morris, pracoval ve vedení americké tajné agentury NSA, která se zabývala mimo jiné i bezpečností počítačů a bezpečnými šifrovacími algoritmy. Robert patřil mezi nenápadné studenty katedry počítačů na Cornell University a u toho by zůstalo, kdyby se mu nepodařilo při experimentování s autoreplikovatelnými kódy nakazit dalších 2 000 počítačů[15].

Princip autoreplikovatelného kódu byl teoreticky znám již dříve a úkolem Robertova programu bylo předávat zpět do definovaného bodu informace o velikosti sítě internet. Tehdejší internet však nebyl tak rozsáhlou heterogenní sítí jako dnes, a tak Morrisův kód se měl šířit velmi pomalu poštou, zjišťovat rozsah připojení jednotlivých strojů pomocí unixového příkazu „finger", použít tuto informaci pro vytvoření vlastní kopie na jiném stroji a předávat zjištěné informace zpět. Chyba v programu však způsobila, že pracoval s maximální rychlostí a velmi rychle se rozšířil

[13] Rozdíl mezi účty činil 0,75 dolaru, tedy částku zcela zanedbatelnou. Avšak účty musí „sedět" a taková drobná částka se hledá nejhůře.

[14] Jednalo se v podstatě o heslo.

[15] To se událo 2. listopadu 1988.

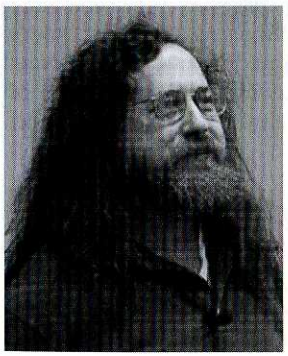
po síti. Alespoň tolik o tom říká legenda. Robert T. Morris byl obviněn, postaven před soud a odsouzen[16] ke třem letům vězení, 400 hodinám obecně prospěšných prací a pokutě 10 400 dolarů[17].

Kevin David Mitnick

Za nejslavnějšího hackera světa je obvykle považován Kevin Mitnick. Svými průniky do systémů nejrůznějších společností údajně způsobil škodu téměř 300 milionů dolarů. Sám o sobě říká: „Před skutečným hackingem jsem se věnoval phreakingu. To je zkoumání telefonních sítí přibližně stejným způsobem, jakým dnešní hacker zkoumá sítě počítačové". Třeba domácí stanici jednoho svého kamaráda jsem změnil v ústředně na veřejný telefonní automat. Takže když dotyčný kamarád chtěl telefonovat a zvedl sluchátko, ozvalo se: „vhoďte prosím minci".

Kolem legendárního hackera se navíc vytvořil velkolepý mýtus, který mu přisoudil nabourání databází FBI a úpravu záznamů o své osobě. Podařilo se mu prý dostat do počítačů amerického Pentagonu a byl na jediné kliknutí myši od rozpoutání jaderné války. Jakkoli je jeho legenda populární, zdá se, že mnoho je mu přidáváno. Sám Mitnick označuje mnohé z těchto legendárních hacků za fámy, které měly s realitou jen velmi málo společného.

Dne 15. února 1995 byl zatčen a obviněn z krádeže, narušování soukromí a mnoha dalších trestných činů. I když se Mitnik bránil a objevily se názory, že celý případ je zinscenován a částky, které byly vyčísleny jako škoda, nemají reálný základ, byl odsouzen. Propuštěn byl 21.ledna 2000 s podmínkou, že se nesmí po následující tři roky dotknout počítače, což je paradoxní u vědomí toho, že většina útoků Kevina Mitnika byla založena na sociálním inženýrství. V současnosti je Kevin Mitnick uznávaným expertem na bezpečnost a vlastní firmu Mitnick Security Consulting, LLC[18].



Richard Matthew Stallman

Richard Stallman, hacker „staré gardy", je znám spíše jako propagátor a zakladatel „Free Software Foundation" a „League for Programming Freedom". V roce 1971, když navštěvoval první ročník Harvardské univerzity, pracoval jako programátor v laboratoři umělé inteligence na MIT, kde se stal členem tamější hackerské komunity. Po absolvování bakalářského studia fyziky přešel na MIT, nicméně studium nedokončil a zůstal na svém původním místě programátora.

Během svého působení v laboratoři umělé inteligence byl Stallman významným kritikem omezování přístupu k výpočetní technice. Jeho reakce na instalaci přístupového systému v počítačové laboratoři MIT byla typická – prolomil heslo prostým zadáním nulového řetězce a všechny uživatele seznámil s tím, že odstranil přístupový systém.

Richard Matthew Stallman, sám sebe označující za „RMS" je typickým příkladem člena staré gardy, bojující za svobodu v politice šíření informací a zejména softwaru. Stallman je sice prezidentem „Free Software Fundation", ale v duchu hackerských tradic nepobírá žádný plat. Nevlastní dům, automobil ani mobilní telefon. Údajně se vyjádřil tak, že mobilní telefon si koupí tehdy, až bude obsahovat volný software[J01]. Žije skromně z honorářů za své projevy, stipendií a cen (např. MacArthur Fellowship nebo Takeda Award).

4.4 Hackerské programové nástroje

Technologie, se kterou hackeři soutěží a kterou používají, nutně potřebuje programové nebo i hardwarové nástroje, aby ji bylo možno analyzovat a ovládat. Následující přehled hackerských nástrojů není samozřejmě úplný a zahrnuje převážně nástroje známější a používanější. Podle typu použití je možno hackerské techniky rozdělit na:

- ✓ Hardwarové nástroje, kam patří např. techniky hledání bezpečnostních děr v čipových kartách. Bylo by mylným předpokladem do hackerské komunity zahrnout pouze programátory, vždyť první techniky phreackerů byly v podstatě hardwarové blue-boxy a tímto označením se mnohá technická zařízení pro neoprávněný přístup označují dodnes.
- ✓ Softwarové neboli programové nástroje, které v hackerské komunitě převažují a jejich přehled je uveden v následujících kapitolách.
- ✓ Sociální inženýrství, neboli techniky zneužití lidského elementu.

I když se hackerské nástroje neustále zdokonalují a automatizují, nejdůležitější součástí hackerského útoku je a zůstává sama osoba hackera. Jsou to jeho nabyté vědomosti, znalosti a dovednosti, které určují úspěšnost útoku. Bezhlavé použití volně dostupných nástrojů tak, jak to předvádějí script-kiddies, může být sice nebezpečné, ale s prvým hackingem to nemá nic společného.

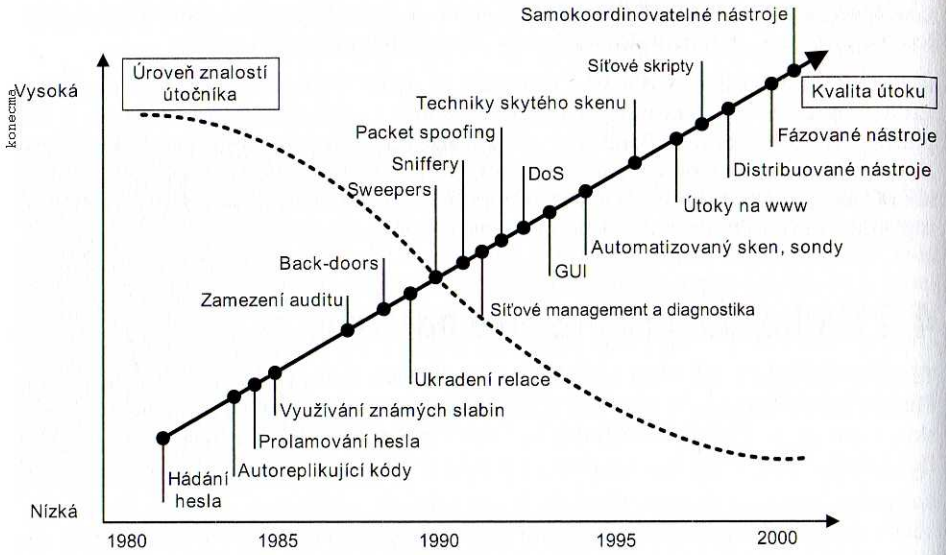
4.4.1 Vývoj hackerských nástrojů

První hackerské nástroje z počátku osmdesátých let minulého století byly založeny na schopnosti hackera pochopit psychologii obsluhy počítače a uhodnout používané heslo. Vzhledem k malému zabezpečení tehdejších systémů a nepatrné povědomosti obsluhy těchto systémů o zajištění bezpečnosti uložených informací nebylo uhodnutí hesla pro dobrého psychologa většinou složité. V polovině osmdesátých let se objevují první autoreplikující kódy a prolamovače hesel, založené na postupném zkoušení možných kombinací povolených znaků. Zároveň se objevují první skutečně hackerské pokusy o odhalení chyb nebo slabin systému a jejich využití.

[16] Americká administrativa ho obvinila podle tzv. Computer Fraud and Abuse Act.

[17] Po návratu z vězení se pohyboval v různých zaměstnáních a jeho snad nejpikantnější pozice byla správce sítě pro „Ig Nobel awards", což je ceremonie pořádaná časopisem parodujícím vědecký svět.

[18] Viz internetové stránky www.mitnicksecurity.com a další servery patřící jeho firmě (např. defensivethinking.com, mitsec.com, kevinmitnick.com nebo mitnicksecurity.com). Tyto webové servery se staly předmětem hackerského defacementu v roce 2003, kdy je napadla skupina DkD[!] a BugBear. V roce 2006 se útok opakoval, tentokrát ze strany pakistánské skupiny FBH. Stránky obsahovaly velmi vulgární výrazy napadající Kevina Mitnika.

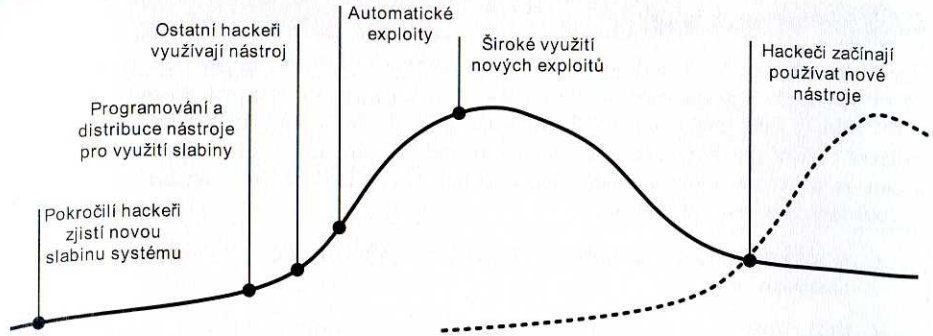


Obr. 4.2: *Historie vývoje hackerských nástrojů*

V té době se významně rozvíjí síťování počítačů a do hry vstupují síťové protokoly se všemi prvotními nedostatky, techniky vzdáleného přístupu a systémy řízení přístupu. Objevují se první back-doors následované technikami o podvržení nebo ukradení síťové relace. Aby hacker zjistil, jakým způsobem je možno síť napadnout, musel nejdříve odposlechnout provoz, k čemuž sloužily sniffery, a následovně zakrýt svoji skutečnou síťovou totožnost podvrženými pakety (packet spoofing). Mezi hackerské nástroje vstupuje první skutečně síťový útok založený na malé propustnosti přenosového kanálu – Denial of Service.

Současně se složitostí přípravy i vlastního útoku se objevují nástroje vybavené grafickým rozhranním a zavádí se automatizace některých kroků založená buď na náhodné volbě dalšího kroku nebo na analýze odezvy cíle útoku. Automatizace síťového skenu a techniky skrytého skenu rozšiřují možnosti útočníků při odhalování slabých stránek systémů a zejména již rozšířených webových technologiích. Následující generace nástrojů je již sofistikovanou verzí poměrně složitých řadičů distribuovaných metod útoku, jež umožňují postupné fázování útoku, změnu nebo modifikaci útoku podle reakce cíle a vzájemnou koordinaci distribuovaných nástrojů.

Se vzrůstající složitostí sítí a náročnějšími analýzami chráněných systémů vzrůstá i složitost hackerských technik a nástrojů. Ochranné systémy umožňující včasné varování před útokem jsou další mezí, kterou musí hackerské nástroje zvládat, přizpůsobovat časování ataků, metody a postupy útoku tak, aby nebyly příliš brzo odhaleny. Přípravě nových nástrojů se věnuje jen hrstka skutečně špičkových hackerů, ostatní, alespoň se lze domnívat, jsou produktem týmové práce programátorských skupin pracujících v žoldu organizovaného zločinu, terorismu nebo zvláštních služeb, specializujících se na vedení informatického boje.



Obr. 4.3: *Životní cyklus exploitu*

Exploit, neboť tak se program pro využití slabiny systému nazývá, nemá příliš dlouhou životnost. Jak je uvedeno na obr. 4.3, po analýze systému a objevení nové slabiny pokročilými hackery následuje programování nástroje a jeho distribuce. Nový nástroj začínají využívat ostatní hackeři, avšak protože se ze začátku šíří pouze v užší hackerské komunitě a zdokonaluje se, jeho použití je omezené. Následuje vydání automatizovaného nástroje, který stačí stáhnout a spustit, což je pravý ráj pro script-kiddies. Exploit se začne široce využívat, všimnou si ho dodavatelé operačních systémů a antivirových programů a vydají „patch" neboli záplatu. Pečlivější správci systému novou bezpečnostní záplatu co nejdříve nainstalují a původní exploit ztrácí smysl a mizí z hackerského světa. Protože však slabin neubývá, objeví se exploit na novou slabinu a celý životní cyklus se opakuje.

Toto je běžný a neustále se opakující cyklus hrozby a protiopatření, který doprovází celou bezpečností problematiku v informatice. A protože útočník je vždy o krok před správcem systému a pravděpodobně se nikdy nepodaří aby tomu bylo naopak, je tento životní cyklus základním rytmem boje s kybernetickými útoky.

Vývoj hackerských nástrojů velmi přesně kopíruje vývoj softwaru a je zejména ovlivňován novými bezpečnostními politikami, které jsou v programovém díle realizovány. Doba, kdy otevřenost systémů a jejich nedokonalost umožňovala různé triky z příkazového řádku již odezněla. Současné hackerské nástroje se však vyvíjí nejenom s novými bezpečnostními politikami, ale rovněž se rozšiřují s novými softwarovými technologiemi. Četné a stále se vyvíjející webové technologie vedou např. k přípravě infikovaných vestavných podprogramů (plug-in), mobilních kódů nebo upravených skriptů.

Postup ve zdokonalování hackerských nástrojů se samozřejmě promítá i do vývoje hackerské komunity. Dá se tvrdit, že zhruba do roku 1985 byla hackerská komunita společností odborníků, kteří přesně věděli co mohou způsobit a dokázali odhadnout důsledky svého konání. Postupně s rozšiřováním povrchních znalostí o výpočetní technice, a tedy i o hackingu, začali do komunity pronikat jedinci, kteří chápali hacking jako prostředek zviditelnění, prosazení nebo získání nějaké moci. První vážné počítačové podvody, ke kterým došlo na konci osmdesátých let a jejichž následkem došlo ke kriminalizaci hackerské komunity, byly právě projevem penetrace hackerské komunity takovými jedinci.

Spolu s vývojem hackerských nástrojů, doplňováním automatizmů a „user-friendly" interface se do hackerské komunity zahrnuje i velká skupina „kvazihackerů", kteří nejsou schopni odhadnout následky svého konání. Mnohdy používají takové vysoce automatizované nástroje i děti a adolescenti s minimálními znalostmi výpočetní techniky. Původní hackerská komunita se ztrácí a nastupuje nová, daleko agresivnější avšak méně odborně připravená komunita „lammerů".

konecma

4.4.2 Prolamovače hesel

„Password crackers" jsou jedním z nejstarších nástrojů používaných hackery. Slouží, jak již název napovídá k prolomení ochrany nebo autorizace, která je prováděna statickým heslem[19]. Princip jejich práce je jednoduchý – zkouší nejrůznější kombinace znaků, které podle uvážení autora prolamovače nebo jeho uživatele připadají v úvahu a pokud autorizace projde je nalezené správné heslo odesláno hackerovi. Existují dva základní druhy útoků realizovaných prolamovači hesel:

- ✓ slovníkové útoky (dictionary attack), které zkouší použít známá slova z vlastní databáze slov,
- ✓ útoky hrubou silou (brute-force attack), které postupně generují všechny možné kombinace potřebné délky z vybraných znaků a zkouší, zda náhodou nevyhovují zadanému heslu.

Kvalitní prolamovače obsahují slovník možných znakových kombinací, z nichž sestavují hesla, což umožňuje rychlejší nalezení shody, neboť jsou odstraněny zcela nesmyslné (alespoň podle autora slovníku) kombinace znaků. Jejich použití je snadné, mnohdy disponují kvalitním a přehledným grafickým rozhranním, které umožňuje nastavit parametry prolamování hesla. Jejich kvalita se dá posoudit podle obsahu slovníku a zejména rychlosti se kterou dokáží generovaná hesla ověřovat.

Dnes je volně k dispozici množství prolamovačů a nalezení vhodného volně stažitelného prolamovače na internetu není žádným problémem. Rychlost prolamovačů používaných na odhalení hesel k zakódovaným souborům např. Microsoft Word nebo Acrobat se pohybuje zhruba od 50 000 hesel za sekundu na běžném počítači, existují však i velmi kvalitní prolamovače schopné ověřit až milion hesel během jedné sekundy. K nejvýznamnějším faktorům které ovlivňují rychlost prolamovače patří:

- ✓ rychlost počítače, na němž nástroj běží,
- ✓ typ prolamovaných dat, resp. typ souboru,
- ✓ umístění dat nebo souboru (na lokálním disku, v síti, na webu apod.),
- ✓ struktura zakódovaného souboru.

Pro zajímavost je možné uvést tabulku s odhady času potřebného na prolomení hesla, když budeme používat běžný stolní počítač a metodu hrubého útoku. Tato tabulka vychází z počtu všech možných kombinací použitých znaků a odhadované rychlosti práce běžného prolamovače – viz Tab. 4.2. Jak je vidět, vyplatí se delší heslo, složené z co nejširší kombinace znaků.

[19] Moderní bezpečnostní techniky používají dynamických hesel, které jsou závislé na čase přístupu a uživatel musí vždy použít zvláštní kalkulátor k vygenerování aktuálního hesla.

Kombinace použitá pro heslo	Odhad doby práce prolamovače
4 velká nebo malá písmena	několik sekund
4 velká a malá písmena, libovolně kombinovaná	několik sekund
4 velká a malá písmena a číslice v libovolné kombinaci	několik sekund
5 velkých nebo malých písmen	méně než jedna minuta
5 velkých a malých písmen v libovolné kombinaci	cca 6 minut
5 velkých a malých písmen a číslic v libovolné kombinaci	cca 15 minut
8 velkých nebo malých písmen	cca 58 hodin
8 velkých a malých písmen v libovolné kombinaci	cca 21 měsíců
8 velkých a malých písmen a číslic v libovolné kombinaci	cca 7 let
10 velkých nebo malých písmen	cca 5 let
10 velkých a malých písmen v libovolné kombinaci	cca 4648 let
10 velkých a malých písmen a číslic v libovolné kombinaci	cca 26984 let

Tab. 4.2: *Odhady doby práce prolamovače podle typu hesla*

V síťovém prostředí se nedají prolamovače použít přímo neboť autorizační algoritmy většinou obsahují ochranný algoritmus, který vyžaduje časový interval mezi dvěma zadáními hesla, a tak omezuje počet možných pokusů v daném časovém úseku. Často je omezen i počet „omylů" a po několika neúspěšných pokusech se přístup zcela zablokuje a o obnovení přístupu je třeba znovu absolvovat byrokratický postup přidělení nového hesla.

4.4.3 Backdoors

Backdoors neboli zadní vrátka jsou velmi výstižným názvem pro kódy, které po instalaci na cílový počítač umožňují jeho vzdálené řízení. Jedná se o oblíbený hackerský nástroj a jakmile hacker objeví bezpečnostní díru, jeho prvním krokem je nainstalování backdoors. Typický hacker má vždy v záloze několik počítačů s tajně nainstalovaným nástrojem pro vzdálené řízení a čím je lepší, tím více strojů má k dispozici. Tyto, tzv. kompromitované stroje jsou pak používány k podnikání dalších útoků na cílový stroj. Často tento řetěz mezi útočníkem a cílovým strojem může mít i deset nebo více zkompromitovaných strojů, které izolují a chrání původního útočníka před odhalením.

Kvalitní backdoor lze těžko zjistit, zvláště pokud není často používán, a hackerovi poskytuje úplnou kontrolu nad kompromitovaným strojem. Komunikace mezi nástrojem uvnitř kompromitovaného počítače a hackerem se uskutečňuje pomocí nástrojem spuštěné služby na portu s vysokým číslem nebo je maskována jako standardní služba jako např. http (webový přístup, port 80), telnet (terminálový přístup, port 23) nebo ssh (kryptovaný kanál na portu 22). Tyto maskované služby většinou nejsou odfiltrovány firewally, a tak jsou přístupné i přes bezpečnostní prvky sítě. Moderní backdoors mají zdokonalenou komunikaci a využívají většinou protokolů některých interaktivních nástrojů komunikace jako je IRC, oblíbené ICQ nebo MSN messenger. To umožňuje lepší ukrytí komunikace a jistý komunikační komfort.

Jeden z nejslavnějších backdoors se jmenuje Back Orifice a přesto, že byl poprvé představen na konferenci „Black Hat Security" v roce 1998, je dodnes volně stažitelný z in-

ternetu[20]. Jeho původní verze umožňovala úplnou kontrolu nad systémy Windows 95 a Windows 98 a to včetně editování souboru registrů, restartu počítače nebo zobrazení hesel z vyrovnávací paměti počítače či sdílení prostředků. Back Orifice může být doplňován dalšímu funkcemi, které rozšiřují možnosti jeho použití[21]. Po proniknutí do cílového počítače je Back Orifice nainstalován jako běžný .exe soubor[22] a po startu počítače je spuštěn jako běžná služba.

Po úspěchu původní verze byla připravena i zdokonalená verze umožňující kompromitaci systémů Windows NT a Windows 2000 pod názvem Back Orifice 2000[23]. Tento nástroj obsahuje celou řadu vylepšení, např. vývojový kit umožňující vytvářet obtížně detekovatelné mutace, skrytý režim práce, kdy se maskuje jako „Remote Administration Service", nebo vlastní maskování v tabulce běžících procesů jako „explorer.exe".

Od Back Orifice bylo odvozeno několik dalších nástrojů, z nichž nejznámější je NetBus. Poskytuje lepší grafické rozhranní než Back Orifice, má přehlednější ovládání, avšak komunikuje prostřednictvím protokolu TCP na portech 12345 a 12346, což zjednodušuje jeho odhalení a zvyšuje pravděpodobnost odfiltrování této komunikace firewallem. Do třetice zbývá jiný populární backdoor agent, SubSeven, který vykazuje větší stabilitu, je jednodušší při používání a má více funkcí než Back Orifice nebo NetBus. Mezi zajímavé funkce SubSeven patří např. možnost ftp připojení celého disku C:, kdy se napadený počítač tváří jako FTP server, skenování portů z kompromitovaného počítače nebo funkce pro vtipálky – ukradnutí myši či možnost vzdáleného tisku.

4.4.4 Skenery

Skenery slouží pro zjištění otevřených portů počítače, a tedy i služeb, které na něm běží. Skener tak útočníkovi velmi rychle zjistí základní informace o cílovém počítači a může sloužit i k získávání informací o operačním systému. Sken otevřených portů může být předzvěstí potenciálního útoku, a proto systémy se snaží tyto tzv. portskeny detekovat a spojení s možným útočníkem na nějakou dobu přerušit nebo učinit jiná bezpečnostní opatření.

Problém skenování spočívá zejména v různých nebo spíše různě přesných implementacích síťových protokolů, resp. jejich standardů. Tyto odchylky v implementaci na jedné straně mohou skenování značně komplikovat a dávat falešné výsledky, na druhé straně ale umožňují nenápadnou detekci systémů podle odchylek v detailech implementace standardů. Kromě detekce otevřených portů umožňují skenery i identifikaci služby, která jen běží na příslušném portu.

Skenerů existuje celá řada, je možné vzpomenout např. „Strobe" pro FreeBSD, nebo NetScan a SuperScan pro platformu Windows.

4.4.5 Sniffery

Slovo „sniff" znamená v angličtině „čichat", „čenichat"nebo „čmuchat" a název „sniffer" je tedy přiléhavou volbou pro program odposlouchávající síťový provoz a „čmuchající", co se kde děje. Nejedná se přímo o nástroj útoku, spíše o prostředek k shromáždění informací potřebných pro přípravu útoku. Rozhodující pro získání správných informací je umístění snifferu v síti. Zejména v přepínaných sítích, kde je společný segment minimalizován, je použití snifferu problematické, neboť většina informaci jde mimo sniffer.

Práce snifferu je jednoduchá, přepne síťové rozhranní do tzv. promiskuitního módu, a tak přijímá všechny pakety, které se na síti pohybují bez jakékoli další filtrace. Tyto pakety jsou zaznamenány a dále analyzovány – typ protokolu, IP adresy, MAC adresy, nastavění příznaků apod. Součástí analýzy je vydělení datové části s obsahem přenášené zprávy. Tak je možno odposlechnou komunikaci v síti, zachytit otevřeně přenášená hesla nebo jiné citlivé údaje.

Nejjednodušší sniffery jako např. Ethereal zobrazují analýzu obsah paketů ve struktuře paketu podle příslušného standardu, přičemž výpisy údajů včetně přenášených informací jsou v hexadecimální nebo znakové formě. Do jisté míry jsou schopny složit celý průběh relace, ale je vždy obtížnější se v datech vyznat. Profesionální sniffery nebo specificky zaměřené sniffery dokáží složit celou relaci a zobrazit ji v běžné formě. Např. sniffer odposlouchávající pouze spojení elektronické pošty dokáže analyzovat a složit přenášené informace tak, že výsledek je podobný typickému mailovému archivu ve formě webových stránek. Jiné profesionální sniffery dělí síťový provoz podle protokolů v graficky přehledném stromě a hacker, nebo ten kdo sniffer používá, si může vybrat jaký provoz chce sledovat.

Mimo uvedeného příkladu sniffer Ethereal, je možno vzpomenout např. BUTT, což je klasický sniffer pro Windows NT, nebo dsniff, jenž obsahuje speciální funkci na odchytávání autentizačních sekvencí.

4.4.6 Rootkity

Rootkit je podle definice soubor technik pro skrývání činností prováděných na operačním systému. Samotný název „rootkit" je poněkud zavádějící a vychází z prostředí v němž rootkity vznikly – z unixových operačních systémů a vychází z pojmenování účtu superuživatele, neboli administrátora unixového systému. Jedná se vlastně o podmnožinu nástrojů back doors a i jejich funkce je velmi podobná. Avšak na rozdíl od backdoors, které na unix-like systému budou pravděpodobně brzo odhaleny, rootkit zůstává po kompromitaci účtu superuživatele stále v utajení. V praxi jde vlastně o upravené běžně užívané systémové programy, jako např. ps, top, inetd nebo jiné, které jsou modifikovány tak, aby administrátor nic nepoznal a hacker měl ke stroji neomezený přístup.

První techniky typické pro rootkity se objevily v osmdesátých letech a jejich účelem bylo většinou odstranění záznamů o podezřelých aktivitách uživatelů, tedy vlastně vymazání části nebo celého záznamu o provozu – logu. V roce 1994 se objevil první rootkit pro operační systém SunOS a o dva roky později Linux rootkit. Do historie rootkitů se nepřímo zapsal Back Orifice, který ukázal na nedostatky v systému Windows. Moderní rootkity s důmyslnými backdoors a odposlechem sítě se objevují až po roce 2002.

Do povědomí laické veřejnosti vstoupily rootkity v souvislosti s aférou firmy Sony BMG Music Entertaiment. I když se jednalo o zdánlivě promyšlený tah proti počítačovému pirátství a porušování autorských práv, dopad skandálu na společnost Sony byl nesmírný. Vše začalo tak, že firma Sony se pokusila o implementaci systému XPC[24], jenž měl působit jako ochrana autorských práv ve stylu DRM[25]. Princip této ochrany spočívá v tom, že na kompaktním disku je na datové stopě nahrán zvláštní program označovaný jako XCP. Při

[20] Pro případné zájemce je na adrese www.cultdeadcow.com/tools.

[21] Např. jedna rozšiřující funkce dokáže připojit kompromitovaný počítač na specifický IRC kanál označený #BO_OWNED a oznámit jeho IP adresu. Každý, kdo je na tento kanál připojen, může kompromitovaný počítač ovládat pomocí Back Orifice klienta.

[22] Implicitní jméno tohoto souboru je <mezera>.exe.

[23] Volně ke stažení na adrese http://sourceforge.net/projects/bo2k, kde jsou rovněž verze pro Linux, Windows XP a další.

[24] Rozšířená ochrana proti kopírování – eXtended Copy Protection. Jedná se o programový balík, která byl vyvinut britskou firmou „First 4 Internet" a prodáván jako ochranný systém pro kompaktní disky.

[25] DRM – Digital Rights Management – metoda řízení přístupů k dílům, jež jsou předmětem autorské ochrany.

pokusu přehrát tento disk na počítači s operačním systémem Windows, se bez vědomí uživatele nainstaluje XCP do počítače a umožní přehrát disk ve vlastním počítači, ale zabrání v přístupu ostatním programům, a tak znemožní kopírování disku nebo vytváření MP3 z obsahu disku. XCP se nainstaluje skrytě tak, že jej není normálními prostředky vidět a uživatel nemá ani žádnou možnost ho odinstalovat. Pro tyto vlastnosti se kompaktním diskům firmy Sony obsahujícím XCP vžilo označení Sony rootkit.

Antipirátský pokus firmy Sony byl odhalen a publikován hackerem Markem Russinovichem [R02] a následovaly protesty uživatelů a žaloby na firmu Sony. Následovně firma Sony vydala opravný program, který měl vše uvést na pravou míru, nicméně výsledek byl zcela opačný. Záplata totiž neodstraňovala XCP, prováděla jenom změny, které nic neřešily a navíc vytvářely v systému bezpečnostní díru. Nakonec byla firma Sony donucena stáhnout všechny nosiče s XCP a vyměnit je zákazníkům bezplatně za média, která XCP neobsahovala. To byl smutný konec jednoho rootkitu, který však veřejnost na existenci podobného software upozornil.

4.4.7 Nástroje DoS

Zkratka DoS znamená „Denial of Service", neboli potlačení služby. Tento typ útoku doznal rozkvětu na přelomu století a od základního potlačení služby se dále odvozují specifické útoky podobného ražení, jako např. potlačení přístupu DoA – „Denial of Access". Myšlenka tohoto útoku je jednoduchá – pokud nemohu zaútočit přímo na cílový stroj, zaútočím na jeho spojovací cesty. Existuje několik základních metod DoS:

- ✓ zahlcení odesíláním jalových paketů z více strojů (tzv. DDoS – Distributed Denial of Service),
- ✓ zahlcení příkazem ping do sítě cílového stroje,
- ✓ zahlcení volných systémových prostředků.

V prvním případě musí útočník kompromitovat dostatečné množství strojů, aby složením jejich přenosových kapacit, resp. kapacit spojových cest, jimiž jsou připojeny, převýšil přenosovou kapacitu kanálu, kterým je připojen cílový stroj. Z kompromitovaných strojů pak začne posílat libovolné pakety na IP adresu cíle a vzhledem k jejich množství dojde k zahlcení přístupového kanálu k cílovému stroji, jenž se tak stane nepoužitelný. Nevýhodou tohoto postupu je nutnost získání dostatečného množství kompromitovaných strojů a ztráta kontroly nad těmito stroji v okamžiku spuštění útoku. Obranou je relativně jednoduché odfiltrování adres kompromitovaných strojů na směrovačích.

Druhý případ využívá vlastnosti síťových mechanizmů a zejména protokol ICMP[26]. Jednou z vlastností tohoto protokolu je možnost zjištění existence počítače s danou IP adresou pomocí příkazu ping. Pokud však odešleme příkaz ping na adresu sítě, nikoliv počítače, odpoví nám všechny počítače v příslušné síti. Útočníkovi tedy postačí, aby na adresu sítě poslal příkaz „ping" s podvrženou adresou cílového počítače a ostatní počítače v síti se postarají o zahlcení cílového počítače odpovědmi na ping.

Poslední možnost je zahlcení pakety SYN, což jsou pakety používané pro sestavení spojení v protokolu TCP. Systém, který obdrží paket SYN, odešle odpověď a čeká na potvrzení spojení. Tento čas čekání se pohybuje v desítkách vteřin až minutách a během této doby jsou rezervovány příslušné systémové prostředky pro chystané spojení. Pokud tedy útočník odešle např. sto paketů typu SYN na cílový stroj, pak zcela jistě vyčerpá volné systémové prostředky a cílový stroj se stane nepřístupným – nemá k dispozici dostatek prostředků pro realizaci spojení.

[26] Internet Control Message Protokol.

4.4.8 Trojské koně

Trojské koně patří mezi nejoblíbenější hackerský nástroj současnosti. Jedna se o malé programy, které jsou zabaleny do volně stažitelného kódu utility nebo do nové bezplatně poskytované hry. Trojské koně se používají na nejrůznější účely, od pouhého monitorování činnosti cílového počítače až po zneužití pro útok DoS. Zajímavou variantou trojských koní jsou „dataminery[27]" neboli programy, které po nainstalování monitorují činnost uživatele a zajímavé údaje odesílají do sběrného místa. Ty rozlišuje podle předem známých kritérií, např. při přihlašování k účtu v bance zaznamená stisknuté klávesy, a tak prozradí hackerovi přístupové kódy k manipulaci s účtem[28].

Mezi známé trojské koně patří např. Whack-a-mole, což je hra s krtkem obsahující uvnitř backdoor program NetBus, BoSniffer, který se tváří jako program na odstranění backdoor programu BackOrifice, ale ve skutečnosti ho sám instaluje. Existují nástroje, které umožní vytvořit vlastní program s trojským koněm. Např. nástroj eLiTeWrap spojí kód trojského koně a nosného programu, přibalí k němu nezbyté řízení pro rozbalování a vytvoří novou modifikaci trojského koně.

4.4.9 Nástroje průzkumu sítě

Nejdůležitější činností před každým útokem je průzkum terénu. Celou řadu informací může útočník získat z otevřených zdrojů, a tak nejobyčejnějším nástrojem je běžný prohlížeč. Na internetových stránkách firem je možno získat celou řadu informací nejenom o majiteli internetových stránek, ale často i o topologii nebo vybavení lokální sítě. Jedná se spíše o „sbírání střípků" a metody sociálního inženýrství, ale výsledkem může být poměrně kompaktní obraz cíle, který útočníkovi značně usnadní jeho záměr.

Při prohledávání webovských stránek se útoční nesoustředí jenom na vnější informace uveřejněné na vizuálním vzhledu stránky, ale otevře si její zdrojový kód, jenž může být zdrojem dalších zajímavých informací. Mnohé editory html stránek dávají do zdrojového kódu často další informace, jako datum a čas vzniku, informace o dalších stránkách nebo dokonce i jméno zhotovitele. Když nic jiného, otevřením kódu stránek se útočník dozví o nástroji, který je použit pro přípravu kódu, a tyto informace může dále využít.

Nástroje průzkumu sítě jsou většinou jednoduché programy, které zjišťují propojení a další technologické vlastnosti elementů cílové sítě. I obyčejný příkaz ping nebo tracert vede k získání celé řady informací o cílové síti. Hackeři tyto nástroje automatizovali, doplnili grafikou a lze je stáhnout nebo spustit přímo na internetu[29]. Úplným pokladem pro útočníka jsou špatně nakonfigurované DNS servery se záznamy o struktuře celé obsluhované sítě.

4.4.10 Debuggery

Nástroje používané běžně při ladění nového programu, jsou neodmyslitelnou pomůckou každého hackera. V okamžiku, kdy se podaří odhalit nějakou bezpečnostní díru, nastupuje analýza kódu a ověřování funkce exploitu, který bude zjištěnou bezpečnostní slabinu využívat. Postup je obvykle takový, že útočník se snaží vložit svůj kód do místa,

[27] „Data Mining" – dolování dat, techniky pro vyhledávání souvislostí v rozsáhlých databázích.

[28] Některé systémy obcházejí toto nebezpečí pomocí tzv. grafické klávesnice, což je obrázek klávesnice na displeji, na němž se znaky k odeslání vybírají myší. Nicméně, stejně musí být uloženy do nějaké vyrovnávací paměti, a tak dobře navrženého trojského koně neobelstí.

[29] Typickým serverem s množstvím vhodných nástrojů je http://tools-on.net A. K. Yezhova s řadou užitečných skriptů spustitelných i přes WAP.

které chce využít. Obvykle se ukládá jenom skok na adresu, kde bude uložen výkonný kód exploitu a zbytek se doplňuje nevýkonnými instrukcemi, např. NOP (No operation). Při napadení se provede skon na útočníkův kód, ten se vykoná a opět se skočí zpět do původního kódu.

konecma

Debugger umožní ověření správné funkce kódu, ale mnohdy i nalezení nejvhodnějšího místa pro uložení odskoku a výkonného kódu útočníka. Toho lze využít i při odhalování částí kódu pro kontrolu platné licence k programu. V tomto případě útočník zjišťuje, kde se ukrývá podprogram, kontrolující zda přidělené číslo licence odpovídá správnému číslu, a tedy zda program je provozován jeho původním vlastníkem. Crackeři používají debugger na nalezení tohoto podprogramu a jeho následné odstranění, čímž zbaví program jeho ochranných prvků. Takový program je pak možno spouštět nebo kopírovat bez toho, aby nový vlastník kopie disponoval uživatelským oprávněním k tomuto programu. Mezi populární debuggery v hackerské komunitě patřily Soft-Ice[30] nebo TRW 2000.

Jenom malé procento programátorů chrání své programy proti použití debuggerů. Existují dvě základní možnosti, jak program chránit:

- ✓ „antidebuggerovými" postupy při programování, kdy se vkládají instrukce a data v nezvyklém pořadí, což má vést ke zmatení debuggeru,
- ✓ vložením zvláštního kódu, který identifikuje stav, kdy program sám zjišťuje, že je zkoumán debuggerem a podle toho přizpůsobí své chování[31] [C04],
- ✓ zakódováním již přeloženého kódu[32].

Někteří programátoři namítají, že ochrana proti debuggerům nemá smysl, jiná skupina ji naopak velmi prosazuje. Je pravdou, že ne všichni crackeři dokonale ovládají antidebugingové triky, a tak stačí pouze nějaký jednoduchý „programový úskok", aby jim znesnadnil život. Mnoho crackerů spoléhá na debuggery, které jsou schopny odstranit antidebuggingové části programu, např. pro dřívější systémy Win9x, NT a Win2k to byly Frog-Ice nebo IceDump, avšak vývoj na obou stranách probíhá, a tak nemusí být vždy úspěšní. Nicméně je třeba si uvědomit, že ochrana použitím anti-debuggingových metod, která velmi dobře funguje na malém programu, může zcela selhat ve velkém programovém projektu.

4.5 Warez

Warez, neboli výroba a rozšiřování pirátského software, je trestná činnost, jejíž historie je delší než historie internetu. První pirátské kopírování hudby umožnily již audio kazety, technologie videa zase umožnila pirátské šíření filmů na videokazetách. Prvním masivně šířeným pirátským software byly hry na osmibitových počítačích. Zdálo se, že s nástupem nových nepřepisovatelných technologií CD-ROM a DVD se warez vytratí, avšak netrvalo dlouho než se objevily vypalovací zařízení, a tak dnes je pořízení digitální pirátské kopie levnější, než originál.

[30] Původní Soft-ICE pro DOS byl napsán zakladateli firmy NuMega Frankem Grossmanem a Jimem Moskunem v roce 1987. V současné době je tento debugger pro Microsoft Windows dodáván firmou Compuware, která provedla akvizici NuMega Technologies v roce 1997.

[31] Ke správné práci debuggeru je třeba, aby zkoumaný program bylo možno v libovolném místě zastavit. K tomu slouží tzv. breakpointy, ukazatele na místa v programu, kde chceme zastavit program. Běžnou metodou je, že instrukce v uvedeném místě se změní na instrukci přerušení (např. INT 3, kódovaný v architektuře Intel jako byte s hexadecimální hodnotou 0xCC) a v podprogramu přerušení se provede kód debuggeru. Např. tyto změny v programu umožňují detekování přítomnosti debuggeru.

[32] Často používaná tzv. XORovací smyčka, která na začátku programu „přeloží" jeho kód z jinak nečitelné formy. Existuje samozřejmě ještě celá řada požívaných metod, avšak není cílem této publikace je podrobně popisovat a čtenář jistě najde další zdroje informací v této oblasti.

Šíření nosičů a vytváření trhu warezu je však relativně pomalé, a proto opravdový nástup warezu nastal až s rozvojem rychlého internetu, odkud je možné stáhnout pirátské kopie programů, filmů nebo hudby již několik dnů po jejich oficiálním vydání. Aktivita warezu natolik pronikla do prostředí výrobců nosičů, že je možné získat pirátské kopie i týdny před tím, než dojde k vydání originálu.

4.5.1 Warez a jeho organizace

Warez tvoří uzavřená komunita lidí, jejichž „hobby" je zpřístupňování pirátských kopií na internetu ve formě tzv. „release". Tato komunita se nazývá „warez scéna" a vznikla již v době osmibitových počítačů Commodore 64, Atari a ZX Spectrum a dalších, které byly zejména zaměřeny na relativně jednoduché, avšak v té době nesmírně populární počítačové hry např. tetris. První šíření „release" probíhala na privátních BBS[33]. Později se warez scéna rozšířila na personální počítače a přesunula se vznikající celosvětovou síť internet. Předmětem warezu se tak kromě her staly i uživatelské programy, kopie audio CD v různých formátech, nejčastěji ve formátu MP3, kopie filmů na DVD[34] nebo digitalizované kopie klasických filmů.

Warez scéna je často popisována jako sportovní soupeření warez týmů [W03]. Základním pravidlem vydávání releasů jenom toho, co není volně a legálně k dispozici zdarma. Jednotlivé týmy se specializují na různé produkty a tedy i druhy releasů. I uvnitř těchto týmů může dojít k dalšímu dělení na skupiny specializující se jenom na příslušný okruh produktů – např. na různé hudební žánry (klasická, jazz ...), druhy filmů (klasické, akční, sci-fi, ...) apod. Týmy se identifikují jmény a jednotlivá release se označují zkratkou tohoto jména. Jméno týmu musí být na warez scéně unikátní a tvůrci nepostrádají smysl pro humor, a tak se objevují často různé slovní hříčky, např. „CiA" neoznačuje americkou zpravodajskou agenturu, ale skupinu „Crackers in Action". Členové skupin se identifikují přezdívkami a je pravidlem, že člen nesmí být ve více skupinách, pokud jsou konkurenční. Členové týmu komunikují většinou pomocí IRC a schází se na svém kanále, který je většinou chráněný dohodnutým heslem a skrytý před ostatními uživateli IRC. Oblíbenými IRC sítěmi jsou ty, který umožňují šifrovat připojení k serveru[35]. Nepovolaný uživatel nebo operátor serveru tak sice vidí komunikaci, nicméně jenom jako nesmyslnou změť znaků. Proti zjištění IP adresy připojených uživatelů se používají takzvané tzv. bouncery[36].

Warez scéna je velmi dobře organizovaná, její členové jsou z celého světa a mnohdy se osobně nikdy nepotkají, znají se jenom pod svými přezdívkami a funkcemi v týmu. Základní funkce v týmu jsou rozděleny následovně:

- ✓ Leader neboli vůdce skupiny rozhoduje o všem důležitém, včetně přijímání nových členů, kontroly chodu skupiny a jednání se „siteop" o „affils" – viz dále. Ve velkých skupinách má zpravidla několik pomocníků (councils), což jsou většinou spoluzakladatelé skupiny a společně vytvářejí pravidla, kterými se tým řídí.
- ✓ Supplier je osoba, bez níž se žádný tým neobejde, neměli by totiž co vydávat. Úkolem suppliera je zajišťovat nové, dosud nikým nevydané produkty pro release.

[33] BBS – Board Bulletin Service, komunikační server, k němuž se uživatelé připojuje prostřednictvím telefonního modemu a linky, předchůdce dnešních webů.

[34] Tyto kopie se pomocí ztrátové komprese DivX zmenšovaly na rozsah jednoho až dvou CD-ROM a záznam nevynikal žádnou zvláštní kvalitou. V současné době jsou však díky zvyšujícím se rychlostem připojení k internetu a diskovým kapacitám k dispozici i plné kopie disků DVD.

[35] Např. sítě EfNet a Linknet, které umožňují protokol SSL. V českém teritoriu to je např. server irc.sh.cvut.cz.

[36] Jedná se v podstatě o proxy server pro IRC, spouštěný většinou na kompromitovaném počítači. Jeho adresou je pak nahrazena skutečná IP adresu uživatele.

Supplier musí mít k danému produktu nějaký přednostní přístup a často to tedy jsou lidé z řad IT publicistů, beta testerů, prodejců software nebo pracovníků nahrávacích společností. Díky strategicky vhodně umístěnému supplierovi se mohou zejména hudba a filmy objevit na internetu i týdny před oficiálním uvedení na trh;

- ✓ Ripper je nižší úroveň crackera a jeho úkolem je převádět produkty od supplierů do podoby vhodné k release. Rukou rippera prochází produkt, který sice má ochranu proti kopírování, ale k jejímu překonání stačí dostupný software a hardware[37]. Mnohdy to technicky zručný supplier zvládne sám.
- ✓ Cracker patří k technicky nejvyspělejším postavám warez scény. Jejich úkolem je reverzní inženýrství a odstraňování ochran proti kopírování nebo nelegálnímu spouštění. Obvykle se jedná o velmi inteligentní jedince, většinou dobré programátory. Cracker soutěží nejen s obtížností ochrany, ale i s časem. Skupina si nemůže dovolit vydat nefunkční release, ale přesto musí být hotova jako první. Odstranění ochrany má několik základních variant:
  - ✓ *Získání platného licenčního klíče (viz carder). Nicméně existuje možnost, že program periodicky kontroluje svůj klíč na serveru výrobce a tak se snadno pozná, že byl klíč byl kompromitován.*
  - ✓ *Přepsání částí programu tak, aby žádný klíč nebyl vyžadován, případně stačila náhodná posloupnost znaků. Jakmile je takové místo v programu nalezeno pak se jeho modifikace týká několika instrukcí. Nejvíce je warez scénou uznáváno vytvoření generátoru klíčů, kdy cracker musí pochopit algoritmus kontroly klíčů natolik, aby jej byl schopen simulovat a vytvářet klíče pro zadané jméno nebo adresu. Výsledkem práce crackera je malý program - generátor klíčů (keygen), který se dodává spolu s původním programem[38].*
  - ✓ *U programů chráněných hardwarovým klíčem obchází crackeři tuto funkci programu pomocí modifikace software podobně jako při použití softwarových klíčů. Zkušenější crackeři někdy emulují funkci hardwarového klíče vlastním ovladačem příslušného portu (LPT, COM, USB). Pokud je jako hardwarový klíč použito instalační CD nebo DVD, cracker raději modifikuje program a ověřování originálnosti CD z něj odstraní.*
- ✓ Carder má za úkol získávat čísla a údaje o majitelích kreditních karet, které jsou pak zneužívány k online nákupům klíčů, původního software pro release nebo pro zajištění potřebného provozního vybavení. Čísla karet se většinou získávají napadáním špatně zabezpečených serverů s placeným členstvím, kam je zadávají sami jejich uživatelé při placení členského příspěvku[39].
- ✓ Tester má za úkol řádně otestovat připravený release a předá packagerovi, který ho připraví podle pravidel skupiny, doplní informační soubor .nfo[40] a předá release k distribuci.

[37] Jedná se zejména o audio CD a DVD filmy a jejich převod do vhodného tvaru, ve kterém jsou podle pravidel skupiny tyto produkty vydávány.

[38] Tato varianta selhává v případě, že program kontroluje vydané klíče na serveru výrobce. Rovněž v případě, kdy jsou klíče podepisovány pomocí asymetrické kryptografie, je nemožné generovat nový klíč bez znalosti tajného klíče výrobce.

[39] V převážné většině se jedná o porno servery.

[40] Neoficiální typ souboru .txt, který obsahuje jméno skupiny a základní údaje o release nelegálního software. Je součástí release a obvykle má charakter ascii-art, obrázku skládaného ze znaků ASCII.

- ✓ Siteop je správce warezového serveru a nemusí být členem žádné skupiny. Jeho úloha je samostatná a výjimečná, sám rozhoduje o tom, se kterými skupinami bude jednat o tzv. „affils"[41], vytváří a kontroluje pravidla site, udržuje server a IRC kanál, řeší problémy uživatelů.

Jak je zřejmé, warez scéna je velmi organizovaná, s vlastními pravidly a funkcemi jednotlivých členů. Spolu s tím, jak jsou měněna pravidla provozu na internetu nebo ochranné prvky programů a vyvíjen tlak na postih za šíření nelegálních kopií, mění se i warez scéna, precizuje svoji ochranu a metody komunikace.

4.5.2 Příslušníci warez scény a jejich motivace

Týmy warez scény zahrnují jednotlivce z celého světa. Skupiny bývají mezinárodní, jejich členové se většinou znají jen přes internet, společným komunikačním jazykem bývá angličtina. Stáří příslušníků warez scény se pohybuje většinou mezi sedmnácti až třiceti léty, ale nejsou výjimkou i starší jedinci. Nejčastěji se jedná o studenty, programátory, novináře a pracovníky hudebních nebo filmových vydavatelství.

Warez komunita je poměrně uzavřená okolnímu světu a je obtížné se do ní dostat, i když skupiny často rekrutují nové členy pomocí .nfo souborů. Většinou jde ale o pozice ve skupině, vyžadující buď mimořádné schopnosti (cracking, hacking), přednostní přístup k produktům (supplier) nebo možnost poskytnutí hardware či rychlého internetového připojení (siteop).

Základním principem není zisk a celá warez scéna je postavena na bázi non-profit[42]. Její členové nemají žádný zisk z toho, co pro scénu udělají a toto pravidlo dodržují. Jedním z nejpřísnějších tabu warez scény je vypalovat a prodávat release nebo prodávat či pronajímat získané účty na sites cizím osobám. Za takový přestupek je zjištěný viník bez milosti vyloučen, dostane zákaz přístupu na IRC kanál své skupiny a jsou mu odstraněny možnosti přístupu na FTP servery. Informace o viníkovi (přezdívka, IP adresy…) se rozešlou ostatním skupinám.

Motivace každého příslušníka warez scény, když chybí motivace zisku, může být odlišná, avšak lze nalézt společné prvky. Jednou z prvních motivací je rychlý přístup ke všem releasům ve scéně bez složitých hledání a čekání ve frontách. Uživateli releasů jsou tedy v první řadě členové scény samotné[43]. Druhým, téměř klasickým důvodem je touha po uznání a respektu. Tedy být členem té nejrychlejší skupiny a sdílet spolu s ostatními trochu uznání, které se mu v reálném světě nedostává. Respekt každé skupiny roste s počtem prvotních releasů, správci FTP serverů sledují, které skupiny vydávají nejvíc releasů a snaží se je získat jako své affils. Rovněž servery jsou hodnoceny podle poskytnuté diskové kapacity, rychlosti připojení a renomé affils skupin. Jedním z cílů skupin je dostat se na co nejlépe hodnocené servery, a tak získat nejlepší místo ve statistikách. Celá warez scéna připomíná velmi blízce týmové sportovní zápolení, kde vítězí ten nejrychlejší a nejaktivnější. Člen, který má slabé výsledky je nemilosrdně vyhozen ze skupiny, a na jeho místo nastoupí nový, jenž je přijat pouze na zkušební dobu, během níž musí prokázat své schopnosti.

[41] Affils (od affiliate – přidružený) je dohoda mezi skupinou a správcem FTP serveru, zajišťující pro server exkluzivitu ze strany skupiny. To znamená, že se každý release skupiny objeví na affils serveru s předstihem před ostatním.

[42] Abychom byli přesní. Bohužel neexistuje jen non-profit warez, ale i profit warez, který je pro společnost mnohem nebezpečnější.

[43] Typickým členem warez scény je fanda holdující netypickému hudebnímu žánru. Skupině, která je na tento žánr specializovaná poskytne několik originálních CD měsíčně, které sám zakoupí, a za to může snadno stáhnout všechna ostatní CD, která ten měsíc vyšla. Mnoho warezových týmů píše do svých .nfo, že jejich releasy jsou určeny pouze pro členy warez scény.

4.5.3 Prostředky šíření pirátských dat

Nejčastějším prostředkem pro šíření release slouží internetový protokol FTP popř jeho modifikace. Protože současné prostředky FTP umožňují přímé kopírování souborů mezi servery, klient FTP na straně člena warez scény může pouze řídit přesuny a přes jeho vlastní internetové připojení nemusí procházet žádné velké objemy dat. Tento druh přesouvání dat se nazývá FXP[44] a na jeho fungování je založena většina práce warez scény.

Síť warez scény se skládá z FTP serverů, které mají datovou kapacitu v řádu stovek gigabyte až několik terabyte a internetové připojení o rychlosti minimálně 10Mbitů, často i mnohem rychlejší. Operační systém těchto serverů je většinou Linux s implementovaným softwarem glFTPd nebo RaidenFTPd.[45] Na každém z těchto serverů je implementován vlastní IRC kanál, kam se mohou připojit uživatelé, kteří mají na server přístup. Na tento kanál vstupuje rovněž speciální skript provázaný s FTP serverem, který oznamuje aktivity probíhající na FTP serveru. Každý server je rozdělen na několik sekcí stanovených správcem, jenž se liší podle typu release (mp3, DivX, ...). Každá sekce serveru má stanovena vlastní pravidla omezující, jaké release se zde smí objevit[46]. Přístup na server mají zejména vybraní členové skupin, které mají uzavřenou s majitelem serveru (siteop) dohodou „affils", a jimž je přiděleno platné jméno a heslo unikátní pro každého uživatele.

Skupina nejprve připraví svůj release na svém FTP serveru[47] a pak jej pomocí FXP přesunou na své affil servery do skrytého adresáře a pomocí speciálního skriptu zpřístupní release na všech serverech najednou. Zpřístupnění release je automaticky oznámeno na příslušných IRC kanálech. Od této chvíle se release považuje za vydaný a kterýkoli uživatel serveru ho může zkopírovat pomocí FXP na další servery, k nimž má přístup. Motivací uživatelů serveru k šíření release je kreditní systém, kdy se každému uživateli počítá jako záporný počet bytů z dat, které přenesli z vlastního na jiný server, a jako kladný, většinou trojnásobný, počet bytů z dat nahraných na vlastní server[48]. Další motivací jsou statistiky jednotlivých uživatelů a skupin automaticky generované a zveřejňované o půlnoci vždy ze soboty na neděli.

Soutěžení skupin spočívá v tom, že stejný release nesmí vydat více skupin a vyhrává ta, která jej vydá jako první. Výjimkou je, když první skupina svým release poruší pravidla. V tom případě je release označen jako „nuked" a smazán z FTP serverů. Jiná skupina může vydat nový release[49], pokud prokáže chybu předchozí skupiny. Pravidla jsou stanovena pro celou warez scénu představiteli nejvýznamnějších skupin[50] specificky pro každý druh release.

Uveřejněním release končí „pobyt" nelegálního produktu v síti warez scény. I když by někteří její členové byli nejraději, kdyby ji nikdy neopustil, produkt se dále dostává mezi běžné uživatele nejrůznějšími způsoby. Původní warez byl šířen na volně dostupných warez serverech, nicméně jednalo se o metodu krajně nebezpečnou. V současné době převládají technologie založené na principu peer-to-peer[51], kde každý klient sítě nejenom stahuje od ostatních, ale rovněž poskytuje vlastní uložené informace ke stažení. Mezi nejpopulárnější sítě pro warez scénu patří technologie BitTorrent. Tento systém pro sdílení souborů na síti byl napsán Bramem Cohenen a nutí uživatele sítě, aby nejenom stahovali, ale rovněž poskytovali další obsah z vlastního repertoáru ke stažení[52].

I když BitTorrent[53], stejně jako všechny pirátské peer-to-peer sítě, vznikl s legálním cílem sdílení souborů se značným objemem dat, zejména různých distribucí Linuxu a dalšího volného software, časem se objem pirátského obsahu vyšvihl k téměř 50%. Využití BitTorrentu k distribuci warezu bylo umožněno vznikem specializovaných serverů, jež spojují funkce vyhledávání a poskytování souborů. Servery spravují moderátoři, jejichž hlavní činností je detekování a odstraňování torrentů[54] obsahujících falešná, nekvalitní, špatně pojmenovaná nebo duplicitní data.

Objem dat procházejících systémem BitTorrent může být ohromující. Snad nejobsáhlejší statistika systému byla uveřejněna v [B02], kde byla shrnuta data za osm měsíců měření sítě v měsících červnu 2003 až březnu 2004. Monitorovala se dostupnost jednotlivých komponent systému, přibývání nových torrentů, dostupnost trackerů a aktivity jednotlivých stahujících peerů. Zajímavé je, že uvedená statistika byla publikována IT zpravodajským serverem The Register dne 18. prosince 2004 [B03], tedy pouhé čtyři dny po vyhlášení války BitTorrentu americkou asociací filmového průmyslu (MPAA) [B04].

4.5.4 Válka s warez scénou – případ nikdy nekončícího souboje

Uveřejňování nelegálních warez kopií uměleckých děl a programů dělá starosti zejména organizacím na ochranu autorských práv. A tak válka vyhlášená americkou asociací MPAA (The Motion Picture Producers of America) byla pochopitelnou reakcí na ohrožení zisků filmového a gramofonového průmyslu. Hlavním cílem války vyhlášené BitTorrentu se logicky staly nejslabší místa technologie, servery a trackery .torrent souborů. Stejného dne finská policie na popud Business Software Alliance (BSA) zavřela a zkonfiskovala server s více jak 10 000 uživateli a provedla domovní prohlídku u třiceti moderátorů. [B05]. Následujícího dne sami operátoři BitTorrent serveru „suprnova.org" raději ukončili provoz [B06]. Další tiskové zprávy slavnostně ohlásily zatčení hongkongského piráta jako vůbec první případ kriminálního postihu běžného uživatele sítě Bittorrent [B07] a soudní procesech s moderátory šesti BitTorrent serverů [B08]. Bylo to poprvé, kdy nebyly cílem jen kopie DVD filmů, ale i televizní seriály pořízené digitálním záznamem. Zpráva také nadšeně

---

44 FXP – File eXchange Protocol je metoda přenosu dat, která používá FTP protokol pro přenos dat z jednoho FTP serveru na jiný FTP server bez nutnosti, aby data procházela počítačem připojeného klienta.

45 glFTPd (www.glftpd.com) a RaidenFTPd (www.raidenftpd.com) jsou přenosové metody podporující šifrovaný přenos dat mezi dvěma FTP servery.

46 Tato omezení zhruba odpovídají specializacím warezových skupin, tedy rozdělení dle žánrů hudby, u filmů minimální rating dle internetové databáze IMDb apod.

47 Tento server se v žargonu warez scény nazývá „dump".

48 Existují skupiny nazývané courriers, které samy nic nevydávají, ale pouze přenosem cizích releasů mezi servery se snaží získat co nejlepší hodnocení.

49 Označuje se jako tzv. „proper release", neboli „ten správný release".

50 K setkání dochází opět na IRC a stanovuje se např. jak má vypadat název release, minimální povinný obsah informačních .nfo souborů, kvalita mp3 souborů apod.

51 Peer-to-peer, neboli od uživatele k uživateli, je princip propojování v počítačových sítích, kde každá strana spojení jej může iniciovat a má stejnou odpovědnost. Označení „peer-to-peer" je matoucí, zejména je-li používáno v kontrastu s centrálně řízenými systémy. V praxi však sítě peer-to-peer potřebují pro svoji práci další informace z pomocného serveru. Např. známá síť Napster byla označována jako síť peer-to-peer, ale adresář uživatelů byl uložen na centrálním serveru.

52 BitTorrent byl poprvé uveřejněn v roce 2001 a podobná technologie je používána i ostatními populárními systémy pro výměnu souborů dat, např. KaZaA. Nepoužívají sice centrální adresář jako Napster, ale systém distribuovaných „hubů" nebo „supernodů", které slouží pro výměnu počáteční informace k založení spojení. Tak je zvýšena bezpečnost uživatelů proti odhalení i když různé organizace pro ochranu autorských práv používají podvržené „huby" nebo „supernody" pro odhalení uživatelů nelegálních produktů.

53 Viz www.bittorrent.com.

54 Torrent je malý soubor s koncovkou .torrent, který obsahuje metadata o poskytovaných distribuovaných datech ve formě hashů bloků těchto dat, a adresu speciálního serveru nazvaného „tracker", jenž sbírá informace o klientech zvaných „peer". Soubor .torrent je vystaven na stránkách poskytovatele. Uživatel si tento soubor stáhne a spustí BitTorrent klient, který se připojí na tracker a z něj získá IP adresy ostatních klientů. S nimi se pak klient přímo spojí a navzájem si vymění bloky dat. Hashe z .torrent souboru slouží k ověření integrity těchto bloků.

konec cma

konstatuje, že přes 90% dosud obžalovaných serverů bylo úplně zavřeno a celkový počet serverů v provozu se snížil o 40%.

Veškerý optimismus MPAA je však pryč za necelý týden – kopie dlouho očekávaného filmu „Star Wars 3: Revenge of the Sith" se objevuje na BitTorrentu již v den své celosvětové premiéry [B09]. Asi za týden MPAA oznamuje, že „Elite Torrents", server s více jak 100 000 uživateli a 8,5 miliony přístupů denně, který poskytoval Star Wars, je „odhalen a zavřen" [B10]. Je paradoxní, že tentýž den uvádí Bram Cohen do provozu oficiální vyhledávač torrent souborů a i když pouze indexuje obsah ostatních serverů a sám žádné torrenty neposkytuje, MPAA a ostatní organizace se na něj okamžitě zaměřily. I když až dosud není tvůrce protokolu součástí soudních jednání, neboť protokol je věc zcela legální, uveřejněním vyhledávače tvůrce pomáhá uživatelům najít ilegální obsah a to může být v budoucnosti použito proti němu.

Ztráty filmového průmyslu v důsledku pirátství byly vyčísleny na 3,5 miliardy dolarů v roce 2004, více než 5,4 miliardy v roce a stále se zvyšují. Organizace pro ochranu autorských práv využívají všechny dostupné prostředky, aby růst ztrát z porušování autorských práv zastavily. Neváhají sáhnout ani k výhružkám nebo zastrašujícím kampaním. Jsou však i tací, kteří si z těchto snah tropí žerty. Mezi ně patří např. norský server http://thepiratebay.org, který v části „Legal threats" zveřejňuje jak obsahy výhružných e-mailů od společností typu Microsoft, Dreamworks, EA, Sega nebo Apple, tak odpovědi správců serveru, v nichž se často těmto společnostem vysmívají.

Je zřejmé, že aktivity warez scény jsou vesměs ilegální, a tak logickou reakcí je aktivita represivních složek dotčených států projevující se v zatýkání a odsuzování členů warez scény k vězením nebo pokutám. Vzhledem k povaze a dokonalé organizaci warez scény to ale není jednoduché. Uzavřenost skupin, jejich globální působnost a příslušnost jejich členů k různých státním jurisdikcím znesnadňuje jak získávání důkazů, tak i možnosti reakce orgánů činných v trestním řízení. K účinnému zásahu je nutná přesná koordinace policejních složek v několika státech; ojedinělá akce jen utlumí na několik dní aktivity warez scény a většinou si vysloužíí posměch. Zásahy proti warez scéně jsou proto zřídkavé, ale dlouho připravované a poměrně rozsáhlé. Mezi největší známou akci patřila operace Fastlink [B11], která byla spuštěna dne 22. dubna 2004 v deseti evropských státech a USA najednou a trvala 24 hodin. Během této akce bylo identifikováno 100 osob[55], zajištěno 200 počítačů z čehož bylo 30 serverů obsahujících pirátský software v hodnotě téměř 50 milionů dolarů. Na akci v režii FBI, jejímž agentům se podařilo infiltrovat warez scénu, spolupracovaly organizace ochraňující autorská práva, jako BSA, ESA, MPAA a RIAA. Mezi zatčenými byl např. šestadvacetiletý šéfredaktor herního časopisu Game-Over.net z Los Angeles [B12], který byl crackerem herních ochran.

Každá taková akce část scény na nějakou dobu zastraší. Někteří raději odejdou nadobro, zejména starší členové, kteří si už vysloužili ostruhy, mají vlastní rodinu a nestojí jim za to riskovat v této adrenalinové hře. Aby však takové represivní akce měly trvalejší účinek, musely by se zřejmě odehrávat častěji a ve větším rozsahu. I když neexistují volně dostupné statistiky, z letmého pohledu na weby typu www.theisonews.com se nezdá, že by se počet releasů zmenšoval nebo zpomalovalo se jejich vydávání.

[55] Většinou se jednalo o leadery a jiné důležité členy skupin vydávajících release her jako Fairlight, Kalisto, Echelon, Class a Project X, a skupin produkujících soubory MP3, např. skupina APC.

5.

Kyberprostor a právo

Spolu s nástupem nových technologií se objevují i nové druhy trestné činnosti, kterým se lidská společnost snaží zabránit. Všeobecná deklarace lidských práv, Mezinárodní pakt o občanských a politických právech, různé mezinárodní dohody, smlouvy a deklarace, to všechno jsou nástroje, kterými chce společnost demonstrovat vůli se potýkat s nelegálními aktivitami[1] namířenými proti společnosti jako takové i proti členům této společnosti, lidem.

Protože právní předpisy vznikají po celou dobu existence lidstva jako formalizovaná projekce uznávané morálky společnosti, jejich vývoj je dlouhodobý a nestačí bouřlivému nástupu technologií. To je důvodem proč pro mnohé nelegální činy nemáme v současné době prostředky na jejich potlačení, neumíme je přesně definovat, a tak je nejsme schopni zařadit ani do litery trestního zákona. Nicméně v následujícím se pokusíme alespoň o přehled možností, které právní nauka skýtá, s cílem nalézt analogie nebo cesty, jež by posunuly naše právní chápání kybernetických trestných činů správným směrem.

[1] Právo chápe nelegální činnost jako činnost jsoucí v rozporu s právem. V tomto případě je však nelegální činnost chápána poněkud volněji, a to jakož i ty činnosti, které jsou sice společensky nebezpečné, ale nejsou regulovány právem, ačkoliv by se dalo očekávat, že by regulovány být měly.

Pro Českou republiku a její občany je důležité pojetí práva platné na území státu tak, jako pro občany jiných států pojetí práva v jejich zemi. Tento rozpor v právních systémech patří k největším problémům při postihování nelegálního chování v globálním kyberprostoru, např. v případech porušování autorského práva. Existují dva základní typy právní kultury – **právo kontinentální** a **právo angloamerické**[2].

Kontinentální Evropa vychází v současné formulaci práva především z práva přirozeného, což ji neodlišuje nijak významně od angloamerické právní kultury. Základní rozdíl je v pramenech práva, v jeho dělení na právo veřejné a právo soukromé, odlišné právní terminologii a v pojetí legality. V angloamerickém světě je právo neustále nově interpretováno a v nalézání správného rozhodnutí hrají roli nejen precedenty[3] ale i „zdravý rozum", který se opírá o přesvědčení, že dobro a zlo lze vždy identifikovat a na základě toho jednat. Základním kamenem angloamerického pojetí práva je ústava s neustále přidávanými doplňky a systém precedentů. Na rozdíl od angloamerického světa je Evropa postavena na konzervativní víře v morálně neutrální systém norem, které je třeba dodržovat a prostor pro jejich interpretaci je relativně malý. Kontinentální právo tedy vychází z ústavy a systému nižších právních norem – zákonů, vyhlášek a předpisů, které jsou schvalovány a vydávány zákonodárným sborem. Rozdíl mezi angloamerickou tradicí a evropským kontinentálním přístupem je patrný už z toho, že tam, kde angloamerické právo mluví o „vládě práva" (Rule of Law), Evropané mluví o právním státu (Rechtsstaat). Toto chápání práva se přenáší i do mezinárodních vztahů, a tak zatímco Evropané uznávají systém mezinárodního práva v jeho podobě po druhé světové válce, angloamerický svět mezinárodní právo interpretuje na základě „zdravého rozumu"[4].

Dalším důležitým pojmem pro pochopení práva je jeho dělení na **právo soukromé a právo veřejné**. Zatímco výrazným znakem veřejného práva je asymetrie jím upravených právních vztahů, odpovídající vztahu stát–občan, soukromoprávní vztahy lze charakterizovat symetrií a rovností účastníků. Tyto rysy veřejného a soukromého práva se promítají i do charakteru příslušných právních předpisů. Veřejnoprávní předpisy, např. trestní zákon, obsahují vesměs kogentní právní normy, které říkají přesně co musí nebo nesmí být provedeno a od těchto norem není přípustné se odchýlit. Tedy podle veřejného právo je možno dělat jenom to co právo přikazuje[5]. Naopak soukromoprávní předpisy, jejichž představitelem je třeba občanský zákoník, obsahují z větší části dispositivní právní normy, jež dávají stranám smluvní volnost. Soukromé právo, na rozdíl od práva veřejného umožňuje dělat vše, co není zákonem zakázáno.

Než se začneme zabývat právními aspekty kyberprostoru a kybernality, pokusme se shrnout základní principy, kterými se právní názory řídí[6] a upřesněme si pohled na trestní právo hmotné tak, jak jej chápe zákon č. 140/1961 Sb. ve znění pozdějších předpisů (Trestní zákon, dále uváděný jenom zkratkou TZ), a na procesní úkony v trestním řízení podle zákona č. 141/1961 Sb. v platném znění, neboli zákona o trestním řízení soudním. To je nesmírně důležité, neboť některé právní normy, které se zdají laikům zcela jednoznačné, mohou podléhat desítkám variant výkladů s protichůdnými závěry, i když všechny byly

[2] Správnější by bylo mluvit o typech třech – kontinentálním, angloamerickém a islámském, avšak v zásadě se označují za základní jenom první dva typy.

[3] V českém právu existují tzv. judikáty, což jsou publikovaná rozhodnutí soudů. Zvláštní význam pro trestněprávní praxi má „Sbírka soudních rozhodnutí a stanovisek", kde publikovaná rozhodnutí byla po připomínkovém řízení schválena k publikaci trestněprávním kolegiem Nejvyššího soudu České republiky. Judikáty, na rozdíl od precedentů, však nejsou právně závazné.

[4] Tyto rozdílné principy chápání práva se projevují i v názorech na vojenské zásahy USA ve světě, např. válka v Iráku. Jedná se o zásadní rozpor, který leží jako neřešitelná otázka mezi Evropou a Amerikou – viz např. [K01]

[5] Uvedený přístup je poněkud zjednodušující, vycházející z rozlišení podle právních subjektů. Zdánlivě tak dochází ke směšování „kogentnosti normy" s legální licencí, což by ve skutečnosti bylo nepřípustné.

[6] Právními principy se řídí nejenom právní názory, ale zejména aplikace a interpretace právní normy a samozřejmě i samotná tvorba právních norem.

učiněny na základě standardních výkladových metod a prostředků. Je nutné přiznat, že právní nauka má svoji logiku, která nemusí být vždy shodná s logikou informatika nebo člověka zabývajícího se informačními technologiemi, a s touto skutečností vždy počítat.

5.1 Krátký kurs trestního práva pro informatiky

Trestní právo, tak jak je obecně chápáno, je souhrnem právních norem práva veřejného, které chrání zájmy společnosti, práva a oprávněné zájmy fyzických a právnických osob před jednáním nebezpečným pro společnost. Za tím účelem stanoví co je trestným činem a jaké sankce, tedy tresty nebo ochranná opatření, je možno pachateli trestného činu uložit[7]. Trestným činem ve smyslu výše uvedených právních předpisů obvykle chápán čin nebezpečný pro společnost, jehož znaky jsou uvedeny trestním zákoně. Avšak čin, jehož stupeň nebezpečnosti pro společnost je nepatrný, i když jinak vykazuje znaky trestného činu, trestným činem není[8]. Při užívání a výkladu trestního práva je třeba rozlišovat:

- ✓ trestní právo hmotné specifikuje základní podmínky trestní odpovědnosti a uvádí výčet jednotlivých trestných činů[9] a sankce, které lze uložit pachateli za spáchaný trestný čin,
- ✓ trestní právo procesní, které upravuje postup orgánů činných v trestním řízení[10], a tak chrání práva a oprávněné zájmy fyzických i právnických osob

Spácháním trestného činu vzniká vztah mezi pachatelem trestného činu na jedné straně a represivními složkami státu, které jsou povinny dozírat na dodržování zákona, na straně druhé. Úlohou trestního práva je ochrana společnosti před trestnými činy a prostředky, které k tomu používá, jsou uvedeny v zákoně (např. tresty, ochranná nebo výchovná opatření apod.).

Je nutno si uvědomit, že účelem trestního práva není jenom represe, tedy újma, kterou je pachatel trestného činu nucen za spáchaný trestný čin strpět, ale i prevence, tedy zejména hrozbou takové újmy. Přitom prevenci trestných činů je nutno považovat za jeden ze základních úkolů trestního práva, přičemž je nutno rozlišovat:

- ✓ prevenci speciální, zaměřenou na odsouzeného pachatele trestného činu,
- ✓ prevenci generální, zaměřenou na ostatní členy lidské společnosti.

5.1.1 Zásady trestního práva

Trestní právo se vyvíjelo po celou historii lidstva a v různých dějinných obdobích mělo různý charakter. Mezi nejstarší zákonné předpisy patří tzv. zákony dvanácti římských desek[11], které obsahují kodifikaci římského práva a jsou výsledkem kompromisu mezi

[7] Po nabytí účinnosti zákona č. 218/2003 Sb. o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže již nejsou sankcemi jen tresty a ochranná opatření, ale též trestní a výchovná opatření. Trestním opatřením jsou např. obecně prospěšné práce, výchovným opatřením např. soudní napomenutí s výstrahou.

[8] U mladistvých se vyžaduje, aby nebezpečnost činu resp. provinění byla pro společnost „vyšší než malá" (viz § 6 odst. 2 zákona 218/2003 Sb.). Podobný požadavek je u některých trestných činů vojenských (viz § 218 TZ).

[9] Čin neuvedený v tomto zákoně není trestným činem.

[10] Upravuje mimo jiné postup při zjišťování trestného činu, při dokazování a rozhodování o spáchání trestného činu, ale také stanovuje úkony při výkonu rozhodnutí nebo předcházení a zamezování trestné činnosti

[11] Leges duodecim tabularum – dvanáct bronzových desek, které byly vystaveny na Foru Romanu. Tyto zákony byly sepsány v letech 451 až 449 př. n.l. několika desetičlennými radami decemvirů. Po vpádu Gallů do Říma (389 př. n.l.) se desky ztratily a je pravděpodobné, že byly zničeny a k jejich obnově již nedošlo.

patriciji a plebejci, kteří požadovali písemné sepsání zvykového práva neboť patricijové vždy vykládali nepsané zvykové právo ve svůj prospěch. I když desky byly později při vpádu Gallů zničeny, jednalo se o zásadní dokument, z něhož vycházelo nejen celé období římské republiky, ale navazovali na něj i římští císaři. Tyto desky obsahovaly zejména základy práva procesního, dědického, rodinného a základní zásady trestního práva, i když toto bylo pojato pouze okrajově.

Obecně přijatý názor je, že trestní právo má sekundární charakter, tedy je závislé na ostatních odvětvích práva – ústavním, občanském nebo rodinném. Tento názor zároveň vypovídá o charakteru trestního práva, který se označuje princip **„ultima ratio"**. To znamená, že trestní právo má zasahovat do společenských vztahů pouze tam, kde jde o závažné poruchy těchto vztahů a kde již nelze ponechávat na občanech či jiných subjektech, aby se nápravy domohli cestou jiného práva.

Zásady současného trestního práva formuloval v 18. století německý právník Anselm Feuerbach a shrnul je do čtyř základních pravidel, které označil jejich vlastnostmi v latině:

- ✓ **Stricta**, trestní právo se řídí pouze zákony včetně ústavních a nesmí být použity jiné podzákonné normy, např. vyhlášky.
- ✓ **Scripta**, zákon musí být psaný, což vylučuje použití např. obyčejů a zvykového práva.
- ✓ **Certa**, právní norma musí být jasná, srozumitelná i laikům, určitá a jednoznačná. Právě srozumitelnost zákona i laikům, kdy by se zákon měl vyhýbat vágním formulacím, je v některých jiných oblastech narušena „poslaneckou tvořivostí".
- ✓ **Praevia**, zákon, resp. v něm popsaný trestný čin musí být definován dopředu a teprve následovně aplikován.

Z výše uvedených pravidel se odvozují významné zásady trestního práva – **„nullum crimen sine lege"** – žádný trestný čin bez zákona – a **„nulla poena sine lege"** – žádný trest bez zákona. Z těchto dvou zásad vyplývá, že jenom zákonem je možné stanovit jaké jednání je trestným činem a jaký trest lze za spáchání trestného činu uložit[12]. Tedy trestný čin musí být přesně popsán v trestním zákoně a teprve tehdy, kdy jsou naplněny všechny jeho znaky, je jej možno za trestný čin označit. Zároveň pro každý trestný čin stanoví zákon druh a výměr sankce, která může být za dotčený trestný čin uložena.

Zákaz retroaktivity neboli zpětné působnosti, patří k dalším zásadám trestního zákona a vyjadřuje povinnost posuzovat trestný čin podle zákona, který byl v době jeho spáchání účinný. Tedy pokud čin v době jeho spáchání nebyl trestný, nemůže být jeho pachatel stíhán, přestože pozdější zákonná úprava mohla tentýž čin za trestný čin označit. Platí jediná výjimka – pokud by pozdější zákonná úprava byla pro pachatele příznivější, pak se jeho čin bude posuzovat podle této pozdější právní normy[13].

Zásada demokratismu spočívá v rovnosti všech občanů před zákonem a vyvozování individuální odpovědnosti za zavinění. Tato zásada vychází z konstatování, že bez svobody jednotlivce není ani svoboda společnosti a přiznává prioritu právům jednotlivců. Zároveň však je nutno dbát **zásady humanismu**, jenž spočívá na vyrovnanosti zájmů jednotlivce a celku, neboť trestní právo významně zasahuje do lidských práv, a tedy i přístup k pachateli musí být humánní.

[12] O vině a trestu v oblasti trestního práva může rozhodnout jenom soud [Z01].

[13] Viz čl. 40 odst. 6 Listiny práv a svobod [Z01] nebo § 16 Trestního zákona [Z02].

V **zásadě ekonomie** trestního práva se ukazuje pomocná úloha trestní represe, kdy prostředky trestního práva jsou až krajní a nastupují k ochraně zájmu až jako poslední[14]. Zásadou ekonomie se nazývá proto, že s vymáháním trestní odpovědnosti, ukládáním a výkonem trestů jsou obvykle spjaty ty největší náklady. Velmi specifickou zásadou je **zákaz analogie** k tíži pachatele, která je v trestním právu hmotném zakázána v jakékoliv formě. V trestním právu procesním je však analogie v zásadě přípustná a výjimkou jsou zejména případy zasahující do lidských práv. Zásada **„ne bis in idem"** – ne dvakrát v téže věci, se uplatňuje zejména v trestním právu procesním, i když její důsledky se projevují i v trestním právu hmotném[15].

5.1.2 Trestní právo a související obory

Trestní právo je nejenom prostředkem k uplatnění pořádku a nástrojem ochrany společnosti před nebezpečnými činy. Trestní právo je rovněž vědeckou disciplínou, která se dělí na dva obory:

- ✓ „de lege lata" zabývající se studiem současného trestního práva a jeho interpretací,
- ✓ „de lege ferenda", což je spíše filosofickou disciplínou, zabývající se úvahami o vývoji trestního práva v budoucnosti.

Trestní právo velmi úzce souvisí s dalšími právními obory, zejména s právem ústavním, které je jeho základem. Ústavní právo mimo jiné upravuje základní práva a svobody občanů, z čehož vyplývají pro trestní právo některé výše uvedené zásady. Úzce souvisí s mezinárodním právem, zejména pak s mezinárodním právem trestním, jež je součástí mezinárodního práva veřejného[16]. Součástí právního řádu jsou dnes i některé mezinárodní smlouvy[17], k jejichž dodržování se Česká republika zavázala. Pokud zákon stanoví něco jiného než mezinárodní smlouva, použije se ustanovení mezinárodní smlouvy[18].

Trestním právem jsou chráněny i oblasti, které mají svoji úpravu ve správním právu a v posledních letech se slibně rozvíjí i správní právo trestní. Je pak úlohou zákonodárců, aby zvážili, které činy ztratily svoji nebezpečnost pro společnost a bylo by vhodné je přesunout do správního práva trestního a naopak, které přestupky prohlásit za trestné činy. Z hlediska trestně právního postihu je důležité občanské právo nebo právo, které obsahují instituty, jež je nutno sekundárně chránit trestním právem. Rovněž postupy upravující občansko právní řízení obsahují řadu případů, které je nutno chránit trestním zákonem, např. křivou výpověď svědka nebo nepravdivý znalecký posudek.

Mezi související obory trestního práva patří především kriminalistika, která jako samostatný vědní obor se zabývá zkoumáním a objasňováním zákonitostí vzniku, vyhledávání, zajišťování a využívání zachytitelných stop trestného činu a jejich využitím jako důkazů v soudním řízení. Součástí oboru je vypracovávání metod a postupů, stanovování prostředků a ope-

[14] U práva lze vysledovat hierarchii, kde trestní sankce je na posledním místě. Tato hierarchie má na nejnižším stupínku morální odsouzení a následují zvyšující se váhy trestů – disciplinární potrestání, občanskoprávní sankce, správní odpovědnost a teprve nakonec trestní odpovědnost.

[15] Okolnosti činu se nesmí přičítat dvakrát.

[16] Tato oblast práva se rozvinula zejména po druhé světové válce, zejména s procesy, které po válce následovaly, např. vojenský tribunál v Norimberku.

[17] Je to přechod o dualistické koncepce práva ke koncepci monistické.

[18] Mezinárodní smlouva má tedy aplikační přednost. V právnických kruzích však panuje spor týkající mezinárodní smlouvy o lidských právech a základních svobodách, neboť vzdor textu čl. 112 Ústavy ČR, je Ústavní soud ČR považuje za součást ústavního pořádku, který je hierarchicky nadřazen „obyčejným" zákonům.

rací pro úspěšné odhalování, vyšetřování a předcházení trestné činnosti. Spolu s dalšími znaleckými disciplínami je převážně součástí úkolů trestního řízení.

Kriminalistika čerpá zejména z kriminologie, vědy o zločinnosti, jejich pachatelích a obětech [K02]. Nelze opomenout ani další související obory, viktimologii – vědy o obětech trestných činů a penologii – vědy zabývající se problematikou trestů z hlediska jejich účinku a způsobu výkonu. S ohledem na technologické trestné činy můžeme náš výčet ukončit i vědou zabývající se projevy kybernality, tedy zkoumáním a objasňováním mechanizmů technologických trestných činů páchaných v kyberprostoru.

5.1.3 Výklad trestních zákonů

Výklad trestních zákonů a jejich praktická aplikace je mnohdy předmětem právnických sporů. Účelem výkladu je zjistit skutečný smysl zákona, a tak každý právník může hledat skutečný smysl skrz zájem svého klienta. Nicméně tak jednoduché to není a právní nauka rozlišuje několik druhů výkladu trestních zákonů:

- ✓ Podle toho kdo výklad provádí:
  - ✓ Výklad autentický, který je prováděn orgánem, jenž zákon vydal nebo je k výkladu zákona výslovně zmocněn.
  - ✓ Výklad legální není v České republice podáván a spočívá ve výkladu zákona orgánem k tomu zmocněným.
  - ✓ Výklad soudní,v České republice nejběžnější, je výklad podávaný orgány činnými v trestním řízení v praxi. Výklad zákona podaný soudem vyšší úrovně je pro soud nižší úrovně závazný jenom v jednotlivé věci[19].
  - ✓ Výklad vědecký nebo teoretický, který je obsažen v odborných monografiích a podle autority zpracovatele může ovlivňovat praxi i vést ke zdokonalování právních norem.
- ✓ Podle metody a prostředků výkladu:
  - ✓ Výklad gramatický nebo též filologický, kterým se vymezuje smysl zákona na základě sémantiky a syntaxe běžného vyjadřování.
  - ✓ Výklad systematický, tedy výklad zákonů z hlediska celého právního řádu.
  - ✓ Výklad logický, který je mnohdy jako metoda odmítán neboť se považuje za nutný požadavek každé metody výkladu.
- ✓ Podle poměru výkladu k doslovnému znění zákona:
  - ✓ Výklad doslovný.
  - ✓ Výklad restriktivní neboli zužující, který je z hlediska trestního zákona poněkud problematický[20].
  - ✓ Výklad extenzívní, který se musí na rozdíl od analogie (viz dále) pohybovat přesně v rámci normy. V našem právním řádu je používán velmi zřídka.

[19] Judikatura vydávaná Nejvyšším soudem ve Sbírce rozhodnutí a stanovisek není pro soudy nižších instancí nebo jiné orgány činné v trestním řízení právně závazná. Je však významná z hlediska sjednocování práce těchto orgánů.

[20] Při limitním pojetí takového výkladu trestního zákona by např. vznikala každému občanu povinnost oznámit trestný čin (viz § 168 trestního zákona) na základě toho, že se o něm dověděl z denního tisku.

Z uvedených metod výkladu je pro praxi nejdůležitější výklad logický, který se promítá do všech výkladů zákona. Pro činy v kyberprostoru bude důležitá analogie, resp. její přípustnost v mezích stanovených trestním zákonem.

Logický výklad staví na přesně definovaných postupech při interpretaci a argumentace je někdy velmi blízká analytickému myšlení informatiků. Základní postupy při interpretaci zákona jsou:

- ✓ **Argumentum a simili**, neboli výklad normy podle podobného ustanovení, jehož se trestní zákon sám mnohdy dovolává. Např. při zjišťování skutkové podstaty činu bude třeba jednotlivé znaky vykládat podle jejich povahy a typických účinků, jenž mohu být uvedeny v jiném ustanovení apod.
- ✓ **Argumentum a maiori ad minus** (výklad zákona od většího k menšímu); v literatuře [N11] je uveden příklad spočívající v možnosti zániku trestnosti účastenství (§ 10 TZ) při uplatnění argumentu a maiori ad minus. Podle této úvahy je dobrovolné upuštění od pokusu trestného činu snazší (tedy „od menšího", snazšího) než zamezení další činnosti osoby, kterou pachatel k tomuto trestnému činu navedl nebo jí pomáhal (tedy „k většímu"). Pokud pachatel takové osobě zabrání čin dokonat, nebude trestný pro některou z forem účastenství podle § 10 TZ. Jestliže se však jeho úsilí nezdaří, nebo jeho krok ke zmaření předmětného trestního činu bude spočívat pouze v oznámení státnímu zástupci nebo policejnímu orgánu v době, kdy již není možno dokonání činu zabránit, bude se jednat jenom o polehčující okolnost.
- ✓ **Argumentum a minori ad maius** (od menšího k většímu); podobně jako v předchozím se v literatuře [N11] uvádí příklad, založený na úvaze, že není-li příčetný ten, kdo pro duševní poruchu nemůže rozpoznat nebezpečnost činu pro společnost nebo ovládnout své jednání („od menšího"), je nepříčetný spíše ten, komu schází obě tyto schopnosti („k větším").
- ✓ **Argumentum a contrario** (výklad z opaku, sporem), kdy negací tvrzení dojdeme k jeho praktickému uplatnění v konkrétním případě, např. je-li v zákoně vymezeno ohrožení lidí jako „nebezpečí smrti nebo těžké újmy na zdraví[21]", pak uvedeným logickým výkladem dojdeme k závěru, že nebezpečí pouhého ublížení na zdraví by z hlediska požadovaného následku k trestnosti nestačilo [N05].

Velmi důležitým pojmem z oblasti trestního práva je analogie, neboli obdoba. Analogií rozumí trestní zákon tzv. subsumpci[22] případu v trestním zákoně výslovně neuvedeného pod podobný, jenž je v zákoně uveden. Pojem analogie a zejména omezení analogie v trestním právu má dlouhou historii a jeho první kořeny jsou spatřovány již v Magna Charta Libertatum[23] a francouzském Prohlášení lidských a občanských práv.

Zákaz analogie v neprospěch obviněného platí snad ve všech trestních řádech na světě, a to ve dvou směrech:

- ✓ analogií nelze rozšiřovat podmínky trestnosti, tedy aplikace zásady „nullum crimen sine lege",
- ✓ tresty a ochranná opatření lze ukládat jenom na základě zákona, tedy opět aplikace zásady trestního práva „nulla poena sine lege".

[21] Viz § 179 odst. 1 trestního zákona.

[22] Subsumpcí (podřazením) se v právu nazývá postup, při němž se skutkové podstatě přiřazuje ta právní norma, jejíž hypothesa je jí naplněna.

[23] Magna charta libertatum neboli Velká listina práv a svobod byla vydána 15. června 1215 v Anglii anglickým králem Janem Bezzemkem. Tento dokument, omezující pravomoc panovníka ve prospěch šlechty a měšťanstva a garantující nezávislost církve na králi, se stal základem anglického a amerického práva.

Analogie ve prospěch pachatele trestného činu je přípustná, pokud jde o důvody omezující trestnost. Lze rozeznat dva základní druhy analogie – „analogie legis" neboli použití nejbližší právní normy podle zákona a „analogie iuris", která spočívá v použití nejbližší právní normy podle práva.

Analogii je nutno odlišit od extensivního výkladu zákona, který se uskutečňuje v souladu s účelem trestního zákona a jen v jeho mezích, kdežto analogie tyto meze překračuje. Stejně tak je nutno odlišit analogii od logické argumentace podle podobnosti (viz „argumentum a simili"), které se mnohdy dovolává sám zákon[24].

5.1.4 Působnost trestních zákonů

Pod pojmem působnosti trestních zákonů se rozumí okruh společenských vztahů, v nichž se zákon uplatňuje. Od působnosti je třeba odlišovat platnost a účinnost trestního zákona. Platný je ten zákon, který byl navržen, projednán, schválen a vyhlášen podle ústavních předpisů a stal se tak součástí právního řádu. Účinný je zákon, podle kterého má být v daném případě jednáno; účinnost zákona může být zrušena nebo změněna vydáním nového zákona nebo jeho novelizací a je v zákoně vždy výslovně uvedena nebo není uvedena vůbec[25].

V právní nauce se rozlišují tři základní typy působnosti zákona

- ✓ **Působnost časová**, která říká, že trestný čin se posuzuje podle zákona účinného v době spáchání trestného činu.
- ✓ **Působnost místní** se vztahuje, jak již název říká, k posuzování trestných činů spáchaných na území České republiky bez ohledu na to jaké je občanství pachatele trestného činu. Platí zásada teritoriality vycházející ze suverenity každého státu, podle niž se v podstatě stíhají všechny činy spáchané na příslušném státním území. Místní působnost je založena na čtyřech principech:
  - ✓ **teritoriality** (§ 17 TZ), kde rozhodujícím je místo spáchání činu, za něž se považuje místo, kde došlo k jednání nebo k následku trestného činu nebo kde k následku mělo dojít[26];
  - ✓ **personality** (§ 18 TZ), kde rozhodující je občanství nebo u osob bez státní příslušnosti místo jejich trvalého pobytu;
  - ✓ **ochrany** (částečně v § 19 TZ), kdy stát si chrání své vlastní nejdůležitější zájmy, ať už byl čin spáchán kdekoli a kýmkoli;
  - ✓ **univerzality** (§ 20 a částečně § 19 TZ), kdy stát v zájmu mezinárodní spolupráce rozšiřuje aplikaci trestního zákona i na činy spáchané mimo území státu cizím státním příslušníkem, ačkoliv nesměřují proti zájmu státu[27].
- ✓ **Působnost osobní** nebo též věcná se vztahuje na všechny pachatele trestných činů a na všechny trestné činy v oblasti trestního práva. Nevztahuje se tedy na přestupky a správní delikty. Některé osoby jsou však zčásti vyňaty z působnosti trestního zákona; jedná se o tzv. exempce, které se odůvodňují jejich osobním postavením.

Nejzávažnějším bodem působnosti trestních zákonů pro oblast kybernetických trestných činů je působnost místní. Jak je uvedeno výše, místem spáchání trestného činu se rozumí místo, kde došlo k jednání majícímu znaky trestného činu nebo místo následku trestného činu či místo, kde k následku trestného činu mělo dojít[28]. Tedy místem trestného činu je ve tomto smyslu rovněž místo, kde nastal nebo měl nastat účinek. I když trestní zákon řeší např. trestnost činu spáchaného na palubě lodi nebo letadla registrovaného v České republice, na případy páchání trestných činů v globálním kyberprostoru lze vztáhnout pouze princip tzv. distančních deliktů uvedených v § 17 odst. 2 trestního zákona. Ten se však zabývá pouze případem, kdy se pachatel dopustí na území republiky jednání, které vede k porušení nebo ohrožení zájmu chráněného zákonem, i když účinek nastal nebo měl nastat zcela nebo zčásti v cizině[29].

Je tedy problematické stíhání pachatele, který útokem na výpočetní systém umístěný v České republice způsobí značnou škodu, avšak sám se bude nacházet v jurisdikci, kde jednání, jenž vedlo ke způsobení škody, není trestné. Chování pachatelů v kyberprostoru, který sám jurisdikcí není, je proto mnohdy obtížné postihnout bez účinných mezinárodních dohod a spolupráce.

5.1.5 Trestný čin

Trestný čin je pro společnost nebezpečný čin, jehož znaky jsou uvedeny v trestním zákoně[30]. Mezi znaky trestného činu se řadí:

- ✓ **Znak materiální**, tj. nebezpečnost činu pro společnost, který souvisí s mírou ohrožení chráněných zájmů.
- ✓ **Znaky formální**, uvedené v trestním zákoně, které zahrnují:
  - ✓ Znaky obecné, tj. znaky, které jsou společné všem trestným činům. Sem patří zejména vlastnosti pachatele trestného činu např. jeho věk a příčetnost.
  - ✓ Znaky typové, které popisují jednotlivé typy trestných činů a souhrn těchto znaků právní nauka označuje jako skutkovou podstatu trestného činu.

Znaky trestného činu jsou uvedeny nejen v dispozici, ale mohou být uvedeny i v jiných zákonech a jsou obligatorní[31]. To znamená, že chybí-li některý ze znaků nebo je zastoupen v menší míře, než vyžaduje skutková podstata, pak se nejedná o trestný čin[32].

Nauka o trestním právu velmi podrobně rozebírá typové znaky trestných činů a za tím účelem je třídí do čtyř skupin:

- ✓ Znaky charakterizující objekt trestného činu, kde objektem trestného činu jsou všechny společenské vztahy, zájmy a hodnoty, které jsou chráněny trestním právem[33].

---

24 Příklad lze najít přímo v textu trestního zákona, kde se používají formulace např. „jiných podobně nebezpečných látek" nebo „jiného podobného nebezpečného jednání" (§ 95 nebo § 179).

25 Obvykle se platnost zákona uvádí v jeho posledním odstavci. Pokud není platnost uvedena vůbec, stává se zákon účinným patnáctým dnem od jeho vyhlášení ve Sbírce zákonů.

26 Místo činu je trestním zákonem rozšířeno i mimo území České republiky, a to na Antarktidu a podle tzv. „principu vlajky".

27 Všechna uvedená ustanovení o místní působnosti se uplatňují subsidiárně, t.j. jenom tehdy, pokud mezinárodní smlouva nebo zákon nestanoví něco jiného.

28 Podmínka „jednání" nebo „následku" může být splněna i jenom částečně.

29 Vedle „distančních deliktů" se ještě rozlišují tzv. „tranzitní delikty", např. zásilka drog putujících přes několik států. Právní teorie se kloní k názoru, že místem činu jsou všechna místa, kde se rozvíjela příčinná souvislost mezi jednáním a následkem, tedy v předcházejícím příkladě všechna místa, přes která byla předmětná zásilka dopravována.

30 Citace ustanovení § 3 odst. 1 trestního zákona.

31 Trestní právo rozlišuje dispozice popisné, které popisují znaky trestného činu a mají být přesné a konkrétní, dispozice blanketní, jenž předpokládají bližší úpravu v více právních normách a dispozice odkazovací, které ukazují na jinou, ale jenom jednu, konkrétní právní normu.

32 To ale neznamená, že konkrétní čin nemůže být posuzován jako přestupek nebo jiný správní delikt.

- ✓ Znaky charakterizující objektivní stránku trestného činu, která někdy bývá označována jako vnější stránka trestného činu a dělí znaky na obligatorní, kam patří jednání, následek a příčinný vztah a fakultativní, zahrnující dobu a místo spáchání trestného činu, formu jednání a způsob provedení, hmotný předmět útoku a účinek. Hmotným předmětem útoku přitom chápeme osoby a věci, na které pachatel útočí[34] a účinkem změna nebo nebezpečí změny na hmotném předmětu útoku[35].
- ✓ Znaky charakterizující subjekt trestného činu, jak bývá v nauce trestního práva označován pachatel.
- ✓ Znaky charakterizující subjektivní stránku trestného činu, kam patří zejména zavinění, které je obligatorním znakem subjektivní stránky skutkové podstaty trestného činu. Rozeznáváme:
  - ✓ Zavinění úmyslné (dolózní), které zahrnuje úmysl přímý (dolus directus), kdy pachatel chtěl porušit nebo ohrozit chráněný zájem, a úmysl eventuální (dolus eventualis), kdy pachateli věděl, že svým jednáním může porušit nebo ohrozit chráněný zájem a byl s tím srozuměn.
  - ✓ Zavinění z nedbalosti (kulpózní), které rozlišuje nedbalost vědomou, kdy pachatel věděl, že může porušit nebo ohrozit chráněný zájem, ale bez přiměřených důvodů spoléhal, že k takovému stavu nedojde, a nedbalost nevědomou, kdy pachatel nevěděl, že svým jednáním může porušit nebo ohrozit chráněný zájem, ač o tom vzhledem k okolnostem a svým osobním poměrům vědět měl nebo mohl[36].

Fakultativní znaky charakterizující subjektivní stránku trestného činu zahrnují:

- ✓ Motiv (pohnutku) trestného činu, čímž chápeme vnitřní podnět, který vyvolal rozhodnutí pachatele spáchat trestný čin. Pohnutka může být okolností jak přitěžující tak i polehčující.
- ✓ Účel (cíl) trestného činu, který je výjimečně obligatorním znakem trestného činu a obvykle slouží k jemnějšímu rozlišení skutkových podstat[37].

Popis znaků skutkové podstaty trestného činu tvoří převážnou část trestního zákona a jsou uvedeny nejen v části zvláštní, kde jsou rozděleny trestné činy podle objektu, ale i v části obecné. Znaky trestného činu jsou odrazem skutečnosti a přesná, jednoznačná formulace těchto znaků přispívá k dodržování zásad trestního práva.

5.1.6 Pachatel

Pachatel je subjektem trestného činu a označuje se jím ten, kdo naplnil svým jednáním všechny znaky trestného činu. Za pachatele trestného činu je však považován též spolupachatel, návodce, organizátor aj. Trestní zákon považuje za pachatele i toho, kdo se dopustí přípravy trestného činu (viz §7 trestního zákona) nebo pokusu trestného činu (viz § 8 trestního zákona)[38].

Pachatelem může být pouze osoba fyzická, nikoli právnická[39], musí dovršit určitý věk a musí být příčetná. Pachatel může ke spáchání některých trestných činů, mimo vysloveně „vlastnoručních činů", použít jiné osoby, tzv. „živého nástroje". V takovém případě se označuje jako nepřímý pachatel a v praxi se může jednat o případy zneužití osoby nepříčetné nebo dítěte popř. použití osoby jednající ve skutkovém omylu[40]. Pokud je trestný čin spáchán více osobami, hovoříme o spolupachatelství a každá osoba je trestně odpovědná tak, jako by trestný čin spáchala sama. Spolupachatelství je prakticky možné jenom u úmyslného trestného činu, u nedbalostních trestných činů se vyskytuje zřídka. Významnými znaky spolupachatelství je společné jednání směřující k následku (účinku) trestného činu a úmysl tento čin spáchat právě společným jednáním.

Jiným pojmem v této oblasti je účastenství, čímž je chápána úmyslná účast více osob na trestném činu, která je namířena proti témuž chráněnému zájmu a směřuje k témuž účinku. Trestní zákon rozeznává tři formy účastenství[41]:

- ✓ Organizátorství trestného činu (§ 10, odst. 1, písm. a) trestního zákona), což je zákonem považováno za nejzávažnější formu účastenství a organizátorem se rozumí osoba, která trestný čin zosnovala nebo řídila.
- ✓ Návod k trestnému činu (§ 10, odst. 1, písm. b) trestního zákona) směřuje k tomu, aby se jiná osoba rozhodla spáchat sama úmyslný trestný čin[42]. Pokud však naváděná osoba byla již rozhodnuta spáchat trestný čin k němuž je naváděna, půjde o tzv. psychickou pomoc.
- ✓ Pomoc k trestnému činu (§ 10, odst. 1, písm. c) trestního zákona) je nutno odlišit od návodu k trestnému činu. Pomocníkem je ten, kdo jinému poskytne nebo opatří prostředky, popř. odstraní překážky, a tak mu umožní spáchat trestný čin (tzv. pomoc fyzická). Pokud pomocník utvrzuje pachatele v předsevzetí spáchat trestný čin, poskytuje mu radu apod. jedná se tzv. pomoc psychickou. Pomoc ke spáchání trestného činu je vždy jednání úmyslné a od spolupachatelství se odlišuje tím, že pomocník nenaplňuje znak jednání charakterizující hlavní trestný čin.

Určení osoby pachatele není v oblasti kybernetických trestných činů jednoduchou úlohou. Největším problémem je ztotožnění fyzické osoby pachatele s nástrojem trestného činu – počítačem, IP adresou apod. Pokud se jedná o útok proti obsahu např. diskové jednotky, pak fenomén nepopiratelnosti provedení trestného činu konkrétní osobou je významným krokem v důkazním řízení před trestním soudem.

---

33 Trestní právo nechrání všechny zájmy, ale jen ty, kterým společnost přikládá zvláštní význam.

34 Nelze zaměňovat s objektem trestného činu, nebo s prostředky použitými ke spáchání trestného činu (např. zbraň).

35 Často se v laickém pojetí zaměňuje účinek s následkem. Např. účinkem trestného činu vraždy je smrt člověka, ale následkem se rozumí porušení zájmu na ochraně života člověka.

36 Mezi okolnosti patří mimo jiné i odborná erudice pachatele, což je důležité zejména při posuzování kybernetických trestných činů.

37 Cíl činu je např. obligatorním znakem subjektivní stránky trestného činu teroru podle § 93 TZ, kde cílem je vynutit si splnění nějakých podmínek.

38 Srovn. též §89 odst. 1 TZ.

39 Připravovaná novela trestního zákona počítá se zavedením trestní odpovědnosti i právnických osob. Podle současného znění trestního zákona je u právnických možno trestně obvinit osoby, které jejím jménem v konkrétní případě jednají.

40 Např. nepřímý pachatel označí taxikářovi cizí kufr za svůj a ten ho naloží a odveze. Taxikář byl v tomto případě živým nástrojem nepřímého pachatele a „živé nástroje" zpravidla nejsou trestně odpovědné za svůj čin. Pokud však k takovému jednání dojde z nedbalosti, nelze trestní odpovědnost jednoznačně vyloučit.

41 Účastenství je trestné jen ve spojení s pokusem trestného činu nebo s dokonaným úmyslným trestným činem.

42 V této souvislosti je zejména zajímavá úloha tzv. „agenta provokatéra", jehož činnost by byla podle současného znění trestního zákona pravděpodobně trestná.

5.1.7 Trestní právo procesní

Trestní právo procesní (formální) upravuje postupy při trestního řízení, zejména procedurální postup trestních orgánů v trestních věcech. Trestním řízením rozumíme zákonem upravený postup orgánů v činných v trestním řízení, jejichž úkolem je zjistit zda byl spáchán trestný čin, určit jeho pachatele, uložit pachateli trest nebo ochranné opatření podle zákona a rozhodnutí vykonat. Zároveň má trestní řízení působit k upevňování zákonnosti, předcházení a preventivnímu zamezení trestné činnosti a k výchově občanů. Trestní právo procesní a trestní právo hmotné popsané v předchozích kapitolách spolu úzce souvisí – trestní právo hmotné se realizuje způsobem, který je stanoven v trestním právu procesním.

Trestní proces se výrazně odlišuje od procesu civilního. Zatímco civilní proces je zpravidla sporem dvou soukromých osob, v trestním řízení před soudem stojí proti sobě vždy veřejný žalobce zastupující stát (státní zástupce) a obžalovaný z trestného činu. Princip rovnosti se v trestním procesu realizuje jinak než v civilním a požaduje jisté vyvážení ve prospěch obžalovaného, který je tváří v tvář státním orgánům silně znevýhodněn.

Podobně jako trestní právo hmotné má i trestní právo procesní několik zásad, ze kterých vychází. Mezi základní zásady patří:

- ✓ Zásada **presumpce neviny**, kdy se na osobu proti níž se vede trestním řízení hledí jako na osobu nevinnou, dokud vina není vyslovena pravomocným rozsudkem soudu. Obviněný má právo, aby s ním bylo jednáno bez předsudku viny, což se projevuje i v dokazování - vinu neprokazuje obviněný, ale orgán činný v trestním řízení. Během řízení se zjišťuje skutkový stav, o němž nejsou důvodné pochybnosti v rozsahu nezbytném pro rozhodnutí[43].
- ✓ Zásada **přiměřenosti**, která každému orgánu veřejné moci ukládá, aby přijal jen tak účinné opatření, jehož je v konkrétní situaci nezbytně třeba k dosažení zamýšleného účelu, tedy např. v případě odsouzení musí být uložená sankce úměrná společenské nebezpečnosti trestného činu, okolnostem, za nichž byl trestný čin spáchán apod.
- ✓ Zásada **vyhledávací** kladoucí důraz na stejně pečlivé objasňování okolností směřujících ve prospěch obviněného jako v jeho neprospěch, tedy orgán činný v trestním řízení musí zjistit skutkovou podstatu úplně a podle pravdy.

Další principy zahrnují zásadu práva na obhajobu, zásadu práva na odepření výpovědi, zásadu stíhání jen ze zákonných důvodů, zásadu legality nebo princip „ne bis in idem" neboli nemožnost odsouzení dvakrát za tutéž věc[44] atd.

Trestní právo procesní rozeznává subjekty, tedy orgány a osoby, které mají z hlediska svých pravomocí vliv na průběh trestního řízení a jimž trestní řád dává k vykonávání vlivu určitá procesní práva nebo určité procesní povinnosti. Sem patří např. soud, státní zastupitelství nebo orgány policie. Naproti tomu osoba proti které se trestní řízení vede, její obhájce a další zúčastněné osoby mají v trestním řízení přesně stanovená práva. Významnou roli hrají osoby se samostatnými právy – svědek, znalec a tlumočník. Zejména úloha znalce je v procesech zabývajících se kybernetickými trestnými činy velmi významná, protože soud nebo soudce nemůže nikdy být specialistou pro danou oblast a spoléhá tedy na výpovědi expertů, které z hlediska práva a okolností trestného činu hodnotí.

[43] V případě pochybností následuje rozsudek o zproštění viny, neboť platí zásada vyplývající z presumpce neviny, že nedokázaná vina dokazuje nevinu.

[44] Zásada „ne bis in idem" brání nejen opakovanému odsouzení, ale též opětovnému trestnímu stíhání téže osoby v téže věci, jestliže existuje pravomocné rozhodnutí tvořící překážku „res iudicata" (viz § 11 odst. 1 písm. f) – h), odst. 4, § 11a Trestního řádu).

Součástí trestního řízení je dokazování, jehož úkolem je zjistit zda došlo ke spáchání trestného činu a určit pachatele tohoto trestného činu. Za tím účelem se provádí dokazování, tedy zjišťování skutkového stavu, o němž nebudou pochybnosti. Každá strana má právo navrhovat důkazy a tvrzení a vyjadřovat se k důkazům a tvrzením. Důkazy mohou být přímé např. výslech osoby obviněného, svědka, znalce či obsah předložených listin, zpráv zachycených na médiích apod. nebo nepřímé, např. sociálně psychologický profil pachatele. Přímé důkazy dokazují přímo zjišťovanou skutečnost, např. svědek viděl trestný čin. Nepřímé důkazy dokazují skutečnost jinou, ale takovou, z níž lze učinit logický úsudek ve vztahu k dokazované skutečnosti[45]. Průběh a způsob dokazování je v trestním právu procesním přesně stanoven a úzkostlivě dodržován. Trestní řád přitom stanoví, jakým způsobem, v jakém rozsahu a za jakých podmínek mohou státní orgány zasahovat do občanských práv při vyhledávání důkazů.

Pro důležitost osoby znalce se ještě zastavme u jeho úlohy v trestním řízení. Znalec zpracovává pro soud odborné vyjádření, jenž má obvykle písemnou podobu, a které může mít buď formu odborného stanoviska nebo znaleckého posudku[46]. Odborné stanovisko může zpracovat i jiná osoba, kterou uzná soud ke zpracování odborného stanoviska za způsobilou, a nemusí se nutně jednat o znalce. Znalecký posudek obvykle nastupuje, až když pro složitost posuzované otázky nepostačuje odborné stanovisko.

Znalcem je osoba jmenovaná příslušným soudem a uvedená v seznamu znalců[47]. Úlohu, práva a povinnosti znalce určuje trestní řád [Z03] a další právní předpisy, např. [Z04]. Znalec může být trestán za nepravdivý znalecký posudek podle § 175 trestního zákona. Je orgánem činným v trestním řízení přizván v případě, že k objasnění skutečnosti důležité pro trestní řízení je nutno mít odborné znalosti. Orgán činný v trestním řízení je oprávněn přibrat jednoho nebo více znalců a znalec je oprávněn přibrat jednoho nebo více konzultantů, nicméně za zpracovaný posudek odpovídá soudem jmenovaný znalec[48].

Znalcem může být v konkrétním případě soudem ustanovena i osoba, fyzická nebo právnická, která není zapsána do seznamu znalců, ale která má podle názoru soudu potřebné odborné znalosti pro zpracování odborného vyjádření. V těchto případech jsou většinou vyzývány katedry vysokých škol nebo ústavy akademie věd. Zúčastněné strany mají právo navrhovat znalce nebo namítat k osobě znalce nebo jeho odbornosti. Mohou samy předložit znalecký posudek zpracovaný znalcem z jejich popudu nebo mohou soudu předložit návrh na výslech znalce v hlavním líčení. Znalec může odepřít posudek za stejných podmínek jako svědek nebo specificky podle § 11 zákona č. 36/1967 Sb. v poslední platné úpravě [Z04], a to v případě, že pro jeho poměr k věci, k orgánům provádějícím řízení, k účastníkům nebo k jejich zástupcům je pochybnost o jeho nepodjatosti.

Znalecký posudek má obligatorně stanoveny tři části – **nález**, tedy popis toho co znalec zjistil, **posudek**, shrnující úsudek znalce učiněný na podkladě odborných znalostí o skutečnostech, k jejichž objasnění byl povolán, a **znaleckou doložku** identifikující znalce, obory pro které byl jmenován a prohlášení o tom, že znalec si je vědom následků vědomě

[45] Častý omyl detektivních filmů – tím, že je při domovní prohlídce nalezena vražedná zbraň s otisky osoby, proti níž je vedeno trestní řízení, je důkaz nepřímý. Dokazuje pouze to, že tato osoba držela vražednou zbraň, ale nikoliv, že zabíjela.

[46] Případy, kdy se znalec vyjadřuje do protokolu k položené otázce ad hoc, jsou zřídkavé. Většinou je vyzván ke zpracování posudku a k soudnímu řízení je obvykle pozván pro vyjasnění některých jeho pasáží.

[47] Zvláštní postavení mají znalci jmenovaní ministrem spravedlnosti a tzv. znalecké ústavy, což jsou právnické osoby pověřené ministrem spravedlnosti k výkonu znalecké činnosti v daném oboru.

[48] Znalec může být přizván v kterémkoli stadiu trestního řízení, tedy např. i policií vyhledávající důkazy trestného činu. Časté jsou v oblasti kybernetické trestné činnosti tzv. forenzní analýzy počítačů zabavených při domovních prohlídkách.

nepravdivého znaleckého posudku. Ve znaleckém posudku musí znalec vysvětlit, se kterými skutečnostmi se seznámil a jak dospěl ke skutečnostem v závěru. Závěry znaleckého posudku by měly být ověřitelné, případné důkazní experimenty by měly být kdykoliv proveditelné znovu. Z tohoto důvodu je nutno, zejména při forenzních analýzách zachytit prvotní stav zkoumaného stroje na nepřepisovatelné médium a zajistit aby tento stav mohl být kdykoliv obnoven[49].

konecma

Znalec není oprávněn hodnotit důkazy vzhledem k ostatním skutečnostem řízení ani řešit právní otázky (§ 107 odst.1 TŘ). Jeho povinností je vysvětlit souvislost zajištěných důkazů s předmětným trestným činem a vyjádřit ke všem alternativám. Nezáleží na tom, zda znalec zajistil důkazy při výkonu své funkce, zpracování znaleckého posudku, nebo zda mu byly předloženy orgány činnými v trestním řízení. Znalecký posudek jako důkaz hodnotí soud, resp. orgány činné v trestním řízení, a to včetně případných námitek dotčených stran. Avšak v případě, kdy se orgán činný v trestním řízení odchýlí od posudku, je povinen toto odůvodnit.

Poslední součástí trestního práva procesního je ochrana před následky nesprávného rozhodnutí. Opravných prostředků je celá řada počínaje stížností, odvoláním, odporem proti trestnímu příkazu, dovoláním, stížností pro porušení zákona a v poslední řadě je obnova řízení. Ke všem opravným prostředkům však musí vést nesouhlas s konkrétními vadami procesu, nepodstatné vady nemohou být důvodem ke zrušení nebo změně rozhodnutí. Opravné prostředky se dělí na řádné, kam patří např. odvolání a mimořádné, např. stížnost pro porušení zákona.

V rámci procesního práva je nutno při řešení kybernetických trestných činů využívat mezinárodní spolupráce. I pro tuto oblast upravuje trestní právo procesní postupy mezinárodní justiční spolupráce v trestním řízení. Tyto postupy vymezují materiální podmínky právní pomoci, obsah institutů spolupráce států a řeší otázky pravomoci a příslušnosti. V případě, že pro příslušný případ neexistuje mezinárodní smlouva, nebo daná otázka není v příslušné smlouvě řešena, použijí se subsidiárně ustanovení trestního řádu. Mezinárodní smlouvy obvykle řeší např. případy převzetí cizího trestního řízení, převzetí a výkon cizího rozsudku nebo tzv. extradiční řízení, které spočívá ve vydání občana České republiky do České republiky k trestnímu stíhání nebo k výkonu trestu[50].

5.2 Legislativní zázemí postihu kybernetické kriminality

Než se blíže seznámíme se stavem současné české legislativy, je nutno konstatovat, že na současný stav v oblasti informačních a komunikačních technologií není důkladně připravena žádná evropská legislativa. Jednotlivé trhliny jsou „záplatovány" případ od případu a celkové koncepční pojetí této oblasti se teprve rodí. Lépe na tom není ani legislativa zámořská, která však díky své odlišné právní metodice, spočívající na právních precedentech a dodatcích ústavy, má pro jednotlivé incidenty již své vzory.

[49] To je důležité zejména pro zpracování tzv. revizních posudků (přezkumů), tedy případů, kdy znalecký posudek je některou stranou tak vážně napaden, že soud uloží zpracování nového znaleckého posudku nebo posouzení předloženého posudku jiným znalcem.

[50] Extradiční řízení se týká nejenom vydání osoby z cizího státu do České republiky, ale též z České republiky do cizího státu. Vydání občana České republiky do cizího státu nepřípustné, nicméně nově je upraveno předání do nebo z členského státu Evropské unie, kdy k trestnímu stíhání je možné předat českého občana do členského státu EU.

5.2.1 Česká legislativa

Základní zákony, které jsou v oblasti informatiky a telekomunikací nejčastěji uplatňovány jsou:

- ✓ Občanský zákoník, neboli zákon č. 40/1964 Sb. ve znění pozdějších úprav a jeho prováděcí předpis, kterým je nařízení vlády č. 258/1985 Sb. Tento základní předpis je důležitý zejména proto, že jednoznačně definuje jednak vlastnické právo a jednak entity, proti kterým je kriminální činnost namířena – právnické a fyzické osoby. Někdy je třeba chápat ustanovení tohoto zákona poněkud šířeji, protože dikce „předmět svého vlastnictví" může zavádět k fyzickému pojetí „předmětu vlastnictví". To v mnoha případech není v případě informačních technologií pravdivé.
- ✓ Obchodní zákoník, pod číslem 513/1991 Sb. v podobě začleňující poslední novely upravuje postavení podnikatelů, obchodní závazkové vztahy, jakož i některé jiné vztahy, které s podnikáním souvisejí. Jeho uplatnění bude zejména v případech, kdy nelegální aktivity budou souviset se smluvním nebo podobným vztahem, upraveným v tomto zákoně.
- ✓ Zákon o elektronických komunikacích č. 127/2005 Sb., který nahradil původní telekomunikační zákon č. 151/2000 Sb. pokrývá širokou škálu působení telekomunikačních a podobných společností na trhu, přičemž z našeho hlediska upravuje některé důležité aktivity související s případným nezákonným chováním subjektu v prostředí počítačové sítě. Součástí tohoto zákona je nejenom podmínka dodržování telekomunikačního tajemství, ale i např. ustanovení zakazující používat automatických systémů volání bez lidské účasti pro účely přímého marketingu bez předchozího souhlasu dotčeného účastníka (§ 85 odst. 1, písm. g).
- ✓ Autorský zákon v posledním znění podle zákona č. 121/2000 Sb. vyprovokoval řadu soudních procesů, kde se žalující strany domáhaly práva autorství k programům nebo podobným produktům. I když tato oblast je mimo problematiku, kterou se hodláme zabývat, je natolik živá, že následující kapitolu věnujeme popisu základních aspektů pohledu na tyto případy.
- ✓ Zákony související s ochranou průmyslového vlastnictví, jako např. zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví, zákon č. 137/1995 Sb., o ochranných známkách nebo zákon č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích.
- ✓ Zákon o ochraně osobních údajů souvisí velmi úzce s ochranou telekomunikačního tajemství, ale má i jistou působnost v oblasti databází obsahujících takové údaje, které by mohly vést k jednoznačné identifikaci osoby. Tento zákon označovaný jako č. 101/2000 Sb. navazuje na směrnici 95/46/EC Evropského parlamentu a Rady z 24. října 1995, o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů [E15]. Ta zase vychází z úmluvy č. 108, o ochraně osob se zřetelem na automatizované zpracování osobních dat, kterou Česká republika podepsala dne 8. září 2000 [E16].
- ✓ Trestní zákon č. 140/1961 Sb. ve své poslední úpravě a s ním související předpisy by měly sloužit jako represivní nástroj v okamžiku prokázaného porušení některého zákonného předpisu, které spadá do sféry trestní odpovědnosti. Bohužel, v těchto případech je mnohdy výklad zákona takový, že některé typické kriminální delikty v počítačovém prostředí se jenom velmi obtížně začleňují do stávající osnovy zákona. Rovněž dokazovací procedura je v těchto případech většinou složitá, neboť procesní dokazování je stavěno na klasických důkazních metodách.

konecma

- ✓ Zákon o některých službách informační společnosti vedený jako zákon č. 480/2004 Sb., který upravuje zejména odpovědnosti poskytovatelů služeb a šíření obchodních sdělení. Očekávalo se od něj, že bude vhodným nástrojem boje proti spamu, avšak jeho dopad je téměř nulový.
- ✓ Zákon o regulaci reklamy č. 40/1995 Sb. reguluje ve své poslední úpravě i některé elektronické nešvary, jako je „spam".

Mezi další zákony české legislativy související s touto problematikou patří zákon o elektronickém podpisu č. 227/2000 Sb. s prováděcím předpisem č. 304/2001 Sb., zákon o svobodném přístupu k informacím č. 106/1999 Sb. a zákon o informačních systémech veřejné správy č. 365/2000 Sb. Na tyto předpisy navazuje standardizační činnost bývalého Úřadu pro veřejné informační systémy, jehož úkoly byly převzaty ministerstvem informatiky.

5.2.2 Mezinárodní legislativní aktivity

Předpisy a směrnice evropské unie, které bezprostředně souvisí s informatikou a telekomunikacemi jsou spíše předmětem jednoúčelových doporučení nebo naopak koncepčních materiálů velmi širokého záběru. Pro oblast informatiky je to základní dokument eEurope+ [E05], připravený za spolupráce členských i kandidátských zemí, který se však soustřeďuje spíše na směry rozvoje informatiky v členských zemích než na problematiku bezpečnosti. Rámcový dokument Evropské unie, který je zdrojovým textem pro úpravy telekomunikačního zákona ve všech členských zemích, jenž se skrývá pod označením 2002/21/EC [E06] postihuje ve svých některých ustanoveních i problematiku telekomunikačního tajemství. Odvozené dokumenty [E07], [E08] a [E09] pak upřesňují některá ustanovení tohoto dokumentu. Většina těchto dokumentů je i součástí zákona o elektronických komunikacích.

Podstatným přínosem Evropské unie, který zasahuje oblast bezpečnosti a kriminality na internetu je [E10] postihující bezpečnostní problematiku v oblasti propojených počítačových sítí v celé šíři. Zabývá se jak bezpečností informačních infrastruktur tak i odpovídajícími právními procedurami a opatřeními jak na legislativní úrovni, tak i mimo ni. Tento materiál vznikl jako výsledek práce speciální komise, která plnila deset bodů akčního plánu dohodnutého na schůzce G8 v listopadu 1997 [E11].

Aktivity mezinárodních organizací se s ohledem na stoupající povědomí o zneužívání informačních systémů při organizované nelegální činnosti dostávají do popředí dění. Evropská komise založila společnou pracovní skupinu složenou z odborníků Evropské unie a Spojených států zaměřenou na metodiku ochrany kritické komunikační infrastruktury, Organizace spojených národů připravila již v roce 1986 stručný „Manual on the prevention and control of computer related crime", který byl v roce 2001 upraven s ohledem na současný vývoj. Země OECD iniciovaly již v roce 1986 studii „Computer-Related Crime: Analysis of Legal Policy", která se stala základem pro doporučení pro návrh bezpečných informačních systémů pro členské státy OECD.

Po teroristickém útoku na Spojené státy 11. září 2001 aktivity v oblasti detekce nelegálních aktivit v datových sítích a jejich postihu dále posílily. Zelenou dostaly již delší dobu nepříliš veřejně propagované myšleny legálního monitorování aktivit podezřelých subjektů na datových sítích, které jsou prováděny oprávněnými orgány státu. Zvýšil se tlak na legislativu a rozšiřování právního vědomí v oblasti „digitálního práva", objevila se řada dříve přehlížených možností a manažeři spolu se správci sítí si uvědomili, jak důležitá je bezpečnostní politika uplatňovaná v jejich systému.

5.3 Jak definovat kybernetickou kriminalitu

Kybernetická kriminalita, označovaná v anglické literatuře mnohdy jako „IT crime" nebo „cybercrime" může velmi zjednodušeně řečeno, znamenat jakýkoliv čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených. Oficiálních definicí počítačové kriminality existuje celá řada, avšak většina z nich vychází z podstaty uvedené výše. Podle materiálu OSN, který se zabývá počítačovou kriminalitou jsou jejím obsahem *„Tradiční zločinné aktivity jako krádež, podvod nebo padělání, tedy činy trestné ve většině zemí na světě. Počítač rovněž tvoří prostředí pro nové činy spočívající ve zneužití počítačů, které jsou nebo by měly být ve své podstatě trestné."* [U01]. Ve stejném materiálu se UN snaží odlišit dva základní případy – náhodné a neúmyslné použití počítače, které vede ke vzniku škody, a úmyslné použití počítače jako nástroje nebo předmětu kriminálního deliktu.

Jeden z nejvyšších evropských orgánů, Rada Evropy, začala projevovat zájem o řešení problematiku počítačové kriminality již koncem osmdesátých let. Na základě studie vypracované v roce 1989 byla publikována doporučení pro úpravy a vytváření nových zákonů, které by měly kriminalizovat činy, spáchané prostřednictvím počítačových sítí v doporučení RE č. 9 z roku 1989 [E12] nebo informačními technologiemi v doporučení RE č. 13 z roku 1995[E13]. V roce 1997 byla ustavena Komise expertů na zločin v kyberprostoru (Committee of Experts on Crime in Cyber-Space), která pracovala na návrhu mezinárodní dohody, usnadňující mezinárodní spolupráci při odhalování počítačových zločinů [E14].

5.3.1 Klasifikace podle mezinárodní dohody o kyberzločinu

Dohoda je určena pro řešení problémů spojených s mezinárodním charakterem počítačového zločinu a požaduje, aby signatářské země kriminalizovaly určitá jednání, které je možné zařadit do oblasti počítačového zločinu včetně přijetí norem, které umožní tuto trestnou činnost postihovat. Text dohody dělí jednotlivé skutkové podstaty podle jejich obsahu takto:

- ✓ Zločiny proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů, jež se dále dělí na:
  - ✓ nezákonný přístup,
  - ✓ nezákonné odposlouchávání,
  - ✓ narušování dat,
  - ✓ narušování systémů,
  - ✓ zneužití prostředků.
- ✓ Zločiny se vztahem k počítači, které jsou děleny na:
  - ✓ počítačové padělání,
  - ✓ počítačový podvod.
- ✓ Zločiny se vztahem k obsahu počítače, což je především dětská pornografie.
- ✓ Zločiny se vztahem k autorským nebo obdobným právům.

Návod a pomoc k výše uvedeným typům činů může být řešen také v rámci trestní odpovědnosti právnických osob. Doufejme, že obecné procesní normy uvedené v tomto dokumentu, zvláště pak opatření pro vyhledávání a zajišťování dat, uložených v počítačích nebo přijímaných v reálném čase usnadní dokazování a zpracování důkazů v rámci této trestné činnosti.

5.3.2 Klasifikace podle eEurope+

Rovněž akční plán eEurope+ zdůrazňuje velkou důležitost bezpečnosti počítačových struktur a boje proti kybernetickému zločinu a klade si za cíl zvýšit bezpečnost informačních infrastruktur a zajistit, aby orgány činné v trestním řízení měly veškeré přiměřené prostředky k činnosti. Podobně jako chystaná dohoda, tak i akční plán kategorizuje jednotlivé počítačové zločiny na:

- ✓ zločiny porušující soukromí (ilegální sbírání, uchovávání, modifikace, zveřejňování a šíření osobních dat),
- ✓ zločiny se vztahem k obsahu počítače (pornografie, zvláště dětská, rasismus, vyzývání k násilí apod.),
- ✓ ekonomické (neautorizovaný přístup a sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody apod.),
- ✓ zločiny se vztahem k duševnímu vlastnictví (autorské právo apod.).

I zde jsou uvažovány procesní prostředky, včetně monitorování komunikace, zajištění dopravovaných dat, anonymního přístupu a užití zdrojů, jurisdikce a hodnoty počítačových dat v důkazním řízení.

Ani české orgány nezahálely a Ministerstvo vnitra zpracovalo vlastní koncepci boje proti trestné činnosti v oblasti informačních technologií, kterou doplnilo rozsáhlou analýzou. Je pravdou, že tato analýza se soustřeďuje daleko více na snadno uchopitelnou oblast porušování autorských práv, nelegální kopírování a softwarové pirátství, ale jsou v ní i některé odstavce, pojednávající o pronikání prostřednictvím telekomunikačních technologií. V následujících kapitolách se seznámíme s technologickým pohledem na některé kritické body určování povahy deliktu.

5.3.3 Klasifikace podle dopadu konkrétního skutku

Jednou z dalších možností klasifikace je systém, strukturovaný podle zamýšleného účinku, respektive podle napadeného chráněného zájmu. Můžeme pak rozeznat:

- ✓ Trestný čin proti osobě, kam patří útok proti pověsti, pomluva, vydírání, obtěžování, krádež identity (vydávání se za někoho s cílem ho v první řadě znectít, poškodit ho v rodinném nebo společenském životě), nenáležité nakládání s osobními údaji, atd. Příkladem může být situace, kdy je digitální prostředek využit pro úpravu audiovizuálních projevů. Výsledek může být situace, kdy je projev řečníka upraven tak, že zvuk i obraz plně korespondují, i když se původní projev nesl ve zcela jiném duchu. V tomto konkrétním případě se ve vojenské terminologii jedná o důležitým prostředek psychologického útoku, podkopávající důvěru v konkrétního mluvčího.
- ✓ Trestný čin proti vlastnictví, kde můžeme dále rozeznat případy:
  - ✓ Kdy je přímým dopadem činu další obohacení se na úkor poškozeného (odčerpávání majetku z účtu nebo využívání služby na účet poškozeného[51]. Škoda může být i značně vysoká, pokud je platba vázána na objem dat nebo čas.
  - ✓ Kdy je následkem činu „úspora" nákladů útočníka, jenž by jinak byly ziskem postiženého (investice do koupě software, audiovizuálních nahrávek, atd.); sem patří případy porušení autorských práv, defraudace dat, atd.
  - ✓ Kdy zisk útočníka a ztráta poškozeného spočívá v dalším nezákonném šíření neoprávněně získaných dat: software, audiovizuálních nahrávek, atd., ať již za úplatu nebo bez ní; do této oblasti spadá i průmyslová špionáž uskutečněná prostřednictvím informatických prostředků (krádež výsledků výzkumu, patentů, marketingových strategií apod.).
  - ✓ Kdy je škoda napadeného subjektu odvozena od vratného či nevratného zničení, poškození či pozměnění jeho dat (sabotáž, vandalismus – viz např. „defacement"); informace tak nemůže být spolehlivě použita pro účel, ke kterému je určena; často jsou přitom změněna pouze některá data a to v obtížně rozlišitelných detailech, útok se tedy projeví až s určitým zpožděním.
  - ✓ Kdy je škoda napadeného subjektu založena na tom, že jeho služba není dostupná (Denial of Service resp. Denial od Access). Útok zabrání autorizovanému přístupu ke zdrojům, nebo způsobí zpoždění časově kritických operací. Tento typ útoku je používán např. pro potlačení konkurenčních serverů a provedení vyžaduje široce koordinovanou akci většího počtu počítačů.
  - ✓ Kdy je škoda založena na zneužití informace, která byla neoprávněně získána z informačních a komunikačních sítí v reálném světě (např. informace o trase přepravy velkých finančních prostředků).

Další možnosti, kterými je např. klamavá reklama, nebo naopak, šíření nepravdivých informací poškozujících protivníka mohou využít jak veřejně přístupné mediálními prostředky, tak i přímo protivníkův informačním systému, který byl jinými prostředky předem kompromitován:

- ✓ Trestný čin proti veřejnému zájmu, veřejnému pořádku nebo mravnosti, kam můžeme zahrnout pobuřování, šíření poplašné zprávy, kybernetický terorismus, politicky motivovaná špionáž, šíření nelegální pornografie, šíření nenávisti, schvalování zločinu a nabádání k němu nebo propagaci toxikomanie, atd.

Je zřejmé, že jednotlivé skupiny uvedené klasifikace se v detailech navzájem prolínají, avšak je to jedna z možných klasifikací, která není sama o sobě vyčerpávající.

5.3.4 Klasifikace kybernality z hlediska skutkových podstat

Základním ustanovením platného trestního zákona, které se týká kybernality, je § 257 a „Poškození a zneužití záznamu na nosiči informací". Jeho znění popisuje, i když jen ve vztahu k informacím, co není dovoleno s daty dělat. Paragraf je jediným ustanovením, které je určeno pro informační technologie jako takové a postihuje vysoce kvalifikovanou trestnou činnost. Zákon se zaměřuje na tři formy činnosti, kterými jsou:

- ✓ Neoprávněné užití informací; často je rovněž uváděno do souvislosti s § 105 „Vyzvědačství", § 106 „Ohrožení utajované informace", § 107, který postihuje vyzrazení utajované informace z nedbalosti, § 128 „Zneužívání informací v obchodním styku" nebo § 239 či § 240, které postihují porušování tajemství dopravovaných zpráv. Vlastní podstatou incidentu je prozrazení resp. jakákoli forma zneužití získaných informací, nacházející se na nosiči informací, např. zkopírování seznamu zákazníků a jeho předání konkurenci.
- ✓ Zničení, poškození nebo učinění informací neupotřebitelnými; často rovněž jako „Poškozování cizí věci" podle § 257.
- ✓ Zásah do technického nebo programového vybavení počítače; často rovněž ve spojitosti s § 257 „Poškozování cizí věci".

[51] Tzv. „theft of service".

rok	zjištěno	objasněno	tj. objasněno %
1993	12	4	33,3
1994	4	0	0,0
1995	10	6	60,0
1996	14	7	50,0
1997	9	8	88,9
1998	76	74	97,4
1999	60	56	93,3
2000	21	15	71,4
2001	24	20	83,3
2002	27	8	29,6
2003	33	5	15,2
2004	35	16	45,7
2005	37	18	48,6

Tab. 5.1: *Vývoj trestného činu dle § 257a „Poškození a zneužití záznamu na nosiči informací" [B17]*

Řadu dalších jednání lze postihnout samostatně, případě v rámci jednočinného souběhu s trestným činem podle § 257a. V trestním zákoníku lze nalézt následující případy v členění podle dotčených paragrafů.

- ✓ § 178 „Neoprávněné nakládání s osobními údaji" – podstatou činu může být prozrazení osobních údajů jiné osobě nebo umožnění jiným osobám, aby se s nimi seznámily, např. situace, kdy zdravotnický personál poskytl z počítače seznam pacientů s konkrétní diagnózou distributorovi léčiv.
- ✓ § 124c postihující použití nepravdivého nebo neúplného údaje pro vydání dokladu potřebného pro orgány kontrolující zboží a technologie podle zvláštních předpisů, § 125 „Zkreslování údajů o stavu hospodaření a jmění" a § 148 „Zkrácení daně, poplatku a podobné povinné platby". Podstatou uvedených činů jsou různé varianty zásahů do technického nebo programového vybavení počítače, resp. úprava účetních záznamů v informačním systému podnikatele, např. s cílem zatajení příjmů a tím snížení daňové povinnosti.
- ✓ § 150 „Porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu", § 151 „Porušování průmyslových práv" a § 152 „Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi". Podstatou těchto činů jsou různé formy porušování autorských práv kopírováním cizích autorských děl (distribuce programů, kopírování stránek, umísťování cizích autorských děl na vlastní stránky a na servery), neoprávněné užívání počítačového programu, což lze chápat jako užívání autorského díla bez souhlasu autora (počítačové pirátství).
- ✓ § 247 „Krádež", § 248 „Zpronevěra" a § 249 „Neoprávněné užívání cizí věci". Jedná se zejména o případy, kdy pachatel pomocí počítače převede finanční prostředky z účtu jednoho vlastníka na svůj vlastní účet nebo na účet jiného subjektu. Takový převod prostředků může být proveden jak úmyslně tak i z nedbalosti. .... Může být i § 250 (srov. § 89, odst. 18).
- ✓ § 250 „Podvod" a § 250c „Provozování nepoctivých her a sázek". Záměrem pachatele je uvedení někoho v omyl, což umožní jeho vlastní obohacení, a to nikoliv pouze informacemi, ale přímo materiálně, např. podvodné transakce s podvodným zbožím, penězi či falešnými identifikacemi při nákupu a prodeji. Sem patří i páchání podvodů spočívajících v zadávání nepravdivých čísel nebo čísel cizích platebních karet při nákupu v internetovém obchodě, internetová „letadla" či jiné internetové pyramidové hry, jejichž podstatou je přerozdělování finančních prostředků vložených hráči do hry zejména ve prospěch pořadatele. Zvláštností dokazování v tomto případě je, že účastníkům není zaručena objektivnost hry, v čemž spočívá podvodné jednání ze strany organizátorů hry.
- ✓ § 93 „Teror", § 95 „Teroristický útok, § 96 „Záškodnictví", § 97 „Sabotáž", trestné činy obecného ohrožení shrnuté v hlavě čtvrté TZ pod § 179, § 180 a zejména pro oblast útoků na telekomunikační zařízení § 182 „Poškozování a ohrožování provozu obecně prospěšného zařízení z nedbalosti". Jedná se o případy, při nichž jsou prostřednictvím nelegálních operací v rámci informačních a komunikačních technologií ohroženy životy a zdraví lidí, dopravní systémy, letecký provoz, nemocnice apod. Nezáleží na tom, zda je či není v takových situacích deklarována politická motivace útoku, resp. zda se jedná o úmyslnou aktivitu, nebo nedbalost.
- ✓ § 176 „Padělání a pozměňování veřejné listiny", § 209 „Poškozování cizích práv" a § 249b „Neoprávněné držení platební karty". Pozměňování počítačových nebo jiných dokumentů je prováděno prostřednictvím úpravy dokladů, ze kterých jsou zaváděna data do počítače, úpravou dat uložených v počítači, úpravou dat v průběhu počítačové operace nebo úpravou dat na výstupní počítačové sestavě. Tyto skutky mohou často být spáchány v jednočinném souběhu s jinými hospodářskými trestnými činy.
- ✓ § 164 „Podněcování", § 165 „Schvalování trestného činu", § 198 a § 198a „Hanobení národa, etnické skupiny, rasy a přesvědčení", § 199 „Šíření poplašné zprávy", § 202 „Výtržnictví", § 205 „Ohrožování mravnosti" a § 260 „Podpora a propagace hnutí směřujících k potlačení práv a svobod člověka". V uvedeném kontextu lze využít např. znění zákona 46/2000 (Tiskový zákon), spolu s ustanovením § 89 odst. 4 Trestního zákona, kde se uvádí, že trestný čin je spáchán veřejně, jestliže je spáchán obsahem tiskoviny nebo rozšiřovaného spisu, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem. Internet je v tomto případě chápán jako „jiný obdobně účinný způsob".

5.4 Vztahy autorské a vlastnické v kybernetické oblasti

Základem každého protiprávního jednání v oblasti počítačové kriminality je technologické zázemí, které je svou povahou poměrně vzdálené běžné trestné činnosti i zaběhlým mechanismům práce orgánů činných v trestním řízení. Proto dokazování a klasifikace počítačového deliktu je většinou velmi obtížné. Přitom přesné definice, které jsou v informatice zcela běžné, přeloženy do právnického jazyka, by byly velmi vhodným nástrojem v této oblasti. Pozice experta, soudního znalce či jiného odborníka, který má v právním prostředí objasnit a prokázat povahu trestného činu je tedy velmi svízelná.

Při klasifikaci deliktu jde většinou o typické činy krádeže např. datových souborů s různým obsahem, které mohou být i dále rozšířeny o činy související s ochranou osobních údajů (§ 178 TZ), ohrožení utajované informace (§ 106 TZ) apod., porušení autorského práva

(§ 152 TZ), porušení průmyslových práv (§ 151 TZ), šíření obsahu snižujícího lidskou důstojnost (např. pornografie podle § 205 TZ), extremismu, nebo i o trestný čin pomluvy (§ 206 TZ). Specifickými činy jsou případy, kdy dochází k mechanickému nebo elektronickému znehodnocení informace např. podle § 257a TZ. Velmi ožehavým tématem je přitom povaha dotčené informace, kdy odlišným výkladem může dojít k jiné klasifikaci podle autorského zákona a jiné v případě, kdy se bude jednat o majetkové právo.

konecna

5.4.1 Autorské právo a programová díla

Autorské právo[52] je součástí práv plynoucích z „duševního vlastnictví" a jedná se o specializované odvětví práva, zabývajícím se nároky tvůrců autorských děl[53] při využívání jejich tvorby. Prostřednictvím institutu porušování autorského práva v § 152 Trestního zákona poskytuje stát autorům chráněných děl ochranu a Autorský zákon jim dává výlučné možnosti rozhodovat o některých aspektech využívání jejich děl[54].

Obecně je rozšířen mylný názor spočívající v představě ochrany nápadu, myšlenky či ideje. Avšak, autorské právo chrání pouze konkrétní díla, konkrétní vyjádření takových myšlenek nebo idejí, a to díla v konkrétní objektivně vnímatelné podobě. Současně autorské dílo musí být pouze jedinečným výsledkem tvůrčí činnosti autora, fyzické osoby, a za dílo nelze považovat zejména námět díla sám o sobě, denní zprávu nebo jiný údaj sám o sobě, myšlenku, postup, princip, metodu, objev, vědeckou teorii, matematický a obdobný vzorec, statistický graf a podobné předměty samy o sobě (§ 2 odst. 6 AZ).

Autorské právo je v České republice ošetřeno autorským zákonem č. 121/2000 Sb., který vychází z několika mezinárodních úmluv, zejména tzv. Bernské úmluvy z roku 1886 a Všeobecné úmluvy o autorském právu uzavřené v Ženevě v roce 1952[55]. Zákon 121/2000 Sb. přesně specifikuje předmět autorského díla v § 2, kde v odstavci 1 je uvedeno: „Předmětem práva autorského je dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam." Zároveň podle odstavce 2 téhož paragrafu se za autorské „dílo považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Za dílo souborné se považuje databáze, která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem".

5.4.1.1 Obsah autorského práva

Autorská práva, která vznikají okamžikem, kdy je dílo vyjádřeno ve smyslu autorského zákona, lze rozdělit do dvou základních skupin – výlučná **práva osobnostní** a výlučná **právo majetková**. Mezi práva osobnostní patří zejména právo autora rozhodnout o zveřejnění díla a právo osobovat si autorství[56]. Jinými osobnostními právy jsou práva na nedotknutelnost díla a udělení souhlasu k jakékoli změně nebo jinému zásahu do díla[57]. Základním znakem osobnostních práv je, že autor se jich nemůže vzdát, jsou nepřevoditelná a smrtí autora zanikají (§ 11 odst. 4 AZ)

Majetková práva poskytují autorovi výlučné právo na rozhodování o užívání jeho díla a zároveň mu umožňují udělit jiné osobě, ať už právnické nebo fyzické, oprávnění k výkonu tohoto práva. Poskytnutím oprávnění k užití díla majetková práva autorovi nezanikají, vzniká mu pouze povinnost strpět zásah do práva dílo užít jinou osobou v rozsahu vyplývajícím ze smlouvy. Smlouvou s autorem získává nabyvatel pouze oprávnění k výkonu majetkového práva.

Avšak, na rozdíl od práv osobnostních, jsou majetková autorská práva předmětem dědictví a získají je dědici po autorově smrti v běžném dědickém řízení[58]. Majetková autorská práva trvají, podle současného znění zákona, po dobu autorova života a 70 let po jeho smrti. U děl spoluautorů se počítá doba trvání ochrany od smrti posledního spoluautora. Dílo, u kterého uplynula doba ochrany majetkových práv, se nazývá volné dílo a každý ho může volně užít.

Podstatným institutem v oblasti autorského zákona je „právo dílo užít", k čemuž dochází v případě, kdy autor k takovému užití svolil. Do rozsahu tohoto práva na užití díla patří:

- ✓ právo na rozmnožování díla,
- ✓ právo na rozšiřování díla či jeho rozmnoženiny,
- ✓ právo na pronájem díla či jeho rozmnoženiny,
- ✓ právo na půjčování díla či jeho rozmnoženiny,
- ✓ právo na vystavování díla či jeho rozmnoženiny,
- ✓ právo na sdělování díla veřejnosti (provozování živě či ze záznamu, přenos provozování díla, vysílání rozhlasem či televizí apod.).

Kromě těchto práv do majetkových autorských práv patří také právo na odměnu, a to jak při prodeji nebo opětném prodeji díla, tak právo na odměnu v souvislosti s rozmnožováním díla.

Autor se může svých práv domáhat občanskoprávní žalobou, která může směřovat k určení svého autorství, zákazu ohrožení svých práv[59], odstranění následků zásahu do práva včetně poskytnutí přiměřeného zadostiučinění omluvou či finančním odškodněním. Autor také může vyžadovat náhradu škody a vydání bezdůvodného obohacení. Nicméně při porušení autorského práva dochází rovněž k trestného činu podle § 152 trestního zákona, který může být v trestněprávním řízení potrestán peněžitým trestem, propadnutím věci, ale také odnětím svobody až na dvě léta[60].

5.4.1.2 Specifická ustanovení o počítačových programech

Vzhledem k výjimečnosti postavení počítačových programů jako specifického díla věnuje autorský zákon pozornost programům v několika zvláštních paragrafech. Nejprve je definována ochrana počítačového programu v § 65 odst. 1: „Počítačový program, bez ohledu

52 Často bývá zaměňováno za tzv. „copyright", což je obdoba autorské ochrany v angloamerickém právním řádu. Není však s pojetím autorského práva kontinentálního zcela totožná.

53 Původně je jednalo pouze o umělecká díla, tedy autorský zákon chránil zejména spisovatele, hudebníky nebo filmaře. Později byl rozšířen na všechny produkty dušení autorské činnosti a v současné podobě chrání i programátory.

54 Podobnou ochranu poskytuje Trestní zákon v § 151 i duševnímu vlastnictví v oblasti průmyslové, avšak ta je chráněna jinými právními mechanismy podrobně specifikovanými v oblasti práva průmyslového.

55 V roce 1967 vznikla Světová organizace duševního vlastnictví – „World Intellectual Property Organization (WIPO)", která se zbývá podporou trendů směřujících k ochraně duševního vlastnictví.

56 Osobování autorství zahrnuje i právo rozhodnout, zda a jakým způsobem má být autorství uvedeno při zveřejnění díla.

57 Toto právo je zejména důležité v oblasti počítačových programů, kde by každý, kdo chce upravit cizí autorské dílo, měl nutně získat autorův souhlas. Nicméně právě v této oblasti je celá řada výjimek – viz dále.

58 Tato majetková práva musí být v dědickém řízení ohodnocena a dědici z nich musí zaplatit daň.

59 Sem patří např. požadavek na zákaz neoprávněné výroby, obchodování, dovozu či vývozu, sdělování veřejnosti apod.

60 Nebo až na pět let, pokud pachatel získal značný prospěch či dopustil-li se činu ve značném rozsahu.

na formu jeho vyjádření, včetně přípravných koncepčních materiálů, je chráněn jako dílo literární." Zároveň však v následujícím odstavci potvrzuje obecnou zásadu autorského práva, když uvádí: „Myšlenky a principy, na nichž je založen jakýkoli prvek počítačového programu, včetně těch, které jsou podkladem jeho propojení s jiným programem, nejsou podle tohoto zákona chráněny".

konec strany

Z těchto ustanovení lze dovodit hned několik závěrů, které jsou často ve svatém nadšení pro ochranu autorství přehlíženy. Autorský zákon nechrání myšlenku, na níž je program založen, stejně jako metodu, teorii nebo vzorec. Je tedy zřejmé, že pokud budou existovat dva programy, jejichž činnost bude založena na stejném výpočetním principu, např. algoritmu, pak každé autorské zpracování tohoto principu bude jedinečným autorským dílem podle zákona. Podobně je tomu i z druhé strany, kdy bude stejný výstup z počítačového programu, např. webová stránka. Pokud tento výstup je produkován různými programy, jedná se o různá autorská díla ve smyslu zákona[61].

V následujících paragrafech však autorský zákon omezuje ochranu programů konstatováním, že do práva autorského nezasahuje oprávněný uživatel rozmnoženiny počítačového programu pokud:

- ✓ Rozmnožuje, překládá, zpracovává, upravuje či jinak mění počítačový program, je-li to potřebné k užití počítačového programu v souladu s jeho určením, včetně opravování chyb programu (§ 66, odst. 1, písm. a).
- ✓ Zhotoví si záložní rozmnoženinu počítačového programu, je-li to potřebné pro jeho užívání (§ 66, odst. 1, písm. b).
- ✓ Zkoumá, studuje nebo zkouší sám nebo jím pověřená osoba fungování počítačového programu za účelem zjištění myšlenek a principů, na nichž je založen kterýkoli prvek počítačového programu, činí-li tak při zavedení, uložení počítačového programu do paměti počítače nebo při jeho zobrazení, provozu či přenosu, (§ 66, odst. 1, písm. c).
- ✓ Rozmnožuje kód nebo překládá jeho formu při rozmnožování počítačového programu nebo při jeho překladu či jiném zpracování, úpravě či jiné změně, jsou-li takové rozmnožování nebo překlad nezbytné k získání informací potřebných k dosažení vzájemného funkčního propojení nezávisle vytvořeného počítačového programu s jinými počítačovými programy, jestliže informace potřebné k dosažení vzájemného funkčního propojení nejsou jinak snadno dostupné a tato činnost se omezuje na ty části počítačového programu, které jsou potřebné k dosažení vzájemného funkčního propojení (§ 66, odst. 1, písm. d).

Uvedená omezení navíc pro činnosti uvedené v odstavci 1 písm. d) ukládají zákaz poskytnutí informací o výsledcích takové činnosti jiným osobám ani nesmí být využity k jiným účelům než k dosažení vzájemného funkčního propojení nezávisle vytvořeného počítačového programu. Dále nesmí být informace být využity ani k vývoji, zhotovení nebo k obchodnímu využití počítačového programu v podstatě podobného v jeho vyjádření nebo k jinému jednání ohrožujícímu nebo porušujícímu právo autorské[62].

[61] Něco jiného je grafický vzhled stránky, který může být chráněn jako jiné umělecké dílo. Nicméně v tomto případě není právní praxe zcela zajedno, zda na takovou stránku je nutno nahlížet jako na autorské dílo ve smyslu autorského zákona, nebo jako na průmyslový vzor, tedy institut spadající do oblasti průmyslových práv. Průmyslovým vzorem se většinou rozumí „vzhled výrobku, spočívající zejména ve znacích linií, obrysů, barev, tvaru, struktury nebo materiálu výrobku samotného, nebo jeho zdobení". Jde tedy o vizuálně vnímatelnou vlastnost výrobku, kterým je v daném případě webová stránka.

[62] Zde zákonodárce poněkud zamlžil podstatu autorského díla, když použil velmi neurčité označení „programu v podstatě podobného". Bude potom na soudu, aby určoval míru podobnosti, což může být činnost velmi obtížná a zatížená významnou subjektivní chybou.

5.5 Program, data a databáze

Častým případem, který řeší soudy, bývá porušování autorského zákona, speciálně pak ustanovení týkajících se autorského práva k programu. Přitom základní otázka, zda vůbec předmět sporu spadá do působnosti autorského zákona, zůstává neřešena. Tedy to podstatné, co musí nejdříve vzít soud v úvahu, je odpověď na otázku zda charakter trestného činu vůbec splňuje podmínky, které jsou při stanovení skutkové podstaty rozhodující. Odpověď na tuto otázku je podstatná pro klasifikaci a správné začlenění trestného činu podle znaků skutkové podstaty.

Zejména složité je vyhodnocení v případě, kdy podstata předmětu trestného činu je nehmotná a vysvětlení rozdílu spočívá na správném výkladu definic, jejichž charakter leží mimo právní oblast. Tak je tomu právě u trestných činů souvisejících s porušením autorského práva, kam spadá rozhodnutí podle § 152 TZ. Ne vždy se totiž jedná o program, jenž je chráněn autorským zákonem a je možno bezpečně najít všechny znaky skutkové podstaty uvedeného trestného činu. Z toho důvodu se definicí tohoto rozdílu zabývali právní autority téměř ve všech zemích světa. Poměrně jasný závěr byl učiněn pro evropské země ve směrnici Evropské unie 91/250.

5.5.1 Definice programu

Řada sporů spadajících do působnosti autorského zákona vyvolala legislativní iniciativu směřující k definici programu jako autorského díla. V prvé řadě je to ustanovení autorského zákona, které říká, že autorské dílo musí být jedinečným výsledkem tvůrčí činnosti autora a vyjádřeno v jakékoli objektivně vnímatelné podobě (§ 2 odst. 1 AZ), kde autorem se rozumí fyzická osoba, která dílo vytvořila. Současně je možno akceptovat stanovisko evropské komise, vyjádřené ve směrnici č. 91/250 [E02], jež sama nedefinuje podstatu programu, ale odvolává se na stanovisko skupiny expertů uvedené v [C05]. Podle tohoto stanoviska počítačový program je „vyjádření množiny instrukcí v jakékoli formě, jazyku, záznamu nebo kódu, které je určeno k tomu, aby podle něj počítač vykonával danou úlohu". Tato definice není zcela vyčerpávající, ale uvědomíme-li si, že instrukce je „jediný způsob jak lze změnit vnitřní stav stroje" [J02], pak je celkem snadné odlišit počítačový program v jakékoliv formě od dat[63].

Velmi často dochází k nepřesnosti při výkladu tohoto pojmu, kdy za počítačový program jsou vydávány i znakové řetězce generované jiným programem, např. příkazy pro tiskárnu v jazyce HPGL. To je v rozporu s požadavkem autorského zákona, který vyžaduje aby se jednalo o dílo fyzické osoby. Programem v tomto případě je pouze množina instrukcí[64], která vykonala úlohu tisku. Znakové řetězce generované touto množinou instrukcí jsou pak daty, určenými pro zpracování jinému počítači – v tomto případě řídícímu procesoru tiskárny.

[63] Na tomto místě by bylo vhodné se ještě zmínit o studijním materiálu Evropské unie, který se zabývá patentovatelností návrhů implementovaných pomocí počítače [E04].

[64] Nezáleží na tom, že tato množina instrukcí srozumitelně zapsaná v programovacím jazyku byla přeložena autorem do podoby srozumitelné pro počítač – strojového kódu. I tento překlad je produktem autora, který překladač používá jako nástroj ke zhotovení konečné podoby díla.

konecma

Podobně jako v předchozím případě je možno posuzovat znakové sady (fonty) určené pro generování znaků na tiskárně nebo obrazovce. Tam je situace o to složitější, že znak sám, nebo znaková sada by na první pohled mohla být posuzována jako autorské dílo (obdobně jako např. umělecká grafika). Jedná se však o průmyslový vzor, který je chráněn ve smyslu zákona 207/2000 Sb. o ochraně průmyslových vzorů, kam patří každý grafický symbol a typografický znak[65]. Z hlediska autorského práva je znak datovou jednotkou určenou pro zpracování programem (např. v tiskárně). Nezáleží na tom, v jaké formě byla tato data k dalšímu zpracování předána.

5.5.2 Data a databáze

Dalším specifickým případem jsou databáze. Základním dokumentem pro orientaci může být směrnice Evropské komise č. 96/9/EC z 11. března 1996 [E03], která se zabývá právní ochranou databází. V českém autorském právu je situace poněkud zatemněná, neboť jednoznačně nerozlišuje mezi strukturou databáze, která je zřejmě dílem autorským, a jejím obsahem, na který je nutno nahlížet jako na vlastnictví sui generis. Pro tyto dvě entity je právní režim velmi odlišný a může dojít ke zmýlení [B13]. Ostatně česká interpretace uvedené směrnice si nezadá s originálem, jehož znění bylo často kritizováno a docházelo i ke zcela nečekaným odezvám na předmětný dokument. Klasickým případem je spor Britského dostihového výboru se sázkovou kanceláří William Hill Organization Ltd., v němž se jednalo o využití veřejně přístupné databáze k řízení sázek [U02].

Z hlediska autorského práva je databáze definována jako „soubor nezávislých děl, údajů nebo jiných prvků systematicky nebo metodicky uspořádaných a individuálně přístupných elektronickými nebo jinými prostředky bez ohledu na jejich formu vyjádření". K databázi autorský zákon zřídil naprosto nové právo – právo pořizovatele databáze. Toto právo pořizovatele je chápáno právě jako právo vlastnické a vztahuje se k obsahu databáze, tak jak bylo uvedeno výše. Stanovisko OSA k tomuto zvláštnímu právnímu institutu je poněkud složitější a v konkrétním případě bude záležet na individuálním pohledu příslušného soudu, jak bude konečný verdikt vypadat [H04].

5.5.3 Porušování autorských práva k programu

Otázku postihů za porušení autorského zákona řeší § 152 trestního zákona o porušování autorského práva, práv souvisejících s právem autorským a práv k databázi následovně: „Kdo neoprávněně zasáhne do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci."

Trestné činy proti duševnímu vlastnictví se velmi rozšířily zejména s rozmachem internetu. Mezi faktory, které k tomu přispěly můžeme zařadit:

- ✓ Dostupnost nelegálních kopií autorských děl, kdy kopie díla může být pořízena během několika minut a s poměrně nízkými náklady.

[65] Musí se jednat o symbol nebo typografický znak průmyslově používaný. Např. písmové sady, které jsou určeny pro tisk knih, jsou zařazeny podle tzv. Lokarnského třídění do třídy 18-03. Třída 18 přitom zahrnuje tiskařské stroje a tedy poplatky za průmyslová práva platí výrobce stroje, který příslušnou znakovou sadu dodal, nikoliv tiskárna. Obdobně je možno usuzovat i na znakové sady používané v počítačích.

- ✓ Specifika autorských práv spočívající v jejich nehmotné podstatě. Pohled na autorská práva a duševní vlastnictví vyžaduje jiné chápání veřejností, než je běžné pro většinu ostatních trestných činů.[66]
- ✓ Vysoká cena softwarového vybavení, vycházející z faktu, že ceny software se výrazněji ve světě neliší, a tak vzniká mnohdy nepoměr mezi cenami software a kupní silou obyvatel.

Mezi nejčastější činnosti, kdy je porušován autorský zákon, patří kopírování díla. Zdánlivě, vzhledem k nehmotné podstatě duševního vlastnictví, nevzniká žádná přímá škoda, protože vlastník neutrpí žádnou újmu, jeho dílo není nijak poškozeno. Nicméně z hlediska autorského zákona je i kopírování díla jednak samo o sobě jeho užití a jednak obvykle vede k dalšímu neoprávněnému užívání díla.Velmi specifické pro prostředí internetu a výpočetní techniky je vznik kopií děl při běžném provozu a často bez vědomí uživatele. Kdykoliv například prohlížíme fotografie na internetu, vytváří se zároveň kopie díla. Na tuto skutečnost myslel zákonodárce v § 37 autorského zákona kde uvádí, že do práva autorského nezasahuje ten, kdo zhotoví při užití díla dočasnou nebo náhodnou rozmnoženinu díla v elektronické podobě, která nemá samostatný hospodářský význam, jejímž účelem je umožnit snadnější využití díla, a jejíž zhotovení je nedílnou a nezbytnou součástí technologického postupu zpřístupnění díla, včetně takové rozmnoženiny, jež umožňuje účinné fungování přenosového systému.

Téměř klasickým porušením autorského zákona je neoprávněné šíření díla, zejména po internetu. Zpřístupnění díla může být uskutečněno např.:

- ✓ Vystavením díla na webové stránky, což je nejjednodušší způsob uveřejnění, kde k provedení dostačují pouze základních znalostí a jako softwarové vybavení postačí prohlížeč webových stránek. Tento způsob je použitelný pro menší objemy dat a stránky obvykle nemají příliš dlouhého trvání.
- ✓ Použitím FTP a podobné služby určené k přenosu souborů, což se může odehrávat jak na vlastních volně přístupných serverech, umístěním na jiný přístupný server či server s omezeným přístupem nebo v posledním případě na kompromitované cizí počítače.
- ✓ Prostřednictvím elektronické pošty, což je poměrně zdlouhavé, neboť používaný protokol SMTP není určen pro přenos souborů. Tato forma obvykle slouží například k rozšiřování menších literárních nebo grafických děl v uzavřené komunitě.
- ✓ V sítích peer-to-peer, které jsou nejsilnějším prostředkem pro ilegální sdílení a výměnu dat.

Mezi poměrně častá porušení autorského zákona patří zásah do díla nebo jeho úprava. I když zákon umožňuje do programového díla zasahovat, přesně specifikuje kdy a za jakých okolností je uživatel k zásahu do počítačového programu oprávněn. Protože zákon je nadřazen smlouvě platí, že i když smlouva by zakazovala zásah do software a oprávněný uživatel by chtěl program pozměnit v rozsahu povoleném zákonem, může tak učinit.[67] Zřejmým porušením autorského zákona ale bude např. odstranění bezpečnostních prvků chránících program před zneužitím nebo odstranění identifikačních prvků programového díla.

Posledním charakteristickým porušením autorského zákona je neoprávněné užití díla. Pokud jde o programové produkty, je značným problémem prokázání neoprávněného užití

[66] Pokud někdo odcizí hmotný majetek, vzniká tím jasná újma majiteli. V případě duševního vlastnictví však újma není tak zřejmá, protože vlastník „vlastně o nic nepřišel". Mnozí lidé tedy z nevědomosti, jiní z přesvědčení, nevidí na svých přečinech proti duševnímu vlastnictví nic nezákonného.

[67] Toto omezení licenčního ujednání může být např. užitečné, pokud softwarová firma ukončí podporu produktu, nebo tato firma zanikne a v programu se objeví bezpečnostní problémy, které je nutné opravit pro bezpečné používání aplikace.

díla, pokud k němu nedojde přímým zneužitím celé nelicencované aplikace. Je samozřejmé, že autorský zákon chrání jak dílo jako celek, tak jeho části a zároveň se vztahuje jak na dílo dokončené, tak i na jeho jednotlivé vývojové fáze a části. Programy publikované jenom v uzavřené spustitelné verzi je obvykle obtížné využít, avšak u programů s dostupným kódem nemá pachatel žádné problémy s jeho získáním. Pokud je takový „open source" použit v uzavřeném přeloženém a spustitelném programu, nedá se jeho původ dost dobře prokázat[68].

5.6 Nové typy protiprávního jednání

Spolu s nástupem nových technologií se objevují i nové druhy trestné činnosti. I když jsme v předchozích kapitolách uvedli, že v mnoha případech lze zařadit technologickou trestnou činnost mezi delikty spadající do působnosti příslušných paragrafů trestního zákona, existují některé typy jednání, jejichž klasifikace může být obtížnější. Variant těchto deliktů existuje řada a v následujícím jsou uvedeny jen ty nejběžnější případy[69].

5.6.1 Hacking

Hacking je snad nejstarším deliktem, který v původním pojetí lze jenom těžko označit za trestný čin, neboť nelze vyčíslit škodu, která byla způsobena. Ostatně, někdy ani správce systému neví, že mu do systému hacker pronikl. Motivací původní hackerské subkultury nebylo způsobení škody, ale pouze radost z osobního vítězství nad technikou, spolu se získaným obdivem hackerské komunity.

Zjednodušeně bychom v současném pojetí mohli definovat hacking jako proniknutí do počítačového nebo řídícího systému jinou než standardní cestou při obejití nebo prolomení jeho bezpečnostní ochrany. Právní úprava, která by postihovala hacking jako takový je velmi obtížná. Bylo by možno použít ustanovení § 257a TZ, který hovoří o poškození nebo zneužití záznamu na nosiči informací. Zdá se, že pokud nedojde ke škodě, nikomu není způsobena újma, nebo hacker či třetí osoba nemá z průniku do systému neoprávněný prospěch, pak podstata tohoto trestného činu je nenaplněna[70]. Nicméně skutková podstata § 257a TZ nevyžaduje ke svému naplnění, aby došlo k účinku a postačuje, že pachatel jednal v úmyslu tento účinek způsobit. Skutková podstata bude tedy naplněna, jestliže pachatel získá přístup k nosiči informací ve shora uvedeném specifickém úmyslu. Jestliže k účinku nakonec nedojde, může to mít vliv na společenskou nebezpečnost trestného činu, avšak formálně bude trestný čin dokonán.

5.6.2 Kybernetické výpalné

Jakkoli se zdá toto slovní spojení nesmyslné, jedná se o nový typ trestné činnosti založený na strachu z prezentované hrozby průniku do spravovaného nebo vlastněného systému s následujícím zneužitím nebo zničením dat. I když ze strany vyděrače to mnohdy může být pouze využití neznalosti vydírané strany, je to zcela nová projekce klasického deliktu do počítačového prostředí, kterou se zejména může rozmáhat organizovaný zločin. V tomto případě jedinou ochranou, kterou ohrožení strana může použít, je důkladná analýza rizik spojených s narušením spravovaného systému a tomu odpovídající náklady na ochranu nebo vyplácené výpalné.

Pokud jde o právní hodnocení trestného činu připadá zde možnost uplatnění § 235 TZ, tedy stejného jako při klasickém trestném činu vydírání[71], s možností rozšíření o § 257 a, jenž byl diskutován v předcházejícím.

5.6.3 Šíření materiálů se závadným obsahem

Tento trestný čin, zahrnující šíření pornografie, materiálů podporujících extremismus nebo materiálů podobného obsahu spadá spíše do trestní odpovědnosti poskytovatele obsahu než do trestní odpovědnosti správce počítačového systému a nejedná se o nový druh trestné činnosti, spíše o nové médium pro její vykonávání. Je to jistá moderní projekce klasického trestného činu např. podle § 205 TZ nebo podle § 198[72]. Většina zmíněných ustanovení klasifikuje tyto trestné činy odnětím svobody až na tři roky.

5.6.4 Zneužití internetových stránek

S rozšiřováním elektronické komunikace dostal nový rozměr i jeden z nejstarších trestných činů – pomluva, v našem trestním zákoně označená § 206. Bohužel, s tou se setkáváme velmi často a oddělení „zrna od plev" není vždy jednoduché. Tak jako dříve studenti vyjadřovali svůj neúspěch u učitele hanlivými nápisy na nejrůznějších místech[73], až z některých sloganů se stal sport, dnes potichu a jednoduše vyplivnou jedovatou slinu na internet v domnění, že vlastně nepáchají nic tak hrozného. Opak je pravdou. Takové počínání je hodnoceno podle již zmíněného § 206 TZ a protože čin je spáchán pomocí „sdělovacího prostředku", jedná se tedy o kvalifikovanou skutkovou podstatu, je nutno počítat s dvouletou horní hranicí trestní sazby včetně možnosti zákazu činnosti.

Forma spáchání takového trestného činu je při všeobecné dostupnosti internetu jednoduchá a může spočívat třeba v uvedení telefonního čísla spolu s obscénní fotografií (která samozřejmě nepatří dotčené osobě, nebo je výsledkem fotomontáže) na stránkách erotické seznamky[74]. Jiný případ, který je velmi častý, je vytvoření internetových stránek vyjadřujících názory jejich autora, často doplněné faktickými nebo smyšlenými komentáři třetích stran.

K takové činnosti většinou láká falešný pocit anonymity na internetu, avšak pokud se nejedná o velmi promyšlený postup, autor může být snadno vysledován. Protože pomluva nemůže být prezentována jako nedbalostní trestný čin, může dojít k poměrně složitému dokazování skutečnosti, že pachatel věděl, že uvedené informace jsou neopravdivé. For-

[68] Programy publikované s otevřeným zdrojovým kódem v podstatě nemohou obsahovat zcizený kód, protože to může být kdykoliv odhaleno, avšak programy dodávané jako spustitelné balíky mohou použití jiného zcizeného kódu úspěšně zatajit.

[69] V tomto místě neuvádím takové činy jako je cyberstalking, neboli obtěžování s využitím technologie jako zasílání SMS, mailů apod. nebo zcizení identity, což je aktivita nesmírně narůstající. V USA je krádež identity jeden z nejrychleji rostoucích zločinů, jen za rok 2005 byly zneužity osobní údaje 9,9 milionů osob.

[70] Trestní sazba u zmíněného paragrafu je až jeden rok a při splnění dalších podmínek může být zvýšena až na pět let.

[71] Sazba podle § 235 TZ je do tří let, při zvlášť závažných případech však až 12 let odnětí svobody.

[72] Ustanovení § 205 TZ se vztahuje k ohrožování mravnosti, § 198 TZ k hanobení národa, etnické skupiny, rasy a přesvědčení. Obdobná použitelná ustanovení jsou § 198a TZ, který postihuje podněcování nenávisti vůči skupině osob, omezování jejich práv a svobod nebo § 260 hovořící o podpoře a propagaci hnutí směřujících k potlačení práv a svobod člověka.

[73] Na konci šedesátých a počátku sedmdesátých let se populární slogan, označující jednoho z profesorů ČVUT přízviskem hovězího dobytka, vyskytoval snad po celém světě. Bylo studentskou pýchou, umístit jej na co nejkurióznějším místě – bruselském atomiu nebo egyptské pyramidě, i když mnohdy ani nevěděli o koho jde.

[74] Z českého prostředí je znám případ, kdy pod jménem kandidátky do obecního zastupitelstva byly vytvořeny internetové stránky s nabídkou erotických služeb včetně mobilního telefonního čísla a doprovodných fotomontáží. To se projevilo nejenom ve výsledcích voleb, ale uvedená osoba utrpěla i značnou újmu, a tak se domáhala satisfakce u soudu.

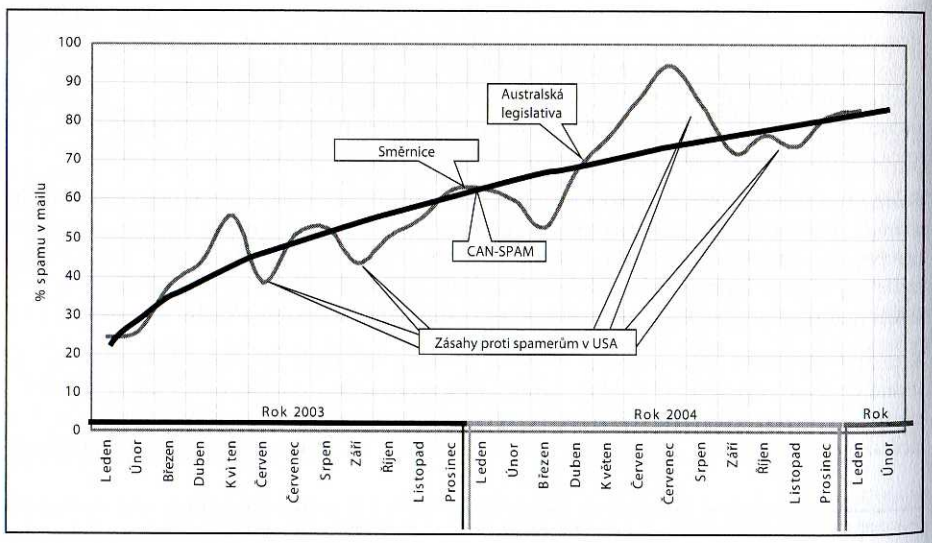
málně je trestný čin pomluvy dokonán sdělením nepravdivého údaje, který je způsobilý značnou měrou poškodit jeho vážnost u spoluobčanů. Dokazování této skutečnosti je však věc běžné agendy orgánů činných v trestním řízení, kde pouze médium použité pro šíření informace má svou specifiku[75].

konec

5.6.5 Spamming

Pod pojmem spamming se rozumí zasílání nevyžádané elektronické pošty obvykle s reklamním obsahem. Tento typ nepříjemného přímého marketingu, který obtěžuje zejména tam, kde doba připojení nebo objem přenesených dat je účtováno, je starý jako elektronická pošta sama. Spammeři získávají elektronické adresy nejrůznějším způsobem, kde nejběžnější zdroj jsou různé www konference, IRC, ICQ, registrační stránky pro služby „zdarma" nebo obdobné komunikující objekty, ve kterých může být elektronická adresa jednou z přenášených informací. I když existuje celá řada programů, které spam dokáží odfiltrovat, jejich trvalá účinnost je pochybná, neboť spameři tento mechanismus znají a pro jeho obejití často mění adresu odesílatele[76]. V poslední době jsou pro filtraci spamu používány zejména tzv. Bayesovské filtry, založené na vyhodnocení pravděpodobnosti spamu na základě analýzy struktury přijaté zprávy.

Spam je velmi obtížným efektem spojeným s elektronickou komunikací. K potlačení spamu směřovala již mnohá opatření a návrhy, nicméně jeho nárůst je téměř nezastavitelný. Jak ukazuje obr. 5.1 lze očekávat, že objem spamu v elektronické poště překročí v krátké době devadesátiprocentní hranici.



Obr. 5.1: *Trend ve vývoji spamu*

[75] Toto by si měli uvědomit i vydavatelé různých internetových časopisů a blogů. Před zákonem jsou zodpovědní stejně, jako kdyby jejich vydání mělo „papírovou" verzi.

[76] Nejenom textový údaj v datové části zprávy (tedy položku „From: xxx .. x"), ale i údaj v hlavičce zprávy za řetězcem MAIL FROM:

právní pohledy na možnost postihnutí spamu se různí. Např. jeden názor tvrdí, že pokud bude možno z adresy jednoznačně identifikovat příjemce, pak se jedná o trestný čin podle § 178 TZ[77] a to nejenom tehdy, jsou-li tato data poskytnuta spammerovi třetí osobou, ale i v případě, že je získá sám. Avšak ustanovení § 178 odst. 1 se týká pouze osobních údajů shromážděných v souvislosti s výkonem veřejné zprávy. Následující odstavec téhož paragrafu zase váže diskutovanou skutečnost jednak na získání osobních údajů v souvislosti s výkonem povolání, zaměstnání nebo funkce a jednak na porušení mlčenlivosti stanovené právním předpisem. A tak můžeme dojít i k názoru, že pod žádnou z diskutovaných skutkových podstat nebude spadat jednání osoby, která si přisvojí osobní údaje shromážděné jinak než v souvislosti s výkonem veřejné správy, např. koupí od třetí osoby, a pak na takto získané adresy rozesílá spam. Podobné stanovisko lze zaujmout i v případě, že spammer získá osobní údaje sám a nepůjde o údaje shromážděné v souvislosti s výkonem státní správy. Tím, že rozesílá zprávy nesděluje ani nezpřístupňuje osobní údaje jiné osobě než té, které se týkají. Navíc, zřejmě nemá ani povinnost mlčenlivosti.

Jiná možná klasifikace se vztahuje k porušení některých ustanovení zákona č. 127/2005 Sb. o elektronických komunikacích, který např. v § 120 odst. 1 písm. g) označuje za přestupek „použití adresy elektronické pošty pro odeslání zprávy nebo zpráv třetím osobám bez souhlasu držitele adresy elektronické pošty". Odpovědnost ve správním řízení formuluje § 118 zákona o elektronických komunikacích, kde se za správní delikt považuje zaslání nevyžádané zprávy bez souhlasu účastníka.

O regulaci spamu se pokusil rovněž zákon o některých službách informační společnosti, publikovaný pod číslem 480/2004 Sb. V tomto zákoně se zákonodárce snažil, i když poněkud nešťastně, o regulaci zodpovědnosti za ukládaný nebo přenášený obsah, kde by alespoň část odpovědnosti padla na bedra poskytovatele služby. V §7 a následujících je spam označen jako „šíření obchodního sdělení" a § 11 ukládá správní sankce při nevyžádaném šíření takové informace až ve výši deseti milionů Kč.

Poslední možností je použití ustanovení § 2 odst. 1, písm. e) zákona o regulaci reklamy č. 40/1995 Sb. Nevyžádaná pošta musí mít v tomto případě reklamní charakter a vést k nákladům[78] na straně adresáta nebo jej obtěžovat. Porušení tohoto ustanovení je trestáno peněžitou pokutou, která může být na základě posouzení příslušného orgánu uložena až do výše dvou milionů Kč.

5.6.6 Warez

Moderní počítačové pirátství, které je doprovodným fenoménem používání informačních technologií a rozmachu internetu, je většinou skupinovou záležitostí. Jedna část skupiny pracuje na prolamování ochranných prvků programových produktů, zatímco druhá část se specializuje na jejich šíření pomocí www serverů a získávání financí na jejich provoz umisťováním reklamy na pornografické servery nebo servery s erotickým obsahem na svých stránkách. Tato reklama obvykle nezkušeného „loosera" zahltí přívalem samovolně se otevírajících oken aniž by se ke kýženému software dostal.

Warezy spíše jsou jakýmsi pozůstatkem minulosti, dnes jsou používány spíše pro šíření tzv. cracků, tedy programů umožňujících zrušení ochrany u programových produktů, jejichž plné verze jsou ke stažení z internetových stránek dodavatele nebo jsou na reklamních CD, avšak jsou časově nebo jinak omezeny. V současné době jsou daleko rozšířenější pro-

[77] Tento paragraf formuluje trestní odpovědnost při neoprávněném nakládání s osobními údaji a určuje trestní sazbu až do výše pěti let.

[78] Těmito náklady je např. alikvotní část ceny, kterou adresát platí za internetové připojení.

gramy pro sítě peer-to-peer, které umožňují výměnu hudebních souborů, videa a dalších. Postihnutí nelegálního obsahu šířeného v síti peer-to-peer je samozřejmě daleko složitější než když je k šíření použit server warez.

konecma

Právní posouzení v tomto případě je jednoduché. Jedná se o porušení autorských práv na které se vztahuje § 152 trestního zákona, který umožňuje uložit propadnutí věci, peněžitý trest nebo trest odnětí svobody až na dva roky. Tato trestní sazba může být za jistých podmínek zvýšena až na pět let.

5.6.7 Cracking

Po trestné činnosti označované hacking a warez je zcela přirozené, že je nutno uvést i formu, která je s těmito dvěma neoddělitelně spjata. Jedná se cracking, tedy prolamování nebo obcházení ochranných prvků elektronických nebo programových produktů s cílem jejich neoprávněného použití. Cracking používá celou řadu metod od prostého debugování spuštěného programu až po tzv. reverse engineering. Cracking je často používaná metoda při průniku do systému, kde cílem crackingu není „zprovoznění" programu chráněného „softwarovým" nebo „hardwarovým" klíčem, ale zjištění informací důležitých pro umožnění neoprávněného přístupu do cílového systému. Nejčastěji se jedná o tzv. „password cracking" – zjišťování hesla pro přístup do systému. Password cracking má širokou škálu metod od snahy uhodnout heslo pomocí slovníku nejčastěji používaných hesel, použití hrubé síly při zkoušení všech možných kombinací znaků přicházejících v úvahu až po sofistikované algoritmy snažící se o zpětnou rekonstrukci odpovídající kombinace znaků ze zakódovaného řetězce hesla, uloženého v systémovém souboru s hesly.

Trestní klasifikace tohoto typu činnosti může být velmi rozličná a pokud právnické nebo fyzické osobě, která je vlastníkem systému vůči němuž je útok crackingem prováděn, nevznikla prokazatelná škoda, může být od stíhání zcela upuštěno[79]. V ostatních případech se obvykle jedná o porušení autorského práva (§ 152 TZ) nebo poškození či zneužití záznamu na nosiči informací (§ 257a TZ).

5.6.8 Sniffing

Neoprávněné „odposlouchávání" komunikace na síti, činnost zdánlivě nevinná, může mít rovněž svoji trestní kvalifikaci. Obvykle je předzvěstí nějaké další ilegální činnosti, např. „zachycování" hesel pro chystaný průnik do jiného systému, ale samo o sobě je naplněním trestného činu podle § 239 TZ – porušování tajemství dopravovaných zpráv. Pokud dojde ke zneužití takto získané informace např. jejím prozrazením třetí straně, pak je na řadě § 240 TZ. Trestní sazby jsou nejvýše dva roky.

Výše uvedená úvaha je však více méně hypotetická, neboť samo dopadení pachatele takového činu je téměř nemožné, a to nemluvím o problémech s dokazováním. Něco jiného je, bude-li takové odposlouchávání soustavně provádět soukromý subjekt za účelem získání informací sloužících k následujícím krokům vůči odposlouchávanému subjektu. V tom případě bude použití takových informací samo o sobě evokovat obvinění ve smyslu výše uvedeného paragrafu.

V této souvislosti považuji za nutné uvést jednu, poměrně málo známou skutečnost. Internetové adresy, záznamy o provozu sítě a ostatní záznamy umožňující jednoznačně identifikovat osobu, ke které se vztahuje nějaká činnost na síti, je předmětem ochrany hned podle dvou zákonných ustanovení – telekomunikačního zákona a zákona o ochraně osobních údajů.

[79] Nicméně viz diskuze k 5.6.1, Hacking.

Naivní správce sítě, který tyto údaje poskytne třetí osobě, se tak vystavuje postihu podle výše citovaného ustanovení trestního zákona. Zvláštní případem je úkon, kdy poskytnutí takových údajů požaduje orgán policie. Zde je nutno odlišit dva základní případy reakce správce sítě v případě, kdy je o sdělení takové skutečnosti orgány policie požádán. Rozhodující pro tento případ je, zda organizace, které síť patří, je poskytovatelem služby elektronických komunikací ve smyslu zákona o elektronických komunikacích[80]. Pokud ano, může se správce sítě dožadovat předložení povolení soudu k poskytnutí takových údajů a pokud není předloženo, nemusí tyto údaje poskytnout[81]. Pokud organizace, které síť patří, není poskytovatelem služeb elektronických komunikací, pak se jedná o skutečnost, kdy je správce sítě povinen podat policii vysvětlení na základě zákona o policii[82].

5.6.9 Cybersquatting

Pod tímto záhadným názvem se skrývá donedávna legální blokování internetových domén. Zaregistrování domén s názvem velkého podniku, instituce nebo produktu a spekulace s prodejem tohoto jména má již svůj zenit za sebou a dobíhající legislativa už asi nebude mít co postihovat. Svůj význam měl cybersquatting v době, kdy velké firmy na internet vstupovaly, nebo se rozhodovaly uvést na internetu své výrobky. Dnes spíše než porušování práv plynoucích z ochranné známky připadá v úvahu tzv. nekalá soutěž. K té může dojít např. tehdy, kdy bude zaregistrován doména mající název známého produktu a pod touto doménou bude běžet aplikace internetového obchodu se zmíněným výrobkem. Soudní spory ve všech těchto případech jsou nejednoznačné a zřejmě se justice potýká s oblastí, která jí není zcela přístupná.

Právní kvalifikace v této oblasti spadá spíše do oblasti porušování práv průmyslových a ustanovení o nekalé soutěži. V prvém případě je možná kvalifikace podle § 150 TZ, porušování práv k ochranné známce, obchodnímu jménu nebo chráněnému označení původu, jenž je ohodnocena peněžitým trestem, propadnutím věci nebo jiné majetkové hodnoty, nebo trestem odnětí svobody až na dva roky. Druhý případ nekalé soutěže spadá pod § 149, kde je možno uložit tresty podobné jako v předchozím případě s omezením výše trestu odnětí svobody až na jeden rok.

Množství problémů souvisejících se spory o doménová jména vedlo sdružení CZ NIC k vydání nových pravidel k registraci doménových jmen v doméně .CZ, která vstoupila v platnost 1. srpna 2004. Tato pravidla mimo jiné obsahují i ustanovení o řešení sporů o užívání doménového jména, která se však vztahují pouze k doménám zaregistrovaným nebo prodlouženým po tomto datu. O té doby existuje totiž povinnost držitele doménového jména vyjádřit kvalifikovaný souhlas s platným zněním nových pravidel v okamžiku registrace, prodloužení registrace nebo změny držitele doménového jména. Ve smyslu těchto pravidel jsou spory týkající se doménových jmen registrovaných držitelem řešeny Rozhodčím soudem při Hospodářské komoře ČR a Agrární komoře ČR[83]. Nicméně i tak záleží na osobě držitele doménového jména zda se rozhodne řešit spor s využitím obecného soudu nebo přijmout pravidla a využít rozhodčího soudu. Soubor rozhodnutí soudů České republiky ve věci doménových jmen je možno nalézt na uvedeném serveru www.nic.cz.

[80] Tedy, jednodušeji řečeno, zda má živnostenské oprávnění k poskytování telekomunikačních služeb.

[81] K těmto údajům patří např. IP adresa a její vlastník, záznamy o provozu apod. Jsou známy případy, kdy tyto údaje byly poskytnuty třetím osobám naivními správci sítě, kteří si zřejmě neuvědomili, že tímto okamžikem spáchali trestný čin.

[82] Viz § 12 zákona 283/1991 Sb. o Policii České republiky. Odepřít podání vysvětlení je umožněno pouze ve zvláštních případech citovaných uvedeným zákonem.

[83] Údaj, zda držitel doménového jména souhlasil s pravidly, je k dispozici v části prohledávání na www.nic.cz u každého doménového jména.

6.

Nelegální aktivity v kyberprostoru

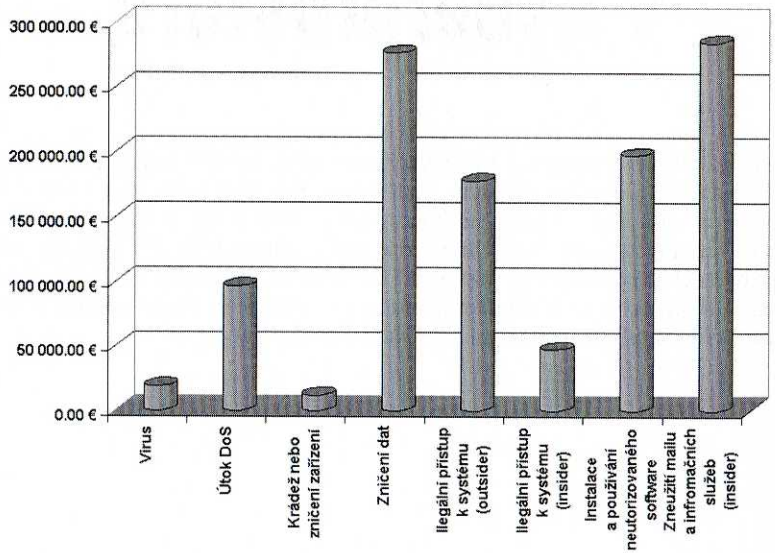
Objem nelegálních a kriminálních aktivit v kyberprostoru každým rokem roste. Každoroční přehledy vydávané Computer Security Institute a FBI o tom vydávají svědectví. Internetová zločinnost však roste i na starém kontinentě – v Německu se internetová zločinnost podílela na hmotných škodách z celkové kriminality plnými 57%. Přitom počet internetových trestných činů představoval pouhých 1,3% celkové kriminality. [C06]. Není ani divu, kybernetická kriminalita je velmi lukrativním a relativně bezpečným zdrojem nelegálních příjmů jak dokládá tabulka zpracovaná z údajů FBI (viz Tab. 6.1).

Druh aktivity	Podíl na celkovém objemu ztrát (%)	Průměrná ztráta na jeden případ (USD)
Nigerijské dopisy	2,7	5 000
Podvody s kreditními kartami	4,4	240
Zneužití důvěry (zaměstnanci)	2,3	2 025
Investiční podvod	6,2	2 000
Nedodání zboží z internetových obchodů	14,6	410
Podvody na internetových aukcích	41,0	385

Tab. 6.1: *Ztráty způsobené některými nelegálními činnostmi v kyberprostoru*

Obdobné údaje uvádějí i další zdroje. Např. podle [S03] je průměrná ztráta způsobená počítačovým zločinem odhadována na 400 000 USD, zatímco průměrná ztráta při „klasické" bankovní loupeži je asi 6 000 USD. Přitom podle téhož zdroje je pravděpodobnost uvěznění pachatelů více než trojnásobná při klasické loupeži než při počítačovém podvodu[1].

Tak jak narůstá objem nelegálních aktivit vzrůstají i ztráty, které jsou těmito aktivitami způsobeny. Podle některých pramenů mohou celkové ztráty dosáhnout až 10^{11} USD za jeden rok, nicméně v této kalkulaci jsou zahrnuty veškeré náklady na provoz internetu a veškeré finanční operace na internetu prováděné, takže uvedená částka může být významně zkreslena. Ztráty způsobené nelegálními činnostmi na internetu se velmi obtížně vyčíslují, neboť mnohé nelegální aktivity nejsou oznámeny nebo odhaleny, nicméně graf na obr. 6.1 ukazuje podíl těchto ztrát způsobených jednotlivými fenomény [R05]. Vynechány jsou ztráty způsobené finančními podvody a krádežemi chráněných informací, které se výrazně od ostatních případů liší – ztráty finančními podvody se odhadují na 3,4 milionu EUR, ztráty zcizením chráněné informace o něco výše, na 3,5 milionu EUR.



Obr. 6.1: *Ztráty způsobené jednotlivými typy nelegálního chování*

[1] Některé statistiky uvádějí pravděpodobnost, že počítačový zločinec skončí za mřížemi je asi 1 : 26 400!

Pro případného útočníka není složité při současných technických možnostech odchytit a zneužít údaje přenášené prostřednictvím veřejných sítí zejména tehdy, když jsou minimálně používány metody ochrany informací. Přitom podle výzkumu společnosti Datamonitor většina společností věnuje na zabezpečení své firmy méně než 5 % svého rozpočtu věnovaného na pořízení a podporu informačních technologií a podíl 20 % nebo více dává na bezpečnost jen necelých 10 % firem. [P04].

Přitom ne všechny případy jsou evidovány policií. Zejména banky, jejichž zisky jsou závislé na důvěře klientů, velmi nerady předávají jakékoli oznámení policii a z obavy z nežádoucí publicity raději oželí finanční ztrátu. Všeobecně platí, že zjištěna bývá jenom malá část celkové trestné činnosti na internetu a k odhalení často vede jenom náhoda.

6.1 Metody pachatelů kybernality

Taxonomie kybernetických incidentů mohou vycházet z nejrůznějších hledisek. Snad nejjednodušší přístup je rozdělení na případy lidmi přímo nezpůsobené, kam patří:

- ✓ poruchy technického charakteru jako selhání hardware, software, výpadek elektrického napájení, porucha klimatizace apod.,
- ✓ přírodní katastrofy – povodně, požáry apod.,

Incidenty související s lidským zaviněním, které mohou být dále děleny na:

- ✓ Úmyslné, které jsou přímo vedeny s cílem určitým způsobem poškodit systém nebo jeho uživatele:
  - ✓ Pasivní jako např. sledování toku informací (odposlech), tedy případy, kdy útok přímo neovlivní výkon systému, avšak může ovlivnit některé parametry bezpečnosti. Vzhledem k tomu, že se neprojevuje na vnějším chování systému, je takový incident obtížně detekovatelný.
  - ✓ Aktivní, kdy dochází k pozměňování dat. Aktivní útok v sobě obsahuje průvodní znaky, které umožňují jeho detekci, neboť dochází ke změnám v napadeném systému. Téměř všechny vzdálené útoky jsou aktivní, protože ovlivňují vnitřní stavy systému a obsahují aktivní komponenty.
- ✓ Neúmyslné, zapříčiněné chybou operátora či uživatele, nebo důvěřivostí vůči k postupům sociálního inženýrství.

Je zřejmé, že technologická úroveň zabezpečení informační a komunikační techniky neustále roste. Proto je pozornost útočníků často věnována tomu „nejslabšímu článku" systému, jímž je sám člověk – uživatel. Ten může nezamýšleným vyzrazením určitých informací snadno degradovat celou technologicky orientovanou ochranu konkrétního informačního systému. S tím souvisí i možnost dělení počítačových incidentů podle podílu „vnějších" a „vnitřních" faktorů, umožňujících jejich provedení:

- ✓ Útoky z vnějšího prostředí subjektu (tedy ryzí hacking či cracking).
- ✓ Útoky zevnitř subjektu. Pachatelem v takovém případě bývá současný nebo bývalý zaměstnanec konkrétního napadeného subjektu nebo jiná osoba, která má přístup do nitra subjektu. Útočník při svém postupu vychází ze znalosti vnitřního uspořádání systému, prostředí ve kterém je systém umístěn, konkrétní informační technologie i vnitropodnikových procesů, případně navíc disponuje i určitou úrovní

oprávnění přístupu k výpočetní technice nebo k informačnímu systému[2]. Častou obětí „insiderů", jak se takový pachatel nazývá, jsou společnosti, pracující s velkými finančními prostředky, zejména finanční ústavy. Jen velmi málo jsou činu insiderů technologicky komplikované. Většinou se jedná o relativně jednoduché a přímočaré aktivity založené na znalosti systému a přístupových práv, stejně jako na znalostmi nedostatků v bezpečnostní politice subjektu[3].

- ✓ Útoky kombinované – úmyslné. V tomto případě dochází k selhání zaměstnance či jakékoliv osoby, znalé podrobností o zabezpečení systému. Ke konkrétnímu činu se ale taková osoba neodhodlá sama, ale informace a poznatky, kterými disponuje, předá třetí straně, která jich využije k aktivitám směřujícím k napadení systému.
- ✓ Útoky kombinované – neúmyslné, kdy osoby uvnitř subjektu nevědomky umožní či usnadní útok zvnějšku. V těchto případech můžeme rozeznat:
  - ✓ Metody „sociálního inženýrství", jejichž základem je schopnost zneužít důvěřivosti osob uvnitř konkrétního systému, s cílem získat od nich informace, nutné pro průnik do systému (např. heslo), nebo je přimět k jiné pro systém škodlivé činnosti[4].
  - ✓ Invazivní kódy, kam např. patří e-mailoví červi. V tomto případě se snaží útočník textem zprávy přimět adresáta, aby vykonal určitou činnost např. klikl na soubor v příloze mailu, apod. Výjimkou nejsou ani případy, kdy oprávněný uživatel nebezpečný software sám do svého systému nainstaluje když uvěří, že instalace příslušného programového vybavení je nutná pro lepší funkci jeho systému.
  - ✓ Poplašné zprávy tzv. hoaxy, které přinášejí různá sdělení, od spíše humorných až po katastrofická[5].

Uvedené příklady demonstrují, jak velkou roli hraje „počítačová negramotnost" a bezpečnostní školení osob, uvnitř jednotlivých organizací. Zvláště ve velkých podnicích, kde nejsou jasně stanovena bezpečnostní pravidla, mohou uvedené metody vést k úspěchu.

Typickým příkladem zneužívání naivního uživatele je postup zvaný phishing[6]. Podstatou metody usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtů apod. za účelem jejich pozdějšího zneužití, je vytvoření podvodné zprávy šířené např. elektronickou poštou, s pomocí níž se pachatel snaží zmíněné údaje z uživatele vylákat[7]. Zprávy jsou maskovány tak, aby co nejvíce imitovaly důvěryhodného

[2] Například v USA bylo v posledních letech pouze cca 6 % pachatelů kybernetických útoků proti konkrétním institucím z prostředí mimo tyto organizace; 24 % pachatelů bylo přímo zaměstnaných na výpočetním středisku postižené organizace a 70 % se rekrutovalo z koncových uživatelů výpočetní techniky v poškozené organizaci.

[3] I když to přímo s trestnou činností nesouvisí, je možno při této příležitosti vzpomenout určité „jemnější" formy negativního působení pracovníků oddělení informačních technologií, např. správců sítě, která se nazývá „IT-Governance". Jedná se o případy nátlaku, kdy uvnitř konkrétního subjektu takové osoby de facto „vydírají" různými hrozbami poruchy, ztráty dat a dalších magických událostí laiky, včetně vedení subjektu, s požadavky na konkrétní techniku či privilegia.

[4] Příkladem může být situace, kdy se některému zaměstnanci firmy telefonující hacker představí jako administrátor, který momentálně není u sebe v kanceláři a potřebuje jeho spolupráci při ověřování určité funkce systému. Proto požaduje zaměstnancovo heslo nebo jinou důvěrnou informaci.

[5] Příkladem může být zpráva, která označovala jeden z důležitých systémových souborů Windows (nejčastěji sulfnbk.exe) za virus a požadovala po uživateli jeho odstranění. Po vymazání souboru přestal operační systém fungovat.

[6] Slovo „phishing" je kombinací z „fishing" a „phreaking". Do češtiny se někdy překládá jako „rybaření".

[7] Podle serveru „Antiphishing" je úspěšnost phishingu vysoká, asi 5 %. Počet pokusů o phising rychle stoupá. Zatímco v listopadu 2003 bylo zaznamenáno necelých 30 unikátních útoků touto metodou, v březnu 2004 jich už bylo 420 (z toho 110 cílených na eBay, 98 na Citibank a 63 na Paypal).

odesílatele. Může jít třeba o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu (použití dialogového okna, předstírajícího, že je oknem banky – tzv. spoofing). Podobně funguje tzv. „maškaráda", tedy situace, kdy útočník přesměruje provoz, směřující na konkrétní adresu na adresu falešnou podobně nebo stejně vypadající, a tak se snaží přistupující osoby přesvědčit, že jsou na známé důvěrné adrese. Tímto způsobem bývají často zcizována čísla kreditních karet a jejich PIN[8].

Příkladem phisingu může být pokus o útok na server eBay uvedený na obr. 6.2. Viditelná adresa na stránce sice odpovídá adrese serveru eBay, avšak skutečný link směřoval server útočníka. Po kliknutí byl uživatel přesměrován na server útočníka, který se ale tvářil jako server eBay, a zde vyplnil všechny příslušné formuláře, aby zachránil své konto u eBay. Ale nejen, že konto nezachránil, ale ještě útočníkovi předa citlivé údaje o své osobě a potřebné přístupové kódy[9].

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Copyright © 1995-2005 eBay Inc. All Rights Reserved.

Obr. 6.2: *Příklad phishingu, souvisejícího s internetovým obchodem e-Bay v prosinci 2005*

Prostudujeme-li scénář phishingu, pak si asi většina čtenářů řekne, že člověk musí být hodně naivní, aby na takovou léčku skočil. V případě phishingu tedy vina z nezanedbatelné části padá na důvěřivost uživatelů a útočník z této lidské slabosti promyšleně těží.

Phising však odstartoval nebezpečnější variantu útoku zvanou „pharming", která je sofistikovanější a především nebezpečnějším. Jedná se vlastně o útok na DNS server, na kterém dochází k překladu doménového jména na IP adresu. Pokud pak uživatel ve svém internetovém prohlížeči zadá adresu například své banky, pak při úspěšném útoku nedojde k překladu na odpovídající IP adresu, nýbrž nějakou jinou, podvrženou. Pokud budou stránky na podvržené adrese dostatečně věrohodně imitovat známé stránky banky používané útočníkem, pak nic netušící uživatel zadá požadované přihlašovací údaje a obdaruje jimi útočníka. Obrana před pharmingem na straně uživatele není vůbec jednoduchá.

[8] Prvním známým případem pokusu o uplatnění phishingu v prostředí bankovní sféry České republiky se v březnu 2006 stala Citibank. V povědomí rovněž vstoupil útok na klienty České spořitelny v létě 2006.

[9] Tento způsob vylákání údajů se také někdy nazývá „skimming".

Na konec této kapitoly jenom shrňme co všechno může útočník použít, aby způsobil škodu a sám se obohatil. Jsou to zejména:

konecma

- ✓ osobní data klientů či zaměstnanců,
- ✓ seznamy klientů zaměstnavatele,
- ✓ různé druhy obchodního tajemství, např. marketingové plány.

Nicméně škoda může být způsobena i jinými způsoby elektronické manipulace, která povede k:

- ✓ znepřístupnění dat jejich majiteli, zcizení kopie dat spojené se jejich prodejem nebo následným vydíráním,
- ✓ podvržení dat,
- ✓ zmanipulování dat při výběrovém řízení,
- ✓ sociotechnickému útoku se znalostí postupů,
- ✓ vydírání prostřednictvím nenahraditelnosti,
- ✓ poškození pověsti (dezinformace)
- ✓ nekalé konkurence (používání firemního softwaru, hardwaru).

Jinými druhy elektronické manipulace může být dokonalá znalost příslušného software, zejména nedokumentované přechody do privilegovaného režimu nebo nedokumentované části kódu.

6.2 Insideři a nespokojení zaměstnanci

Díky informačním technologiím a množství informací, které firmy denně potřebují pro svůj provoz, se objevila zcela nová skupina hrozeb označovaná jako „nespokojení zaměstnanci" nebo v širším pojetí „insideři". Nespokojený zaměstnanec nebo insider je pro firmu v mnohém nebezpečnější než profesionální tým útočníků zvenku zejména pro jeho vědomosti o chodu firmy, které nashromáždil během své pracovní činnosti, a mnohdy znalostem klíčových informací o zabezpečení. Cizí útočník musí před zahájením útoku pojmenovat hlavní slabiny bezpečnostního systému firmy. Současný či bývalý zaměstnanec jistě prošel bezpečnostním školením, které mu v identifikaci slabých článků systému napomohlo. Také znalost přihlašovacích jmen a hesel, i v případě že již pracovní poměr skončil, je při útoku cennou devizou.

Metody útoku nespokojeného zaměstnance se značně liší podle toho, jestli je stále v pracovním poměru, nebo mu byl pracovní poměr ukončen. Zásadní rozdíl je tedy v dostupnosti prostředků a v chování potencionálního pachatele, kdy současný zaměstnanec se více obává možnosti prozrazení. K současnému zaměstnanci lze nalézt stopy snadněji než k člověku, který společnost již dávno opustil.

Dá se říci, že v převážné většině je motivem protizákonného jednání finanční zisk. Spokojenost zaměstnance ve firmě je ovlivněna celou řadou faktorů, ale výše částky na výplatní pásce je pro většinu zaměstnanců zásadní. V mnoha případech nejde jen o existenční nouzi ale i o soutěžení a porovnávání, neboť pro mnohé mzda vyjadřuje míru uznání jejich schopností. Motivace zisku může být i zástupná; pachatel se nechce obohatit, ale zakrýt např. předchozí ztrátu, kterou způsobil.

Mnohé pachatele však k útoku proti zaměstnavateli, mnohdy již bývalému, však nevede potřeba zisku, ale jiné lidské pohnutky. Pro propuštěného zaměstnavatele to může být touha po pomstě, demonstrace vlastních schopností, kdy chce zklamaný jedinec bývalému zaměstnavateli ukázat jak dobrého zaměstnance se zbavil[10]. Nelze pominout ani motiv soupeření, kdy prostřednictvím běžných pracovních nástrojů, ať už se jedná o počítač nebo charakter obchodní smlouvy, soupeří se svými kolegy v zaměstnání nebo se svými bývalými kolegy. Typickými nástroji takového soupeření je „přenos" firemního know-how nebo demonstrace slabin bývalých kolegů prostřednictvím útoku na jejich práci[11].

6.2.1 Možnosti jednotlivých profesí

Každý pracovník, každá profese a každá pozice ve firmě má své atributy, kterými rámuje svůj postoj a svoje možnosti vůči firemnímu informačnímu systému. Podle toho může i zaměstnanec na příslušné úrovni těžit ze své pozice při získávání informací důležitých k provedení útoku. Možnosti jednotlivých pozice jsou vyhodnoceny dále.

6.2.1.1 Manažer, vedoucí pracovník

Vedoucí pracovník nese největší část zodpovědnosti za provedená rozhodnutí. Z pozice své funkce má přístup k většině důležitých informací včetně těch s nejvyšším stupněm utajení, takže se nikdo nad jeho otázkami nepozastavuje. Pro vysoce postaveného manažera není tedy problém informace získat (okopírovat pro svoji potřebu nebo pro prodej třetí straně), změnit (ve svůj prospěch svůj nebo prospěch třetí strany), nebo v nejkrajnějším případě některé nebezpečné nebo obtížné informace zničit.

6.2.1.2 Správce objektu

Tito zaměstnanci obvykle nemají k ohrožení znalostního fondu firmy dostatečnou kvalifikaci[12]. Mohou však poskytnout příležitost ke spáchání trestné činnosti. Bezpečnostní opatření konstruovaná s předpokladem, že se útočník nemůže někam fyzicky dostat, v tomto případě selhávají. Významné riziko představuje rovněž nedbalost osoby správce např. při nedbalé kontrole vpustí do objektu již bývalého zaměstnance, ignoruje prohledávání odváženého odpadu z firmy apod.

6.2.1.3 Právník/účetní

Pracovník právního oddělení firmy může svého zaměstnavatele poškodit zejména vypracováním nevýhodné či zcela chybné smlouvy. Pokud uzavírá smlouvu se spřátelenou stranou může získat i nemalou finanční pozornost. Nicméně může spáchat také tento čin z nedbalosti, nebo i s úmyslem vytvořit zaměstnavateli škodu. Důslednou kontrolou lze tento druh rizika výrazně minimalizovat.

Podobného provinění se může dopustit i účetní. Svou úmyslně špatnou prací může vytvořit účetní chyby, které potom anonymně oznámí, aby došlo k provedení auditu. Jestliže toto pozměnění dokumentů vyvolá řízení proti firmě, tak se těžko může bránit tím, že zaměstnanec pochybení vytvořil úmyslně, aby firmu poškodil. Motivem účetního může být také

---

[10] Tento motiv je nejčastější u vysoce kvalifikovaných profesí.

[11] Např. proniknutí do systému jako důkaz propustnosti zabezpečení podnikové počítačové sítě nebo neschopnosti nového správce systému, který nastoupil na místo propuštěného pracovníka.

[12] Pokud se s tímto cílem nenechají zaměstnat a nejsou na provedení útoku připraveni.

maskování způsobené ztráty nebo vlastní obohacení[13]. I když používané účetní programy obsahují celou řadu kontrol, omezujících účetní práci pouze na nezbytné úkony, přesto je dostatek příležitostí k pochybení.

konecma

6.2.1.4 Správce databáze

Pracovník spravující chod firemní databáze se stará mimo jiné o kontrolu přístupu k datům, shromažďuje a vyhodnocuje protokoly o provozu apod. Jeho pracovní náplň ho staví do role nejvýše postaveného kontrolora provozu firemních dat [V01]. Jelikož je nejvýše postavenou osobou v této oblasti, dostává se do vhodné pozice k neoprávněné manipulaci s daty, aniž by byl výrazně ohrožen odhalením. Má v rukou všechny nástroje, aby falešnými daty zakryl svou skutečnou činnost. Případné provinění lze odhalit pouze náhodně nebo hloubkovým auditem. Z praxe je znám případ, kdy FBI zachytila pokus nespokojeného zaměstnance, který konkurenční společnosti nabídl kompletní databázi zákazníků jejich rivala za 20 000 dolarů[14].

6.2.1.5 Programátor

Všichni členové vývojového týmu, kteří by se pokusili vložit do kódu nějaké nedokumentované rysy, by měli být odhaleni, jestliže celý tým dodržuje potřebné bezpečnostní směrnice. Jejich nejdůležitější součástí je vzájemná kontrola práce, i když většinou náhodná, aby objem práce kontrolou příliš nenarostl, a podrobná dokumentace vytvářeného produktu. Příkladem nebezpečného rysu může být nedokumentovaný vstup do privilegovaného režimu bez nutnosti prokázat potřebná oprávnění.

Jeden ze způsobů, jak by se programátor mohl obohatit vhodnou úpravou programu, je popsán v kultovní knize McNeala „Poradce", která byla i zfilmována. Zde autor operačního systému pro velkou banku v Anglii vytvořil program tak, že při zaokrouhlování se nižší hodnoty zlomků sčítaly a posílaly se na jeho konto[15]. Vzhledem k obrovskému počtu operací součet nepatrných částek rychle rostl a na kontě pachatele přibývaly miliony, které nikomu nescházely[16].

Bohužel v mnoha i velkých organizacích panuje značná volnost při přípravě nového programového vybavení a poukazování na nutnost dodržování alespoň základních bezpečnostních pravidel při vývoji software je odmítáno s poukazování na nárůst nákladů[17].

[13] Známý je případ bývalých účetní firmy Cisco Systems Geofreye Osowskiho a Wilsona Tanga, kteří si při neoprávněném přístupu do počítačového systému společnosti Cisco vydali sami sobě akcie společnosti Cisco za téměř 8 milionů dolarů.

[14] Podobný případ je znám i z České republiky, kdy zaměstnanec jednoho peněžního ústavu zkopíroval data o klientech na CD a nabízel toto CD k prodeji. Velmi nebezpečné jsou databáze udržované outsourcovanými „ostrahami objektů", které zapisují jak jméno návštěvníka tak i osobu, kterou navštívil. Konkurence, která takovou databázi získá z ní snadno vyhodnotí případný záměr sledovaného rivala na trhu.

[15] Tento postup se nazývá „salámová metoda".

[16] Bankovní programy obvykle pracují s několika desetinnými řády pod nejmenší hodnotou rozlišitelnou v příslušné měně. Např. pokud nejmenší hodnotou bude jeden haléř, pak program bude provádět příslušné bankovní operace na setiny haléře a výslednou sumu na celé haléře zaokrouhlí. Tak při každé operaci vznikne nepatrná částka, která teoreticky nikomu nechybí.

[17] Mohu z vlastní soudně znalecké praxe potvrdit, že i v organizacích profesionálně se zabývajících programováním a zaměstnávajících desítky programátorů se velmi často aplikuje metoda „hordy".

6.2.1.6 Správce sítě/systému

Správce sítě je nejvyšší autoritou ve svém oboru a podobně jako správce databáze i firemním mágem, který vždy vyřeší spletitý problém s výpočetní technikou. Používáním odborného slangu je většinou laikům velmi vzdálen a jeho kontrola běžnými způsoby je nesmírně obtížná, takže ji většinou nikdo neprovádí. Nestojí nad ním žádný dohled, který by odhalil nechráněná slabá místa vzniklá z nedbalosti nebo úmyslně[18], a umožňující jiné osobě neoprávněný přístup. Specifickým činem správců systému je útok na vlastní systém, který má demonstrovat proniknutelnost jeho obrany a který může být motivován nejenom nespokojeností se zaměstnavatelem, ale třeba i snahou získat financování na nákup dalšího hardware a software. Škoda může také vzniknout nedodržováním směrnic o kontrole a dokumentaci provozu.

6.2.2 Co říkají statistiky a průzkumy

Skupina „insiderů", neboli vlastních pracovníků firmy je středem zájmu mnoha průzkumů a statistických šetření. Skupina pro národní počítačové trestné činy amerického FBI (National Computer Crime Squad) odhaduje, že kolem 80 % počítačových trestných činů je pácháno „zevnitř", tedy buď přímo zaměstnanci a nebo osobami, které se nějakým způsobem dostanou do prostor firmy. Z toho 85-97 % proniknutí do systémů a krádeží dat není vůbec zjištěno [I02]. Je zřejmé, že kriminalita nespokojených zaměstnanců nemůže být nikterak opomíjena a je třeba se jí věnovat.

Potencionálními pachateli jsou i lidé, na níž v bezpečnostní politice firmy bývá často zapomínáno. Správce budovy, uklízečka, zahradník, to jsou osoby, které mohou mít jednoduchý přístup do prostor, které jinak pečlivě hlídáme a přístupy do nich u ostatních zaměstnanců sledujeme. A i oni mohou být nespokojenými zaměstnanci. Velmi nebezpečnost skupinu tvoří najímané bezpečnostní agentury jenž mají dokonalý přehled o pohybech osob ve firmě a mohou v některých případech fungovat jako „trojské koně" konkurence.

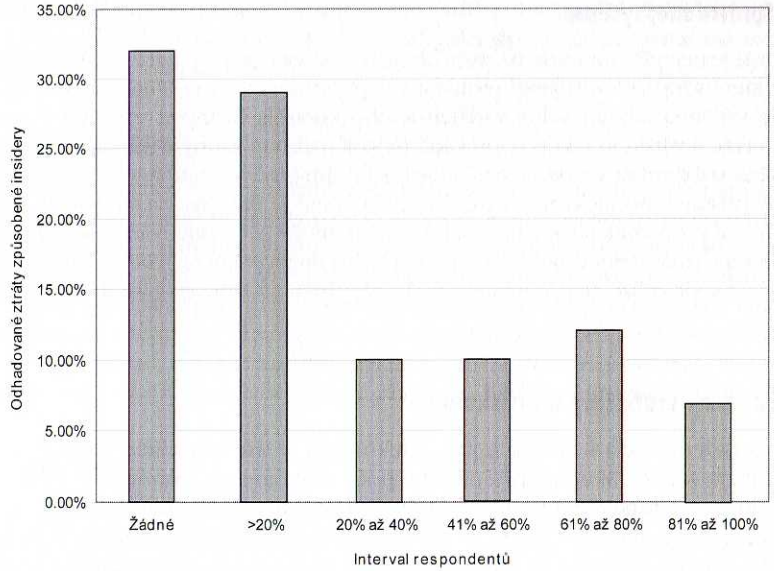
Když se podíváme na grafy které uvádí Peschl [P05] ve své starší práci[19], vidíme, že s počítačovými zločiny spáchanými zaměstnanci se setkalo plných 61 % respondentů a jsou hned po virech druhou největší hrozbou firem. V roce 2002 uveřejnila konzultační firma Gartner [M03] odhad, že více než 70 % neautorizovaných vstupů do informačních systémů je pácháno zaměstnanci. Z tohoto počtu až 95 % vede ve svém důsledku k významným finančním ztrátám. Z ostatních studií zaměřených na tuto oblast [F03] vyplývá, že téměř 53 % zaměstnavatelů věří, že jejich současní zaměstnanci představují větší riziko pro infrastrukturu společnosti než bývalí zaměstnanci nebo lidé zvenčí. Je vidět, že i sami zaměstnavatelé si uvědomují riziko, které pro ně nespokojení zaměstnanci představují.

Mezi největší agentury, které se zabývají vyhodnocováním rizika spojeného s útoky v kyberprostoru patří Computer Security Institute. Tato agentura vydává každoročně přehled jednotlivých aspektů nebezpečnosti v informačních technologiích v průzkumu nazvaném Computer Crime and Security Survey. V přehledu 2006 [G03] je zajímavý odhad ztrát způsobených insidery, který vychází z odpovědí 536 respondentů – viz obr. 6.3.

[18] V praxi jsem se setkal s případem, kdy správce sítě, v níž byla umístěna velmi citlivá data, a proto síť nebyla z venku přístupná, z pohodlnosti tajně instaloval modem na svoji telefonní linku, aby mohl provádět správu sítě „z postele".

[19] Ve své práci se opírá o materiál [C07].

konecma



Obr. 6.3: *Ztráty způsobené útoky „insiderů" vyjádřené v procentech*

Jak je vidět, na rozdíl od předchozích studií, pouze téměř třetina respondentů věří, že skupina insiderů a nespokojených zaměstnanců netvoří žádné nebezpečí. Jak vyplývá ze zprávy, pouze 7 % respondentů předpokládá, že insideři mají na svědomí více než 80 % ztrát v jejich organizaci. Podobné hodnoty udávaly zprávy z minulých let. Jak je vidět, jednotlivé studie jsou ve značném rozporu v pohledu na kriminalitu vlastních zaměstnanců, ať už jde o skupinu nespokojených nebo jinak motivovaných pracovníků.

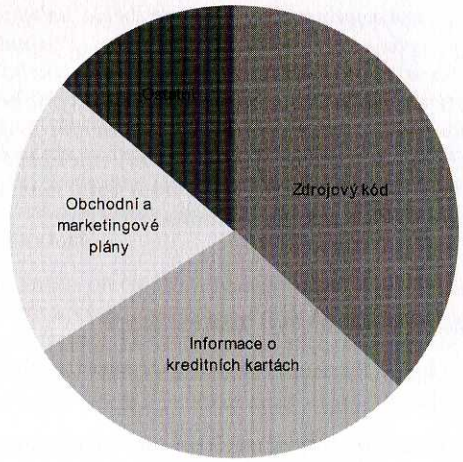
Pokud pro další informace nahlédneme do zprávy Computer Crime & Abuse Report [C08], kterou na 6 266 případech počítačových zločinů spáchaných v rozmezí 01. 01. 2001 – 31.12.2002 zpracovali na Asian School of Cyber Laws pak zjistíme, že podle této zprávy se na trestných činech souvisejících s informačními systémy podílelo 52 % zaměstnanců a bývalých zaměstnanců[20]. Vnější útočníci, kteří cíleně útočí na uložené informace, představují pouhých 11 % a jsou téměř stejně nebezpeční jako skupina Script Kiddies (8 %). Téměř 30 % útoků představuje konkurence a obchodní rivalové, kteří často používají zaměstnance a nebo bývalé zaměstnance k získání informací nebo přístupu k systému.

Uvedená zpráva je rovněž zajímavá pro její pohled na strukturu zcizených dat[21], která je uvedena na obr. 6.4. Úspěšné útoky jen v malém procentu zahrnují neautorizovaný přístup[22] a převažuje použití maligního kódu nebo sociálního inženýrství.

[20] Z toho činí 21 % stávající a 31 % bývalí zaměstnanci.

[21] Data byla zcizena ve 33 % případů.

[22] Podle citované zprávy se činí útoky přes komutované linky (dial in) 18 % a internetové útoky 15 %.



Obr. 6.4: *Struktura zcizených dat*

I když jedna skupina tzv. „analytiků" ve sdělovacích prostředcích varuje především před nárůstem organizovaných skupin útočících na informační systémy zvenčí a druhá naopak zdůrazňuje, že větší množství útoků pochází zevnitř, především od nespokojených zaměstnanců, nelze na základě dosud provedených průzkumů podepřít ani jeden názor. Situace je poměrně nepřehledná, a to navzdory očekávání obou stran. K nejasnosti situace zejména přispívá, že mnoho incidentů není hlášeno, a tedy ani formálně vyšetřováno. Přesto většina ochranných a preventivních mechanismů je orientována především na vnější hrozbu, a to zejména proto, že dodávky bezpečnostních programů a řešení představují poměrně dobře prosperující trh. Nicméně není možno podcenit úlohu insiderů, ať už jde o nespokojené zaměstnance nebo pracovníky jinak motivované. Pro ilustraci uveďme na konec této kapitoly několik případů zjištěných útoků, které byly způsobeny interními zaměstnanci firem[23].

Zaměstnanec, pracující po 11 let ve Stamfordu, v pobočce společnosti Omega v Connecticutu jako správce počítačové sítě, byl usvědčen ze škody ve výši 10 milionů dolarů, jež způsobil firmě smazáním interních programů. Více než 1000 programů svého zaměstnavatele smazal svým programem čítajícím jen několik řádek kódu.

Bývalý zaměstnanec finanční instituce byl obviněn z trestných činů, získání nepovoleného přístupu k informacím instituce, počítačového podvodu, zneužití osobních údajů a finanční zpronevěry. Tato obvinění byla vznesena na základě zjištění, že zaměstnanec získával soukromá data klientů firmy (mimo jiné číslo řidičského průkazu, údaje o kreditní kartě, výši zůstatku na účtu) a poskytoval je třetím osobám za úplatu. Útočníkem byl odcházející zaměstnanec, který si tak chtěl přilepši na úkor svého zaměstnavatele[24].

[23] Příklady pocházejí ze serveru http://www.usdoj.gov.

[24] Jedná se o velmi častý případ při přecházení pracovníků ke konkurenčním firmám. Jednou ze zásad při oceňování společnosti je, že hodnotu společnosti určují její zákazníci. Tím, že odcházející zaměstnanec si při odchodu zkopíruje databázi zákazníků své firmy a v nové firmě osloví bývalé zákazníky přímo, aby pokračovali ve spolupráci s ním i když pod novou firmou, zvyšuje svoji cenu pro nového zaměstnavatele. Přivedením nových zákazníků totiž velmi efektivně zvyšuje podíl nového zaměstnavatele na trhu. Nemusí však vždy jít jen o nové zákazníky, může se jednat např. o důvěrné informace o produktech, připravovaných marketingových strategiích apod.

konecma

Na základě anonymního udání proběhla nebytových prostor v sídle středně velké severomoravské společnosti. Předmětem prohlídky byly počítače užívané společností. Podle zpracovaného znaleckého posudku byly na počítačích nainstalovány mimo jiné počítačové programy společností Autodesk a Microsoft, ke kterým firma nebyla schopna doložit licence ani nabývací doklady, v celkové hodnotě přibližně 670 tisíc korun. Jednatel společnosti byl v této souvislosti obviněný z trestného činu porušování autorských práv[25].

6.2.3 Kategorizace nelegálních aktivit zaměstnanců

Nelegální aktivity nespokojených zaměstnanců a obecně insiderů lze najít v několika oblastech. Patří k nim zejména:

- ✓ Neoprávněné využití strojového času, kam spadají všechny aktivity, které zatěžují počítačové vybavení firmy k jiným než pracovním účelům, např. tisk vlastních materiálů na tiskárnách, brouzdání po internetu, stahování dat z internetu, hraní počítačových her a podobně. Zejména brouzdání a stahování velkých objemů dat nutí zaměstnavatele k nasazování stále k větších a větších omezení a často končí úplným zákazem přístupu k internetu a povolení pouze daných stránek pro firemní použití. Druhotné škody vznikají zaměstnavateli tím, že brouzdáním v pracovní době se snižuje produktivita práce zaměstnanců.
- ✓ Krádeže počítačového spotřebního materiálu, zejména spotřebního – disket, papírů do tiskárny, náplní tiskáren apod. V mnoha firmách takovéto jednání do jisté míry tolerují, jinde se mu již začínají bránit.
- ✓ Neoprávněný přístup a nebo pokus o získání přístupu k datům, která nespadají do zaměstnancova perimetru. Rovněž do této kategorie spadá oblast dat, k nimž zaměstnanec sice může mít přístup, ale pouze pro účely výkonu své práce. Pokud získává data nad její rámec, jedná se o neoprávněný přístup[26].
- ✓ Krádež hardware je vlastně běžný trestný čin krádeže a jen z jakýchsi podivných důvodů je zařazována do kategorie počítačové kriminality.
- ✓ Krádeže software jsou specifické pro oblast počítačové kriminality a jsou i častější než krádeže hardware. Taková krádež není na první pohled vidět, poškozenému vlastně nic nechybí, a tak se velmi často ani nezjistí. Zajímavým právním případem je vykrádání programů jeho vlastními autory, tedy případ, kdy autor v pracovním poměru připraví pro svého zaměstnavatele program a následovně přejde ke konkurenci, kde je pověřen sepsáním podobného software. Obvykle se netrápí s vymýšlením nových procedur a převezme původní program s minimálními úpravami. Pokud působí obě firmy na malém a podobném trhu, pravděpodobně se to brzo projeví a způsobí to nemalé problémy právního charakteru[27].
- ✓ Úmyslné fyzické poškozování hardware připomíná dobu, kdy tkalci ničili nové stroje v přesvědčení, že jim berou práci. Příčinou k takovému chování může být afekt zaměstnance („to zařízení nefunguje, tak do něho praštím"), odložení práce do které se zaměstnanci nechce nebo prostá msta vůči zaměstnavateli.
- ✓ Smazáním dat nebo software může vzniknout firmě významná škoda[28] (viz poznámka str. 119). I když by všechna data měla být zálohována a k programům existovat instalační CD, pokud chce obeznámený zaměstnanec spáchat takový čin, zničí i zálohy dat. Přitom vše může vypadat jako nehoda a ne záměrný útok. Zejména nepříjemné je, pokud se jedná o software vyvinutý „na míru" nebo o zdrojové kódy nového programového produktu.

Kategorizace trestných činů a přečinů u bývalých zaměstnanců i stávajících zaměstnanců nemůže být úplným výčtem všech možností, avšak ukazuje co přichází v úvahu a nač si zaměstnavatel musí dávat pozor. Ne nadarmo se říká, že pod svícnem je nejvíc tma a již nejeden podnikatel musel po útoku zvnitřku ukončit svojí činnost. Případy ukradených klientů, technologií, zdrojových kódů a posléze zrod vlastního podnikání jsou velmi časté.

I když jsme se již zabývali statistikami a průzkumy s víceméně bezzubým závěrem, nelze pro doplnění opomenout zajímavou společnou studii Carnegie-Mellon Univerzity a US Secret Service „Insider Threat Study" [I03], která podrobně analyzuje padesát případů počítačových útoků provedených zevnitř společnosti. Závěry, ke kterým se studie dobrala lze shrnout následovně:

- ✓ Většina (59 %) útočníků byla v době útoku již bývalými zaměstnanci postižených společností, 41 % z nich ještě v době útoku ve firmě působila.
- ✓ Způsob jakým útočník opustil své místo, byl kategorizován takto:
  - ✓ 48 % případů propuštění,
  - ✓ 38 % vlastní rezignace,
  - ✓ 7 % odeslání na nucenou dovolenou nespecifikované délky.
- ✓ Většina byla ve firmě zaměstnána na plný úvazek (77 %) a na technické pozici (86 %), např. správce sítě, programátor, technik, IT specialista.
- ✓ Drtivou většinu útočníků tvořili muži (96 %), zhruba polovina z nich byla v době útoku ve stavu manželském, pouze necelá třetina byla předtím trestána za jiné přestupky (např. automobilová havárie s následky).
- ✓ 82 % postižených organizací byla v soukromém sektoru a většina byla aktivní v informačních technologiích a telekomunikacích.

Studie dále uvádí, že nejčastějším důvodem k útoku byla událost vztahující se k práci, např. propuštění z práce, spor se zaměstnavatelem, spolupracovníkem, nebo přeložení na jiné oddělení, a většina útočících byla motivována touhou po pomstě. Velká část útoků byla plánována dopředu a blížící útok se dal rozpoznat ze změny chování zaměstnance; v řadě případů se útočníci svěřili některému ze svých kolegů a někdy dokonce útokem otevřeně hrozili. Pokud jde o charakteristiku útoku pak:

- ✓ většina útočníků měla v době nástupu do zaměstnání administrátorská práva, ale v době útoku měla autorizovaný přístup jen necelá polovina z nich;
- ✓ útoky byly provedeny ze vzdáleného počítače a mimo pracovní hodiny;

[25] Příklad je převzat z databáze http://www.bsa.org/czechrepublic. Jedná se o typickou pomstu odcházejícího zaměstnance, který může i podobnou situaci před odchodem zinscenovat.

[26] Sem spadá i nelegální obchodování s těmito daty, viz Příklad 2 výše.

[27] Z vlastní soudně znalecké praxe mohu uvést případ, kdy takto učinila skupina programátorů, a to několikrát. Pokud je mi známo, k soudnímu jednání nedošlo a firmy to řešily vzájemně mezi sebou mimosoudním vyrovnáním.

[28] Smazání dat patří k nejstarším počítačovým kriminálním činům. Řadí se k nim také první počítačový trestný čin v bývalém Československu, kdy operátor počítače ze msty přemazal permanentním magnetem data na páskách počítače používaného správou sociálního zabezpečení k výpočtům důchodů. Výplata důchodů se tak zpozdila, celý čin byl tehdy postaven politicky a pachatel byl odsouzen.

- ✓ v 60 % případů byl při útoku kompromitován nějaký účet – buď cizím uživatelem s heslem, nebo neautorizovaný uživatelský účet vytvořený samotným útočníkem;
- ✓ v devíti případech z deseti nebyl útočníkovi zakázán dálkový přístup (remote access), což je přinejmenším překvapivé;
- ✓ přes 70 % útoků bylo odhaleno lidmi, kteří neměli bezpečnost ve firmě na starost;
- ✓ útoky způsobily firmám finanční ztráty, měly vliv na obchodní operace organizací a poškodily jejich reputaci.

Jak ze zprávy vyplývá, útok byl téměř vždy nastartován negativním incidentem týkajícím se zaměstnance, a tak by zaměstnavatelé měli věnovat zvláštní pozornost pracovníkům u nichž k takovému incidentu došlo. Bylo by vhodné, aby s těmito případy počítala i firemní bezpečnostní politika, která by specifikovala zásady přístupu k těmto potenciálně nebezpečným zaměstnancům.

6.2.3.1 Možnosti nespokojených zaměstnanců, kteří setrvají ve firmě

Základem rozboru možností nespokojeného zaměstnance, který zůstává ve firmě je jeho pozice a rozsah uživatelských práv. Nejčastěji to bude zaměstnancem, který má běžná uživatelská práva, a tedy bude využívat prostředky zaměstnavatele pro své soukromé účely. I když neprovádí přímo žádný trestný čin, rozhodně se nechová korektně vůči firmě. V tomto smyslu může běžný zaměstnanec:

- ✓ **Instant Messaging**, používání Instant Messaging nepředstavuje velkou hrozbu pro bezpečnost firemního systému, i když principiálně je možné pomocí děr v těchto programech kompromitovat příslušný stroj, a tím získat vnitřní přístup do firemní sítě. Další riziko je předávání informací z firmy ven pomocí této služby.
- ✓ **„Streamovaná" videa**, sledování videa je velmi častý úkaz, který významně ukrajuje ze síťových zdrojů a snižuje efektivitu zaměstnance. Vysoká zátěž firemní linky může blokovat nebo brzdit uživatele, kteří mají v úmyslu pracovat.
- ✓ **Peer-to-Peer programy**, tedy programy pro sdílení dokumentů, programů a dat mimo to, že linku, kterou zaměstnavatel pro svoji firmu pořídil mohou sebou nést prvky trestných činů neoprávněného kopírování audiovizuálních děl a software, ke kterým je využívána technika zaměstnavatele[29].
- ✓ **Nepovolené aplikace**, spouštěním nepovolených aplikací se riskuje zavlečení virové infekce do firemního počítačového systému.

Uživatel, který disponuje větším oprávněním přístupu k informacím, např. manažer, může předávat důvěrné informace konkurenci, pořizovat kopie interních dat jako jsou databáze klientů, receptury, pracovní postupy, tipy na investice nebo marketingové plány a strategie firmy, pro vlastní využití nebo za účelem jejich výnosného prodeje.

Administrátorská práva umožňují přístup ke všem prostředkům a informacím, s nimiž třeba ani běžně nepracuje. Pomstychtivý administrátor může např. škodit zpomalováním systému, jeho poškozováním nebo dalšími triky, které na první pohled nemusí ani vypadat jako úmysl. Zneuctěný správce může po síti šířit viry, poškozovat hardware, likvidovat či záměrně poškozovat data;

[29] Další skrytou hrozbou jsou viry, které se podle průzkumů skrývají ve 60 % programů stažených prostřednictvím peer-to-peer sítě Kazaa.

6.2.3.2 Možnosti nespokojených zaměstnanců, kteří firmu opustí

Škála možností pro přípravu pomsty zaměstnance, který odchází za vypjaté situace z firmy, je široká. Nejjednodušší případy zahrnují zničení hardware, buď zřejmé a viditelné a nebo maskované, které se projeví až po nějaké době, smazání dat software, popř. ponechání maligního kódu na počítači, který zaměstnanec používal. Administrátoři systémů si před svým odchodem nechávají na serverech otevřená zadní vrátka, případně časovanou bombu či trojského koně na serveru.

Jiné možnosti jsou pro bývalé zaměstnance, kteří svůj odchod neplánovali, ale přesto touží po nějaké té „pomstě". Nabízí se např. využití přístupového kódu do doby než bude kód změněn nebo uživatel ze systému smazán. Běžné je využití kontaktů navázaných v průběhu zaměstnání a získání přístupových kódů bývalého kolegy, nebo jej přímo požádat o zpřístupnění klíčové informace; výhodou je znalost bezpečnostních procedur fungujících ve firmě. Znalost způsobů sestavování mailových adres umožní zaplavení bývalého zaměstnavatele anonymní nevyžádanou poštou, je-li zaměstnanec zkušený hacker sám, může pokusit o průnik do systému a získat odtud informace nebo pozměnit webové stránky. Jinou možností je přesměrování pošty či pozměnění směrovacích tabulek nebo záznamů DNS.

6.3 Vliv lidského faktoru na únik informací

Dříve než opustíme problematiku insiderů a nespokojených zaměstnanců, bylo by vhodné vzpomenout další faktory, které jsou nebezpečné pro firmu a pocházejí z vlastní lidských zdrojů. Výzkumné práce ukazují, že lidská chyba nebo opomenutí je příčinou 70 až 80 % havárií [R03]. Projekce této hodnoty je uvedena v [C09], kde autoři dochází k závěru, že úspěšný počítačový útok byl založen v 63 % na lidské chybě.

Lidská chyba může mít různé sociálně psychologické příčiny, může k ní docházet na různých místech v organizaci, avšak vždy bude doprovázena slabinami v organizaci a řízení nebo v nedostatku chápání principů bezpečnosti. Empirické výsledky ukazují, že organizace mezi dvěma krajními oblastmi minimalizace chyb v oblasti bezpečnosti:

- ✓ Procedurální, založený na přesné soustavě pravidel formovaných v bezpečnostních politikách a jiných vnitřních normách organizace.
- ✓ Volní, vycházející z vůle vlastních zaměstnanců eliminovat vlastní chyby a založenou na podpoře této snahy řetězcem školení a tréningů.

Procedurální přístup vychází z přesné definice cílů organizace, které jsou známy předem, a jež formují soustavu procesů nutných k dosažení plánovaného výsledku. Tento typ svázané předpisové struktury je vhodný zejména tam, kde je organizace významně hierarchicky strukturována a obsahuje značný podíl pracovníků s minimální potřebou kreativity. Je však zřejmé, že sebedokonalejší struktura předpisů nemůže zabránit lidské chybě, může ji jen minimalizovat[30]. Existují také četné případy, kdy bezpečnostní „kultura" organizace pokulhává za současným vývojem ve světě IT nebo je s ním zcela nekonzistentní. V následujícím textu budou uvedeny některé typické oblasti selhání, ač uvolněnou informací jsou ve své podstatě malicherné, mohou umožnit úspěšný kybernetický útok.

[30] Dokonalá předpisová struktura není v žádném případě synonymem kvality bezpečnostních procedur.

6.3.1 Nerozpoznání možné hrozby

Tato oblast hrozeb spočívá zejména v nízkém ohodnocení obsahu zpráv, které jsou o organizaci veřejně přístupné. Mnohdy se jedná zdánlivě o nevinnou informaci, která však v sobě nese dostatek prvotních znalostí pro případného útočníka.

Uvedený problém začíná u uveřejnění obsahu doménové registrace na webových stránkách správce příslušné domény – viz obr. 6.5. Pouze asi 10 % organizací se snaží tyto údaje anonymizovat, a tak jednoduchým dotazem může útočník získat poměrně cenné údaje o osobě, která zodpovídá za technickou a organizační stránku příslušné sítě. Data uvedená v zápisu pak mohou sloužit jako prvotní podklad pro útok metodami sociálního inženýrství.

Prohlížení kontaktu

Aktuální registrace

Identifikátor kontaktu	OLDSTAR1
Jméno	Vladimir
Příjmení	Novak
Datum narození	4. 6.1979
Typ dokladu	
Číslo dokladu	
E-mail	oldstar1@mbox.mojedomena.cz
Telefon	+420 123 456 789
Fax	+420 987 456 321
Způsob upozornění na změny	
E-mail pro oznámení	oldstar1@mbox.mojedomena.cz
Heslo	Ne
Registrace od	10.08.2001

Adresa
Novákova 152, 146 00 Praha 4 - Nusle

PGP veřejný klíč

Sitemap | FAQ

Obr. 6.5: *Stránka s údaji o osobě technického kontaktu (web registrátora)*

Jiným případem absence vnímání případného rizika pro organizaci je uveden na obr. 6.6. Jednoduchý dotaz prostřednictvím vyhledávače, kde bude zadáno slovo „firewall" a jméno organizace, najde část diskuze, v níž je uvolněna poměrně citlivá informace týkající se firemní sítě. Základním aspektem ztráty ocenění případného rizika je fakt, že administrátoři a systémoví inženýři velmi často vyhledávají pomoc na diskuzních fórech a sami takovou asistenci jiným poskytují.

```
... je to vazne ... potrebuju koupit takovy firewal, který mi
zdvladne 2 az 10 Mbit abych propojil nase kancelare v (uvedeny
adresy) . Asi mi nezbejva nic jineho, nez to protahnout
vzduchem a nerad aby se na to nekdo chytil a sniffoval na
nasi siti ... v te konfiguraci se mi jedna o pripojeni k sajtu
(uvedena adresa serveru)...
```

Obr. 6.6: *Část textu z diskuzního fóra, kde správce sítě jedné pojišťovací firmy diskutuje o zabezpečení své sítě*

I když výměna informací je jedním ze základních aspektů sítě internet, v některých případech se stává hrozbou pro organizaci. Mezi informace, které mohou být jednoduše získány z internetu pomocí vyhledávací strojů, např. Google, patří:

- ✓ konfigurace firewallů,
- ✓ současné a minulé technické problémy příslušné sítě,
- ✓ operativní údaje, týkající se instalace firewallů nebo vůbec sítí.

Mnohdy jsou tyto informace umístěny na stránkách firem, které technologii instalovaly a uvádí konfigurace v případových studiích. Hledanou informaci o síti zjistit též vyhledáním problémů s danou sítí spojených – např. zadáním slova „problem" a jména příslušné sítě nebo organizace do „Google Newsgroups" je možno najít celou řadu detailů o cílové síti.

Výše uvedené příklady absence vnímání citlivosti informace ukazují, jak zaměstnanci organizace zodpovědní za provoz sítě nebo dokonce její bezpečnost ztrácí potřebnou obezřetnost při řešení technického problému v „počítačové" komunitě. Útržky zdánlivě nedůležitých informací může útočník složit v poměrně věrný obraz cílové sítě a na takto získané informaci útok založit.

6.3.2 Nedokonalá normativní báze

Rues a Kunz analyzovali bezpečností rizika počítačových sítí asi padesáti velkých firem, kotovaných na burze [R03]. Všechny měly svá pravidla, struktury, procesy a politiky. Empirická analýza však ukázala, že nedostatkem není nedokonalá předpisová stránka, ale nekvalitní a podceněná normativní báze používání internetu zaměstnanci při práci. Problém neleží ani tak v té části bezpečnostní politiky firmy, která definuje způsoby používání internetu, jako v nedostatku kontroly nad obsahem informací, jež směřují z firmy ven.

Citovaná zpráva ukazuje, že zaměstnanci používají své podnikové adresy pro vyřizování korespondence, která nemá nic společného s jejich prací, souvisí např. s jejich činností v politické straně, aktivitami ve volném čase nebo dokonce s vyhledáváním sexuálních služeb. Aby podpořili svoje závěry, ve zprávě je doloženo vyhledání slova „pokemon"[31] v souvislosti s názvem velké firmy z oblasti pojišťovnictví. Vyhledávací stroj vrátil 320 referencí na toto téma jejichž bližší analýzou bylo zjištěno, že se jedná o korespondenci otců nebo matek shánějících pro své potomky specifické karty pokemónů.

Internetový normativ je ve většině firem omezen na časový limit „brouzdání" po webových stránkách. To vychází z poměrně jednoduché úvahy, že čas strávený neproduktivním „brouzdáním" je čas neproduktivní. To co není pokryto bezpečnostní politikou, jak vyplývá z citované studie, je obsah a povaha informace, kterou si zaměstnanci s okolním světem vyměňují. Tato omezení připadají v úvahu zejména tam, kde hrozí únik citlivé informace, tj. účast v různých newsgroups a chatování.

6.3.3 Problém bezpečnostní kultury

I když slovní spojení „bezpečnostní kultura" nepatří zrovna ke slovním spojením na první pohled srozumitelným, asi nelze studovanou skutečnost jinak vyjádřit. Analýza dokumentů, které organizaci opouštějí prostřednictvím elektronické komunikace, ilustruje, že zejména technická řešení jsou často hledána mimo organizaci bez zjevné snahy ponořit se do problému hlouběji [T01]. Kvalita předávané zprávy a její informační bohatost, např. konfigurace hardware, otázky související s nastavením programového vybavení nebo systému apod., se

[31] Dětské hrací karty.

většinou vztahují ke specifickým problémům uvnitř organizace. Panuje všeobecný pocit, že řešení takových problémů může být nalezeno snadněji mimo danou organizaci, a tak vznikají diskuze na fórech, které obsahují poměrně značné množství údajů o informačním systému organizace.

Stinnou stránkou této otevřené diskuze, jak je asi zřejmé, je fakt, že jsou uvolněny některé důvěrné informace, které mohu být vytěženy potenciálním útočníkem. Tato situace je o to nepříjemnější, že jednotlivé příspěvky do diskuze zůstávají na fórech poměrně dlouho a mohou být snadno vyhledány např. Googlem a seřazeny tak, že dají poměrně vydatný obraz o informačních technologiích v organizaci.

6.3.4 Obchodní partneři a zaměstnanci

Slovo „organizace" samo o sobě vyvolává představu složitého provázaného systému. Jeho komplexnost je dána nejenom složením jeho prvků a množstvím jednotlivých komponent, ale také objemem informací, které systém – organizace, vyměňuje s okolím [W04]. Analogie s tímto tvrzením může být nalezena i v případech unikání „nevhodných" informací mimo organizaci. V kontextu úniku nevhodné informace je zřejmé, že hrozba nemusí být zřetelná uvnitř organizace. To je patrné zejména tam, kde potřeba generovat nové příjmy a vytvářet nové obchodní příležitosti žene podnikatele k uveřejňování podrobností o zajímavých referencích, např. publikování zpráv ve formě tzv. „white papers", kde jsou uváděny podrobnosti specifického řešení nebo implementace u daného klienta. Potřeba nových obchodních příležitostí však často vede k uveřejňování informací a detailů, které není nutno v uvedeném kontextu zveřejňovat, a často může vést k ohrožení klienta nebo vlastní firmy.

Příkladem je stránka na obr. 6.7. kde jsou uveřejněny nepotřebné detaily implementace u klienta ve snaze přitáhnout dalšího případného zákazníka (např. software firewallu). Často zdrojem těchto nepotřebných detailů je marketingová složka firmy, která si zakládá na dobře znějících názvech z technického prostředí v domnění, že to zvýší „odbornost" firmy v očích zákazníka. Podobným problémem mohou být i informace předávané nechtěně bývalými zaměstnanci. Nejedná se o to, že by úmyslně uváděli podrobnosti spojené s jejich působením ve firmě, avšak důkladně vyplní dotazník k žádosti o nové zaměstnání s dobrým úmyslem stimulovat zájem potenciálního zaměstnavatele nebo personální agentury. Opět jednoduchým pokusem s vyhledávacím strojem Gogole zjistíme[32], že při zadání řetězce „(resume OR curriculum) +engineer +project" povede k vyhledání dotazníků obsahujících např. požadavky na:

- ✓ jméno a detaily projektu, na němž jste pracoval,
- ✓ technologie používané v projektu uvedenou firmou,
- ✓ počet lidí pracujících na projektu,
- ✓ problémy a řešení implementovaná ve specifickém projektu nebo
- ✓ finanční data projektu.

Z tohoto hlediska není pro konkurenci složité soustředit seznam projektů souvisejících s příslušnou firmou a zjistit potřebné detaily[33].

[32] Bylo vyhledáváno v bohatší anglické části webových stránek.

[33] Na tomto místě je vhodné upozornit na „publikační hysterii" mezi vědeckými pracovníky. Ta je zřejmě podporována velkými firmami, které zejména ze zemí bývalého východního bloku, kde chybí bezpečnostní prověrka vědeckých publikací, získávají nezměrné množství nových poznatků v podstatě zadarmo. Autoři v touze po publikaci v renomovaném časopise jsou schopni uvést v článku i bezpečnostně citlivé informace a poměrně omezená množina těchto časopisů je průběžně sledována, informace ověřeny a posléze použity nebo rychle patentovány.

Success Story

Industry/Market
Automotive

Applications/Solutions
- ..... Content Management Server
- Oracle 8i database
- Sun Cluster 3.0 software
- Checkpoint firewall software
- Tuxedo middleware

Products/Services
- 2 Sun Enterprise 4500 servers
- 4 Sun Enterprise 420R servers
- 8 Sun Enterprise 450 servers
- 2 Netra T1 servers
- Sun StorEdge disk arrays
- Solaris Operating Environment
- Sun Professional Services
- SunSpectrum PlatinumSM Support Services

Obr. 6.7: *Reference k projektu informačního systému pro významného výrobce*

6.3.5 Možná obrana proti úniku informací

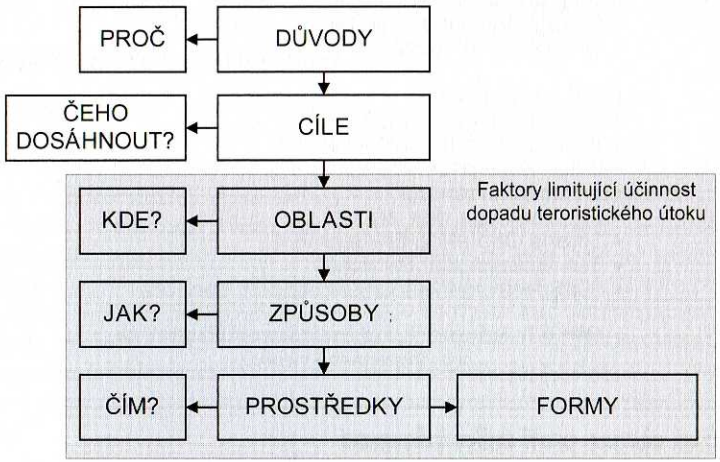
I když by se dalo říci, že každá obrana proti nevědomému lidskému selhání je těžká, pokusme se alespoň nastínit několik postupů a pravidel, které by bylo vhodné dodržovat:

1. Podpora vážně míněné výchovy pracovníků k robusní bezpečnostní „kultuře" – vedoucí pracovníci firmy musí nejenom jasně formulovat základní principy, ale také je sami dorživat.
2. Vytvořit prostředí se silnou individuální vazbou na bezpečnostní politiku, tedy zejména používat interní vzdělávací mechanizmy a neopomínat na pravidlené opakování kurzů i praktické prověřování získaných poznatků (např. formou simulovaných útoků).
3. Zajistit, aby instrukce, pravidla a pokyny v bezpečnostní politice byly formulovány jasně a srozumitelně.
4. Zajistit, aby pracovníci získali správný přístup ke vnímání hrozby úniku informace. zejména tak, že každý pracovník pochopí a porozumí základním rysům tohoto bezpečnostního rizika.
5. Zajistit pravidelné prověřování informací a označování kvalifikace materiálů v organizaci široce přístupných.

Těchto pět pravidel by mělo pomoci organizaci minimalizovat riziko úniku informace, a to i nevědomého. Nicméně zaměstnanec je jen chybující člověk, a ani při největší pečlivosti a přípravě není možno obsáhnout všechny varianty, které informační systémy pro únik informací představují.

6.4 Terorismus a jeho projekce do kyberprostoru

Terorismus představuje jednu z aktuálních forem globálních hrozeb. Lze sledovat jeho nárůst a rozšiřování do podstatné části světa. Historické materiály dokládají, že terorismus byl vždy prováděn s konkrétním cílem a z počátku byly teroristické akce motivovány spíše ideologicky. Postupem času tato motivace přešla do náboženské a nacionalistické roviny, která se zejména v poslední době výrazně upevnila. Každý teroristický čin je soustředěn na tři základní faktory – oblast, způsob a prostředky realizace (viz obr. 6.8). Při jejich optimální kombinaci jsou následky teroristického útoku ničivé.

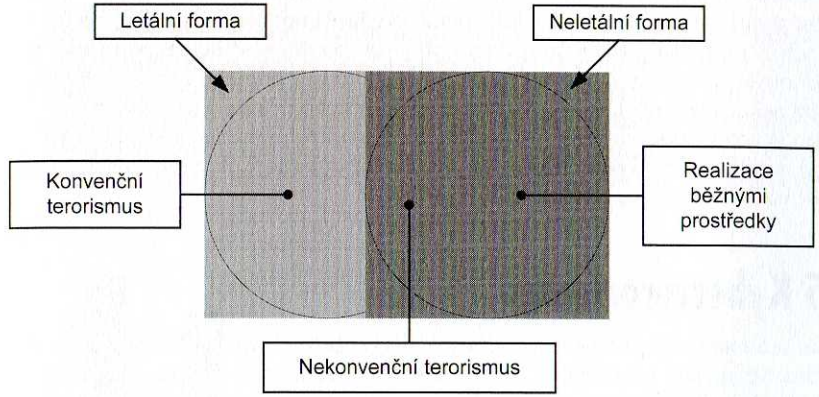


Obr. 6.8: *Schéma procesu realizace teroristických akcí*

K teroristickým akcím dochází z řady různých podnětů. Většinou chtějí teroristické organizace na sebe upozornit, neboť teroristický útok je zviditelněním jejich ideologie, a hrdě se ke svým útokům hlásí. Jindy, ve snaze o minimalizaci rizika, volí strategii anonymity. Faktorem ovlivňujícím toto chování a celý proces výběru cílů teroristických akcí, jsou prvotní důvody terorismu, kam patří:

- ✓ Politický terorismus, který lze dále podle rozhodujícího motivu dělit na:
  - ✓ separatistický, jehož hlavním důvodem je snaha teroristických skupin o získání vlastního státu nebo alespoň autonomie;
  - ✓ revoluční, který bývá také označován jako protistátní a jeho hlavní příčinou je nespokojenost se stávajícím politickým režimem.
- ✓ Náboženský terorismus, kdy teroristické skupiny zpravidla vedou válku za vyhlášení „svatého božího státu", který by byl založen na „božím" pořádku, v souladu s příslušným náboženstvím. Jedná se o specifickou formu fanatismu, kdy teroristé se považují za „boží bojovníky", kteří jsou předurčeni ke zničení současného „zlého světa" a vytvoření „nového" světa jen pro „vyvolené".
- ✓ Kriminální terorismus zahrnuje skupiny provozující organizovaný zločin jejichž hlavním cílem je získání finančních prostředků provozováním ilegálních aktivit. Svoji činnost většinou nejrůznějšími způsoby maskují nebo prohlašují za útoky extrémistických skupin.
- ✓ Psychotický terorismus, což je individuální druh terorismu, jehož hlavním důvodem je vytvoření pocitu uspokojení u duševně nemocného člověka. Aktérům stačí, pouze když jejich čin vyvolá pozornost a hrůzu, které jim zpětně přinášejí zvrácené potěšení a uspokojení.

Terorismus můžeme rozdělit podle formy na letální a neletální formy terorismu, kde první skupina se vyznačuje použitím běžných prostředků pro realizaci násilí. Letální terorismus může být dále členěn na dvě podskupiny, lišící se použitými prostředky, na konvenční terorismus a nekonvenční terorismus. Do podskupiny konvenčních forem letálního terorismu se řadí útoky páchané pomocí běžně dostupných bojových prostředků, např. střelných zbraní, zatímco mezi nekonvenční formy letálního terorismu řadíme zneužití zbraní hromadného ničení[34].



Obr. 6.9: *Vztahy letálních a neletálních forem terorismu*

V oblasti kyberprostoru jsou však běžnější neletální formy terorismu nebo útoky, při kterých jsou využívány moderní nástroje v kombinaci s letálními prostředky. Konvenční forma neletálního terorismu zahrnuje tři podskupiny:

- ✓ Neozbrojený terorismus, často označovaný termínem „unarmed terrorism", je způsob vedení teroristických akcí, při nichž jsou prostředky každodenního života použity novým způsobem, a to jako zbraň či donucovací prostředek[35].
- ✓ Kyberterorismus, který patří mezi největší nebezpečí 21. století. Principem kyberterorismu je, zjednodušeně řečeno, zneužívání výpočetní a telekomunikační techniky včetně internetu jako prostředku a prostředí pro uskutečnění teroristického útoku. Jedná se podobně jako u klasického konvenčního teroristického útoku o plánovanou činnost, motivovanou zpravidla politicky či nábožensky a realizovanou spíše malými skupinami než vojensky organizovanými strukturami[36]. Jak bude uvedeno dále, cílem těchto skupin je především ovlivnění veřejného mínění či politických elit, čímž se odlišují od hackerství. Vzhledem k rychlému šíření komunikačních

---

[34] Otázka zneužití jaderných zbraní jednotlivcem či skupinou je velmi diskutována již od druhé poloviny 70. let. Vzhledem k náročnosti výroby a udržování této zbraně se však nadále předpokládá, že teroristické skupiny touto zbraní dosud nedisponují. To však již nemusí platit pro státy podporující terorismus. Jsou však zaznamenány případy zneužití chemických nebo biologických zbraní, které jsou relativně dostupné např. chemické útoky japonské náboženské skupiny Om Supreme Truth v letech 1994 a 1995, kdy byla použita bojová látka sarin nebo biologické útoky poštovními zásilkami se sporami antraxu v roce 2001 na území USA.

[35] Jedná se např. o dopravní prostředky jako je automobil, letadlo, vlak či loď jako nosičů výbušnin nebo přímo jako ohrožující zbraň.

[36] Toto tvrzení není zcela jednoznačné. Existuje více než čtyřicet zemí disponujících arzenálem pro vedení informatického boje, který může být použit. A je možné, že tyto prostředky jsou k dispozici i státům podporujícím terorismus, kterými mohou být použity ve „vojenském rozměru".

a výpočetních systémů po celém světě, představuje kyberterorismus významné nebezpečí a je teroristickými skupinami využíván ve stále rostoucí míře;

- ✓ Mediální terorismus, někdy také označovaný jako psychologický terorismus. Jedná se o plánované zneužívání hromadných sdělovacích prostředků a dalších psychologických prostředků v době míru, za účelem ovlivnění názorů celé populace nebo cílených skupin obyvatelstva.
- ✓ Procesní terorismus zaměřující se na zneužití základních principů demokracie a jejího soudního aparátu.

Nekonvenční forma neletálního terorismu zahrnuje, podobně jako u letálních forem, nekonvenční zbraně, mezi které lze zařadit zbraně využívající principy akustiky, optiky a elektromagnetického pulsu[37]. Hlavním efektem při jejich použití je vyřazení protivníka nebo jeho elektronických systému na určitou dobu z boje, a to bez přímého ohrožení života. Součástí použití nekonvenčních zbraní je i vyvolání psychického účinku a jeho využití. Je zřejmé, že do této skupiny bude rovněž patřit použití informatických zbraní s ohledem na jejich možný dopad na infrastrukturu protivníka, a tím i na životně důležité funkce státu, např. bankovnictví, zásobování obyvatelstva apod.

6.5 Kyberterorismus

Pojem terorismus je pro běžného občana něco obtížně kontrolovatelného, nepředvídatelného. Ve spojení s termínem „kybernetika" se k sémantice obávaného pojmu ještě přidává strach z magie informačních technologií, na nichž je moderní společnost závislá. Ač se pojem „kyberterorismus" se stal v poslední době velmi frekventovaným i v běžném jazyce, nebyl doposud tento pojem přesně definován. Poprvé byl použit v devadesátých letech minulého století Barry Collinem, pracovníkem Institute for Security and Inteligence v Kalifornii. Ten v roce 1996 popsal několik scénářů, které svou povahou odpovídaly kyberteroristickému útoku [C10], a tak otevřel pole pro zkoumání možností kyberteroristů a dopadů jejich aktivit.

Mezi scénáři se vyskytl i často zmiňovaný populární scénář kybernetického útoku, kdy terorista ovládne systém řízení leteckého dopravního provozu, který se skládá z rozsáhlé sítě počítačů. Nicméně právě v tomto případě je nutno si uvědomit, že ani počítače v letecké dopravě neovládají všechno, pouze poskytují služby člověku, který je ovládá. I kdyby začaly poskytovat špatné informace nebo přestaly poskytovat informace úplně, tak je na konci vždy pilot, člověk, který se musí rozhodnout[38].

Nejčastěji citovaným pramenem definice kyberterorismu je [D01], kde autorka uvádí: „Kyberterorismus je konvergencí terorismu a kyberprostoru. Je obecně chápán jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů". Abychom mohli výše teroristický akt pojmenovat kyberterorismus podle zmíněné definice, musí se citovaný útok odrazit v násilí proti jedinci nebo společnosti, nebo musí způsobit dostatečnou škodu na

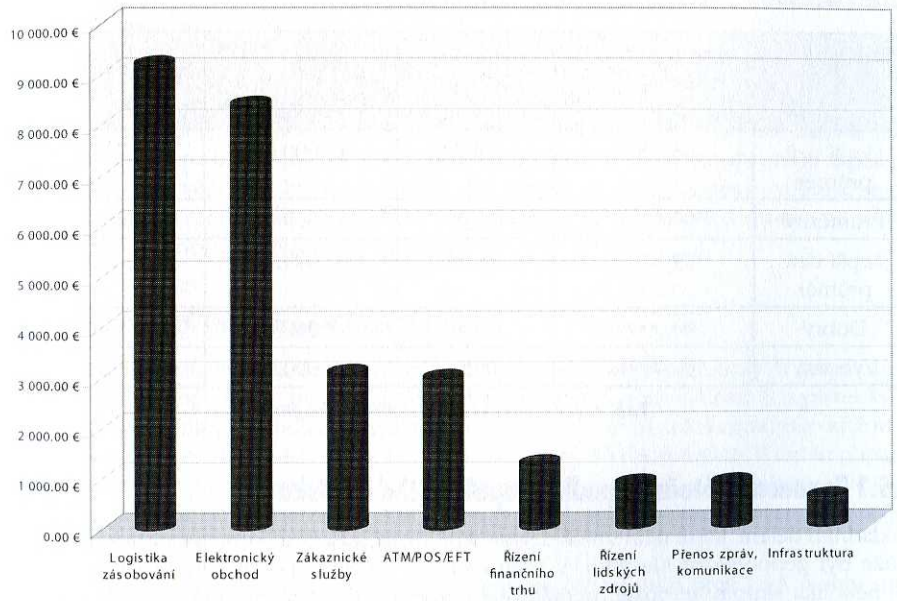
[37] Vzhledem k tomu, že se jedná o zbraňové prostředky, které jsou neustále ve vývoji, nejsou zatím příliš rozšířeny. Pro vojenské účely je také relevantním důvodem absence smrtícího či těžce zraňujícího efektu a vysoká finanční náročnost tohoto typu zbraně.

[38] Součástí výcvikového programu pilotů je zvládání krizových situací souvisejících s výpadkem řídícího systému a pilot musí umět rozpoznat, kdyby se letecký dispečer zmýlil. Navíc i v letecké dopravě platí pravidla podobná silničním, takže i v případě, že by celý systém vypadl, měla by se všechna letadla dostat bezpečně na zem.

to, aby budil strach. V tomto smyslu jsou za akty kyberterorismu považovány útoky proti kritické infrastruktuře a útoky, které nenarušují neklíčové služby obvykle pokládány za akty kyberterorismu nejsou.

I když se autorka pokusila o velmi přesnou definici kyberterorismu, opomněla jeden důležitý fakt, který doprovází veškeré teroristické aktivity v kyberprostoru – psychologický moment napadení protivníkovy sítě jakýmkoli způsobem. Tento efekt, dostatečně znásobený hrozbami a jinými metodami psychologické války, může být postačující k tomu, aby uvnitř protistrany vyvolal takovou míru strachu, jež sekundárně povede k významným fyzickým, ekonomickým nebo jiným škodám značného rozsahu. A právě na tento sekundární efekt mnohé kyberteroristické skupiny sázejí.

Scénáře kybernetických útoků jsou mnohdy předmětem kritiky a obviňování, že bez korektních podkladů uvádějí enormní výše škod a následků. Je pravdou, že některé scénáře jsou poněkud nadsazené, nicméně škody způsobené výpadky informačních systémů mohou dosahovat skutečně značných rozměrů. Na obr. 6.10 je graf ukazující odhadované ztráty způsobené výpadkem informačního systému trvajícím jednu minutu. Ztráty jsou děleny podle typických segmentů trhu, ve kterých se informační systémy nejvíce uplatňují[39].



Obr. 6.10: *Ztráty za jednu minutu výpadku informačního systému*

Je zřejmé, že mnoho aktivit již vyžaduje vysokou dostupnost systémů, obvykle bez přerušení v tzv. režimu 24x7. Dosažení tohoto stavu není jednoduché, avšak společnosti takovou spolehlivou službu vyžadují zejména ze tří základních důvodů:

- ✓ **Globalizace obchodu a podnikatelských aktivit**, kdy mnoho firem si otvírá své zahraniční kanceláře, avšak z obchodních důvodů chce udržet systém centralizovaný. To znamená, že databázové systémy a aplikace centrálního systému musí být k dispozici kdykoliv.

[39] Údaje o ztrátách vycházejí z číselných údajů uvedených v [R05].

- ✓ **Tlak konkurence**, kdy pokud jedna společnost, např. banka, rozšíří svoje úřední hodiny, ostatní to musí udělat také, jinak přijdou o část zákazníků. To opět vede k rozšíření nároků na podpůrné informační systémy.
- ✓ **Ztráty při výpadku systému** – již poněkud starší studie FIND/SVP Strategic Research Division Report z roku 1992 ukazuje, že průměrná ztráta na příjmech po dobu výpadku informačního systému činí asi 1 300 USD za jednu minutu výpadku. Tato studie byla zpracována ještě před významným rozšířením internetu a zahrnula poměrně rozsáhlou škálu respondentů počínaje výrobci, přes zdravotnictví pojišťovnictví, dopravu až po telekomunikační sektor. Je tedy zřejmé, že firma, která nebude disponovat systémem poskytujícím služby v režimu 24x7 bude automaticky přicházet o značné příjmy každou minutou, kdy její systém nebude k dispozici.

V této souvislosti je zajímavé uvést, jakou dostupnost by měl systém mít, aby byl schopen konkurence. Odpověď dává tab. 6.2, kde jsou uvedeny parametry systému podle jeho hodnocení. Podobně jako v předchozím vychází tabulka z dat uveřejněných v roce 2004 v [R05]. Je pravděpodobné, že nároky na minimalizaci výpadků systému budou ještě stoupat, nicméně i tak je zřejmé, že rozdíl necelých dvou procent v době výpadku systému se může projevit ve ztrátě řádu jednotek milionů dolarů.

Hodnocení systému	Podíl provozního času (typický)	Výpadky za rok (v hodinách)	Ztráty za neplánovaný výpadek (v USD)	Ocenění rizika neplánovaného výpadku (v USD)
Horší než průměr	98,000%	174,72	42 000,00	7 338 240,00
Průměrný	99,000%	87,36	42 000,00	3 669 120,00
Lepší než průměr	99,500%	43,68	42 000,00	1 834 560,00
Dobrý	99,900%	8,736	42 000,00	366 912,00
Výborný	99,999%	0,09	42 000,00	3 780,00

Tab. 6.2: *Ocenění rizika výpadku systému*

6.5.1 Taxonomie útočníků podle geopolitického hlediska

Základním dělení, které nám umožní jistou klasifikaci působení kyberteroristických skupin může být geopolitické hledisko. V tomto smyslu můžeme potenciální útočníky rozdělit do několika skupin: teroristé, nepřátelské národní státy, sympatizanti teroristů nebo jiní odpůrci nějaké politiky a náhodné hackery bez politické motivace, kteří pouze vyhledávají vzrušení a věhlas ve své komunitě.

6.5.1.1 Teroristické skupiny

Není známo, zda mezinárodní teroristická organizace Al-Kajdá nebo jiné teroristické skupiny už vyvinuly kybernetické zbraně, ani jak jsou jejich schopnosti v této oblasti velké. Naproti tomu je jisté, že teroristické skupiny používají informační technologie a internet k plánování svých akcí, získávání peněžních prostředků, šíření propagandy a svých výhružek[40]. Odsouzený terorista, Ramzi Yousef, který byl odpovědný za plánování prvního bombového útoku na World Trade Center v roce 1993, měl ve svém laptopu v zašifrovaných souborech

[40] Viz např. únosy civilistů v Iráku.

uloženy plány dalších teroristických útoků, včetně plánovaných bombových útoků na 12 dopravních letadel v Pacifiku. Pozdější útoky na WTC a Pentagon 11. září 2001, stejně jako odhalení britských bezpečnostních sil, že IRA měla v plánu zničit elektrárny v okolí Londýna, dokazují touhu teroristů udeřit na kritická centra infrastruktury, na nichž moderní informační společnost závisí. Útoky na WTC si nevyžádaly jen ztráty na životech a majetku, ale také uzavřely burzy a zničily důležitou součást finanční infrastruktury New York City. Tento trend může být varovným signálem před hrozbou zneužití informačních technologií jako zbraně proti klíčovým centrům infrastruktury západní společnosti.

6.5.1.2 Nepřátelské národní státy

Některé země, zejména ty označované Spojenými státy za „osu zla"[41], by se mohly v budoucnu stát terčem amerických vojenských operací. O mnohých z těchto států je známo, že vyvíjejí kybernetické prostředky pro špionáž proti ostatním státům, průmyslu, nebo finanční sféře. Hovoří se rovněž o možném použití informatických zbraní proti USA a spojencům. Americký Defense Science Board odhaduje, že v budoucnu na Spojené státy zaútočí připravený protivník využívající široké spektrum kybernetických zbraní a technik. Mezi potenciálními protivníky spatřují zejména o Čínu, Severní Koreu, Kubu a Rusko, o kterých je známo, že takovéto technologie vyvíjejí [D02].

Informatický zbrojní potenciál je velmi oblíben, neboť asymetrické válečné strategie jsou jednou z mála možností, jak soupeřit s nepřítelem, který má totální převahu vojenské i ekonomické síly. Země s rozvinutými kybernetickými zbraněmi by jistě infoware použily v případě napadení ze strany koalice vedené USA. Navíc existuje možnost, že i státy, které by nebyly přímo zapojeny do odvetných akcí vůči USA, by mohly spustit útok kybernetickými zbraněmi vydávajíc se při tom za nějakou „teroristickou" zemi, neboť původce kybernetického útoku může za sebou zametat stopy a zanechávat falešná vodítka.

6.5.1.3 Sympatizanti teroristů a protiameričtí hackeři

Z historických trendů vyplývá, že kybernetické útoky sympatizantů teroristických skupin a lidí s protiamerickým popř. jiným „proti" zaujetím budou častější než útoky teroristů či nepřátelských států. Pokud bude blízký východ chápat americkou kampaň boje proti terorismu jako křížovou výpravu proti islámu, může zde vzniknout celá nová generace kyberteroristů. V tomto případě by mohly proslulé „promuslimské" hackerské skupiny jako „G-Force", „The Pakistan Hackerz Club" nebo „Doctor Nuke" využít své schopnosti proti Spojeným státům a jejich spojencům a zároveň vychovat zkušené následovníky.

Existují také reálné hrozby, že by se skupiny s jakýmkoliv zaujetím proti USA mohly spojit a vytvořit širokou nepřátelskou koalici zahrnující mezi jiným náboženské fanatiky, extrémistické skupiny, odpůrce americké podpory Izraele a čínské hackery. Antikapitalistické a antiglobalizační hnutí v minulých letech už využilo násilnou taktiku, aby ukázalo svůj odpor vůči hodnotám definujícím globální status quo. Po teroristických útocích 11. září je dokonce někteří z nich prohlašovali za spravedlivou odvetu americkému imperialismu. Tito extremisté a i umírnění podpůrci jejich hnutí by se mohli zapojit do kybernetické kampaně proti USA a jejich spojencům. Do této informační války by mohli přispět i čínští hackeři, kteří cítí, že mají s USA nevyrovnané účty. Navíc jsou někteří Číňané stále rozhořčeni neúmyslným bombardováním čínské ambasády v Bělehradě v roce 2000.

[41] Např. Sýrie, Írán, Súdán, Severní Korea apod. Americká administrativa tento seznam vždy upravuje na základě analýzy mezinárodní situace.

6.5.1.4 Vyhledavači vzrušení (thrill seekers)

Jakýkoliv konflikt odehrávající se v kyberprostoru přitahuje obrovské množství hackerů a zejména script kiddies, kteří se chtějí „přihřát polívčičku a proslavit se útokem na cíl vysoké důležitosti. Tato kategorie útočníků není vedena ani politickým ani ideologickým zápalem, nýbrž pouhou exhibicionistickou touhou. I když se jedná o poměrně velkou skupinu, která využívá vzniklý kyberkonflikt, její aktivity jsou relativně malou hrozbou pro počítačové systémy západních zemí. Úroveň propracovanosti jejich útoků je, v porovnání s jinými účastníky konfliktu, většinou velmi nízká, neboť používají zejména prefabrikované hackerské nástroje. Rovněž jejich motivace není tak vysoká a v případě, že se konflikt prodlužuje, ztrácí zájem. Naproti tomu pravděpodobnost útoku ze strany těchto skupin je extrémně vysoká díky mediální sledovanosti situace, což zvyšuje možnost „proslavit" se.

I když této kategorii útočníků nebyla přisouzena vysoká nebezpečnost, zůstává zde stále možnost, že díky nim bude odstaven z provozu nějaký kritický systém. Například přesto, že DDoS útoky proti prominentním webovým serverům jako CNN a Yahoo! a množství červů a virů v poslední době neukazují žádnou politickou nebo finanční motivaci, každý z těchto útoků má velký ekonomický dopad a může způsobit vážné škody.

6.5.2 Aktivity teroristů vůči informačním technologiím

Při pokusu o kategorizaci možných útoků proti informačním technologiím protistrany dojdeme k následujícím třem základním skupinám:

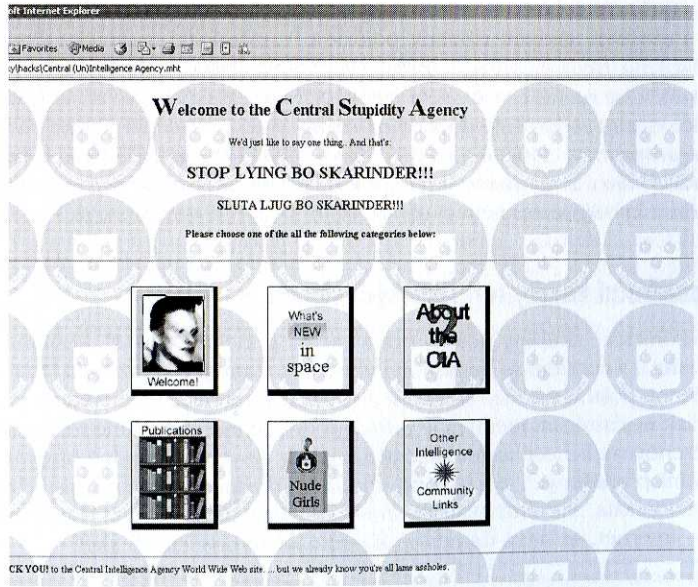
- ✓ Přímý útok na lokální technologii – druh útoku je závislý na povaze lokality a na významu umístěné technologie v celkovém rozměru cílové infrastruktury. Pomineme-li klasické fyzické útoky, pak nejjednodušším případem může např. sémantický útok, kdy defacement webových stránek se omezí na změnu jejich obsahu[42]. Útoky na infrastrukturu kritických systémů mohou ve svém konečném dopadu vést nejenom ke značným ekonomickým škodám, ale i ke ztrátám na životech.
- ✓ Souběžný útok, kdy v rámci fyzického útoku namířeného proti jinému cíli, je zasažena i informatická nebo telekomunikační infrastruktura. Takový případ většinou vede pouze k degradaci provozních parametrů zasažené komunikační infrastruktury a nemusí mít nutně fatální následky. Daleko významnější je ztráta dat, ke které dojde při fyzickém zničení nosičů informace, nebo zničení provozní technologie.
- ✓ Zneužití technologie k řízení teroristické organizace. Zejména globální charakter informatického a telekomunikačního prostředí umožňuje předávání informací a koordinaci teroristických aktivit na celém světě. Uvádí se, že např. útok na WTC v New Yorku byl organizován právě s využitím internetu[43].

Ve svých aktivitách jsou kyberteroristů vedeni podobnými cíli jako teroristé používající klasické prvky zastrašování. Kyberterorismus však zdůrazňuje některé specifické složky zejména v klasifikaci dopadu kybernetického útoku, kam mimo jiné patří:

- ✓ Okázalost útoku, kdy útočník způsobí škodu velkého rozsahu nebo dosáhne významné publicity. Např. útok typu DoS na známý internetový obchod způsobí sice škodu provozovateli, která je vyčíslitelná objemem možných realizovaných prodejů v době výpadku, ale daleko větší je škoda způsobená negativní publicitou plynoucí ze způsobené nedostupnosti nebo nespolehlivosti serveru.
- ✓ Faktor zranitelnosti, jenž patří mezi typické psychologické zbraně kyberterorismu. Útočník přitom demonstruje snadnou zranitelnost serveru protivníka ať už jednoduchým zahlcením záplavou zpráv – útok DoS, nebo defacementem serveru protivníka, kdy původní stránky jsou nahrazeny ideologickým materiálem protivníka nebo podvrženou verzí původní stránky.

Zejména defacement protivníkova serveru, používaný často kyberteroristickými skupinami jako psychologická zbraň může mít nejrůznější formy, např.:

- ✓ Náhrada loginové stránky vedoucí ke krádeži přihlašovacích údajů uživatelů umožní získat prostředky nebo informace pro další operace skupiny.
- ✓ Změny v provázání odkazů na stránky a URL mohou vést ke zmatení návštěvníka serveru.
- ✓ Změny na stránkách významných organizací nebo firem mohou vést k pocitu snižování jejich autority. Tyto změny mohou být založeny na náhradě celé stránky výsměšným textem nebo obrázkem, ale často spočívají pouze v nepatrné úpravě, které si pravidelný návštěvník nemusí ani všimnout. Např. změna akčních cen nebo drobná úprava názvu firmy jsou případy takových defacementů[44].



Obr. 6.11: *Populární defacement stránky agentury CIA provedený švédskými hackery 19. září 1996*

[42] Tato změna může být nápadná a např. zesměšňovat protivníka, prezentovat útočníkovu ideologii nebo jinak psychologicky působit. Může to však být i změna nepatrná, která změní pouze nějaké údaje na webových stránkách a takový defacement bude sloužit buď k získání důvěrných informací (defacement loginovací procedury) nebo ke zmatení protistrany (chybné pokyny uveřejňované na webových stránkách) – viz dále.

[43] Nemusí se však jednat jenom o internet. Právě v souvislosti s citovanou teroristickou akcí se uvádí, že nějakou dobu před útokem na WTC byl aktivován družicový komunikační systém Iridium, který byl pro malou ekonomickou návratnost již delší dobu mimo provoz. Přitom významný vlastnický podíl na tomto systému náleží osobám blízkým Al Kajdě.

[44] V počítačové komunitě se traduje změna loga na hlavním serveru CIA, která tam zůstala bez povšimnutí poměrně dlouho. Název „Central Intelligence Agency" byl změněn na „Central Stupidity Agency" [103]

Mezi metody používané kyberteroristy patří:

- ✓ Fyzické napadení, tedy neautorizovaný fyzický přístup do prostor vyhrazených pro provozní složky technologie nebo jejich části. Cílem útoku může být např. umístění odposlechového nebo podobného zařízení přímo v místě koncentrace technologie, kopírování dat přímo z nosičů nebo fotografování obsahu displeje. Není vyloučena ani fyzická destrukce zařízení nebo jeho odcizení.
- ✓ Spuštění útoku typu DoS nebo DoA či rozšířením maligního kódu (viry, červi), kdy většinou nejde o proniknutí do cílového systému, ale útok má spíše sloužit k degradaci jeho činnosti a znemožnění jeho řádného používání.
- ✓ Defacement webových stránek nebo jiný sémantický útok – útoky tohoto typu jsou nejnebezpečnější v případě, kdy podvržená stránka má stejný nebo téměř stejný vzhled jako původní stránky. Takový útok je obvykle určen k získání důvěrných údajů jako jsou přihlašovací údaje, čísla a piny kreditních karet, zdravotních informací apod.
- ✓ Útoky na klíčové uzly internetu. Zejména se jedná o útoky na jmenné doménové servery DNS. Překlad jmen na podvržené adresy a tím změněná místa určení zpráv nejenom, že způsobí zmatek v celé příslušné doméně, ale může sloužit i k získání datových toků od síťových uzlů, které by jinak byly nedosažitelné.
- ✓ Útoky na slabiny směrovacích protokolů, které mohou sloužit k odklonění datových toků od cílových uzlů nebo k jejich duplikaci a odklonu. Typickým cílem takového útoku je odposlech přenášených zpráv nebo podvržení či změna zprávy.

Významný aspektem kybernetického útoku je jeho asymetrie, kdy několik málo specialistů může s relativně malými náklady poškodit hospodářství technicky vyspělého státu natolik, že si jeho obnova může vyžádat roky. Skutečnost, že kybernetický útok může zasáhnout současně na řadě míst světa naráz, přírodní překážky a vzdálenost zde nehrají roli, a zapříčinit tak dalekosáhlé dopady na reálný svět, činí scénář kybernetického útoku přitažlivý nejen pro tzv. „zločinné státy" či teroristické skupiny, ale i pro osamoceně jednající vyděrače[45]. Provázanost moderní společnosti na informační systémy je tak vysoká, že bez ochrany kyberprostoru ztrácí efekt ostatní bezpečnostní strategie.

6.5.3 Komunikační kanály teroristických skupin

Přesto, že teroristické skupiny pracují isolovaně na principu „netvar", komunikaci s ostatními skupinami a s centrem se nemohou vyhnout. K tomu jim slouží celá řada prostředků, počínaje běžnou poštou a konče šifrovanou mobilní komunikací nebo satelitním systémem Iridium. Avšak nejčastějším médiem je pravděpodobně internet. Mimo to, že umožňuje téměř neomezenou rozličnost komunikačních technik, dovoluje i snadné šifrování, utajování nebo ukrývání přenášených zpráv a při vhodném postupu i obtížně zjistitelnou identitu odesilatele i adresáta. Všechny tyto vlastnosti nahrávají teroristickým skupinám, a tak kyberprostor – internet, se stává doménou koordinace teroristických akcí.

[45] Je třeba podotknout, že stále rostoucí propojenost světa a vzájemná závislost všech složek moderní civilizace, významně omezuje možnost kybernetických útoků, iniciovaných státy. I tzv. „zločinné státy" jsou do té míry zapojeny do globálních počítačových sítí, že kolaps světových finančních trhů, který by masový kybernetický útok patrně způsobil, by negativně dopadl i na ně. To však nemusí odradit nestátní aktéry, jako jsou nadnárodní teroristické skupiny. Jim mohou být výkyvy světové ekonomiky lhostejné, resp. s nimi mohou počítat ve svých plánech.

Kategorizovat techniky používané teroristickými skupinami pro komunikaci je obtížné, avšak jako jedny z nejoblíbenějších se jeví steganografické techniky ukrývání informace[46]. Je to zejména proto, že klasické šifrování sice zamezí zjištění obsahu zprávy, ale prozradí, že je zpráva šifrovaná, a tedy její obsah je přinejmenším „podezřelý". Steganografické techniky nejsou tak snadno identifikovatelné a hledání steganograficky zpracované zprávy je velmi obtížné.

Příkladem může být komunikace nejznámější teroristické skupiny Al-Kajdá. Pro přenosy informací o chystaných teroristických útocích byly používány obrázky na pornografických webech se stenograficky ukrytou informací a chatové místnosti zaměřené na sport nebo pornografii pro sdělování jednoduchých upozornění na nové zprávy[47]. Ve volných bitech formátu .jpg byly ukrývány nejenom texty, ale i plány cílových objektů, fotografie cílů nebo mapy. Steganografické metody se ukázaly jako velmi účinné při minimálních nákladech na jejich realizaci – celá řada programů je volně stažitelná z internetu nebo jsou k dispozici za minimální poplatky[48]. Steganografické programy mohou zakrýt nejenom textovou nebo grafickou informaci, ale mohou sloužit k přenosu i zvukového záznamu nebo videozáznamu. Stejně tak se nemusí orientovat pouze na formát .jpg, ale mohou používat volné bity ve formátech .gif , .mp3, .bmp. .wav apod.

Předmětem steganografické manipulace nemusí však vždy být dostupný soubor, ale může být použit přímo text elektronické zprávy. Např. program „Spam Mimic Encode" vytvoří z regulérní krátké zprávy jinou zprávu, nerozeznatelnou od spamu, a tak ji vlastně ukryje. Přijatá „spamová" zpráva je pak dekódována zpět programem „Spam Mimic Decode" do čitelné podoby[49].

6.5.4 Ideologické zneužívání kyberprostoru

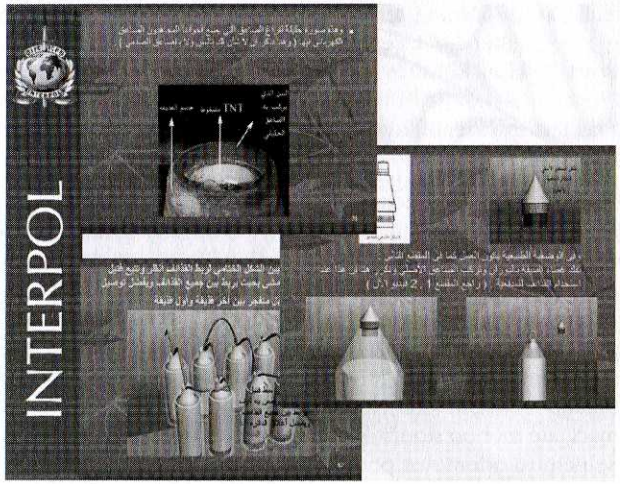
I když je tato kapitola věnována kyberterorismu, a tedy útokům proti infrastruktuře realizovaným prostředky informatického boje, není možno neuvést i další případy zneužití kyberprostoru pro šíření závadných informací nebo pro psychologické operace související s mediálním terorismem. Internet poskytuje zcela výjimečné možnosti extremistickým a teroristickým skupinám i jednotlivcům, a to zejména v oblasti rychlé a relativně utajené komunikace, kdy slouží ke vzájemné výměně informací a pokynů, k plánování a koordinaci akcí nebo převodu finančních prostředků. Podstatnou měrou se podílí na šíření propagandy, získávání a mobilizaci nových aktivistů, sympatizantů či sponzorů; obhajobě teroristických činů a podněcování jednotlivců k jejich páchání. Internetové servery teroristických skupin často obsahují návody na výrobu improvizovaných zbraní, viz obr. 6.12, nebo rafinovanou propagandu zacílenou na mladší generaci.

[46] Steganografické techniky staví na ukrývání informace v množství jiné nezávadné informace, nikoliv na jejím šifrování. Jejich první použití se datuje do starověkého Řecka, kde zpráva byla vytetována na vyholenou hlavu posla. Potom, co mu vlasy opět narostly, byl se zprávou, ukrytou v houštině vlasů, vyslán. Po vyholení byla zpráva opět čitelná. Mezi steganografické techniky se řadí i různé tajné inkousty, voskové tabulky apod.

[47] Tyto internetové komunikační kanály používané Al-Kajdá byly americké zpravodajské službě známy již na počátku roku 2001, tedy ještě před útokem na WTC.

[48] Např. „Hide and Seek", „StegoDos", „ White Noise Storm", „S-Tools" a další.

[49] Viz *http://www.spammimic.com/*.



Obr. 6.12: *Návody k výrobě bomby zveřejněné na serverech teroristické skupiny (zdroj Interpol)*

Obr. 6.13: *Komiks vybízející k zapojení do sebevražedných útoků v rámci palestinko-izraelského konfliktu*

Bezmála všechny teroristické skupiny a organizace provozují své internetové stránky. Obvykle jsou zveřejňovány v několika jazykových mutacích a nechybí ani speciální stránky zaměřené na děti a ženy obsahující pohádky či komiksy, do nichž jsou zapracovány příběhy sebevražedných atentátníků – viz obr. 6.13. Interaktivní způsob komunikace s teroristickou sítí, kdy obě strany zůstávají v anonymitě a nikdy se nesetkají vede k fenoménu, který se nazývá „samoradikalizace" a „samovýcvik". Osoby procházející tímto výcvikem působí izolovaně od ostatních teroristů, jednotlivců či malých skupin, plánují a připravují nebo provedou teroristický útok, aniž by se kdy přímo setkali s ideovými vůdci teroristické sítě, ke které se o své vůli hlásí[50].

Monitorování stránek těchto organizací policejními orgány a zpravodajskými službami je nesmírně nákladné. Není k dispozici dostatečný počtu analytiků, schopných alespoň rámcově monitorovat, natož hloubkově studovat, všechny existující stránky zejména v arabštině. I kdyby to bylo technicky snadné likvidovat tyto internetové stránky, bylo by to spíše kontraproduktivní, neboť zánik stránek na jednom serveru by vedl k jejich otevření na serveru jiném, který by se musel obtížně dohledávat. Monitorované stránky serverů teroristických skupin jsou na druhou stranu často zdrojem informací, užitečných i pro bezpečnostní složky a v případě jejich systematického odstraňování by teroristé mohli začít používat jiný, obtížněji monitorovatelný způsob komunikace.

[50] Za zatím patrně nejtěžší případ takového vývoje jsou označovány teroristické útoky, k nimž došlo v Londýně v červenci roku 2005.

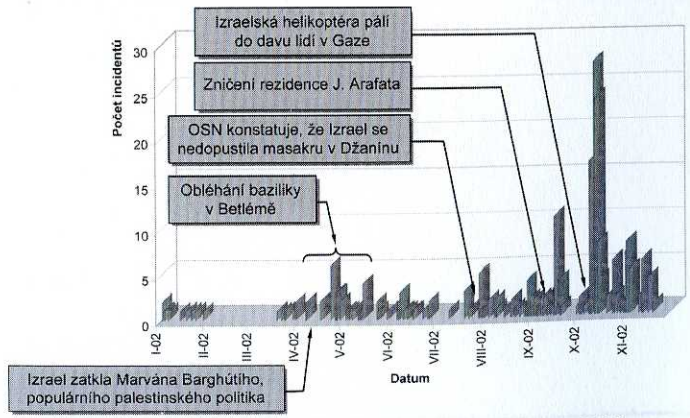
I když se ozývají názory, že teroristé dávají přednost vizuálním efektům, způsobeným například bombami a internet jim slouží spíše k propagandě a vzájemné komunikaci, nemusí to platit věčně. Kyberteroristický útok a likvidace určitého segmentu infrastruktury může být stejně tak efektním doprovodným jevem „klasického" teroristického útoku. V současné době se zejména objevují doprovodné jevy v kyberprostoru, které reagují na konkrétní akce stran zapojených do teroristického střetu.

Příkladem může být vývoj defacementů, které se poměrně dobře sledují, v oblasti palestinsko-izraelského konfliktu. Tato oblast tvoří ze studijního hlediska optimální prostředí, neboť je výrazně teritoriálně ohraničená, jak zeměpisně tak i kyberprostoru, a alespoň jedna strana sporu disponuje vysokým počtem serverů v samostatné doméně. Na obr. 6.14 je uvedena četnost defacementů serverů umístěných v izraelské doméně .il. Jak je vidět, četnost napadání těchto serverů koreluje s významnými událostmi na palestinsko-izraelské scéně a je možno tvrdit, že nárůst počtu napadení serverů izraelské strany je úměrný společenskému vnímání „hrůzy" iniciačního aktu. Pro úplnost zbývá doplnit, že všechny uvedené události byly doprovázeny i klasickými sebevražednými útoky palestinských teroristů na území Izraele [J04].

V širším pohledu je možno najít i jiné typy útoků než defacement, avšak ty se obtížněji prokazují. Můžeme nalézt např. významné zvýšení aktivity izraelských hackerů, kteří na únos tří izraelských vojáků 6. října 2000 odpověděli vytrvalými DDoS útoky na servery Palestinské samosprávy, Hamasu a Hizbaláhu. Propalestinské skupiny zase v odvetě napadaly servery izraelského parlamentu (Knesset), Ministerstva obrany, Ministerstva zahraničí, Izraelské centrální banky, burzy cenných papírů v Tel Avivu a dalších [I04].

Palestinské útoky, které byly označeny jako „kyber-džihád", využívaly strategii stupňované eskalace. Podle jedné ze zúčastněných skupin, „UNITY" bylo fázování útoků následující

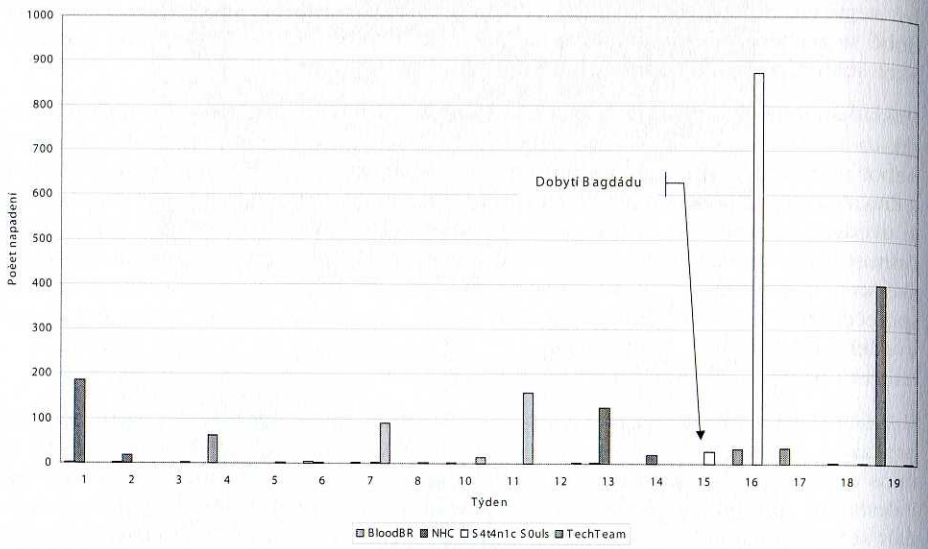
- ✓ Fáze 1 se zaměřuje na Izraelské vládní servery.
- ✓ Fáze 2 proti Izraelské ekonomické infrastruktuře jako Izraelská centrální banka.
- ✓ Fáze 3 zahrnuje útoky proti komunikační infrastruktuře, zejména proti hlavnímu izraelskému ISP NetVision.
- ✓ Fáze 4 útoky stupňuje a přidává útoky na zahraniční cíle.



Obr. 6.14: *Četnost napadení domény .il v roce 2002*

Podobné aktivity bylo možno sledovat v kyberprostoru i po dobu války v Iráku, i když v tomto případě bylo monitorování obtížnější. Problém spočíval zejména v tom, že na jedné straně byly síly aliance vedené USA a americké servery nejsou jednotně umístěny do domény .us, ale nalézají se zejména v generických doménách .com, .edu, .gov apod. Nicméně, jak ukazuje obr. 6.15, i zde bylo možno nalézt vzrůst aktivit v některých doménách, zejména po dobytí Bagdádu.

konec ma

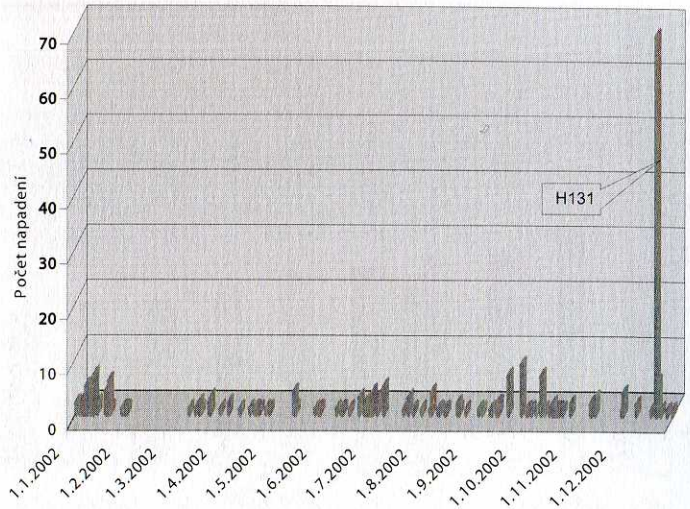


Obr. 6.15: *Vývoj četnosti napadání webových stránek během války v Iráku*

V obou výše uvedených případech byly stránky použité k defacementu zaměřeny ideologicky k pojednávanému tématu, tj. k palestinsko-izraelskému konfliktu nebo k válce v Iráku – viz defacementy uvedené dále.

Česká republika nepatří mezi země, jimž by se defacementy kyberteroristických skupin vyhýbaly. Doména .cz byla v nedávné minulosti vystavena celé řadě útoků, resp. výhrůžek takovými útoky, např. v souvislosti s pořádáním summitu Mezinárodního měnového fondu a Světové banky v roce 2000 a summitu Severoatlantické aliance v roce 2002. Zdokumentováno je napadení 61 českého serveru skupinou H131[51] na podzim 2002 po rozhodnutí českého parlamentu o vyslání jednotky armády České republiky do Afgánistánu.

[51] Deklaruje se jako pro-arabská hackerská skupina.

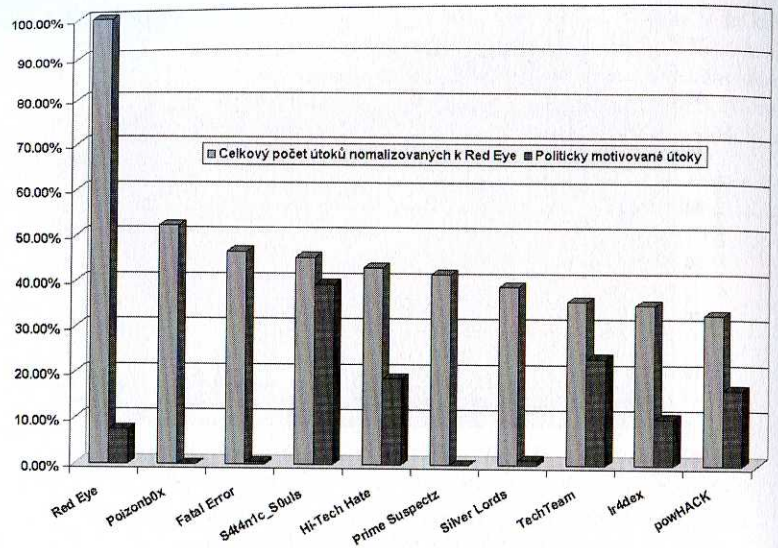


Obr. 6.16: *Napadení českých serverů po rozhodnutí parlamentu o vyslání českých jednotek do Afgánistánu*

6.5.4.1 Politicky motivované útoky hackerských skupin

Provedení informačního útoku na síť nebo server protivníka je věc technologicky nesmírně náročná, vyžadující podrobnou a dokonalou znalost technologií a programovacích technik. Z tohoto důvodu jsou často k ideologickému boji v kyberprostoru získáváni členové významných hackerských skupin, nejčastěji z proudu označovaného H4H. Účast hackerské skupiny v ideologickém boji může mít tři základní charakteristiky:

- ✓ člen hackerské skupiny je zároveň členem teroristické organizace,
- ✓ člen hackerské skupiny je příznivcem, vyznavačem nebo prostým sympatizantem s názorovým příklonem k ideologii hlásané příslušnou teroristickou skupinou,
- ✓ hackerská skupina nebo její část se dohodne se zástupci teroristické skupiny a následovně provádí napadaní serverů jako součást „obchodního případu" uzavřeného mezi těmito stranami.

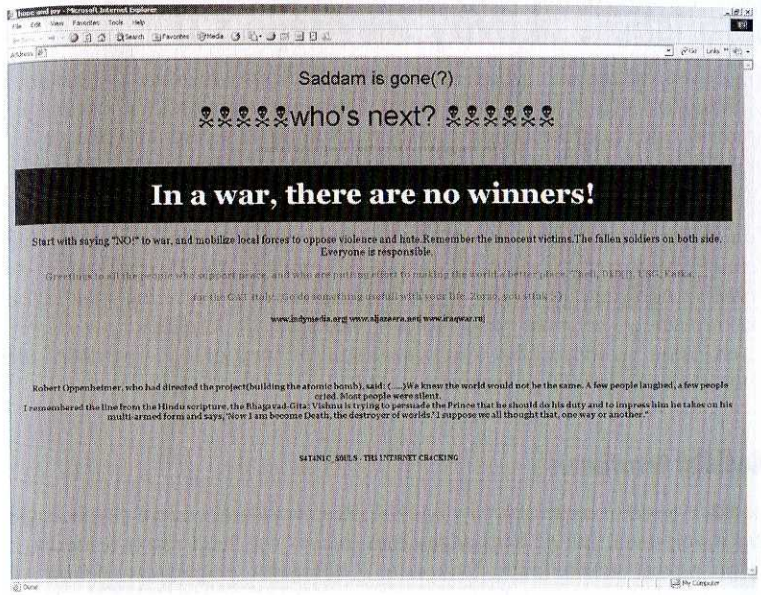


Obr. 6.17: *Politicky motivované útoky hackerských skupin*

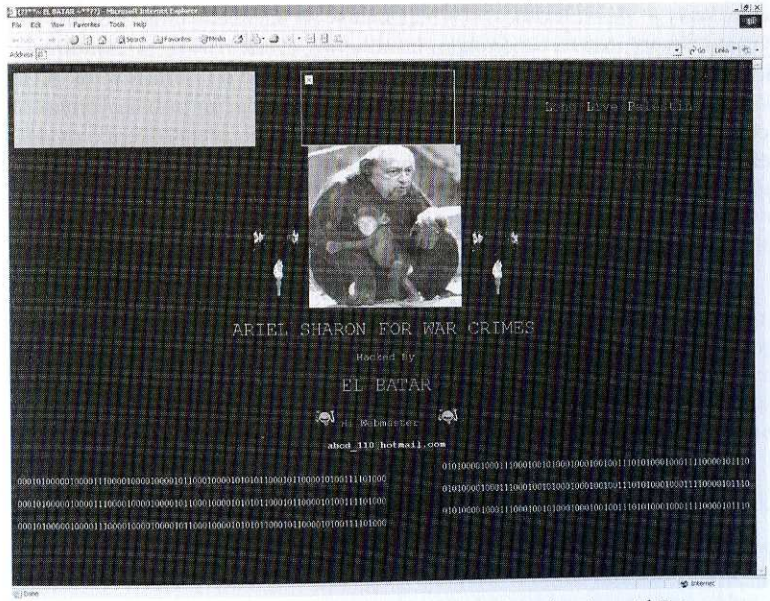
První dva případy vedou obvykle k samostatné činnosti jednotlivého hackera ve prospěch této teroristické skupiny a jeho aktivity nemusí být ani teroristické skupině nebo hackerské skupině známy. Třetí případ vede na běžné „obchodní" řešení a není výjimkou, že jedna hackerské skupina uzavře několik „kontraktů" s různými teroristickými skupinami.

Jak je uvedeno v [J04] řada předních hackerských skupin přiznává politicky motivované útoky (viz obr. 6.17), které slouží jedné nebo druhé straně střetu. Charakteristika těchto útoků je většinou na úrovni „psychologických operací", tedy defacementu prováděného na serverech protistrany. Úroveň zpracování stránky vložené na server protivníka se liší od jednoduchých graficky nebo textově provedených nápisů vyjadřujících nějaké stanovisko až po zdařile provedené dynamické webové prezentace. Příkladem prvního typu defacementu může být napadání britských serverů skupinou po skončení války v Iráku (viz obr. 6.18), druhý typ defacementu pochází od skupiny El Batar[52] a souvisí s napadáním serverů v doméně .il propalestinskými skupinami (viz obr. 6.19).

[52] Název skupiny je velmi příhodný, neboť v arabštině znamená totéž jako destruktor nebo ničitel.



Obr. 6.18: *Defacement použitý v souvislosti s válkou v Iráku (skupina S4T4N1C_S0ULS)*



Obr. 6.19: *Defacement používaný propalestinskou skupinou El Batar*

6.6 Teroristické aktivity související s IT

konecma

Rozvoj masových sdělovacích prostředků používající elektronická média doznal v poslední polovině minulého století nebývalých změn. Dostupnost prakticky libovolné informace, neuvažujeme-li o její faktické hodnotě, v kterémkoli místě a čase vzbudila ve společnosti ještě větší hlad po informacích, nicméně na druhou stranu paradoxně snížila práh citlivosti vůči nepravdivým informacím a dezinformacím.

Zneužívání elektronických informačních kanálů pro politické nebo komerční záměry následovaly velmi rychle i parciální skupiny prosazující singulární cíle. Pro marketing osobností[53], idejí[54] a návrhů není lepší mediální prostředí než internet nebo elektronické prostředky masové komunikace – televize nebo rádio. V následujících kapitolách uvedeme příklady tří typů „terorismu" souvisejícího s informačními technologiemi – mediální terorismus, procesní terorismus a tzv. IT governance.

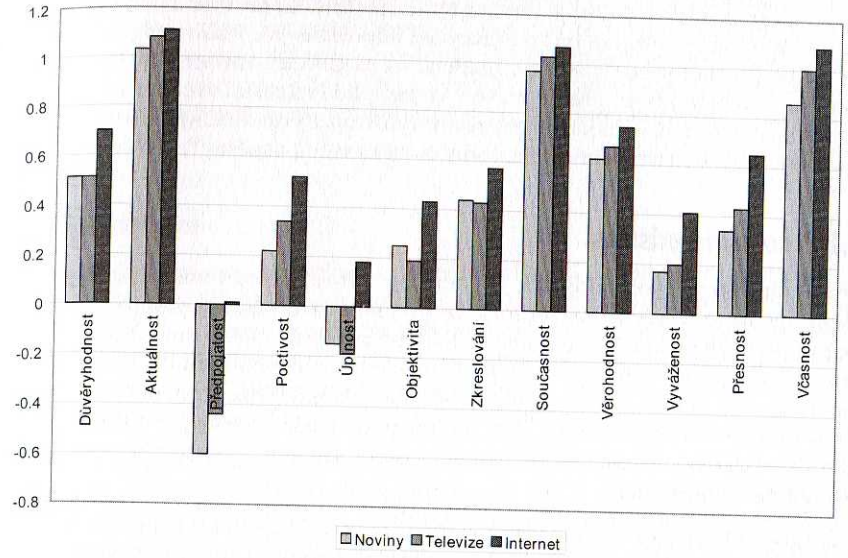
6.6.1 Mediální terorismus

Pojem mediální terorismus se objevil v souvislosti s metodami vedení psychologické války a mediální manipulací. Jak již sám název říká, hlavní roli hrají masová media, mezi něž internet i po právní stránce patří. Dokonce, v některých případech přebírá roli daleko významnější, než by mu příslušela. Je zajímavé, že důvěra v elektronická média je daleko vyšší než důvěra v média běžné – noviny, televizi nebo rozhlas (viz obr. 6.20), a to ve všech oblastech. Sociologové přikládají v tomto kontextu váhu zejména pocitu svobody vyjadřování, který je vlastní jedinci pohybujícímu se na internetu. Graf uvedený na obr. 6.20 dokazuje tuto skutečnost na americkém kontinentě, avšak rozložení jednotlivých skupin se nebude v Evropě příliš lišit. Zejména v postkomunistických zemích se dá předpokládat větší náchylnost věřit informacím na internetu než informacím publikovaným oficiálními sdělovacím prostředky. To zřejmě vyplývá ze zakořeněného přesvědčení o ovládání těchto typů sdělovacích prostředků vládnoucí stranou či opozicí[55].

[53] Pojem osobnost v českém slovníku díky mediálnímu zneužívání deklasoval stejně jako označení celebrita. Tyto termíny používané novináři k zesílení dojmu z vyprávění pak vyústí až k paradoxům jako např. označení „česká alkoholická celebrita", který byl použit v televizním dokumentu popisujícím chování a život alkoholika.

[54] Za typické se v této oblasti dá označit chování některých nevládních organizací, které Václav Klaus označil jako NGOismus. Rysy teroristického chování vykazují i některé ekologické skupiny označované podle toho za ekoteroristy.

[55] Je dlužno poznamenat, že média se ani nesnaží, aby tento názor byl změněn.



Obr. 6.20: *Důvěra občanů v různé typy médií*[56] *(zdroj dat School of Communication University of Miami, 2002)*

Vyjdeme-li ze známé skutečnosti, že touha novináře mít článek na první straně svého listu se po staletí nezměnila, pak mechanismy ovládání mediální sféry jsou nasnadě. Vyvoláním a postupným přiživováním afér a kauz, jejichž zázemí je mnohdy nepodstatné, mohou mediální magnáti odvrátit pozornost mas od skutečných problém, nebo jimi tyto problémy zakrýt[57].

Mezi základní metody zneužití kyberprostoru pro mediální terorismus patří

- ✓ Vydávání internetových novin a časopisů, které budou významnou část svého obsahu přebírat od svých „korektnějších" internetových kolegů, nicméně výběrem zpráv a vlastními příspěvky budou směřovat ke změně názoru svých čtenářů ve svůj prospěch
- ✓ Kybertronika – neboli zneužívání podprahového vnímání. V těchto případech je do souborů reklamních banerů na webech nebo „flash" prezentací zakomponován jeden obrázek s požadovanou zprávou, který je běžně neviditelný a je vnímán pouze podprahově[58]; např. do nevinné reklamy na výhody poskytované jistou cestovní kanceláří může být zakomponován jeden snímek s extrémistickým textem nebo grafikou.
- ✓ Haktivismus, provozování aktivistických stránek a serverů s touto tematikou.
- ✓ Aktivistický spam lze v některých případech zařadit rovněž mezi metody mediálního terorismu, neboť k rozšíření zprávy je použito veřejné médium, často jej zasílají různé aktivistické skupiny (ekologické, náboženské apod.) s cílem získat podporu pro svůj program ať už finanční nebo podpis pod případnou svoji proklamaci.

[56] Zdrojem dat je School of Communication University of Miami a data pocházejí z roku 2002.

[57] Je až s podivem jak velké pozornosti se dostává v české veřejnosti bulvárním novinám a časopisům a jak se vytrácí požadavek na korektnost klasického média.

[58] Obrázek může být buď dynamický, tzn. zjeví se pouze na nepatrný zlomek sekundy, který vědomě nestačíme rozpoznat, nebo zakomponován jako nevýrazný vzor do pokladové grafiky

Metody informačního boje a v jistém smyslu i „mediálního terorismu" jsou se vzrůstající frekvencí využívány nejenom pro mezinárodní terorismus, ale i jako prostředek dezinformační nebo psychologické operace zaměřené na modifikaci smýšlení širokých mas např. v kontextu volebního boje. Přitom právě v zemích, kde mediální výchova nebyla součástí základního vzdělávání, je mediální terorismu využívající jednoduchých metod působících na nejjednodušší behaviorální mechanismy člověka velmi úspěšný[59].

konec ma

6.6.2 Procesní terorismus

Procesní terorismus svoji podstatou by nemusel být označován ani za součást kyberterorismu, nicméně je zde zařazen proto, že podobně jako některé druhy kyberterorismu zneužívá prvky demokracie a je postaven na sebezničujícím efektu demokratického řešení sporů. Základem procesního terorismu je zneužití zákonných ustanovení nebo pravidel a soudní moci k vyvolání mnohdy až absurdního soudního řízení, které ve svém dopadu vede k omezení bezpečnostních prvků států pod rouškou odstraňování nezákonností. Často úzce souvisí s mediálním terorismem, neboť mnohdy je spojen se společenskými aférami nebo kampaněmi[60].

Aktéry procesního terorismu jsou většinou různé nevládní organizace a spolky, které spatřují v takovém konání zejména možnost získání mediální pozornosti nebo skupiny právníků, jimž procesní terorismus skýtá příležitost nejenom k získání popularity, ale i zvýšení jejich příjmů. Nastartované procesy se většinou falešně dovolávají lidských práv nebo jiných právních a morálních norem, které mají ve společnosti podporu a jsou chápány jako ohrožení každého občana. Přitom jejich pozadí může být politické nebo komerční a vlastní kauza je pouze prostředníkem k dosažení cíle[61].

Silná podpora konání takových organizací a spolků je zejména v zemích, které procházejí nebo prošly významnou společenskou změnou a kde je úloha bezpečnostních složek politizována[62]. Následky procesního terorismu se většinou projeví v soudním omezení některých činnost bezpečnostních nebo obdobných složek a následovně i v omezení bezpečnosti státu jako takového. Negativní roli v těchto případech hrají média, které takovým procesům dávají skandální nádech a vytvářejí atmosféru, která neprospívá korektním a objektivním rozhodnutím[63].

[59] Přímo klasickým případem je metoda odsouzení jedince do „méněcenné" skupiny těch, kteří nevědí co je správné jednoduchým a účinným heslem. Např. v padesátých letech minulého století bylo oblíbenou odsuzovací frází komunistů heslo „Kdo nejde s námi, jde proti nám". Často se do nesprávné skupiny zařazuje pomocí zjednodušeného odsudku např. „odmítají reformy", „nechápou potřeby společnosti" apod., aniž by cíle uvedené v heslech byly definovány. Jedinec se tak dostává pod psychologický nátlak vytvářející v něm pocit, že se sám ocitá na pokraji společnosti (mediální směr toku informací je jednosměrný, není možno s ním na stejné úrovni interagovat), a tak se snaží o přidružení k těm „správným směrům", aby se tohoto pocitu zbavil.

[60] Pokud jsou k dispozici dostatečné prostředky, je možno pro takovou kampaň najmout specializovanou agenturu, která je schopna např. i uspořádat demonstrace, připravit mediální podklady apod.

[61] Není žádným tajemstvím, že mnohé aféry související s „průnikem hackera" do bankovního systému jsou často vyvolány jinou komerční stranou v rámci konkurenčního boje. Scénář je přitom standardní a začíná nějakým poměrně nevýznamným útokem na bankovní systém (většinou napadení konta klienta banky, ale průnikem do jeho nechráněného počítače). Následuje medializace případu, který je jako „bankovní aféra" rozpitvávána médii. Po čase tato kampaň vyprchá, nicméně může značně poškodit cíl útoku – banku.

[62] Sem můžeme např. zařadit země s lokálními formami náboženského nebo politického terorismu (např. v Evropě Irsko) nebo některé postkomunistické země.

[63] Např. hrozba procesem s Českou republikou pro záznamy o telekomunikačním provozu, které podle § 97 zákona o elektronických komunikacích je povinna uchovávat právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací. Jedná se pouze o záznamy provozního charakteru a stejné ustanovení je ve všech telekomunikačních zákonech v Evropě. Soudním procesem hrozila na podzim 2006 organizace Iuridicum Remedium. Podobné procesy vyvolala v Irsku organizace Digital Rights Ireland.

Jiným případem je procesní terorismus vyvolaný se zřejmým ekonomickým cílem. Většinou se jedná o vyvolání řetězce soudních procesů, které jsou ze zákona financovány státem, nebo významného procesu, který je financován skrytou zájmovou skupinou[64]. Všechny procesy tohoto typu zatěžují soudní systém, vyvolávají negativní nálady obyvatelstva vůči jedné nebo druhé skupině sporu a v konečném dopadu mohou ohrozit i bezpečnostní mechanizmy státu.

6.6.3 IT governance

Vedoucí osobnost strategického výzkumu v Center for Digital Government[65] Paul Taylor zmiňuje ve svém článku [T04] obtíže, na něž ukazuje studie CIA zpracovaná pro americkou vládu. Tato studie se zabývala vlivem informačních technologií na vládní mechanismy a uváděla, že vlády obecně budou mít stále menší kontrolu nad tokem informací, technologií a finančních transakcí, ať už zákonných nebo nezákonných, které budou překračovat hranice států. Původní koncept vázající tyto toky na hranice států pravděpodobně vymizí.

I když původní studie byla směřována jiným směrem, je zřejmý stále vzrůstající vliv informačních technologií nejenom na vlastní technologické procesy, ale i na související rozhodovací procesy. Se stále zvyšující se závislostí na informačních technologiích vzrůstá tedy i vliv těch, kteří tyto technologie spravují a ovládají, na jim nadřízenou exekutivu. Postupný vznik „IT governance", čímž je označován stav, kdy fakticky dochází k nenásilné, ale výrazné dominanci firemních složek, odpovědných za správu a provoz informačních technologií, vede k nenápadnému ovlivňování rozhodnutí exekutivy. Požadavky, záměry a strategie IT součásti instituce začínají ovlivňovat i její původní zaměření. Firma se technologizuje, důraz na bezporuchový a vysoký výkon výpočetního systému se stává prvotním zájmem vedení firmy a i nesmyslné nebo nepodstatné požadavky útvarů IT jsou exekutivou plněny. A to zejména tehdy, když je vhodně vytvořena situace „ohrožení" důležité dodávky nebo nějaké podstatné funkce firmy.

Praxe rozeznává několik základních typů vztahů podle rozložení rozhodovacích práv ve firmě nebo podle možnosti ovlivnění rozhodnutí vztahujících se k IT:

- ✓ Obchodní monarchie – rozhodování spočívá na jednotlivci nebo skupině jednotlivců sestávající z managementu obchodních složek firmy. Může být prováděno formou kolektivních rozhodnutí nejvýše postavených pracovníků těchto složek s výkonnými pravomocemi. Exekutiva IT je z rozhodování vyloučena a v rámci svých pravomocí rozhoduje nezávisle.
- ✓ IT monarchie – rozhoduje jednotlivec nebo skupina jednotlivců z oblasti IT s příslušnými výkonnými pravomocemi.
- ✓ Feudalismus – rozhodovací proces je plně v rukou vedoucích pracovníků obchodních jednotek, držitelů rozhodovacích práv ke klíčovým procesům nebo jimi delegovaných zástupců.
- ✓ Duopolie – existují dvě poměrně nezávislé rozhodovací skupiny, jedna skupina IT exekutivy a další skupina formovaná z jiných součástí firmy.

[64] Do této skupiny patří např. aféra s emigraci Romů do Kanady, která údajně byla ekonomickou aktivitou kanadského právníka českého původu, jenž za zastupování těchto osob v imigračním řízení (i neúspěšném) byl odměňován kanadskou vládou. Jiným případem jsou např. tzv. ekologické procesy většinou financované konkurenčními skupinami v daném tržním segmentu (např. atomová vs. uhelně-energetická lobby).

[65] Center for Digital Government je národní výzkumná a poradenská instituce v USA, zaměřená na politiku nasazování a využívání informačních technologií. Jejími hlavními zákazníky je federální vláda a lokální vládní instituce.

- ✓ Federální uspořádání, kdy jsou pravomoci sdíleny po odborných liniích a v nejvyšším orgánu má každá tato odborná skupina svého zástupce s odpovídajícími pravomocemi.
- ✓ Anarchie – svědčí o totální ztrátě hierarchie ve firmě, a každý si dělá co chce.

Vztahy mezi jednotlivými typy organizace řízení a jejich souvislostí s vlivem IT útvarů zobrazuje tabulka 6.3 převzatá z [W08]. Je zřejmé, že uvedená taxonomie obsahuje i typy řízení ve kterých je evidentní převzetí exekutivních procesů nebo jejich významné ovlivnění managementem IT.

Typ rozhodování	Rozhodovací doména									
	Principy práce IT		Strategie infrastruktury IT		Architektura IT		Potřeba obchodních aplikací		Investování do IT	
	Podklady	Rozhodnutí	Podklady	Rozhodnutí	Podklady	Rozhodnutí	Podklady	Rozhodnutí	Podklady	Rozhodnutí
Obchodní monarchie	0	27	0	7	0	6	1	12	1	30
IT monarchie	1	18	10	59	20	73	0	8	0	9
Feudalismus	0	3	1	2	0	0	1	18	0	3
Federace	83	14	59	6	46	4	81	30	93	27
Duopolie	15	36	30	23	34	15	17	27	6	30
Anarchie	0	0	0	1	0	1	0	3	0	1

Tab. 6.3: *Rozdělení jednotlivých vlivů*

Vrátíme-li se k původnímu tématu, je nasnadě, že z hlediska použitých prostředků a metod se v případě jedná o neviditelný nátlak vyvolaný hrozbami, mnohdy nereálnými. Tento tlak je však velmi latentní a těžko se prokazuje zejména tehdy, když specializace firmy je značně vzdálena od prostředí výpočetní techniky. Složitost systémů IT umožňuje v podstatě vždy předložit materiál dostatečně fundovaně zdůvodňující proč se má udělat příslušné opatření, i když vlastní cíl tohoto opatření může být velmi vzdálen od předložené argumentace a navrhovaného opatření.

6.6.4 Trendy kyberterorismu

Výše uvedené případové studie ukazují přímou souvislost mezi politickými konflikty a kybernetickými útoky hackerských skupin. Dále je možno vysledovat, že tyto útoky mají konkrétní politické a ekonomické následky. V izraelsko-palestinském konfliktu kybernetické útoky bezprostředně souvisí s událostmi jako sebevražedné atentáty nebo minometné ostřelování.

Zvyšuje se také počet útoků souvisejících s politickým, náboženským nebo názorovým střetem, např. defacementy webových serverů v indické doméně vzrostl ze 45 na 250 za 3 roky[66] [G04]. Přibližně 1 200 amerických webových serverů, včetně těch patřících americké vládě, bylo zasaženo DDoS útoky nebo defacementem během jednoho týdne roku 2001 [W05]. Nárůst četnosti útoků byl spojen s nárůstem jejich propracovanosti a koordinovanosti. Srbští útočníci opakovaně narušovali komunikační infrastrukturu NATO během jugoslávské operace. Analýza cílů v kyberprostoru ukazuje na nová nebezpečí pro země, které dostatečně nezabezpečí svou informační infrastrukturu. Mezi nejhodnotnější elektronické cíle patří sítě, servery nebo směrovače, jejichž narušení má nejenom psychologické, ale i finanční, politické nebo strategické dopady. Informační systémy spojené s důležitou infrastrukturou musí být považovány za pravděpodobné cíle teroristů.

[66] Jedná se opět o typicky vymezenou oblast jak geograficky, tak v kyberprostoru a útoky jsou připisovány pákistánským hackerům.

Jedním z hlavních trendů kybernetických útoků, včetně těch bez zjevné politické motivace, je jejich stále vzrůstající složitost a propracovanost. Ať už motivováni finančně nebo pouze výzvou prolomení obrany informačních systémů, hackeři postupně zvyšují kvalitu svých útoků celé roky. Navíc široké a rychlé rozšiřování skriptů využívajících nové „exploity" umožňuje i neznalým script kiddies využívat různé pokročilé techniky, což se projevuje ve zvýšení počtu pokusů, i když nezdařilých. Mezi příklady možných cílů v budoucnosti mohou patřit

- ✓ Infrastruktura bankovních a finančních institucí; i když v tomto odvětví byly většinou provozovány hlavně privátní a podnikové sítě s omezeným vnějším přístupem, požadavek ceny za telekomunikační služby směřuje k výstavbě chráněných sítí uvnitř veřejné infrastruktury, což může snížit jejich bezpečnost.
- ✓ Hlasové komunikační služby; jejich zranitelnost je zejména ze strany zaměstnanců obeznámených s technickými detaily chráněného firemního software, kterým jsou tyto systémy řízeny[67]. Toto se týká rovněž tísňových linek a propojení integrovaného záchranného systému.
- ✓ Elektrická rozvodná síť obsahuje prvky, které technikům umožňují odstavit část sítě v případě přírodních katastrof; ty se však snadno mohou stát cílem pokusů o kybernetickou manipulaci projevující se jako výpadky energetické sítě.
- ✓ Infrastruktura ropného průmyslu je závislá na počítačových systémech dohledu a sběru dat a na správě energetických systémů. Zranitelnost těchto systémů vůči kybernetickým útokům může ovlivnit celou řadu dalších odvětví.
- ✓ Zdroje vody a samotná vodní díla, která jsou dálkově spravována pomocí senzorů a ovladačů, mohou být ze vzdáleného místa napadeny podobným způsobem jako rozvodné energetické sítě. Je tedy nutno dbát nejen na fyzickou bezpečnost, ale i na bezpečnost souvisejících informačních systémů.

Je zřejmé, že moderní společnost bude vystavována nebezpečí kyberteroristického útoku na své informační systémy stále častěji. Vzhledem ke stále se modernizujícímu arzenálu útočníků, jehož rozmanitost roste se zvyšujícím se počtem různých aplikací směřovaných do informatické oblasti bude boj s kybernetickým terorizmem a kriminalitou soupeřením bez viditelného konce.

[67] Nemusí to být nutně pouze hlasové služby, např. převážná většina výrobců směšovačů staví jejich bezpečnost na strategii utajování vnitřních mechanismů zařízení, tedy „security by obckurity".

7.

Kybernetické války a infoware

Jakkoli to zní tajemně, pojem kybernetické nebo informační války se zařadil do běžného slovníku vojenských stratégů. Termíny „information war", „cyber war", „information warfare" nebo „infoware" se objevily již v době studené války, která byla obrovskou příležitostí pro financování a rozvoj metod informačního boje, nicméně vážnosti se jim dostalo až s prudkým rozvojem komunikačních a informačních technologií na konci minulého století. V literatuře se termín „informační válka" poprvé objevil pravděpodobně v roce 1976 ve studii „Weapons Systems and Information War" [R06], kterou zpracoval Thomas P. Rona pro firmu Boeing Corporation[1]. Informační válka je v této studii definována jako „boj rozhodovacích systémů". V širším významu lze informační válku chápat jako součást státní politiky, která usiluje o dosažení národních zájmů s minimálním použitím tradiční vojenské síly. V tomto smyslu informační válka představuje „politickou válku", v níž použité zbraně nejsou sice viditelné a zřejmé, zato jsou však velice konkrétní ve svých účincích [N06].

[1] V současné době se tomuto tématu významně věnuje Bruce Berkowitz z Hoover Institution při Stanfordské Univerzitě, který rovněž pracuje pro RAND Corporation, např. [B15] .

konecma

Kybernetické války lze definovat jako aktivity vedené nebo koordinované státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka. Její součást, informační válku, je ale také možno chápat i jako válku o informace, jako boj, který svádějí lidé pracující s informacemi, případně střet, kde hlavní zbraní je právě informace.

Řada států dnes intenzivně pracuje na konceptu informační války. V případě tzv. zločinných států přitom hraje klíčovou roli zjištění, že jejich síly by jen stěží mohly uspět ve standardním vojenském střetu s nejvyspělejšími státy světa. Proto zaměřují své strategické aktivity směrem k možnostem boje v kyberprostoru. Informační válka je boj velmi specifický a ve svém základě personálně a materiálně relativně nenáročný. Často se vyzdvihuje její asymetrická povaha, kdy nezjištěný[2] nebo překvapivý útok, může podkopat obranyschopnost o poznání silnějšího a „bohatšího" protivníka a způsobit škody mnohonásobně větší než byly náklady na jeho provedení.

Kybernetické střety sebou také nesou nový název válečného arzenálu – infoware. Pod tímto termínem se rozumí souhrn všech bojových prostředků zaměřených na zničení informační nebo elektronické infrastruktury protivníka a informatických prostředků k vedení elektronického boje. Následující kapitoly se mnohdy budou těmto prostředkům věnovat.

7.1 Metody informačního boje a jejich účinky

Senzace chtiví žurnalisté, autoři thrillerů a dobrodružných románů ba i malíři komiksů nám již několik let nabízí představu hackerů, kteří shazují letadla, převádějí na svá konta miliardy dolarů, hrozí vypuštěním jaderné rakety a během přestávky se odpočinkově napojují na vojenské pozorovací družice. Realita se však zdá být jiná a nikoliv tak dobrodružná.

Navzdory romantickým představám romanopisců není infoware nic víc, než prostředek k ovlivnění virtuálních cílů. Jeho schopnost ovlivnit dění mimo síť je velmi omezená, neboť na něj mohou působit pouze nepřímo. To však ani zdaleka neznamená, že by aktivity infoware v informačním systému byly neškodné, neboť společnost používá počítačové systémy k zajištění mnohých ze svých bytostně důležitých funkcí. A právě prostřednictvím infoware mohou být tyto funkce ochromeny nebo přinejmenším narušeny.

Příkladem takového systému zranitelného prostřednictvím sítě jsou telekomunikace, kde ekonomické škody, způsobené rozsáhlejším výpadkem komunikačních sítí mohou být nesmírné nehledě na to, že jejich výpadek ovlivnil koordinaci např. lékařské pohotovosti nebo hasičů. To samozřejmě významně sníží schopnost společnosti účinně reagovat např. na přírodní katastrofu nebo teroristický útok. Součástí telekomunikační sítě je i internet, i když k útokům na klíčová zařízení, zejména TLD servery, příliš často nedochází – hackeři by si totiž tímto útokem zlikvidovali svůj „životní prostor" a tedy i „bojiště". Nicméně tato hrozba je reálná v kritické situaci a za využití již známých metod infoware.

Obdobně zranitelné mohou být prostřednictvím telekomunikačních připojení i informační systémy sloužící k řízení inženýrských sítí, jako elektrárny nebo vodárny. I když zatím neexistují v otevřených zdrojích potvrzené významné případy útoku proti takovým systémům, byl medializován případ, kdy nespokojený bývalý zaměstnanec vodárenské společnosti zneužil své znalosti systému a síťovým útokem způsobil vypuštění přehrady. Při této příležitosti je nutno dodat: bez specifických znalostí takového systému není podobný útok nejenom možný, ale ani pravděpodobný.

[2] Vojenská operace v kyberprostoru zpravidla nestojí o publicitu, zprávy o takovém útoku se dostávají na veřejnost pouze v případě absolutní nezbytnosti. Obvykle jsou zřejmé pouze vnější důsledky, avšak příčina je skryta nebo neodhalena.

Jedním z nejčastějších cílů, který může být a bývá napadán jsou banky. Jejich informační systémy jsou velmi rozsáhlé a většina z nich dnes umožňuje vzdálený přístup přes internet. I když hodnověrnost banky je jejím „zbožím" a ve svých marketingových materiálech vždy velice zdůrazňují jak dbají na bezpečnost, průzkumy ukazují na některé nedostatky [B16]. Navíc, banky v obavě ze ztráty klientů často podobné incidenty spíše utají, nebo dokonce přistoupí na podmínky útočníků nebo kybernetických vyděračů.

Konkrétní slabina bankovních systémů spíše spočívá v počtu připojovaných laických klientů na jejich informační systém. Většina útoků, které jsou publikovány v tisku má právě takovou příčinu – napadení počítače klienta banky a zneužití jeho přístupových práv. Jiným případem je medializace nějakého nepodstatného bezpečnostního incidentu konkurencí; ta je téměř častější než skutečně podniknutý útok.

Všechny výše zmíněné slabiny představují civilní cíle útoku, které mohou být zasaženy infoware. Takové útoky většinou nazýváme „útoky na infrastrukturu" a ty nemusí nutně spočívat v jejím narušení, ale např. ve zneužití pro změny důležitých informací, které následně vedou k nesprávným krokům. Rozsáhlý útok tohoto druhu by mohl významně ovlivnit i vojenské operace.

Využití infoware přímo v ozbrojeném střetu je rovněž možné. I když zřejmě nepůjde o hacking řízených střel nebo ovlivňování palubních systémů letadel, např. zanesení viru do palubní sítě letadlové lodě není nereálné. Mimo klasických zpravodajských technik či dezinformace může být infoware použito např. k narušování podpůrných struktur; kompromitací systémů zajišťujících zásobování úzce spolupracujících s civilními systémy a dalším přímým či latentním aktivitám. Přitom třeba zanesení viru do významné řídící vojenské sítě nemusí být ani takový problém – např. americká letadlová loď USS Carl Vinson[3] měla na své palubě na konci 90. let instalovánu síť LAN založenou na technologii Windows NT, sloužící k řízení chodu celé lodi [M06][4]. Lehkost, s jakou je možno do takové sítě zanést vir, je všeobecně známa.

7.2 Informační válka

Informační válka používá zbraně podobné kriminálním aktivitám na internetu, avšak je nutno odlišit informační válku od počítačové kriminality. Jakákoli nelegální operace jednotlivce nebo skupiny v kyberprostoru, která vede k porušení zákona patří do oblasti počítačové kriminality. Může se jednat o náhodné nebo plánované aktivity, individuální útok nebo útok, který je součástí plánu nějaké skupiny. Vedení informační války nikdy nebývá náhodným procesem odděleným od ostatního dění a předpokládá koordinovanou činnost mnoha složek při použití informace jako zbraně informační války na dvou úrovních – státní a vojenské.

Nejvýraznější vlastností prostředků informační války – infoware, je jejich dosah, resp. potenciální schopnost útočníka na kterémkoli místě planety, kde existuje připojení k síti, napadnout cíl na jiném, libovolně vzdáleném místě. Navíc, prostředky věnované na spuštění a přípravu informatické zbraně jsou ve srovnání s potenciálními škodami, které by mohla napáchat, zanedbatelné. A tak potenciální konflikt je výrazně asymetrický. Útočník vystačí s minimálním vybavením, zatímco jakékoli ochranné kroky je třeba provádět plošně a ve velkém rozsahu, což vede k nesrovnatelně vyšším nákladům na obranu.

[3] USS Carl Vinson je nukleární letadlová loď s výtlakem 95 000 tun, která nese na své palubě 80 letadel a její obsluha čítá na 6 000 námořníků.

[4] Mimo jiné – tento údaj zjištěný z otevřených zdrojů je viditelným důkazem, jak může uniknout podstatná informace jenom díky snaze marketingu zviditelnit produkt firmy.

konecma

Obrana před informatickým útokem je i tak problematická. Jednak je obtížné útočníkovi zabránit v dalších akcích a jednak pozice útočníka nemusí být na území napadeného, což omezuje běžné prostředky obrany. Rovněž se ztrácí klasické rozdělení cílů na „frontové" a „týlové"; všechny cíle jsou stejně přístupné a všechny je potřeba adekvátně bránit. V tomto smyslu mizí i rozdíly mezi civilními a vojenskými cíli a tradičně civilní cíle na domácím území mohou být napadeny daleko snadněji než vojenské.

To co patří mezi nejnebezpečnější charakteristiky informační války, je čím dál tím větší závislost vojenských informačních struktur na civilních – armádní systémy používají stejný hardware a software jako je používán v civilním sektoru. Uvědomíme-li si, že současný komerční software, např. operační systémy, je svým rozsahem i architekturou takový, že jeho přesné vlastnosti jsou téměř neověřitelné a v mnoha případech i neznámé, potenciální riziko kompromitace civilních a vojenských cílů je téměř srovnatelná.

Mezi poslední typické charakteristiky je setření ostrého časového ohraničení konfliktu, vedeného informatickými prostředky, a relativně snadná dostupnost prostředků infoware. Převážnou většinu infoware tvoří software, a tak není žádný problém tyto prostředky sdílet v libovolně velké skupině, teritoriální vzdálenost nehraje roli a je velice obtížné šíření prostředků infoware kontrolovat.

Cílem informační války je oslabení pozice jiných států, podvrácení jejich státních základů a narušení státního zřízení pomocí informačního působení na politickou, diplomatickou, ekonomickou a sociální sféru společenského života prováděním psychologických operací a jiných demoralizujících a rozvracejících aktivit v kyberprostoru. Na vojenské úrovni jsou informační operace soustavou opatření, které se provádí v rozsahu vojenské moci státu podle rozhodnutí vojenských velení a jako součást strategických vojenských operací. Informační operace jsou zaměřeny na dosažení informační superiority a na obranu svých informačních systémů. Důležitým rysem informační války je, že mohou být použity jakékoliv vojenské a technické prostředky, které jsou k dispozici, ale zároveň musí být dodrženy formální, právní, morální, diplomatické, politické a vojenské normy. Jedním z důležitých úkolů informačních operací vojenských sil je působení na nepřítele v době, kdy teprve vzniká nebezpečí vypuknutí války, aby ovlivnily pro sebe příznivým způsobem rozhodování nepřítele. Je zřejmé, že významnou úlohu v těchto operacích zastávají zpravodajské služby.

Informační válka se obvykle dělí do sedmi odděleně definovaných skupin, ale jejich oddělené použití nepřinese takové výsledky, jako když jsou vhodně kombinovány. Dělení do skupin se označuje anglickými názvy příslušného infoware a je následující:

- ✓ Command-and-Control Warfare (C2W) – prostředky a válečná oblast zaměřená proti řídícím a velitelským centrům protivníka včetně komunikačních kanálů.
- ✓ Zpravodajský (Intelligence) Warfare (IW) – prostředky skutečné informační války založené na syntéze a analýze informací, zde je hlavní úloha zpravodajských služeb.
- ✓ Elektronický Warfare (EW) – elektronické zbraňové systémy zahrnující nejrůznější prostředky elektronické povahy, např. elektromagnetická děla nebo grafitové bomby, některé publikace zahrnují do této oblasti i kryptografické techniky [L01].
- ✓ Psychologický Warfare (PW) – psychologická metody manipulace veřejného mínění, mediální terorismus a ostatní metody psychologické války.
- ✓ Hacker Warfare (HW) – metody a prostředky pro vojenské operace vedené hackerskými nástroji a postupy proti serverům a informatické infrastruktuře protivníka.
- ✓ Ekonomický Informační Warfare (EIW) – ekonomické prostředky ovlivňující potenciál protivníka v ekonomické oblasti, vychází se z ekonomické hodnoty informace získané prostřednictvím IW.
- ✓ Cyber Warfare (CW) – prostředky pro vedení kybernetické války; Libicky do této skupiny zahrnuje nejrůznější prostředky neuvedené v předcházejících skupinách, jež umožňují futuristické scénáře budoucích válek na úrovni kyborgů v science fiction.

7.3 Command-and-Control Warfare

Jak uvádí americké ministerstvo obrany „C2W je vojenskou strategií implementující informační válku na bitevním poli jejíž součástí je fyzické zničení". Jedná se tedy o souhrn strategií informační války implementovaný ostatními prostředky informační války – elektronickými, zpravodajskými, kybernetickými a ekonomickými[5].

Hlavní úlohou tohoto prostředku je oddělení nepřátelského velení od výkonných složek – vojska [D03]. Oddělení velení od výkonných složek je strategický postup používaný v armádách odpradávna. Ve středověku vedla ztráta velitele ve většině případů k neúspěchu celé vojenské akce. V průběhu vývoje válečné teorie a válečného umění stoupal význam a role vojevůdce, což vedlo ke vzniku instituce tzv. „generálního štábu" – orgánu zodpovědného za plánování, organizování a kontrolu válečných operací. Postupně se tedy strategie oddělení velení rozšířila na zničení celé velitelské skupiny – generálního štábu. Podle Martina Libického ztráta velení armády v moderní době může být také rozhodující pro vyhrání války, zvlášť pokud k tomu dojde ve správnou dobu. Pro provedení této operace není nezbytné použití střelných zbraní, ale postačí použít prostředky působící v informační oblasti – počítačové viry, elektromagnetické zbraňové systémy nebo triviální přerušení dodávek elektrického proudu [L01]. Použití těchto prostředků se hodně zjednodušuje faktem, že pro úspěšně provedený útok ani nemusíme mít přesnou informaci o umístění štábu nepřítele.

Existují i situace, kdy ke zneškodnění nepřítele je postačující zničení jedné osoby – vůdce organizace, strany nebo státu. Podle RAND Corporation existují tři základní typy operací pro odstranění vůdce:

- ✓ operace zaměřená konkrétně proti osobě vůdce,
- ✓ operace zaměřené na iniciativu a přispívání k sesazení vůdce pomocí vyvolávání vnitřních spiknutí a vzpour,
- ✓ operace přispívající k sesazení vůdce pomocí vnější vojenské invaze.

Systém řízení a velení byl a bude nejdůležitějším aspektem armádních operací a pochopitelně největší pozornost a investice budou věnovány vývoji technologií pro tyto systémy a jejich ochranu. V již zmiňované publikaci [L01] její autor uvádí, že „v budoucnu by bylo velmi omezené stavět válečnou strategii na předpokladu, že systém řízení a velení může byt vyřazen z provozu". Mnohem efektivnějším způsobem je přerušení komunikačního spojení mezi vedením a výkonným systémem. Právě význam přerušení komunikačního kanálu vzrůstá s vývojem elektronických telekomunikačních prostředků stejně jako zařízení určených k narušení funkce komunikačního systému nepřítele. Současně však existuje nebezpečí použití podobných informačních prostředků nepřítelem, a tak hrozba nepřátelského útoku na řídící systémy vede decentralizaci systému řízení armády, vytváření náhradních sítí, používání speciálních prostředků k obraně informací a vývoji nových technologií.

[5] Někdy je možno najít i označení C4I – Command, Control, Communication, Computer, Information Warfare.

7.4 Zpravodajský warfare

Zpravodajské prostředky v kyberprostoru jsou ve svém principu senzory umístěné v komunikačních kanálech. Na rozdíl od jiných druhů infoware, které jsou určené k poškození informačních technologií, se zpravodajský infoware zaměřuje návrh, ochranu a nebo potlačení systémů, které jsou zaměřeny na vyhledávání informací, které by mohly vést k ovládnutí „bitevního pole". Pod slovem senzor si můžeme představit nejenom známé „štěnice", ale i velmi komplexní systémy schopné např. napojení na systém řízení palby v reálném čase či zpracovat analýzu rozložení bitevního pole a odeslat výsledky bojovým jednotkám.

Cílem zpravodajských prostředků je tedy nejenom získání informací nezbytných pro vedení vojenských operací, ale analýza situace a dezinformace nepřítele. Snad nejlépe vystihl tento cíl Mao TseTung: „Abychom dosáhli vítězství, musíme udělat všechno pro to, abychom zapečetili oči a uši našich nepřátel, učinili je němými a hluchými, vytvořili zmatek v hlavách nepřátelských velitelů a přivedli je do blázince." [M04]. Můžeme tedy rozdělit prostředky IW na prostředky útočné a prostředky obranné.

7.4.1 Útočné prostředky infoware

Prostředky zpravodajské války patřící do oblasti infoware zpravidla vytvářejí rozsáhlé distribuované systémy, umožňující syntézu informací z mnoha kanálů. Pro představu o využití těchto senzorů je můžeme rozdělit do čtyř kategorií:

- ✓ vzdálené senzory, kam můžeme zahrnout kosmické stanice, satelity se speciálním posláním, ale i seismické senzory nebo speciální akustické senzory,
- ✓ blízké senzory jsou většinou prostředky umožňující navádění a ovládání, jako například bezpilotní letecké nosiče (UMA, UAV[6]) vybavené speciálními přehledovými technologiemi nebo podobně vybavené námořní bóje apod.,
- ✓ místní senzory, většinou jednodušší zařízení pro detekci nejrůznějších zněm okolí - akustické, gravimetrické, biochemické, optické apod.,
- ✓ zbraňové senzory umístěné přínos na příslušném bojovém prostředku nebo tvořící jeho součást – např. infračervený radar apod.

V současné době není problémem zpravodajských prostředků infoware způsob získaní dat, ale problém co nejefektivnějšího zpracovávání načtených dat. Přitom takové systémy musí pracovat nejen efektivně, ale i co nejrychleji a nejspolehlivěji.

7.4.2 Obranné prostředky infoware

Tyto prostředky většinou slouží k ochraně „senzorů". Základem řešení je znemožnit protivníkovi změnu v architektuře senzoru, zjištění jeho funkce nebo, což je nejhorší případ, jeho zneužití ke klamání protistrany. Obrané metody můžeme rozdělit do tří skupin:

- ✓ Fyzické zničení senzoru v okamžiku napadení nebo odhalení.
- ✓ Vyřazení systémů, které senzor používá, z provozu, což je vlastně obdoba předchozího řešení s menším ekonomickým dopadem.
- ✓ Tradiční utajování nebo klamání při umisťování senzorů – jejich umístění do oblastí s vysokým stupněm rušivých elementů, které zmatou případné hledače těchto prostředků. Populární jsou rovněž falešné cíle nebo nástražné systémy, které se chovají podobně nebo vypadají stejně jako aktivní senzor, ale slouží pouze ke zmatení nepřítele, jenž odhalováním a zkoumáním nástrahy jenom ztrácí čas.

[6] UMA – UnManned Aircraft, UVA – Unmanned Air Vehicle.

7.5 Elektronický warfare

Největší rozvoj v oblasti elektronických vojenských prostředků proběhl v době studené války, kde právě elektronické prostředky hrály jednu z hlavních rolí. S vývojem na obou stranách se však možnost využití elektronických metod stále komplikovala, neboť protivník nezahálel a neustále vylepšoval ochranu a přizpůsoboval ji možnostem elektronického warfare.

Elektronický warfare zahrnuje metody, zaměřené na oblast elektronického spektra a využívající toto spektrum pro bojovou nebo zpravodajskou činnost. V zásadě lze rozdělit elektronický warfare na radioelektronický warfare a kryptografický warfare. Zatímco radioelektronický warfare je zaměřen na fyzickou podstatu přenosu informací, kryptografický warfare je orientován na jeho logickou podstatu.

7.5.1 Radioelektronický warfare

Radioelektronické prostředky infoware je možno rozdělit podle jejich funkce na prostředky:

- ✓ elektronického rušení, které představují ofenzivní aktivitu s cílem celkové neutralizace nebo omezení možnosti efektivního využití radioelektrických systémů během vojenských operací,
- ✓ elektronické obrany, kam patří zejména aktivity spojené s obranou vlastních radioelektrických prostředků před rušením,
- ✓ elektronického zabezpečení, zahrnující aktivity spojené s detekcí, identifikací a určením polohy elektronických prostředků nepřítele, které mohou být zdrojem průzkumného nebo informačního nebezpečí.

V současné době se většina elektronického warfare zabývá rušením radarových systémů, nebo naopak jejich ochranou před rušením a odhalením. K tomu mohou být použity i prostředky fyzické destrukce, které obsahují směrově citlivé senzory v oblasti kmitočtů vysílaných radarem. Dalším cílem EW je rušení komunikačních kanálů protivníka popř. jejich odposlech, dekódování a dešifrování přenášených zpráv. Snad právě proto jsou do této oblasti zahrnuty i metody kryptografie.

7.5.2 Kryptografický warfare

Populární kryptografický stroj Enigma, který za druhé světové války umožňoval německé armádě poměrně dlouho utajovat zprávy přenášené rádiem, je velmi nedokonalým předchůdcem dnešních kryptografických systémů založených na matematických metodách, jejichž zdolání je obtížné. Možnosti, které přenesla výpočetní technika do kryptografie se projevily nejenom ve vojenství, ale zhruba od 70. let i v ochraně komerčních systémů a informací. V roce 1978 byl v USA uveřejněn šifrovací standard DES, což je symetrický šifrovací algoritmus, kde pro šifrování a dešifrování je použit stejný klíč. Právě v tom spočívá jeho slabina, neboť je vyžadován velmi bezpečný kanál pro přenos šifrovacího

klíče. Zaručit požadovanou bezpečnost přenosové cesty klíče není snadné, a proto se jedná o nahrazení tohoto standardu novým šifrovacím algoritmem AES[7].

konecma

Asi ve stejnou dobu vznikl Diffie-Hellmanův algoritmus, který je založen na asymetrické metodě, a je znám jako metoda s veřejným klíčem. Pro šifrování se používá dvojice klíčů, kdy dešifrování zprávy je možné jen pomocí páru klíčů, z nichž jeden může být veřejný. Jiný asymetrický šifrovací algoritmus je např. RSA, který byl připraven autory Rivestem, Shamirem a Adlemanem a je poměrně často používán i v dnešní době. Velmi zjednodušeně řečeno, text zprávy se v tomto případě kóduje pomocí přirozených čísel a samotné šifrování je prováděno umocňováním čísla reprezentujícího tento text.

Kryptografie hraje významnou roli v elektronické válce a může být použita jak v obranných systémech, kde se používá k zabezpečení přenosu dat veřejným komunikačním kanálem, tak i při „útočných" akcích, kde její hlavní úloha spočívá v dešifrování zpráv, které mohou přinést užitečnou informaci o cílech protivníka.

7.6 Psychologický warfare

Psychologická válka patří k nejstaršímu druhu informační války a je používána již odpradávna. Její podstatou jsou metody nenápadného a postupného vkládání myšlenek, názorů nebo přesvědčení do podvědomí nepřítele s cílem ovlivnit jeho rozhodování ve svůj prospěch. Často kombinuje s fyzickými válečnými operacemi s cílem snížit morálky nepřítele.

Pojem „psychologická válka" se v širším slova smyslu sjednocuje s válkou v ideologické oblasti, tedy vlivem propagace a mediálního tlaku na ideologickou a emocionální stránku jedinců. Právě v tomto významu se psychologická válka nejčastěji chápe jako součást informační války. V užší pojetí se dá na psychologickou válku nahlížet jako na všestranný vliv na masovou psychologii. V obou případech se metody psychologické války nemusí omezit jenom na nepřítele, ale mohou sloužit i jako pozitivní „nástroj" pro zvýšení morálky ve vlastních řadách.

Psychologická válka je velmi důležitou součástí informační války neboť moderní válečné strategie posunují klasické válečné umění do pozadí a bojují o lidské vědomí, o vytvoření „správného" společenského názoru. Velmi precizně tuto strategickou doktrínu vyjádřil americký generál John Shalikashvili[8]: „My nezvítězíme do té doby, než CNN začne vysílat, že jsme zvítězili", a tak jednoznačně ukázal na roli, kterou v tomto druhu války hrají masová média. Média se tak staly třetí stranou každého ozbrojeného konfliktu, a to kterou stranu podpoří ve značné míře určuje výsledek[9]. Globalizace mediální sféry, a kyberprostor stavící na prostoru necenzurovaných informací do ní nesporně patří, vede k dominanci mediální říše, vytvářející „potřebnou realitu" a manipulujících podvědomím lidí podle své potřeby. Dochází tak k přechodu vlivu od mocných států na mediální impéria.

[7] AES – Advance Encryption Systém, známý též jako Rijndaelův algoritmus.

[8] John Malchase David Shalikashvili (*27.6 1936), americký generál, náčelník štábu v letech 1993 až 1997. Narozen ve Varšavě, rodiče pocházeli z Gruzie.

[9] Nelze vzpomenout poslední válečné operace USA v Jugoslávii a Iráku. Počátku vlastní válečné činnosti vždy předcházela obrovská zpravodajská kampaň, zacílená na diskreditaci protivníka a vytvoření obrazu nepřítele.

Důležitou roli v tomto případě hraje tzv. percepční warfare, jehož princip může být osvětlen na následujícím případě percepčního útoku a obrany. Předpokládejme, že strana A vlastní nějaký prostředek, který ji v konfliktu zvýhodní před stranou B. Strana B tedy může podniknout akce směřující buď ke zničení tohoto prostředku, resp. jeho efektu, nebo se může pokusit o manipulaci vnímání – percepce – významu tohoto prostředku stranou B vzhledem k ostatním prostředkům, které má strana B k dispozici. Druhé možnosti může být dosaženo několika způsoby, avšak nejběžnější je změna nazírání strany A na tento prostředek, kdy se vychází z omezených schopností vnímání dané situace jedincem. Rozdíl při vnímání „struktury rozmístění" na šachovnici mezi nováčkem a velmistrem spočívá v objemu jim známých „struktur". Tedy pokud se na šachovnici vyskytne struktura, která není ani jednomu z nich známa, pak velmistr nemá v tomto smyslu výhodu. S využitím této podobnosti můžeme tvrdit, že percepčním útokem je útok na schopnosti velitelů vnímat strukturu „bitevního pole" a nalézat v ní jim známé struktury. Omezením schopnosti vnímat specifické „struktury" nebo vytvářením „struktur" známých pak můžeme velitele dovést k očekávaným mechanismům konání, které bude ve prospěch strany B i přesto, že uvedený prostředek poskytuje výhodu, již neviditelnou, straně A.

7.7 Hacker[10] warfare

Hackerské války jsou založeny na napadení informačního systému. Od fyzického boje se liší tím, že každý hackerský útok je vždy specifikován vlastnostmi konkrétního napadeného systému, neboť právě využití slabých míst umožňuje hackerovi se zmocnit řízení systému nebo napáchat jiné škody. Dobře provedený útok na systém může vyřadit z provozu celé řídící a kontrolní centrum nebo senzory. Rovněž může způsobit výrazné ekonomické ztráty vyřazením ekonomicky důležitých center, nemluvě o roli těchto útoků v ekonomické a politické špionáži[11]. Významný podíl HW je při vedení politické a ideologické propagandy nebo používání metod percepčního managementu, tedy obecně při implementaci metod psychologického boje v kyberprostoru. Základní metody vedení hackerských útoků spočívají zejména v:

- ✓ infikování systému pomocí virů,
- ✓ instalaci Trojského koně, který následně umožní skrytý vstup do systémových dat,
- ✓ instalace logické bomby, programu, který po určitém signálu zahájí ničení dat, odepírání přístupu k informačním zdrojům nebo zmate systém a jeho uživatele,
- ✓ vytváření skrytých interfaců pro vstup do systému.

[10] Zdá se být anachronismem používat slovo hacker v tomto spojení, když v předcházejících kapitolách jsme ocenili etiku hackerů a zneužití hackerských metod jsme označili jako crackerství. Nicméně v následujícím je používáno toto spojení spíše jako známá fráze pro soubor technik a metod, než jako označení virtuální komunity. Prosím, aby čtenář i nadále tento rozpor bedlivě vnímal.

[11] V této souvislosti je možné připomenou hackerský průnik do serveru japonského ministerstva obchodu provedený pod řízením americké špionážní agentury CIA v roce 1996. Americký zástupce Mickey Kantor tehdy vedl jednání o importu amerických vozů na japonský trh a tento útok vedl k významné změně dojednaných podmínek [S05].

Ve vztahu k napadenému systému hacker může zaujímat např. některou z následujících pozici:

- ✓ Zcela cizí osoba, která nemá přístupová práva, a tak může použít k útoku jen prostředky globální sítě.
- ✓ Pracovník společnosti, který nemá legální přístup k napadenému systému, např. uklízečka, vrátný, pracovník servisní firmy, který se pokouší zjistit např. heslo legálního uživatele, a tak umožnit použití systému s oprávněným přístupem uživatele nebo administrátora.
- ✓ Uživatel systému, který má minimální přístupová práva, avšak má legitimní přístup k systému. Jeho prostřednictvím může hacker může atakovat systém, s využitím chyb nebo slabin v programovém zabezpečení a administraci systému.
- ✓ Administrátor systému získaný protivníkem. Takový „hacker" má veškeré legální práva pro provedení úspěšného útoku na systém a spíše jde o metody vedoucí k zahlazení stop a ukazatelů na konkrétního útočníka. Často stačí, že pouze poskytne přístup k systému, ostatní činnosti mohou být vykonávány zcela nezávisle.
- ✓ Programátor systému, který má největší příležitost vkládat do systému různé nedokumentované funkce, které mu později umožní neoprávněný vstupu do systému.

Konkrétní způsob útoku však vždy záleží na architektuře systému, nicméně některé běžné metody je možno použít u téměř každého informačního systému, např.:

- ✓ Zcizení přístupových informací, ke které dojde cíleným „špehováním" při zadávání přístupových informací uživatelem, zneužitím hesel zapsaných do diářů a na papírky, krádeží vnějšího nosiče informací (Touch Memory, Smart Card, USB Stick apod.), nebo prostým phishingem.
- ✓ Tipování hesla a to buď neoptimalizované nebo optimalizované nějakou podmínkou (většinou se jedná o metody „brute force").
- ✓ Skenování pevného disku uživatelů - postupné čtení souborů, uchovávaných na pevných discích serveru. Pokud je hackerovi zamítnut přístup k nějakému souboru, pak pokračuje ve skenování dál. Je-li obsah harddisku je dostatečně velký, je zde prakticky jistota, že při určování přístupových práv k souborům se administrátor dopustil alespoň jedné chyby. I když se jedná o poměrně primitivní způsob útoku, je to metoda poměrně efektivní, nicméně musí být provedena legálním uživatelem systému.
- ✓ Obdoba výše uvedeného způsobu pro zdroje lokální sítě.
- ✓ Sběr a prohledávání „odpadu", neboli prohledání odpadkových košů na disku se soubory předchozích uživatelů, pokud to umožňuje systém.
- ✓ Lokální útok typu DoS. Tento útok je zaměřen na celkové nebo částečné narušení provozu systému, ke kterému může dojít při.
- ✓ Kumulaci zdrojů – program se snaží získat veškeré systémové zdroje počítače, které může mít, např. přisvojí si nejvyšší prioritu a spustí krátký nekonečný cyklus.
- ✓ Bombardování systému úlohami, které zabírají maximální objem systémových zdrojů.
- ✓ Odesílání nesmyslných požadavků, které dříve nebo později vyvolají fatální chybu.

Do této skupiny však můžeme zahrnout i útoky, které lze provést na úrovni sítě, např.:

- ✓ odposlouchávání provozu, kdy se zmocníme paketů adresovaných jiným počítačům,
- ✓ odklon paketů na směrovačích,
- ✓ podvržení fiktivního směrovače,
- ✓ vnucení paketů – do sítě jsou odesílány pakety s podvrženou zpáteční adresou s cílem navázat spojení ze serverem se stejnými přístupovými právy jako uživatel, který původně pakety posílal.

Hacker warfare je nezbytnou složkou každého infoware a představuje vlastní základ pro další strategické operace informačního boje. V současné době je možno konstatovat, že téměř každý politický konflikt, týkající se států nebo kontroverzních politických stran vyvolává vlnu hackerských aktivit. V jejich množství je pak obtížné rozpoznat, zda se jedná o ojedinělé aktivity hackerů nebo hackerských skupin, nebo o koordinované aktivity při ověřování prostředků informatického boje.

7.8 Ekonomický informační warfare

Pod ekonomický informační warfare zařazujeme veškeré aktivity směřující k zastavení nebo přerušení toku informací nebo změnu jejich směrování s cílem získat ekonomickou převahu. Hodnota informačního ekonomického warfare spočívá v jeho schopnosti narušovat největší hodnoty jakékoliv ekonomiky – informace. S ohledem na předcházející definici můžeme rozeznávat dvě formy EIW informační blokádu a informační imperialismus [L01].

7.8.1 Informační blokáda

Informační blokáda je metoda s oblibou používaná Spojenými státy a Velkou Británií. Blíže ji lze specifikovat jako ekonomická omezení způsobená určité zemi s cílem přinutit ji ke změně stávající politiky. Je nutno si uvědomit, že prosperita společnosti je stejně závislá na pravidelném přítoku informace jako na přísunu materiálních zásob. Omezení přístupu k některým informacím může ochromit ekonomiku stejně dobře, jako omezení zahraničního obchodu.

Informační blokáda se ve svém důsledku projeví jako ekonomická blokáda připravuje postižený stát o výhody mezinárodního obchodu. Rovněž snižuje schopnost postiženého čelit psychologické válce nebo ji provozovat. Blokáda informačních toků bez blokády fyzického přítoku zboží má pouze jedinou variantu – blokádu informací přenášených elektronickou cestou. V případě, že fyzický přístup zůstane nedotčený, přístup k tištěným materiálům i obšírným databázím na informačních nosičích je zachován. Narušeno je jen obchodování vedené v reálném čase a omezí se přístup k obrovským informačním tokům.

Otázka však spočívá v účinnosti ekonomických blokád včetně informační blokády. Jejich výsledky často nejsou nejlepší. V devadesátých letech minulého století podepsal prezident Clinton asi 60 zákonů a nařízení, jejichž cílem bylo blokovat přibližně čtyřicet vybraných zemí. Tento výběr představoval asi 40 % lidské populace a téměř pětinu amerického vývozu. Závěry studií expertů potvrdily, že ztráty exportu činily téměř 19 miliard dolarů, nicméně blokované země to příliš nepoznamenalo. Důvody jsou dva:

- ✓ Jednalo se o země, kde životní úroveň průměrného obyvatele je i beztak nízká a totalitní režimy v těchto zemích vždy nalezly kanály k uspokojení svých vlastních nároků.
- ✓ V uvedených zemích došlo k posílení obchodních rivalů amerických firem, jejichž zahraniční trh v USA nebyl příliš významný, a tak jejich obchodní blokáda v USA nevedla k jejich značným ztrátám. Navíc tyto firmy získaly v blokovaných státech nemalý vliv a firmy USA se v těchto zemích nebyly vítány.

7.8.2 Informační imperialismus

Libicky v [L01] uvádí: „Věřit v informační imperializmus znamená věřit v současný ekonomický imperializmus. To znamená, že trh je válka. Státy se vzájemně perou o nadvládu v strategickém a ekonomickém průmyslu". Toto tvrzení vychází z faktu, že se každý stát specializuje na určité druhy průmyslu a rozvitý mezinárodní obchod umožňuje saturaci ostatních potřeb. Nicméně některé druhy průmyslu jsou efektivnější a přínosnější, a tak je vyvíjen značný tlak na takové oblasti, které přinášejí výrobu s maximální přidanou hodnotou.

To ale vyžaduje intenzivní výzkum, neustálé zlepšování dovedností a technologií a získávání informací, které umožní následující dominanci a prosperitu v průmyslovém světě. Následkem je i kýžená ekonomická dominance přinášející možnost diktovat své ceny a podmínky na světovém trhu. Taková ekonomická dominance je jedním z hlavních faktorů umožňujících státu zaujmout i politicky významné místo na světové scéně.

Schopnost ochránit vlastní informace a také získat informace o technologiích používaných ekonomickým soupeřem patří k základům ekonomické války. Jednou z metod jak získat tyto informace je průmyslová a obchodní špionáž, která pro tyto účely hojně používá hackerské útoky na komunikační kanály a servery zájmového subjektu.

7.9 Kybernetický warfare

I když k pojmu kybernetický warfare přiřazujeme většinou různé futuristické scénáře, lze některé rysy tohoto typu boje vysledovat i v současném kyberprostoru. Taková válka vedená prosti nepříteli v kyberprostoru je součástí scénářů vyspělých vojenských systémů a spojuje v sobě kyberterorismus, sémantický útok a simulovanou válku. Cílem útoku jsou telekomunikační systémy, útok na data se provádí prostřednictvím telekomunikačních kanálů místo fyzických zbraní a výsledek je často závislý na umění správně použít získaná data proti nepříteli.

Metody sahají od kompromitace osob zveřejněním privátních informací, záměrné publikaci klamných informací nebo jejich vložení do osobních spisů nějaké osoby nebo napadení webových stránek nepřítele a umístění na nich výhružné i propagační informace s cílem zastrašení – defacement. Je možno vysledovat dva základní trendy v této oblasti:

- ✓ Hackerskou válku, vedenou hackerským warfare a vyvolávající náhlá nebo systematická selhání systémů nebo zabránění v jejich provozu.
- ✓ Sémantický útok, kdy systém pokračuje v provozu a je vnímán jako správně fungující složka, avšak generuje výstupní informaci rozdílnou od reálné. Možnosti takového útoku závisí na předpokladech a charakteru konkrétního systému a velmi často se sémantické útoky používají pro percepční management.

Mezi základní principy kybernetické války můžeme zařadit následující charakteristické prvky:

- ✓ Útočník se vždy snaží schovat v kyberprostoru. Nakolik ale kyberprostor vyvolává dojem falešné anonymity, není to tak jednoduché. Jakákoli aktivita se odrazí v přenosu dat, a tak se kybernetický útočník musí snažit schovat své aktivity v existujících tocích dat. Změny vyvolané jeho aktivitou nesmí mít snadno detekovatelný charakter.
- ✓ V kyberprostoru vždy existuje entita, která má povolení a možnost provést přesně tu aktivitu, kterou potřebuje útočník k dosažení svého cíle. Jedním ze základních úkolů útočníka je jakýmkoli způsobem převzít práva této entity.
- ✓ Kyberprostor není teritoriálně omezen, což je vlastnost reálného světa.

Některé přední světové analytické společnosti předpokládají, že neustále rostoucí závislost států na internetu, může vyprovokovat závody v kybernetickém zbrojení. Podle jejich odhadů bude brzy úroveň infiltrace internetových technologií do ekonomického, politického a sociálního života lidstva tak vysoká, že se bude muset zařadit do skupiny „kritické infrastruktury". Internetová síť začne hrát dominantní roli v životě každého státu, proto útok, který bude na ní zaměřen, vyvolá úplné ekonomické a politické ochrnutí státu.

7.10 Infoware versus konvenční ozbrojené složky

Infoware v té podobě, jak jej známe dnes, není určeno k nahrazení klasických ozbrojených složek. Jeho funkcí je a i v dohledné budoucnosti bude spíše podpora ostatních armádních složek a časem se stane jednou ze složek ozbrojených sil. Infoware bývá často přirovnáváno k letectvu, kde podobnost je spatřována zejména ve schopnosti zasahovat cíle na velké vzdálenosti a se značnou rychlostí, a tak pohotově reagovat na vývoj situace. Dalším společným rysem, který je infoware i letectvu přisvojován je dominance, která může výrazně napomoci ostatním složkám. Stejně jako letectvo samo o sobě nedokáže obsadit nějaké území, informační převaha je významnou pomocí ostatním složkám armády přesto, že kybernetický útok sám o sobě není schopen poškodit fyzické objekty[12].

Jinou složkou armády, se kterou bývá infoware často srovnáváno, je rozvědka. Zde je paralela jasná – v obou případech jde o získávání informací od protivníka, případně zabránění protivníkovi v podobných aktivitách. Při použití se z infoware stává jedním z nenahraditelných nástrojů rozvědky. V tomto smyslu je informační válka zaměřena především na ekonomický, politický a morální stav každého jedince, což se pak projevuje na organizaci nebo státu jako celku. I když nemůže působit výrazně fyzicky[13], její psychologický a ekonomický dopad je obrovský.

Informační válka přináší globalizaci válečných aktivit, neboť vzhledem k použitým prostředkům téměř nezáleží na lokalizaci nepřítele. Její průběh může být latentní, i když dopady vítězství nebo prohra jsou později promítnuty do reálného světa. Fyzické oddělení protivníků vede k virtualizaci střetu a tím současně k selhávání základních etických, morálních a citových bariér. Její nebezpečí spočívá zejména v tom, že se podobá počítačové hře, že štáb může válčit z pohody kanceláře a nemusí daleko jezdit, aby počítal úspěchy ztráty. Informační válečník nikdy nestane nepříteli tváří v tvář a nepocítí bezprostřední dopad svých činů.

Mechanizmy a prostředky informační války změnily po staletí platná pravidla válečného umění, stávají se je jeho součástí, avšak ještě nedospěla k takovému stádiu, kdy mohou existovat samostatně. Masivní mediální kampaně jsou průvodním zjevem každé vojenské operace ve světě. Mechanismy informačního boje se přesunuly z válečného arsenálu i do politiky a ekonomiky. Nicméně informační boj zůstává a ještě dlouho bude součástí konvečních ozbrojených složek, schopných klasické hrozby bezprostředním fyzickým násilím.

7.11 Budoucí perspektivy vývoje infoware

Závislost společnosti na informačních systémech je značná a neustále roste. To znamená, že i počet potenciálních cílů pro útoky pomocí prostředků infoware se zvyšuje. Dochází k neustálému vývoji jak těchto bojových prostředků tak i oblastí ve kterých mohou být použity. To může vést k závěru, že infoware bude v budoucnu zaujímat významnější pozici.

[12] To platí pouze v primárním pohledu. Sekundární efekty zasažení řídících systémů např. vodního hospodářství se samozřejmě mohou projevit ve fyzické destrukci objektů.

[13] Je nutno uvést, že např. elektronická válka podporuje právě vývoj fyzických zbraní – zvyšuje jejich efektivitu, přesnost a účinnost.

Velkou výhodou dnešního infoware je současný laxní přístup k bezpečnosti informačních systémů, který je v budoucnosti neudržitelný, a to zejména v klíčových částech infrastruktury. Není pravděpodobné, že by k této změně došlo náhle a zřejmě bude nutné, aby došlo k velkému a medializovanému informačnímu incidentu s katastrofálními následky, aby se na tento problém upoutala pozornost dostatečného množství vlivných osobností, institucí a vlád.

Významnou oblastí, kde se dá očekávat rychlý rozvoj technologií infoware je podniková sféra. I když průmyslová špionáž funguje prakticky od doby, co je průmysl průmyslem, lze očekávat, že spolu s rozvojem podnikových informačních systémů dojde i k rozšíření těchto aktivit a k ještě většímu pronikání prostředků infoware do této oblasti. Prostředky zpravodajského software a elektronické špionáže jsou již dnes používány velkými korporacemi, které vytvářejí uvnitř své struktury dovedně maskované jednotky „business intelligence". A současně s tím, jak si špičkoví manažeři stále více uvědomují cenu informace, jak začínají využívat její moc v souvislosti s ekonomickými a politickými nástroji, dochází i k opatrnému podporování ne zrovna legálních aktivit, při kterých se snaží potřebné informace získat. Zdá se, že právě na tomto poli sehraje infoware svoji nezastupitelnou roli.

7.12 Příklady informačních střetů

Úvodem této kapitoly je nutno konstatovat, že z veřejných zdrojů nelze získat žádné informace o čistě kybernetickém útoku, který by vedl k přímým zraněním nebo násilí. Často jsou kybernetické útoky zařazovány mezi akty občanské nespokojenosti, stejně jako například veřejné demonstrace, nebo kyberteroristické aktivity. Mnohé z nich jsou motivovány především politickými a sociálními podněty, ale jejich klasifikace jako kybernetického útoku je čistě na úsudku autora.

Nicméně je možno uvést dva typické příklady kybernetických konfliktů, resp. konfliktů, které se odehrávaly v kyberprostoru, ale jejichž prapůvodní příčinou byl fyzický střet. V následujícím popíšeme dva různé typy konfliktů – doprovodné hackerské útoky během války v Kosovu a americko-čínskou hackerskou válku z roku 2001.

7.12.1 Konflikt v Kosovu

Kosovská válka byla poslední evropskou válkou 20. století, a první válkou NATO. Byla to také válka, pro kterou média implicitně i explicitně vytvářela důvody. Z právních a politických důvodů válkou nikdy nazývána nebyla a ironický závěr Anthonyho Cordesmana[14] [I05] jenom tuto skutečnost dokresluje: „Jednou z lekcí moderní války je, že tato válka už nesmí být nazývána válkou." Obecně se válka v Kosovu označuje jako dílo donucovací diplomacie.

Pozoruhodným doprovodným zjevem války v Kosovu je selhání zpravodajských agentur. Např. Defence Intelligence Agency ani nezařadila v únoru 1999 Kosovo do svého přehledu světových ohnisek nepokojů. CIA zase vybrala čínské velvyslanectví za cíl raketového útoku v domnění, že jde o jugoslávské federální ředitelství zásobování[15]. Nicméně i kombinace počasí, rolnické vychytralosti a technicky velmi primitivní diverze zmátla multimiliardové moderní zbraně NATO, které se snažily najít a zničit srbské obrněné jednotky v Kosovu. Ukázalo se

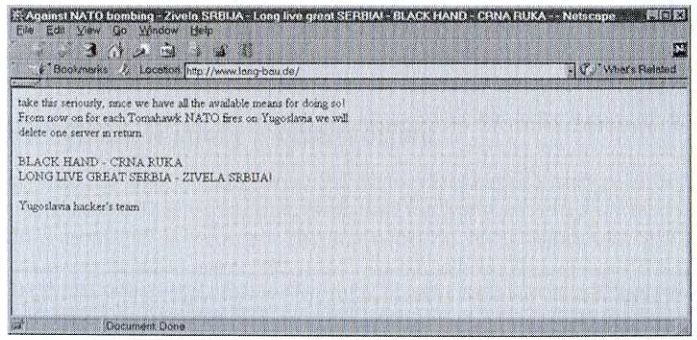
[14] Dr. Anthony H. Cordesman je expertem agentury „Center for Strategic and International Studies" a ředitelem „Center's Middle East Program". Zároveň působí jako vojenský analytik pro ABC a byl poradcem amerického velení v Evropě.

[15] Toto byl jediný terč navržený CIA.

např., že laserem řízené bomby se dají velmi špatně používat v mracích a v Kosovu je na jaře vždy zataženo. Výkvět technologické dokonalosti – střely s plochou dráhou letu zamířené na radary systému protivzdušné obrany byly zmateny jednoduchou taktikou: Srbové na několik vteřin radar zapnuli, pak ho zase vypnuli. A dezorientované rakety se zatoulaly do Bulharska. Srbové stavěli falešné „lákací" mosty z umělé hmoty a NATO je zničilo, postavili pece na dřevo, s komíny natočenými tak, že vypadaly jako hlavně a NATO je sejmulo s dokonalou přesností. Srbové dali na zadní části nákladáků natřená polena a NATO opět vyhovělo.

Obr. 7.1: *Defacement stránky amerického serveru v doméně .com srbskou skupinou KHG*

Opakem této primitivní strategie zaměřené na dokonalou technologii protivníka byly kybernetické útoky zaměřeny proti infrastruktuře NATO. Po dobu bombardování byly webové stránky NATO vystaveny neustálým útokům, které byly podle zdrojů NATO iniciovány hackery přímo podporovanými jugoslávskou armádou. Na všech serverech NATO, které hostují mezinárodní webovou stránku NATO a e-mailové služby, byl zpozorován DDoS útok typu „ping saturation" a mailové servery byly neustále bombardovány záplavou e-mailů obsahujících viry [M05]. Tyto útoky opakovaně vyřazovaly z provozu servery NATO. Po zásahu čínské ambasády posílali čínští hackeři zprávy typu: „Nepřestaneme útočit, dokud neskončí válka!!!" na americké vládní stránky.



Obr. 7.2: *Defacement německého serveru lang-bau.de jinou prosrbskou skupinou*

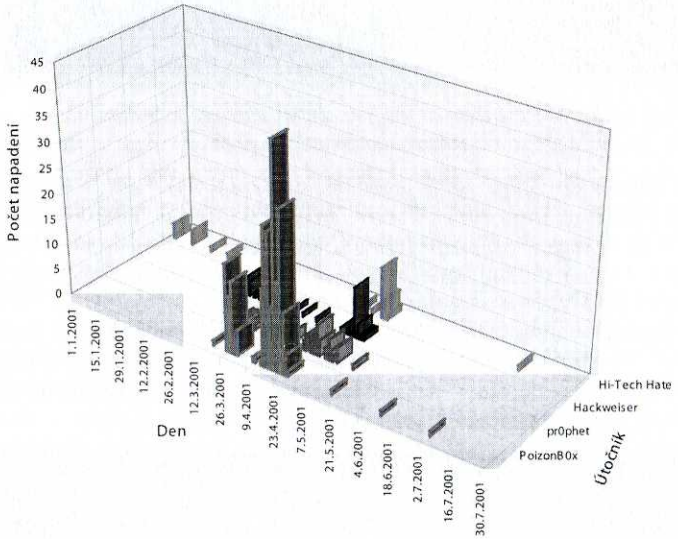
konecma

Ve stejné době jako útoky na servery NATO se objevovalo mnoho defacementů stránek americké armády, vlády i komerčních firem, které měli na svědomí srbští, ruští a čínští sympatizanti jugoslávské vlády. Ačkoliv služby přímo spojené s bombardovací kampaní NATO nebyly těmito útoky dotčeny, útoky proti komunikační infrastruktuře způsobily vážné poruchy vnitřních i vnějších komunikačních služeb [M05].

7.12.2 Americko-čínský konflikt v roce 2001

Dne 1. dubna 2001 se srazil americký výzvědný letoun EP-3 s čínskou stíhačkou v blízkosti čínského pobřeží. Čínský letoun spadnul do moře a americkému pilotovi se podařilo nouzově přistát na čínském ostrově Hainan. Americká posádka byla zadržena, umístěna do hotelu, z něhož nesměla vycházet, a letoun EP-3 byl podroben velmi detailnímu technickému zkoumání[16]. Vznikla poměrně napjatá situace mezi USA a Čínou, jedna diplomatická nóta stíhala druhou.

Politické napětí se postupně projevilo i ve vzrůstajícím počtu kybernetických útoků. Následující politický konflikt mezi oběma mocnostmi byl doprovázen vzájemnými kyberútoky a defacementy webových stránek na obou stranách. Navíc obě strany byly významně podpořeny skupinami hackerů po celém světě. Čínské skupiny jako „Honker[17] Union of China" a „Chinese Red Guest Network Security Technology Alliance" organizovaly masivní a vytrvalé útoky proti americkým cílům, které vedly americké Národní centrum ochrany infrastruktury (NIPC) k tomu, aby dne 26. dubna vydalo varování o zvýšené aktivitě hackerů proti americkým systémům v období od 30. dubna do 7. května [N07].

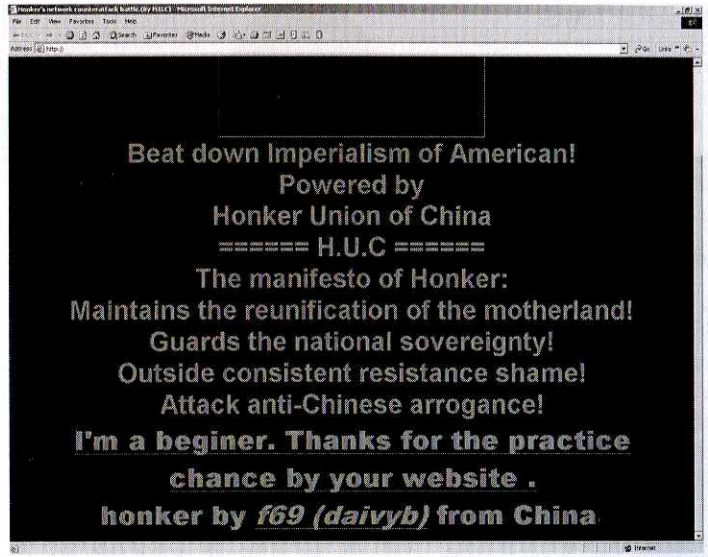


Obr. 7.3: *Statistika odvetných útoků proamerických hackerů v inkriminovaném období*

[16] Podobnou akci podnikla americká strana v roce 1976, když pilot sovětské armády, který později požádal o politický azyl v USA, přistál na americké půdě s vojenskou stíhačkou. Američtí odborníci podrobně letoun prostudovali, rozebrali ho a poslali po částech v bednách zpět do SSSR.

[17] Honker je slangový výraz pro hackera v čínštině.

Následkem vyhrocené politické situace byla kybernetická válka mezi pročínskými a proamerickými hackerskými skupinami. Pročínští hackeři vytvořili nový server KILL_USA a umístili na něj celou řadu volně stažitelných programů umožňujících útoky na americké servery. Odveta proamerických hackerů netrvala dlouho, neboť téměř vzápětí se objevil server KILL_CHINA s obdobným obsahem, ale tentokrát určeným pro útoky na čínské servery. Jak proameričtí tak pročínští hackeři využívali internetová diskusní fóra a IRC k plánování a organizování útoků proti „nepřátelským" cílům[18].



Obr. 7.4: *Defacement amerického serveru provedený skupinou H.U.C.*

Zajímavé je, že ani americká ani čínská vláda tyto útoky nesankcionovaly. Alespoň je tak možno usoudit z toho, že ačkoliv tyto aktivity byly dostatečně známé, ani čínské ani americké úřady nikoho nezadržely. Poté, co asi 1 200 amerických serverů, včetně těch patřících Bílému domu, letectvu a dalším, bylo vystaveno DDoS útokům nebo napadeno defacementem s pročínským obsahem, útoky přestaly[19]. Během útoků probíhaly tiskem nejrůznější úvahy o tom, zda se nejedná o organizovanou hackerskou válku. Fred Cohen, známá osobnost v oblasti internetové bezpečnosti prohlásil, že existují důkazy, že hackerské útoky na americké servery byly povoleny a podporovány čínskou vládou [L02]. Usoudil tak zejména z toho, že „hacking" je v Číně posuzován jako trestný čin proti majetku, a proto předpokládal, že k takovému masovému sdružení útočníků muselo existovat „vládní požehnání". Dalším dokladem, který předložil byla analýza červu 1i0n, který napadal linuxové servery, získával informace o jejich konfiguraci a posílal je zpět do Číny. Později byly tyto servery napadány většinou útoky DDoS.

7.12.3 Další významné střety v kyberprostoru

Kybernetické války začínají téměř neznatelně doprovázet téměř každý politický, náboženský nebo vojenský konflikt. Dnešní internet, propojující miliony serverů a uživatelských stanic se stává virtuálním bojištěm, ať tomu tak chceme nebo ne. Mezi nejpopulárnější a nejznámější

[18] Zajímavý je postoj některých hackerských skupin k této válce, např. hackerská skupina Pr0phet vyzývala obě strany, aby s válkou skončily [T02].

[19] Stojí za to poznamenat, že řada známých červů jako 1i0n, Adore a Code Red pravděpodobně vznikla v Číně.

metody patří defacement, kdy jsou původní stránky serveru nahrazeny novými, které obsahují specifické politické nebo sociální poselství. V předcházejících kapitolách byly podrobně rozebrány dva populární střety – útoky během války v Jugoslávii a čínsko americká hackerská válka. Při popisování metod kyberterorismu jsme uvedli příklady palestinsko-izraelských virtuálních soubojů. I když tyto kybernetické války patří k nejvýznamnějším známým aktům boje v kyberprostoru, připomeňme ještě několik dalších.

konecma

7.12.3.1 Čína versus Taiwan

Během prezidentských voleb napadali čínští hackeři v srpnu a září 1999 taiwanské servery. Používali zejména metodu defacementu, a to nejenom proti politickým a ekonomickým institucím, ale zasaženy byly i servery elektrárenské společnosti, telekomunikačních firem a servery řízení letového provozu. Podle některých zdrojů byla cílem napadení 195 serverů snaha negativně ovlivnit nebo narušit taiwanskou infrastrukturu.

7.12.3.2 Indie versus Pakistan

Proindičtí a propakistánští hackeři tráví již léta v kybernetických střetech jejichž základním motivem jsou národní a etnické rozdíly. Od ukončení války v Kašmíru v roce 2000 hackeři obou stran neustávají ve svých virtuálních soubojích. Mezi nejznámější aktéry patřila skupina G-Force Pakistan, původně teritoriálně zařazená do oblasti Pakistánu, později však byla identifikována jako skupina pakistánských hackerů žijících v USA. Propakistánští hackeři jsou mnohem aktivnější v této oblasti, do konce roku 2005 napadli více než 500 indických serverů zatímco proindičtí hackeři jenom několik pakistánských[20].

7.12.3.3 Japonsko, Jižní Korea a Čína

Rok 2001 byl poznamenán v této oblasti několika kybernetickými střety, jejichž spouštěcím mechanismem bylo chování Japonska. V prvním týdnu dubna 2001 napadli jihokorejští hackeři server japonské vládní organizace odpovědné za publikaci učebnice historie, ve které byla hrubě zkreslena úloha Japonska ve druhé světové válce. Neochota japonské strany přiznat odpovědnost za své chování během druhé světové války vedla v Jižní Koreji k vlně nenávisti vůči Japonsku. Projihokorejští hackeři, zejména studenti tamních univerzit, napadli a vyřadili z provozu několik velkých serverů patřících japonskému ministerstvu školství, Liberální demokratické straně Japonska a nakladateli, který učebnici vydal.

Stejně tak se zachovali pročínští hackeři po návštěvě japonského premiéra na místě kontroverzního válečného památníku Yasukuni Shrine[21]. Jako výraz svého pohoršení napadli několik serverů náležejících japonským firmám a vědeckým institucím. Situace se však ještě zhoršila, když japonská vláda krátce poté oznámila začátek těžby nafty a zemního plynu z plošin ve východočínském moři. A aby toho nebylo málo, téměř současně vyšla ona inkriminovaná japonská učebnice historie. Japonské vládní servery byly zahlceny jalovým provozem z čínské a jihokorejské strany, došlo i k několika defacementům. Čínské webové servery uveřejňovaly výzvy, aby internetoví uživatelé zahlcovaly japonské servery svými požadavky a k dispozici byly dány i potřebné programy.

[20] Samozřejmě, že významnou roli v tomto nepoměru hraje počet serverů v obou doménách. Zatímco indická doména .in reprezentuje cca 12 % adresového prostoru přiděleného APNIC, pakistánská doména .pk zahrnuje necelá 4 % tohoto prostoru.

[21] Yasukuni Shrine je válečný památník v Tokiu pocházející z roku 1869 a věnovaný duchu vojáků, kteří padli za japonské císařství. Oficiální návštěvy tohoto památníku vždy vyvolávaly alergickou reakci u Jižní Koreje a Číny, neboť na tomto památníku jsou uvedena i jména válečných zločinců odsouzených pozdějšími vojenskými tribunály.

8.

Průmyslová špionáž

Metody informačního boje a infoware jsou předmětem zájmu nejen ve vojenských kruzích, ale nebývalé popularity dosahují zejména u velkých průmyslových korporací, kde např. obchodní informace, informace o technologiích a technologických postupech patří k tomu nejdražšímu, co firma vlastní. Vytváření jednotek „business intelligence", které se zabývají studiem volně dostupných materiálů o konkurenci je jenom vrcholem ledovce všech podobných aktivit. To co není vidět, jsou metody průmyslové špionáže, a ty mimo jiné používají celou řadu hackerských technik k proniknutí do informačních systémů konkurence, získání informací o jejím obchodních zájmech, marketingových plánech nebo připravovaných produktech.

Průmyslová špionáž, jak se obecně tyto aktivity nazývají, je špionáž páchaná s komerčními cíli a ve své podstatě nemá nic společného s aktivitami rozvědky, které jsou zaměřeny na bezpečnost státu[1]. Její legální část – „business intelligence", věnuje svoji pozornost studiu materiálů publikovaných konkurencí nebo nezávislými výzkumnými organizacemi, obsahu

[1] V době studené války byla průmyslová špionáž velmi úzce spjata s orgány rozvědky, neboť dosažení potřebné technologické úrovně ve státem vlastněných podnicích bylo předmětem státního zájmu.

patentových přihlášek, nebo sledování aktivit konkurenčních společností a korporací[2]. Pečlivě doplňovaná databáze o pohybu významných obchodníků konkurence a její následující analýza může přinést např. významné informace o projektech, na níž se konkurence zaměřuje, skladbě jejich segmentu trhu apod. Nelegální aktivity mohou sahat od korupce, vydírání nebo krádeže informací až po násilné trestné činy.

konecma

Průmyslová špionáž komerčních organizací se nemusí vždy zaměřovat pouze na svoji konkurenci, ale jejím předmětem mohou být i vlády zemí, které připravují rozsáhlé vládní kontrakty. Podmínky uvedené ve smlouvách, náklonnost k nějakému řešení nebo rozsah a objem případné korupce mohou být závažným zdrojem informací, které ovlivní výsledné jednání a tedy i uzavření smlouvy. Náklady na provádění těchto činností samozřejmě společnosti rozpouštějí do jiných účetních položek, avšak lze předpokládat, že náklady na aktivní „business intelligence" i na ochranu proti takovým postupům budou nezanedbatelnou součástí provozu každé velké firmy.

8.1 Známá fakta

Ztráty způsobené zcizením informací se podle některých časopisů pohybují v okolí 450 tisíc USD na jednu krádež. Celkové ztráty způsobené zcizením obchodních nebo technických informací se odhadují na 100 miliard USD ve Spojených státech a na 35 miliard USD v Evropě. Téměř 90 % ztrát vychází informací zachycených v telekomunikačních sítích, tedy odposlechů[3]. V oficiální zprávě americké vlády, která se zabývala úniky informací, se uvádí, že „výroba, prodej, instalace a používání ilegálních zařízení pro odposlech, představuje multimiliardový průmysl na území Spojených států". Podle téhož zdroje jsou ročně instalována nelegální odposlechová zařízení v hodnotě převyšující 800 milionů USD a stejných zařízení nakoupí fyzické osoby každý den za téměř 6 milionů[4]. Uvedená čísla samozřejmě nezahrnují náklady představující nákup a instalaci profesionálních prostředků pro vojenské potřeby, policii a zpravodajské služby. Ročně je zjištěn odposlech u více než 6 500 společností.

Uvedená čísla jsou alarmující a to nejenom z hlediska uvedených ztrát, ale především pro svůj rozsah a dopad. Ochrana informace jako nejdražšího produktu 21. století se tedy jeví jako zásadní, neboť každý kdo chce v tržní ekonomice existovat musí vyvinout maximální snahu co nejvíce informací získat a co nejlépe vlastní informace ochránit.

8.2 Únik informací klasickou formou

Nejjednodušším kanálem úniku informací, který se obtížně zjišťuje technickými prostředky, je prozrazení důležité informace některým z pracovníků firmy. K tomu může dojít nejen z neznalosti nebo neopatrnosti, ale často i za slušnou odměnu od konkurenční firmy. Nicméně i při dodržování maximální opatrnosti je možné, aby informace se z firmy dostala

[2] Naivita výzkumníků zejména z postkomunistických zemí, kde je uměle vyvoláván tlak na publikování zejména v časopisech s vysokým tzv. „impakt faktorem", je vtaným jevem pro tyto útvary. Do rukou pracovníků „business intelligence" se dostávají cenné informace o stavu výzkumu a nových objevech za nepatrnou cenu předplatného těchto časopisů. V zemích, které historicky chápou ochranu informace jako jednu ze základních složek svého rozvoje, např. USA, podléhá publikace nových informací v časopise nebo na konferenci „cenzuře" ze strany patentového oddělení firmy, výzkumného ústavu nebo univerzity.

[3] Tady je nutno upozornit, že se jedná o nelegální odposlechy, nikoliv o ony politiky s oblibou napadané odposlechy prováděné zejména policejními složkami.

[4] Do této hodnoty nejsou započtena zařízení nakupovaná společnostmi a dalšími právnickými osobami.

prostřednictvím technologických kanálů. I když se politicky nejlépe medializují odposlechy telefonních hovorů a sledování e-mailové korespondence, celá řada informací uniká téměř nevědomky z kanálů zcela otevřených.

8.2.1 Technologické kanály

Technologickými kanály úniku můžeme nazvat veškeré metody úniku informací, kde jsou použity technologické prostředky. Mezi nejjednodušší a nejznámější prostředky patří dálkové mikrofony nebo kamery umístěné v prostorách podniku nebo na těle jednající osoby. V případě snímání zvuku se jedná obvykle o vysoce citlivé elektretové mikrofony, jež dokáží bez problémů monitorovat i šepot ve velkých místnostech. Dokonalost těchto jednoduchých zařízení je však obdivuhodná – ty nejdokonalejší pracují s digitálním šifrovaným signálem přenášeným na dálku, jsou spínány na dálku nebo aktivovány hlasem. Spojení citlivého mikrofonu a miniaturní CCD kamery umožňuje přenos nejenom zvuku, ale i obrazu ze zájmového prostředí. Rozměr takového zařízení přitom dosahuje zhruba hrací kostky a potřebný otvor pro objektiv kamery je o něco větší než jeden milimetr a často se dodávají zabudované do předmětů denní potřeby.

Zajímavou metodou je odposlech pomocí odrazu laserového paprsku od některého rezonujícího objektu v místnosti. Provádí se tak, že laserový paprsek se zaměří na tento rezonující objekt, což může být např. i okno, a jeho nepatrné výchylky způsobené akustickým vlněním v místnosti se převádějí na elektrický signál a výsledný odposlouchaný hovor se zaznamenává.

Poměrně jednoduchým způsobem získání informací je odposlech telefonních linek. Na rozdíl od dob, kdy pevné telefonní přístroje byly analogové a stačilo připojit další telefonní přístroj k lince, abychom mohli hovor monitorovat, digitální přístroje tento typ odposlechu poněkud komplikují. Zavedení digitálních technologií do pevných sítí až na úroveň účastnické stanice sice ztěžuje tento typ odposlechu, ale pokud není použito šifrování signálu přímo na místě jeho vzniku, tedy v telefonní stanici, není to zase až tak nepřekonatelná překážka.

Zvláštní kapitolou jsou odposlechy mobilních telefonů. Přestože paranoidní politici neustále upozorňují na to, že jejich mobil je odposlouchávám, je taková činnost běžně velmi obtížně proveditelná. Jednoduché to bylo v případě sítě NMT450, která předcházela GSM telefonii a používala nešifrovaný analogový přenos – stačil běžný přijímač pracující ve správném kmitočtovém pásmu, aby umožnil monitorování telefonu sítě NMT. Odposlech sítí GSM je daleko komplikovanější. Jednak je přenos realizován v digitální formě, kde je v jednom kanále sdíleno značné množství hovorů a je i hovor šifrován[5]. Odposlech GSM telefonu třetí osobou je finančně náročný, příslušná zařízení jsou obtížně získatelná a i v případě, kdy jsou k dispozici, je nutno být neustále odposlouchávané telefonní stanici nablízku – tedy mezi odposlouchávanou osobou a příslušnou základnovou stanicí tzv. BTS[6].

K odposlechu telefonních hovorů je dlužno poznamenat ještě jednu podstatnou charakteristiku odposlechu. Většina občanů se totiž domnívá, že cílem odposlechu je zjistit obsah hovoru, a tak považuje silné šifrování za dostatečnou ochranu. Avšak to není vždy pravdou

[5] Je pravdou, že algoritmus A5 sloužící k ochraně přenosu mezi mobilním telefonem a základnovou stanicí „tajnou" šifrou byl prozrazen a navíc v jejím návrhu bylo objeveno několik chyb, nicméně i tak je odposlech hovoru na síti GSM dalo obtížnější než na pevných telefonních sítích.

[6] Navíc, mnohé GSM telefony umožňují zvýšení bezpečnosti pomocí volání v šifrovaném módu. V jednom přístroji jsou obsaženy dva telefony v jednom, standardní mobilní telefon a mobilní telefon navržený pro volání v šifrovaném módu. Při volání v šifrovaném módu se aktivují datové přenosy a bezpečný algoritmus pro šifrování hlasu – většinou minimálně 128 bitový šifrovací klíč. Cena takového telefonu také odpovídá jeho použití – téměř 100 000,- Kč za kus.

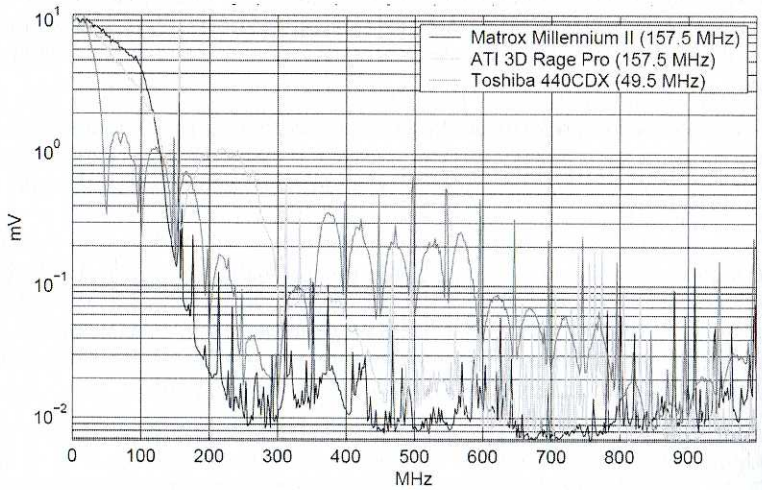
– s odposlechem je spojena ještě celá řada údajů, které zašifrovat nejdou – kdo hovořil s kým, odkud hovořil a kdy byl hovor uskutečněn. Tyto informace tvoří významnou část vytvářené zájmové databáze o odposlechu a mnohdy jsou významnější než vlastní obsah hovoru.

konecma

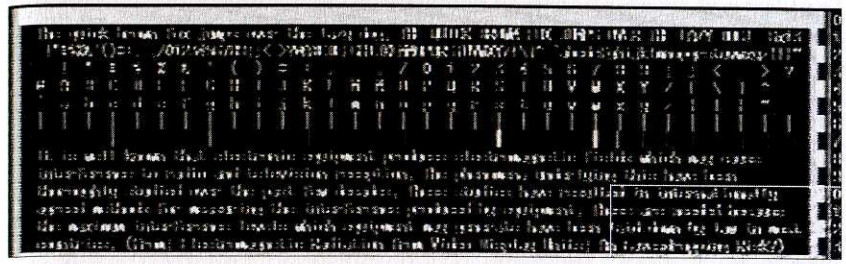
Často se mluví o „odposlechu" monitorů počítačů, tedy zobrazování toho, co zájmová osoba na monitoru vidí. I když o tom mnohdy firmy příliš nepřemýšlí, takový odposlech je poměrně jednoduchý. Jeho princip je založen na způsobu, jak je na displeji obraz vytvářen. Vlastní signál nesoucí informaci je rozmítán po obrazovce dvěma pomocnými signály horizontálního a vertikálního rozkladu. Tento informační signál v sobě obsahuje i značky umožňující synchronizaci těchto pomocných signálů. Přitom kmitočet informačního signálu leží v oblasti radiového spektra, a tak se takový signál poměrně dobře šíří prostorem. Na obr. 8.1 je spektrum signálu, které je vyzařováno běžnými grafickými kartami. Jak je vidět, naměřené hodnoty pole jsou poměrně vysoké a pohybují se v širokém pásmu od nejnižších kmitočtů až po téměř jeden GHz. Přitom se zřejmě jedná o harmonické kmitočty a tudíž vlastní informační obsah bude uložen v poměrně úzkém pásmu několika desítek MHz.

Pokud provedeme experiment, při němž použijeme běžný komunikační přijímač pracující v pásmu stovek MHz, pak můžeme původní obsah obrazovky na běžném analogovém monitoru rekonstruovat z přijatého signálu. První rekonstrukce obrazu pochází z analogového monitoru, na němž byl zobrazen text obsahující známou testovací anglickou větu „The quick brown fox jumps over the lazy dog" jak malými, tak i velkými písmeny a celou sadu čísel, grafických znaků apod. Dále následoval doplňující anglický text.

V prvním případě na obr. 8.2 byl použit komunikační přijímač pracující na kmitočtu 292 MHz a nastavenou šířkou pásma 20 MHz. Anténa byla umístěna ve vzdálenosti cca 3 m od monitoru. Text je relativně čitelný, i když je místy rozmazaný. Tento efekt je způsoben zejména malou šířkou pásma a umístěním nosné frekvence do místa, kde grafická karta poměrně málo vyzařuje.



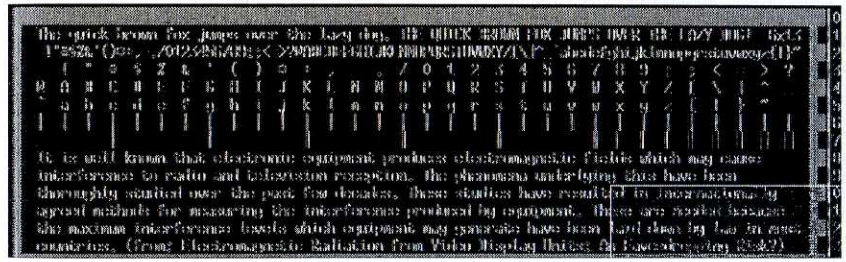
Obr. 8.1: *Vyzařované spektrum různých typů grafických karet*



Obr. 8.2: *Rekonstrukce textu s přijímačem na kmitočtu 292 MHz, šířka pásma 20 MHz*

Příklad na obr. 8.3 ukazuje změnu, kdy parametry přijímače byly nastaveny na kmitočet nosné vlny 480 MHz se šířkou pásma 50 MHz při zachování stejné vzdálenosti antény od monitoru. Je zřejmé, že obrysy písma jsou ostřejší, text se stal čitelnější a zmizely některé „slité" plochy.

Ještě markantnější bude rekonstrukce textu, který byl vytvořen na monitoru, do něhož vstupuje digitální signál vytvářený grafickou kartou. Příklad rekonstrukce textu z digitálního monitoru při náběhu systému Linux je na obr. 8.4 a pro příjem je použit komunikační přijímač pracující na kmitočtu 350 MHz se šířkou pásma opět 50 MHz. Vzdálenost antény byla stejné jako při předchozích experimentech, tedy 3 m. Pokud bychom změnili polohu antény a zvětšili vzdálenost např. na 10 m, stále ještě budeme schopni rekonstruovat text ze zájmového monitoru, nicméně vzhledem ke snížení poměru signál/šum budou jednotlivé znaky méně zřetelné.



Obr. 8.3: *Rekonstrukce textu s přijímačem pracujícím na kmitočtu 480 MHz, šířka pásma 50 MHz*

konec ma

Obr. 8.4: *Rekonstrukce textu digitálního monitoru*

S rozvojem komunikačních technologií a miniaturizace vzrůstá rozmanitost zařízení použitelných pro penetraci do zájmového prostředí a získávání informací z něho. Ochrana před takovými metodami je čím dále složitější a nákladnější. Největší problém spočívá v nekontrolovatelném používání takových technologických zařízení. Ačkoliv jsou na jednu stranu neustále, s odvoláváním na ochranu lidských práv, zostřovány zákonné podmínky nasazování technologických zařízení pro monitorování nelegálních činností orgány činnými v trestním řízení a zpravodajskými službami, na druhou stranu roste objem nelegálních odposlechů a technologických metod získávání informací kriminálním podsvětím, organizovaným zločinem, ale i dobře utajenými složkami velkých firem.

8.2.2 Sběr informací v sítích

Většina informací je získávána z veřejně přístupných zdrojů legálními prostředky, je ukládána do velkých databází, které jsou následovně tříděny a metodami dolování informací jsou z nich získávány skryté vztahy. Tak pracuje většina zvláštních služeb, analytiků a ostatních pracovníků, jejichž úkolem je hledat skryté zákonitosti v kybersvětě. Metody „legálních" postupů se za dobu existence internetu a telekomunikací nesmírně zdokonalily a často nevinná žádost plně respektující zákon o svobodném přístupu k informacím[7] může ve svém důsledku vést k získání obchodního tajemství firmy nebo jiných utajovaných informací.

Jedním z nástrojů, jak žádat o informace, je elektronická pošta – je to rychlé, jednoduché, automatizované, snadno se dají převést data z odpovědi do databází a utajit původ tazatele. Podobným zdrojem informací jsou internetové diskusní skupiny, kde lze obsah analyzovat buď pasivně, pouhým sledováním vývoje diskuze, nebo aktivním zasahování do diskuse a kladením cílených dotazů. Stejně je možno vytěžovat různá diskusní fóra nebo internetové chaty.

[7] Zákon č. 106/1999 Sb.,o svobodném přístupu k informacím.

Do skupiny pololegálních aktivit získávání informací můžeme zařadit metody, které jsou sice legální, ale nepříliš etické. Sem patří metody sociálního inženýrství, kdy jsou zasílány např. falešné požadavky o průzkum prostřednictvím elektronické pošty, uskutečňovány podvržené telefonáty sledující jakýsi marketingový výzkum nebo jsou zájmové subjekty kontaktovány jinými způsoby, ale vždy tak, aby druhá strana a její zájmy nebyly jasně patrné. Jiná metoda vychází ze snadné záměny webových stránek a odkazů na tyto stránky v elektronické poště. Útočník přitom spoléhá na důvěřivost uživatele, který nespatřuje v na první pohled známé adrese nic neobvyklého, a tak příslušné webové stránky navštíví. Složení návštěvníků této stránky, jejich reakce a další, mnohdy nevýznamné atributy chování, mohou být ve svém souhrnu základem pro velmi specifické závěry.

Poslední skupinou jsou nelegální aktivity, kam můžeme zahrnou najímání agentů zejména z řad nespokojených zaměstnanců, krádeže informací nebo notebooků[8] a neoprávněné vniknutí do informačních systémů. Využívání hackerských praktik pro vnikání do informačních systémů spadá do této kategorie a v dnešní době, kdy mají společnosti uloženy svá data na počítačích připojených do internetu, jsou jejich možnosti velmi rozsáhlé. Jenom málo incidentů v této oblasti bylo zdokumentováno nebo zveřejněno; s ohledem na vlastní důvěryhodnost mnohé instituce takové případy tají.

Průnik do sítě Microsoft

Dne 27. října 2000 oznámilo vedení firmy Microsoft, že do její sítě měla po jistou dobu omezený přístup neznámá skupina hackerů. Zároveň však zástupci firmy poskytli pouze málo doplňujících informací, což bylo způsobeno faktem, že vyšetřování se teprve rozbíhalo a možných teorií o průběhu útoku bylo mnoho. Teprve v dalších dnech zveřejnila firma nejpravděpodobnější teorii o útoku.

S největší pravděpodobností začal útok již měsíc před jeho odhalením, a to zasláním emailu obsahujícím vir W32.HLLW.Qaz (je rovněž znám jako Qaz.Trojan.)[9]. Pokud je tento virus spuštěn najde v počítači soubor notepad.exe, přejmenuje ho na note.com a sám sebe zkopíruje do počítače pod názvem notepad.exe. Při každém spuštění programu notepad provede nejprve virus svůj kód, a následovně spustí původní aplikaci notepad. Šíření infekce v místní síti probíhá podobným způsobem – virus vyhledá počítač v místní síti, který by mohl infikovat, přejmenuje místní soubor notepad.exe a sebe vydává za původní aplikaci. Podstatné ovšem je, že pomocí emailu odešle IP adresu infikovaného počítače, a nastaví rozhraní WinSock tak, že umožní vzdálenému uživateli připojení k počítači a získání kontroly nad tímto strojem.

Zajímavé je, že v době, kdy útok začal, již byl virus W32.HLLW.Qaz () znám stejně jako ochrana proti němu. Bylo tedy překvapením, že síť Microsoftu nebyla proti tomuto viru chráněna a hackeři uspěli díky laxnímu přístupu řadových zaměstnanců Microsoftu. O tom svědčí i to, že teprve za měsíc po útoku si zaměstnanci všimli e-mailů odcháze-

[8] I když většina z nich má cenu pouhého hardware, odborné prameny uvádějí, že asi na 15 % z nich se nacházely informace, které mohly být cílem takového útoku. Informace se stávají jedním z hlavních aktiv podniku, a proto jsou krádeže notebooků mnohdy orientovány tímto směrem. Někdy není ani třeba, aby notebook byl ukraden – výprodeje použitých notebooků z velkých firem jsou mnohdy dobrým zdrojem informací, které neopatrní uživatelé ponechali na discích.

[9] Tento virus byl poprvé identifikován v Číně v červenci roku 2000.

jících na e-mailový účet v Petrobradě, které obsahovaly IP adresy a hesla k infikovaným počítačům. Nekontrolovaný přístup, který útočníci získali, jim umožnil dlouhou dobu zkoumat síť Microsoftu zevnitř a zjistit, kde se ukládají zdrojové kódy. Vedení firmy přiznalo, že útočníci mohli spatřit kód některých právě vyvíjených aplikací, ale zcela jistě neviděli kód hlavních produktů (os Win 2000, MS Office atp.) a v žádném případě nedošlo k jakékoliv změně ve zdrojových kódech[10].

Firma Microsoft označila celý incident za průmyslovou špionáž, pravděpodobně z toho důvodu, že takové vyšetřování spadá do pravomoci FBI. Je však možné, že opravdu o špionáž šlo, neboť obraz celého útoku nezapadá do obvyklého obrazu internetového výtržníka. Chybí obvyklý prvek kompromitace společnosti, způsobení rozruchu a potřebný exhibicionismus autorů takového útoku. Snaha zůstat v utajení a vytěžit zdroj svědčí spíše o jasném cíli, kdy z výsledků nebude těžit přímo útočník, ale „třetí strana".

Trojský kůň v Malam Systems

Firma Malam Systems patří k významným společnostem nejenom na izraelském trhu[11]*. V roce 2005 se do několika počítačů firmy dostal trojský kůň a díky němu z firmy unikaly důležité informace, mimo jiné i materiály týkající se účasti společnosti ve vládním výběrovém řízení. Zakázka, o kterou firma usilovala, měla hodnotu několika set milionů šekelů*[12]*. Motiv útoku byl zřejmý, a tak se celou záležitostí začala zabývat izraelská policie. Velmi brzy začala zatýkat první podezřelé a do konce května 2005 bylo zatčeno 18 lidí včetně vedoucích pracovníků z místní pobočky firmy Volvo, pracovníků dvou místních mobilních operátorů a největší izraelské satelitní televize. Na žádost izraelské policie byli v Londýně zatčeni dva hackeři z Velké Británie, kteří byli najati k vytvoření použitého trojského koně. Zaměstnavateli obviněných hackerů byli soukromí vyšetřovatelé pracující v Izraeli. Celý organizovaný tým byl obviněn z průmyslové špionáže, nahrávání počítačových virů, nabourávání počítačů, odposlouchávání, narušování soukromí a správy nelegálních databází*[13].

Přesto, že je tento případ velmi podobný předchozímu, jeho významným znakem je organizace skupiny a použití viru naprogramovaného na zakázku. Takový vir je samozřejmě mnohem nebezpečnější než virus, který je již znám. To je dáno zejména způsobeno charakterem práce antivirových systémů, které musí mít k dispozici vzorek viru, aby byly schopny stejný vir odhalit. Navíc, pro distribuci viru použili útočníci nejenom elektronickou poštu, ale i kompaktní disky, které do firmy propašovali. A bývá obvyklou nectností, že antivirový program je např. kvůli zvýšení výkonu počítače, nastaven pouze na skenování příchozích e-mailů a uživatel plně důvěřuje médiím kolujícím na pracovišti. Na závěr je nutno podotknout, že zmíněný virus na zakázku nebyl rozhodně dokonalý. Chyba v kódu viru mohla vést k poškození operačního systému počítače, pokud by nedokázal odeslat nasbíraná data. Podle odborníků tento virus rozhodně nebyl dílem zkušeného tvůrce virů.

Uvedené dva příklady reprezentují průniky do velkých firem pomocí virů, zejména v elektronické poště. Zatímco první případ je typické selhání bezpečnostní politiky společnosti, druhý případ je daleko nebezpečnější, neboť používá dosud neznámý nástroj – vir vyrobený na zakázku. Jak je uvedeno výše, proti takovým virům se lze jenom obtížně chránit, neboť antivirový systém nemá k dispozici vzorek viru a tudíž ho nemůže odhalit. Existují sice obecné metody hledání nebezpečného kódu, ale zatím nejsou tak dokonalé, aby odhalily každý nový virus.

I když veřejnost je díky médiím poměrně dobře obeznámena s běžnými viry, nebezpečí virů na zakázku je stále ještě podceňováno. A pokud by se spojily nedostatky v dodržování bezpečnostní politiky s kvalitně vyrobeným virem na zakázku, může být informační systém napadené společnosti monitorován aniž by cokoliv bylo zpozorováno. A pokud je za tímto monitorováním konkurence, pak to napadená firma pocítí až v okamžiku, kdy se jí přestává dařit a propadá se „do červených čísel".

[10] Mikko Hypponen, bezpečnostní expert firmy F-Secure se dokonce vyjádřil v tom smyslu, že „útočníci v zásadě měli technické prostředky ke změně zdrojových kódů, což vyvolává otázky ohledně důvěryhodnosti budoucích verzí aplikací firmy Microsoft" [D04].

[11] Firma působí na trhu IT a má asi 1200 zaměstnanců.

[12] V přepočtu se jednalo o zakázku větší než jedna miliarda korun.

[13] Jedná se o trestné činy podle místní úpravy trestního zákona.

9.

Globální odposlech

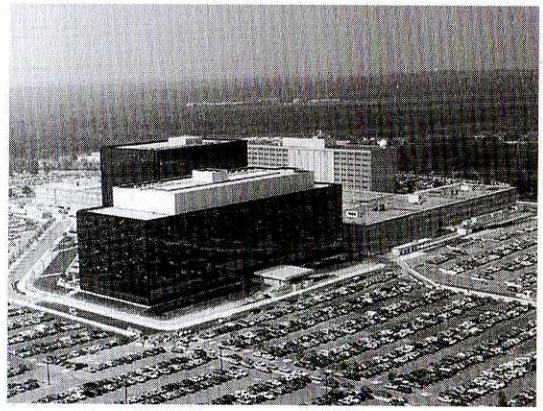
Na úvod této kapitoly si nemohu odpustit drobnou poznámku. Neuplyne měsíc, aby média neinformovala nebo podrobně nepopisovala aféru související s telefonními odposlechy. Občané se pohoršují, občanská sdružení brojí, zejména v České republice, proti metodám policejního státu. A nikdo z nich si neuvědomuje, že „velký bratr" je už po několik desetiletí hlídá, aniž by k tomu měl svolení nějakého soudu nebo o tom odposlouchávané osoby informoval.

Přehledové monitorovací systémy[1] jsou běžnou výbavou vojensko politických aliancí, které je ve velkém používají zhruba od padesátých let minulého století. Jejich úkolem je včasné získání co nejpřesnějších strategických informací, zejména mimo hranice státu, a jejich analýza směřující k podpoře strategického rozhodování ozbrojených složek na základě informací o hrozícím nebo potenciálním nebezpečí. Ve světě se do instalace a provozu těchto zařízení investuje přes 20 miliard Euro ročně a odhaduje se, že je instalováno až 120 přehledových systémů různé velikosti. Jejich významné využití je však rozděleno mezi asi

[1] Často jsou tyto systémy zahrnovány pod společné označení SIGINT – SIGnal Inteligence, které se dále dělí na COMINT – COMmunication INTelligence (vytěžování elektronických informačních zdrojů) a ELINT – ELectronic INTeligence (určování elektronických informačních zdrojů – lokalizace, charakter spektra apod.).

konecma

20 států. Přestože původní úkol těchto systémů spočíval v získávání zpravodajských informací vojenského charakteru, přesouvá se jejich využití v poslední době i do ekonomické oblasti, kdy informace vytěžené přehledovým odposlechovým systémem jsou „kupovány" velkými firmami a slouží jako podklad pro jejich rozhodování.



Obr. 9.1: *Hlavní budova National Security Agency ve Fort Mead, USA [N08]*

Nejčastější metodou je monitorování radiového provozu a odposlech satelitů, ale není výjimkou ani instalace kabelových odbočnic u dálkových kabelů. Většina systémů zpracovává nesmírný objem získaných informací na principu vydělení zájmového provozu z toku dat s následující analýzou podle klíčových slov. Není však neobvyklé ani použití hlasové analýzy u telefonních hovorů nebo hlubší formální analýzy textových zpráv. Mezi nejznámější systémy patří Echelon provozovaný aliancí UK/USA a ruský systém FAPSI. Nicméně podobné systémy, i když menšího rozsahu provozují i další země – Francie, Německo, Švýcarsko, Čína a některé další asijské země, Izrael, Indie nebo Pákistán. Většina vyspělých států považuje globální zpravodajství za klíčové, ale i menší evropské národy, jako Dánsko nebo Holandsko nedávno vybudovaly stanice, umožňující zpravodajsky zpracovávat odposlechy civilní satelitní komunikace.

9.1 Historie globálního odposlechu

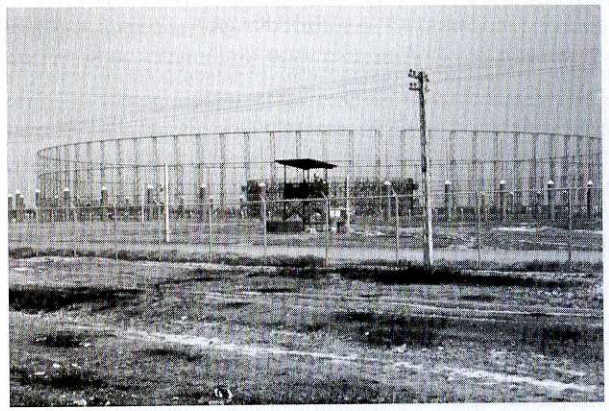
Popsat historii globálních odposlechových systémů není jednoduché, většina informací je stále předmětem nejpřísněji střeženého tajemství a ověřování informací občas proniknuvších do veřejných médií je téměř nemožné. Je tedy nutno, aby čtenář následující řádky bral s rezervou – ne vše co je zde napsáno, může být ověřeno.

Globální odposlech, přísně utajovaný elektronický systém, datuje svůj vznik do období druhé světové války a byl jedním z důsledků rozmachu rádiového přenosu jako základu telekomunikací. I když radioelektronické technologie umožnily vládám, armádě a dalším uživatelům přenášet zprávy na mezikontinentální vzdálenosti, zásadním problémem byla možnost odposlechu. I přes významný rozmach kryptografických metod pro šifrování radiových zpráv nevedla tato cesta k úspěchu. Během druhé světové války se západním Spojencům podařilo rozluštit stovky tisíc německých a japonských signálů. Jak toho dosáhly, je i desítky let po válce přísně střeženým tajemstvím[2].

[2] Je všeobecně známo, že jeden ze zakladatelů moderní informatiky Alan Turing pracoval během druhé světové války v dešifrovacím oddělení anglické armády. Na pomoc kryptologům měl tehdy sloužit počítač COLOSSUS sestavený ze součástí telefonních ústředen přímo na příkaz anglického premiéra W. Churchilla. Rovněž na jeho příkaz byl stroj po druhé světové válce včetně dokumentace zničen. Dnes existuje jeho částečná maketa složená podle poznámek pamětníků.

9.1.1 Aliance UK/USA

Krátce po skončení druhé světové války začala studená válka[3] mezi komunistickým blokem ve střední a východní Evropě a aliancí západních států. Součástí této studené války byla rozsáhlá zpravodajská činnost na obou stranách, a tak americká Národní bezpečnostní služba NSA[4] a britské Vládní ústředí komunikací GCHQ[5] začaly budovat globální odposlechovou síť. Základem pro tuto činnost byla tajná dohoda označovaná jako UK/USA *Agreement* z roku 1947, která umožnila sloučit britský a americký systém, obslužný personál a přijímací stanice. Během druhé světové války totiž britská zpravodajská služba GCHQ vybudovala rozsáhlou síť odposlechových stanic. Řada z nich se nacházela jak na území britského impéria, tak i v zemích se silným britským vlivem – Bermudách, Kypru, Gibraltaru, Iráku, Singapuru a v Hong Kongu. Tyto stanice doplnila americká síť s tisíci dalších trvale provozovaných odposlechových stanic a po rozšíření dohody UK/USA o tři země britského společenství – Kanadu, Austrálii a Nový Zéland přibyly stanice pokrývající severní oblasti Tichého oceánu a arktické oblasti území Sovětského svazu. Později se připojily i další země západního bloku včetně Norska, Dánska, Německa a Turecka. Tyto země podepsaly se Spojenými státy dohodu o využívání informací z této odposlechové sítě jako „třetí strany". Tak vznikl ucelený řetězec stanic provozovaných v západní sféře vlivu, který umožňoval monitorování signálů pozemních a leteckých sil zemí Varšavské smlouvy.



Obr. 9.2: *Anténní pole FLR-9 odposlechové stanice v Nong Soong, Thajsko [H06]*

Technologie používaná odposlechovým systémem Echelon obsahuje mnohá zajímavá řešení, např. obrovskou talířovou anténu používanou pro přenos zpráv do Spojených států odrazem od povrchu Měsíce – tím se znemožnil odposlech tohoto přenosu. Jednou z největších odposlechových stanic na světě byla stanice Kagnew Station v Asmaře v Eri-

[3] Studenou válkou se označuje období několika desítek let po druhé světové válce a její formování bylo dáno výsledkem druhé světové války, kdy na jedné straně byl vliv hegemonie SSSR a na druhé straně snaha západních spojenců po získání vlivu v Evropě. Ta došlo k vytvoření dvou vojenských bloků – západního bloku, který se zformoval v NATO, a východního bloku, který na sebe vzal podobu Varšavské smlouvy tvořené SSSR a jeho satelity. Vztahy mezi těmito dvěma bloky byly značně napjaté a přerostly ve studenou válku, která se krom politických rozporů a rozsáhlých zpravodajských aktivit provozovaných oběma bloky projevila i v některých vojenských konfliktech – korejská válka, vietnamská válka, Arabsko-izraelské války apod.

[4] NSA – National Security Agency je jednou z nejmocnějších zpravodajských agentur světa. Byla založena v roce 1952 na základě nařízení prezidenta Trumana a je prezentována jako státní struktura, která vykonává „nejdůležitější a vysoce specializované technické a koordinační funkce spojené s národní bezpečností". Hlavní štáb se nachází ve Fort Meadow mezi Washingtonem a Baltimore, kde pracuje kolem 38 tisíc zaměstnanců. Ještě větší počet pracuje v pobočkách v různých koutech světa Známými hlavní úkoly NSA jsou tzv. digitální zpravodajství, ochrana vládních informací, a kryptografické služby.

[5] GCHQ – Government Communications Headquarters.

trei[6], která byla v provozu od roku 1941 až do svého uzavření v roce 1970 [H05]. Odposlechové stanice byly vybaveny ohromnými anténními systémy sledujícími komunikaci na všech vlnových délkách a příjem několika stanicemi současně umožňoval určit i polohu sledovaných vysílačů. Jednou z největších anténních konstrukcí je 500 metrů široké pole antén označované jako FLR-9, které bylo používáno od roku 1964. Americké námořnictvo podobné stanice zřídilo ve Španělsku, v Německu, Skotsku, Thajsku, na ostrově Guam a později v Portoriku s cílem zpravodajsky sledovat kubánský režim.

konecma

Globální odposlechový systém Echelon byl využíván i k podpoře lokálních ozbrojených střetů – když Spojené státy otevřely bojové linie ve Vietnamu, australští a novozélandští operátoři pracovali na podpoře této války, na stanici označené kódovým číslem UKC201 v Little Sai Wan v Hong Kongu byl monitorován pohyb letecké obrany Severního Vietnamu v době, kdy americké bombardéry B52 útočily na Hanoj a na další cíle v Severním Vietnamu[7]. V době studené války však byly sledovány nejen zprávy ozbrojených sil Varšavského paktu, ale i civilní komunikace včetně komerčních rádiových spojů mezi velkými evropskými městy[8]. Předmětem zájmu byly i zprávy o vůdcích afrických guerillových hnutí a dokonce byly sledovány některé významné americké osobnosti, jako herečka Jane Fonda, dr. Benjamin Spock a stovky dalších lidí, zejména kvůli jejich odporu vůči válce ve Vietnamu. V sedmdesátých letech minulého století byly zpravodajské aktivity různě přeskupovány a roce 1976 vznikla zvláštní civilní jednotka, která měla zachytávat a analyzovat civilní a diplomatické zprávy. Tato jednotka se soustředila na neamerickou diplomatickou komunikaci a sledovala např. francouzskou a italskou diplomatickou korespondenci.

Aktivity související s globálním odposlechovým systémem neušly pozornosti americké veřejnosti zejména po slyšení ředitele NSA generála Lew Allena před výborem americké Sněmovny reprezentantů[9] v srpnu 1975 a američtí zákonodárci začali zkoumat, zda tyto operace nejsou protiústavní. Avšak výsledek šetření zvláštní skupiny ministerstva spravedlnosti USA byl jako obvykle velmi diplomatický – „shromažďování zpráv o amerických občanech bylo neúmyslným důsledkem sledování mezinárodní rádiové a kabelové komunikace".

Počátkem sedmdesátých let minulého století je rovněž poznamenáno přechodem „ruční analýzy" zpráv na strojovou a základní operace vyhledávání klíčových slov je prováděna počítačovými systémy. Činnost těchto analytických strojů je podobná dnešním internetovým vyhledávačům, kdy stroj hledá určitá slova, fráze nebo kombinace slov a označuje všechny zprávy, v nichž se taková slova nebo kombinace slov vyskytují. NSA vyvinula dokonce zvláštní procesor pro rychlé vyhledávání dat, který se později objevil i na komerčním trhu. Procesor obsahoval zvláštní hardware s výkonnými funkcemi pro porovnávání znakových řetězců schopnými pracovat s libovolným systémem ukládání textových informací.

Po pádu železné opony v roce 1990 a ukončení studené války byly některé informace odtajněny, nicméně dlouhodobé aktivity globálního zpravodajství zůstávají nadále přísně utajeny. Viceadmirál William Studeman, ředitel NSA v roce 1992 charakterizoval cíle NSA jako snahu „poskytnout Spojeným státům globální přístup. K tomu zcela evidentně slouží i současné funkce Echelonu, které s rozmachem celosvětové sítě internet nabyly na významu.

[6] Eritrea je část území bývalé Etiopie (Habeš), která se oddělila v roce 1993. Společná hranice je dodnes předmětem sporů a ozbrojených střetů.

[7] Velká Británie se však oficiálně k těmto lokálním válkám stavěla neutrálně.

[8] Práce analytických skupin byla rozdělena tak, že jedna skupina sledovala Sovětský svaz a jeho spojence zatímco druhá analytická skupina sledovala všechny ostatní státy. Ta byla později označována jako „ROW" (Rest of the World).

[9] Generál Allen přiznal, že NSA systematicky zachytává mezinárodní komunikaci a zpracovávány jsou také zprávy zasílané a přijímané americkými občany.

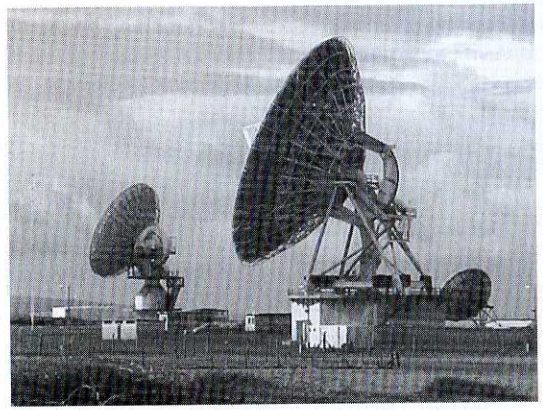
9.1.2 Úloha NSA v digitálním zpravodajství – Echelon

Hlavními odběrateli informací získaných odposlechem nejrůznějších médií jsou Bílý dům, Pentagon, FBI, Ministerstvo obchodu, Ministerstvo financí, CIS[10] a některé další organizace. Původním úkolem NSA bylo včasné upozornění na možný útok na Spojené státy, přičemž doba odezvy nesměla překročit 48 hodin. Hlavní doménou je pozorování různých objektů, odposlechy telefonů a zachycování písemné korespondence. Součástí těchto prací v době studené války byla analýza časopisů, vědeckých článků, příruček atp., které byly vydávány v Sovětském svazu.

Ještě do vytvoření NSA měla CIS, díky smlouvám s velkými podniky a telekomunikačními společnostmi, neomezený přístup k informacím jak státního, tak i obchodního významu. Jednou z hlavních povinností CIS byla pomoc NSA při získávání informací pomocí speciálních technických prostředků a prolamování cizích šifer. Získané informace se posílaly do hlavního štábu NSA, kde se analyzovaly. Později všechny tyto operativní aktivity převzala NSA včetně jejich plánování a provádění[11].

V roce 1970 se ředitel NSA Heiler přiznal, že úspěchy agentury jsou z velké části založeny na shromažďování a analýze informací, které byly získány kradením šifer. Zajímavý byl v tomto případě postoj FBI, které nechtělo spolupracovat při získání šifer „nelegální" metodou. Šéf FBI Hoover dokonce odsoudil nezákonné pronikání na území zahraničních velvyslanectví a informoval vedení NSA o tom, že FBI bude pracovat s NSA v tomto směru pouze na přímý rozkaz prezidenta USA[12].

Vývoj speciálních nástrojů pro odposlech vedl k tomu, že v USA fakticky existoval rozpor mezi skutečnou činnosti NSA a zákonem. Téměř čtvrt století činnost NSA byla natolik utajená, že nesměla být jmenována v souvislosti s jinými organizacemi USA. Tento rozpor se pokusil vyřešit v roce 1976 Kongres a navrhl zákon o odposlechu, který byl v roce 1978 podepsán prezidentem. Avšak v roce 1981 byly práva agentury dále rozšířeny – např. právo na průnik do budov vyslanectví cizích zemí nevydával již prezident, ale nejvyšší státní zástupce apod.[13]



Obr. 9.3: *Antény stanice v Morwenstow [E17]*

[10] Central Intelligence Service.

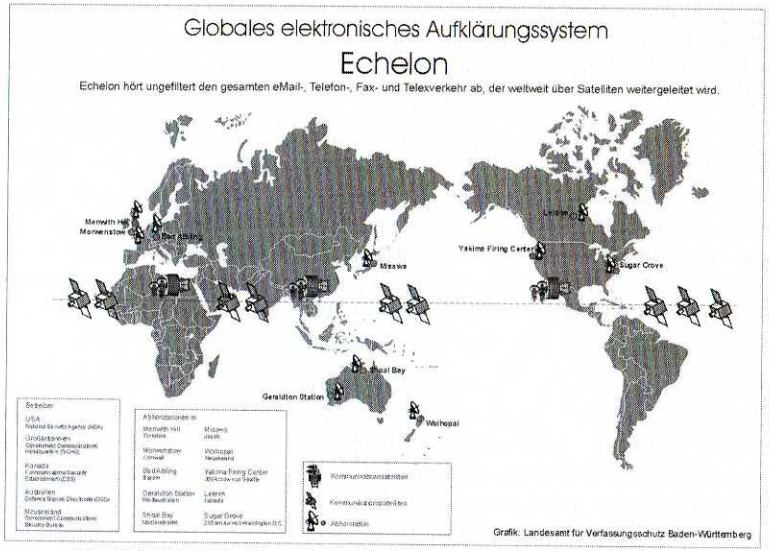
[11] Mezi tyto aktivity patř. např. verbování kryptologů nebo nelegální montáž odposlouchávacích zařízení.

[12] Bezpečnostní služby USA mohly získávat zpravodajskou informaci pouze mimo území USA a na území USA byl třeba souhlas prezidenta (např. se nesměly bez svolení soudu odposlouchávat telefonní hovory amerických občanů). Poté co NSA dostalo 27. dubna 1971 povolení od prezidenta USA provádět odposlech i uvnitř Spojených států, definitivně zvítězilo nad FBI.

[13] I když byla v souvislosti s působením NSA vyvolána řada sporů, většina z nich skončila na ochraně státního tajemství a bezpečnosti USA, např. [N09].

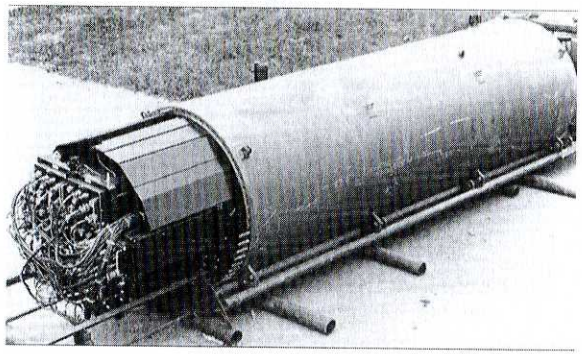
konecma

Největší týchou NSA je systém digitálního odposlechu Echelon, který je schopen zachytávat informace z celého světa, např. NSA kontroluje veškeré informace posílané přes satelity Intelsat[14], což je dáno vysokým počet pozemských stanic odchytávajících signály ze satelitů např. stanice Morwenstow (Velká Británie) zachycuje data ze satelitů nad Atlantikem, Evropou a Indickým oceánem, které pokrývají Evropu, Afriku a Severní Asii a stanice Geraldton (Australie) pokrývá komunikaci nad Asií a jižním Tichým oceánem. Pro zachycení dat ze satelitů, které se nachází nad územím Ruska, bylo vytvořeno speciální centrum poblíž Bad Aibling[15] (Německo).



Obr. 9.4: *Přehledná mapa rozmístění stanic systému Echelon [W06].*

Součástí systému jsou i optické přehledové satelity, které mají rozlišení pozemního objektu lepší než 80 cm[16], např. nad územím Ruska se nachází tři satelity jejichž poloha umožňuje přelet nad libovolným bodem Ruska minimálně dvakrát za den.



Obr. 9.5: *Odbočnice nalezená na podmořském kabelu poblíž Kamčatky [C12]*

[14] Tyto satelity využívají téměř všichni světoví telekomunikační operátoři.

[15] Je to vůbec největší centrum NSA s množstvím satelitních přijímacích antén a technologickými budovami umístěnými v hloubce 25 metrů pod zemí.

[16] Např. satelit označovaný jako Kichoul-11.

Současný systém se velmi odlišuje od toho původního – podle četných zdrojů je schopen zachycovat nejenom telefonní hovory, ale i e-mailové zprávy, přenos dat z internetu, satelitních dat apod., s rychlostí kolem tří miliard zpráv za jednu sekundu[17]. Zachycená informace se nejprve filtruje a pak se dalšími postupy zpracovává. Udává se, že 90 % veškeré informace je zahozeno. Součástí Echelonu nejsou jenom pozemní stanice a satelity, např. v roce 1982 byla objevena odbočnice na jednom transoceánském kabelu mezi USA a Evropou. I když další zařízení objevena nebyla, dá se předpokládat, že to nebylo jediné.

Americká strana dlouho nechtěla existenci Echelonu přiznat i přesto, že vlády Austrálie a Nového Zelandu dopustily existenci tohoto systému. První oficiální zmínka o Echelonu proběhla v roce 1988 a následovně se tímto problémem zabývala speciálně vytvořená evropská komise. Její členové byli překvapeni množstvím faktů, které svědčily o existenci Echelonu a tím, jak jeho síla byla podceňována [W07]. V roce 2000 rozpoutala zpráva skotského novináře Duncana Campbella „Intereception Capabilities" velmi ostré diskuse mezi Evropskou unií a USA. Francouzská vláda obviňovala USA z toho, že USA poskytuje data shromážděná Echelonem americkým společnostem[18].

9.1.3 Ekonomické využití Echelonu

Americký systém Echelon slouží nejenom pro obranné a vojenské cíle, ale je také využíván civilním sektorem. Zejména velké firmy získávají z Echelonu za nemalé poplatky informace související s jejich obchodní činností. Tak např. v roce 1994 byla zachycena informace o jednání mezi firmou Airbus a saúdskoarabskými aeroliniemi o nákupu nových letadel. Součástí odposlechů byly záznamy o telefonních hovorech a faxech přenášených satelitními spoji, ve kterých se mimo jiné objevovala informace o výši úplatků nabízených saudskoarabskému zákazníkovi. Úplná informace byla předána americké konkurenci Airbusu firmám Boeing a McDonnel-Douglas, které následovně kontrakt v objemu cca 6 miliard USD získaly [K04].

Rok předtím zaznamenal systém Echelon videokonferenci mezi José Ignacio Lópezem a nejvyšším představitelem firmy Volskwagen Ferdinandem Piëchem, v níž López nabízel firmě Volkswagen obchodní a technologická tajemství společnosti General Motors (nákupní a výrobní ceny, plány nových vozů apod.). Tyto informace vedly k odhalení José Lópeze a později k aféře šéfa Volkswagenu [L03].

9.2 Technologie Echelonu

Systém Echelon je soubor odposlechových sond a výkonného mechanizmu zpracování získaných informací. Tyto komponenty jsou soustředěny zejména do stanic speciálně zaměřených na mezinárodní telekomunikační satelity, používané telefonními společnostmi většiny zemí. Kromě satelitů a rádia, což jsou hlavní metody přenosu velkého množství veřejných, obchodních a vládních komunikací, je odposlouchávána a zpracovávána i informace, přenášená podmořskými kabely nebo pozemními mikrovlnnými spoji[19].

[17] Ve zprávě Výboru pro zpravodajské služby Senátu USA bylo v dubnu 2002 uvedeno, že systém Echelon provádí 650 milionů odposlechů denně. [H07]

[18] Bývalý ředitel CIA reagoval na tento výpadek prohlášením, že Francie dává úplatky.

[19] Mikrovlnné pozemní sítě jsou tvořeny řetězy vysílacích věží, které si předávají zprávy mezi věžemi v přímé viditelnosti po celé zemi. Tyto sítě zajišťují většinu pozemních komunikací a jejich odposlech zajišťuje přístup jak k mezinárodním podmořským komunikacím, tak i k hlavním mezinárodním komunikačním linkám napříč kontinenty. Zřejmě jsou i cílem rozsáhlého odposlechu vnitrostátních komunikací.

Zatímco zařízení k odposlechu radiových a satelitních komunikací používající velké parabolické antény je poměrně dobře zdokumentována, neboť je obtížné velké anténní systémy delší dobu utajit, síť odposlechu pozemních komunikací, umístěná v budovách podél mikrovlnných tras nebo podzemních kabelů, prakticky zdokumentována není. Zařízení jsou separátně vyvíjena pro různé standardy a obsahují možnost odposlechu starších analogových okruhů převážně používajících frekvenční multiplex včetně separátorů pro moderní digitální okruhy[20]. Všechna zařízení jsou vyráběna a dodávána americkými firmami v jejichž vedení je bývalý pracovník NSA a většina z nich se nachází v Silicon Valley nebo Marylandu. Tato zařízení se identifikují jak AST[21] nebo IDEAS, což jsou firemní názvy dvou hlavních dodavatelů pro systém Echelon.

Prvním krokem analýzy je výběr zájmových kanálů z celého spektra signálů dodávaných z odposlouchávaných satelitů, kabelů nebo mikrovlnných spojů. Pro tento úkol, který se nazývá širokopásmová extrakce signálů, se používá celá řada speciálních zařízení – transpondérů, rozložených po celé trase zpracování signálu. Úkolem transpondérů je mimo vlastní příjem signálu i jeho identifikace a klasifikace a prvotní analýza. Např. model 195 označovaný jako „Wideband snapshot analyser", který je na počátku celého řetězce, odděluje s vysokou rychlostí odposlechnutá data, provádí jejich předběžnou analýzu a předává je dále k jednotce označované „Flexible Data Acquisition Unit". Ta byla schopna na počátku 21. století zaznamenávat, přehrávat a analyzovat data z kanálu pracujícího rychlostí 2,488 Gbit/s[22], což odpovídá např. 40 000 telefonních hovorů[23].

Po prvotní analýze a rozdělení komunikačních kanálů na jejich základní obsahové části přichází na řadu signálové procesory, které vydělí zprávy a signály z požadovaných kanálů – telefonní komunikace, faxová komunikace, datová komunikace mezi analogovými modemy apod. Rychlost práce těchto signálových procesorů je obdivuhodná, např. signálový procesor model 128 byl schopen zpracovat až 16 kanálů E3, což reprezentuje datový tok přes 500 Mbit/s, a vydělit až 480 zájmových kanálů. Jeho následovník v roce 2000, model 132 už byl schopen sledovat až 56 700 kanálů a vydělit z nich přes 3000 zájmových kanálů.

Následující proces zahrnuje filtrování dat a jejich zpracování. Většina těchto operací je prováděna na výkonných pracovních stanicích vybavených speciálním softwarem. Základní zpracování umožňující zobrazení běžných informací o hovoru (číslo volající a volané stanice, typ přenosového protokolu apod.) je možno umístit i na notebook a vydělené kanály přenášet k dalšímu zpracování na vzdálenou stanici vybavenou výkonnější technikou. K přenosu se používá zvláštní šifrovaný standard NSA „Collected Signals Data Format"[24]. Dokonalejší systém „TrailMapper" umožňuje pracovat až s rychlostí 2,5 Gbit/s, analyzovat libovolný typ přenosového systému[25] a předávat k dalšímu rozboru získaná data.

Dalším krokem v řadě je zpracování získaných dat podle toho zda se jedná o hlasovou, telefonní, komunikaci, fax a nebo datovou komunikaci. Tzv. „Data Workstation" je navržena

[20] Pro státy používající americkou normu se základním blokem T1 (24 telefonních hovorů) jsou používána jiná zařízení než pro evropské kruhy pracující se základním blokem E1 (30 telefonních hovorů).

[21] AST obecně znamená, že se jedná o „zařízení určené pro průzkum cizích telekomunikačních signálů na území USA" a označuje společnost Applied Signal Technology, Inc. ze Sunnyvale v Kalifornii.

[22] Rychlost podle standardu SONET OC-48.

[23] Model Model 990 „Flexible Data Acquisition Unit" mohl mít až 48 GB paměti pro operační data.

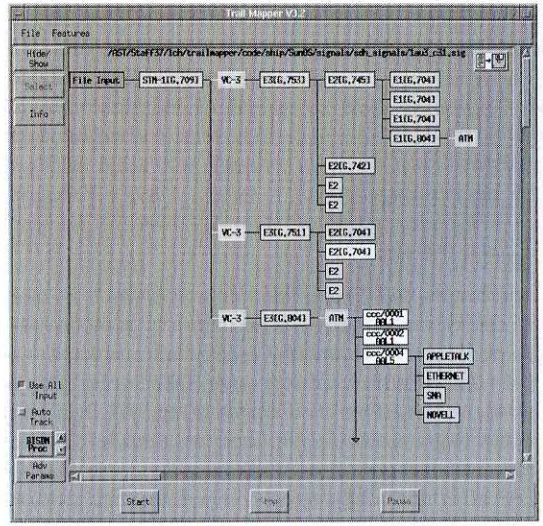
[24] „Collected Signals Data Format" (CSDF) je definován v „US Signals Intelligence Directive 126" a manuálu vydaném NSA. Další publikace NSA, které se k problematice vztahují jsou „The Voice Processing Systems Data Element Dictionary" a „The Facsimile Data Element Dictionary" pocházející z roku 1997.

[25] TrailMapper byl původně navržen pro analýzu přenosových systémů používajících technologii ATM.

tak, aby dokázala kategorizovat všechny aspekty datové komunikace včetně zpracování mailových zpráv nebo přenosu souborů po internetu. Původní datové stanice byly schopny zpracovat až 10 000 různých signálů, avšak v současné době se předpokládá kapacita mnohem vyšší.

Faxové zprávy jsou analyzovány pracovní stanicí označovanou „Fax Image Workstation", která je navržena pro extrémně rychlou analýzu uloženého obrazu. Ačkoliv neexistuje exaktní popis zmiňovaného systému, zcela určitě je použit OCR[26] software, kterým se převádí grafický dokument do textové podoby zpracovatelné následujícími „slovníkovými procesory". Bohužel OCR software neumožňuje rozpoznání ručně psaných dokumentů, a tak je jejich zpracování obtížnější i s ohledem na počet jazyků, které systém sleduje. Existují i názory, že s ohledem na obtížnost rozpoznání ručně psaného textu jsou faxové zprávy psané rukou poměrně bezpečné.

Další pracovní stanice jsou orientovány na výběr zpráv z komerčních pagingových systémů (stanice je označována jako „Pager Identification and Message Extraction") nebo na sledování videokonferencí – zařízení označované „Video Teleconferencing Processor" je schopno současně zaznamenávat až dvě videokonference najednou. Přestože systémy umožňující sledování GSM komunikace nejsou prezentovány dvěma hlavními dodavateli NSA, jejich použití je v současnosti nesporné. Na tom je rovněž vidět, jak se úloha odposlechových systémů pomalu přesouvá od svého původního cíle – sledování vojenské a diplomatické komunikace, do oblastí bezprostředně souvisejících s ekonomikou a občanskou komunikací[27].



Obr. 9.6: *Výstupní obrazovka programu „Trailmapper" ukazující automatickou detekci jednotlivých kanálů a protokolů v digitálním přenosovém systému STM-1 [C12]*

Základní metodou práce systému Echelon je analýza provozu, která je zdrojem prvotních informací i v případě, že se jedná o komunikaci šifrovanou. Z provozu jsou vydělena data identifikující volající a volanou stranu a některé statistické ukazatele, např. v případě telefonního hovoru jeho délka, denní doba apod. Tyto informace slouží pro vytvoření vzorku, který je dále analyzován, dáván do souvislostí s ostatními podobnými hovory a vytvářeny

[26] OCR – „optical character recognition".

[27] Obvykle se to zdůvodňuje bojem proti terorismu, což je bohužel poměrně silný a pravdivý argument.

sítě personálních asociací[28]. Vytváření sítí personálních asociací a jejich hloubkové analýzy jsou principální metodou analýzy telefonních hovorů v systému Echelon.

konecma

9.2.1 Vyhledávání zájmových informací

Tam, kde se nejedná o telefonní hovor, ale o komunikaci, která může být převedena na strojově zpracovatelný text, přichází na řadu metoda vyhledávání klíčových slov na tzv. „slovníkových počítačích". Echelon používá dva základní typy analýzy – prohledávání řetězců a tématickou analýzu[29]. Každá z těchto metod má své výhody a omezení.

Prohledávání řetězců není nic jiného než operace prováděná nad tokem dat, kdy je porovnáván tento tok bit po bitu s předloženým souborem vzorků. Nakolik se zdá tato operace časově náročná, organizace systému Echelon umožňuje paralelní distribuované zpracování ve výkonných vyhledávacích strojích[30] umístěných na sledovacích stanicích systému Echelon. Jednotlivé seznamy vyhledávaných slov jsou rozděleny do kategorií, na něž je odkazováno čtyřmístnými čísly. Každá z agentur má přiděleny určité kategorie podle toho, za jakou část zpravodajských informací v rámci zpravodajské sítě zodpovídá a pracuje asi s 10 až 50 klíčovými slovy v každé kategorii. Klíčová slova zahrnují jména zájmových osob, lodí, organizací, zemí a názvy sledovaných subjektů. Součástí slovníku jsou i známá telefonní a faxová čísla, internetové adresy jednotlivců, obchodních organizací a vládních úředníků, kteří jsou terčem sledování. Tato slova jsou většinou součástí textu zprávy, a tak jsou počítačovými slovníky snadno rozpoznána.

Agentury rovněž specifikují specifické kombinace klíčových slov, aby se usnadnilo vyhledávání požadovaných informací podobně jako v internetových vyhledávačích. Mohou hledat např. diplomatické kabelogramy, které obsahují kombinaci vybraných slov nebo naopak, které obsahují jistou kombinaci slov a neobsahují jiná slova. Slovníky mají na starosti „slovníkoví manažeři" v jednotlivých agenturách, kteří je pravidelně aktualizují na základě nových požadavků. Vyhledávací rychlosti jednotlivých strojů se liší a podle dostupných informací byl jeden z nejméně výkonných systémů „Pattern Recognition Processor PRP-9800" od firmy Ideas schopen v reálném čase analyzovat tok telekomunikačního kanálu E-3[31] podle slovníku cca 1 000 slov.

Tematická analýza byla rozpracovávána v NSA od osmdesátých let a její základ spočívá na myšlence vložení jisté dávky inteligence do stroje, který by následovně byl schopen asociovat dokumenty podle předložené jednoduché otázky nebo příkazu – např. „Najdi všechny dokumenty související s dodávkami zbraní do země XXX!" nebo „Kdy a kde se setkali XXX a YYY?". V rámci výzkumných prací v oblasti tématické analýzy byla zavedena a patentována metoda označovaná jako N-gramová analýza, která má sloužit k rychlému třídění informací uložených ve strojově čitelné podobě – textu, a to nezávisle na obsahu a jazyku textu [D05]. Její princip je velmi jednoduchý a spočívá v porovnávání dvou textů, kde z jednoho je vyděleno okénko délky N, které se posouvá přes druhý text[32]. Přitom se sleduje kolikrát dojde ke shodě textu v okénku s předloženým textem. Jednoduchost metody umožňuje její implementaci v reálném čase nejenom na textové soubory, ale i zvukové nebo video soubory, resp. toky dat.

Počítače provádějící analýzy textů jsou propojeny komunikačními linkami, po nichž se přenášejí zašifrované informace do databází v ústředích pěti agentur[33], sdružených v alianci UK/USA. Každá agentura získává zprávy pouze z jí svěřené oblasti působení a nemá přístup k nezpracovaným zprávám ostatních agentur[34]. Speciálně vyškolení analytici v jednotlivých agenturách mají prostřednictvím kategorizovaných přístupových práv vstup pouze do svého adresáře, kde je uveden setříděný seznam odposlechnutých a zachycených dat náležejících příslušnému analytikovi. Každá zpráva je označena kódem určujícím její charakter, např. zda se jedná o japonské diplomatické kanály z Latinské Ameriky nebo zprávy o Nigérii, distribuci šifrovacích technologií apod.

Analytik vybere svou kategorii subjektů, a tak získá svůj zájmový „výsledek prohledávání", který ukazuje, kolik zpráv bylo zachyceno v síti Echelon o tomto subjektu. Následovně je těmito zprávami možno listovat, a pokud se zpráva zdá analytikovi zajímavá, vybere ji a začne zpracovávat. Pracovní statistiky ukazují, že jeden sběrný systém v Echelonu může generovat asi milion záznamů za půl hodiny. Kanálové filtry odstraní většinu záznamů a k dalšímu zpracování jich přejde cca 6 500, z nich je vybráno cca 1 000 záznamů splňujících další kritéria. Pouze deset z těchto vybraných záznamů je běžně vybráno analytiky k dalšímu studiu a z objemu zachycených informací je zpracována pouze jediná analytická zpráva.

9.2.2 Hlasové a šifrované kanály

Nakolik se zdá celý systém výkonný a unikátní, existuje několik slabých míst, v nichž technologie dosud neposkytuje natolik pozitivní výsledky, jak by mohlo být očekáváno[35]. I když se technologie stále vyvíjí, jedná se o omezení vycházející spíše z teoretických studií než o omezení pouze technologická. Do kategorie slabých míst můžeme zařadit tři oblasti – strojová analýza telefonního hovoru a vyhledání klíčových slov, identifikace mluvčího a šifrované kanály.

Více než 40 let usiluje NSA o implementaci systému, který by automaticky vydělil z proudu dat telefonní hovor zájmové osoby a vyhledal v něm klíčová slova. I když se zdá, že v době, kdy jsou uváděny na trh jednoduché hlasem ovládané stroje nebo diktovací systémy pro PC bude realizace takového systému snadná, není to tak jednoduché. Problém spočívá v tom, že zpravodajské aplikace, na rozdíl od diktovacích systémů, musí pracovat s rozsáhlou množinou mluvčích a jazyků, kde výslovnost zájmové osoby nebylo možno předem „natrénovat". Navíc, každý z nich má jistou fyziologickou diferenci mluvidel, existuje celá řada dialektů nebo vad řeči. Pro zpravodajské systémy, kde neexistuje předchozí znalost o tom, co bude řečeno ani v jakém jazyce to bude řečeno, odposlechnuté signály mohou být zatíženy zkreslením, hlukem z prostředí nebo pouze šumem při příjmu a zpracování, jsou systémy rozpoznávání klíčových slov ve spontánní řeči příliš zatíženy chybami, než aby byly ve větším rozsahu použitelné[36].

---

[28] Prakticky to znamená přehled o tom, kdo a s kým komunikuje. Tento ukazatel má mnohem vyšší důležitost, než by se na první pohled zdálo, a odkazy na samospasitelnost šifrování obsahu hovorů pozbývají v této souvislosti váhy.

[29] V původním označení „topic analysis".

[30] Např. v osmdesátých letech byl pro NSA vyvinut speciální rychlý procesor označovaný FDF (Fast Data Finder), který byl později odtajněn a používán firmou Paracel ve speciálních databázových systémech vyráběných pro jiné vládní organizace USA. Paracel označoval tyto stroje jako „nejrychlejší a nejpřesnější systémy pro adaptivní filtraci dat".

[31] E-3 je Evropský telekomunikační standard označující kanál s přenosovou rychlostí 34 Mbit/s.

[32] I když tato metoda byla autorem označena jako sémantická analýza, do podstaty sémantické neboli významové analýzy má ještě velmi daleko. Její hlavní předností je jednoduchost a tedy i možnost implementace v reálném čase.

[33] Tato ústředí jsou podle dostupných informací ve Washingtonu, Ottawě, Cheltenhamu, Canberře a Welingtonu.

[34] Přístup na jednotlivých stupních je striktně řízen a kontrolován. I když ostatní agentury mohou požádat o slovníky těch ostatních, není to jednoduchá procedura a ne vždy jsou slovníky uvolněny.

[35] Je nutno konstatovat, že veškerá zde uváděná fakta pocházejí z veřejně dostupných informací. Je tedy možné, a více než pravděpodobné, že technologie používané NSA v současnosti jsou mnohem dokonalejší a zvládají daleko složitější úkoly, než jaké jsou zde popisovány.

[36] Komerční diktovací systémy obvykle vyžadují trénink, aby si na mluvčího zvykly, než dosáhnout dostatečně malé chybovosti. Pokud mají reagovat na množinu mluvčích vyžadují většinou kvalitní signál a očekávaný slovník mluvčích. I když současné metody rozpoznávání souvislé řeči naznačují možnosti takového použití [P06, J05], rutinní nasazení v Sigint systémech bude pravděpodobně zatím omezené.

konecma

Jako příklad lze uvést použití metody Markovovských modelů[37], které byly testovány na vzorku několika tisíc telefonních rozhovorů vedených v americké angličtině. Pravděpodobnost nalezení 22 klíčových slov se pohybovala mezi 45 až 68% s deseti nesprávnými identifikacemi klíčového slova na jedno takové slovo za hodinu. Převedeme-li tyto údaje do rozsahu slovníků používaných systémem Echelon, tedy asi 1 000 slov, pak při hodinové konverzaci dostaneme asi 220 falešných poplachů[38] a 300 klíčových slov nebude zjištěno vůbec. To jsou hodnoty pro Sigint systémy nepoužitelné. I když se tato cesta zdá obtížná, NSA se nevzdává a rozšířila výzkum do oblasti tématické analýzy hlasových kanálů.

S podobnými problémy se setkává i automatická identifikace mluvčího na jejímž vývoji pracují různé firmy pro NSA již od roku 1993. I v této oblasti však je stav věcí nejpřísnějšího utajení, neboť podle zákona musí být jakákoliv informace značena jako „tajná", pokud její obsah vykazuje „významný pokrok mezi technikami známými ve vědecké komunitě".

Již od čtyřicátých let se NSA pokoušela o narušení bezpečnosti kryptografických systémů používaných v Evropě. Mezi její priority patřila švýcarská firma Crypto AG, která byla významným dodavatelem šifrovacích strojů a metod pro evropské země a jež těžila ze své pozice v neutrálním státě[39]. NSA se podařilo narušit tento kódovací systém a po jistou dobu zcela nerušeně dekódovala diplomatickou poštu více než 130 zemí. Jako obvykle se nejednalo o selhání technologie, ale svoji roli v celé tajné akci sehrála žena, kryptoložka NSA Nora L. MacKebee.

V sedmdesátých letech se pokoušela firma Crypto AG převést svůj šifrovací stroj na mikroelektronickou součástkovou základnu a v této věci spolupracovala s výrobci mikroprocesorů a integrovaných obvodů. Firmu navštěvovali konzultanti odborných firem počínaje specialisty na návrh elektronických obvodů a konče odborníky v šifrovacích postupech. Jedním z nich byla i Nora L. MacKebee[40], údajně bývalá kryptoložka NSA. Mezi konzultanty se pravděpodobně pohybovalo více agentů, avšak z veřejných pramenů vyplývá, že právě NSA se podařilo změnit šifrovací algoritmus ve svůj prospěch a několik desetiletí bez problémů sledovat diplomatickou poštu [M07].

Cíl intervence NSA byl jednoduchý – zatímco se kódovací systém musí zdát ostatním kryptologům spolehlivý, musí mít slabinu ve prospěch NSA. Základem pro práci stroje byl dlouhý numerický klíč, který musel uživatel nastavit před použitím stroje a dynamicky ho měnit. Tyto klíče si každý uživatel volil sám, a tak by byly NSA nedostupné. Agentce MacKebeeové se podařilo přesvědčit designéry, aby šifrovací klíč byl přenášen vždy před posílanou zprávou ve zvláštním velmi silném šifrovacím režimu, který by nebyl uživatelům znám. Zato byl znám NSA, a tak u každé zachycené zprávy nejdříve byl dešifrován klíč[41] pomocí algoritmu známého NSA a pak byla snadno dešifrována následující zpráva. Informace z takto šifrovaných zpráv tak mělo NSA k dispozici někdy ještě rychleji, než jejich řádný adresát.

[37] Jedná se o tzv. Markovovské modely se skrytými parametry, kde jr systém modelován na základě pozorovatelných vnějších parametrů a předpokládá se o něm, že je Markovovský. Z pozorovatelných parametrů jsou za daného předpokladu určovány skryté parametry systému. Nekdy jsou jednodušší varianty této metody označovány jako dynamické Bayesovské modely.

[38] Termín používaný pro případ, kdy je zjištění oznámeno, ale klíčové slovo nebylo nalezeno.

[39] Mnoho vlád zcela oprávněně nedůvěřovala produktům nabízeným mocnostmi a tak švýcarská firma těžící z pozice Švýcarska během světových válek a jeho integrity byla vítanou variantou.

[40] Bob Newman, inženýr z firmy Motorola uvádí, že se několikrát setkal na schůzkách s pracovníky firmy Crypto AG, kde byl přítomna i Nora L. Mackebee, ale nikdy ho nenapadlo, že by byla agentem zpravodajské služby USA [S04].

[41] Klíč byl přenášen v zakódované formě v servisní části zprávy a byl označena jako „hilfsinformationen", pole sloužící k přenosu pomocných informací. Ty byly však pomocí pouze pro NSA.

Stejný postup použilo NSA v polovině 90. let, kdy vznikly obavy z používání bezpečnostních šifer zabudovaných do softwarových produktů firem Microsoft, Netscape a Lotus. Oslovené firmy souhlasily s úpravami software, které povedou ke snížení bezpečnosti kódu v aplikacích prodávaných mimo území USA. Např. pro Lotus Notes to znamenalo snížení délky šifrovacího klíče na 64 bitů, což technologii NSA umožňuje dešifrovat potřebnou informaci nejdéle během několika měsíců. Navíc, firma Lotus zabudovala na žádost NSA do systému Lotus „zadní dvířka" přidáním informačního pole WRF („workfactor reduction field"), které obsahovalo 24 bitů ze 64bitového klíče použitého pro šifrování mailové korespondence mezi uživateli mimo Spojené státy[42]. Toto pole bylo kódováno metodou veřejného klíče, jejíž detaily byly známy pouze NSA. Dešifrování „tajné" komunikace pak bylo pro NSA otázkou několika sekund [L04]. Podobný systém je zabudován do všech exportních verzí browserů firem Microsoft a Netscape. Oba, podle specifikace, používají 128bitový šifrovací klíč, avšak s každou zprávou je přenášeno prvních 88 bitů použitého klíče, tedy pouze 40 bitů je „tajných". Podle dostupných zdrojů má téměř každý počítač v Evropě tedy zabudován standardní vlastnost – „NSA workfactor reduction system", který usnadňuje NSA (a pouze NSA) prolomení šifrovacího kódu a zjišťování obsahu „zabezpečené" korespondence.

9.2.3 Odposlech Internetu

Internet sám o sobě byl původně sítí navrhovanou pro armádní používání a byl také sponzorován ministerstvem obrany USA. Dramatický nárůst internetové komunikace a její přerod v celosvětovou komunikační síť vedl samozřejmě i k rozvoji metod a postupů při sledování internetové komunikace. Pro americké Comint služby má jednu nespornou výhodu – významná část přenosové kapacity se nachází na území Spojených států nebo se na toto území připojuje, a tak i významná část celosvětové komunikace prochází síťovými uzly ležícími na tomto území.

Směrování v síti internet je mimo jiné i závislé na obsazenosti jednotlivých tras. Vzhledem k časovému posunu mezi Evropou a Spojenými státy pak může dynamické směrování přesunout paket z jednoho evropského uzlu do jiného např. přes uzel v Kalifornii, protože provoz je v té době na území spojených států minimální a přenosové trasy jsou volné. Všechna tato fakta vedou k tomu, že na území Spojených států je k dispozici značný objem tranzitního internetového provozu.

Odposlech internetového provozu může být realizován buď na mezinárodních komunikačních trasách (např. satelitní spoje) nebo v hlavních internetových uzlech. Zatímco odposlech komunikačních tras může zůstat utajen, zřízení odposlechu v internetovém uzlu může být snadno prozrazeno. Nicméně právě druhá varianta poskytuje přístup k většímu objemu dat za použití jednodušších třídících postupů. Enormní objem dat je významně redukován faktem, že NSA je zákonem povoleno odposlouchávat pouze provoz, který má svůj počátek nebo je ukončen v cizí zemi, a tak významná část komunikace je „zahozena", aniž by byla zaznamenána nebo analyzována.

Technologie odposlechu je mnohem jednodušší a základem jsou objemné databáze krátkodobých dat, která jsou dále analyzována. Např. podle [C11] americká Defence Evaluation and Research Agency udržuje databázi o velikosti cca 1 TB, kde jsou udržována data vyměňovaná na diskusních skupinách Usenet. Databáze se chová jako kruhová vyrovnávací

[42] Systém Lotus Notes byl používán ve velkém zejména ve Švédsku, kde si pomocí tohoto systému vyměňovaly korespondenci nejenom soukromé osoby, ale i státní organizace a členové parlamentu. Na základě článku [L04], který vedl ke značnému pobouření ve Švédsku, firma Lotus přiznala, že taková zadní dvířka v systému Lotus Notes skutečně jsou.

paměť a jsou v ní k dispozici informace za posledních cca 90 dní. Podobná databáze „Deja News" obsahuje obdobná data vyměňovaná na webových diskusních fórech.

konecma

Zajímavým produktem je prohledávací stroj, který periodicky projíždí webové servery a katalogizuje jejich obsah. NSA má k dispozici i programové roboty, které periodicky kontrolují zájmové webové servery a zkoumají změnu jejich obsahu[43]. Běžný internetový provoz procházející USA je odbočován v hlavních uzlech internetu (IXP – Internet Exchange Points) na území Spojených států a dále analyzován [M07]. Podobně jako ve všech předchozích případech existují smlouvy mezi NSA a hlavními telekomunikačními firmami na území USA, hlavní výrobci software Microsoft, Lotus a Netscape jsou žádání o úpravy exportních verzí svých programů. Tyto skutečnosti byly prokázány během soudního líčení s hackerem, který se pokusil proniknout do počítačů amerických leteckých sil a jako důkazy byly proti němu použity odposlechy internetového provozu předložené svědkem z NSA. Později, když byl požádán, aby prokázal způsob jak tyto záznamy získal, a tedy uveřejnil metodu odposlechu internetu používanou NSA, odmítl tyto důkazy poskytnout a celé řízení bylo zrušeno [C13].

9.3 FAPSI a SOUD

Studená válka však nedala příležitost jenom západním spojencům, ale obdobné aktivity byly vyvíjeny i na druhé straně železné opony. Sovětský svaz však začal o něco později a to sloučením dvou oddělení KGB, osmého (bezpečnost komunikace) a šestnáctého (elektronické zpravodajství). Vedoucím projektu byl Nikolaj Nikolajevič Andrejev, kterého v roce 1973 vystřídal Igor Vasiljevič Maslov. Zrození globální odposlechové agentury procházelo různými peripetiemi a organizací, která bezprostředně předcházela jejímu vzniku, byla Komise státní komunikace, která vznikla po rozdělení KGB v srpnových událostech 1991[44]. Následovně, během necelého roku, byla vytvořena FAPSI[45]. Generálním ředitelem byl jmenován A. V. Starovojtov. Oficiální znak FAPSI však byl určen až v roce 1999 nařízením prezidenta Ruské federace číslo 338. FAPSI[46] je nezávislý federální orgán s výkonnou pravomocí, spadá přímo pod pravomoc prezidenta Ruska a je vlastně ruským ekvivalentem americké NSA.

Štáb FAPSI se nachází na náměstí Dzeržinského v Moskvě v hlavní budově dnešní FSB[47]. Velká výzkumná laboratoř se nachází v Kuncevo nedaleko hlavního města. Významným úkolem FAPSI byla ochrana informací a první systém této ochrany byl vytvořen v Sovětském svazu v roce 1973. Vzhledem ke globální politické situaci tento systém pracoval především pro Ministerstvo obrany a vojensko-průmyslový komplex. Ochrany informací se zde dosahovalo především za pomoci principu maximálního utajení čehokoliv, což vedlo k tomu, že přístup k některým informacím byl neprávem blokován. Přitom v Sovětském svazu neexistovaly jakékoliv zákony, které by určovaly práva pro přístup např. k osobním údajům. V té době byla ztráta informace v Sovětském svazu byla prakticky nemožná. Dnes jsou případy, kdy informace státního významu je prodávána jiným státům, téměř na denním pořádku, i když je nutno podotknout, že od nástupu prezidenta Putina se situace zlepšuje[48].

Situaci v ruských službách dokresluje případ z devadesátých let, který byl široce rozebírán v tisku. Základ aféry spočívá ve výjimečném postavení FAPSI, která přesto, že ruské zákony zakazují vládním zaměstnancům účast v podnikání, má v tomto případě výjimku. Za jejího přispění byly založeny dvě stínové společnosti, Simaco a Roskomtech, které vedl Valerij Monastyreckij, od roku 1994 ředitel ekonomického úseku FAPSI. Boj o moc v ruské rozvědce vyvrcholil zatčením Monastyreckého dne 12. dubna 1996 pro zneužití pravomocí. Argumentem ruské kontrarozvědky bylo, že krátce před zatčením začal pracovat pro německou BND. Po svém zatknutí obvinil Monastyrecký ředitele kontrarozvědky Barsukova z toho, že chtěl do vládních úřadů namontovat odposlechová zařízení od společností spojených se CIA. Na veřejnost se dostaly i informace o zneužití pravomoci dalších vrcholových představitelů FAPSI.

Stejně jako i její americký protějšek FAPSI je naprosto uzavřená speciální služba, která pracuje v oblasti zpravodajství. Pracovníci FAPSI veřejně mluví pouze o jedné straně činnosti služby – ochrana informace, a přitom zcela opomíjejí druhou a podstatnější stranu, zpravodajskou činnost FAPSI. Na rozdíl od FSB (bývalé KGB) neprošla bezprostředně po rozpadu Sovětského svazu velkými organizačními změnami, počet pracovníků[49] této organizace je mnohem větší než u FSB a jiných speciálních služeb a má dokonce i vlastní vojska. FAPSI pracuje zejména v rámci Ruské federace, v zahraničí těsně spolupracuje s SVR a GRU[50]. Podává denní zprávy přímo prezidentovi. Z celkového počtu zpravodajských informací přijímaných prezidentem téměř 80 % pochází ze zdrojů FAPSI. Podobně jako NSA, FAPSI nepracuje jen pro státní a vládní instituce, ale také vykonává placené služby pro privátní zákazníky. Informace získané FAPSI jsou využívány v rámci vojensko-průmyslového komplexu, vědecko-výzkumnými institucemi a ruskými průmyslovými či obchodními firmami a bankovním světem. FAPSI je také aktivní v rámci státního a mezinárodního kryptografického trhu.

V oblasti „informační války" plní FAPSI jak obranné, tak útočné úkoly. Na jedné straně hraje ústřední roli v ochraně ruské informační a komunikační sítě, na druhé straně se pokouší získat tajné informace infiltrováním se do vnitřních komunikačních systémů zahraničních společností a vládních institucí. Shromažďuje komunikační hardware, kryptologické algoritmy a další s tím spojený materiál, čímž se snaží udržet kontakt s posledním rozvojem pokrokových komunikačních technologií a bezpečnostních vynálezů a metod. Podle původního zákona je hlavní činnosti FAPSI zřizování a zajišťování provozu, bezpečnosti, vývoje a zdokonalování telekomunikačních spojů pro státní orgány, ochrana státního tajemství, zřizování a provoz kryptografické báze komunikace uvnitř Ruska i v zahraničí a zejména zpravodajská služba s využitím telekomunikačních technologií. Součástí těchto služeb je poskytování informací, které mají důvěrnou povahu a jsou nezávislé na jiných zdrojích - jedná se jak o vojenské informace, tak i politicko-ekonomické informace. Tyto

[43] Např. webový server http://www.jya.com/crypto.htm, který nabízí rozsáhlé otevřené materiály obsahující informace o aktivitách Sigint, Comint a kryptografických novinkách, je pravidelně prohlížen „robotem" z NSA, který zjišťuje přítomnost nových souborů a v případě, že je najde ihned je zkopíruje [C11].

[44] Předsedou komise byl jmenován A.V. Staravojtov, zákon o zřízení komise pro státní komunikace podepsal Michail Gorbačov 10. října 1991.

[45] FAPSI – Federalnoje agenstvo pravitelstvennoj svjazi i informacii, Federální agentura státní komunikace a informace.

[46] 11. března 2003 prezident Ruské federace podepsal nařízení, které oficiálně zrušilo FAPSI a na její bázi vytvořilo Službu speciální komunikace a informace (Služba specialnoj svjazi i informacii pri Federalnoj službě ochrany Rossijskoj Federacii), která je podřízena Federální službě obrany Ruské federace. Nicméně i nadále budeme používat název FAPSI, protože úkoly ani metody se nezměnily.

[47] Dříve KGB.

[48] Není bez zajímavosti, že sám Putin má úzké vazby na ruské tajné služby. Po skončení studií práv na leningradské univerzitě nastoupil v roce 1975 do KGB, kde působil především jako agent v Německé demokratické republice. V roce 1990 se vrátil do Ruska a nastoupil na petrohradskou univerzitu jako zástupce rektora. Když v roce 1996 odešel z Petrohradu do Moskvy, dostal se do čela Federální bezpečnostní služby, nástupkyně KGB a předsedal i důležité Bezpečnostní radě Ruské federace.

[49] Odhaduje se, že FAPSI jenom v elektronickém zpravodajství zaměstnává více než 40 000 osob.

[50] SVR – Sluzhba Vneshney Razvedki (zahraniční rozvědka), GRU – Gosudarstvennoje Razvedovatelnoe Upravlenie (státní zpravodajská služba).

informace mají sloužit pro potřeby rozhodování v oblasti státní bezpečnosti, ekonomiky, vědy a techniky, mezinárodních vztahů a ekologie.

FAPSI, podobně jako NSA, má téměř neomezená práva a žádná jiná státní organizace nesmí zasahovat do její činnosti. Podobně jako tomu bylo v Sovětském svazu, pracovníci FAPSI nikdy nesmí opustit Ruskou federaci a součástí jejich přijímací procedury je podpis oficiálního dokumentu se závazkem nikdy neopustit území Ruské federace. I když FAPSI musí postupovat podle zákona[51], skutečnost je jiná. Podle některých zdrojů jsou všechny telefonní hovory, všechny e-maily a poštovní korespondence zachytávány a analyzovány. Situace je o to horší, že v zemi panuje totální kontrola státního aparátu a FAPSI se tak stalo nesmírně mocným nástrojem kontroly nad procesy probíhajícími v Rusku.

Nehledě na konec studené války, zájem Spojených států o získání informací z Ruska nepohasl. Jedná se nejen o informace státní povahy, ale i průmyslové a vědecké informace. Početné vědecké skupiny FAPSI neustále pracují na zdokonalení kryptografických metod. Podle nepotvrzených zdrojů pracují v této oblasti nejlepší ruští matematici, jejíž jména jsou však zcela utajena. I když mají k dispozici naprosto všechno na co mohou pomyslet, nemají žádnou vlastní identitu, žijí pod smyšlenými jmény v naprostém utajení.

SOUD – Sistema objedenonovo učota dannych o protivníkově neboli systém sjednoceného shromažďování dat o nepříteli vznikl podobně jako Echelon v době studené války. Smlouva o vytvoření systému SOUD mezi zeměmi východního bloku byla podepsána v roce 1977 a naplno začal systém pracovat teprve od roku 1979. Spouštěcím momentem pro vytvoření SOUDu byly Olympijské hry v Moskvě v roce 1980 a jeho prvním úkolem bylo shromažďování informací o možných nepřátelských akcích západních tajných služeb během her. Členy SOUDu byly v této době tajné služby SSSR, Bulharska, Maďarska, Polska, Československa, Mongolska, Kuby, NDR a Vietnamu. Databáze SOUDu byla přístupna pouze pro nejvyšší pracovníky speciálních služeb zemí Varšavské smlouvy a obsahovala údaje o agentech, nepřátelských organizacích, novinářích, kulturních a obchodních atašé, pracovnících leteckých společností – o všech osobách, které mohly být potenciálně nebezpečné pro Sovětský svaz. Doba zpracování dotazu nepřesahovala 4 hodiny, což je na technologii konce sedmdesátých let velmi dobrý výsledek.

Hlavní štáb SOUDu sídlil v Moskvě a komunikační rádiové spojení zajišťovalo propojení s ostatními částmi SOUDu, které sídlily buď na sovětských ambasádách v zahraničí nebo měly k dispozici své vlastní objekty. Hlavní výpočetní systém byl rovněž v Moskvě a radiovým spojem byl propojen s druhým výpočetním systémem umístěným v tehdejší NDR. SOUD rovněž vybudoval velkou odposlechovou stanici na Kubě, která měla monitorovat dění na americkém kontinentě. Komunikační kanály SOUDu byly převážně používány pro přenos diplomatické pošty, avšak část provozu obsahovala i zprávy výpočetního systému.

Po sjednocení Německa se výpočetní systém na jeho území rychle dostal pod kontrolu BND stejně jako archivy východoněmecké tajné služby STASI. Změny v Evropě vedly k omezení provozu SOUD na několik zemí, mezi něž patřily např. Vietnam a Kuba. Od roku 1996 je komunikační struktura SOUD používána ruským ministerstvem zahraničí a SVR. Operátory SOUDu jsou přeskupená FAPSI a GRU (Gosudarstvennoe razvedovatelnoe upravlenie – státní zpravodajská služba).

[51] Zákon o federálních orgánech pro státní telekomunikace a informace.

10.

Sociální inženýrství

Kdybych měl vybrat motto této kapitoly, pak bych s největší pravděpodobností neváhal nad známou citací Alberta Einsteina: „Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost; ačkoli tím prvním si nejsem zcela jist". Dějiny sociálního inženýrství jsou dějiny lidské hlouposti a slabin lidského vnímání – vlastností, které jsou po celou historii lidstva dnes a denně zneužívány.

V kultovní knize sociálního inženýrství Kevina Mitnika „Umění klamu" [M08] definuje autor rozdíl mezi podvodníkem a sociotechnikem. Ten, kdo mámí z lidí peníze je obyčejný podvodník, ale kdo využívá manipulace a přesvědčování vůči firmám se záměrem získání informací je sociotechnik[1]. Triviální sofistika, která by určitě neobstála před soudem. Ostatně jak tyto postoje, tak i soudní líčení měly nádech mediální aféry, sloužící spíše k popularizaci Kevina Mitnika. I rozsudek odůvodněný slovy „vyzbrojen klávesnicí je nebezpečím pro společnost" má příchuť spíše marketingového sloganu než suchého zdůvodnění výroku soudu.

[1] V hypotetickém rozdílu mezi sociotechnikem, který není hnán touhou po penězích, ale touhou po zdolávání překážek, získávání nových vědomostí a testování svých možností a podvodníkem spočívala i část obhajoby Kevina Mitnika.

konecma

Nicméně Mitnikova aféra upozornila na jeden z nejslabších článků počítačových systémů – člověka. Tajemství lehkosti překonávání zábran a získávání přísně tajných informací z podniků, úřadů či jiných institucí tkví spíše v osobnosti sociotechnika, která podobně jako osobnost podvodníka musí v prvé řadě budit důvěru. Techniky ovlivňování lidí uváděné v citované knize nejsou nové, jsou jen přeneseny do nového prostředí a důvtipně využívají manipulace prostřednictvím moderních technologií. Mitnick tak ukázal, jak klamná je představa bezpečnosti soukromých i služebních dat, jak snadné je obejít systémy za miliony dolarů zneužitím lidí, kteří je obsluhují.

Americký Computer Security Institute uvedl ve svých výzkumech z roku 2001, že během roku zaznamenalo 85 % dotázaných organizací narušení počítačového zabezpečení a 64 % zaznamenalo ztráty z důvodu počítačových vloupání, a to přesto, že byly uplatněny nejrůznější bezpečnostní technologie. Přesto, že tyto technologie jsou vypracovány do posledního detailu ve snaze minimalizovat riziko spojené s používáním počítačů, zapomíná se na to nejdůležitější – lidský faktor. Iluze založená na myšlence, že bezpečnostní produkty samotné zajistí opravdové bezpečí vychází z mylné představy o síle bezpečnostních technologií – bezpečnost není výrobek, ale proces. Není to jenom technologický problém, ale i problém lidí a řízení. Lze očekávat, že s vývojem stále dokonalejších bezpečnostních technologií, které znesnadňují hledání děr v systému, se budou útočníci stále více zaměřovat na lidské slabosti. Překonání lidské bariéry je častokrát mnohem jednodušší a často vyžaduje investice v hodnotě nákladů na telefonní hovor, nemluvě o menším riziku.

Existuje mnoho definic sociálního inženýrství, které jsou si více či méně podobné. Sociální inženýrství označováno za „umění jak přimět ostatní lidi, aby splnili Vaše přání" nebo za „psychologické triky hrané na oprávněné uživatele systému za účelem získání přístupu do tohoto systému" apod. Obecně však se jedná o zneužití nejslabšího článku, o chytrou a promyšlenou manipulaci přirozené důvěřivostí člověka. Sociotechnik, vystupující pod pseudonymem Harl, k tomu ve vystoupení Access All Areas III dodává: „Na světě neexistuje žádný počítačový systém, který by nebyl závislý na lidech. To znamená, že tato bezpečnostní slabina je univerzální, nezávislá na platformě, síti či druhu vybavení. Kdokoliv, kdo má přístup k jakékoliv části systému, fyzicky či elektronicky, představuje potencionální bezpečnostní ohrožení." [H08].

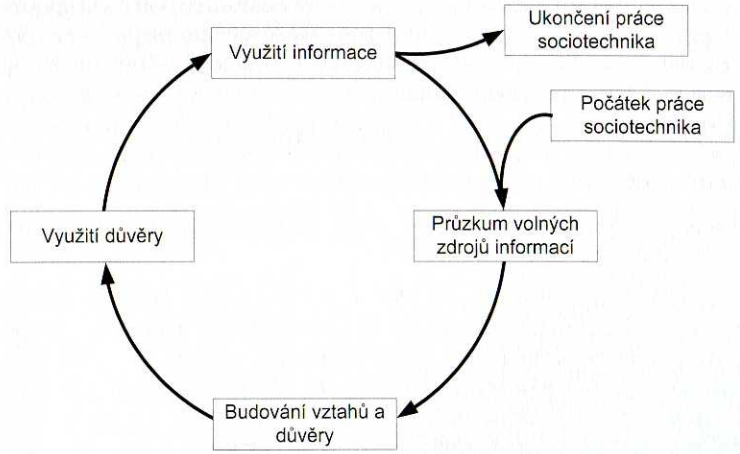
10.1 Metody sociologického útoku

Techniky založené na selhání lidského faktoru nebo využívající podvědomé zvyky a vlastnosti jedince jsou základem sociotechnických metod[2]. Sociotechnik zneužívá slabých míst v bezpečnostní politice firmy, své schopnosti manipulace a vytváření připravených situací. Vlastní práce sociotechnika začíná průzkumem volných a dostupných zdrojů informací, nejčastěji webových stránek firmy, různých marketingových materiálů nebo i inzerátů, viz obr. 10.1. Na základě zjištěných skutečností začíná budovat vztahy s vytypovanými osobami a získává si jejich důvěru, kterou následovně zneužije pro získání potřebné informace. Zde by měl sociotechnický cyklus skončit, avšak mnohdy se opakuje v novém prostředí, neboť získání jedné informace v tomto cyklu nemusí vést k dokončení plánovaného útoku

Sociotechnické útoky se odehrávají ve dvou úrovních – fyzické a psychologické. Ochrana proti sociotechnickým útokům spočívá v dobře zpracované bezpečnostní politice firmy a v jejím důsledném dodržování. V bezpečnostní politice by měly být zahrnuty všechny části firmy, které mohou být vystaveny útoku, a přinejmenším hierarchie důvěrnosti všech dokumentů

[2] Jednou z nejjednodušších a nejpodlejších metod sociálního inženýrství je krádež informací. Ta má svá specifika vycházející zejména z toho, že ukradená informace nikomu nechybí. V tomto textu se však oblastí krádeží informací zabývat nebudeme.

a způsoby, jak s takovými dokumenty zacházet. Sem patří i jednoznačná a jasně formulovaná metoda klasifikace dokumentů[3]. Přitom nesmíme zapomínat, že do kategorie dokumentů je nutno zahrnout i média s citlivým obsahem a uvědomit si, že disketu nebo pevný disk nestačí pouze vymazat. Informace i po „vymazání" na disku zůstává a pomocí speciálních, ale běžně dostupných nástrojů jej lze uvést do původního stavu.



Obr. 10.1: *Sociotechnický cyklus*

10.1.1 Volné zdroje

Pod volnými zdroji je možné si představit informace přístupné veřejnosti, které jsou k dispozici na síti, v tištěné podobě nebo které je možno získat jiným zákonným způsobem, např. dotazem na tiskovém oddělení firmy, uplatněním zákona o svobodném přístupu k informacím[4] apod. Někdy je to až k neuvěření, co všechno lze zjistit použitím internetových vyhledávačů[5]. Užitečné jsou různé databáze, např. „whois", nebo YellowPages, které jsou plné obchodních kontaktů. Podstatným zdrojem jsou webové stránky cílové firmy, její reklamní brožury, obchodní historie apod. V těchto zdrojích se vyskytuje množství jmen, telefonních čísel, emailových adres a dalších, zdánlivě neužitečných informací, které však pro sociotechnika skládajícího tyto útržkovité informace v jeden celek mohou být nesmírně užitečné.

Internet skýtá mnoho možností pro sociální inženýrství a patří k jednomu z velmi užitečných nástrojů sociotechnika, jehož role při vyhledávání informací nemusí být vždy pasivní. Možnost vytvořit stránku tvářící se jako seriózní stránka firmy nabízející uživateli např. za zaregistrování zdarma dárek může sloužit jako trojský kůň k získání hesel zaregistrova-

[3] Otázka jasné metodologie klasifikace dokumentů (důvěrné, tajné apod.) bývá často podceňována. Z obecného hlediska je stejným prohřeškem zařadit dokument do vyšší klasifikace než odpovídá obsahu jako obsah dokumentu podcenit do nižší klasifikace. Zároveň se velmi často stává, že dokument je označen jako „obchodní tajemství", avšak pouze na základě pocitu zpracovatele. Pokud se takové omezení týká odmítnutí předložení dokumentu některému státnímu orgánu, pak je nutno si uvědomit, že pojem „obchodní tajemství" je přesně definován a není možno si do tohoto termínu dosadit cokoliv (viz Část V zákona 513/1991 Sb. – obchodní zákoník).

[4] Zákon 106/1999 Sb. ze dne 11. května 1999.

[5] S těmito informacemi musí sociotechnik pracovat opatrně. I když vyhledávač najde na internetu množství informací, obecně je jejich spolehlivost velmi malá. Sociotechnik musí velmi vážit relevanci takto zjištěné informace vzhledem k ostatním získaným materiálům.

ných obětí[6]. Úspěšnost je poměrně vysoká, podobně jako u podvržených e-mailů při tzv. „phishingu", obvykle okolo 20 %.

konec

Technici a správci sítí nejsou vševědoucí a tráví mnoho času na síti. Proto i tam hledají pomoc kdy narazí na problém, který neznají nebo jej nejsou schopni vyřešit. To jsou otevřené dveře pro sociotechniky, kteří zahrají roli rádce a v dialogu, například internetové diskusi, vylákají z oběti množství informací. I tady nemusí sociotechnik pouze pasivně čekat na příležitost. Pokud již částečně zná prostředí, může problém, který správce musí řešit, sám předem způsobit, a pak už jenom čekat v konferenci. Tomuto postupu se říká reverzní sociální inženýrství a má tři fáze:

- ✓ sabotáž – kdy útočník způsobí závadu v systému,
- ✓ inzerci – kdy nabízí své vědomosti k vyřešení problému,
- ✓ asistenci – kdy skutečně pomáhá závadu odstranit a mezitím získává jinak nepřístupné informace.

Jiným nebezpečím jsou e-maily a jejich přílohy, vesměs vycházející z již známé metodiky „phishingu". V jednodušších případech zabírá e-mail s žádostí o heslo, kde podepsaný autor e-mailu je např. správce firemní sítě (i když skutečným autorem je sociotechnik). Běžné jsou přílohy, které po otevření spustí trojského koně, a tak je získán přístup k potřebné informaci. Základem všech těchto metod je ale získání správné e-mailové adresy cílové osoby. Oblíbený způsob tvoření adres, který vytváří adresu ve tvaru <jméno>.<příjmení>@<emailový server organizace> je tak jednou z největších bezpečnostních děr využívaných sociotechniky.

Jedním z velmi bohatých otevřených zdrojů informací jsou kupodivu odpadky odvážené z firmy. Množství informací, které je možno získat prohledáváním odpadků vyvážených z firmy je až neuvěřitelné a sociotechnik takový bohatý „otevřený" zdroj určitě nevynechá. Mnoho lidí si totiž ani neuvědomuje, co vlastně vyhazují – účty za telefon, výpisy z bankovních účtů, materiály spojené s prací apod. V průměrném firemním odpadkovém koši může být nalezena řada přesných aktuálních informací o stavu firmy, plánech, kontaktech, firemní telefonní diáře, tabulky struktury zaměstnanců firmy, manuály bezpečnostních pravidel, kalendáře schůzek, událostí a dovolených, systémové manuály a výjimkou nejsou ani vytištěné důvěrné informace, přihlašovací jména a hesla do sítě, vytištěné zdrojové kódy, CD-ROMy, diskety a jiná záložní média nebo firemní předtištěné obálky a formuláře, nepoužívaný hardware a mnoho dalšího. Metoda prohledávání odpadků je široce používána nejen sociotechniky, ale i policií při hledání důkazů nebo výzvědnými službami[7].

Pro zkušeného sociotechnika odhalí telefonní diáře odhalí jména a telefonní čísla lidí, za které je možno se potom vydávat. Tabulky struktury zaměstnanců zase ukáží, kdo má ve firmě jaké postavení a bezpečnostní manuály na co je třeba dávat pozor. Kalendáře zase informují, kdo má kdy jakou schůzku[8], kdo a kdy je nebo není přítomen ve své kanceláři. Systémové manuály, vytištěné zdrojové texty, loginy a hesla jsou tím nejlepším „průvodcem",

[6] Většina uživatelů internetových služeb používá stejné heslo pro všechny služby, protože se jim nechce pamatovat více variant. Na takto podvržené stránce stačí nechat uživatele zaregistrovat, vyplnit „bezpečné" heslo a poté s touto databází lidí i s jejich hesly, e-mailovými adresami nebo jinými informacemi zkoušet jejich schránky, další účty apod.

[7] Jakkoli se to zdá nemožné, některé firmy jsou schopny např. vyhodit do odpadků i celá magnetická média, diskety nebo pevné disky, jejichž obsah není ani v nejmenším porušen.

[8] Např. záznamy z knihy návštěv jsou velmi dobrou orientací v obchodní politice firmy, neboť prozrazují její obchodní partnery a zákazníky. Pokud je taková kniha návštěv v elektronické podobě, pak je neocenitelným zdrojem informací pro sociotechnika.

jak napadnout informační technologii firmy. A staré pevné disky a jiné paměti se dají opravit a jejich obsah zrekonstruovat do původní podoby.

10.1.2 Budování důvěry

Průnik do zabezpečené firmy často začíná od získání informace či dokumentu, který je zdánlivě bezvýznamný, je obecně dostupný a nepříliš důležitý. Většina lidí v organizaci tedy nevidí důvod, proč by měl být chráněný a mnoho bezvýznamně vyhlížejících informací může být pro sociotechnika cenných. Nejčastěji je tedy sociotechnický útok zaměřen na osobu, která si neuvědomuje důležitost informací, s nimiž pracuje a které poskytuje jiným. Přitom prvním předpokladem úspěšné práce sociotechnika je předpoklad, že pracovníci firem nejsou žádní hlupáci a očekávání podezíravosti nebo odporu. Na to musí být vždy připraven, a tak plán sociotechnického útoku se připravuje jako šachovou partii, kde je nutno předvídat otázky, jež může oběť klást a připravovat si patřičné odpovědi.

Jednou z typických oblastí práce sociotechnika, po získání předběžných informací z volných zdrojů, je budování pocitu důvěry a vytvoření vztahu s obětí. Sociotechnik si uvědomuje, že jeho práce je časově náročná, že nemůže na oběť „tlačit", a tak se obvykle první rozhovor připravený sociotechnikem týká obyčejných každodenních záležitostí. V situaci, kdy lidé nemají k podezíravosti důvod, si sociotechnik snadno získá jejich důvěru. Pak nastává období vytěžování oběti, kdy tyto zcela obyčejné rozhovory mohou být proloženy nevinnými otázkami vedoucími k získání cílové informace. Mnohdy oběť ani netuší, že se stala zdrojem důležitých informací.

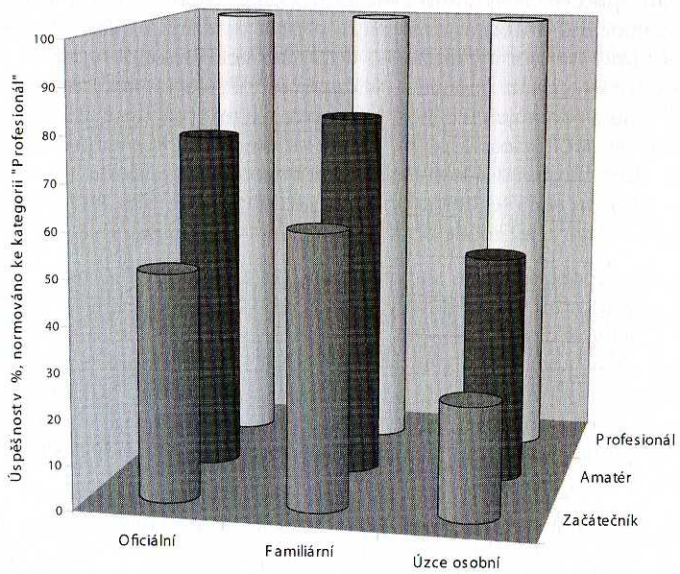
Podstatným a nezanedbatelným rysem práce sociotechnika, který uplatňuje při jednání se svou obětí, je znalost firemního nebo odborného žargonu. To, že správně používá různé výrazy a slovní obraty běžné ve firmě nebo v daném oboru podvědomě pomáhá k přesvědčení oběti, že jedná s někým „známým", s někým ze své firmy. Naopak, pokud se útočník vyjadřuje nejistě a neobvykle, nepoužívá správná označení pro různé služby, věci nebo oddělení, oběť zbystří a útočník se stává jejích očích podezřelý. Proto používání správného žargonu, odkazování se na jména jiných zaměstnanců, sebejisté vystupování a rozmlouvání o běžných pracovních povinnostech patří k základní výbavě zkušeného sociotechnika a vydatně pomáhá útočníkovi k nepozorovanému „pohybu" po firmě.

Součástí sociotechnického útoku je vhodně zvolená komunikační strategie. V zásadě je možno tyto strategie rozdělit na tři základní přístupy, které sociotechnik volí podle svého odhadu mentality cílové osoby:

- ✓ Oficiální komunikační strategie, kdy v rozhovoru není připuštěn familiární tón, celá komunikace probíhá velmi působivě, dělně a seriózně; během tohoto typu rozhovoru nemusí sociotechnik znát osobní údaje o cílové osobě, avšak je nutno, aby komunikace vyznívala velmi profesionálně, tudíž se musí velmi dobře orientovat v odborném zaměření cílové osoby.
- ✓ Familiární komunikační strategie vycházející ze znalostí alespoň některých osobních údajů a rysů cílové osoby; často sociotechnik vyhledává pro tento typ útoku oběť opačného pohlaví a nejednou volí, zejména v českém prostředí, žertovný až flirtující tón. Familiární komunikační strategie vyžaduje nejenom orientaci v prostředí cílové osoby, ale i jisté herecké vlohy, umožňující sociotechnikovi používat modulaci hlasu jako součást zvolené strategie[9].

[9] To se týká zejména komunikace po telefonu nebo jiném prostředku přenášejícím hlas (Skype, Microsoft NetMeeting apod.). Právě u této kategorie, na rozdíl od obou zbývajících, hraje modulace hlasu významnou roli.

- ✓ komunikační strategie úzce osobní spočívající ve vyvolání přesvědčení v cílové osobě, že se dlouho znáte a jste důvěrní přátelé. Jedná se o nejsložitější sociotechnický útok vyžadující řadu podrobných informací o oběti. Tento útok může velmi často selhat na neznalosti nebo nepřesvědčivosti nepatrného detailu, který vyvolá dominový efekt vzrůstající nedůvěry.



Obr. 10.2: *Úspěšnost útoku podle typu komunikace*

Důležitost volby vhodné komunikační strategie vyplývá zejména z toho, že pouze nepatrné procento sociotechnických útoků zahrnuje fyzické setkání sociotechnika a cílové osoby – oběti. Většina útoků je prováděna pomocí telekomunikačních prostředků nebo internetu, což zjednodušuje předstírání totožnosti a manipulaci s cílovou osobou.

10.2 Prostředky a cíle sociotechnického útoku

Pro sociotechnický útok jsou používány nejrůznější kombinace prostředků, metod a prostředí. K základním prostředků sociotechnika patří telefon, e-mail, internetový chat v reálném čase, běžná korespondence (papírová) nebo osobní kontakt. Posledně jmenovaný prostředek byl již označen za jeden z nejvíce rizikových pro sociotechnika, nicméně útočník může zvolit méně ohrožující variantu a s využitím informace o cílové osobě může jednat jejím jménem, proniknout fyzicky do budovy nebo zájmového objektu apod.

10.2.1 Telefonní útoky

Mezi nejstarší metody sociálního inženýrství patří telefonní útoky, které jsou založeny na anonymitě mluvčího. Telefon patří mezi nejoblíbenější a nejúčinnější zbraň sociotechniků; dají se v něm skrýt nebo předstírat emoce a zejména skutečná podoba či identita volajícího. I když se zaváděním signalizace a identifikace příchozího hovoru již není tak jednoduché předstírat jinou identitu a „skryté číslo" je vždy podezřelé, oblíbenost telefonních útoků neklesla. Mezi nejvíce zranitelné části podniku patří „help desk" – informační linky. Pracovníci informačních linek jsou sice trénováni v asertivním chování vůči volajícím a aby byli ochotní, přátelští a podávali informace, nicméně operátorům „help desku" je v podstatě jedno, kdo volá nebo proč potřebuje zrovna ty informace, které si žádá. Jejich vzdělaní v oboru bezpečnosti nebývá věnována ve firmě zvláštní pozornost, dostávají nevelký plat, a tak jednoduše odpoví na otázky a přejdou k dalšímu volajícímu. Pokud není přesně definována bezpečnostní politika pro help-desk a jednoznačně stanovena struktura informací, které mohou být podávány, pak tato část firmy je úplným rájem pro sociální inženýry.

Profesionální sociotechnici s Kevinem Mitnickem v čele se domnívají, že v telefonních útocích mají velkou výhodu ženy. Žena s příjemně znějícím hlasem na druhém konci linky, žádající „drobnou" informaci, má velkou výhodu, zvláště při komunikaci s příslušníkem opačného pohlaví. I když to není pravidlem, v rozhovoru sociotechnika může příjemný hlas být pomocníkem při snaze útočníka vzbudit v oběti důvěru, a naladit se na stejnou vlnu[10]. Nejvýznamnější roli hraje schopnost sociotechnika odhadnout psychické rozpoložení oběti útoku a na něj reagovat. Může nasadit např. ležérní tón konverzace nebo mluvit jasně a přímo, chvíli „poklábosit", mluvit vážně nebo vtipkovat. To vše patří k divadelnímu představení sociotechnika.

Pokud útočník nepoužije techniku přímého dotazu, pak je důležité rozmělnit konverzaci do množství nepodstatných detailů, otázek a odpovědí a mezi tuto „hovorovou vatu" vložit otázky, které nás skutečně zajímají. Sociotechnik nikdy neukončuje hovor ihned potom, co se dověděl pro něj důležité informace, protože volaný si zpravidla nejvíce pamatuje několik posledních okamžiků telefonátu, a tak poslední část rozhovoru je věnována většinou nějaké neškodné konverzaci. Sociotechnik nikdy nenaléhá[11], může to celý útok zhatit a v případě, že se hovor nevyvíjí tak, jak by měl je nutno s použitím zdvořilostních frází hovor nenápadně ukončit. Dobře zvládnout telefonický útok není snadné a vyžaduje to schopnost improvizace a jisté herecké vlohy. Sociotechnik musí být vnímavý na nepatrné odchylky chování oběti nepanikařit, když se hovor nevede podle jeho představ. Cesta k úspěšnému zvládnutí telefonního útoku vede přes dlouhá léta praxe.

10.2.2 Metody přesvědčování obětí

Všechny metody sociotechnického útoku mají společný cíl – přelstít oběť útoku. Mezi základní faktory, které ovlivňují výsledek útoku patří:

- ✓ Schopnost sociotechnika přesvědčit oběť, že je pánem situace, vše dělá ze své vlastní vůle a bude za to odměněna. Přitom odměna nemusí být hmotná, stačí např. dobrý pocit z potěšení nadřízeného nebo z dobrého skutku přátelské výpomoci.
- ✓ Nebýt příliš vtíravý a nevyvíjet velký nátlak na oběť. Ten často vede k podráždění oběti a následnému nezdaru.
- ✓ Být přátelský. Když už všechno selže, tak přátelský úsměv a tón hlasu může pomoci i v jinak prohrané situaci. Většina z nás totiž ráda věří v dobrotu ostatních lidí, ráda věří v poctivost svého kolegy.

S použitím výše uvedených pravidel využívají sociotechnici psychických vlastností obětí, které tvoří prakticky neodstranitelné „bezpečnostní díry". Mezi nejběžnější slabiny v této oblasti, které jsou sociotechniky využívány, patří:

[10] Samozřejmě i opačný efekt je možný, příjemný mužský hlas je významnou pomocí při rozhovoru se ženou.

[11] Výjimkou je případ „silového zájmu", kdy sociotechnik předstírá vysoce postaveno osobnost a předpokládá, že oběť se zalekne a vyhoví jeho přání.

- ✓ Pocit zbavení se odpovědnosti – oběť snáze splní útočníkovo přání, když má pocit, že celá tíha zodpovědnosti neleží jenom na ni. Pro vyvolání takového pocitu stačí zmínit pár dalších jmen spolupracovníků, kteří jsou také zapojeni do celého procesu, nebo prohlásit, že nějaký vyšší nadřízený už vše schválil, a tudíž je vše v nejlepším pořádku.
- ✓ Naděje na lepší postavení ve firmě – když oběť uvěří, že při splnění požadavku dostane nějakou odměnu, vždy ji to pobídne úkol splnit. Odměna může být už výše zmiňované potěšení nadřízeného, získání výhody před nějakým svým soupeřem, nebo jenom potěšení ze slibně znějícího ženského hlasu na druhé straně telefonu.
- ✓ Důvěra – vytvoření pocitu důvěry, jak již několikrát bylo zmíněno, je jedním z nejdůležitějších kroků v sociotechnickém cyklu. Sérií krátkých dialogů a interakcí útočník pomalu buduje důvěru mezi sebou a obětí a doba věnovaná této přípravě se mu vyplácí.
- ✓ Morální povinnost – vyvoláním přesvědčení, že se děje bezpráví a kterému právě oběť může zabránit akcí, kterou útočník vyžaduje.
- ✓ Pocit viny – nikdo se nechce cítit vinen, proto se každý snaží takovýmto pocitům vyhnout. Vytvořením scénáře a situace, které zapůsobí na oběti vytvoří psychický tlak a oběť se bude snažit zbavit pocitů viny, které jsou uměle navozenou situací vyvolány a udělají vše, co je třeba.
- ✓ Touha být užitečný – vrozený altruismus u většiny lidí je vede k dobrému pocitu z vykonaného dobra, a tak ráda někomu pomůže, zvlášť pak muži „bezmocným" ženám.

Pokud sociotechnik zná dobře chod firmy, pak ideálním cílem jeho útoku je nový zaměstnanec. I když třeba toho ještě neví tolik o firmě ve které pracuje, jeho výhodou je, že nezná ještě hodně svých spolupracovníků a pro vyvolání dobrého prvního dojmu ochotně ukazují svoji vůli spolupracovat, jakož i rychlost s níž svěřené úkoly provádějí. Nový pracovník je rád, když o něj někdo, v tomto případě útočník, projeví zájem a snaží se mu pomoci[12]. Na oplátku je pak sám také ochoten vyhovět s nějakou „maličkostí" a ztrácí obezřetnost.

Zvláště účinné a oblíbené je v těchto případech použití autoritativního přístupu. Už samotné jméno někoho z blízkých spolupracovníků vysoké exekutivy společnosti může být dostačující. Uvádění jmen jiných zaměstnanců, např. odvolání na sekretářku generálního ředitele, kdy sociotechnik použije její křestní jméno, je obvykle používáno pro vyvolání dojmu, že máme blízké kontakty s osobou ve firmě vysoce postavenou. Pro takového člověka oběť ochotněji něco udělá, neboť se domnívá, že tím získá nějakou výhodu.

Nejenom nový zaměstnanec je dobrým cílem útoku, také vydávání se za nového zaměstnance a prosba o pomoc je často používána sociálními inženýry. Tento přístup nazýváme obrácením rolí. Je např. běžné, že noví zaměstnanci se dobře nevyznají v obsluze některých programů, a tak správce systému je na takové situace zvyklý a mnohokrát už musel někomu něco vysvětlovat nebo s něčím pomáhat. Tedy situace, kdy se mu útočník v roli nového zaměstnance svěřuje se svými problémy není neobvyklá, a tak trpělivě naslouchá a pomáhá útočníkovi získat to, co potřebuje[13].

[12] A to třeba i v situaci, kterou útočník sám vyvolá.

[13] Podobné je to i s policií. Dobrý sociotechnik se nebojí kontaktu s policií a když je to potřeba, není pro něj problém na policii zavolat a získat informaci, kterou potřebuje.

10.2.3 Útoky nástroji internetové komunikace

Mezi nástroje přímé komunikace patří komunikační nástroje s okamžitým spojením, kam můžeme zařadit např. ICQ, NetMeeting, IRC[14] nebo i webové „chaty". Velmi silným nástrojem přímé komunikace je elektronická pošta. Principy sociotechnické práce, i když se jedná o jiné médium, zůstávají stejné – využití lidských slabostí pro získání požadované informace. A s tím ruku v ruce jdou metody sloužící k vyvolání dojmu, že oběť se rozhodla sama a správně.

Snad nejběžnějším nástrojem k vylákání potřebné informace je elektronická pošta, kde mezi základní metody patří tzv. „phishing", což se česky překládá jako „rhybaření". S touto metodou jsme se již setkali v předcházejících kapitolách, a tak víme, že cílem phishigu je vylákání utajované informace z oběti útoku. Obvykle se jedná o přístupové heslo, číslo kreditní karty nebo jiné údaje podobného typu. Příkladem takového „rhybářského mailu" je text odeslaný klientům České spořitelny, a nejenom jim, vyzývající je k „aktivaci nového systému bezpečnosti vlastních účtů" – viz obr. 10.3. Pomineme-li fakt, že žádný správce bezpečnostních systémů banky by takový mail neposílal, pak je vhodné si všimnout vlastního textu zprávy, který obsahuje řadu slohových i gramatických chyb. Obvykle instituce tohoto typu se snaží hromadně rozesílané dopisy alespoň trochu gramaticky a slohově „vyčistit", avšak text tohoto mailu porušuje základní gramatická pravidla viz např. „všechny naši klienti", „nejsou tyto data". I použití špatné české transkripce anglického termínu „fraud", kterým se označují „krádeže" v telekomunikačním a informatickém prostředí, by mohlo upozornit podivnost tohoto sdělení[15]. Zajímavá je i hlavička mailu, obsahující

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci.
Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku.
Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu.

S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem.
Do 1.listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu.
Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

Vy jste byl (a) zvolen (a) jako jeden z ucastniku finalniho stadia testovani systemu.
V soucasne dobe Vam navrhujeme vyuzit odkaz https://www.servis24.cz/ebanking-s24/
a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system.
V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti.
Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji.

Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu,
v opacnem pripade budou Vase ucty zablokovany do okamziku uplneidentifikace Vasi osoby. Proto doporucujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.

S pozdravem, Oddeleni Banky pro ochranu pred frodem.

Obr. 10.3: *Text „rhybářského" mailu z 11. října 2006*

[14] Některé tyto prostředky jsou rovněž používány pro řízení chování kompromitovaných počítačů, a tak např. k synchronizaci útoků typu DDoS.

[15] I když jsme si již zvykli na označování funkcí a útvarů v českých firmách pomocí nejrůznějších, mnohdy zkomolených anglických názvů, název „Oddeleni Banky pro ochranu pred frodem" je přeci jenom příliš násilné.

zcela nepravděpodobnou cestu případného mailu z poštovního serveru České spořitelny a v neposlední řadě i adresa a stránka, na níž se klient dostane po kliknutí na odkaz v těle mailu – *http://210.211.139.140:9070/index.htm*. V první řadě se nejedná o stránku se zabezpečeným protokolem https, který originální stránka Servisu 24 České spořitelny požaduje a následovně lze zjistit, že adresa serveru nepatří České spořitelně, ale náleží do sítě indické firmy Videsh Sanchar Nigam Ltd., jež poskytuje připojení v Bombaji.

konec cma

Jak uvádějí nejrůznější prameny, výtěžnost „rhybaření" je poměrně vysoká – až 20 % uživatelů se nachytá na různé sliby, potřebu zabezpečení svých účtů apod. Nicméně mnohdy je možno využít i skryté touhy zjišťovat skrytě tajemství druhých. Příkladem je článek na serveru *http://www.robin-skate.estranky.cz*, kde autor nachytal několik desítek uživatelů právě na touhu stát se alespoň na okamžik hackerem [I06].

Při analýze textu citovaného v obr. 10.4 je zřejmé, že základem úspěšného „rhybaření" je důmyslný a dobře napsaný reklamní text působící na psychiku uživatele – v tomto případě na její „temnější" část. Atraktivní téma útoku na cizí mailovou schránku, kdy následovně můžete překvapit svého známého znalostí obsahu jeho mailů nebo přístupových práv, popř. si budete tajně pročítat něčí korespondenci jistě vzbudilo zájem. Následující, pro znalého člověka poněkud nesmyslný, příběh o „správcích v terénu" měl vzbudit důvěryhodnost[16] a poměrně komplikovaný popis formátu e-mailu donutit čtenáře, aby se nad ním zamyslel, a tak nevěnoval pozornost všem souvislostem. Autor měl možnost ovládat funkci webové stránky, a tak vypnul komentáře, aby se čirou náhodou neobjevil negativní ohlas, kdo by na tento chyták upozornil.

Je pozoruhodné, kolik uživatelů na tento trik naletělo, a to i uživatelů zkušených – viz komentáře pod článkem, když je autor o několik hodin později zapnul a dodal k článku vysvětlení. Některé byly peprné, jiné sebekriticky litovaly vlastní hloupost a celý trik oceňovaly. Nejzajímavější byly komentáře, které napadaly autory z trestné činnosti, a zcela opomíjely fakt, že úmysl trestného činu byl zejména na straně toho, kdo chtěl návod uvedený v článku použít[17]. Při bližší analýze textu zjistíme i další záludnosti, např. předmět L4_Tr1N3. Zkušený čtenář hackerské transkripce ihned vidí původní význam La Trine[18] , a to by ho mělo zarazit. Stejně tak požadavek na zaslání hesla k mailové adrese útočníka – v tomto případě je útočníkem ten, kdo používá postupu uvedeného v článku. Nicméně, jak autor následovně konstatuje, na udanou adresu get.password@seznam.cz mu přišlo několik desítek mailů a následovně ho administrátoři Seznamu požádali o stažení článku a adresu zablokovali[19]. Tím sice zkazili autorovi pointu celého příběhu, neboť na přijatý mail se odesílala automatická odpověď „Člověče, příště se zamysli, než uděláš takovou hloupost a pošleš někomu cizímu své vlastní heslo", ale zároveň ukázali, že jsou to správci na svém místě.

[16] Abych pravdu řekl, nevím proč by administrátoři mailové služby Seznamu měli někam jezdit zvláště, když se jedná o neplacenou službu pro veřejnost. A když už by potřebovali v „terénu" zjišťovat hesla věřím, že by nepoužili takový nebezpečný nástroj.

[17] Toto tvrzení není tak zcela pravdivé, protože mailová adresa get.password@seznam.cz patřila autorovi, který se takto stal příjemcem informací o přístupových právech osob, jejichž důvěry zneužil (pokud se na tento mail skutečně odesílaly uvedené údaje).

[18] La Trine je e-zin na serveru http://www.dgx.cz, ale také prostý český výraz pro záchod.

Jak zjistit heslo na Seznam Email

Nechtěl jsem věřit tomu, že to funguje. Jde totiž o neskutečně primitivní trik. Proč dělat povyk kolem bezpečnostních děr Internet Exploreru, když obrovské trhliny zejí úplně jinde? Takže jsem to vyzkoušel...

Cituji:

Tento fígl jsem objevil náhodou, když jsem sledoval při práci admina ze Seznamu. Je to prosté: na server zašle požadavek (speciální email), ten jej vyhodnotí a pošle zpět odpověď. Administrátoři Seznamu to používají při práci „v terénu". Teď prozradím přesný tvar emailu, kterým lze získat heslo k jakékoliv schránce na Seznamu Email.

Email je třeba odeslat na adresu *get.password@seznam.cz*. Jako předmět se musí uvést L4_Tr1N3. Zpráva musí být přesně v tomto formátu:

$src:adresa@seznam.cz (tedy adresa. k níž chcete znát heslo)

auth:vase_adresa@seznam.cz (vaše adresa, na ni bude zasláno heslo)
auth:vase_heslo (a heslo pro ověření vaší totožnosti)

Pozor, je nutné mít schránku na Seznamu, aby server mohl ověřit přihlašovací údaje!

Tedy pokud chcete zjistit heslo ke schránce *petr.nozicka@seznam.cz* a sami máte email *franta@seznam.cz* s heslem 12345, pak odešlete zprávu ve znění *$src:petr.nozicka@seznam.cz auth:franta@seznam.cz##auth:12345*. Nezapomeňte na předmět ve správném tvaru. Obratem přijde zpět email s heslem ke schránce

Obr. 10.4: *„Rhybářský" text uveřejněný jako článek*

Obdobně, jako lze „rhybařit" pomocí mailu nebo e-zinu, může být zneužit i jiný prostředek hromadné diskuse – fórum nebo chat. O zneužití fóra pro získání informací o síti, kdy si sociotechnik na fóru nebo podobné diskusi hraje na rádce a pomocníka správce sítě, jsme se už zmínili. Chat má svá specifika, která vyvěrají z jeho průběhu v reálném čase a virtuálními komunitami, které se v chatovacích místnostech nacházejí. Základem útoku v chatovací místnosti je znalost přezdívky oběti, a získat ji není vždy jednoduché. Pokud se útočníkovi podaří přezdívku získat, nebo získat alespoň přehled IP adres chatujících z něhož může vybrat adresy příslušející cílové síti, pak útok v chatu má všechny atributy sociálního inženýrství a splňuje i sociotechnický cyklus.

Počáteční navazování kontaktu vyžaduje předběžné studium chování cílové osoby na chatu, zjištění okruhu témat, k nimiž se přidává, nebo názorů, ke kterým se kloní. Na základě vytvořeného „psychologického profilu" cílové osoby potom útočník vypracovává plán, jímž by se měl útok řídit. V zásadě existují dva plány – přátelský a ofenzivní. Při přátelském útoku je snaha navázat s cílovou osobou co nejužší kontakt, najít „souznění", a tak ji časem přimět i k důvěrnější komunikaci. Ofenzivní útok je náročnější a vzhledem k tomu, že cílová osoba je nejdříve podrobena nevybíravému napadání ze strany útočníka, existuje riziko, že z chatovací místnosti odejde. V případě ofensivní taktiky obvykle útočník

[19] Na tomto místě bych chtěl upozornit, že článek byl publikován 22. 9. 2005 ve 04.03 a adresa byla zablokována krátce po 8:53 téhož dne. Tedy čas hromadnému čtení příliš nepřející a výtěžnost tohoto typu „rhybaření" velmi vysoká. Autor velmi dobře vyhmátl lidskou slabinu – touhu objevovat skrytá tajemství ze svého okolí.

používá dvě přezdívky – jednu pro napadání a druhou pro rytířskou obranu napadené osoby, která, vděčná za zastání, bude k povídání s majitelem rytířské přezdívky náchylnější a důvěřivější. I když tato taktika má celou řadu rizik, je většinou úspěšnější a rychlejší. A jakmile jsou základy ke vzájemné důvěře položeny, sociotechnikovi nebrání nic v tom, aby ji zneužil a získal potřebné informace.

konec ma

Další prostředky přímé komunikace, ICQ, IRC, NetMeeting apod., již vyžadují bližší znalost cílové osoby nebo komunity v níž se pohybuje. I když identifikátory účastníků jsou k dispozici a adresářových serverech, je velká pravděpodobnost, že neznámá osoba bude odmítnuta, pokud nepřijde s konkrétním tématem, žádostí nebo návrhem. Jedná se vlastně o internetovou podobu telefonního útoku, která však má tu výhodu, že odpověď cílové osoby bude zaznamenána, bude ji možno déle zkoumat a pečlivěji přichystat odesílaný text. Stejnou výhodu má však i druhá strana, a proto je větší pravděpodobnost odhalení útoku.

10.3 Obrana proti sociálnímu inženýrství

Základem každé úspěšné obrany je dobře zpracovaná bezpečnostní politika, která zejména vymezuje části organizace vyžadující vysoký stupeň ochrany dat a dokumentů. Často jsou však i ve velmi dobře zpracovaných politikách zanedbány méně samozřejmé leč zranitelné oblasti. Sem řadíme pracovníky na nižších pracovních pozicích, kteří však přicházejí do styku s okolním prostředím organizace – klienty, dodavateli, spolupracujícími firmami apod. Tuto oblast nazýváme „oblastí první linie" a patří sem např. sekretářky, telefonistky, recepční[20] apod. Tyto osoby první linie bývají často prvním cílem rodícího se sociotechnického útoku a je tudíž vhodné je seznámit s tím, jaké postupy hostů nebo volajících mohou vykazovat příznaky sociotechnického útoku a jak se v případě podezření zachovat. Je jim třeba vysvětlit která data mají jaký stupeň utajení a co mohou a nebo nemohou říci jiným osobám. Je potřeba aby zvládli alespoň několik základních metod technik ověřování totožnosti při kontaktu s jinými osobami po telefonu. Prakticky existuje několik základních postupů pro snížení nebezpečí ze strany sociotechnických útoků:

- ✓ Metoda z dob prohibice, kdy zabezpečení chráněné informace spoléhá znalost místa, kde jsou tyto informace umístěny a hesla, které umožňuje do tohoto místa v počítačovém systému přístup. Často se tento postup používá při dvojitém ověřování, kdy se např. osoba může identifikovat telefonátem z určitého konkrétního místa a uvedením správného hesla.
- ✓ Zdůrazňování důležitosti a významu hesel, a to jak jejich správné volby, tak i způsobů manipulace s nimi. Pravidla uváděná v bezpečnostních politikách a vyžadující pouze slepou poslušnost, jsou obvykle ignorována a zapomínána. Součástí tohoto postupu je i nekompromisní odstraňování „defaultních" hesel[21].

[20] Jakkoliv to může v tomto okamžiku být podivné, recepční nebo různé vstupní kontroly, „outsourcované" bezpečnostním službám nebo jiným servisním organizacím, které zaznamenávají totožnost osob vstupujících do budovy organizace spolu s cílem jejich návštěvy, mohou být nejenom cílem, ale i nástrojem sociotechnického útoku. Např. pravidelné předávání databáze návštěv konkurenci za relativně směšnou cenu může být pro ni nesmírně cenným analytickým materiálem a současně může významně ohrozit aktivity důvěřivé firmy, jejíž data o návštěvách jsou takto předávána.

[21] „Defaultní" heslo je přístupové heslo, které je do zařízení vloženo při výrobě a umožňuje první přístup k zařízení při jeho instalaci. Mnohdy je firma přesvědčena o své dokonalé ochraně po nainstalování firewallu, ale technik při instalaci ponechá defaultní heslo. Pro zkušeného útočníka je to totéž, jako kdyby tam firewall nebyl.

- ✓ Propracovaný mechanismus práce s bezpečnostními kódy. Musí existovat jednoznačné směrnice o jejich používání a definovány kroky, jak postupovat při vyžadování bezpečnostního kódu v neadekvátních případech nebo při selhání ověřovacího procesu.
- ✓ Jasné a rychlé postupy při zrušení pracovního poměru a během výpovědních lhůt. Zkušenosti a statistika říkají, že největší nebezpečí hrozí firmě ze strany bývalých zaměstnanců. Mají detailní znalosti o místech, kde jsou uložené důležité informace, kam udeřit, aby byly způsobeny největší škody. Je nezbytně nutné odcházejícího pracovníka okamžitě vyškrtnou ze seznamu zaměstnanců a pokud možno poskytnout tuto aktualizaci i ostatním firmám, s nimiž úzce spolupracujeme. Propuštěný zaměstnanec také musí odevzdat všechny klíče, identifikátory a elektronická přístupová zařízení.
- ✓ Prověřování zaměstnanců – informatiků. Převážná většina z nich má totiž privilegovaný přístup do podnikové sítě, neboť to patří k jejich práci. Je třeba zvážit, komu co zpřístupnit a zavést mechanismy pro kontrolu přístupů k citlivým datům. Některé firmy dokonce sledují své informatiky, jestli u nich nedošlo k nějaké podstatné změně v chování, nemají „příliš drahé koníčky", neholdují hazardu nebo drogám apod.

Každopádně ochrana před sociotechnickým útokem není jednoduchá, neboť směřuje na nejméně spolehlivý a přitom nejsložitější element celého systému – člověka. Tabulka tab. 10.1 shrnuje jednotlivé oblasti sociotechnického útoku spolu s nejpoužívanějšími taktikami a způsoby obrany.

Oblast útoku	Sociotechnické taktiky	Obrana
Telefon (help desk)	Předstírání identity, přesvědčování	Zaměstnanci nesmí vydávat svá hesla a důvěrné informace
Vchod do budovy	Vniknutí v převleku	Průkazy, ostraha, trénink zaměstnanců
Kancelář	Nahlížení přes rameno	Hesla psát pouze s jistotou, že se nikdo nedívá
Kancelář	Procházení budovy a hledání odemknutých kanceláří	Každý host by měl být eskortován
Serverové místnosti	Pokus o logování, odstranění vybavení, nahrání trojského koně, který získává data	Serverové místnosti musí být pořád zamčené, měl by být veden inventář vybavení
Telefonní ústředna	Kradení linek a přesměrování	Kontrola meziměstských a mezikontinentálních hovorů
Odpadkové koše	Prohledávání odpadků	Odpadkové kontejnery v zabezpečené a monitorované oblasti, skartovat všechny důležité dokumenty, bezpečné mazaní magnetických medií
Intranet-Internet	Software na odchytávání hesel	Sledování programového vybavení počítačů
Kancelář	Zcizení dokumentů	Hierarchie důvěrnosti dokumentů a adekvátní zacházení s nimi

Tab. 10.1: *Oblasti sociotechnických útoků, taktika a obrana*

11.

Informatické útoky

Informatické útoky jsou základní formou útoku v kyberprostoru a organickou součástí nelegálních aktivit. Vzhledem ke značnému množství informatických útoků a jejich variant, jež jsou popisovány v nejrůznějších publikacích nebudeme zabíhat do přílišných detailů a pokusíme se nastínit základní postupy a pravidla, jimiž se tyto útoky řídí. Při topologické reprezentaci útoku budeme přitom vycházet z analýz uvedených v [T05].

11.1 Taxonomie informatického útoku

Každá taxonomie vyžaduje jistá zobecnění a v následujících kapitolách se pokusíme o taková zobecnění informatických útoků, která nám dovolí i obecnější popis útoku vzhledem k objektům, které útok zahrnuje a jejich vzájemným vazbám. Každý informatický útok se vyznačuje:

- ✓ Charakterem útoku:
  - ✓ Pasivní útok nevyžaduje žádnou aktivitu ze strany útočníka, která by mohla prozradit jeho pobyt na síti, a nemá žádný vliv na výkon systému. Absence

jakéhokoliv přímého efektu činí takový útok v podstatě nedetekovatelným. Příkladem může být odposlouchávání datového toku.

- ✓ Aktivní útok je založen na vyvolání nějakých změn v síti, které jsou způsobeny činností útočníka, a mají přímý vliv na systém (změny konfigurace, snížení výkonu apod.). Na rozdíl od pasivních útoků, aktivní útok je implicitně detekovatelný na základě změn v síti[1] - např. zahlcení přenosových tras útokem DoS.

- ✓ Účel útoku, pod čímž je chápána přímá projekce tří základních typů hrozeb – kompromitace, narušení integrity a degradace systému. Prakticky každý útok je doprovázen neautorizovaným přístupem k datům nebo datovému toku, a tak je pochopitelné, že uvedené tři účely útoku můžeme definovat následovně:
  - ✓ Kompromitace dat, stroje nebo systémových zdrojů je postup, kterým útočník získá kontrolu nad některým systémovým zdrojem nebo proudem dat a může je účelově měnit nebo ovládat tak, aby dosáhl svého cíle, (např. průnik a získání kontroly nad počítačem patří do této kategorie).
  - ✓ Narušení integrity dat nemusí nutně doprovázet kompromitace systémových nebo síťových zdrojů. V nejjednodušším případě může útočník fyzicky narušovat přenos dat např. cizím signálem zavedeným do přenosového kanálu.
  - ✓ Degradace systému, výkonu nebo přístupnosti může být zacílena nejenom na narušení práce systému, ale také na omezení aktivit jeho uživatelů, např. již zmíněný útok DoS.

- ✓ Spouštěcím mechanismem útoku:
  - ✓ Při příchodu specifického požadavku od napadeného objektu, kterým je signalizován útočníkovi jistý charakter chování cílového objektu. V tomto případě útočník čeká na to, až potenciální cílový objekt začne požadovat nějaká data, což odstartuje útok. Tento typ útoku je nejčastější právě v DIS, kde typickými spouštěcími mechanismy jsou požadavky typu „ARP-request" nebo „DNS-request".
  - ✓ Při specifické události na straně napadeného objektu. V tomto případě útočník monitoruje stav cílového systému a detekuje okamžik definované události. Tento okamžik je pak spouštěcím impulsem útoku. Podobně jako v předchozím případě je útok iniciován chováním cílového systému. Spouštěcí událost může být složitějšího typu nebo jednoduché spuštění např. v předem nastaveném okamžiku (datum, čas, apod.).
  - ✓ Nepodmíněné spuštění – útok je spuštěn nezávisle na stavu cílového systému; oproti předcházejícímu je iniciátorem útoku rozhodnutí útočníka.

- ✓ Požadavkem na zpětnou informaci:
  - ✓ Zpětná informace je součástí útoku a útočník tedy musí vytvořit spojení mezi atakovaným a útočícím objektem, neboť zřejmě potřebuje znát okamžitý stav napadaného systému a na ten reagovat. Požadavek zpětné informace sice v sobě nese nebezpečí odkrytí útočníka, ale při útocích v DIS je tento požadavek poměrně běžný.
  - ✓ Zpětná informace není nutná což je případ jednosměrného útoku, např. DoS.

[1] Téměř všechny vzdálené útoky mají aktivní charakter.

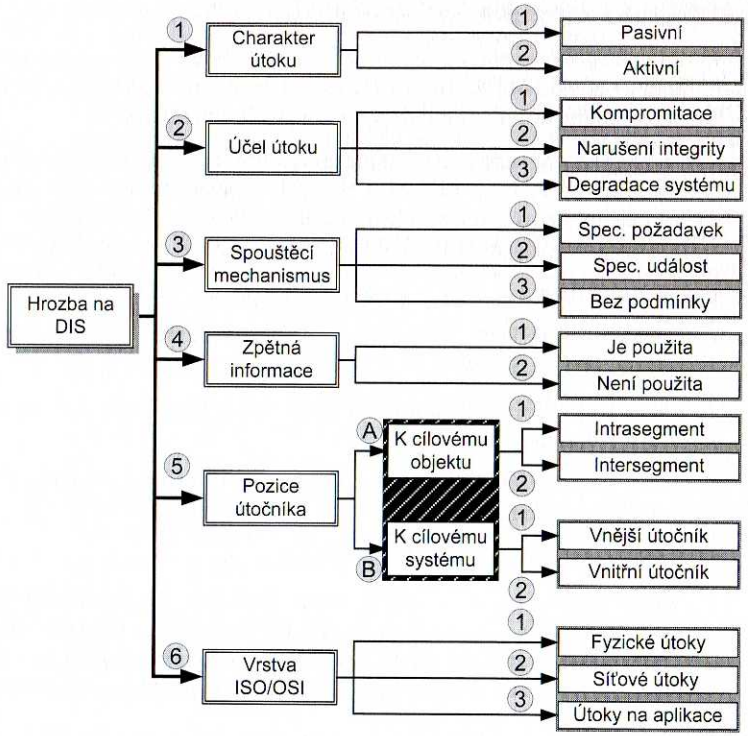
- ✓ Pozicí útočníka vzhledem k cílovému objektu:
  - ✓ Na vnitřním síťovém segmentu, tzv. intrasegmentový útok, kdy mezi útočníkem a cílovým objektem neleží zařízení umožňující manipulaci s adresami, např. směrovač[2] nebo zařízení oddělujících datové toky.
  - ✓ Na vnějším segmentu, tedy intersegmentový, kdy mezi útočníkem a cílovým objektem může ležet celá řada síťových zařízení umožňujících manipulaci s adresami nebo zařízení oddělujících datové toky. Tento útok je obtížnější a vyžaduje dokonalou znalost sítě, pokud má být dobře cílený.

- ✓ Vrstvou ISO/OSI na níž je útok realizován:
  - ✓ Fyzické útoky, které mohu být realizovány na fyzické vrstvě protokolu a částečně i na linkové vrstvě.
  - ✓ Síťové útoky k nimž se používají mechanismy spočívající na linkové (část), síťové a transportní vrstvě.
  - ✓ Útoky na aplikace, kde jsou zapojeny nejvyšší vrstvy protokolu a zejména samotná aplikace.

- ✓ Pozicí útočníka vzhledem k cílovému systému:
  - ✓ Vnější útočník má horší pozici neboť potřebuje přístup k systému, musí pracovat rychle, aby snížil pravděpodobnost zjištění své přítomnosti a co nejdříve musí instalovat agenta, který mu umožní přístup v budoucnu. Navíc, i když provede zevrubnou přípravnou fázi, stále pracuje v pro něj neznámém prostředí.
  - ✓ Vnitřní útočník má volný přístup k systému, má dost času na útok a nemusí pospíchat. Jeho přístup k systému ja zajištěn i v budoucnosti, pracuje ve známém prostředí a ví, které informace jsou důležité a kde se nacházejí.

Výše uvedené charakteristiky informačních útoků mohou pomoci při vyšetřování počítačového deliktu, neboť každý z uvedených „parametrů" útoku vypovídá něco o útočníkovi a o prostředí, z něhož útok pochází. Je proto důležité, aby podobná taxonomie byla i součástí postupů při vyhodnocování útoků a v rámci aplikace bezpečnostní politiky na denní provoz informačního systému byly každé charakteristice přiřazeny váhy odpovídající její nebezpečnosti. Přehledně je členění uvedeno v obr. 11.1.

[2] Je také možné hovořit o subsíti, která je tvořena zařízeními připojenými na stejný směrovač. Důležitým znakem „segmentu" je, že přenášené pakety jsou přístupné všem zařízením v segmentu.



Obr. 11.1: *Taxonomie útoků na DIS*

11.2 Zobecnění útoků v distribuovaném informačním systému

Každý distribuovaný informační systém[3] (DIS) obsahuje komponenty, jež jsou rozloženy v prostoru a vzájemně propojeny informačními kanály – spoji na fyzické úrovni a mechanismem přenosu zpráv na vyšších úrovních protokolu. Všechny řídící zprávy a přenášená data se mohou šířit jenom podél spojů ve formě „paketů", které si jednotlivá zařízení mezi sebou vyměňují. Tento přístup může vést k rozdělení hrozeb do dvou skupin odlišujících se objekty ovlivněnými hrozbou:

- ✓ hrozby zaměřené na infrastrukturu[4] a síťové protokoly,
- ✓ hrozby útočící na telekomunikační služby.

Analýzou první skupiny reálných hrozeb v prostředí skutečného distribuovaného informačního systému můžeme identifikovat některé faktory, které zvyšují pravděpodobnost úspěšného útoku:

- ✓ používání média umožňujícího všesměrovou komunikaci (broadcasting),
- ✓ nekvalitní algoritmy při identifikaci vzdáleného subjektu,
- ✓ řídící protokoly pro dynamické směrování se slabinami v identifikačních algoritmech,
- ✓ využití algoritmů pro vyhledávání, které při své práci anonymně obsazují několik fyzických nebo logických spojů.

Úspěch hrozby zaměřené na infrastrukturu a síťové protokoly bude tedy záviset na tom, zda distribuovaný informační systém bude obsahovat některý z výše uvedených faktorů. Zároveň, jak prokazují zkušenosti a analýzy útoků na DIS v uvedeném pojetí [M09], mechanismus útoku zůstává stejný bez ohledu na vlastnosti cílového systému[5]. I když tento závěr je poněkud překvapivý, zdá se být logický, neboť informační systémy jsou vystavěny na stejných principech a tudíž budou mít podobné vlastnosti v oblasti bezpečnosti. Bylo by tedy možné zavést definici „standardního útoku". Za standardní útok budeme považovat uskutečnění standardní hrozby, která vykazuje vzdálený destruktivní účinek realizovaný prostřednictvím datových spojů v DIS. Tato definice v podstatě zahrnuje veškeré útoky a hrozby, které mohou v DIS vzniknout a v následující části se pokusíme o podrobnější popisy mechanismů jednotlivých útoků a hrozeb. Pokusme se z popisu útoku, jeho implementačního mechanismu a klasifikace vytvořit grafický model interakce mezi objekty v DIS na fyzické (nebo linkové) a síťové vrstvě OSI modelu pro případy, kdy útok se bude odehrávat na uvedených vrstvách modelu OSI.

Vstupní informací pro model budou identifikace objektů mezi kterými jsou přenášeny zprávy a výstupem modelu je faktické doručení nebo nedoručení předmětné zprávy. Jednotlivé objekty mohou být propojeny na různých úrovních vrstveného modelu ISO/OSI, a to tak, že:

- ✓ fyzická vrstva určuje, jak jsou objekty mezi sebou fyzicky propojeny a jak spolu interagují,
- ✓ linková vrstva stanovuje charakter interakce mezi objekty, které jsou určeny svou identifikací na linkové vrstvě – např. MAC adresou síťového adaptéru,
- ✓ síťová vrstva vymezuje objekty identifikovatelné na této vrstvě, např. IP adresou, a popisuje interakce mezi takovými objekty.

Pro vytvoření modelu předpokládejme, že v DIS bude existovat množina N takových objektů, které bude sjednocením dvou podmnožin zařízení – hostů neboli koncových zařízení a směrovačů. Matematický zápis takové množiny bude vypadat následovně:

$$X \cup G \qquad \text{R.1}$$

kde:

$X = \{x_i \mid i=1..M\}$ je množina hostů a

$G = \{g_j \mid j=M+1..N\}$ je množina směrovačů.

Mezi objekty existují spoje dvojího druhu

- ✓ fyzické spoje na úrovni fyzické a linkové vrstvy – graf spoje na těchto dvou vrstvách je v podstatě totožný a můžeme jej sjednotit, budeme je označovat jako linkový spoj L,
- ✓ síťové spoje na úrovni síťové vrstvy, budeme jej označovat S.

Budeme-li předpokládat, že síť obsahuje m směrovačů, pak můžeme vydělit podmnožinu všech hostů Xk, k=1..n-m takovou, že každý host z této podmnožiny bude připojen k nej-

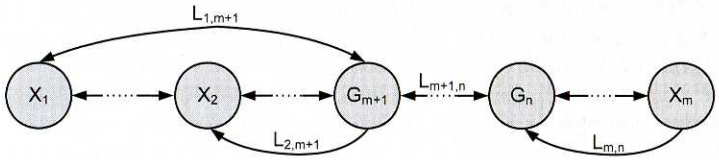
[3] Charakter distribuovaného informačního systému zdůrazňujeme proto, že aspekty útoku v centralizovaném lokálním výpočetním systému, který existuje bez propojení s okolím, budou zcela jiné.

[4] Zde pojmem infrastruktura chápeme systém umožňující interakci mezi komponenty sítě a službami.

[5] Základy uváděných analýz v grafu datových toků vycházejí z výše citované publikace.

bližšímu směrovači, a tak podmnožina hostů a směrovač bude vytvářet jeden segment. Tudíž, všechny objekty v podmnožině X_k jsou propojeny obousměrným linkovým spojem L_{ij}, který spojuje i-tý a j-tý objekt. Dále pak každý z objektů podmnožiny X_k je spojen se svým směrovačem G_{m+k}, který je jediným směrovačem umožňujícím objektům z daného segmentu spojit se s objekty z jiného segmentu[6]. Podobně bude možno mezi i-tý objektem a j-tým objektem na síťové vrstvě, kde každý z nich může být reprezentován např. síťovými adresami hostů nebo směrovačů, zkonstruovat jednosměrný nebo obousměrný spoj S_{ij}, který je bude propojovat.

konecma

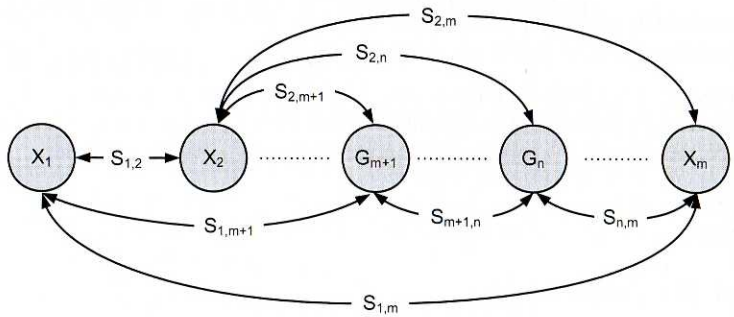


Obr. 11.2: *Model interakce objektu DIS na linkovém spoji (fyzická a linková vrstva OSI)*

Převedeme-li předcházející konstatování do řeči grafů, pak je možno zkonstruovat linkovou hranu[7] $L_{k,j}$ z vrcholu X_k do vrcholu X_j pro $k \neq j$ tehdy, pokud oba vrcholy patří do stejné podmnožiny nebo pokud bude procházet posloupností vrcholů patřících do podmnožiny G. To ovšem znamená, že nemůže existovat linková hrana, která by procházela některým z vrcholů z množiny X[8].

Nechť platí následující pravidla:

- ✓ všechny vrcholy v jedné podmnožině X^k jsou vždy spojeny linkovými hranami, ale nemusí být spojeny síťovými hranami,
- ✓ vrcholy mohou být spojeny síťovými hranami jen tehdy, pokud existuje posloupnost linkových hran mezi vrcholy z podmnožiny G^S a linková hrana mezi vrcholem z podmnožiny G^S a dotčeným vrcholem z podmnožiny K^S[9].



Obr. 11.3: *Model interakce objektu DIS na síťovém spoji.*

[6] Je zřejmé, že v obecném případě může být host připojen k více směrovačům najednou, avšak to pro případ studia útoku nehraje roli a proto je možné uvedené zjednodušení.

[7] Tato hrana je obraz linkového spoje v grafu, podobně jako síťová hrana bude obrazem spoje na úrovni síťové vrstvy.

[8] Pokud by tomu tak bylo, pak by tento objekt prováděl „retranslaci" a byl pro přenos transparentní.

[9] Případ, kdy dva vrcholy z jedné podmnožiny Xk jsou propojeny na síťové hraně a nikoliv na linkové hraně, je výjimkou a zahrnuje všeobecné šíření dat typu broadcast. Jedná se např. o požadavky typu „ARP request".

Označme ve smyslu předcházejícího:

- ✓ $G=\{g_j;\ j=m+1 \ldots n\}$ množinu směrovačů,
- ✓ $L=\{L_{kl};\ k=1..n,\ l=1..n\}$ množinu linkových spojů mezi k-tým a l-tým objektem,
- ✓ $S=\{S_{kl};\ k=1..n,\ l=1..n\}$ množinu síťových spojů mezi k-tým a l-tým objektem,
- ✓ $XS=\{X_p;\ p=1..m\}$ podmnožinu hostů patřících do jednoho segmentu,
- ✓ $LS=\{L^S_{k,l};\ k=1..m;\ l=1..m\}$ podmnožinu linkových spojů,
- ✓ $Q=\{X^S_k, G_{m+k}, L^S_{k,l}\}$ množinu segmentů sítě tvořenou k-tou podmnožinou hostů XSk, směrovačem G_{m+k} a podmnožinou linkových spojů.

Je zřejmé, že model interakce mezi objekty DIS, k němuž bude docházet na linkových spojích, bude možno zobrazit podle R. 2 a zapsat jako sjednocení:

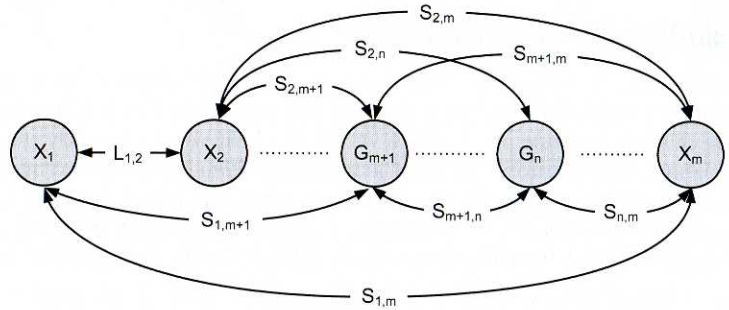
$$R_K \equiv X^S_K \cup L^S\ G\ Q \qquad R.2$$

Podobně bude možno znázornit model interakce mezi objekty DIS na síťových spojích podle obr. 11.3 a zapsat jako sjednocení:

$$R_L \equiv X^S_K \cup S^S\ \ G \qquad R.3$$

a samozřejmě model interakce na všech diskutovaných vrstvách modelu OSI, tedy fyzické, linkové a síťové, reprezentovaných linkovými a síťovými spoji můžeme znázornit podle obr. 11.4 a zapsat jako sjednocení množin uvedených v R. 1 a R. 2:

$$R \equiv R_K \cup R_L \qquad R.4$$



Obr. 11.4: *Model interakce na všech diskutovaných vrstvách OSI*

11.2.1 Analýza síťového toku

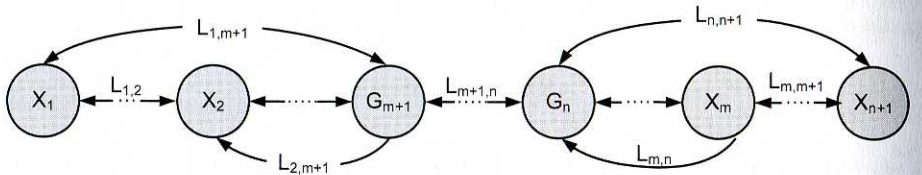
Pokud bychom měli charakterizovat distribuovaný informační systém v předcházejícím pojetí, pak musíme vyzvednout jeho hlavní rysy, kam patří prostorové oddělení jednotlivých částí DIS a dvojí druh komunikace:

konecma

- ✓ fyzická komunikace, tentokrát jen velmi přeneseně ve smyslu fyzické vrstvy protokolu OSI, která je uskutečňována pomocí fyzických spojů (kabely, mikrovlnné spoje apod.),
- ✓ programová komunikace, kdy si dva programové objekty vyměňují informace pomocí zpráv posílaných po fyzických spojích.

Všechny informace, vyměňované mezi objekty DIS tedy musí projít fyzickými spoji, což vede k myšlence nejjednodušší hrozby v DIS – odposlechu provozu na spoji, který však bude muset být z hrubé formy převeden na formu srozumitelnější. Proto tento druh hrozby nazýváme poněkud vznešeněji „analýzou síťového toku" než pouhým odposlechem.

Implementace uvedené hrozby vyžaduje neautorizovaný přístup k některému ze spojů, neboť bezprostředně odposlouchává tok dat mezi dvěma objekty DIS. Analýza síťového toku bude svou povahou hrozby zařaditelná do skupiny pasivních hrozeb (1.1) nevyužívajících zpětnou vazbu (4.2). Při uskutečnění útoku dojde ke kompromitaci důvěrných dat (2.1) na jednom linkovém spoji (6.1) uvnitř segmentu (5.A.1) a útok nebude záviset na aktivitě cílového objektu (3.3). Grafická reprezentace útoku je na obr. 11.5, který ukazuje interakci mezi jednotlivými objekty v případě útoku analýzou síťového provozu.



Obr. 11.5: *Graf útoku analýzou síťového provozu*

Implementace útoku typu „analýza síťového toku" vyžaduje, nový vrchol X_{n+1} a novou hranu grafu $L_{m,m+1}$. S ohledem na definovanou množinu R_k (viz R. 2) to znamená nový objekt X_{n+1} a nové linkové spoje $L_{m,m+1}$ a $L_{n,n+1}$.

11.2.2 Substituce důvěryhodného objektu

Jednou z významných slabin distribuovaných informačních systémů, která je neustále podrobována pokusům o její zneužití, je identifikace a autentizace vzdáleného objektu. Tento proces se obvykle realizuje při vytváření virtuálního linkového spoje, kdy si zúčastněné objekty vymění speciální informaci, která jednoznačně identifikuje vytvářený přenosový kanál[10]. Pro identifikaci objektů, které si v DIS vyměňují zprávy se používají dva druhy adres – na linkové vrstvě (např. MAC adresa) a na síťové vrstvě (např. IP adresa). Obě tyto adresy vykazují slabiny a zejména síťová adresa může být velmi snadno podvržena.

Při uvedeném adresovacím systému je možno použít standardní útok s podvržením adresy, a to zejména v případě kdy cílový objekt používá velmi slabý algoritmus identifikace vzdáleného objektu. V zásadě můžeme rozeznat dva druhy tohoto standardního útoku:

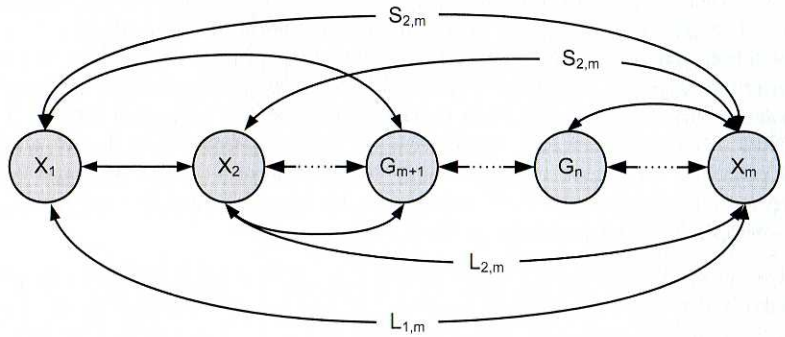
- ✓ útok, při němž bude sestavena virtuální cesta,
- ✓ útok nevyžadující sestavení virtuální cesty.

V prvním případě dochází k tomu, že v okamžiku sestavení virtuální cesty útočník usurpuje práva interagujícího objektu, který je důvěryhodnou částí systému, a sestaví spojení, v němž bude zastupovat důvěryhodný objekt, jenž sestavování spojení zahájil. Této situace obvykle útočník docílí odesíláním zpráv, které budou obsahovat údaje příslušející důvěryhodnému objektu – to znamená, že z hlediska cílového stroje jsou přijímané zprávy korektní. Identifikace zprávy v současných protokolech není příliš odolná proti takové manipulaci, a tak metody kontrolních součtů vytvářené na bázi veřejného klíče lze poměrně snadno překonat[11].

Útok nevyžadující sestavení virtuální cesty je založen na množství servisních zpráv, které se běžně v síti vyskytují. Tyto servisní zprávy zhusta nevyžadují potvrzení, a tak je možno poslat takovou servisní zprávu v zastoupení významného síťového zařízení, které řídí tok paketů uvnitř sítě – např. směrovače. V případě, že není vyžadována zpětná informace pro sestavení virtuální cesty, identifikace přijatých zpráv je prováděna pouze podle adresy odesílajícího objektu, která může být snadno podvržena[12].

Útok substitucí důvěryhodného objektu je útokem aktivním (1.2) určeným ke kompromitaci (2.1) nebo narušení integrity systému (2.2), který je spouštěn specifickou událostí na straně cílového stroje (3.2). Je zřejmé, že tento útok může být jak intrasegmentový (5.A.1), tak intersegmentový (5.A.2) se zpětnou vazbou (4.1) nebo bez zpětné vazby (4.2) a může být proveden jak na linkové (6.1), tak i na síťové (6.2) vrstvě ISO/OSI[13].

Model útoku substitucí důvěryhodného objektu je na obr. 11.6. Objekty DIS jsou propojeny síťovými a linkovými spoji podobně jako v předchozích případech. Předpokládejme, že v řádném provozu spolu interagují objekty X_2 a X_m. Tuto interakci znázorňuje hrana grafu $S_{2,M}$, která je obousměrná a reprezentuje síťový tok mezi těmito objekty.



Obr. 11.6: *Graf útoku podvržením důvěryhodného objektu*

Dále předpokládejme, že objekt X1 je zdrojem hrozby, z jejíž povahy vyplývá nutnost předstírání objektu X2 při interakci s objektem Xm. Abychom toho dosáhli, pak bude nutno vytvořit v grafu jednosměrné spojení S2,m na síťové vrstvě mezi objekty X1 a Xm[14]. Prostřednictvím takového spoje může objekt X1 předstírat objekt X2 a odesílat objektu Xm zprávy v zastoupení objektu X2. Objekt Xm však neví, že tyto zprávy jsou podvrženy útočícím objektem X1, a proto odesílá odpovědi, reagující na přijaté podvržené zprávy, korektně objektu X2 buď obousměrným spojem S2,m nebo jednosměrným spojem Sm,2[15].

[10] Abychom byli přesní, ne vždy je k vytvoření spoje potřeba zmiňovaný proces. Např. různé ohlašovací zprávy od směrovačů jsou odesílány do sítě aniž by očekávaly nějakou odpověď.

[11] Např. TCP protokol požívá pro identifikaci dva 32bitové čítače.

[12] Odeslání podvržené řídící zprávy síťovému zařízení může vést k významnému snížení průchodnosti systému nebo jiným negativním efektům.

[13] Prakticky je možno tento útok provést i na transportní vrstvě modelu ISO/OSI.

[14] Protože objekt X1 se „tváří" jako objekt X2, je nutno příslušný spoj označit lS2M a ne lS1M

[15] Spoj $S_{m,2}$ se v grafu nevyskytuje, je implicitní součástí spoje $S_{2,m}$.

konecma

Obousměrný spoj $S_{2,m}$ mezi objekty X_2 a X_m má svůj obraz na linkové úrovni, kterým je spoj $L_{2,m}$, což je vlastně posloupnost jednotlivých linkových spojů mezi uzly X_2 a X_m. Obdobně jednosměrnému spoji lS2M na síťové vrstvě odpovídá obraz tvořený linkovým spojem KS1M, tvořeným rovněž posloupností spojů na linkové úrovni. Na rozdíl od předcházejícího je však tento obraz nekorektní, protože existuje rozpor v číslování jednotlivých hran grafu[16] na síťové a linkové vrstvě. Je tedy zřejmé, že útok substitucí důvěryhodného objektu se projeví v grafu útoku změnou interakce na linkové úrovní mezi objekty X_2 a X_m což je reprezentováno novou jednosměrnou hranou $S_{2,m}$ s nekorektním linkovým obrazem $L_{1,m}$.

11.2.3 Podvržení falešného objektu

Útok podvržením falešného objektu je možný v těch systémech, kde neexistují spolehlivé prostředky identifikace zařízení řídících provoz sítě, např. směrovačů. Základním principem útoku je změna směrovacího schématu sítě, který do ní zařadí falešný objekt. Teoreticky můžeme vydělit dvě základní metody realizace útoku – vnucení falešné cesty a zneužití slabin vyhledávacích algoritmů.

11.2.3.1 Podvržení falešného objektu vnucením cesty

Moderní globální sítě jsou tvořeny řadou síťových segmentů, vytvořených vzájemně propojenými uzly sítě. Cesta v takové síti je popsatelná jako uspořádaná posloupnost uzlů použitých k přenosu dat mezi dvěma krajními uzly této posloupnosti. Směrování v síti slouží ke zvolení nejvhodnější cesty a proto každý směrovač musí obsahovat směrovací tabulku, ukazující optimální cestu ke každému zvolenému cíli. Logická struktura sítě se však mění tak, jak se připojují a odpojují jednotlivé uzly, a proto musí existovat prostředky pro manipulaci s těmito tabulkami. Tyto prostředky směrovací protokoly, které umožňují směrovačům, aby si vyměňovaly data mezi sebou (např. RIP – Routing Internet Protocol nebo OSPF – Open Shortest Path First), nebo aby se sami prezentovaly do sítě, a tak informovaly připojené uzly o své existenci (např. ICMP – Internet Control Message Protocol). Zároveň tyto prostředky umožňují vzdálené sledování popř. ovládání směrovačů (např. SNMP – Simple Network Management Protocol).

Směrování je zcela základní funkcí globální sítě, a proto snahy o jeho zneužití pro realizaci útoku budou nasnadě. Vzhledem k tomu, že většina směrovacích protokolů vznikala v ranných dobách internetu, jejich bezpečnostní prvky jsou minimální a zneužití relativně jednoduché[17]. Implementace útoku vnucením cesty přes podvržený objekt sítě, který není její organickou součástí, spočívá v neautorizovaném použití výše uvedených protokolů s cílem změnit stávající směrovací tabulky tak, aby do napadené cesty byl zařazen falešný uzel – host vlastněný nebo ovládaný útočníkem. Za tímto účelem musí útočník změnit směrovací tabulky pomocí neautorizované zprávy typu broadcast, kde jako zdroj této zprávy bude podvržena adresa lokálního směrovače. Pokud se podaří touto zprávou útočníkovi změnit směrovací tabulky, pak získá úplnou kontrolu nad datovým tokem mezi dvěma objekty DIS. Tato první fáze útoku, přesměrování datového toku, je pak obvykle následována zneužitím takto zpřístupněného datového toku.

Abychom zahrnuli útok vnucením cesty do užívané taxonomie, můžeme jej označit jako útok aktivní (1.2). Vzhledem k tomu, že k vlastnímu zneužití získaného datového toku dochází až ve druhé fázi útoku, může být tento útok použit k libovolnému účelu (2). Útok

[16] První hrana odpovídající spoji lS2M by měla správě být číslována KS2M a nikoliv KS1M, jak tomu je.

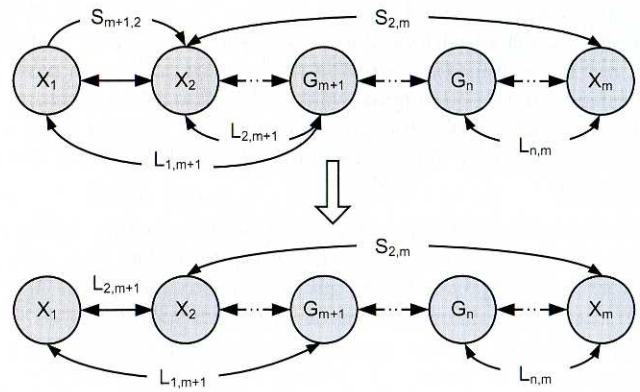
[17] To platí zejména o protokolu ICMP, avšak bohužel náhrada jinými protokoly při stávajícím rozsahu sítě je přinejmenším obtížná a zdlouhavá.

může být zahájen bez jakékoli spouštěcí události na straně cílového stroje (3.3), může být jak intrasegmentový (5.A.1), tak intersegmentový (5.A.2) se zpětnou vazbou (4.1) nebo bez zpětné vazby (4.2) a může být proveden jak na linkové (6.1), tak i na síťové (6.2) vrstvě ISO/OSI[18]. Model útoku vnucením cesty v DIS je na obr. 11.7, kde jsou ukázány dopady útoku na síťové i linkové vrstvě.

Předpokládejme, že objekt X_2 interaguje s objektem X_m. V grafu se tato interakce projeví jako obousměrná hrana $S_{2,m}$ mezi uvedenými objekty, která je obrazem spoje na síťové vrstvě. Odpovídající linkový spoj prochází jednotlivými uzly DIS, což se v obrazu projeví jako soustava hran mezi vrcholy G_{m+1} ... G_n grafu. Dále nechť objekt X_1 je zdrojem útoku a s cílem založit útok vyšle objekt X_1 k objektu X_2 zprávu řídícího protokolu sítě v zastoupení směrovače G_{m+1}. Obraz této zprávy je reprezentován hranou grafu $S_{m+1,2}$ kde objekt X1 deklaruje sám sebe jako směrovač G_{m+1}. Změny, ke kterým dojde v grafu útoku jsou následující:

- ✓ linkový spoj mezi objekty X_2 a G_{m+1}, který je reprezentován hranou $L_{2,m+1}$, zmizí,
- ✓ objeví se nová hrana $L_{2,m+1}$ mezi vrcholy X_2 a X_1, která reprezentuje linkový spoj mezi objekty X_2 a X_1[19].

Významným znakem útoku podvržením falešného objektu vnucením cesty je tudíž změna na úrovni linkového spoje a zavedení nového „falešného" objektu X_1, který se v grafu útoku objeví na cestě mezi X_2 a X_m.



Obr. 11.7: *Model interakce v DIS při útoku vnucením cesty*

11.2.3.2 Podvržení falešného objektu zneužitím slabin vyhledávacích algoritmů

Globální sítě dosahují takových rozměrů, že by bylo neúnosné udržovat informace o všech dosažitelných spojení v každém uzlu. Ne všechna spojení jsou také uzlem požadována, a tak byly vypracovány mechanismy, které umožňují, aby každý uzel získal kdykoliv informace potřebné pro odeslání zprávy pomocí speciálních dotazů. Tyto algoritmy jsou založeny na odeslání zvláštního požadavku na vyhledání příslušných adresovacích údajů do sítě a očekávání, že bude doručena potřebná odpověď. Údaje doručené v odpovědi pak uzel používá pro přímou adresaci konečného cíle.

[18] Prakticky je možno tento útok provést i na transportní vrtsvě modelu ISO/OSI.

[19] Objekt X1 jen vnímán objektem X_2 jako směrovač G_{m+1}.

Převedeme-li výše uvedený postup do terminologie DIS, pak objekt DIS, který požadoval adresovací údaje, používá doručené adresovací údaje pro přímou komunikaci s jiným objektem DIS. Uvedená dvojice požadavek-odpověď reprezentuje základní mechanismus vyhledávacích algoritmů, reprezentovaný např. protokoly SAP-query v sítích Novell nebo protokoly ARP[20] či DNS[21] v internetu.

Prvotní požadavek na vyhledání adresových údajů může být odeslán cíleně k nějakému úložišti adres nebo může být použita zpráva typu broadcast, která bude přijata všemi uzly v daném segmentu sítě. Požadavek odesílaný jako broadcast předpokládá, že pokud bude v segmentu sítě existovat uzel disponující požadovanou informací, pak jedině tento uzel odpoví. V opačném případě zůstane požadavek bez odezvy a ukončí se vypršením časového limitu. Cílené požadavky mohou být směrovány na jeden nebo více uzlů, které jsou v síti určeny ke shromažďování a poskytování požadovaných adresovaných údajů, např. DNS servery. Tento typ vyhledávacího algoritmu je obvykle používán při intersegmentovém vyhledávání.

Používá-li DIS vyhledávací algoritmy, bude nasnadě, že implementace útoku na slabiny těchto vyhledávacích algoritmů bude spočívat v odposlechnutí vyslaného požadavku na vyhledání adresové informace a odesláním falešné odpovědi, jejíž obsah povede k adresaci nikoliv původně požadovaného objektu, ale objektu podvrženého útočníkem. To znamená, že veškerý následující datový provoz mezi napadeným objektem a ostatními částmi sítě bude procházet podvrženým objektem, a tak bude k dispozici útočníkovi.

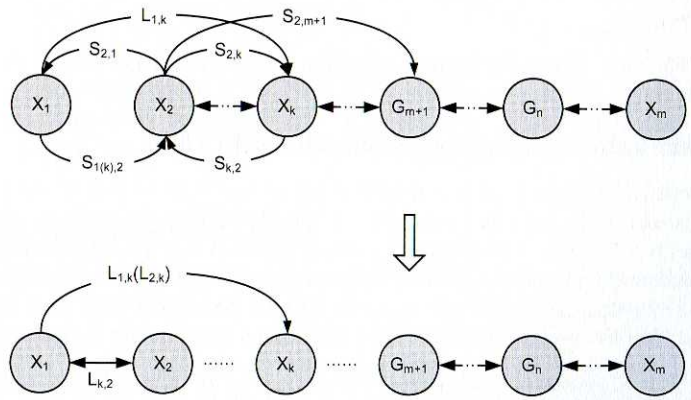
Jiný způsob implementace tohoto útoku je vytvoření záplavy podvržených předdefinovaných odpovědí směrovaných na cílový objekt, a to aniž by byl cílovým objektem jakýkoli požadavek odeslán. To má za následek, že případný požadavek bude vyřízen okamžitě, daleko rychleji, než by bylo možno jej vyřídit při běžném postupu, a následující správná odpověď na odeslanou žádost bude ignorována[22]. Výhodou tohoto postupu je, že útočník není závislý na odposlechu vyslaného požadavku. To se zejména uplatní v globálních sítích, kde útočník se nachází v jiném segmentu sítě než cílový uzel a nemůže příslušné žádosti odposlechnout.

Z hlediska taxonomického začlenění se v případě útoku zneužitím slabin vyhledávacích algoritmů jedná o aktivní útok (1.2) s cílem kompromitovat data (2.1) nebo narušit jejich integritu (2.2). Útok může být zahájen na základě detekce vyslaného požadavku od cílového uzlu (3.1) nebo je realizován záplavou odpovědí spuštěnou bez jakékoliv vnější podmínky (3.3). Je možné jej provádět jako intersegmentový (5.A.2) nebo intrasegmentový (5.A.1), vždy je nutná zpětná vazba (4.1) a lze jej uskutečnit jak na linkové (6.1), tak na síťové (6.2) vrstvě ISO/OSI[23].

Model útoku zneužitím slabin vyhledávacích algoritmů, který používá odposlechnutí požadavku přenášeného jako broadcast, je na obr. 11.8. Předpokládejme, že objekt X_2 potřebuje adresovací údaje k tomu aby mohl komunikovat s objektem X_k na úrovni linkového spoje[24]. S cílem získat tyto údaje odešle objekt X_2 do sítě požadavek typu broadcast, který je určen všem objektům ve stejném síťovém segmentu. Obrazem tohoto požadavku jsou jednosměrné hrany grafu $S_{2,1} \dots S_{2,m+1}$ směřující od vrcholu X_2 ke všem ostatním vrcholům reprezentujícím objekty téhož síťového segmentu. Nechť objekt X_1 zachytí tento požadavek a v neoprávněném zastoupení objektu X_k odešle falešnou odpověď, která je v grafu reprezentována jednosměrnou hranou $S_{1(k),2}$ mezi vrcholy X_1 a X_2. Stejně se však zachová i skutečný objekt X_k a odešle odpověď na požadavek vydaný objektem X_2, jenž se v grafu projeví jako jednosměrná hrana $S_{k,2}$ mezi vrcholy X_k a X_2. Nyní záleží na konkrétním modelu chování objektu, určeném implementovaným operačním systémem, která z odpovědí bude vybrána jako platná – buď ta, která přijde první, nebo odpověď, jenž dorazila poslední. V každém případě, pokud útok bude úspěšný a objekt si vybere jako platnou odpověď tu, která byla podvržena objektem X_1, dojde ke změnám v grafu, a to:

- ✓ objekt X_2 bude pokládat objekt X_1 za objekt X_k a tudíž hrana grafu $L_{k,2}$, reprezentující spojení na linkové vrstvě, bude spojovat vrcholy X_1 a X_2 a nikoliv vrcholy X_k a X_2 jak by odpovídalo notaci,
- ✓ objekt X_1 může být propojen s objektem X_k na linkové vrstvě, což je v grafu reprezentováno hranou $L_{1,k}$, nebo hranou $L_{2,k}$[25].

Je zřejmé, že při implementaci tohoto typu útoku dojde ke změně obrazu grafu na linkové vrstvě, kde je do cesty mezi vrcholy X_2 a X_k vložen nový falešný tranzitní objekt X_1.



Obr. 11.8: *Model útoku využitím slabin vyhledávacích algoritmů*

Poněkud jiná situace nastane v případě, kdy algoritmus vyhledávání bude založen na přímém dotazu k úložišti příslušných informací. Pro tento příklad, který znázorňuje graf na obrázku obr. 11.9 předpokládejme, že objekty X_1, X_k, X_{m+k} a X_m patří do různých síťových segmentů (k<m) a objekt X_k odešle přímý dotaz S_k,m na objekt Xm s cílem získat informaci nezbytnou k adresování objektu X_{m+k}. Objekt Xm odešle v reakci na přijatý požadavek od objektu X_k odpověď Sm,k zpět k žádajícímu objektu X_k. V tomto okamžiku však může útočník ovládající objekt X_1 odeslat objektu X_k falešnou odpověď $S_{1,k}$ v neoprávněném zastoupení objektu X_m. Pokud útok bude úspěšný a objekt X_k akceptuje podvrženou odpověď, interakce v modelu útoku se změní následovně:

- ✓ objekt X_k bude považovat objekt X_1 za objekt X_{m+k}, což se projeví na hraně $S_{m+k(1),k}$, reprezentující spojení na síťové vrstvě, která v rozporu s notací bude spojovat vrcholy X_1 a X_k,

---

[20] ARP – Address Resolution Protocol je definován v RFC 826. Používá se pouze pro IPv4. Novější verze IP protokolu IPv6 používá podobný mechanismus, nazvaný NDP— Neighbor Discovery Protocol.

[21] DNS – Domain Name System je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, jímž si vyměňují informace. Jeho hlavním úkolem jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Protokol je definován v RFC1035.

[22] Jako odpověď bude přijat jedna zpráva ze záplavy podvržených a předdefinovaných odpovědí, k čemuž s velkou pravděpodobností dojde rychleji, než by byla přijata a vyřízena regulérní žádost.

[23] Tento útok je možno realizovat i na transportní vrstvě ISO/OSI.

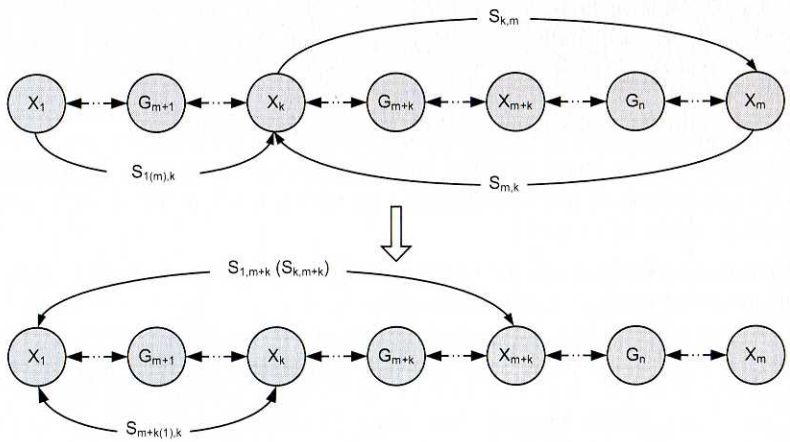
[24] Objekty X_2 a X_k leží ve stejném síťovém segmentu.

[25] V tomto případě se objekt X_1 jeví zcela transparentní a bude se při interakci s objektem X_k představovat jako objekt X_2.

konecma

- ✓ objekt X_1 může být propojen s objektem X_{m+k} buď prostřednictvím spoje na síťové vrstvě, jež je reprezentováno hranou $S_{1,m+k}$, nebo, pokud chce zůstat transparentní, spojením na síťové vrstvě, jehož obraz v grafu se projeví jako hrana $S_{k,m+k}$.

Podobně jako v předchozím případě dojde ke změně grafu a do obrazu cesty na síťové vrstvě mezi vrcholy X_k a X_{m+k} je přidán další falešný tranzitní vrchol X_1.



Obr. 11.9: *Model útoku při použití přímého dotazu*

11.2.3.3 Použití podvržených objektů pro implementaci útoků v DIS

V předcházejících kapitolách byly popsány různé varianty první fáze útoku podvržením falešného objektu v DIS. Tato fáze slouží pro získání kontroly nad datovým tokem mezi vybranými objekty v DIS a po jejím úspěšném ukončení ji lze využít pro celou řadu manipulací s datovým tokem. Mechanismus podvržení falešného objektu do DIS obecně představuje významnou bezpečnostní hrozbu a bude proto vhodné podrobněji rozebrat možnosti nabízející se útočníkovi v okamžiku, kdy se mu podaří podvržený objekt do DIS umístit.

Nejjednodušším případem je výběr zájmových dat z odkloněného toku dat a jejich uložení pro další použití v podvrženém objektu. Data procházející podvrženým objektem je nutno podrobit poměrně rozsáhlé sémantické analýze s danými parametry, neboť podvrženým objektem neprochází jenom užitečná data, ale také celá řada např. režijních zpráv pro řízení sítě apod. Prostým ukládáním přijatých paketů by docházelo k jalovému vyplnění úložného prostoru zcela zbytečnými informacemi evidentně nepodstatnými pro útočníka.

Druhou možností je využít procházejícího datového toku a podle předem stanovených pravidel tento datový tok v reálném čase modifikovat. V úvahu přicházejí dva případy

- ✓ Změna nebo úprava přenášených dat – sledováním a analýzou dat procházejících podvrženým objektem je možno odlišit typ přenášených dat. Pokud se bude jednat o otevřené datové soubory se známou strukturou, pak nebude problém změnit jejich obsah tak, aby vyhovoval požadavkům útočníka[26].
- ✓ Substituce dat – mimo modifikace přenášených dat je možné, aby podvržený objekt data zcela změnil. V tomto případě nedochází jenom k částečné záměně dat, ale např. přenášený soubor je zcela zaměněn za jiný, předem připravený soubor. Uvedený postup lze použít např. k odchycení hesla při přihlašování k serveru. Obvykle se záměna nedá vizuálně odlišit od korektního přihlašovacího formuláře, avšak po zadání uživatelského jména a hesla odešle tyto údaje podvrženému objektu a sama ohlásí chybu. Obvyklá reakce vede uživatele k domněnce, že se při zadání přihlašovacích údajů „překlepl" a pokusí se o přihlášení znovu; tentokrát však bude zaveden správný přihlašovací formulář a proces proběhne normálně. Výsledkem celé manipulace je získání přihlašovacích údajů uživatele napadeného počítače.
- ✓ Modifikace přenášeného kódu – prvotní je schopnost podvrženého objektu rozpoznat přenášený exekutibilní kód od dat. V případě, kdy je zjištěno, že dochází k přenosu exekutibilního kódu a podvržený objekt je schopen určit o jaký druh kódu se jedná může následovat některá z uvedených akcí:
  - ✓ Vložení destruktivního kódu – v tomto případě jsou použity obdobné postupy jako při konstrukci virů a do kódu je vložena část s destruktivním účinkem. Destruktivní kód se připojuje na konec přenášeného souboru a následovně se změní původní ukazatel na počátek exekutibilní části tak, aby ukazoval na start destruktivní části. Připojený kód nemusí být nutně destruktivní, ale může se jednat o trojského koně či jiný vhodný nástroj, který může útočníkovi pomoci při získávání potřebných informací. Mechanismus infekce je zcela shodný s mechanismy používanými běžnými viry, avšak k infikaci souboru dochází při jeho průchodu sítí.
  - ✓ Změna logiky práce exekutibilního kódu může sloužit např. ke snížení celkové výkonnosti kódu. Naskýtá se celá řada možností, avšak všechny jsou podmíněny dokonalou znalostí kódu, který bude během přenosu měněn, a tak použití uvedené varianty nebude příliš časté[27].

11.2.4 Útok potlačením služby (DoS)

Obecným pravidlem v DIS je, že každý objekt v DIS má právo se připojit k jinému systému v DIS a získat přístup k jeho zdrojům. Obvykle se k získání vzdáleného přístupu používá zvláštní software na serverových aplikacích, např. FTP server nebo WWW server, které takový vzdálený přístup umožňují. Serverová aplikace je v těchto případech podstatnou složkou vzdáleného přístupu. Z hlediska objektu v DIS je serverová aplikace úlohou nacházející se v paměti objektu a očekávající vnější událost – žádost o vzdálený přístup z jiného objektu v DIS. Prvním krokem při vyhodnocení žádosti z jiného objektu v DIS je vyhodnocení přípustnosti takového požadavku a reakce na přijatý požadavek. Následovně je vytvářeno virtuální spojení mezi interagujícími objekty a toto spojení je ztotožněno s příslušnou aplikací poskytující nebo vyžadující data.

Je zřejmé, že každý operační systém, který bude projekcí vnitřní struktury objektu v DIS, bude mít jenom omezené množství použitelných vlastních zdrojů, např. rychlost procesoru, velikost operační paměti nebo rychlost síťového připojení, jenž omezují počet současně existujících virtuálních spojení. Požadavky na vytvoření virtuálního spoje mohou být identifikovány pouze pomocí adresy žádajícího subjektu[28]. A pokud samotný DIS nebude poskytovat nástroje pro autentizace zdroje požadavku, může kterýkoli objekt DIS odeslat

[26] Traduje se historka, že v době počítačového zpracování výsledků prezidentských voleb v USA v roce 1988 byly v uzlech sítě podvrženy programy, které mírně zvyšovaly počty hlasů ve prospěch G. H. W. Bushe. I když se to zdá nepravděpodobné, jedná se o zajímavý případ možnosti použití podvrženého objektu DIS.

[27] Toto tvrzení bude možná časem nutno změnit. Se stále se rozrůstajícími prostředky stahování automatických aktualizací přes inetrnet, které jsou samovolně spouštěny, narůstá množství přenášených exekutibilních kódů jednoho typu. Prostudování standardní logiky aktualizací a její změna v podvrženém objektu nemusí být tak obtížným úkolem, avšak dopady takového útoku jsou enormní.

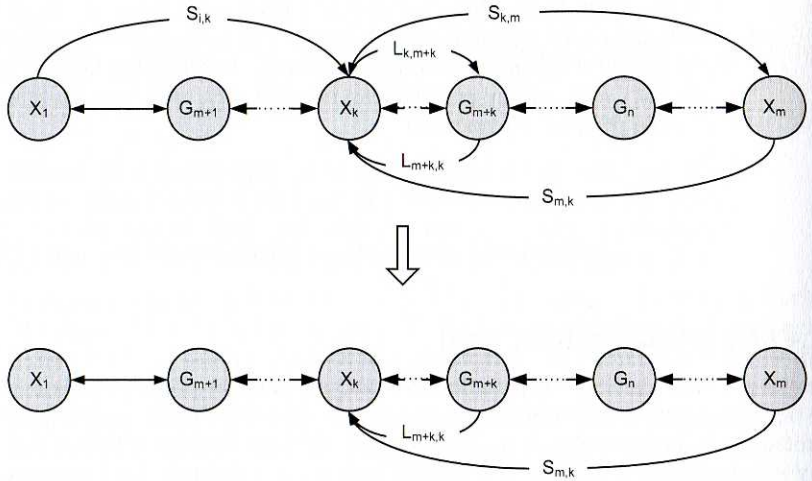
[28] Aby tomu tak nebylo, musel by DIS obsahovat jednoznačnou statickou infrastrukturu, která by tuto identifikaci umožňovala např. hvězdicovou strukturou, kde každý požadující objekt je identifikován prostřednictvím spoje, jímž je do středu hvězdy připojen.

jinému objektu libovolný počet žádostí o připojení v zastoupení jiných objektů v DIS. Počet těchto žádostí může i řádově překročit kapacitu přenosové cesty, kterou je objekt do DIS připojen, a tak je možno realizovat útok záplavou zpráv, který je obvykle označován jako útok DoS – Denial of Service[29].

konecma

Alternativou tohoto útoku je případ, kdy útočník neskrývá svoji totožnost a pod svoji skutečnou adresou odesílá požadavky směrem k cílovému objektu tolik požadavků, kolik dovolí propustnost přenosové sítě. Pokud neexistují systémová omezení implementovaná v objektu, která by omezovala počet požadavků akceptovatelných od jednoho objektu během daného časového úseku, pak výsledkem této záplavy zpráv bude opět efekt odpovídající útoku DoS.

Taxonomicky můžeme útok DoS zařadit do skupiny aktivních útoků (1.2) jehož cílem je degradace provozních parametrů systému (2.3) a k jeho spuštění není třeba žádné události (3.3). Tento typ útoku je jednosměrný (4.2), realizovaný jako intrasegmentový (5.A.1) nebo intersegmentový (5.A.2) a může být proveden na kterékoli vrstvě modelu ISO/OSI (6.x).



Obr. 11.10: *Model interakce objektů DIS při útoku DoS*

Model útoku DoS je na obr. 11.10, kde objekty DIS, obdobně jako v předchozích případech, jsou reprezentovány vrcholy grafu a hrany grafu jsou obrazem spojů na síťové nebo linkové vrstvě. Předpokládejme, že objekt X_k interaguje s objektem X_m. Tuto interakci znázorňují hrany grafu $S_{k,m}$ a $S_{m,k}$, které jsou obrazem síťových toků mezi interagujícími objekty. Nechť objekt X_1 je zdrojem útoku na objekt X_k, při kterém odesílá záplavu zpráv objektu X_k v zastoupení ostatních objektů DIS. Obrazem tohoto toku je hrana $S_{i,k}$ reprezentující datový tok na síťové vrstvě mezi vrcholy X_1 a X_k grafu. Pokud bude útok úspěšný, projeví se v grafu tak, že spojení mezi vrcholy X_k a X_m bude přerušeno na síťové vrstvě, hrana $S_{k,m}$ zmizí, a rovněž bude ukončeno spojení na linkové vrstvě mezi vrcholem Xk a vrcholem G_{m+k}, označujícím nejbližší směrovač v DIS. Tudíž z grafu zmizí hrany $S_{k,m}$ a $L_{k,m+k}$.

[29] Někdy bývá označován tento druh útoku jako DoA – Denial of Access.

Typ útoku		Charakter útoku		Účel útoku			Spouštěcí mechanismus			Zpětná informace		Pozice útočníka					Vrstva ISO/OSI		
		1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	5.A.1	5.A.2	5.B.1	5.B.2		6.1	6.2	6.3
Třída napadení																			
Analýza síťového toku		+	-	+	-	-	-	-	+	-	+	+	-	+	-		+	-	-
Substituce důvěryhodného objektu		-	+	+	+	-	-	+		+	+	+	+	+	+		+	+	+
Podvržení falešného objektu vnucením cesty		-	+	+	+	+	-	-	+	+	+	+	+	+	+		+	+	+
Podvržení falešného objektu zneužitím slabin vyhledávacích algoritmů		-	+	+	+	-	+	-	+	+	-	+	+	+	+		+	+	+
Potlačení služby		-	+	-	-	+	-	-	+	-	+	+	+	+	+		+	+	+

Tab. 11.1: *Sbrnutí jednotlivých typů útoku*

konecma

11.3 Protokoly a metody pro mapování prostředí – internetu

Útoky uvedené a taxonomizované v předcházející kapitole vycházely ze znalosti prostoru, v němž je útok prováděn, a byly studovány na obecném DIS. Je tedy zřejmé, že před začátkem útoku se musí útočník seznámit s prostorem a prostředím, ve kterém má útok uskutečnit.

V reálném případě se bude nejčastěji jednat o internet, a tedy prostředky „mapování" prostoru a prostředí útoku budou vycházet z reálných možností internetu. Mapováním prostředí pak budeme chápat postup, při kterém jsou získány znalosti o topologii internetu, propojení jednotlivých uzlů a případně charakter spojů. Následovně pak bude nutno zjištěné uzly identifikovat a ztotožnit s příslušnými charakteristikami zdrojů.

Celá struktura internetu, tak jak ji dnes známe, staví na rodině protokolů TCP/IP, a tak bude zřejmé, že právě tyto protokoly budou využity i k analýze a mapování prostoru internetu. V následujícím textu jsou uvedeny některé principy, používané pro mapování internetu, s jejichž různými modifikacemi se můžeme setkat nejčastěji.

11.3.1 Mapování s využitím protokolu ICMP

Jedním ze základních prostředků mapování je servisní protokol ICMP. Tento protokol slouží k signalizaci zejména mimořádných událostí v síti a pro účely mapování se nejčastěji používají aplikace spojené s tímto protokolem – příkazy `ping` a `tracert`, popř. jiné programy využívající vlastnosti ICMP protokolu[30].

Základní tvar rámce protokolu ICMP je uveden na obr. 11.11. Mechanismus práce protokolu spočívá v nastavení parametrů odesílaného paketu ICMP („request") a analýze přijaté odpovědi na tento paket („reply"). Protokol ICMP se šíří sítí stejným způsobem jako ostatní IP rámce a není chápán jako vyšší protokol, ale jako součást implementace IP. Hlavička ICMP zprávy obsahuje tři pole:

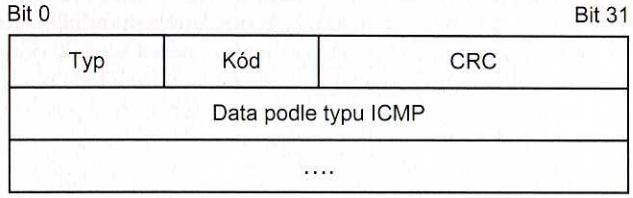
- ✓ TYP je pole s délkou jeden byte, kterým se identifikuje typ zprávy protokolu ICMP a tedy i způsob zpracování zprávy. Pro mapování sítě jsou důležité typy:
  - ✓ 0 – Echo Reply, což je paket odeslaný cílovým uzlem sítě zpět na základě doručení paketu Echo[31].
  - ✓ 3 – Destination Unreachable, chybový paket odesílaný tím uzlem sítě, který nemůže doručit ICMP paket na požadovanou adresu.
  - ✓ 8 – Echo, ověřovací paket odesílaný testovanému uzlu sítě, na jehož základě testovaný uzel sítě odpovídá paketem „echo reply".
  - ✓ 11 — Time Exceeded, tento typ zprávy je odesílán prvkem sítě, který zjistil, že pole TTL v záhlaví IP datagramu má hodnotu 0[32].

[30] Protokol ICMP je součástí rodiny IP protokolů a je definován v RFC792.

[31] Pakety Echo a Echo Reply jsou základním mechanismem práce příkazu ping.

[32] Pole TTL – Time to Live je obsaženo v záhlaví paketu IP protokolu a ve svém původním významu mělo zamezit nekonečnému cirkulování paketů v síti. Původní návrh rovněž počítal s údajem o době života paketu v sekundách, avšak později se ustálila metoda odečítání jedničky při každém průchodu síťovým zařízením. Pokud hodnota TTL dosáhne nuly, je síťové zařízení, které takový paket přijme, povinno jej zahodit.

- ✓ pole KÓD má rovněž délku jeden byte a jeho obsah se liší podle obsahu pole typ a upřesňuje význam přenášené zprávy,
- ✓ pole CRC tvoří kontrolní součet, který zajišťuje pouze první dva byty protokolu ICMP,
- ✓ pole DATA se liší se podle typu, ale chybové zprávy ICMP vždy obsahují prvních 64 bitů datagramu, který je chybou postižen nebo ji způsobil[33].



Obr. 11.11: *Struktura paketu ICMP*

Je zřejmé, že zprávy protokolu ICMP půjdou výhodně použít pro mapování internetu, zejména pak informace o překročené době života paketu. Jeden z případů signalizovaných kódem 0 udává, že položka TTL byla snížena na nulu. Tuto zprávu využívají programy jako `tracert` k tomu, aby zobrazily cestu datového paketu k cíli. Při použití uvedeného principu se zdrojového počítače odešle na cílový uzel paket ICMP „echo request" s hodnotou TTL nastavenou na jedničku. První síťové zařízení na cestě paketu jej zahodí, hodnota TTL tedy klesne na nulu, a vrátí ICMP zprávu „time exceeded". Zdrojový počítač tak dostane od prvního síťového zařízení paket „time exceeded", který v položce „adresa zdroje" má nastavenu adresu tohoto prvního síťového zařízení. Zároveň se měří časový interval mezi odesláním a příjmem paketu, tedy doba odezvy. Následovně se stejná procedura opakuje s hodnotou TTL=2, postupně se hodnoty TTL zvyšují o jedničku až do okamžiku, kdy je od cílového uzlu obdržena zpráva ICMP „echo reply". K ukončení může dojít i z jiných důvodů, např. pokud některý směrovač nezná další cestu. Pak je trasování zprávy ukončeno s hlášením ICMP „destination unreachable".

11.3.2 Použití protokolu UDP

Některé sítě blokují pakety protokolu ICMP a v tom případě je možné použít podobnou metodu, při níž jako nosného protokolu pro odezvu „time exceeded" jsou využívány datagramy protokolu UDP. Stejně jako v předchozím případě zdrojový počítač odešle datagram s hodnotou TTL nastavenou nejdříve na jedničku a očekává od směrovačů, jež se nacházejí na cestě k cíli, odezvy „time exceeded". Pokud některý směrovač po cestě filtruje použitý UDP port, pak vhodnou volbou čísla UDP portu lze nalézt vyhovující hodnotu. Je vhodné volit porty obecně velmi používaných služeb jako např. port 53 služby DNS. Tento typ trasováni používá většina běžně používaných trasovacích programů po předání vhodného parametru.

11.3.3 Použití protokolu TCP

Jak se za dobu existence ukázalo, oba výše uvedené protokoly nesou velká bezpečnostní rizika. Spojení UDP je velmi jednoduché např. unést, falšovat apod. ICMP, alespoň tedy některé jeho pracovní mody, jsou také poměrně náchylné na zneužití. Z těchto důvodů

[33] Vyšší protokoly obsahují v prvních 64 bitech významné údaje, na jejichž základě může operační systém rozhodnout o dalších příčinách chyby.

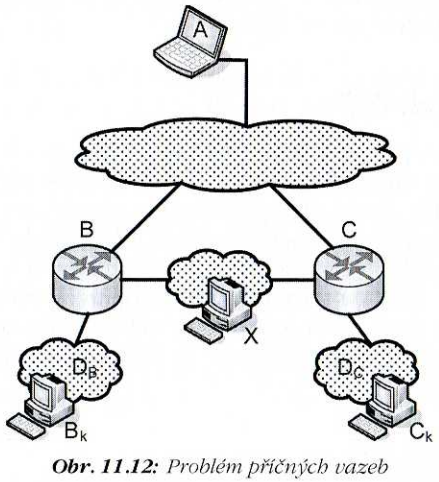
existuje v dnešním internetu trend filtrovat UDP datagramy a některé ICMP pakety, např. právě ty které využívají trasovací programy.

konecma

To vedlo k vývoji alternativy, využívající TCP pakety, která je založena na stejném principu jako předchozí, ale nosnou vrstvou je tzv. polootevřené spojení TCP SYN. Ze zdrojového počítače jsou na cílový počítač odesílány TCP pakety s nastaveným příznakem SYN (tzn. dochází k pokusu o sestavení nového spojení), které většina firewallů propouští. Samozřejmě je stejně jako v předchozím případě potřeba nalézt port, který daný firewall nefiltruje. Pokud je tento port na cílovém počítači zavřený, odešle zpět zdrojovému počítači TCP paket s příznakem RST, indikujícím, že port je zavřený a v případě, že je otevřený, odpoví cíl paketem s příznaky SYN a ACK. To je pro zdrojový počítač postačující reakce, neboť jakákoli odpověď potvrzuje přítomnost cílového uzlu nebo síťového uzlu na cestě paketu. Není tedy nutné, aby zdrojový počítač dále v navazování spojení pokračoval, a proto se spojení nazývá polootevřené. Použitím polootevřeného spojení TCP SYN je možno dosáhnout i některých dalších vylepšení mapovacích technik, např. implementace této metody jménem `tcptraceroute`[34] umí detekovat případ, kdy trasování projde překladem NAT[35] a získat o tom dostatek informací. V současném internetu, kde překlad adres je velice oblíbený a rozšířený, jde o neocenitelnou.

11.3.4 Problémy spojené s trasovacími metodami

Mapování používající trasovacích metod sebou přináší některé technické problémy, které mapování komplikují a ztěžují identifikaci prvků v internetu. Prvním z problémů můžeme nazvat „problémem příčných vazeb" a spočívá v tom, že struktura komunikačních linek tvoří v podstatě obecný graf. Představme si počítač A, ze kterého provádíme trasování, a jenž má přístup ke směrovači B, směřujícímu data do domény D_B, a ke směrovači C směřujícímu do domény D_C – viz obr. 11.12. Mezi směrovači B a C existuje příčná vazba, na níž leží síťový prvek D. Při statickém trasování z bodu A zůstane prvek D skrytý, protože cesta toku dat je určena při odchodu z A tzn. buď data půjdou přes B do domény D_B, nebo přes C do domény D_C.



Obr. 11.12: *Problém příčných vazeb*

[34] Podrobnosti může čtenář najit např. na *http://michael.toren.net/*.

[35] NAT – Network Address Translation je funkce směrovače pro mapování zdrojových nebo cílových IP adres mezi různými adresovými rozsahy. Nejběžnější je tzv. maškaráda, kdy směrovač adresy IP z nějakého rozsahu mění svoji IP adresu a naopak. Počítače ve vnitřní síti LAN za směrovačem používajícím maškarádu pak vystupují v internetu pod jedinou IP adresou.

Řešením tohoto problému je využití více různých zdrojů pro trasování, např. když zdrojem pro trasování bude počítač v doméně D_B a cílem trasování bude počítač v doméně D_C. V takovém případě data budou procházet doménou, v níž se nachází uzel D.

Jiným řešením je technika zvaná source-routing, kdy se mění způsob, jakým jsou pakety dopravovány po síti. Cesta, po které má být paket přenášen je předem určena zdrojem, ze kterého byl paket odeslán, proto název „source-routing". Informace o cestě, kudy se má paket pohybovat jsou umístěny v paketu. Jakmile paket dorazí ke směrovači, nerozhoduje o další pohybu paketu směrovač podle svých tabulek, ale podívá se do příslušného pole paketu, jenž určuje kam se má paket odeslat.

To je zásadní rozdíl oproti standardní technice směrováni „hop-by-hop", kde pakety obsahují pouze informaci o zdroji a cíli cesty a směrovače se samy rozhodují o nejvhodnější cestě paketu. Pro řešení problému příčných vazeb z předcházejícího příkladu můžeme použít techniku „source-routing" až v okamžiku, kdy víme o existenci směrovačů B a C[36]. V paketu, který zdrojový počítač použije pro source-routing nastavíme cíl v doméně DC, avšak jeho trasu specifikujeme tak, aby procházela směrovačem B. Pokud paket projde zjistíme, že mezi B a C se nachází vazba a její identifikace je identifikována stejným způsobem jako u ostatních technik trasování[37].

Nevýhodou trasování je fakt, že trasovací programy neidentifikují směrovače jako takové, ale pouze jejich síťová rozhraní. Přitom každý směrovač může mít několik síťových rozhraní, resp. tzv. „aliasů" rozhraní. K detekci „aliasů" slouží technika, odesílající na směrovač paket s neexistujícím číslem portu, na nějž přijde od směrovače jako odpověď zpráva protokolu ICMP „port unreachable". Nahlédnutím do zdrojové adresy tohoto paketu a jejím porovnáním s cílovou adresou paketu, který byl odeslán směrovači, lze zjistit, zda se jedná o alias (adresy jsou stejné) nebo nikoliv (adresy se liší).

11.4 Odhalování adresové struktury internetu

Protokoly a metody naznačené v předchozí kapitole umožní do jisté míry identifikovat faktickou propojovací strikturu internetu s tím, že informace získané během trasování vypovídají pouze o prvcích, které byly do trasování zahrnuty. Avšak, jak již název „internet" sám říká, podstatné nejsou prvky, ale sítě ze kterých se skládá. Rovněž pro útočníka nebude postačující znalost omezeného počtu prvků na trase k cílovému stroji, ale celé prostředí, které cílový stroj obklopuje. Je proto důležité se seznámit s celou sítí v okolí atakovaného stroje, které je popsáno zejména jeho adresovou strukturou.

11.4.1 Metoda využívající broadcast ping (všesměrový ping)

Metoda popsaná v kapitole 11.3.1 umožňuje sice mapování sítě pomocí protokolu ICMP, ale při prohledávání větší sítě je časově velmi náročná. Zároveň nedává možnost získat podrobnější adresovou strukturu sítě v okolí cílového stroje. Takového výsledku dosáhneme, když mapovací programy upravíme tak, aby používaly adresaci se zprávou ICMP „echo request" adresovanou celé subsíti[38]. Tento tzv. „broadcast ping" obdrží všechny uzly

[36] Směrovače B a C najdeme např. klasickým trasováním.

[37] Problém této metody je že, zdaleka ne všechny směrovače umožňují použití metody „source-routing", zejména pak malé „domácí" směrovače používané v některých menších sítích.

[38] To znamená, že adresa bude obsahovat '255' (zpráva typu „broadcast") nebo '0' (adrersa sítě) na posledním místě IP adresy uzlu, např. 192.168.222.255.

v subsíti a měly by na něj odpovědět[39]. Vyslanou zprávu a přijaté odpovědi můžeme využít k odhalování tvaru síťové masky dané subsítě. Uvědomíme-li si, že síťová maska vlastně určuje, která část IP adresy je adresou subsítě a která část je adresou uzlu, pak postupným zmenšováním délky síťové masky (tzn. zvětšujeme velikost subsítě) a sledováním odpovědi na odeslané zprávy můžeme získat tvar síťové masky dané subsítě. Předpokládejme, že pro odesílání zpráv typu broadcast ping použijeme následující algoritmus:

konecma

```
for mask_len = 31 to 7 do ;předpoklad, že délka masky je mask_len
{
 <sestav všesměrové adresy pro ´0´ a ´255´ a masklen>
 <odešli zprávu „echo request" na tyto adresy>
 if <více než dvě odpovědi na každý ping> then
return mask_len;
 else
continue;
}
```

Možná by se zdálo, že postačí odeslat pouze jeden typ adresy např. '255'. Nicméně v tom případě bychom mohli dojít ke špatnému závěru. Pokud budeme chtít zjistit např. síťovou masku pro adresu 123.56.255.2 a budeme předpokládat, že její skutečná maska má délku 16 bitů, budeme testovat pouze '255' ping. Když však budeme testovat masku délky 24 bitů pak použijeme adresu 123.56.255.255, což způsobí, že budeme testovat broadcast adresu pro subsíť 123.56. Při takovém testu dostaneme několik odpovědí, a tak mylně ve smyslu předcházejícího algoritmu usoudíme, že síťová maska je délky 24 bitů. Právě takové chybě můžeme zamezit při používání obou adres.

11.4.2 Odvozování masky na základě skupiny IP adres.

Tato technika je založena na znalosti několika podobných IP adres. Předpokládejme, že známe adresy uzlů A1, A2, A3 a víme, že všechny jsou vzdáleny jeden přeskok neboli „hop" od směrovače A, jehož rozhraní na straně těchto uzlů, má adresu A[40]. Cílem bude určit adresu subsítě, do které A1, A2 a A3 spadají a odpovídající síťové masky.

Metoda odvozování masky ze skupiny IP adres těží z faktu, že IP adresy spadající do stejné subsítě[41], musí mít jistou část IP adresy shodnou. A to nejméně tu část, která odpovídá adrese subsítě. Pro aproximaci adresy subsítě ze znalosti adres A1, A2, A3 použijeme operaci AND nad bity adresy, např. pokud rozhraní směrovače A bude 128.84.155.194, a adresy uzlů A1-A3 128.84.155.195, 128.84.155.222 a 128.84.155.218 pak postup bude následující[42]:

```
A   =     1100 0010    = 194D
```

[39] Je zřejmé, že metoda vyvolá značný datový tok v subsíti. Z důvodů ochrany před DoS útoky realizovanými tímto způsobem, je odpověď na „broadcast ping" často v operačních systémech potlačena.

[40] Tyto informace lze získat pomocí běžného trasování.

[41] Jsou stejně vzdáleny od rozhraní A, které jim je nejblíže.

[42] Pro zjednodušení jsou ve výpočtu vynechány první tři byty IP adres a zahrnut pouze poslední byte. Na výsledek úvahy nemá toto zjednodušení v daném případě žádný vliv.

```
A1  =     1100 0011    = 195D
A2  =     1101 1110    = 222D
A3  =     1101 1010    = 218D
AND =     1100 0010    = 194D
```

Výsledek operace AND nad bity adresy je 1100 0010, což je první odhad adresy subsítě vycházející z toho, že všechny bity mimo masku mohou nabývat libovolných hodnot. Nicméně, adresový prostor, poskytovaný hledanou subsítí musí pokrýt všechny adresy subsítě, což lze aproximovat operací OR nad bity adres, které máme k dispozici:

```
A   =     1100 0010    = 194D
A1  =     1100 0011    = 195D
A2  =     1101 1110    = 222D
A3  =     1101 1010    = 218D
OR  =     1101 1111    = 223D
```

V našem případě vrátí operace OR nad bity adres hodnotu 1101 1111, což vede ke druhému odhadu ukazujícímu, že adresový prostor hledané subsítě musí zahrnovat nejméně posledních 5 bitů. Vrátíme-li se k prvnímu odhadu masky subsítě a uvážíme-li skutečnost, že bity masky sítě musí zaujímat spojitou oblast adresy počínaje nejméně významným bitem, pak můžeme konstatovat, že

- ✓ subsíť nemůže být 1100 0010 podle našeho prvního odhadu,
- ✓ posledních pět bitů masky by mělo být ve tvaru 0 0000.

Z toho vyplývají čtyři možnosti adresy subsítě. Pokud první tři byty pokládáme za známé, pak poslední byte adresy subsítě může začínat 110, 11 nebo 1. V této chvíli není možno udělat přesnější odhad neboť máme k dispozici pouze čtyři adresy A, A1, A2 a A3. Pokud při dalším experimentování zjistíme, že např. existuje v subsíti adresa A4 ve tvaru 128.84.155.2 s posledním bytem v binární podobě 0000 0010, která je také vzdálena od A jeden hop, pak bitové AND bude 0000 0010, což eliminuje možnosti 110, 11 a 1. Nyní již můžeme vyvodit přesný závěr, že adresa subsítě je 128.84.155 a tedy síťová maska musí být 255.255.255.0. Tato metoda je přesná, pokud objevené IP adresy zkoumané subsítě jsou dostatečně rozprostřeny v adresovém prostoru dané subsítě, takže operace AND vrátí použitelný výsledek.

11.4.3 Hádání platných adres

Poslední metoda je založena na vybírání 32bitových hodnot, které s velkou pravděpodobností leží v adresovém prostoru zkoumané subsítě. Při výběru hodnot, které mají reprezentovat hádané adresy, se vychází z následující úvahy: získáme-li nějakou adresu ze zkoumané subsítě ve tvaru A.B.C.D, pak je pravděpodobné, že adresa A.B.C.1 bude rovněž platná, protože se používá často jako adresa směrovače subsítě. To by odpovídalo masce podsítě 255.255.255.0. Déle existuje vysoká pravděpodobnost, že získáme-li odezvu od síťového uzlu s adresou „k", pak bude existovat uzel s adresou ležící v malém okolí adresy „k", např. „k+1". Tato lokalita referencí prakticky znamená, že existuje-li např. adresa 123.58.2.50, pak je velká pravděpodobnost, že bude existovat i uzel s adresou 123.58.2.51.

Existují i další empirické vztahy mezi adresami, které mohu ledacos prozradit. Např. existuje-li IP adresa ve tvaru A.B.C.129, pak se často jedná o adresu směrovače pro subsíť s maskou

dlouhou 25 bitů. Totéž lze pozorovat např. u IP adresy ve tvaru A.B.C.193, která často náleží směrovači pro subsíť s maskou dlouhou 26 bitů atd. Na základě těchto pozorování můžeme využít následující heuristiku pro vygenerování dočasné množiny adres:

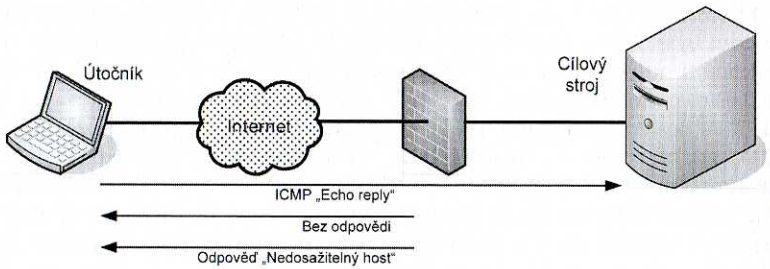
konecma

```
foreach <adresa od které máme odezvu>
{
<přidej do dočasné množiny N adres v okolí adresy, od které
    existuje odezva>;
 if (<adresa končí 1, 63, 129, nebo 193>)
<přidej N náhodných adres se stejným prefixem do dočasné mno-
    žiny>;
}
```

Výběr čísla N určí, jak agresivně bude heuristika plnit adresový prostor. Pokud je N velké, tak najde všechny aktivní uzly, ale také mnoho neplatných adres. Jestliže je N malé, tak většina odhadů je správných, avšak mnoho uzlů nemusí být nalezeno, protože algoritmus předčasně skončí.

11.4.4 Inverzní mapování

Inverzním mapováním nazýváme postup, při kterém se útočník pokouší pomocí skenování sítě získat informace o neaktivních adresách v chráněném segmentu sítě a na jejich základě zjistit adresy přiřazené aktivním zařízením ve zkoumaném segmentu sítě. Konfigurace sítě a princip inverzního mapování jsou na obr. 11.13.



Obr. 11.13: *Princip inverzního mapování*

Základní princip inverzního mapování spočívá na chování firewallu, který zamezí odezvě na pakety „Echo request" ICMP protokolu, ale propustí pakety odpovědi „Echo reply", neboť nemůže vědět, zda některý z počítačů za firewallem nevyslal požadavek „Echo request" a nečeká právě na odpověď.

Jednotlivé fáze inverzního mapování vyžadují nejdříve identifikovat síť, ve které je třeba najít adresy zařízení za firewallem. Následovně jsou odesílány pakety „Echo reply" na možné adresy v cílové síti a očekávám reakci. Pokud obdržíme odpověď ve formě paketu ICP „Host nedosažitelný", znamená to, že firewall nenalezl příslušný host na chráněné straně během ARP dotazu. Avšak pokud nedostaneme odpověď vůbec, pak je téměř jisté, že byla blokována firewallem a hledaná adresa se v chráněné síti vyskytuje. Získané informace je pak možno použít při vytváření topologie cílové sítě.

11.5 Generování topologie sítě

Vycházejíce ze známých protokolů, metod a principů popsaných v předchozích kapitolách můžeme rozšířit kusé informace o zkoumané cílové síti na postupy, sloužící k mnohem komplexnějšímu prozkoumávání internetu a topologie cílové sítě. Základní algoritmus použitý pro takovou činnost je většinou nějakou obdobou následujícího algoritmu:

```
<určit dočasnou množinu IP adres>
foreach <element v dočasné množině>
{
 if (<adresa je v dočasné množině je platná?>)
    {    <zjistit, zda a jak souvisí s ostatními adresami
    v „trvalé množině" a přidat ji do trvalé množiny>;
    <použít tuto adresu k vygenerování dalších IP adres a přidat
    je do dočasné množiny>
    }
}
```

Když výše uvedený algoritmus skončí, obdržíme podklad pro topologickou reprezentaci uzlů, směrovačů a subsítí. Obsah těchto informací je velmi závislý na modifikaci uvedeného algoritmu a na protokolu, který je pro zjišťování topologie sítě použit. Některé varianty si ukážeme v následujícím.

11.5.1 Implementace s protokolem SNMP

Algoritmus využívající protokol SNMP předpokládá, že tento protokol je realizován na všech prvcích sítě. SNMP (Simple Network Management Protocol), je protokol umožňující monitorovat zařízení, připojená do sítě a umožňující výměnu informací o konfiguraci a stavu uzlů sítě. Protokol se skládá ze tří hlavních komponent:

- ✓ „Managed device", což je síťový uzel existující ve spravované síti, který obsahuje zvláštní software – agenta SNMP. „Managed device" sbírá a skladuje řídicí informace a zpřístupňuje je pro řídicí systém NMS pomocí protokolu SNMP. Jako „managed device" mohou vystupovat veškerá adresovatelná zařízení, např. směrovače, servery, přepínače apod.
- ✓ SNMP agent je software umístěný na managed device, který má lokálně specifické znalosti o řídících síťových informacích „svého uzlu" a překládá je do formy kompatibilní se SNMP.
- ✓ Network Management System (NMS) je aplikace umožňující monitorování a správu přiřazených zařízení pomocí protokolu SNMP. V síti musí existovat alespoň jeden NMS, pokud má být síť prostřednictvím SNMP spravována.

Pro spuštění topologické analýzy sítě při použití modifikace obecného algoritmu využívajícího protokol SNMP musíme do prvotní dočasné množiny přidat směrovač, jenž je bránou pro uzel, ze kterého je prováděn průzkum[43]. Potom je možno analýzou směrovací tabulky

[43] Ten může být nalezen klasickým trasování ze zdrojového uzlu.

tohoto směrovače[44], která je dostupná pomocí protokolu SNMP, nalézt všechny sousední směrovače, jež tento, z našeho pohledu „kořenový" směrovač zná.

konec ma

Tyto směrovače přidáme do dočasné množiny a postupně hledáme pro každý směrovač v dočasné množině všechny jeho sousedící směrovače. Uzly podsítě, která náleží nějakému rozhraní tohoto směrovače, pak získáme ze záznamu v ARP tabulce směrovače[45]. Prohledávání sítě s pomocí protokolu SNMP a vytváření její topologie je velmi rychlé a přesné, neboť topologie sítě je vlastně uložena v jednotlivých směrovacích tabulkách (RouteTable a ArpTable), nicméně vyžaduje na všech směrovačích přítomnost agenta SNMP.

11.5.2 Použití DNS a broadcast ping

Pokud budeme zkoumat konkrétní doménu, můžeme použít pro její analýzu informace uložené na serveru DNS ve spojení s mechanismem „broadcast ping". Pro tento případ je nutno předpokládat, že daná doména umožňuje tzv. „DNS zone transfer[46]" a použití žádostí o odpověď na broadcast adresy. Nejdříve se provede „DNS zone transfer", kterým získáme adresy všech uzlů v doméně. Následovně je nutno eliminovat neplatná jména z adresového prostoru a určit všechny subsítě. Pro oba tyto úkony již známe metody – uzly prověříme žádostmi o odezvu, subsítě odhalíme pomocí některé z výše uvedených metod. Abychom se ujistili, že pomocí zone transferu jsme získali informaci o všech uzlech včetně uzlů v subsítích, použijeme broadcast ping na nově objevené subsítě. Algoritmus pro tento případ by tedy mohl vypadat následovně:

```
<dočasná množina> = <adresy získané z „DNS zone transfer">
foreach <uzel z dočasné množiny> do
    ping <tento uzel>;
if (<uzel se ozval>) then
    <trvalá množina> = <trvalá množina> + <tento uzel>;
<tato subsíť> = <funkce na odhalování subsítí>(<tento uzel>);
<trvalá množina> = <trvalá množina> + <tato subsíť>;
if (<tato subsíť> je neznámá?) then
    <broadcast ping>(<tato subsíť>);
foreach (<uzel který odpovídá>) do
{
    <přidej uzel, který odpovídá do této subsítě>;
    <dočasná množina> = <dočasná množina> + <uzel který odpovídá>;
};
```

[44] V tabulce ipRouteTable (MIB entry) tohoto směrovače příkazem GetIpRouteTable.

[45] Opět prostřednictvím protokolu SNMP příkazem GetArpTable.

[46] Jedná se o mechanismus umožňující replikaci databází jmenných serverů DNS, které slouží k překladům.

Tento algoritmus bohužel není ani efektivní, ani rychlý, neboť odhalování subsítí je pomalé. Navíc silně závisí na dostupnosti „DNS zone transfer" a odezvách na broadcast, které nemusí být z bezpečnostních důvodů dostupné.

11.5.3 Použití trasování

Poslední diskutovaná metoda se nespoléhá na tak silné předpoklady jako je přítomnost SNMP či DNS zone transfer, jako metody předchozí, ale staví na pravděpodobnostní heuristiky podobné jako při odhalování subsítí. Jediným předpokladem pro realizaci tohoto algoritmu je podpora trasování a funkce „DNS lookup", která vrátí všechny IP adresy, asociované s příslušným směrovačem. Základní myšlenka tohoto postupu spočívá ve vytvoření náhodných IP adres spadajících do adresového prostoru domény. Trasováním standardními postupy, které bude zaměřeno na tyto adresy, odkryjeme další směrovače v síti a metoda pro odhalování subsítí založená na množině několika známých IP adres pak odhalí danou subsíť.

Algoritmus této metody by se choval podobně jako algoritmus pro odhalování podsítí pomocí omezené množiny uzlů (viz kapitola 11.4.3). Vzhledem k tomu, že algoritmus používá jen příkazy ping, standardní „DNS lookup" a trasování, je široce použitelný. Problém spočívá ve stanovení správné velikosti přídavku ke skupině adres, tedy v původním značení „N". Abychom odhalili všechny uzly musíme volit N velké, což algoritmus znatelně zpomaluje. Pro N malé zase nemusí být všechny uzly nalezeny, a tak je uvedená metoda vhodná zejména tam, kde více záleží na odhalení směrovačů a subsítí než na odhalení všech uzlů.

11.6 Identifikace zdrojů v internetu

Pod pojmem zdroj v síti nebo zdroj v internetu budeme rozumět objekt, který nabízí nějaké informace, popř. je sám o sobě je nositelem takové informace[47]. Příkladem prvního objektu může být např. server připojený do sítě, příklad druhého objektu jsou dokumenty, obrázky a jiné soubory.

Identifikací zdroje budeme rozumět proces sloužící k určení druhu informací, které příslušný zdroj poskytuje. Míra přesnosti a hloubky určení charakteru zdroje informací je samozřejmě relativní. V některých případech bude k identifikaci zdroje postačovat např. zjištění, že se jedná o webovský zdroj, jindy bude nutno určit k jaké „vnitřní" aplikaci tento webovský zdroj slouží, např. zdroj napojený na aplikaci sloužící k poskytování bankovních služeb.

Internetový zdroj je v konečném důsledku většinou aplikace, poskytující nějaké informační služby. Tak jako IP protokol jednoznačně identifikuje výpočetní systém v internetu, protokol TCP (resp. UDP) identifikuje aplikaci na tomto systému. Proto jednoznačná lokace a identifikace internetového zdroje ve výše uvedeném smyslu je určena trojicí IP adresa, port, transportní protokol.

Organizace IANA, resp. pro Evropu RIPE, přiděluje tzv. „dobře známé porty". To jsou porty, jejichž číslo je přiděleno konkrétní službě a následně uveřejněno, takže pokud někdo chce využívat tuto službu, dopředu ví, na jaký port se má s žádostí obrátit. Základní identifikační proces pracuje tak, že pokud je známa existence informačního zdroje v nějaké lokaci, tzn.

[47] Mohli bychom odlišit ještě prvek sítě, což je objekt související přímo se síťovou strukturou, např. směrovač, přepínač nebo subsíť.

je známa adresa a číslo portu, pak stačí podle seznamu dobře známých portů identifikovat charakter zdroje podle čísla portu. Celá věc však má několik problémů:

konecma

- ✓ Standard IANA je pouze doporučení, a to nezabrání případným odlišným realizacím - zdroje mohou poskytovat informace na nestandardních portech, nebo na standardních portech poskytovat jiné služby.
- ✓ Zdroj vůbec nemusí mít přiděleno číslo portu organizací IANA, a to zejména v případě, kdy se bude jednat o specifickou aplikaci, která využívá vlastních „volných" čísel portů.
- ✓ Je aplikování řízení přístupu k informačnímu zdroji, jako firewally, aplikační ochranné mechanismy, apod. To vede k nepřístupnosti portu nebo zkreslení jeho původní úlohy.

11.6.1 Skenování portů

Při skenování portů odesíláme na cílový počítač odesílány specifické pakety, většinou žádosti o připojení[48] nebo zprávy „echo" protokolu ICMP, s cílem nalézt službu, běžící na příslušném portu. Pokud je standardní port otevřen a tedy služba lokalizována, už není problémem vytvořit generické připojení a pomocí dotazu na aplikační úrovni zjistit parametry očekávané služby.

Většina aplikačních protokolů v tomto případě usnadňuje práci v tom smyslu, že ihned po připojení odešle nějaký druh uvítací zprávy, např. OpenSSH odešle ihned po připojení klientovi zprávu „SSH-2.0-OpenSSH_4.1". Problém je s aplikacemi, které se takto nechovají nebo jsou umístěny na nestandardních portech. V tomto případě obvykle útočník nejprve odešle nějaký nesmyslný požadavek, většinou obsahující problematické a nestandardní znaky, počká, zda aplikace odpoví chybou. Z chybové zprávy většinou nebývá problém zjistit, o jakou aplikaci se jedná, a tedy i jakou informační službu poskytuje.

11.7 Techniky identifikace operačního systému

Jednou ze základních a prakticky nejdůležitějších informací pro útočníka je informace o operačním systému běžícím na cílovém stroji. Pokud to není zřejmé z otevřených zdrojů, bude nutno použít vhodné metody, které útočníkovi umožní zjistit charakter operačního systému „na dálku", tedy bez řádného uživatelského přístupu na příslušný cílový stroj. I když většina počítačů v síti podporuje výměnu dat v rodině protokolů TCP/IP, budou existovat sítě např. IPX, AppleTalk nebo Token Ring, které jsou dodnes podporovány poměrně malou podmnožinou operačních systémů. V následujícím se zaměříme na vzdálenou identifikaci systémů připojených přes sítě podporující TCP/IP, přičemž budeme rozeznávat dva základní přístupy k identifikaci operačního systému:

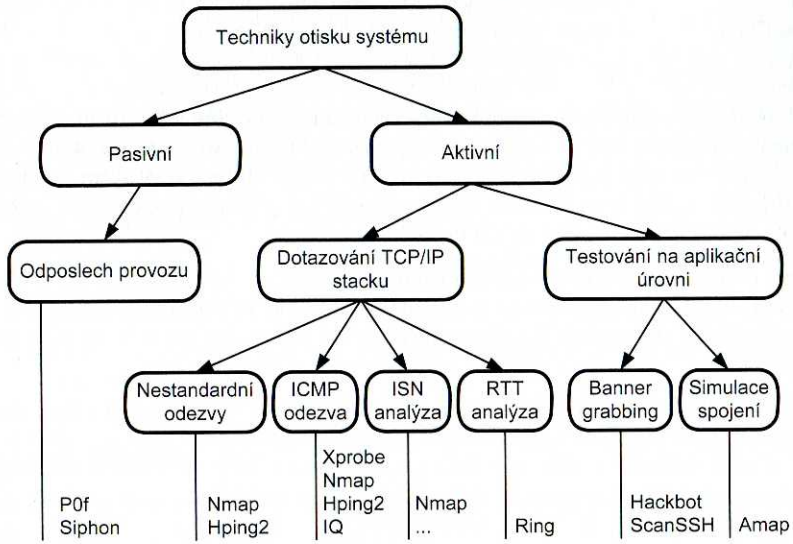
- ✓ Aktivní identifikací operačního systému se rozumí metoda, při které jsou zdrojovým počítačem vyvolávány reakce cílového stroje. Na základě charakteru odpovědi cílového stroje se útočník snaží o co nejúplnější a nejpřesnější určení operačního systému běžícího na vzdáleném stroji. Tento způsob není příliš vhodný pro útočníka, protože ten riskuje odhalení již při prvních pokusech o identifikaci zařízení v síti.
- ✓ Pasivní identifikace je založena na odposlechu zpráv generovaných cílovým strojem. I když v tomto případě je útočník nezjistitelný, doba potřebná pro identifikaci systému je mnohem delší a počet míst, kde je možno pakety odesílané cílovým stroje odchytit je velmi omezen.

Obecně je možno říci, že aktivní způsoby identifikace systému jsou mnohem rychlejší než metody pasivní. Ty naopak chrání útočníka před odhalením, avšak za cenu větších obtíží při výběru místa odposlechu paketů. Tab. 11.2 shrnuje vlastnosti jednotlivých způsobů identifikace [F04].

Aktivní identifikace		Pasivní identifikace	
Pro	Proti	Pro	Proti
rychlá	snadno zjistitelná	extrémně utajená	zdlouhavé zjišťování
nemá zvláštní požadavky na přístup k cílovému stroji	citlivá na klamavé odezvy	velmi přesná	vyžaduje specifický přístup k cílovému stroji
	nepřesná, pokud je modifikován IP stack	imunní vůči klamavým odezvám	vyžaduje jeden nebo více SYN paketů
	vyžaduje řadu otevřených portů		nepřesná, pokud je modifikován IP stack

Tab. 11.2: *Porovnávací tabulka základních metod zjišťování OS*

Znalost postupů pro zjištění operačního systému, označovaných často jako „OS fingerprinting", je klíčová jak pro útočníka, tak pro bezpečnostního administrátora, který se naopak snaží těmto postupům zabránit. Rozdělení jednotlivých technik spolu s uvedením typických programů, které tuto techniku používají, je na obr. 11.14.



Obr. 11.14: *Techniky otisku systému – rozdělení*

[48] Např. TCP connect() nebo TCP SYN half-open.

Z výše uvedeného je zřejmé, že pro přesnější určení operačního systému a jemnější rozlišení mezi verzemi bude vhodné kombinovat jednotlivé metody. Přitom je potřeba, aby vybraný sortiment metod splňoval např. uvedená kriteria[49]:

konecma

- ✓ Přesnost, tedy schopnost detekovat operační systém správně.
- ✓ Neutralita vůči firewallům, resp. transparentnost; to znamená, že by metoda by měla používat protokoly a postupy takové, aby procházet firewallem, aniž by si ten průchodu všiml.
- ✓ Malá síťová zátěž spočívá nejen v co nejmenším počtu odeslaných paketů potřebných pro zjištění operačního systému, ale také v jejich vhodném výběru (nepoužívají nebezpečné pakety).
- ✓ Rozšiřitelnost, aplikace sloužící k rozpoznávání charakteru operačních systémů musí umožňovat jednoduché doplnění nové vzorů a detekčních metod do databáze.
- ✓ Rychlost, která by umožnila detekci v krátkém čase, a tak i sken rozsáhlých sítí a zjištění všech operačních systémů v nich běžících.

11.7.1 Metoda „banner grabbing"

Tato metoda je velmi jednoduchá, neboť vychází z informací, které o sobě sám systém poskytne při připojení v úvodní oznamovací zprávě, tzv. „banneru". Většina metod používajících „banner grabbing" nevyžaduje žádný speciální program, mnohdy se stačí připojit na příslušný server jako v následujícím příkladu, kde byl banner získán při ohlášení ftp služby serveru:

```
>> telnet.exe ftp.xxxxxxxx.cz 21
<< 220 ProFTPD 1.2.9 Server (ftp.sauto.cz) [ftp.sauto.cz]
>> SYST
<< 215 UNIX Type: L8
```

Z výše uvedeného příkladu je zřejmé, že bez jakýchkoli problému lze zjistit, že testovaný server používá systém Unix[50]. Není to sice nijak přesná informace, ale již znatelné omezení možností. Do této části nepřímo spadá i vyvolání chyby služby na cílovém počítači, protože příslušná služba často – není-li nastavena správně – často vypíše detailní informace o chybě, ze kterých lze často mnoho vyčíst.

Podobné informace do svých odpovědí zahrnují i ostatní služby. Správci o tom vědí, a tak často nahrazují standardní bannery upraveným textem, který nemá tak významnou vypovídací schopnost, nebo uvádí klamavou informaci. Z těchto důvodů není metoda bannerů příliš spolehlivá.

Existují však další formy „grabbingu", např. „grabbing" souborů. Jedná se zejména o spustitelné soubory a knihovny a pro rozlišení např. mezi operačními systémy Unix a MS Windows lze využít i textové soubory. Každý operační systém má svůj formát pro ukládání spustitelného kódu a analýzou jeho struktury lze přibližně určit typ operačního systému. Jedinou obranou proti tomuto typu „grabbingu" je zajistit, aby se útočníkovi nedostal do rukou žádný soubor, což je v praxi nemožné. Avšak z hlediska správce systému je výhodou, že uvedená metoda určí typ operačního systému jen velmi zhruba.

[49] V praxi samozřejmě nejsou všechny tyto požadavky splněny.

[50] V tomto případě byla verze systému vyžádána přímo od serveru příkazem SYST, který je možno zadat ještě před přihlašovací procedurou. Takový postup je běžný zejména u serverů se službou FTP, aby protější strana věděla, jaký formát výpisů má očekávat. Ne vždy však tento příkaz odpoví správně. Dnes se běžně používá unixový výpis souborů, a tak většina serverů, i ty které běží např. pod Windows odpoví na příkaz SYST právě řetězcem UNIX a L8.

11.7.2 Skenování otevřených portů

Se skenováním portů jsme se již setkali u identifikace zdrojů v internetu. Tehdy bylo celkem jedno zda daný port byl otevřen nebo zavřen. Při identifikaci operačního systému slouží otevřený port ke dvěma možným účelům:

- ✓ v přípravné fázi je použit pro některé druhy aktivního rozpoznávání operačních systémů,
- ✓ přímé využití k rozpoznávání operačních systémů.

Nejjednodušší způsob využití otevřených portů pro identifikaci operačního systému je podle služeb, neboť každá specifická služba má standardně přidělen určitý port. Podle otevřených portů lze tedy odhadnout, jaké služby na počítači běží, a tedy i přibližně jaký operační systém je na počítači instalován. Zjistíme-li na serveru otevřený port např. 1433, pak snadno zjistíme, že tento port je standardně přiřazen MS SQL Serveru. Pokud není tento port administrátorem přiřazen jiné aplikaci, pak na něm také MS SQL pravděpodobně běží. A jelikož MS SQL Server je pro platformy MS Windows, lze předpokládat, že na cíli běží OS z této řady.

Tato metoda je obecně málo spolehlivá, neboť pro administrátory není problém porty jednotlivým službám měnit, zejména jedná-li se o privátní síť[51].

11.7.3 Dotazování IP zásobníku

Pod dotazováním IP zásobníku rozumíme zjišťování, jakým způsobem se chovají některé vrstvy IP protokolu cílového počítače. Tyto vrstvy jsou řízeny ovladači, které jsou buď přímo ovládány jádrem operačního systému nebo s ním jsou velmi těsně propojeny. I když chování TCP/IP protokolu je definováno v příslušných standardech, jednotlivé implementace se mezi sebou v detailech liší. Je to způsobeno zejména tím, že v některých ohledech není definice TCP/IP naprosto striktní, někde ponechává určitou volnost způsobu implementace a některé části jsou nepovinné. Mezi metody dotazování IP zásobníku patří např.:

- ✓ zjišťování reakce cíle na nestandardní pakety,
- ✓ zjišťování reakce na jednotlivé požadavky protokolu ICMP,
- ✓ nalezení parametrů IP a TCP protokolu.

Protože jednotlivé metody se vzájemně prolínají je následující text dělen podle přístupu k datům obsaženým v paketech.

11.7.3.1 Analýza paketu

Analýza dat, která jsou obsažena v paketu odeslaném cílovým strojem při běžném provozu nebo na útočníkův požadavek, je metoda s celou řadou variant stavících na drobných odlišnostech implementace protokolu. Typickým příkladem je metoda používající odeslání paketu na zavřený port.

[51] Pro veřejný server nemá smysl čísla portů měnit, těžko by se na něj pak přistupovalo.

V tomto případě nejdříve vyhledáme zavřený port na cílovém stroji. Na tento port odešleme např. libovolný UDP paket a očekáváme odpověď ICMP – „Port nedosažitelný". Celá procedura je na obr. 11.15. Je zřejmé, že paket odpovědi má uvedenu jinou délku pole v kopii záhlaví původního UDP paketu než byla původně uvedena. Toto je typická odpověď pro operační systém OpenBSD 2.8.

konecma

```
15:47:25.342182 ppp0 > 32.101.233.50.53783 > y.y.y.y.32132:
udp 70 (DF) (ttl 250, id 57568)
                        4500 0062 e0e0 4000 fa11 1dad 2065 e932
                        yyyy yyyy d217 7d84 004e 2db9 0000 0000
                        0000 0000 0000 0000 0000 0000 0000 0000
                        0000 0000 0000 0000 0000 0000 0000 0000
                        0000 0000 0000 0000 0000 0000 0000 0000
                        0000 0000 0000 0000 0000 0000 0000 0000
                        0000
                                                IP – pole celkové
                                                délky se liší o 20 bytu
15:47:25.652182 ppp0 < y.y.y.y > 32.101.233.50: icmp: y.y.y.y
udp port 32132 unreachable
Offending pkt: 32.101.233.50.53783 > y.y.y.y.32132:
udp 70 (DF) (ttl 238, id 57568) (ttl 241, id 61090)
  Záhlaví IP ──→ 4500 0038 eea2 0000 f101 5925 yyyy yyyy
                 2065 e932 0303 7f59 0000 0000 4500 004e
  ICMP ──────── e0e0 4000 ee11 29c1 2065 e932 yyyy yyyy
                 d217 7d84 004e 2db9
```

Obr. 11.15: *Analýza paketu odpovědi na UDP paket*

K aktivní detekci lze využít i protokolu ICMP. Zjišťováním, na které požadavky cíl odpoví, případně jakým způsobem, lze zjistit velké množství informací. Pro detekci se nejčastěji používají pakety:

- ✓ ICMP ECHO s úmyslně špatným zadáním CODE (které má být 0); některé operační systémy totiž při obdržení požadavku ECHO položku CODE kontrolují a jiné ne – podle odezvy lze zjistit, do které skupiny cílový operační systém patří.
- ✓ ICMP GetAddressMask – požadavek velmi vhodný pro detekci operačního systému, protože mnoho operačních systémů tento požadavek nepodporuje a neodpoví na něj.
- ✓ ICMP GetTimestamp – podobně jako v předchozím případě je podporován pouze některými operačními systémy.

Příkladem může být analýza odpovědi na paket ICMP „Echo request", tak jak je uvedeno v obr. 11.16. Zde je analyzována odpověď paket ICMP „Echo reply", který se v případě operačního systému Windows 2000 liší hned ve dvou parametrech.

Programy specializované na odhalování operačních systémů provokují cílový systém k odesílání obdobných paketů a odpovědi porovnávají s vlastní databází „otisků". Pro zajištění vysoké pravděpodobnosti správné identifikace je třeba např. až sedmnácti shodných znaků neboli stejného množství testů cílového systému.

```
17:13:13.081831 ppp0 > x.x.x.x > y.y.y.y: icmp: echo request (DF)
[tos 0x6,ECT]  (ttl 250, id 2779)
                        4506 0044 0adb 4000 fa01 a9a9 xxxx xxxx
                        yyyy yyyy 087b 2fff a51e 2267 0000 0000
  IP záhlaví            0000 0000 0000 0000 0000 0000 0000 0000
  TOS = 0               0000 0000 0000 0000 0000 0000 0000 0000
                        0000 0000
17:13:13.231831 ppp0 < y.y.y.y > x.x.x.175: icmp: echo reply (DF)
(ttl 115, id 59514)
                                                Kód = 0
                        4500 0044 e87a 4000 7301 5310 yyyy yyyy
                        xxxx xxxx 0000 387a a51e 2267 0000 0000
                        0000 0000 0000 0000 0000 0000 0000 0000
                        0000 0000 0000 0000 0000 0000 0000 0000
                        0000 0000
```

Obr. 11.16: *Analýza odpovědi na paket ICMP*

Další možností je analýza paketu SYN při pokusu o navázání spojení s cílovým strojem [T03]. Takový pokus je celkem běžnou procedurou a nebude tudíž vypadat příliš podezřele. Základem je odeslání paketu TCP SYN sloužící k navázání spojení. Po přijetí tohoto paketu cílový stroj odešle útočníkovi paket SYN-ACK a již z hlavičky tohoto paketu je možno zjistit celou řadu údajů. Jedna z možností je např. analýza položky „Time To Live" protokolu IP, který různé operační systémy nastavují různě – viz tab. 11.3 Hodnoty TTL pro různé systémy.

Operační systém	TTL	Operační systém	TTL
AIX	60	Solaris 2.x	255
Cisco Router ISO 12.2.1	255	SunOS 4.1.3/4.1.4	60
DEC Pathworks V5	30	Ultrix V4.1/V4.2A	60
FreeBSD 2.1R	64	VMS/Multinet	64
HP/UX 10.01	64	VMS/TCPware	60
HP/UX 9.0x	30	VMS/UCX	128
Irix 5.3	60	VMS/Wollongong	128
Irix 6.x	60	Windows 2000	128
Linux 2.2	64	Windows 95	32
Linux 2.4	64	Windows 98	32
MacOS/MacTCP 2.0.x	60	Windows 98 SE	32
NetGear FM114P	64	Windows for Workgroups	32
penBSD 2.9	64	Windows ME	128
OS/2 TCP/IP 3.0	64	Windows NT 3.51	32
OSF/1 V3.2A	60	Windows NT 4.0	128
QNX Neutrino OS	255	Windows XP Professional	128

Tab. 11.3: *Hodnoty TTL pro různé systémy*

Většina operačních systémů používá doporučenou standardní hodnotu z RFC, např. téměř všechny OS MS Windows používají standardně hodnotu 128. Položka TTL není jediná, která se liší podle implementace operačních systémů. Databáze, vybudované pro „OS fingerprinting", obsahují celou řadu detailních hodnot jednotlivých bitů v hlavičkách a ostatních částech protokolů, které se liší podle druhu operačního systému. Analýzu

paketu je možné provádět jak při aktivním rozpoznávání operačních systémů vyvoláním nějaké odpovědi, tak i při pasivní analýze zachycených paketů.

konecma

11.7.3.2 Využití paketů nulování – RST

Při základní operaci připojování k serveru v síti odpoví server paketem SYN-ACK pro další postup při vytváření spojení. Pokud ale port, na který je směrován požadavek na vytvoření spojení, bude uzavřený, server odpoví paketem RST-ACK, tedy paketem s nastaveným bitem nulování. Analýzou tohoto paketu můžeme zjistit řadu informací o operačním systému vzdáleného počítače, aniž bychom spojení s ním skutečně vytvořili. Tabulka 11.4 ukazuje odezvy RST-ACK spolu s příslušnými identifikovanými operačními systémy [I07].

Operační systém	Délka paketu	IP ID	DF	TTL	Sekv. číslo	Okénko
Solaris8	40	>0	1	64	0	0
WinME, Win2K Server	40	>0	0	128	0	0
RedHat Linux 2.4.2	40	=0	1	255	0	0
RedHat Linux 2.0.30	40	>0	0	255	0	0
AIX Version 4	40	>0	0	60	0	0

Tab. 11.4: *Odezvy vybraných operačních systémů v paketu RST-ACK*

11.7.3.3 Zjišťování časových intervalů

Mezi jednu z nejpřesnějších metod identifikace operačních systémů patří analýza časových intervalů mezi opakovanými odpovědmi SYN-ACK. Základ metody spočívá ve vyslání SYN paketu k cílovému stroji, který odpoví paketem SYN-ACK. Korektní procedura zahrnuje povinnost zdrojového stroje, tedy toho, který odeslal paket SYN, aby na paket SYN-ACK odpověděl potvrzovacím paketem ACK. Pokud cíl do určité doby neobdrží paket ACK, zkusí znovu vyslat SYN-ACK, neboť předpokládá, že se paket ztratil.

Analýza počtu opakování a časových intervalů mezi opakovanými pakety je základem identifikační metody. Zdrojový stroj, který vyslání paketu SYN-ACK inicioval, sice bude přijímat a zaznamenávat tyto pakety, ale potlačí odpovědi ACK. Ve chvíli, kdy cílový stroj ukončí vysílání odpovědí ACK, porovná se počet zachycených paketů SYN-ACK a časové intervaly mezi pakety s údaji uloženými v databázi a vybere se ten operační systém, který má nejbližší hodnoty ke zjištěným. Úspěšnost této metody v praxi přesahuje 95 % a ve spojení s jinými metodami je téměř stoprocentní.

OS	Počet opakování	Intervaly [s]
Linux 2.2.14	7	3,5-6,5-12,5-24,5-48,5-96,5-120,5
Linux 2,4	5	4,26-6-12-24-48,5
Windows 98	3	3-6-12
Windows 2000	2	3-6
FreeBSD 4.	4	3-6-12-24[52]

Tab. 11.5: *Intervaly a počet opakování pro jednotlivé operační systémy*

[52] Pokud nepřijde odpověď ACK do 30 s od poslání posledního SYN-ACK, vyšle se ještě paket RTS (Reset).

Vzhledem k tomu, že algoritmus používá standardní způsob navazování spojení, je obrana proti tomuto typu útoku velmi obtížná. Jedinou možnou obranou je buď omezení počtu SYN-ACK paketů propuštěných přes firewall nebo instalace speciálních programů, které kompletně simulují IP zásobník jiného operačního systému. Pokud je takovýto program dostatečně kvalitní, pak dokáže zmást většinu pokusů o detekci operačního systému.

11.7.4 Pasivní detekce OS

Metody pasivní detekce jsou vlastně podmnožinou metod aktivní detekce s tím, že si útočník nemůže vyžádat takový typ paketu, který by potřeboval, ale musí čekat, než takový paket bude cílovým počítačem vyslán. Na druhou stranu však pasivní detekce je těžko odhalitelná a může získávat SYN pakety, které jsou velmi bohatým zdrojem pro analýzu.

11.7.4.1 Analýza SYN paketů

Jak již bylo vzpomenuto, analýza SYN paketů je bezesporu nejsilnější metodou pasivní detekce operačních systémů. Využívá se při ní většina údajů z hlaviček protokolů TCP i IP, které jsou neocenitelným zdrojem informací pro identifikaci systému.

	Bity 0 - 3	4 - 9	10 - 15	16 - 31
0	Zdrojový port			Cílový port
32	Sekvenční číslo paketu			
64	Číslo potvrzení paketu			
96	Ofset dat	Rezervováno	Příznaky	Okénko přenosu
128	Kontrolní součet			Ukazatel „Urgent"
160	Volitelné pole			Výplň
+	Data			

Obr. 11.16: *Hlavička protokolu TCP*

Struktura hlavičky protokolu TCP je na obr. 11.16 a jednotlivá pole znamenají:

- ✓ Zdrojový port je port procesu generujícího datagram.
- ✓ Cílový port určuje, kterému procesu na cílovém uzlu jsou data určena[53].
- ✓ Sekvenční číslo prvního datového bytu v segmentu (pokud není nastaven příznak SYN). Pokud je nastaven příznak SYN, jedná se o tzv. „initial sequence number" (ISN) a první datový byte má číslo ISN + 1.
- ✓ Číslo potvrzení paketu má význam pouze když je nastaven kontrolní bit ACK a je nastaveno na hodnotu, již odesílatel očekává v poli „Sekvenční číslo" v následujícím paketu. Je-li ustaveno spojení, je toto číslo vždy posíláno.
- ✓ Ofset dat je číslo vyjádřené odpovídající posunu o 32bitová slova. Indikuje, kde v segmentu začínají data přenášená tímto datagramem.
- ✓ Rezervované šestibitové pole by mělo být vždy nulové.

[53] Port je číslo, které rozlišuje proces v rámci uzlu. Při navazování spojení nejsou důležité pouze IP adresy, ale i čísla portů. Informace tvořená dvojicí <IP adresa, číslo portu> je nazývána „socket" a představuje úplnou informaci o cíli TCP komunikace.

konecma

- ✓ Příznaky zajišťují „handshaking" a ostatní procesy související s přenosem. Jejich význam je:
  - ✓ URG – platný ukazatel hodnoty „Urgent".
  - ✓ ACK – potvrzení přijetí, „Acknowledgement".
  - ✓ PSH – funkce „Push", související s agregací dat na jednotlivých vrstvách protokolu.
  - ✓ RST – nulování spojení, „Reset".
  - ✓ SYN – synchronizace sekvenčních čísel.
  - ✓ FIN – oznámení, že odesílající nemá žádná další data.
- ✓ Okénko přenosu ukazuje množství dat bytech, které je potvrzováno najednou.
- ✓ Kontrolní součet není povinný a může být 0.
- ✓ Ukazatel „Urgent" je platný pouze pokud je nastaven příznak URG a ukazuje na konec datové části, která má být přednostně zpracována.
- ✓ Volitelné pole je pole proměnné délky určené pro volitelné parametry TCP, parametr je používán např. pro indikaci maximální velikosti segmentu, kterou je přijímající strana schopna zpracovat apod.
- ✓ Výplň je potřebné množství nulových bitů doplňujících hlavičku tak, aby ležela na 32bitové hranici.

Veškeré údaje uvedené v hlavičce protokolu při tvorbě spojení jsou důležité pro určení operačního systému. Položky jako „Time to Live" nebo „Defragment" v hlavičce IP protokolu spolu s údaji v paketu TCP-SYN při navazování TCP spojení, např. velikost okénka, jsou pak výchozími údaji pro prohledávání databáze otisků systému.

Významným zdrojem informací je volitelné pole („Options"), které může být až 44 bytů dlouhé, obsahovat až 256 různých voleb a celou řadu podrobných údajů. Struktura každého volitelného údaje obsahuje typ volitelného údaje (8 bitů) jeho délku (8 bitů) a data příslušející tomuto volitelnému údaji, jejichž délka se může různit. Mezi nejzajímavější údaje pro identifikaci systému patří:

- ✓ NOOP – „No operation", jednobytové pole, které slouží k zarovnání volitelného pole na hranici slova nebo poloviční slova, pokud je to zapotřebí.
- ✓ MSS – maximální velikost segmentu; tento údaj se udává při navázání spojení a určuje jakou maximální velikost segmentu může akceptovat přijímající strana.
- ✓ Window Scale – je násobitel umožňující měnit nastavení okénka v hlavičce protokolu TCP[54].
- ✓ SACK permitted – povoluje selektivní potvrzování paketů, což je využíváno v případě, kdy dochází k velké ztrátovosti paketů při přenosu.
- ✓ Timestamp – časová značka, která se užívá ke dvěma účelům: pro měření doby oběhu paketu, tzv. RTTM (Round Trip Time Measurement) a k ochraně proti zacyklení sekvence paketů.

[54] Změna měřítka je omezena na mocniny dvou a je kódována logaritmicky, což znamená, že měřítko lze implementovat pouhým bitovým posunem hodnoty okénka.

Výsledkem je identifikace operačního systému, která se nemusí jenom vztahovat k nějakému serveru, ale může to být i operační systém síťového prvku, např. směrovače, který vypoví dostatek informací o slabinách dotčených zařízení. Některé operační systémy a konkrétní hodnoty vybraných polí jsou podrobněji popsány dále.

11.7.4.2 Linux

Pole TTL v hlavičce IP protokolu je u operačního systému Linux standardně nastaveno na 64, velikost okénka v hlavičce TCP se liší podle verze. Operační systém Linux řady 2.2 nastavuje velikost okénka na hodnotu 32120, zatímco verze 2.4 pouze na 5840.

Sekvenční číslo je dalším obvyklým předmětem zkoumání. Linux standardně tuto hodnotu nastavuje v průběhu relace s každým odesílaným paketem vždy o jedničku vyšší. Důležitější ale je, že pro každou novou relaci generuje novou náhodnou hodnotu[55]. Pokud tedy dostaneme několik SYN paketů, měly by tyto hodnoty být vzájemně velmi odlišné.

Nastavení volitelného pole TCP (options) je zajímavé jak s ohledem na obsah těchto voleb, tak i na počet a typ voleb, které jsou operačním systémem implementovány. U Linuxu je standardně podporovány: MSS, SACK permitted, Timestamp, Window Scale a NOOP.

Linux je však jedním z těch operačních systémů, o jehož identifikaci vypovídá již délka SYN paketu. Je to jediný operační systém, který má délku SYN paketu šedesát bytů[56], což sice stačí k určení operačního systému, ale již ne jeho verze.

11.7.4.3 OpenBSD

Operační systém OpenBSD je v současné době považován za jeden z nejbezpečnějších. Pokud však jde o identifikaci tohoto systému, vykazuje několik charakteristických znaků, podle kterých není obtížné jej určit. Tyto znaky jsou:

- ✓ doba života paketu TTL je nastavena na 64,
- ✓ velikost okénka je 16384,
- ✓ nastavení volitelných polí v hlavičce TCP používá stejné jako Linux s tím rozdílem, že místo nastavení jedenkrát NOOP nastavuje pětkrát NOOP, tedy nastavení je MSS, SACK permitted, Timestamp, Window Scale a 5x NOOP,
- ✓ sekvenční čísla jsou nastavována zcela náhodně i v rámci jedné relace,
- ✓ celková délka SYN paketu je 64 bytů[57].

[55] Protokol TCP podmiňuje v této části pouze povinnost odvozovat sekvenční číslo z údaje vnitřních hodin procesoru. To však neznamená, že nemůže být údaj hodin použit jako vstupní hodnota pro generátor náhodných čísel. Linux kalkuluje ISN z hodinového údaje ke kterému je připočítávána hodnota vzniklá jednoduchou hashovací funkcí. Tato funkce se navíc v čase mění. Algoritmus generování ISN v Linuxu byl z bezpečnostních důvodů již několikrát změněn.

[56] Přesněji, platí to u většiny verzí Linuxu, ale např. Linux 2.0.3x má délku SYN paketu 44 bytů.

[57] Od OpenBSD 3.0.x.

konecna

11.7.4.4 Solaris 2.5 až 2.7

Operační systém Solaris firmy Sun je vykazuje následující nastavení:

- ✓ doba života paketu TTL je 255,
- ✓ velikost okénka je nastavena na 8760,
- ✓ volitelná pole v hlavičce TCP umožňují pouze nastavení MSS,
- ✓ sekvenční čísla se vždy zvyšují o 1,
- ✓ celková délka SYN paketu je 44 bytů.

Pro prvotní jednoduché určení, že se jedná o systém Solaris 2.5 až 2.7 stačí zkombinovat hodnotu TTL=255 s faktem, že celková délka SYN paketu je 44 bytů. Existují sice systémy, které mají TTL=255 nebo délku SYN paketu 44 bytů, ale žádný z nich nesplňuje obě tyto podmínky zároveň[58]. Další charakteristikou Solaris 2.5 až 2.7 je, že sekvenční číslo je vždy zvyšováno o jedničku.

11.7.4.5 AIX 4.3

Nastavení jednotlivých parametrů pro operační systém AIX 4.3 je následující:

- ✓ doba života paketu TTL je 64, stejně jako např. Linux a OpenBSD,
- ✓ velikost okénka je nastavena na 16384,
- ✓ volitelná pole v hlavičce TCP umožňují pouze MSS, stejně jako např. Solaris
- ✓ celková délka SYN paketu je 44 bytů,
- ✓ sekvenční čísla se vždy zvyšují o 1.

Identifikovat AIX je o něco pracnější než předcházející OS. Je třeba sledovat všechny položky, nikoli jen vybranou podskupinu jako např. u Solarisu nebo OpenBSD.

11.7.4.6 MS Windows 2000

Poslední operační systém, u kterého se budeme analyzovat hodnoty uvedené v hlavičkách protokolů TCP je MS Windows 2000. Identifikace tohoto OS není nijak náročná. Stačí k tomu většinou jen délka paketu ve spojení s TTL a nastaveními volitelných polí v hlavičce TCP. Jednotlivé parametry jsou:

- ✓ doba života paketu je TTL=128, toto nastavení používají téměř všechny systémy Windows,
- ✓ velikost okénka je 16384, stejně jako např. AIX,
- ✓ nastavení volitelných polí v hlavičce TCP umožňuje MSS, SACK permitted a 2x NOOP,
- ✓ celková délka paketu SYN je 48 bytů,
- ✓ sekvenční čísla se vždy zvyšují o jedničku.

[58] Podobně jako všechny ostatní údaje v této kapitole je i toto tvrzení nutno brát s rezervou. Např. stejnou kombinaci používají třeba zařízení Cisco Catalyst 3500 a naopak, Solaris 9 je nastaven na TTL=64 a délku paketu SYN 48 bytů.

11.7.5 Obecné shrnutí

V předcházejícím byly ukázány základní postupy pro rozpoznávání operačních systémů. Samozřejmě výčet není úplný, ale jedná se spíše o ukázku obecných postupů a principů, kterými se metody rozpoznávání operačních systémů ubírají. Jak udává tabulka tab. 11.6, která zahrnuje pouze údaje o velikosti okénka, přítomnosti MSS, době TTL, nastavení bitu „Don't fragment", velikosti SYN paketu a povolených volitelných polích, i výše uvedený omezený počet charakteristik operačního systému umožňuje jeho poměrně dosti přesnou identifikaci.

Operační systém	Okénko	TTL	DF	SYN paket	Volitelná pole
AIX 4.3.3	32768	64	0	60	M*,N,W0,N,N,T
Alteon ACEswitch	60352	128	1	64	M1460,N,W2,N,N,T,N,N,S
AOL web cache	5840	64	1	52	M1460,N,N,S,N,W0
BSD/OS 3.1-4.3	8192	64	1	60	M1460,N,W0,N,N,T
Cisco Catalyst 3500, 7500 apod.	4128	255	0	44	M*
Cisco Content Engine	5840	64	0	48	M1460,N,N,S
Dell PowerApp	27085	128	0	40	.
FreeBSD 2.0-4.1	16384	64	1	44	M*
FreeBSD 4.4	1024	64	1	60	M*,N,W0,N,N,T
FreeBSD 4.6-4.8	57344	64	1	60	M*,N,W0,N,N,T
FreeBSD 4.8-5.0	65535	64	1	60	M*,N,W0,N,N,T
FreeBSD 5.1	65535	48	1	60	M*,N,W1,N,N,T
HP/UX 11.0	32768	64	0	48	M1448,W0,N
HP/UX B.10.20	32768	64	1	44	M1460
Checkpoint	12xMSS	64	1	44	M1460
IRIX 6.2-6.5	61440	64	0	44	M*
IRIX 6.5 (RFC1323)	49152	64	0	52	M*,N,W2,N,N,S
IRIX 6.5.14m	61440	64	0	48	M*,N,N,S
IRIX 6.5.19	49152	64	0	48	M*,N,N,S
Linux 2.0.3x	512	64	0	44	M*
Linux 2.0.3x	16384	64	0	44	M*
Linux 2.4	4xMSS	64	1	60	M*,S,T,N,W0
Linux 2.4.18	3xMSS	64	1	60	M*,S,T,N,W0
Linux 2.5	4xMSS	64	1	60	M*,S,T,N,W1
MacOS 9.1/9.2	32768	255	1	48	M*,W0,N
NetApp CacheFlow	65535	64	0	60	M1460,N,W0,N,N,T
NetApp NetCache 5.2.1	8192	64	1	64	M1460,N,N,S,N, W0,N,N,T
NetApp NetCache 5.3.1	16384	64	1	64	M1460,N,N,S,N,W0,N

konecma

Operační systém	Okénko	TTL	DF	SYN paket	Volitelná pole
NetBSD 1.3 nebo OpenBSD 2.6	16384	64	0	60	M*,N,W0,N,N,T
NetBSD 1.3 nebo OpenBSD 2.6	16384	64	0	60	M*,N,W0,N,N,T
NetBSD 1.6	16384	64	0	60	M*,N,W0,N,N,T0
OpenBSD 3.0-3.4	16384	64	1	64	M*,N,N,S,N,W0,N,N,T
OpenVMS 7.2	6144	64	1	60	M*,N,W0,N,N,T
PalmOS 3 (na OS Win95)	5xMSS	255	0	44	M536
PalmOS Tungsten C (na OS Win95)	9xMSS	255	0	44	M536
RISC OS 3.70	16384	64	1	68	M1460,N,W0,N,N,T, N,N,?12
SCO Unixware 7.0.	S17	64	1	44	M1460
Solaris 2.5 to 7	S17	255	1	44	M*
Solaris 2.6	S6	255	1	44	M*
Solaris 8	S17	64	1	48	N,N,S,M*
Solaris 9	S34	64	1	48	M1460,N,N,S
Tru64 4.0f	32768	64	1	48	M*,N,W0
Tru64 v5.1a JP4	61440	64	0	48	M*,N,W0
Windows 2000 SP4	65535	128	1	48	M*,N,N,S
Windows 98	8192	128	1	48	M*,N,N,S
Windows 98SE	S44	64	1	48	N,N,S,M*
Windows XP	45xMSS	128	1	48	M*,N,N,S
Windows XP (za firewallem)	45xMSS	128	0	48	M*,N,N,S
Windows XP nebo 2000 SP3	44xMSS	128	1	48	M*,N,N,S

Tab. 11.6: *Charakteristické údaje některých operačních systémů*

Jednotlivé položky v tabulce, pokud nejsou zřejmé, mají následující význam:

- ✓ TTL – hodnota doby života paketu – Time to Live.
- ✓ DF – nastavení bitu „Don´t Fragment".
- ✓ SYN paket – délka paketu SYN.
- ✓ Volitelná pole mají následující význam:
  - ✓ Mxxx – velikost maximálního segmentu „xxx", * znamená proměnná velikost.
  - ✓ N – NOOP.
  - ✓ Wxxx – nastaven měřítka okénka na „xxx", * znamená proměnná velikost.
  - ✓ S – nastavení selektivního potvrzování „SACK permitted".
  - ✓ T – časová značka „Timestamp", T0 je „Timestamp" s nulovou hodnotou.

Další postupy jsou již většinou zaměřeny na upřesnění nebo potvrzení detekce dané verze operačního systému a často se jedná o metody specificky zaměřené na jednotlivou charakteristiku systému. Například upřesnění detekce operačního systému Redhat Linux 7.1 nebo 7.2 se vychází z toho, že uživatel při instalaci využije nabídky instalace firewallu a ponechá standardní volbu „medium security". Toto nastavení vede k typickému obrazu chráněných portů – jsou chráněny porty s číslem nižším než 1023 a několik standardních portů s vyššími čísly (2049 - NSF server, 6000 – Xwindows apod.). Ostatní porty z rozsahu 1024-65535 chráněny nejsou. Navíc, instalovaný firewall místo zahazování nepovolených paketů explicitně pakety odmítá zasíláním informace protokolu ICMP. Pro potvrzení identifikace operačního systému Redhat Linux 7.1 nebo 7.2 by stačilo se připojit na chráněný port a když dostaneme informaci o odmítnutí, existuje velká pravděpodobnost, že komunikujeme s firewallem operačního systému Redhat Linux 7.1 nebo 7.2.

Rozdělení metod na aktivní a pasivní by bylo možno parafrázovat též jako na zjistitelné a nezjistitelné. Pasivní metody se detekují velmi obtížně, nicméně při jejich realizaci je nutné dosáhnout přístupu do takové části sítě, kde pakety mohou být odposlechnuty. Na druhou stranu aktivní metody, které používají standardních postupů, významně se neodchylujících od běžného provozu sítě, mohou být použity ze kteréhokoliv místa v síti a pravděpodobnost jejich zjištění, pokud mezi jednotlivými pokusy bude dostatečně dlouhý časový interval, rovněž není příliš vysoká[59].

Srovnání jednotlivých metod, pokud jde o jejich účinnost a přesnost je obtížné. Pro každou síťovou konfiguraci bude existovat metoda vykazující lepší výsledky i metoda, která zcela zklame. Je proto vhodné používat kombinace jednotlivých metod a usuzovat na detekovaný operační systém teprve na základě porovná jejich výsledků. Jako jedna z nejlepších se dá označit aktivní metoda zjišťování časových intervalů odezvy SYN-ACK, neboť je těžko odhalitelná, stačí jí jen jeden přístupný TCP port a dosahuje velmi dobrých výsledků.

[59] Řada systémů IDS používá mechanismy pro zachycení typických sekvencí při pokusech identifikaci operačního systému.

12.

Vyšetřování kybernetického deliktu

Kybernalita, počítačová a informační kriminalita, se svým charakterem vymyká běžným vyšetřovacím postupům. Uveďme několik základních charakteristik, které jsou pro tento druh kriminality typické:

- ✓ Digitální stopy jsou objemné, značně dynamické a mohou být rozptýleny na velkém geografickém prostoru, jejich životnost může být velmi krátká.
- ✓ Ne vždy lze jako důkazní materiál zajistit napadený hardware, protože by to znamenalo další ztráty pro již tak poškozenou oběť.
- ✓ Škody, resp. ztráty, způsobené kybernalitou, se obtížně zjišťují nebo vyčíslují, což je obecným problémem, spojeným s kriminalitou související s duševním vlastnictvím.
- ✓ K analýze a dešifrování digitálních stop je nutný specializovaný software či hardware.
- ✓ Pravidlem jsou dlouhé prodlevy, související s justiční sférou (např. rozhodnutí o vystavení soudního příkazu). Kvalita a včasnost zajištění digitálních stop přitom zásadně rozhoduje o úspěšnosti dalšího šetření. Průtahy při zajišťování digitálních stop jsou primární příčinou nízké objasněnosti kriminality, související s informačními a komunikačními technologiemi.

- ✓ Zákony, postihující kriminální chování v uvedené oblasti, jsou stále ve vývoji a existují spíše ve fragmentech, vytvořených z hlediska zájmů jednotlivých států. Nedostatky v zákonné sféře byly popsány dříve.
- ✓ Je obecně nízká úroveň akceptace digitálních stop v právní praxi. Obtížně se např. prokazuje, co je originál a co kopie.

Otázka vyšetřování „počítačového deliktu" je sama o sobě věc velmi specifická. Na tenkém ledě se zde potýká specialista v oblasti bezpečnosti počítačových systémů s některými legálními zábranami, které jsou kladeny soukromé osobě při zjišťování informací vedoucí k odhalení útoku a vyčíslení případných vzniklých škod. Pokud jde o interní záležitost uvnitř firmy, existuje ještě jakýsi právní podklad pro zahájení takových „analýz", avšak jakmile vyšetřovací postup překročí její hranice, „vyšetřovatel" se ocitá na velmi tenkém ledě, neboť jemné nuance obsažené v telekomunikačním zákoně a v zákoně na ochranu osobních údajů by mohly nakonec být použity i proti osobě, která takové vyšetřování vede.

Bohužel, orgány policie v těchto případech nejsou dostatečně pružné, většinou nedisponují odborníky potřebných profesí a ani technologické vybavení není na odpovídající výši. V každém případě však je dobré ve vhodném okamžiku požádat orgány činné v trestním řízení o pomoc a nabídnout jim svoje „svědecké" a odborné služby. Žádný zákon totiž nezakazuje, aby vyšetřovatel vašich odborných služeb použil.

12.1 Vyšetřovací rámec

Základem každého vyšetřování technologického deliktu je vyšetřovací rámec, který je nutno stanovit při zahájení každé takové činnosti. Zdá se velmi pravděpodobné, že při počátku vyšetřování, kdy půjde pouze o podezření, nebudeme žádat o okamžitý zásah orgány činné v trestním řízení. Nicméně již od počátku je třeba nakládat se všemi materiály tak, jakoby se jednalo o trestný čin a s předpokladem, že námi připravené materiály mohou být podkladem pro přípravu obvinění a odsouzení pachatele.

Kvalita těchto materiálů musí tedy vyhovovat požadavkům kladeným na dokazování ve smyslu páté hlavy zákona o trestním řízení soudním a to i v případě, že výsledkem šetření nebude podklad pro trestní obvinění, ale třeba jen pro opatření ve smyslu zákona o přestupcích[1]. Zároveň je nutno mít na vědomí, že každý správce sítě, odborník na bezpečnost počítačů nebo i soudní znalec přizvaný potenciálním poškozeným vystupuje v těchto případech jako soukromá osoba, která nemá vůči ostatním aktérů žádná výjimečná práva.

12.1.1 Prevence

Možná, že není na místě mluvit o prevenci v případě, když už k „technologickému deliktu" došlo, ale právě prevence je to, co se velmi často zanedbává a co může ušetřit nejenom náklady na odstranění následků deliktu, ale i nákladů na vyšetřování, dokazování a soudní řízení.

Celou interakci mezi potenciálním nebo skutečný útočníkem a osobami odpovědnými za bezpečný provoz systému lze rozdělit do čtyř kroků:

- ✓ přijmutí takových opatření, která co nejvíce omezí možnost útoku na počítačový systém,
- ✓ testování přijatých opatření a použitých technologií,
- ✓ detekce průniku nebo počátečních přípravných aktivit směřujících k průniku do systému a maximální využití nástrojů, které jsou k tomu určeny; během detekce takové aktivity je možno ve smyslu prvního kroku přijmout okamžitá opatření vedoucí ke zvýšení bezpečnosti ohrožené části systému nebo eliminaci útočníka,
- ✓ vyšetřování průniku, shromažďování důkazů a odstraňování vzniklých škod, což je nejsmutnější kapitolou celého případ.

Primárním úkolem, který může maximálně eliminovat následky případného útoku, bude prevence, tedy přijetí opatření minimalizujících nebezpečí průniku do systému. Tato opatření mohou např. spočívat např. v implementaci softwaru, který účinně zabezpečí každý uzel informačního systému dobře zpracované bezpečnostní politice firmy, všeobecná znalost obecných nebo firemních bezpečnostních standardů a pravidelná kontrola jejich dodržování. Vedení firmy může např. nařídit preventivní kontroly ve všech bodech informačního systému, které jsou na rozhraní s vnějším prostředím[2] a jsou tudíž nezranitelnější. Lze nalézt šest základních oblastí snadné zranitelnosti:

- ✓ identifikace a autentizace uživatele, tedy funkce určená k sestavení relace s uživatelem, kde podstatnou složku tvoří ověření jeho identity; to platí i v případě, kde se neověřuje identita uživatele, ale oprávněnost a identita procesu vyžadujícího relaci,
- ✓ řízení přístupu, které určuje a řídí toky dat mezi procesy, objekty nebo uživateli; tato funkce implikuje používání kategorií přístupových práv, jejich ověřování a administraci,
- ✓ revize přístupů – funkce, která sleduje a zaznamenává pokusy, které mají vyzkoušet přístupová práva a ověřit relevantní bezpečnostní akce,
- ✓ opakovaný přístup k objektům, speciální funkce systému sledující, prostřednictvím řízení přístupu k datovým objektům, jak, kým nebo kdy jsou tyto objekty používány, zejména pokud se jedná o opakované použití téhož datového objektu,
- ✓ preciznost a přesnost, postup zaměřený na korektnost a konzistenci relevantních bezpečnostních informací,
- ✓ spolehlivost služby, která zajistí bezpečný přenos dat komunikačním prostředím.

Všechny tyto oblasti je třeba ověřit nebo zajistit zejména pro včasné zjištění útoku a celkovou znalost slabin systému. K tomu je možno použít celou řadu nástrojů pro testování systému[3] a na základě výsledků testování upravit konfiguraci systému nebo přijmout příslušná bezpečnostní opatření.

12.1.2 Detekce průniku

Preventivní nástroje umožňují testování slabin systému na základě známých metod útoku a tak ověřují ta místa, která jsou nejčastějším místem průniku. Jejich cílem je sladit konfiguraci systému s bezpečnostní politikou. Používají se tak, že testují systém s ohledem na stanovenou bezpečnostní politiku, např. simulátor internetových útoků může simulovat až několik stovek

[1] Zákon 200/1990 Sb. ve znění pozdějších novel.

[2] Pojem vnějšího prostředí je nutno chápat obecněji – rozhraní styku s vnějším prostředím může být i konzole nebo terminál, které používá pracovník firmy pro práci s informačním systémem.

[3] Existují dva základní typy nástrojů – preventivní a zjišťovací. Vhodný druh nástroje je nutno zvolit na základě zvolených cílů.

různých druhů útoků proti serverům, směrovačům nebo firewallům v síti TCP/IP[4]. Výrobci se snaží udržet krok s hackery a pravidelně tyto produkty doplňují o simulace nových typů útoků.

konecma

Jakmile se testováním zjistí, že konfigurace systému vyhovuje definované bezpečnostní politice, nastupuje druhá fáze – zjišťovací. Do systému jsou zavedeny programové nástroje, umožňující detekci probíhajícího pokusu o průnik do systému v reálném čase. Většinou se jedná o programy, které „sedí na pozadí" systému a monitorují činnost v kritických uzlech. Úkolem takového programu je nejenom útok zjistit, ale zároveň identifikovat o jaký útok se jedná a jaké prostředky jsou k tomuto útoku použity. Protože programové produkty, sloužící k simulaci útoku a k detekci průtoku, jsou obvykle součástí celého balíku, dodávaného od stejného výrobce, detekční část analyzuje útoky obdobné těm, které byly simulovány programy v preventivní části balíku.

Detekční programy obvykle nejenom způsobují okamžitý alarm, umožňující správci sítě zasáhnout proti útočníkovi. Zároveň okamžitě blokují případné přístupové cesty, které útočník používá pro své aktivity a generují potřebné záznamy pro pozdější analýzy. Tyto záznamy, u kterých je kladen důraz na ochranu před dodatečnými zásahy, jsou důležité ve dvou případech:

- ✓ Pro statistická zpracování bezpečnostními složkami provozu systému, které mohou na základě analýzy těchto dat navrhnout modifikaci uplatňované bezpečnostní politiky.
- ✓ Jako podklad pro další vyšetřování v případě, že všechny obrané mechanismy selžou a při průniku útočníka do systému dojde ke ztrátě nebo poškození dat, popř. úniku důležitých informací. V tomto okamžiku je nutno se záznamy zacházet jako s potenciálními podklady pro důkazní řízení před soudem, tzn. označit je příslušnými jednoznačnými identifikátory, stanovit režim práce s těmito podklady tak, aby bylo možno identifikovat kdo a kdy s nimi přišel do styku a zejména v případě datových médií, zamezit možnosti dodatečné změny těchto podkladů.

Dobře zpracovaná a zpětně trasovatelná dokumentace je základním předpokladem úspěšného vyšetřování. Při její přípravě je nutno si uvědomit, že kvalifikovaný útočník má snahu zanechat po sobě co nejméně stop a proto je důležitá ochrana generovaných záznamů proti vnější změně. Při kvalitní práci útočníka může útok zůstat neodhalen po dlouhou dobu a teprve analýza nepatrných změn v systému a trocha profesionální paranoii bezpečnostních složek může vést ke zjištění, že útok již dávno proběhl a po útočníkovi se slehla zem. Útočníci typu lammers a loosers obvykle nejsou nebezpeční, neboť používají veřejně dostupné programy, které jsou orientovány na známé bezpečnostní „díry" v systému, jež jsou buď již odstraněny, nebo jsou chráněny v posledním upgrade bezpečnostního software. Bohužel, u méně chráněných systémů může dojít k tomu, že chyba útočníka vede ke spuštění mechanizmů, které dodatečně natropí v systému velkou škodu.

12.2 Metodika vyšetřování

Existuje celá řada metodik, které jsou publikovány renomovanými vyšetřovateli počítačových deliktů. Ve své podstatě jsou vždy tvořeny popisem formálního procesu vyšetřování. Při formalizaci je však nutno si uvědomit, že vlastní proces vyšetřování takového činu není vždy stejný, liší se podle povahy činu a je ovlivněn i osobností vyšetřujícího. Syntéza odborníka soustředěného na špičkové technologie a profesionála, orientujícího se v metodikách

[4] Viz např. Internet Scanner firmy Internet Security Systems (http://www.iss.net).

vlastního vyšetřovacího procesu do jedné osobnosti se vyskytuje jenom zřídka, a proto se vyšetřování počítačového deliktu stává týmovou prací, při níž je nutno odpovědět na pět základních otázek: kdo, co, kde, kdy a proč[5]. Vlastní vyšetřování útoku na počítačový systém nebo průniku do něj se pak musí soustředit na sedm základních cílů, které jsou zde uvedeny v pořadí důležitosti:

1. Vysledovat způsob, jakým útočník pronikl do systému a porozumět jednotlivým krokům průniku. Tento krok můžeme obvykle rozdělit do tří částí:
   - ✓ výběr možných způsobů průniku[6], který slouží k vytvoření hrubé představy a vymezuje pole, na kterém se budeme pohybovat,
   - ✓ vytvoření hypotézy, jak k průniku došlo,
   - ✓ rekonstrukce průniku za dodržení veškeré opatrnosti a při eliminaci případných destruktivních kroků.
2. Vyhodnotit získané informace a rozhodnout o okamžiku, kdy budou přizvány orgány činné v trestním řízení.
3. Získat nezbytné informace umožňující nastavit „past" na útočníka, zejména nalézt místo, odkud útočník do systému proniká (tel. linka, jiná síť, apod.), kde musíme zejména:
   - ✓ zpětně trasovat cestu, po níž útočník do systému pronikl do vyšetřovaného systému, až do úrovně počítače ze kterého mohl být útok proveden,
   - ✓ analyzovat veškeré systémy, které jsou na této cestě.
4. Nalézt motiv, proč útočník si zvolil za svůj cíl právě tento systém.
5. Soustředit co největší množství důkazů o průniku;
6. Shromáždit další informace umožňující zúžit seznam podezřelých subjektů (např. údaje prokazující, že útočníkem nemůže být žádný ze současných zaměstnanců). V procesu shromažďování důkazů může dojít i k nutnosti zabavit počítač předpokládaného útočníka, neboť v něm mohou být uloženy některé důkazy potvrzující identitu útočníka. Tato činnost by však již měla být doprovázena odpovídajícími kroky orgánů činných v trestním řízení.
7. Určit výši škody, která byla útočníkem způsobena, včetně nákladů na vyšetřování incidentu a nákladů na uvedení systému do původního stavu. Veškeré výpočty musí vycházet z existujících právních předpisů[7] a mohou zahrnovat i škodu, která může být nebo byla způsobena únikem důvěrných, např. obchodních, informací.

Z hlediska vyšetřování jsou nejdůležitější kroky dva a tři, zejména rozhodnutí, zda „past" nastražená na útočníka bude připravena ve spolupráci s orgány činnými v trestním řízení nebo zda majitel napadeného objektu a privátní vyšetřovatel tento krok uskuteční sami. Pokud se rozhodnete pokračovat bez přizvání orgánů činných v trestním řízení, je nutno si uvědomit všechna navazující rizika a o to precizněji připravovat, evidovat a vysvětlovat důkazní materiály. Je nutno se připravit i na to, že může dojít k vašemu obvinění, nebo

[5] Těchto pět otázek silně připomíná základní metodu investigativní žurnalistiky.

[6] Ti, kteří četli detektivky proslulého sira Arthura Conana Doylea ví, že je to jedna ze zásad Sherloka Holmese: „Eliminujeme-li nemožné, pak to co zbývá, i když je to nepravděpodobné, musí být pravda."

[7] Např. zákon 151/1997 Sb. o oceňování majetku, nebo zákon 563/1991 Sb. o účetnictví, vše v posledním platném znění. Stanovení výše škody může být samo o sobě velmi složitá záležitost, proto je vhodné se obrátit na znalce v odpovídajícím oboru a přibrat ho jako člena vyšetřujícího týmu.

obvinění osob, které vám poskytly cenné informace, z porušení některých zákonných předpisů tak, jak bylo uvedeno výše (porušení telekomunikačního zákona, zákona na ochranu osobnosti apod.).

konecma

12.2.1 Trasování k iniciátorovi průniku

Zpětné trasování k útočníkovi je obvykle jednou z nejobtížnějších částí vyšetřování zejména v případě, kdy předcházející analýzy vedly ke zjištění, že podezřelý subjekt pochází z vnějšího prostředí. To bude znamenat, že trasování bude probíhat v prostředí internetu a uvědomíme-li si, že zkušený útočník nebude používat svůj vlastní počítač k provedení průniku, ale vytvoří cestu prostřednictvím mezilehlých systémů, které nebudou vykazovat žádnou incidenci s prostředím, ze kterého útočník pochází. Např. v univerzitní síti může být takovým mezilehlým počítačem server jiné části univerzity (útočník z přírodovědné části univerzity může použít např. server humanitní části) nebo počítač organizace, která je propojená do univerzitního systému[8]. Většinou se jedná o počítače, které jsou velmi špatně administrovány a umožňují snadné, nepozorované proniknutí do systému a založení tajného uživatelského konta, které bude následovně použito pro další aktivity útočníka.

Dobře propracovaný útok obvykle používá několik takových „zadních vrátek", které jsou krátkodobě provázány a tak činí dostupnost zdroje útoku daleko obtížnější. Klasický pocit geografické blízkosti rovněž v takovém případě neplatí, ani hledání vztahu mezi použitým mezilehlým počítačem a útočníkem nevede k cíli. Po provedení útoku má útočník snahu o smazání všech záznamů o své činnosti na všech mezilehlých počítačích. Pokud útočí zevnitř napadeného systému, pak u zkušeného útočníka můžeme očekávat, že tam, kde je to možné systém opustí a opět do něj vstoupí nějakou vnější cestou.

Základem zpětného trasování jsou záznamy o provozu systému – logy, avšak můžeme se setkat s problémy, ke kterým patří:

- ✓ nejsou k dispozici logy, které by pokryly časový úsek útoku,
- ✓ logy v době útoku existují, ale jsou pro analýzu nepoužitelné (obsažené informace nejsou adekvátní, log má některé podezřelé rysy),
- ✓ logy jsou změněny, zejména v časovém úseku, kdy proběhl útok,
- ✓ mezilehlý systém „zdánlivě" vypadl během doby útoku,
- ✓ administrátoři mezilehlého systému odmítají spolupracovat,
- ✓ IP adresa uvedená v logu je falešná, předstíraná, a ve skutečnosti nás zavede zcela jinam,
- ✓ log na zasaženém počítači je změněn a nepoužitelný,
- ✓ připojení proběhlo prostřednictvím komutované linky a došlo pouze k jednomu spojení, které není možno trasovat.

Zpětné trasování je tedy plně závislé na uchovaných záznamech, které mohou být změněny. Přitom ke změně logu může dojít ve dvou zcela odlišných případech:

- ✓ Log je změněn útočníkem, a pak se s takto změněným logem musí vypořádat počítačový odborník, který případ vyšetřuje.
- ✓ Log byl změněn tím, kdo případ vyšetřuje, nebo třetí zájmovou stranou. V tomto případě je to záležitost orgánů činných v trestním řízení.

Právě z hlediska druhé možnosti je nutno vždy pořídit alespoň dvě kopie logu z počítače (nebo jakýchkoli stavových záznamů), vždy označené časovým údajem a dalšími podrobnostmi včetně jmen svědků, kteří byli přítomni vaší činnosti. Jedna kopie zůstává nedotčená jako důkazní materiál pro orgány činné v trestním řízení, ostatní jsou použity jako pracovní.

12.2.2 Analýza cesty

Toto je poslední část vyšetřování, kde hraje svoji významnou roli počítačový odborník. V předcházející fázi shromáždil dostatek materiálů o cestě útoků a nyní by měl analyzovat jednotlivé prvky na této cestě. Je nutné, aby si uvědomil rozdíl, který panuje mezi objektivně existujícím důkazním materiálem a vlastním soudním důkazem[9]. Nepodléhejte nikdy dojmu, že máte tolik důkazního materiálu, že „to musí být každému jasné". Mezi vlastním důkazním materiálem a důkazem ve smyslu soudního řízení je ještě dlouhá cesta. Bude dobré si uvědomit tři zásady:

1. Věřit nálezu, pokud patří do kategorie možného. Pokud nenaleznete důkazy, které by váš nález popíraly, věřte tomu, co jste zjistili svými testy, a to i v případě, že incident ukazuje jenom jeden z použitých testů a nejste schopni prokázat chybu v testu. Až budete dávat zjištěné nálezy dohromady, hledejte inkonsistence v nalezeném. Pokud je nenajdete, věřte tomu co jste nalezli.
2. Objasnit rozpory; pokud dva nálezy jsou v přímém rozporu, vraťte se o krok zpět a snažte se tento rozpor odůvodnit nebo porozumět tomu, proč k tomuto rozporu dochází. Můžete nakonec dojít k závěru, že mezi nálezy žádný rozpor není, že je jenom potřeba blíže pochopit funkci použité technologie. Nesnažte se rozumově vysvětlit konflikt jenom proto, abyste se dále pohybovali cestou, kam vás toto vysvětlení láká - může to být léčka. Hledejte podstatu rozporu a pokud budete mít podezření, že jste zjištěné informace jsou zavádějící, opusťte současný postup a začněte jinde.
3. Za žádných okolností neměňte nic v systému, který analyzujete, zvláště pak, když tento systém nebo počítač by mohl být zdrojem útoku. V tom případě zhotovte fyzickou kopii systému a pracujte na této kopii. Nezapomeňte, že můžete být vyzváni k předvedení původního stavu během práce orgánů činných v trestním řízení a druhá strana udělá všechno pro to, aby vaše závěry zpochybnila.

Úkol analyzovat systém nebo počítač, který byl součástí nějakého deliktu, je důkazním procesem, kdy musíme dbát maximální opatrnosti, abychom důkaz nezničili. Vyplatí se dbát několika následujících zásad:

- ✓ Spouštět systém nebo počítač takovým způsobem, aby nedošlo v žádném případě k přístupu do oblastí, v nichž může být uložena citlivá informace. Pokud se bude jednat o personální počítač, je nejvhodnější jej spustit pomocí diskety nebo CD se systémem, který je nastaven tak, že při startu nemění nic na diskových jednotkách. V žádném případě nepoužívejte lokálně instalovaný běžný operační systém – při spouštění dochází k tolika přístupům do systémových oblastí, že výsledný obraz disku může být zcela zničen. Dobrá zásada je používat co nejhloupější operační systém, který je spolehlivý a každý provedený krok lze manuálně ovládnou a prokázat. Na

[8] Tento mezilehlý počítač nemusí být nutně server, může to být prakticky kterákoliv programovatelná součást sítě.

[9] Objektivně existujícím důkazním materiálem je třeba záznam o provozu systému – log. K tomu, aby se stal důkazem pro orgány činné v trestním řízení musí být např. dále prokázáno, že nebyl změněn.

zaváděcí disketu nebo CD můžete uložit ovladače vnějších zařízení, které vám umožní přenést kopie citlivých oblastí na externí médium – přenosný pevný disk nebo třeba vypalovačku CD. V některých případech je možno celý disk fyzicky vyjmout a připojit jej k jinému počítači na kterém se vytvoří jeho fyzická kopie. V tom případě je vhodné upravit připojovací kabel tak, aby byl signál „I/O Write", který umožňuje zápis, potlačen[10].

- ✓ Vytvořit fyzickou kopii pevného disku a přenést ji na testovací počítač. Při vytváření kopie prozkoumat i „inženýrské" oblasti pevného disku a volný prostor, zda tam nejsou ukryta nějaká data, která by bylo možno používat při fyzickém přístupu i mimo služby původního operačního systému.
- ✓ Podrobně analyzovat všechny logy, porovnávat data změny u souborů. S daty změny je nutno zacházet opatrně, je to položka, která se změní nejsnadněji.
- ✓ Analyzovat konfigurační soubory a všechny soubory spouštěné při startu počítače, tzv. „start-up" soubory zejména s ohledem na zjištění případných anomálií.
- ✓ Pokud se jedná o počítač, který připadal v úvahu jako výchozí k provedení útoku, prohlédnout adresáře a hledat možné nástroje pro „hacking". Ty mohu být skryty, nemusí mít známá jména apod. Vhodný je v tomto případě použít některý z nástrojů, který fyzicky přistoupí k alokačním tabulkám a zobrazí je v čitelném formátu. Ukrýt soubor před běžným „explorerem" je snadné a na nástroje tohoto typu lze jen těžko spoléhat.
- ✓ Porovnat kritické soubory se stejnými soubory pocházejícími z ověřeného zdroje. To je důležité zejména proto, neboť existuje celá řada verzí kritických systémových souborů obsahujících „trojského koně", ale se správným kontrolním součtem, délkou i datem poslední změny. To se týká i souboru se systémovými hesly, který by měl být prozkoumán z hlediska možné změny neautorizovaným subjektem.
- ✓ Prozkoumat pevný disk na přítomnost některých specifických klíčových slov, které by se mohly vztahovat k deliktu a to včetně inženýrských a skrytých oblastí disku, uvolněného prostoru a souborů vyrovnávací paměti. V případě, kdy objevíme šifrované soubory, zjistit alespoň základní údaje o použité metodě nebo softwaru, jeho dodavatele a výrobce. Tyto údaje pak mohou posloužit orgánům činným v trestním řízení ke specifikaci dalších kroků vyšetřování.
- ✓ Prověřit komunikační parametry (např. soubor s vytáčenými telefonními čísly, druh připojení apod.) a konfigurace komunikačního software. Může se stát, že podstatné informace budou uloženy někde v prostředí internetu, které bude dostupné síťovými prostředky.
- ✓ Najít podstatné změny v systému souborů, prokazatelně vymazané kritické soubory[11] a existenci neznámých souborů.

Během výše popsaného procesu, kdy analyzujeme obraz počítače, zároveň vytváříme podklady pro sběr důkazních materiálů a vypracování vlastních důkazů. Tento proces zviditelnění obsahu počítače může být doplněn i řadou dalších opatření, která shledáme důležitými – např. pořízení fotografií některých částí, označení součástí systému tak, aby bylo možno kdykoliv zrekonstruovat původní stav (kabelů, periferií) apod. Je-li systém zajištěn v zapnutém stavu, pak je vhodné pořídit fotografii obrazovky a v případě, že je připojena mozaiková nebo podobná mechanická tiskárna, vyjmout tiskací pásku a nahradit ji novou.

Problém s vypnutím podezřelého počítače je sám o sobě nejednoznačný. Proces vypínání může být totiž nastaven tak, aby při běžném postupu vypínání zničil všechny stopy související s vyšetřovaným deliktem. Zároveň, některé systémové soubory mohou zcela zaniknout, např. soubor používaný pro virtuální paměť, kde bude uchován poslední obraz operační paměti počítače, nebo být změněny. Na druhou stranu, vypnutí počítače přerušením přívodu proudu může vést ke ztrátě některých souborů. Nejste-li si jisti, zda v počítači nejsou připraveny postupy, které mohou odstranit důležité informace, je vždy lepší počítač odepínat přerušením dodávky elektrického proudu.

Poslední krok, který již byl několikrát vzpomenut je zajištění a označení důkazu. To bude jednoduché v případě materiálního podkladu, avšak v případě souboru na magnetickém médiu bude obtížné prokazovat, i přes organizační zajištění nezbytně spjatá s ukládáním důkazních materiálů, že právě ten soubor, který předkládáte, nemohl být od okamžiku kdy byl zajištěn někým změněn. Vhodný způsob je zajištění souboru elektronickým způsobem, tedy pomocí programu, který vytvoří hash souboru a na jeho základě jakýsi elektronický podpis. Tento soubor elektronického podpisu pak může být zašifrován např. pomocí PGP[12] vlastním veřejným klíčem. Soubor elektronického podpisu může být kdykoliv dešifrován soukromým klíčem a porovnán s hashem souboru, který slouží jako důkazní materiál. Jakákoliv změna na původním souboru by se měla tímto způsobem projevit.

12.2.3 Informační zdroje na internetu

Dostatek znalostí a informací „up-to-date" je důležitým fenoménem vyšetřování počítačového incidentu. Rozvoj komunikačních a informačních technologií je velmi rychlý a mnohdy publikace v této oblasti, pokud se nezajímají o principy ale o konkrétní případy, velmi rychle zastarávají. Členové vyšetřovacího týmu by tedy měli sledovat poslední vývoj v oblasti bezpečnosti, a tak bude vhodné, když shrneme nejznámější informační zdroje, nacházející se na internetu, které mohou posloužit při rychlé orientaci v současných trendech. K nejzajímavějším stránkám patří:

- ✓ Konference SANS[13], které jsou přístupné přes portál www.sans.org. Jedná se o portál velmi technicky zaměřený s neustále aktuální tématikou a seznamem všech incidentů na celém světě.
- ✓ Portály a weby nejrůznějších institucí zabývajících se počítačovou kriminalitou a bezpečností počítačových sítí.; tyto stránky se soustřeďují na různá specializovaná témata od ryze technických až po metodiky sestavení bezpečnostní politiky firmy nebo analýze rizik. Často jsou i komerčně zaměřeny na produkty nejrůznějšího druhu a kvality. Můžeme sem zařadit např. wwww.gocsi.com organizace Computer Security Institute nebo stránky http://searchsecurity.stage.techtarget.com/home/ sítě TechTarget.
- ✓ Stránky MIS Training Institute, zaměřené zejména na bezpečnostní audit systémů, jež jsou k dispozici na *www.misti.com.*
- ✓ Konference HTCIA[14] na adrese *www.htcia.org* a další.

---

[10] Existují profesionální přípravky, které zamezí zápisu na disk daleko snadněji a jsou použitelné i pro disky se sériovým interface, např. SATA.

[11] Zde je důležité odlišit „organické" vymazání, kde vymazání kritického souboru je důsledkem očekávané relevantní akce systému, od vymazání jako důsledek akce útočníka. Nezapomeňme, že data vymazaného souboru zůstávají na disku, pokud nebyla fyzicky přepsána, a je z nich možno získat celou řadu informací.

[12] PGP – Pretty Good Privacy, je veřejný šifrovací program, který je volně dostupný na internetu i z komerčních zdrojů.

[13] System Administration, Networking and Security Institute, někdy též vykládáno jako SysAdmin, Audit, Network, Security. Organizace založená v roce 1989 ve pojených státech.

[14] High Technology Crime Investigation Association

Zkušeného analytika asi není třeba upozorňovat, že s nalezenými materiály na internetu je nutno zacházet opatrně, neboť na jejich správnost a úplnost není vždy spolehnutí, a to ani tehdy, když se jedná o stránky renomovaných institucí[15].

konecma

12.3 Role orgánů činných v trestním řízení

Neodpustme si úvodní poznámku – ve chvíli, kdy seznámíte orgány činné v trestním řízení s výsledky vašeho dosavadního pátrání, musíte jim přenechat veškeré další řízení vyšetřování. Vaše osoba se stává pouze a jenom svědkem. Rozhodnutí o předání celého případu je manažerským rozhodnutím, které může vycházet z různých, pro technika mnohdy nepochopitelných pohnutek, např.:

- ✓ Jedná-li se o banku nebo organizaci se státním či politickým pozadím, pak často manažeři nechtějí celý případ předat policii, protože předpokládají jeho publicitu, která by díky přirozené náklonnosti tisku ke tvoření senzací mohla mít nepříznivé důsledky na další fungování organizace.
- ✓ Nepovažují to za nutné vzhledem k rozsahu případu; jeho předání na lokální úrovni by možná policie uvítala, ale bohužel prostředky, které jsou v této sféře k dispozici pro řešení technologických deliktů nejsou odpovídající a tak by vyšetřování stejně nikam nevedlo. Důležitým faktorem přitom je zpracovaná bezpečnostní politika firmy, která musí obsahovat rovněž analýzu rizik, a tak předběžně stanovit případy, kdy oznámení deliktu orgánům činným v trestním řízení bude nezbytné.
- ✓ Mnohdy je kriminální delikt důsledkem snahy neloajálních administrátorů o řešení své pozice, svých finančních problémů nebo prostě jejich pomstou firmě, která se k nim podle jejich názoru nezachovala dobře. Vzhledem k obsahu speciálních znalostí, kterými každý systémový administrátor disponuje, je taková „msta" velmi jednoduchá. Manažer pak nechce inzerovat selhání personální politiky firmy.

Při předání celého vyšetřování orgánům činným v trestní řízení se musíme smířit s tím, že pravděpodobně bude narušena komunikace ve firmě, rozšíří se atmosféra podezřívavosti i tam, kde panovala kolegiální atmosféra a může to vést k narušení organizace práce celé firmy.

Při takovém rozhodování je nutno i zvážit, jaké pravomoci může firma použít, aniž by překročila zákon a jaké prostředky na vyšetření případu má k dispozici. Ne každá firma má potřebné odborníky, kteří by správné postupy při vyšetřování zvládli. Orgány činné v trestním řízení mají celou řadu specifických pravomocí, kterými soukromý subjekt nedisponuje. Pokud se však rozhodnete předat celou věc orgánům činným v trestním řízení, je dobré tento krok neodkládat.

12.4 Role privátních vyšetřovatelů, znalců a konzultantů

Většina organizací nemá své vlastní odborníky na vyšetřování počítačových deliktů. I když disponuje technicky zdatným týmem, který může proces vyšetřování nastartovat, v některém z kroků se ocitnou manažeři firmy před rozhodnutím – předat případ policii již nyní nebo ještě přizvat odborníka, konzultanta nebo soudního znalce, který má nejen potřebné znalosti, ale i oprávnění vydávat odborné expertízy. Tento výběr není jednoduchý a nespočívá jenom v nahlédnutí do seznamu znalců a pokynem sekretářce, aby vybraného jedince zavolala. Bohužel, i mezi znalci se pohybují jedinci bez potřebných znalostí, kteří se vezou na vlnách obav o bezpečnost firemních sítí. Dobré je, pokud firma si obraz o vhodných konzultantech učiní již při formulaci své bezpečnostní politiky a průběžně s nimi spolupracuje, i když třeba při řešení triviálnějších problémů. Každopádně je nutné, aby role konzultanta byla přesně specifikována ještě předtím, než je zvolen a přizván.

Získání referencí o případném kandidátu je velmi obtížné. Ne každá firma, která využila jeho služeb při řešení kriminálního nebo podobného problému bude ochotna vystavit mu vysvědčení. Role konzultanta, která mu bude přidělena ve vyšetřovacím týmu se může pohybovat od pouze technického experta v dané oblasti, právního poradce až po odborníka, který zvládá celé spektrum znalostí potřebných k vyšetřování počítačového deliktu. Během vyšetřování bude nutno sestavit speciální tým, který se bude sestávat z odborníků v různých oblastech – od technických expertů přes psychology nebo sociology až po finanční odborníky. Sestavení takového týmu jakož i jednotlivé role jsou předmětem následující kapitoly.

12.5 Vyšetřovací tým

Základem každého vyšetřování deliktu technologického charakteru je podobně jako v jiných oblastech sestavení vyšetřovacího týmu, který rozpracovává navržené hypotézy. Sestavení takových týmů není rutinní záležitostí manažerů, orientovaných do zcela jiného sektoru zájmu. Nicméně dříve nebo později se každá organizace se s nutností vyšetřit nějaký počítačový průnik setká, a proto bude v následujícím uveden základní postup při výběru členů vyšetřovacího týmu a organizaci jeho práce.

V oblasti počítačové kriminality se pro tuto práci ujal zaběhlý policejní termín pro americké speciální jednotky – SWAT[16]. Rovněž se můžeme setkat s názvy CIRT – Computer Incident Response Team nebo CERT – Computer Emergency Response Team. Česká terminologie si moc na podobné názvy nepotrpí a tak se často setkáme s americkým označením, které je ještě pro ozdobu často doplněno slovem Cyber.

12.5.1 Struktura vyšetřovacího týmu

Základním úkolem vyšetřovacího týmu je zjištění příčin incidentu vzniklého s použitím počítačových technologií. Za tím účelem sestavuje vyšetřovací hypotézy a plány, řídí sběr důkazních materiálů, vyslýchá svědky[17], provádí zpětné trasování průniku do počítačového systému, zjišťuje rozsah škod, které při sledovaném incidentu vznikly a vykonává další činnosti, které s vyšetřením počítačového incidentu souvisí. Vyšetřovací týmy mohou být ve větších organizacích tvořeny z pracovníků bezpečnostních složek se speciálním zaměřením a školením v této oblasti, kdy sledování potenciálních bezpečnostních rizik a jejich následné vyšetřování je náplní jejich práce. V menších organizacích jsou takové týmy sestavovány ad hoc z odborníků potřebných profesí. V obou případech je běžné, že

[15] Je to celkem pochopitelné, někdy je to sice neúmyslné, ale jindy jsou materiály neúplné zejména z důvodu ochrany vlastního know-how příslušné instituce.

[16] Anglická zkratka „Special Weapon and Tactics".

[17] Zvláště tento bod je velmi delikátní, neboť z právního hlediska se nejedná o svědeckou výpověď, ale o rozhovor dvou rovnoprávných fyzických osob a neexistuje žádné zákonné oprávnění pro takovouto činnost. Je tedy nutno zachovat maximálně transparentní právní rámec.

do týmu je zahrnut externista - konzultant, který přinejmenším reprezentuje vnější nezainteresovaný pohled na problém. Obvykle je takový tým tvořen jakousi „řídící skupinou", která vede vyšetřování a dalšími odborníky, kterým jsou na základě rozhodnutí této řídící skupiny přidělovány jednotlivé speciální úkoly.

Kdo by měl být členem vyšetřovacího týmu. Obvykle záleží na velikosti firmy, která vyšetřovací tým vytvoří, avšak v řídící skupině by měly být vždy zastoupeny tyto složky:

- ✓ pracovník zodpovědný za bezpečnost informačních systémů,
- ✓ zástupce útvaru interního auditu firmy,
- ✓ reprezentant podnikového útvaru bezpečnosti, pokud takový útvar ve firmě existuje,
- ✓ podnikový právník nebo konzultant specializující se na tuto právní problematiku.

Do širšího výběru mohou být dále zahrnuti:

- ✓ pracovníci útvaru lidských zdrojů, nebo personálního oddělení,
- ✓ mluvčí firmy nebo pracovníci public relations, zvláště pak pokud má firma útvar vnější komunikace, měla by být současně s průběhem vyšetřování připravována strategie, která určí způsoby a formu případné reakce firmy na dotazy médií[18],
- ✓ specialisté z útvaru informatiky, např. experti vyškolení firmami pro instalované technologie,
- ✓ zástupci finančních útvarů firmy,
- ✓ expert na vyšetřování počítačových incidentů, většinou externí konzultant,
- ✓ ostatní experti, tak jak vyžaduje povaha vyšetřovaného činu.

Všichni členové týmu by měli být experty ve svém oboru a měly by jim být poskytnuty dokonalé nástroje umožňující identifikaci počítačového incidentu[19]. Poskytnutí přístupu na internet a zvláštních oprávnění ke vstupu na jednotlivá pracoviště jsou samozřejmostí.

12.5.2 Ustavení vyšetřovacího týmu

Základním dokladem pro ustavení vyšetřovacího týmu by měla být schválená bezpečnostní politiky firmy. Tým obvykle sestavuje pověřený pracovník bezpečnostního útvaru s cílem vyšetřit podezření na průnik do počítačových systémů firmy nebo neoprávněné užití datových souborů vlastněných firmou.

Cílem vyšetřovacího týmu je zjistit všechny dostupné informace a potvrdit nebo vyvrátit výše uvedené podezření, a to v nejkratší časové lhůtě. Časové hledisko je v případě technologických incidentů jedním z nejdůležitějších s ohledem na rychlost probíhajících procesů, a tak včasná diagnostika spojená s preventivními kroky při zahájení vyšetřování může zabránit vzniku následných škod v napadených informačních systémech. Zároveň s tím musí vyšetřovací tým připravit modifikace bezpečnostní politiky firmy a odpovídající úpravy v informačních systémech tak, aby před následujícím útokem, který by použil stejných prostředků, byl systém chráněn.

Protože základním úkolem vyšetřovacího týmu je rychle odkrýt případný útok a přijmout potřebná opatření, měl by být podřízen odpovídajícímu pracovníku v hierarchii řízení firmy, který má dostatečné pravomoci pro realizaci rychlých rozhodnutí. Nezřídka tímto pracovníkem bývá příslušný ředitel[20]. Ten rozhoduje nejenom o přijatých opatřeních, ale také o přizvání externích organizací nebo předání celého případu orgánům činným v trestním řízení. Činnost vyšetřovacího týmu má být zahájena neprodleně a musí pokrýt následující oblasti:

- ✓ identifikaci všech kritických oblastí systému ohroženého útokem,
- ✓ reakci na všechny další incidenty nebo podezřelé stavy systému,
- ✓ plynulá návaznost vyšetřovacích kroků probíhajících bez přerušení až do ukončení práce[21],
- ✓ shromáždění všech dostupných podkladů a klasifikace incidentu, který má být vyšetřován,
- ✓ vlastní vyšetřování a předávání pravidelných zpráv vedení firmy, jejich frekvence je obvykle určena na první schůzce vyšetřovacího týmu s pracovníkem vedení firmy, do jehož pravomoci vyšetřovací tým spadá,
- ✓ stanovení výše napáchaných škod a rozsahu útoku,
- ✓ zajištění všech potřebných důkazních materiálů odpovídajícím způsobem; osoby, které nespadají do vyšetřovacího týmu a mohly by přijít do styku s uchovávanými důkazními materiály musí být prokazatelně poučeny o charakteru těchto materiálů a nakládání s nimi.

Činnost vyšetřovacího týmu se neobejde bez:

- ✓ doporučení pro začlenění dalších odborníků mateřské firmy nebo konzultantů a jejich výběr,
- ✓ návrhu doporuční pro úpravy bezpečnostní politiky firmy, případně urychlená implementace těchto doporučení,
- ✓ kontaktu s orgány činnými v trestním řízení.

To všechno musí být předpokládáno při sestavování vyšetřovacího týmu.

12.5.3 Zodpovědnosti členů týmu

Jak bylo výše uvedeno, vyšetřovací tým tvoří základní řídící skupina, která vyhodnocuje dosažené výsledky a určuje další kroky vyšetřovacího týmu. Jednotliví členové řídící skupiny plní následující úkoly:

- ✓ Pracovník zodpovědný za bezpečnost informačních systémů:
  - ✓ Zprostředkuje informaci o incidentu uživatelům, kteří mohou být tímto incidentem dotčeni,

[18] Na tento krok se často zapomíná a výsledkem je pak trapné popírání evidentních skutečností nebo schovávání se za frázi „bez komentáře". Takový přístup zcela jistě nepřispěje k dobrému jménu firmy.

[19] Např. použité antivirové programy musí obsahovat poslední verzi „update", která zahrnuje i poslední známé viry.

[20] V americké firemní struktuře existuje často funkce označovaná CIO – Chief Information Officer, který má ve svém popisu funkce právě řízení takovýchto aktivit. Pokud neexistuje, jeho funkce přechází na CEO – Chief Executive Officer, nejvyššího rozhodujícího pracovníka firmy.

[21] Zahájení plné práce vyšetřovacího týmu by nemělo trvat déle než dvě hodiny od rozhodnutí o vyšetřování podezření z útoku na počítačový systém nebo od oznámení takového útoku.

- ✓ řídí veškeré odborné složky zabývající se zpětným trasováním útoku, technicko-právní analýzou a všechny aktivity, které bezprostředně souvisí s technologickým zázemím firmy,
- ✓ spolupracuje na celkové analýze útoku,
- ✓ spolupracuje na přípravě konečné zprávy pro vedení firmy,
- ✓ zajišťuje spolupráci kvalifikovaných soudních znalců,
- ✓ musí být k dispozici jako svědek pro orgány činné v trestním řízení.

✓ Zástupce útvaru interního auditu firmy:

- ✓ sleduje práci vyšetřovacího týmu z hlediska použití nejvhodnějších metod a přijímání nejefektivnějších opatření,
- ✓ zajišťuje, aby výsledky šetření byly prokazatelné a opakovaně revidovatelné,
- ✓ prověřuje správnost postupů při zajišťování důkazů a jejich korektní provádění,
- ✓ má zodpovědnost za všechny důkazní materiály, zajištěné během procesu vyšetřování; tuto zodpovědnost však může sdílet s ostatními členy týmu podle jejich odbornosti, nicméně obecná právní odpovědnost v této oblasti leží plně na pracovníkovi vnitřního auditu firmy,
- ✓ zajišťuje, aby byl použity správné postupy při dokumentování veškerých kroků, které byly podniknuty při vyšetřování,

✓ Reprezentant podnikového útvaru bezpečnosti, pokud takový útvar ve firmě existuje:

- ✓ je kontaktní osobou s orgány činnými v trestním řízení,
- ✓ zajišťuje aby při vyšetřování byly použity nejefektivnější a právně korektní metody,
- ✓ zajišťuje, aby informace o incidentu nebyly šířeny mimo uzavřenou skupinu a nedostávaly se do nepovolaných rukou,
- ✓ řídí rozhovory[22] se svědky a podezřelými,

✓ Podnikový právník nebo konzultant specializující se na tuto právní problematiku:

- ✓ sleduje veškeré rozhodování a úkony vyšetřovacího týmu z hlediska jejich legálnosti a zajišťuje, aby při vyšetřování incidentu nebyl porušen zákon,
- ✓ zajišťuje, aby nebyla porušena práva podezřelých osob,
- ✓ obvykle slouží jako mluvčí skupiny směrem k médiím, pokud tuto funkci nepřevezme oficiální mluvčí firmy; v takovém případě s ním probírá detaily jeho vystoupení,
- ✓ provádí revizi každé tiskové zprávy o incidentu, která má být uvolněna pro média,
- ✓ provádí revizi zpráv pro vedení firmy,
- ✓ je kontaktní osobou s právními zástupci dalších stran, dotčených vyšetřováním.

[22] Úmyslně používám termín „rozhovor", neboť termín „výslech" je používán pro právní úkon náležející pouze orgánům činným v trestním řízení.

Mezi povinnosti dalších členů vyšetřovacího týmu, kteří jsou účastni vyšetřovacích kroku, patří:

✓ Pracovníci útvaru lidských zdrojů, nebo personálního oddělení:

- ✓ informování členů vyšetřovacího týmu o personální politice a souvisejících procedurách,
- ✓ doporučení pro zpracování citlivých informací z oblasti personální politiky,
- ✓ doporučení, týkajících se zvláštních pracovních smluv nebo souvislostí s kolektivní smlouvou, očekávanými stanovisky odborových svazů apod.

✓ Mluvčí firmy nebo pracovníci public relations:

- ✓ je jediným spojením s vnějšími médii, úzce spolupracuje s právníky ve vyšetřovacím týmu,
- ✓ spolupracuje s pracovníky vyšetřovacího týmu a obsah předávaných informací musí být upraven tak, aby nenarušil postup vyšetřování,

✓ Specialisté z útvaru informatiky:

- ✓ provádějí revize logů a zpracovávají poznatky o zjištěných anomáliích, podezřelém obsahu nebo aktivitách,
- ✓ předávají zprávy o jakémkoli neobvyklém chování kritických částí systému,
- ✓ zajišťují důkazní materiály podle podnikové bezpečnostní směrnice nebo podle pokynů členů řídící skupiny vyšetřovacího týmu,
- ✓ poskytují podklady pro odhad způsobených škod a rozsahu útoku,
- ✓ po identifikují místo vstupu do systému a předkládají návrhy na případné modifikace nebo úpravu vstupní procedury,

✓ Zástupci finančních útvarů firmy:

- ✓ poskytují vyšetřujícímu týmu informace o finančních aspektech útoku, případně o souvisejících finančních procedurách,
- ✓ provádí finanční audit, je-li ho zapotřebí,
- ✓ spolupracují při vyšetřování podle potřeb a rozhodnutí řídící skupiny,

✓ Expert na vyšetřování počítačových incidentů, kterým je obvykle externí konzultant:

- ✓ pomáhá řídící skupině v orientaci ve speciálních postupech spojených s vyšetřováním incidentu, zejména:
- ✓ optimálních metodách identifikace a klasifikace útoku,
- ✓ souvisejících právních aspektech útoku,
- ✓ způsobech zacházení s důkaznými materiály a metodách jejich předání orgánům činným v trestním řízení,
- ✓ postupech, souvisejícím s vyhledáním a jednoznačnou identifikací útočníka.

Členy vyšetřovacího týmu mohou být ještě další osoby a specialisté, jejichž úloha je určena specifickými potřebami řídící skupiny vyšetřovacího týmu a povahou útoku.

12.5.4 Klasifikace incidentu

konecma

Bezpečnostním incidentem, tak jak byl tento termín používán výše, obvykle rozumíme jakoukoliv událost, která způsobila, že došlo k narušení činnosti počítačového systému, sítě nebo jejích součástí, či byl umožněn neautorizovaný přístup k datům, která následovně byla zmanipulována, vymazána, učiněna nepřístupnými nebo naopak zpřístupněna neoprávněným subjektům. Každý incident se obvykle zatřídí podle nějakých typických znaků do třídy. Toto zatřídění pak již determinuje opatření a další kroky spojené se zjištěním incidentu.

Incidenty obvykla dělíme podle jejich rozsahu do tří tříd[23], kde do nejnižší třídy patří lokální omezené incidenty a do nejvyšší třídy incidenty se škodou velkého rozsahu.

12.5.4.1 Lokální incident – třída 1

Jedná se lokální incident, který nevyžaduje vytvoření vyšetřovacího týmu a jeho vyšetření včetně přijetí odpovídajících opatření je plně v pravomocích příslušného manažera útvaru nebo produktu. Mezi tyto incidenty patří:

- ✓ lokální útoky počítačovým virem,
- ✓ obtěžování na internetu nebo jeho zneužívání,
- ✓ incidenty, které vznikly chybou uživatele nebo systému,
- ✓ jednoduché útoky na známá místa, skenování portů nebo opakované použití funkce ping.

12.5.4.2 Přímé ohrožení systému – třída 2

Tyto incidenty, jejichž vyšetření je již složitější a vyžaduje sestavení vyšetřovacího týmu, obvykle přímo ohrožují majitele výpočetního systému nebo sítě, a to jak přímo napadená zařízení tak i nepřímo finanční nebo jiné atributy firmy. Mezi tyto typy incidentů můžeme zařadit:

- ✓ útoky proti firewallu,
- ✓ koordinované útoky z více míst, někdy se používá termín distribuované útoky,
- ✓ útoky počítačovým virem, kdy zasažení systému je nezvykle vysoké,
- ✓ počítačové podvody[24], při kterých je vlastní systém buď zneužit pro útok nebo je přímo cílem útoku,
- ✓ útoky proti serveru nebo uživatelské aplikaci na serveru,
- ✓ krádež důvěrných informací uložených v systému,
- ✓ útoky proti kritické části systému, která např. pracuje s důvěrnými informacemi nebo je životně důležitou částí systému.

[23] Třída incidentu, jeho znaky, klasifikace a odpovídající reakce na incident jsou podstatnou součástí bezpečnostní politiky firmy.

[24] Původně označované termínem „computer fraud", ze kterého se i v češtině se ujal často používaný termín „fraud".

12.5.4.3 Speciální incidenty – třída 3

Jedná se o takové incidenty, jejichž vyšetřování vyžaduje aktivity mimo standardní bezpečnostní politiku firmy. V těchto případech se může jednat i o incident původně zařazený do první třídy, který byl z nějakých důvodů byl eskalován odpovědným pracovníkem na vyšší řídící místa firmy. Důvodem je např. o podezření z přípravy incidentu většího rozsahu nebo jenom o nejistotu v odhadu rozsahu incidentu.

Vyšetřování incidentu třídy 3 se nejprve zaměřuje na určení povahy útoku a na analýzu rizika. Po ukončení této fáze může být incident klasifikován některou z výše uvedených tříd a zpracován standardním postupem. Složitější situace nastává, pokud se jedná o incident, který je nový nebo o jeho průběhu není dostatek důkazních materiálů. V těchto případech je obvykle nutno provést hlubší analýzu, nastavit ve spolupráci s útvarem informatiky řadu „pastí" a čekat, zdali se prokáže, že „podivné" chování systému je způsobeno jenom technickou nedokonalostí nebo je skutečně projevem vnějšího či vnitřního útoku.

13.

Slovník pojmů

Adware	Advertising support software – programové prostředky, jejichž cílem je předání reklamního sdělení i proti vůli uživatele systému.
Bezpečnostní komunita	Množina institucí v České republice, zahrnující zejména Policii České republiky a všechny zpravodajské služby České republiky. Obdobně se tento termín chápe i v jiných státech.
Botnet, zombie	Síť infikovaných počítačů, ovládaných bez vědomí majitele, které často slouží k rozesílání nevyžádané pošty, ke krádežím identity či k provádění dalších forem kybernetických útoků.
Crimeware	Programové prostředky, používané k aktivitám, zařaditelným do kybernality. Použití tohoto prostředku je zpravidla spojeno s finanční (zištnou) kriminalitou v rámci kyberprostoru.
Informační a komunikační technologie	Veškerá technika, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení.

Informační bezpečnost	Multidisciplinární obor, usilující o komplexní pohled na problematiku ochrany informací během jejich vzniku, zpracování, ukládání, přenosu a likvidace. Obvykle zahrnuje postupy, zabývající se snižováním rizik vztahujících se k informacím a navrhující příslušná organizační, řídící, metodická, technická a právní opatření.
Informační kriminalita (info-crime)	Trestná činnost, pro kterou je určující vztah k software, k datům, resp. uloženým informacím, resp. veškeré aktivity, které vedou k neautorizovanému čtení, nakládání, vymazání, zneužití, změně nebo jiné interpretaci dat, s cílem získat určitou neoprávněnou výhodu. Kriminalita, související s pokročilými technologiemi (high-tech crime)
Informační společnost	Společnost založená na intenzívním využívání informačních a komunikačních technologií. Tato společnost pokládá vytváření, šíření a manipulaci s informacemi za určující část svých ekonomických, kulturních a společenských aktivit.
Informační systém	Funkční celek nebo jeho část, zabezpečující systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Zahrnuje datové a informační zdroje, nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky.
Infoware	Druh programového nástroje, používaného k aktivitám, zařaditelným do kybernality. Infoware může též specifikovat programové aplikace pro informatickou podporu klasických bojových akcí, resp. soubor aktivit sloužících k ochraně, vytěžení, poškození, potlačení nebo zničení informací nebo informačních zdrojů, s cílem dosáhnout významné výhody v boji nebo vítězství nad konkrétním protivníkem.
Kritická informační infrastruktura státu	Komplex informačních a komunikačních systémů a služeb, sloužících k informačnímu zajištění řádné funkce kritické infrastruktury. Obsahuje zejména telekomunikační sítě (internet či jiné přenosové sítě), počítačové systémy a jejich programové vybavení včetně poskytovaných služeb.
Kybernalita	V kontextu této knihy sjednocující pojem, zahrnující veškeré zločinné, neetické, nežádoucí či jinak pro bezpečnost státu a společnosti rizikové jednání, související s fungováním informačních a komunikačních technologií. Vedle tzv. počítačové, resp. informační kriminality, kam řadíme jednání, pokrytá konkrétními skutkovými podstatami trestního zákona, jejichž potírání je věcnou náplní činnosti policejních složek, kybernalita zahrnuje i takové jevy, jako je politicky motivovaná nebo hospodářská špionáž, extrémní politická či přímo teroristická propaganda a tzv. kybernetický terorismus.
Kyberterorismus	Obecně je chápán jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.
Logické bomby (logical bombs)	Programy, které se tajně vkládají do aplikací nebo operačního systému, kde za předem určených podmínek provádějí destruktivní aktivity. Předem specifikovanou podmínkou startující logickou bombu může být například konkrétní datum (výročí určité události – viz. např. „Virus 17. listopad“).
Malware (škodlivý software)	Jakýkoli software, jenž při svém spuštění zahájí činnost ke škodě systému, ve kterém se nachází. Jeho vnější projevy mohou být časovány, nebo reagovat na konkrétní naprogramovanou spouštěcí událost (např. na okamžik, kdy oprávněný uživatel otevře e-mailovou zprávu).
Man in the middle	Softwarový agent, který vystupuje jako prostředník mezi komunikujícími stranami, přičemž z hlediska uživatelů se taková komunikace jeví jako bezchybná. Přitom ale takový postup umožňuje neoprávněné osobě komunikaci nejenom sledovat (odposlouchávat), ale také do ní aktivně vstupovat, měnit obsah předávaných dat, získávat hesla, resp. falešně vystupovat jako jedna z komunikujících stran.
Maškaráda (masquerade)	Případy, kdy se jedna osoba (systém) vydává za jinou, čímž „přesvědčí“ příslušný ochranný systém o tom, že je odpovídající autorizovaná entita, a tak může využívat všech jejích práv a privilegií.
Mocking-bird	Software umožňující monitorovat komunikaci mezi uživatelem a serverem, případně mezi uživatelem a dalším počítačem.
Netware	Programové prostředky, používané k aktivitám, podřaditelným do rámce kybernality.bývá nejčastěji spojován s jiným, než ziskem motivovaným neoprávněným pronikáním do kybernetických systémů (zejm. s tzv. „altruistickým hackingem“).
Počítačová kriminalita (cyber-crime, kyberzločin)	Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité), nebo jako nástroj trestné činnosti.[1] Často se pojem počítačová kriminalita používá i pro tradiční formy kriminality, u níž byly počítače nebo počítačové sítě použity, aby ji usnadnily. Určujícím operacionálním elementem je přitom vždy způsob zneužití výpočetní techniky, vzhledem k jejím specifickým vlastnostem a dominantnímu postavení mezi věcnými komponentami způsobu páchání konkrétního trestného činu.

Počítačové právo	Mezioborová disciplína, zahrnující jak vlastní informatiku, zejména v oblasti budování a využívání informačních, počítačových a komunikačních systémů, tak vybrané právní disciplíny, a to jak soukromoprávního (občanské a obchodní právo, autorské právo atd.), tak veřejnoprávního charakteru (trestní právo, ochrana osobních dat, finanční právo, některé procesní normy, atd.).
Přesměrovávače (re-dial, „pharming crimeware“)	Programy, jejichž úkolem je přesměrovat uživatele na určité stránky namísto těch, které původně hodlal navštívit. Na takových stránkách dochází k instalaci dalšího crimeware (virů), nebo touto cestou dojde ke značnému zvýšení poplatků za připojení k Internetu (prostřednictvím telefonních linek se zvýšeným tarifem).
Replay	Situace, kdy je zachycená kopie legitimní transakce (datová sekvence), opětovně přehrána neautorizovaným subjektem, a to zpravidla s nelegálním úmyslem (např. pro otevření vozidla s centrálním zamykáním).
Sniffing (čmuchání)	Využití programů, které fungují jako zachytávače paketů přenášených po síti. Mohou zachytávat veškerou síťovou komunikaci, která je (pokud není šifrovaná) snadno čitelná a všestranně zneužitelná (včetně zjištění vstupních hesel do konkrétního systému).
Spyware (špionážní software)	Programy, skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval. Takové programy jsou často na cílový počítač nainstalovány spolu s jiným programem (utilita, počítačová hra), s jehož funkcí však nesouvisí.
Trojské koně, keyloggery	Programy, implantované do systému bez vědomí oprávněného uživatele, monitorující specifické činnosti, o které projevuje útočník zájem. Zaznamenávají např. znaky které oprávněný uživatel stiskl na klávesnici (zejm. hesla) nebo stránky, které navštívil. Tyto údaje předávají útočníku k dalšímu zpracování. Ten tak může získat přístupové informace k webovým stránkám, peněžním nebo e-mailovým účtům. Může se jednat i o textový editor, který zároveň ukládá text, který byl jeho prostřednictvím napsán, do skryté části systému, odkud může být vyzdvižen autorem trojského koně. Trojské koně často instaluje nevědomky sám oprávněný uživatel, když instaluje z internetu nebo zdarma distribuovaných CD jiné programy, se kterými jsou však tyto trojské koně spojeny (např. hry či servisní programy – utility).

[1] Definici počítačové kriminality, akceptovaná v rámci Evropské unie zní: Počítačová kriminalita je nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím informačních a komunikačních technologií nebo jejich změnu.

Zadní vrátka (back door)	Specifická forma potlačení bezpečnostní ochrany systému. Může být vytvořena samotným autorem distribuované aplikace, nebo dodatečně, prostřednictvím infoware, aby v případě potřeby posloužila pro vstup do systému bez nutnosti znát příslušná bezpečnostní hesla či kódy, instalovaná oprávněným uživatelem (tj. od specifického vzdáleného uživatele nevyžaduje běžné kontroly hesel). Jejich deklarovaným cílem, např. v souvislosti s operačním systémem Windows, je umožnění servisního přístupu odborníků firmy Microsoft do systému při aktualizaci některých aplikací. Zároveň se však jedná o ideální místo k průniku neoprávněné osoby.

14.

Význam některých zkratek

BND	Bundesachrichtendienst; německá výzvědná služba, její aktivity pokrývají i odposlechovou službu – signálovou špionáž (Sigint).
CCITT	Consultative Committee for International Telephony and Telegraphy; Agentura OSN pro vývoj standardů a protokolů pro telekomunikace; je součástí ITU a občas je označována jako ITU-T.
CEPT	Conference Europeene des Postes et des Telecommunications.
Comint	Communications Intelligence, odposlechová služba, signálová špionáž.
COMSAT	Civil/Commercial communications satellite; satelitní síť pro komerční využití. Pro vojenské komunikační spoje je tato zkratka často používána v přesmyčce – SATCOM.
CRIM	Centre de Recherche Informatique de Montreal, kanadské výzkumné centrum pro informatiku.
CSDF	Collected Signals Data Format; termín používaný v Sigint a označující formát dat pro přenos odposlechnutých signálů.

CSE	Communications Security Establishment, kanadská odposlechová služba.
CSS	Central Security Service; vojenská složka NSA.
DARPA	Defense Advanced Research Projects Agency, agentura amerického ministerstva obrany. Podle ní byla pojmenována první počítačová síť, která později přerostla v internet.
DGSE	Directorate General de Securite Exteriere, francouzská zpravodajská služba orientovaná na zahraničí; k jejím úkolům patří i odposlech – signálová špionáž.
DSD	Defence Signals Directorate, australská odposlechová služba – signálová špionáž.
E1, E3 (etc)	Standardy pro digitální přenos definované CEPT používané mimo severní Ameriku, zejména v Evropě.
ENFOPOL	Označení pro dokumenty EU náležící policejním nebojiným složkám dozírajícím na dodržování zákona.
FAPSI	Federalnoje Agenstvo Pravitelstvennoj Svjazi i Informacii, ruská federální agentura jejímž hlavním úkolem jsou odposlechy a signálová špionáž.
FBI	Federal Bureau of Investigation; americká federální agentura zabývající se dodržováním zákona na území Spojených států a kontrašpionáží.
FISA	Foreign Intelligence Surveillance Act, americký zákon z roku 1978 stanovující procedury a postupy pro fyzický a elektronický dohled a sběr informací o „cizích silách".
FISINT	Foreign Instrumentation Signals Intelligence, název třetí divize Sigint.
GCHQ	Government Communications Headquarters; anglická agentura zabývající se signálovou špionáží.
Gisting	Termín používaný v Sigint, práce analytika, při které doplňuje souvislý text heslovitými označeními hlavních témat komunikace.
IC 2000	Číslo technické přílohy ke standardu telekomunikačního odposlechu.
ILETS	International Law Enforcement Telecommunications Seminář, první standardizační skupina pro definování norem pro použití legálního odposlechu.
Intelsat	International Telecommunications Satellite, satelitní síť.
Iridium	Satelitní systém zahrnující 66 družic na nízké dráze, které umožňují globální komunikaci mezi mobilními telefony.
ITU	International Telecommunications Union, Mezinárodní standardizační organizace.
IUR	International User Requirements (for communications interception); standardy pro odposlech, první standard IUR 1.0 byl navržen ILETS v roce 1994.
IXP	Internet Exchange Point, internetový uzel.
LEA	Law Enforcement Agency, americký termín zahrnující všechny typy organizací pověřených dozorem nad dodržováním zákona.
N-gramová analýza	Metoda pro analýzu textových dokumentů jejímž cílem je výběr dokumentů obsahujících požadované téma.
NSA	National Security Agency, bezpečnostní agentura USA do jejíž působnosti spadá odposlechový systém Echelon.
PTT	Posts Telegraph and Telephone, angloamerické označení pro instituce zabývající se telekomunikacemi.
SCI	Sensitive Compartmented Intelligence; bezpečnostní postup používaný pro omezení přístupu k informacím získaným zejména odposlechem.
Sigint	Signals Intelligence, obecné označení pro signálovou špionáž, činnost při níž jsou odposlouchávány nejrůznější komunikační kanály i mimo území příslušného státu.
SMO	Support for Military Operations, metody a a ktivity směřující k podpoře vojenských operací.
SONET	Synchronous Optical Network, standard pro optické digitální přenosy
SRI	Signal Related Information; termín používaný v signálové špionáži pro označení další informace vztahující se k zachycené informaci.
STOA	Science and Technology Assessments Office of the European Parliament; orgán Evropského parlamentu, který zpracoval první studii zabývající se odposlechovým systémem Echelon.
T1, T3 (etc)	Standardy pro digitální přenos původně definované firmou Bell Telephone System pro severní Ameriku, kde jsou dosud používány.
Traffic analysis	Termín používaný v signálové špionáži; zahrnuje metody analýzy sloužící k získání informace ze zachycených zpráv bez analýzy jejich obsahu, např. studium četnosti dvojic adrese odesílatel/příjemce umožňuje zjistit vzájemné vztahy ve sledované skupině osob.
UKUSA	Aliance UK-USA, která byla základem pro vznik odposlechového systému Echelon.
VSAT	Very Small Aperture Terminal; druh satelitní komunikace s malou přenosovou kapacitou pro obsluhu komunikačních systémů domácností a malých firem.
WRF	Workfactor Reduction Field, pole v přenosovém protokolu obsahující údaje zjednodušující dešifrování zprávy při jejím zachycení odposlechovým systémem. Tato informace je doplňována do amerických softwarových systémů exportovaných mimo USA na zákaladě dohody velkých softwarových firem a NSA.

Rejstřík

P

R

S

Š

T

U

V

W

Y

Z

Čísla

Symboly