Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Psychologie a bezpečnostní systém organizace

Autor: Pavel Klíma

Vedoucí práce: Ing. Čestmír Halbich, Csc

Česká zemědělská univerzita v Praze | Fakulta provozně ekonomická

Katedra informačních technologií | Akademický rok 2007/2008

ZADÁNÍ DIPLOMOVÉ PRÁCE

Pavel Klíma

obor Veřejná správa a regionální rozvoj - k.s. Litoměřice

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název tématu: **Psychologie a bezpečnostní politika organizace**

Struktura diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Obecné požadavky na bezpečnost IS
4. Lidský faktor - podceňovaný činitel bezpečnosti IS
5. Typy průniků do IS
6. Technické zabezepečení IS
7. Managment a bezpečnostní politika organizace
8. Motivace uživatelů a správců IS
9. Závěr
10. Seznam literatury
11. Přílohy

Rozsah původní zprávy: 50 - 60 stran

Seznam odborné literatury:

MITNICK, K. a SIMON, W. Umění klamu 1. vydání. Praha: Helion S. A., 2003. 348s. ISBN 83-7361-210-6
JÍROVSKÝ, V. Kybernetická kriminalita. 1.vydání. Praha: Grada, 2007. 288s. ISBN 80-247-1561-2
MCCLURE, S., SCAMBRAY, J., Kurtz, G. Hacking bez záhad. 5. vydání. Praha: Grada 2007, 520s. ISBN:80-247-1502-3
WENSTROM, M. Zabezpečení sítí Cisco. 1. vydání. Brno: Computer Press, 2003, 784s. ISBN 80-7226-952-6
Hackin9: IT scurity Magazine. Varšava: Software-Wydawnictwo, 2005 -. ISSN 1214/7710
Sbírka zákonů: Zákon č.412/2005 Sb, 101/2000 Sb, Vyhláška NBÚ č. 523/2005 Sb.

Vedoucí diplomové práce: **Ing. Čestmír Halbich, CSc.**

Termín odevzdání diplomové práce: duben 2009

L.S.

.....	ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE	.....
Vedoucí katedry		Děkan

V Praze dne: 9.1.2008

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Psychologie a bezpečnostní systém organizace" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 8.dubna 2009 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Čestmíru Halbichovi, CSc. za jeho čas, trpělivost, odborné vedení a dobré rady při zpracování této práce.

Psychologie a bezpečnostní systém organizace

Psychology and security policy of organisation

Souhrn

Diplomová práce Psychologie a bezpečnostní systém organizace se zaměřuje na identifikaci a definici aktivit ohrožující bezpečnost informačních systémů. Popisuje typy útoků a možnosti obrany proti nim. Zvláštní pozornost je věnována metodám sociálního inženýrství a lidskému faktoru bezpečnosti informačních systému.

Klíčová slova: bezpečnost, bezpečnostní politika, hacking, informační systém, kriminalita, sociální inženýrství, průnik

Summary

The main focus of the diploma thesis Psychology and security policy of organizations is on the identification and definition of activities, which threaten security of the information systems. This work describes variants of attacks and some possibilities protection against them. Special attention is paying to methods of social engineering and human factor in security of the information systems.

Keywords: criminality, hacking, information systems, intrusion, security, security policy, social engineering

Obsah

1 ÚVOD ..... - 10 -

2 CÍL PRÁCE A METODIKA ..... - 11 -

2.1 CÍL PRÁCE ..... - 11 -

2.2 METODIKA ..... - 11 -

3 OBECNÉ POŽADAVKY NA BEZPEČNOST ..... - 12 -

3.1 FYZICKÁ BEZPEČNOST ..... - 12 -

3.1.1 Fyzický přístup ..... - 13 -

3.1.2 Technické podmínky pro provoz IS ..... - 15 -

3.1.3 Vlivy vyšší moci ..... - 15 -

3.2 PERSONÁLNÍ BEZPEČNOST ..... - 16 -

4 LIDSKÝ FAKTOR – PODCEŇOVANÝ ČINITEL BEZPEČNOSTI IS ..... - 18 -

4.1 ČINITELÉ ..... - 19 -

4.1.1 Nespokojení zaměstnanci ..... - 19 -

4.1.1.1 Nejčastější motivy závadového jednání ..... - 19 -

4.1.1.2 Pracovní zařazení v hierarchii organizace a toho vyplývající potenciální ohrožení ..... - 20 -

4.1.2 Hackerská komunita ..... - 21 -

4.1.2.1 Historie ..... - 21 -

4.1.2.2 Kategorie hackerů ..... - 22 -

4.1.2.3 Hackerské nástroje ..... - 23 -

4.1.3 Zločinci a kyberterotisté ..... - 33 -

4.1.3.1 Definice kriminality související s IT ..... - 33 -

4.1.3.2 Klasifikace kriminality v oblasti IT ..... - 34 -

4.1.3.3 Kyberterorismus ..... - 35 -

5 TYPY PRŮNIKŮ DO INFORMAČNÍCH SYSTÉMŮ ..... - 38 -

5.1 TAXONOMIE HROZBY ..... - 38 -

5.2 TECHNOLOGICKÉ PRŮNIKY ..... - 39 -

5.2.1 Kategorizace ..... - 39 -

5.2.1.1 Charakter útoku ..... - 40 -

5.2.1.2 Účel útoku ..... - 40 -

5.2.1.3 Spouštěcí mechanismus ..... - 40 -

5.2.1.4 Zpětná vazba ..... - 40 -

5.2.1.5 Pozice útočníka k cílovému systému ..... - 41 -
5.2.1.6 Pozice útočníka k cílovému objektu ..... - 41 -
5.2.1.7 Vrstva ISO/OSI ..... - 41 -
5.3 PRŮNIKY ZALOŽENÉ NA SOCIOTECHNICKÝCH METODÁCH ..... - 42 -
5.3.1 Příprava útoku ..... - 43 -
5.3.1.1 Získávání informací ..... - 43 -
5.3.1.2 Budování důvěry ..... - 44 -
5.3.2 Metody sociotechnického přesvědčování ..... - 44 -
5.3.3 Formy útoku ..... - 45 -
5.3.3.1 Telefonní útoky ..... - 45 -
5.3.3.2 Útoky z prostředí internetu ..... - 45 -
5.3.4 Obrana proti sociotechnickým útokům ..... - 46 -
5.3.4.1 Klasifikace dat ..... - 46 -
5.3.4.2 Reakce na žádost o informace ..... - 51 -
5.3.4.3 Žádost o provedení činnosti ..... - 52 -
6 TECHNICKÉ ZABEZPEČENÍ INFORMAČNÍCH SYSTÉMŮ ..... - 53 -
6.1 PŘÍSTUPOVÁ PRÁVA A UŽIVATELSKÉ ÚČTY ..... - 53 -
6.1.1 Gestor dat ..... - 53 -
6.1.2 Správce informačního systému ..... - 53 -
6.1.3 Bezpečnostní správce ..... - 54 -
6.1.4 Privilegovaný účet ..... - 54 -
6.2 ZABEZPEČENÍ SERVERŮ ..... - 54 -
6.3 ZABEZPEČENÍ STANIC ..... - 55 -
6.4 ZABEZPEČENÍ EXTERNÍCH DATOVÝCH KOMUNIKACÍ ..... - 55 -
6.5 ZABEZPEČENÍ ELEKTRONICKÉ POŠTY ..... - 56 -
7 MANAGEMENT A BEZPEČNOSTNÍ POLITIKA ORGANIZACE ..... - 57 -
7.1 BEZPEČNOSTNÍ POLITIKA ORGANIZACE ..... - 57 -
7.2 ÚLOHA MANAGEMENTU VE FORMULOVÁNÍ A PROSAZOVÁNÍ BEZPEČNOSTNÍ POLITIKY ORGANIZACE ..... - 57 -
7.3 BUDOVÁNÍ BEZPEČNOSTNÍ KULTURY ORGANIZACE ..... - 58 -
8 MOTIVACE UŽIVATELŮ A SPRÁVCŮ IS ..... - 60 -
8.1 MOTIVACE UŽIVATELE ..... - 60 -
8.2 MOTIVACE SPRÁVCE IS ..... - 61 -
8.3 MOTIVACE BEZPEČNOSTNÍHO SPRÁVCE ..... - 61 -

9 ZÁVĚR ..... - 62 -

10 SEZNAM LITERATURY ..... - 63 -

11 PŘÍLOHY ..... - 66 -

11.1 POKYN BEZPEČNOSTNÍHO ŘEDITELE K OCHRANĚ PROTI SOCIOTECHNICKÝM ÚTOKŮM ..... - 66 -

11.2 SMĚRNICE BEZPEČNOSTNÍHO ŘEDITELE O KLASIFIKACI INFORMACÍ ..... - 70 -

11.3 14 ČASTÝCH BEZPEČNOSTNÍCH CHYB ..... - 75 -

11.4 SEZNAM NEJČASTĚJI POUŽÍVANÝCH PORTŮ ..... - 76 -

11.5 VÝPIS INFORMACÍ Z WWW.RIP.NET ..... - 79 -

11.6 PŘÍKLAD ÚNIKU DAT ..... - 80 -

11.7 PRAKTICKÝ PŘÍKLAD PHISHINGU ..... - 81 -

11.8 SCHÉMA SÍTĚ VPN ..... - 83 -

1 ÚVOD

29. října 1969 byly přeneseny první datové pakety mezi počítači na univerzitách v Los Angeles a Stanfordu. V té době nikdo netušil, že vznikající síť se po čtyřiceti letech rozroste na miliony počítačů a jejich uživatelů propojených celoplanetárními sítěmi Internetu a zasáhne doslova do všech oblastí lidského života. Standardy a protokoly vzniklé v té době používáme jen s malými změnami dodnes. Rychlost rozvoje informačních technologií se vymykala všem dosavadním zvyklostem a lidská společnost nestačila včas tomuto rozvoji přizpůsobit své etické a právní normy.

Prudký rozmach Internetu, který tvůrci jeho standardů nepředpokládali, vyjevil časem bezpečnostní slabiny používaných technologií. Tyto technologie se pochopitelně staly terčem nezákonných aktivit majících za cíl naplnění tužeb starých, jak lidstvo samo – získávat cizí tajemství, obohacovat se na úkor druhého, ale i útočit na samé základy naší společnosti.

Primárním útočníkem i konečným poškozeným nejsou počítače, ale především lidé. Lidem a jejich chování, které zásadně ovlivňuje bezpečnost a funkčnost informačních a komunikačních technologií je věnována tato práce.

2 CÍL PRÁCE A METODIKA

2.1 CÍL PRÁCE

Primárním cílem práce je identifikovat a definovat hrozby ohrožující citlivá data i samotný provoz informačních systémů s důrazem na podceňovaný lidský faktor, popsat a analyzovat druhy průniků do těchto systémů, navrhnout možnosti obrany proti popsaným útokům a odpovědět na otázku, zda s rostoucí úrovní technické ochrany vliv lidské bytosti na bezpečnost informačních systémů klesá.

Sekundárním cílem je formulovat interní právní normu v podobě „Nařízení bezpečnostního ředitele organizace pro ochranu před útoky sociotechnického typu“, kategorizovat data organizace dle citlivosti a stanovit základní pravidla pro manipulaci s nimi.

2.2 METODIKA

Metodika této práce spočívá v popisu a analýze. Pro práci byla použita výzkumná metoda studium dokumentů. Pod pojmem dokument si lze představit psané a tištěné materiály (noviny, knihy, dopisy, zápisky, deníky atd.), ale mohou to být i fotografie, filmy, obrazy, sochy a jiné materiální výtvory člověka. (1)

Blokové diagramy byly vytvořeny programem Microsoft Viso 2003, grafické prvky byly zpracovány programem Adobe Photoshop CS3, pro tabulky byl použit program Microsoft Excel 2007. Skenování sítě bylo provedeno nástrojem Nmap ve verzi 4.85 beta s grafickým rozhraním Zenmap/Umit.

Pro účel práce jsem shromáždil dostupnou odbornou literaturu. Čerpal jsem z vlastních zdrojů, fondů Městské knihovny v Praze a z ověřených pramenů v Internetu. Získané informace jsem doplnil znalostmi a zkušenostmi získanými dlouholetou praxí v oboru. Kompletní souhrn pramenů je sumarizován v seznamu použité literatury v závěru práce.

3 OBECNÉ POŽADAVKY NA BEZPEČNOST

Organizace by měla své informační systémy chránit obdobně jako jiné své investice. Hardwarové části systému i s daty mohou být zničeny či ukradeny nejen teroristy, ale i intrikujícími či nepříčetnými zaměstnanci. Ukrást lze i programové vybavení, jehož hodnota může násobně přečíslit cenu hardwarových komponent. Ovšem nejcennější hodnotou pro organizaci, kterou je nutné chránit, jsou data představující vysoce ceněná aktiva. Tato data je často nutné zabezpečit i z důvodů daných zákonem. Příkladem může být Zákon č. 101/2000 Sb., o ochraně osobních údajů, Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti nebo Zákon č. 21/1992 Sb., o bankách.

Cílem zabezpečení informačního systému by mělo být obecně splnění těchto základních zásad:

- k datům v informačním systému mají přístup pouze oprávněné osoby
- data musí být přístupná tehdy, když jsou potřebná
- musí být prokazatelně zjistitelné, kdo a kdy tato data četl, vložil, upravil nebo odstranil
- musí být zajištěna důvěrnost těchto dat
- musí být ochráněna integrita dat před náhodnou i úmyslnou manipulací či zničením

3.1 FYZICKÁ BEZPEČNOST

Pojem fyzická bezpečnost zahrnuje především tyto okruhy ochrany informačních systémů:

- řízení fyzického přístupu včetně obrany před přístupem neoprávněným
- zabezpečení technických podmínek pro provoz (nepřetržité napájení a jeho kvalita, teplota, vlhkost)
- ochrana před vlivy vyšší moci (záplavy…)

3.1.1 FYZICKÝ PŘÍSTUP

Cílem řízení fyzického přístupu k prostředkům informačního systému by mělo být zamezení přístupu neoprávněných osob k běžným zařízením, jako jsou uživatelské počítače, terminály či tiskárny a zároveň přístup ke kritickým bodům struktury IS (datová úložiště, servery) umožnit pouze osobám k tomu výslovně určeným.

V případě zamezení přístupu neoprávněných osob je nutné definovat a bránit perimetr ochrany objektu (bezprostřední okolí či plášť budov) před jakýmkoli průnikem a definovat body, ve kterých lze do objektu vstoupit a opustit ho. Ochranu lze realizovat pomocí kamerových systémů, detekce pohybu, fyzickou ostrahou a nejlépe kombinací těchto prvků. Ve vstupních/výstupních bodech je nutné rozlišit příchozí osoby na ty, které mají do objektu volný přístup bez doprovodu a na návštěvy s povinným doprovodem. Ostatní osoby nesmí být dále do objektu vpuštěny. Při vstupu musí být každá osoba označena identifikátorem, který jednoznačně definuje její status (kmenový zaměstnanec, osoba s povoleným samostatným vstupem – např. uklízečky, návštěva s doprovodem) a který je povinna viditelně nosit po celou dobu pobytu. Oprávněná osoba, která doprovází návštěvu s doprovodem, za ni odpovídá, dokud objekt tato návštěva prokazatelně neopustí. Je-li objekt členěn do dalších vnitřních zón s omezeným přístupem, je výhodné pro přístup do nich využívat elektronické zámky či turnikety s jednofaktorovou autentizací (typicky PIN nebo čipová karta). Bezpečnostní předpisy musejí vynucovat nošení identifikátorů a ukládat zaměstnancům, aby osoby bez identifikátorů nebo s identifikátorem prokazujícím neoprávněnost pobytu v daném místě, hlásili k tomu určeným osobám, většinou ostraze objektu.

Přístup ke kritickým bodům struktury IS vyžaduje ostřeji nastavená pravidla – pokud se v prvním případě jednalo o režim „kdokoli, komu není zakázáno“, tak druhý případ se řídí pravidlem „pouze ten, komu je povoleno“. Znamená to tedy, že ke kritickým bodům infrastruktury smějí přistupovat pouze ty osoby, které jsou k tomu výslovně zmocněny. Pro identifikaci osob je vhodné při vstupu i výstupu použít dvoufázovou autentizaci (něco znát a něco vlastnit, tedy například PIN a čipovou

kartu). Vchod by měl být ovládán turniketem, umožňujícím na jednu autentizaci vstup pouze jedné osoby a musí vynutit autentizaci i při opuštění prostoru – tedy znemožnit aby na jednu identitu vstoupilo více osob.

Kritické body infrastruktury by měly být chráněny pasivními i aktivními bezpečnostními prvky. Pasivní prvky (bezpečnostní dveře, mříže apod.) by měly odolávat předem definovanou dobu veškerým pokusů o násilný průnik, aktivní prvky (kamery, čidla EZS) by měly tento pokus detekovat, dokumentovat a v ideálním případě vyrozumět ostrahu, která by měla průniku zabránit, dokud pasivní prvky ještě odolávají narušiteli.

Posledním, nikoli však významem, úkolem systému řízení fyzického přístupu je forma technického záznamu veškerých událostí, jež umožňuje v případech vyšetřování bezpečnostních incidentů monitorovat, kdo, kdy, kam měl potenciální přístup, kdo, kde, kdy skutečně byl.

3.1.2 TECHNICKÉ PODMÍNKY PRO PROVOZ IS

Pro bezpečný provoz IS je nutné zabezpečit i odpovídající technické podmínky. Jednou z nich je i odpovídající napájení – napájení z veřejné sítě je často doprovázeno následujícími problémy:

- Výpadek napájení (blackout)
- Dlouhodobé přepětí/podpětí (brownout)
- Napěťová špička/krátkodobý pokles (± 12%)
- Odchylka od standardní frekvence (50Hz)
- Napěťové rázy až 27kV (elektrostatické výboje, přeskoky při spínání)
- Šum
- Harmonické zkreslení (nelineární zátěž – elektromotory)

Vhodným řešením je předsazení nepřerušitelných zdrojů napájení – UPS, nejlépe typu „on-line“, kde se vstupní napětí transformuje a usměrní k paralelně připojeným akumulátorům a poté převede měničem zpět na garantované požadované hodnoty nízkého napětí (většinou 230V/50Hz). UPS umožňuje i řízené vypnutí technologie (řízený shutdown), pokud doba výpadku napájení hrozí přesáhnout dobu, kdy je UPS schopna zajistit napájení z akumulátorů. Je-li zapotřebí zajistit nepřetržitý chod IS, jeví se vhodným zejména pro větší organizace zjistit napájení z dvou či více větví vysokonapěťových rozvodů a (nebo) využití motorgenerátoru.

Dále je nutné zajistit optimální teplotu a vlhkost vzduchu pro provoz technologií. Klimatizační jednotky k tomu určené je vhodné zdvojovat pro případ poruchy a zajistit řízené vypnutí technologie pokud se teplota či vlhkost nedrží v požadovaných intervalech hodnot.

3.1.3 VLIVY VYŠŠÍ MOCI

Vyšší moc můžeme definovat jako objektivně nepředvídatelná a objektivně neodvratitelná náhoda (2). Příkladem mohou být rozsáhlé povodně přesahující známé zátopové oblasti nebo pád letadla.

Základním prvkem ochrany je vytváření pravidelně aktualizovaných bezpečnostních záloh datového fondu organizace a jejich bezpečné ukládání mimo objekt organizace. Dalším krokem je vybudování záložního pracoviště, které je schopné alespoň v omezené míře bezpečnostní zálohy zpracovávat.

3.2 PERSONÁLNÍ BEZPEČNOST

Personální bezpečnost je dalším důležitým faktorem v zabezpečení informačních systémů, za který primárně odpovídá personální útvar organizace. Ten je povinen zajistit ověřování předem definovaných podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k informačnímu systému. Přes nákladnost těchto prověrek je nutné mít na paměti, že každá osoba mající fyzický přístup k prostředkům IS, je potenciálním bezpečnostním rizikem (příkladem tohoto podcenění často bývají neprověření uklízeči, kteří mají přístup k počítačům v kancelářích a většinou jsou ponecháváni bez dozoru). Dále personální útvar zodpovídá za úvodní zaškolení nových zaměstnanců a pravidelné doškolování zaměstnanců stávajících s důrazem na právní a technický rámec ochrany IS. Je vhodné, aby zaměstnanci stvrdili svým podpisem, že byli proškoleni a obsahu školení porozuměli.

Důležitou povinností personálního útvaru je také ochrana osobních dat zaměstnanců. Krom toho, že ji ukládá Zákon č. 101/2000 Sb. o ochraně osobních údajů, tak tato data (mj. osobní číslo zaměstnance, zařazení ve struktuře organizace, jeho nadřízení či podřízení) jsou oblíbeným cílem pachatelů sociotechnických útoků, kterým umožní vydávat se za někoho jiného (zloději totožnosti), lovců mozků či průmyslové špionáže.

Pokud zaměstnanec končí pracovní poměr, je nezbytné, aby o této skutečnosti informoval personální útvar oddělení, zabývající se správou informačních systémů, aby mohlo včas zakázat veškeré lokální i vzdálené přístupy do IS. Je nutné také ke dni odchodu zaměstnance také zrušit jeho oprávnění v systémech řídící přístup do a v objektu organizace a odebrat zaměstnanci technické prostředky umožňující vstup do objektů organizace. Pokud bývalý zaměstnanec navštíví organizaci, je nutné mu vždy

přidělit status návštěvy s doprovodem – ne všichni stávající zaměstnanci musí být o jeho odchodu informováni a on by se tak snadno mohl dostat k citlivým informacím.

Končí-li pracovní poměr výpovědní lhůtou, je vhodné připravit pro tyto případy program vyvedení pracovníka z organizace. Měl by zahrnout omezení přístupu (logického i fyzického) k IS na úroveň nezbytně nutnou pro ukončení pracovního poměru, tedy takovou, kdy už nemá přístup k novým informacím a je zajištěno, že přístup k IS nemůže zneužít k destruktivním útokům.

4 LIDSKÝ FAKTOR – PODCEŇOVANÝ ČINITEL BEZPEČNOSTI IS

Úroveň technologie zabezpečení informačních systémů se neustále zvyšuje. Proto je velmi často středem zájmu pachatelů útoků nejslabší článek řetězu – člověk. Uživatel může svou indiskrecí (vědomou i nevědomou) či chybou, vyřadit z činnosti i ta nejsofistikovanější bezpečnostní zařízení.

Bezpečnostní incidenty, které jsou zaviněny lidským faktorem, lze dále dle Jírovského (3) dělit na incidenty:

- Úmyslné, tedy ty, jež jsou vedeny motivem poškodit systém nebo jeho uživatele, a které se dále dělí na:
    - Pasivní – což je nejčastěji sledování obsahu toku informací (například odposlech). Tyto metody přímo neovlivní chod či výkon systému a díky tomu je jejich detekce obtížná. Jedinou efektivní obranou je šifrování přenášených informací.
    - Aktivní – útokem na komponenty IS – operační systém, aktivní prvky síťové infrastruktury (zejména routery a přepínače). Aktivita útočníka ovšem umožňuje detekci a odvrácení útoku tomu určenými prostředky – firewally, systémy IDP (Intrusion Detection and Prevention System)
- Neúmyslné – které jsou zaviněny chybou či nečinností uživatele. Do této kategorie lze zařadit i úspěšné útoky sociotechnické

Podle pozice útočníka vůči organizaci můžeme rozlišovat útoky přicházející z prostředí:

- mimo organizaci, často označované jako cracking či (lidově a méně přesně) hacking[1]

[1] Slovo Hacker původně v IT komunitě označovalo počítačového specialistu, který své znalosti využíval k odhalování bezpečnostně slabých míst informačních systémů, odstraňování těchto chyb či poskytování informací o nich tvůrcům programového vybavení či správcům „napadených“ sítí. Ti, kteří své

- zevnitř organizace, kdy útočníkem je typicky zaměstnanec atakované organizace[2]. Pachatel při svých aktivitách vychází ze znalosti prostředí, bezpečnostních opatření. Často má k dispozici i potřebná přístupová práva pro práci s informačním systémem organizace.
- Oba přístupy se mohou samozřejmě kombinovat.

4.1 ČINITELÉ

4.1.1 NESPOKOJENÍ ZAMĚSTNANCI

Ztráta loajality stávajícího zaměstnance je vážným bezpečnostním rizikem. Na rozdíl od útočníka přicházejícího vně struktury organizace, je insider vybaven detailní znalostí vnitřního prostředí. Může se pohybovat v prostorách organizace, disponuje přístupem do informačního systému. Zaměstnanec prochází systémem bezpečnostních školení, který za normální situace pomáhá eliminovat zranitelná místa IT infrastruktury nezajistitelná technickými prostředky. Tím je paradoxně informován o slabinách systému a možnostech jejich zneužití.

4.1.1.1 Nejčastější motivy závadového jednání

- Finanční prospěch
- Zamaskování protiprávního jednání
- Touha po pomstě
- Pocit zneuznanosti, demonstrace vlastních schopností
- Konkurence mezi zaměstnanci
- Herostratismus

---

dovednosti využívají k svému obohacení či poškození jiných, jsou v IT komunitě označeni jako cracker či lamer.

[2] Často označovaný jako „insider“

4.1.1.2 Pracovní zařazení v hierarchii organizace a toho vyplývající potenciální ohrožení

4.1.1.2.1 Pracovník ve vedoucí funkci, manažer

Díky své odpovědnosti má v rukou (většinou) i klíčové rozhodovací pravomoci, v oblasti IT jde především o přidělování přístupových práv. Z titulu své funkce může informace požadovat, měnit je a v extrémních případech i ničit. Jakákoli kontrola je u osob na nejvyšších příčkách firemní hierarchie obtížná.

4.1.1.2.2 Správce IT

V oboru informačních technologií je v organizaci autoritou. Kontrola jeho chování laiky je prakticky nerealizovatelná. V rámci správy informačního systému má dispozici řízení přístupových práv celé organizace. Řešením je organizační oddělení bezpečnosti IS od běžné správy a podřízení tohoto oddělení bezpečnostnímu řediteli[3] nebo jinému pracovníkovi odpovědnému za bezpečnost. Odvrácenou stranou tohoto řešení je častá řevnivost mezi správou bezpečnostní a správou IT s výše zmíněnými riziky. Tyto problémy lze eliminovat pouze citlivou personální politikou.

4.1.1.2.3 Tvůrci programového vybavení

Možnost vložení zadních vrátek[4] je významným, známým a přesto často podceňovaným rizikem. U programů vyvíjených v rámci organizace je nutné trvat na bezpečnostní analýze programového kódu i za cenu růstu nákladů na vývoj softwaru. Při provozu komerčního software je nutné změnit všechna defaultně nastavená přístupová hesla, zamezit heslům prázdným a analyzovat chování programu, především jeho provoz v rámci počítačové sítě – otevírání nestandardních portů, komunikace mimo běžný adresový rozsah apod.

4.1.1.2.4 Správce sídla organizace

Riziko tohoto typu zaměstnanců je v jejich prakticky neomezeném pohybu po objektu organizace a díky tomu mohou úmyslně i z nedbalosti umožnit potenciálním

[3] Bezpečnostní ředitel – jeho práva a povinnosti jsou definována v (14), formuluje politiku organizace pro ochranu utajovaných informací

[4] Zadní vrátka – část programového kódu, která umožňuje získat kontrolu nad systémem

útočníkům přístup ke komponentům informačního systému. Nejde jen o přístup ke kritickým prvkům infrastruktury, který je (nebo by měl být) omezen (viz kapitola 3.1 této práce), ale i k řadovým počítačům, tiskárnám i kabeláži. V těchto případech hrozí, že se útočník pokusí instalovat hardwarové či softwarové zařízení pro monitoring provozu (sledování síťového provozu, keylogery).

4.1.1.2.5 Standardní uživatel

U běžného uživatele musí nastavení přístupových práv odpovídat objemu informací, které uživatel pro svou práci potřebuje, nutností je dodržovat zásadu need-to-know[5].

4.1.2 HACKERSKÁ KOMUNITA

4.1.2.1 Historie

Jak ve své práci píše Jírovský (3), pojmenování „hacker“ a termín „hacking“ vzniklo 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.

Tento pojem se do obecného povědomí rozšířil z Massachusetts Institute of Technology, kde slovo „hack“ bylo synonymem pro jednoduché, nekonvenční, efektivní a v neposlední řadě i efektní řešení problému.

První případy hackingu jsou spjaty s rozvojem automatických telefonních ústředen, kdy hlavním cílem hackerů bylo telefonování zdarma.

Od poloviny osmdesátých let minulého století se činnost hackerů zaměřuje na získávání přístupu do cizích informačních systémů, zpočátku prostým hádáním a kradením hesel až po sofistikované hardwarové i softwarové nástroje dnešních dnů. Mezi hackery tehdy patřili i později známé osobnosti jako Linus Torvald – tvůrce operačního systému Linux, Steve Jobs a Steve Wozniak, kteří založili známou firmu Aple. Významné hackerské útoky zachycuje dále uvedená tabulka.

[5] Zásada, že každý může znát pouze ty informace, které potřebuje pro svou práci, ale v takovém rozsahu, aby ji mohl vykonat.

Rok	Událost
1983	Počítač s kódovým označením WOPR (součást vojenského systému s označením BURGR) interpretoval hackerské vniknutí jako odpálení nepřátelské nukleární rakety.
1988	Morrisův „Worm“[6] se vymkl kontrole a napadl 6000 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.
1999	Skupina hackerů vydírá anglickou vládu – ovládla britský vojenský satelit.
2000	Jeden z největších útoků typu DDoS postihl servery eBay, Yahoo, Amazon; ztráty jdou do desítek milionů dolarů
2000	Ukradeny zdrojové kódy MS-Windows a MS-Office
2001	Byl proveden útok na DNS servery. i když se podařilo zjistit útok téměř okamžitě, odstranění následků trvalo dva dny.
2002	Microsoft přerušuje vývoj systému Windows, osm tisíc jeho programátorů je vyškoleno pro oblast bezpečnosti

Tabulka 1. Přehled významných útoků na přelomu století (3)

4.1.2.2 Kategorie hackerů

Základním rozlišením je motiv hackera k činnosti, respektive to, zda je nebo není hackerovo jednání v rozporu se zákonem, zda hlavním zájmem je snaha překonat technický problém, dosáhnout zisku za jakoukoli cenu, podporovat ideologická hnutí nebo působit ve státních službách

[6] Worm – druh počítačového viru

4.1.2.2.1 White hats

Jsou hackery v pravém slova smyslu. Respektují etiku hackera, často pracují ve firmách orientovaných na počítačovou bezpečnost. Jejich specialitou bývají penetrační testy, což jsou pokusy simulovat nepřátelský pokus o průnik do informačního systému organizace s cílem detekovat a odstranit slabá místa v ochranných mechanismech.

4.1.2.2.2 Black hats

Jak název napovídá, jsou pravým opakem „bílých klobouků“. Synonymem je pojem cracker. Primárním motivem je u této skupiny zisk, často se nechávají najímat organizovanými kriminálními skupiny či různými extremistickými organizacemi.

4.1.2.2.3 Hackeři z ideologických důvodů

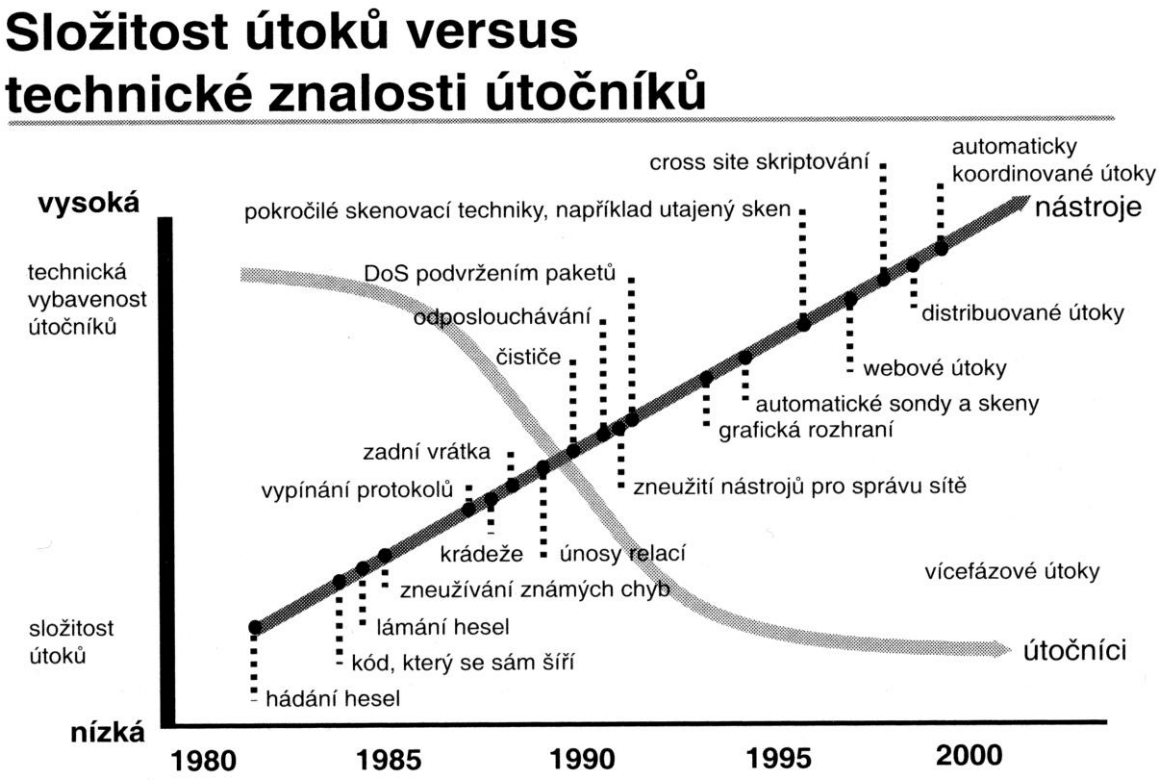
Jsou členy extremistických hnutí, cílem jejich aktivit jsou útoky proti vládním informačním systémům. Příkladem jsou muslimské skupiny často útočící proti izraelským či americkým cílům.

4.1.2.3 Hackerské nástroje

Pro průnik (přátelský i nepřátelský) používají hackeři sofistikované nástroje převážně softwarové ale i hardwarové povahy. Jedním z prvních byla paradoxně schopnost hackera vcítit se do psychiky oběti a odhadnout uživatelská jména a hesla. Na přelomu osmdesátých a devadesátých let se objevují první počítačové viry a programy pro hádání hesel, tzv. password crackers. S rozvojem počítačových sítí lokálních i internetu nastupují první útoky proti síťovým protokolům, zneužití technologií vzdáleného přístupu (RAS), první pokusy o packet-spoofing[7].

Vývoj hackerských nástrojů ukazuje následující graf.

[7] Packet-spoofing – metoda zamaskování vlastní síťové adresy pomocí podvržených paketů



Graf 1- uvedeno v (4)

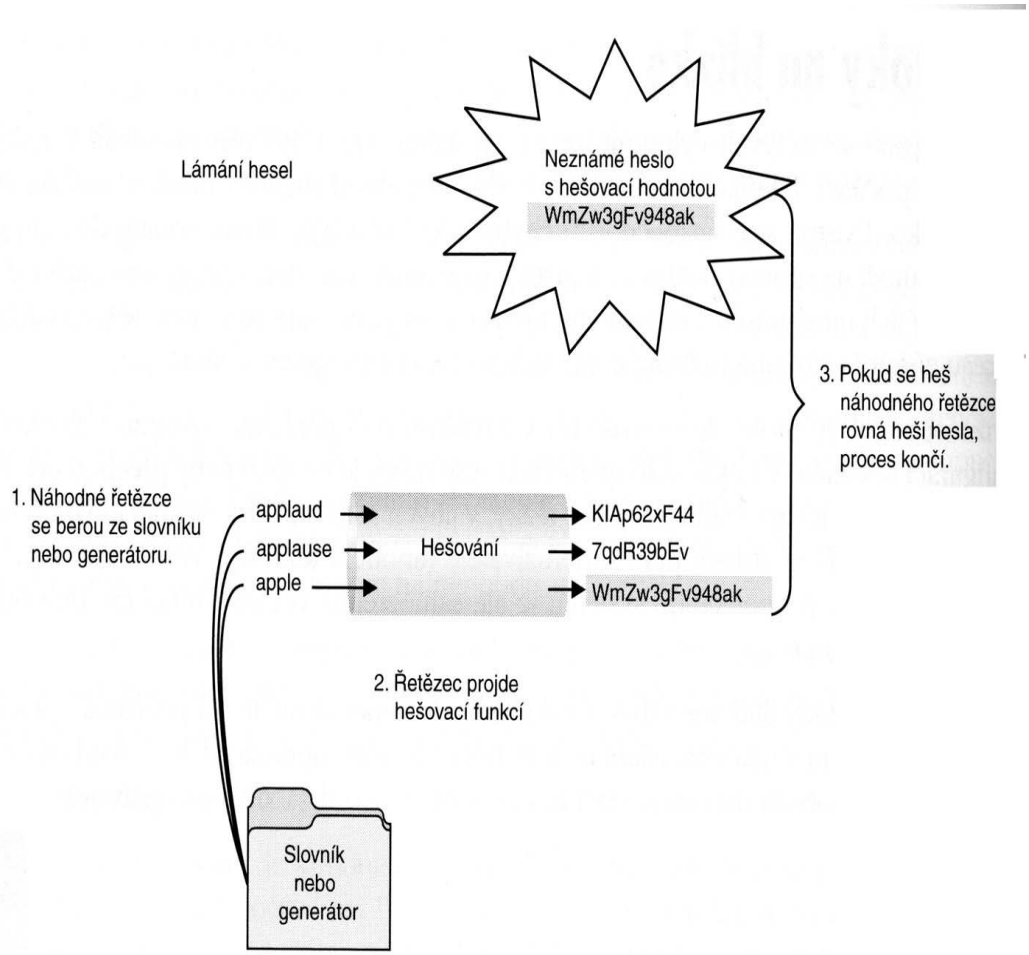
4.1.2.3.1 Password crackers

Tyto nástroje patří k nejstarším technologiím používaných hackerskou komunitou. Jejich hlavním a jediným úkolem je prolomení ochrany postavené na hesle. Tohoto cíle lze dosáhnout dvěma základními způsoby – útokem hrubou silou[8], kdy program postupně generuje všechny možné kombinace znaků a testuje, zda některá z nich neodpovídá hledanému heslu. Druhým způsobem jsou slovníkové útoky[9]. Programy, používající tuto metodu, pracují s rozsáhlou databází slov, výrazů a jejich variant, které testují, zda hledanému heslu odpovídají. V zásadě lze oba typy útoků použít při útoku na vzdálený počítač, tak i na počítač, ke kterému lze přistoupit lokálně.

Při lokálním útoku je často dostupný soubor s hesly (v unixových systémech v souborech /etc/password či etc/shadow, v MS-Windows od verze 2000 v souborech %windir%\WindowsDS\ntds.dit). Aby při kompromitaci tohoto souboru byla hesla

[8] V literatuře označované jako Brute-force-attack
[9] Dictionary-attack

i nadále chráněná, bývá hodnota hesel operačním systémem převedena do hashované[10] podoby. Pro hash se používají algoritmy MD-5, SHA-1 a rodina algoritmů SHA-2. Hesla, generovaná útočnými programy se tedy nejprve musí hashovat a až tato hodnota se porovnává s řetězci, uloženými v souborech hesel. Schéma tohoto postupu je na obrázku číslo 2.



Obrázek 1 – uvedeno v (5)

[10] Hash, hashovaní funkce je matematickou jednocestnou funkcí, která převádí vstupní data na krátký řetězec pevné délky, ze kterého nelze původní data rekonstruovat (na rozdíl od šifrování)

Autoři McClure, Scambry a Kurtz v (5) doporučují pro odhalování hesel v systémech Unix/Linux nástroje Crack od Aleca Muffeta a John the Ripper od autora s pseudonymem Solar Designer. Pro útoky na rodinu systémů Microsoft Windows jsou podle těchto autorů nejvhodnější programy pwdump2, pwdump3e, L0phtcrack a John the Ripper, který je i ve verzi pro Windows.

Vliv délky a složitosti hesla ilustruje tabulka číslo 2. Pro názornost je uvažována rychlost testu jedna kombinace za sekundu, rychlost na soudobých počítačích je řádově vyšší.

Počet znaků	MP	MP+C	MP+C+SZ	VMP	VMP+C	VMP+C+SZ
1	26	36	69	52	62	95
2	325	630	2 346	1 326	1 891	4 495
3	2 600	7 140	52 394	22 100	37 820	138 415
4	14 950	58 905	864 501	270 725	557 845	3 183 545
5	65 780	376 992	11 238 513	2 598 960	6 471 002	57 940 519
6	230 230	1 947 792	119 877 472	20 358 520	61 474 519	869 107 785
7	657 800	8 347 680	1 078 897 248	133 784 560	491 796 152	11 050 084 695
8	1 562 275	30 260 340	8 361 453 672	752 538 150	3 381 098 545	121 550 931 645

Tabulka číslo 2 - zdroj dat (6)

legenda: MP – malá písmena, VMP malá a velká písmena, C – číslice, SZ – tisknutelné znaky (např:. &@./)*

Obranou proti lámání hesel je v první řadě používání hesel kvalitních, tedy dostatečně (alespoň 8 znaků) dlouhých, využívajících kombinací malých a velkých písmen spolu s číslicemi a speciálními znaky. Důležitá je i periodická změna hesla (Národní bezpečnostní úřad ve své vyhlášce (7) stanovuje interval šedesáti dnů pro informace kategorie důvěrné a třiceti dnů pro informace kategorie tajné). Správci systému musí pomocí systémových politik vynucovat zmíněné požadavky hesla na složitost, minimální délku a nastavit i minimálně tří měsíční historii hesel – tedy časový interval, po který se již jednou požité heslo nesmí znovu používat. Nutné je i omezení počtu pokusů, kolikrát lze heslo opakovaně zadat a po vyčerpání nastavit uzamčení uživatelského účtu buď na konkrétní časový interval nebo do odemčení účtu pověřenou

osobou. Druhá varianta je méně komfortní pro uživatele, ale umožňuje správci IS (či bezpečnostnímu správci) detekovat případné útoky na systém.

4.1.2.3.2 Trojan horses

Trojští koně jsou další z oblíbených zbraní hackerů a jsou přesnou softwarovou obdobou svého mytologického předchůdce. Označují se tak programy, které si uživatel sám dobrovolně instaluje do svého počítače, respektive programy, které se bez uživatelovy aktivní spoluúčasti samy nespustí. Trojský kůň je spíše označení cesty, jak se programový kód do počítače dostane, než popis jeho činnosti. Funkce takto instalovaného programu sahají od již popsaných password crackerů k programům typu Backdoor či DDoS popsaných dál.

Programy tohoto typu jsou často součástí různých bezplatně šířených utilit a her, ale často jsou integrovány do tzv. cracků, programů, které nelegálně odemykají komerční software distribuovaný on-line.

Dokladem zrádnosti technologie trojských koní je program BoSniffer. Presentuje se jako bezplatná bezpečnostní utilita, která slouží k detekci a následnému odstranění nechvalně známého backdoorového software BackOrifice[11], ale ve skutečnosti tento program sama instaluje a spouští. Dalším příkladem mohou být infikované spořiče obrazovky, které většina běžných uživatelů za programy ani nepovažuje.

Proti známým a popsaným variantám trojských koní preventivně chrání aktualizované antivirové programy. Ty nepomohou proti novému a rychle šířenému kódu a jsou bezmocné i proti programům psaným na zakázku k průniku do konkrétních systémů. Zde pomůže pouze důsledné dodržování bezpečnostních standardů organizace – tedy zákaz spouštění neprověřených programů a zákaz neautorizované instalace jakýchkoli programů.

[11] BackOrifice je program typu backdoors (zadní vrátka) a slouží ke vzdálenému převzetí kontroly napadeného počítače.

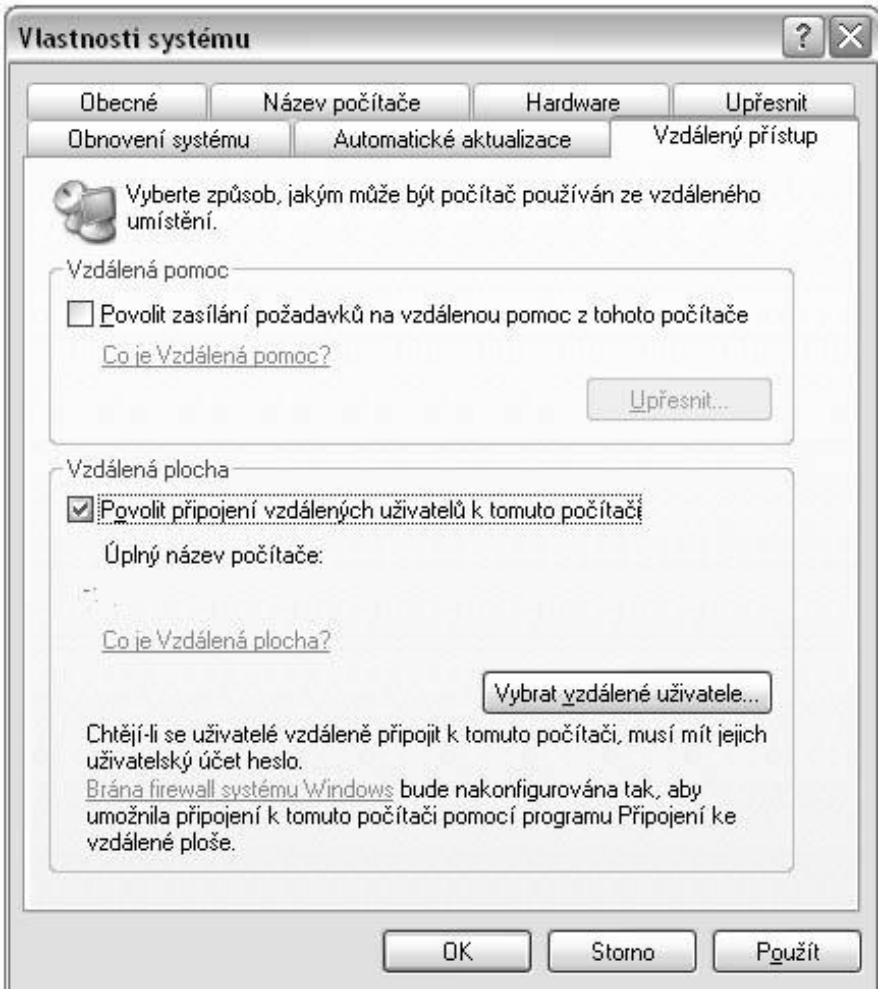
4.1.2.3.3 Zadní vrátka

Neboli backdoors – hlavní úlohou programů tohoto typu je zajištění vzdáleného přístupu na napadený počítač. Tyto aplikace jsou typu klient-server a připomínají svou funkčností standardní software jako je například Symantec pcAnywhere. Serverový kód je instalován na kompromitovaném počítači a umožňuje útočníkovi provádět ze svého počítače (strana klienta) na vzdáleném požadované příkazy.

Serverová část se může šířit formou trojského koně či samovolně v podobě viru. Tak lze zasáhnout buď vybraný konkrétní systém (disponující pro útočníka zajímavými informacemi) nebo naopak infikovat i tisíce počítačů, které je možné použít k dalším útokům. Technologie backdoors se s výhodou používá pro maskování stop při útocích – ke konečnému napadení se použije řetěz kompromitovaných počítačů rozmístěných po celé planetě (nejlépe ve státech s přepokládanou minimální ochotou k mezinárodní právní spolupráci) a tak je možnost vysledování pachatele téměř vyloučena.

Proti popsaným formám backdoors ochrání aktualizované antivirové programy s podobnými omezeními, jaká jsou u trojských koní. Pokud již takovýto program na napadeném počítači běží a není antivirem odhalen ani při následných skenech, je jeho zjistitelnost poměrně obtížná. Pokud není komunikace backdooru maskovaná, lze ji zachytit firewallem jako pokus otevřít porty nestandardních, často vysokých čísel. Využívá-li ovšem tento software pro svou činnost příkladně port 80 (což je standardní port pro protokol http pro přístup na webové stránky) a útočník k počítači přistupuje jen občas, je backdoors prakticky nezjistitelný.

K nejznámějším představitelům této kategorie hackerských nástrojů patří Back Orifice 2000 či SubSeven. Důležité je podotknout, že obdobné technologie jsou nativně součástí moderních systémů Microsoft Windows v podobě „vzdálené plochy“. Pokud jsou tyto komponenty Windows aktivní, umožní v případě liberálně nastavených systémových politik převzetí kontroly nad počítačem stejně jako backdoors. Viz obrázek číslo 2.



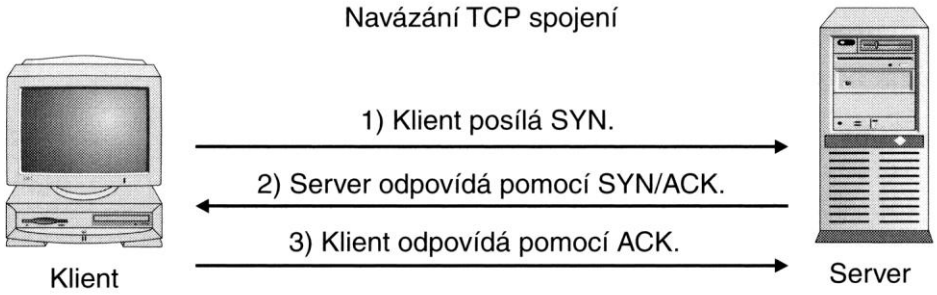
Obrázek číslo 2

4.1.2.3.4 Nástroje pro skenování portů

Skenování portů dává útočníkovi přehled, jaké síťové programy a služby jsou na napadeném počítači aktivní a za určitých podmínek umožňuje detekovat i operační systém, který na cílové počítači běží. Pro hackera jsou nejdůležitější právě síťové služby, které, pokud jsou nekorektně nastaveny nebo jejich kódy obsahují chyby, umožňují útočníkovi získat k napadenému počítači vzdálený přístup.

Samotné skenovací techniky můžeme rozdělit do několika základních skupin:

- Standardní TCP Connect – skener se připojí na cílový port naváže standardní spojení tak, jak je definováno normou RFC793. Tento způsob je snadno detekovatelný běžnými firewally.



obrázek 4 – zdroj (5)

- TCP SYN – half open scan – pokud napadený počítač odpoví pakety SYN/ACK (tj. na portu někdo naslouchá) skener spojení přeruší
- Null TCP scan – na cílový počítač je poslán paket bez jakýchkoli příznaků a port je na cílovém počítači zavřený, měl by tento dle specifice RFC793 odpovědět paketem s příznakem RST
- UDP scan – je-li na cílový port poslán UDP paket a nevrátí-li cílový počítač paket ICMP port unreachable, je port otevřený. Díky charakteru protokolu UDP (bezstavový protokol) je přesnost výsledku skenu snížena.

K typickým nástrojům pro skenování portů patří pro unixové platformy program strobe, jehož autorem Julian Assenge a zejména systém nmap od autora s pseudonymem Fyodor. Příklad výpisu výsledku skenu programu nmap ve verzi 4.85 beta v grafickém rozhraní Zenmap je vidět na obrázku 5.

Skener detekoval s pravděpodobností 94% operační systém Microsoft Windows Server SP2 (který je skutečně nainstalovaný). Správně byly rozpoznány všechny otevřené porty a na portech 1352 korektně identifikována služba Lotus Domino, 1503 a 8081 služba IBM Lotus Sametime. Služby na zbývajících portech 1533 a 8082 nebyly rozpoznány správně – i na těchto portech naslouchala služba IBM Lotus Sametime.

Nejlepší obranou proti skenování portů a nepřátelskému průzkumu sítě obecně je pečlivé sledování logů firewallu a systémů IDP a preventivní zahazování ICMP paketů na hraničním routeru sítě.

Obrázek číslo 5

4.1.2.3.5 Sniffer

Svým původem byly sniffery vhodným nástrojem pro diagnostiku provozu sítě. Během síťového provozu sbírají, ukládají a analyzují data v síťovém segmentu, ve kterém je sniffer připojený. Podmínkou fungování je zapnutí promiskuitního modu síťové karty na hostitelském počítači snifferu. Díky omezení na místní segment sítě je pro zvýšení účinnosti vhodné sniffer nasazovat co nejblíže k páteřní síti organizace.

Sniffery patří k mimořádně nebezpečným nástrojům, protože umožňují přístup k datům přenášeným po síti. Tedy k přenášeným uživatelským jménům a heslům, e-mailům i dokumentům. Moderní sniffery typu Dsniff, jak o nich píší McClure, Scambry a Kurtz v (5), pomocí utility arpredirect objedou většinu přepínačů a mohou tedy snímat data i na přepínané síti.

Při podezření na sledování je možné se pokusit detekovat karty pracující v promiskuitním režimu například pomocí programu Sentinel a na detekovaných počítačích se pokusit sniffer nalézt a odstranit.

Jedinou efektivní obranou proti potenciálnímu odposlechu dat je šifrování síťového provozu technologiemi SSH, IPsec apod.

4.1.2.3.6 Rootkit

Rootkit je definován Jírovským v (3) jako soubor technik pro skrývání činností prováděných na operačním systému. Rootkity pracují na privilegované úrovni 0 tedy se stejnými privilegiemi jako jádro operačního systému. Rootkit se v podobě jaderného modulu (5) instaluje do jádra operačního systému. Díky tomu může kontrolovat a měnit všechny systémová volání. Soubory, které rootkit potřebuje pro svou činnost, může maskovat jako vadné bloky pevného disku nebo v systémech Windows je zapisovat pomocí datových proudů[12]. V privilegovaném režimu se rootkit dokáže odpojit ze seznamu právě aktivních procesů. Některé rootkity dokáží spustit napadený operační systém jako virtuální stroj a tak převzít nad ním kontrolu absolutně.

[12] Alternate Data Stream komponenta MS-Windows pro dodržení kompatibility s operačními systémy firmy Aple.

Základní obranou proti rootkitům je prevence, tak jak již byla popsána u předchozích hackerských nástrojů. Paradoxem ovšem je, že jeden z nejznámějších rootkitů, Sony XCP, je systémem vyvinutým a distribuovaným firmou Sony jako ochrana proti kopírování jí produkovaných kompaktních disků. Je-li již systém napaden, je detekce rootkitu z prostředí napadeného systému ve většině případů vyloučena. Řešením je spustit operační systém z nezkompromitovaného media a pokusit se rootkit odstranit (vhodnými nástroji mohou být i volně šiřitelné programy Klister, sdtrestore či VICE jež jsou vhodnou alternativou ke specializovaným forenzním produktům typu Encase firmy Guidance Software). Často ovšem jedinou jistotou je v těchto případech reinstalace operačního systému.

4.1.3 ZLOČINCI A KYBERTEROTISTÉ

4.1.3.1 Definice kriminality související s IT

Jírovský v (3) definuje kybernetickou kriminalitu jako jakýkoli čin směřující k narušení nebo zneužití počítače nebo počítačového systému a informací v něm obsažených. Hlavní charakteristikám tohoto druhu kriminálního jednání patří:

- kriminalita „bílých límečků“
- vysoká latence – mnoho trestních činů zůstává neobjeveno a neméně velké množství poškození (typicky velké finanční a průmyslové instituce) z obavy ze ztráty prestiže ani neohlásí
- závadové jednání může najednou zasáhnout velké množství fyzických i právnických osob a způsobit jim škody značného rozsahu
- globální dosah internetu zvyšuje reálnou vzdálenost mezi útočníkem a obětí
- je dosaženo vysoké míry anonymity
- je patrná značná míra asymetrie mezi prostředky útočníka (který si volí čas, prostor i technologii k útoku) a napadeného (obrana je plošná, nákladná a díky nemožnosti zaměřit ji na konkrétní útok často i málo účinná)
- v české republice k tomu přistupuje i nízká míra akceptování důkazního materiálu v digitální formě

4.1.3.2 Klasifikace kriminality v oblasti IT

Ve své analýze (8) klasifikuje Mazel IT kriminalitu takto:

4.1.3.2.1 Zločiny proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů:

- nezákonný přístup
- nezákonné odposlouchávání
- narušování dat
- narušování systémů
- zneužití prostředků

4.1.3.2.2 Zločiny se vztahem k počítači:

- počítačové padělání
- počítačový podvod

4.1.3.2.3 Zločiny se vztahem k obsahu počítače

- dětská pornografie

4.1.3.2.4 Zločiny se vztahem k autorským nebo obdobným právům

Dle téhož autora (8) je zaznamenáníhodné i dělení podle akčního plánu eEurope 2002[13]:

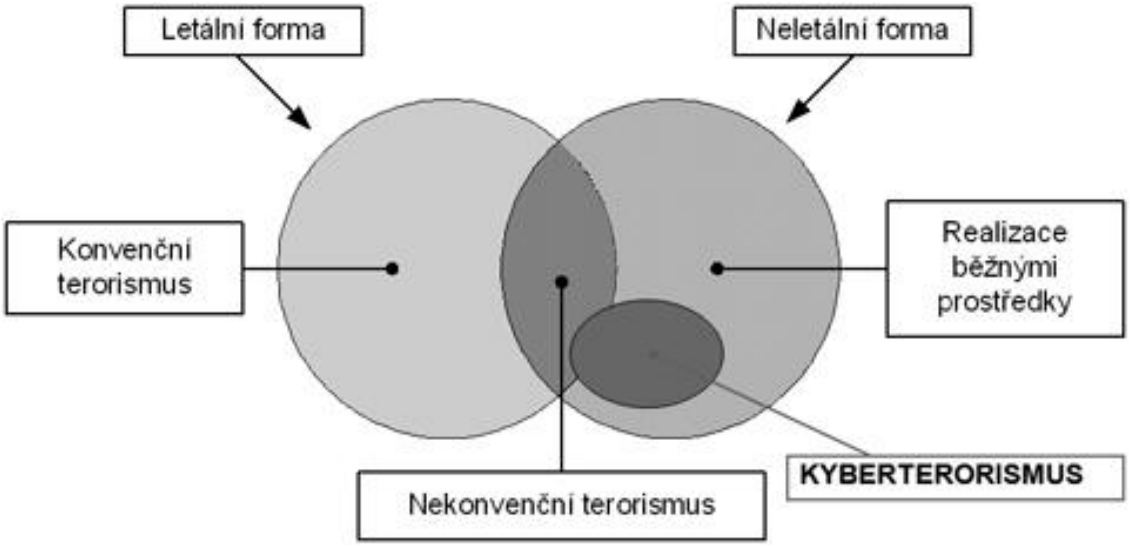
- zločiny porušující soukromí (ilegální sbírání, uchovávání, modifikace, zveřejňování a šíření osobních dat)
- zločiny se vztahem k obsahu počítače (pornografie, zvláště dětská, rasismus, vyzývání k násilí)
- ekonomické (neautorizovaný přístup a sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové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

[13] eEurope 2002 – Iniciativa EU „Informační společnost pro všechny“

4.1.3.3 Kyberterorismus

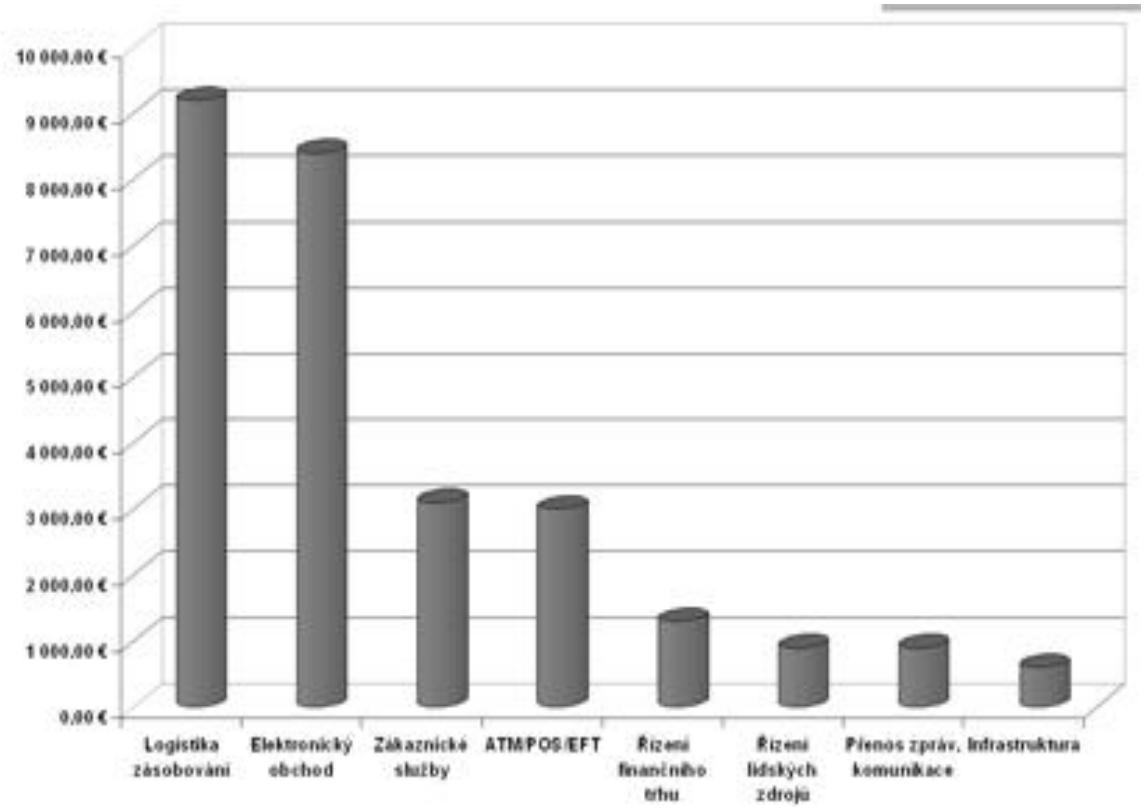
4.1.3.3.1 Definice

Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný 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. Autorkou této definice je Dorthy E. Denningová - citováno dle (9). Pozici kyberterorismu vůči ostatním formám teroristických aktivit dokumentuje obrázek číslo 6.



Obrázek číslo 6 – zdroj (3)

Aby však takovýto útok mohl být chápán jako teroristický, musí být směřován proti infrastruktuře, jejíž vyřazení by radikálním způsobem mohlo ovlivnit normální život společnosti – příkladem může být napadení systémů řízení letového provozu, energetické rozvodné soustavy, vodárenství, burzy a systémy elektronického obchodování. Odhady způsobených ekonomických ztrát za jednu minutu výpadku činnosti IS dle tržního segmentu jsou dobře patrné z grafu číslo 2.



Graf číslo 2- zdroj (9)

4.1.3.3.2 Kategorie útoků

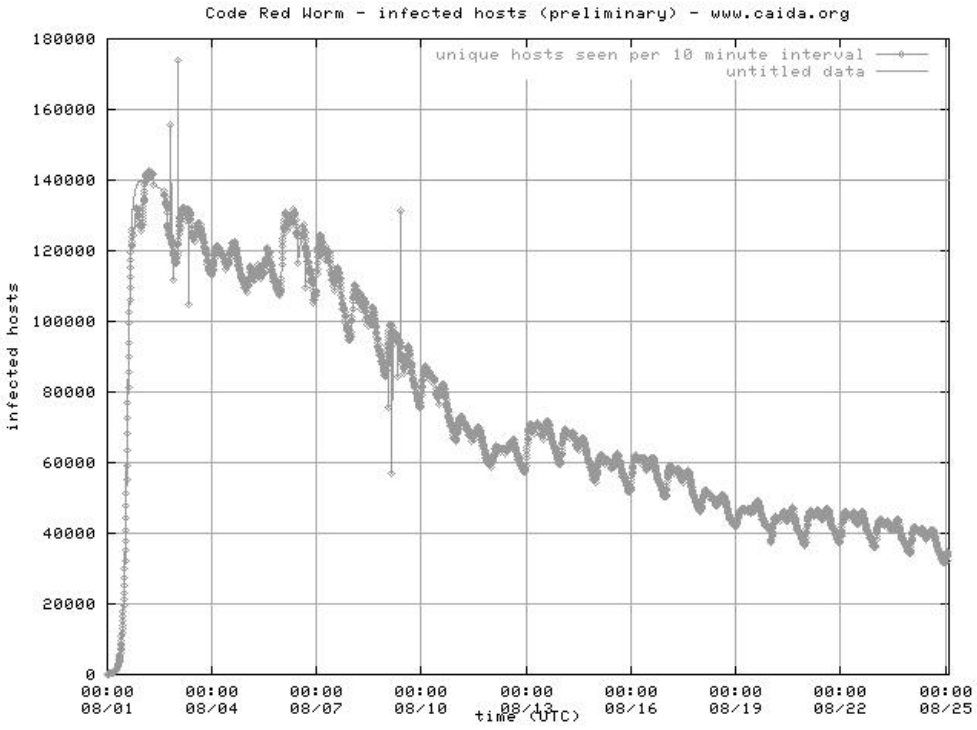
Teroristické útoky proti informačním systémům se dají dělit do několika kategorií.

- bezprostřední útok zaměřený primárně na kritické prvky informační či telekomunikační systému
- nepřímý útok – při útoku na jiný cíl je zasažena i informační a komunikační infrastruktura
- kombinovaný útok – cílem napadení IKS je prohloubení účinku útoku na jiný cíl
- využití informační a komunikační infrastruktury (internetu) pro koordinaci a řízení teroristických aktivit

4.1.3.3.3 Zaměření útoků podle stylu napadení

- Znefunkčnění služby – cílem útoku je vyřadit systém z provozu nebo jeho znestabilnění – toho lze dosáhnout fyzickým útokem na klíčový prvek infrastruktury, útoky typu DoS nebo infiltrací malware[14]. Rychlost šíření malware dobře ilustruje graf číslo 3. Zachycuje časový průběh infekce internetových systémů virem Code Red Worm.
- Odposlech, pozměnění či podvržení informací – cílem je směrování datových toků tak, aby se požadovaná akce realizovala. To je možné provést softwarovým napadením páteřních směrovačů nebo serverů DNS[15]

Kyberterorismus není ideologií, ale spíše technologií, a tak se stává součástí obecných ideologických typů terorismu, jak je definují Foltin s Řehákem v (10), tedy terorismu politického, náboženského, psychotického a kriminálního.



Graf číslo 3 – publikováno v (11)

[14] Malware – obecně programový kód mající způsobit škodu či újmu (viry, trojské koně, ale i reklamní software)
[15] DNS - Domain Name Services - systém, který převádí jmenné názvy na IP adresy

5 TYPY PRŮNIKŮ DO INFORMAČNÍCH SYSTÉMŮ

5.1 TAXONOMIE HROZBY

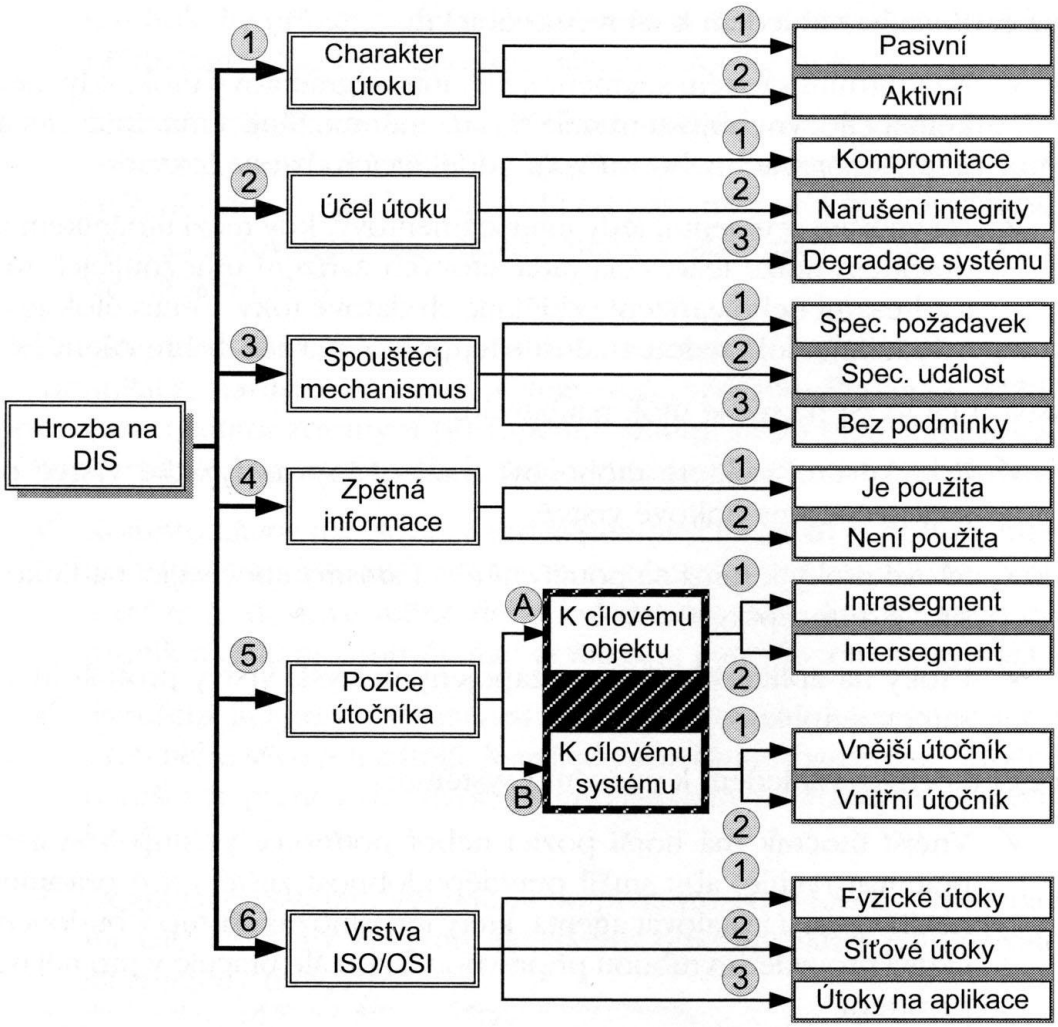
Vzhledem k velkému počtů typů útoků na informační a komunikační systémy je nutné provést jejich základní klasifikaci. Prvotním vodítkem může být objekt útoku. Pak lze rozlišit útoky takto:

- Fyzické útoky – cílem je samo zařízení nebo nosič informace. Příkladem může být krádež pevného disku s citlivými informacemi nebo zničení počítače – k tématu fyzické bezpečnosti odkazuje kapitola 3.1 této práce.
- Technologické útoky – objektem napadení jsou především data – v podobě například databáze jako funkčního systému nebo datového toku na komunikačních linkách. Cílem napadení je kompromitace dat, narušení jejich integrity či jejich zničení.
- Sociotechnické útoky - objektem napadení je člověk. a to buď jako nositel citlivých informací, daleko častěji jako osoba disponující znalostmi, umožňujícími zpřístupnění požadovaných informací. Formou napadení je psychologická manipulace.

5.2 TECHNOLOGICKÉ PRŮNIKY

5.2.1 KATEGORIZACE

Základní kategorizaci útoků popisuje Jírovský v (3) a znázorňuje ji schéma na obrázku číslo 7.



obrázek číslo 7 – publikováno v (3)

Každý pokus o průnik se vyznačuje výše uvedenými charakteristikami:

5.2.1.1 Charakter útoku

- pasivní – vhodným příkladem může být odposlech bezdrátové síťové komunikace – takovýto útok je pro napadeného prakticky nezjistitelný
- aktivní – tento typ útoku předpokládá zásah do síťového provozu či modifikaci konfigurace napadeného systému. Tyto změny jsou zjistitelné[16].

5.2.1.2 Účel útoku

- Kompromitace – dat, ale i operačního systému – je stavem, kdy útočník získá alespoň potenciální přístup k datům nebo získá kontrolu nad napadeným počítačem.
- Narušení integrity – příkladně dat, datového toku – je stav, kdy minimálně nelze garantovat neporušenost dat. Takovým útokem je zarušení mikroreléového spoje nebo poškození databázového souboru virem.
- Degradace systému (výkonu, rychlosti odezvy) – vede k narušení funkcionality systému nebo omezení dostupnosti pro uživatele. Představují ho útoky typu DoS, ale může jím být i fyzický zásah do technického vybavení.

5.2.1.3 Spouštěcí mechanismus

- Požadavek – demand – útočník pasivně vyčkává, dokud potenciální cíl nepožaduje provedení předem specifikované akce. Příkladem jsou DNS cache poisoning attacks[17].
- Událost – even – narušitel aktivně monitoruje chování napadeného systému a nastane-li definovaná událost, provede se požadovaná akce.
- Bez podmínky – jediným mechanismem je rozhodnutí narušitele.

5.2.1.4 Zpětná vazba

- Existuje – například při převzetí řízení napadeného systému – ale zvyšuje pravděpodobnost detekce napadení a identifikace útočníka.

[16] I když mnohdy velmi obtížně – rootkity, malware využívající maskování technologiemi stealth

[17] DNS cache poisoning attacks – umožňují útočníkovi přesměrovávat provoz na podvržené servery

- Neexistuje, respektive není nutná. Příkladem může být již zmíněné zarušení mikroreléového spoje.

5.2.1.5 Pozice útočníka k cílovému systému[18]

- Vnitřní útočník, insider, má dostatečná oprávnění umožňující přístup k systému, disponuje znalostmi osob i prostředí
- Vnější útočník logicky disponuje omezenou sumou informací oproti insiderovi, je ohrožen i komunikací s napadeným systémem, kterou je možné detekovat.

5.2.1.6 Pozice útočníka k cílovému objektu[19]

Zde se spolu s autory McClure, Scambry a Kurtz v (5) domnívám, že skutečnost, zda je či není útočník uvnitř segmentu napadené sítě, není významná. Jírovský v (3) říká, že důležitým znakem segmentu je, že přenášené pakety jsou dostupné všem zařízením v segmentu. Toto tvrzení je nástupem přepínaných sítí překonané.

5.2.1.7 Vrstva ISO/OSI

- útoky na fyzické a spojové vrstvě – odposlech bezdrátového spoje
- útoky na síťové a transportní vrstvě – odposlech IP
- útoky na vrstvě aplikační – napadení ftp či http přenosů

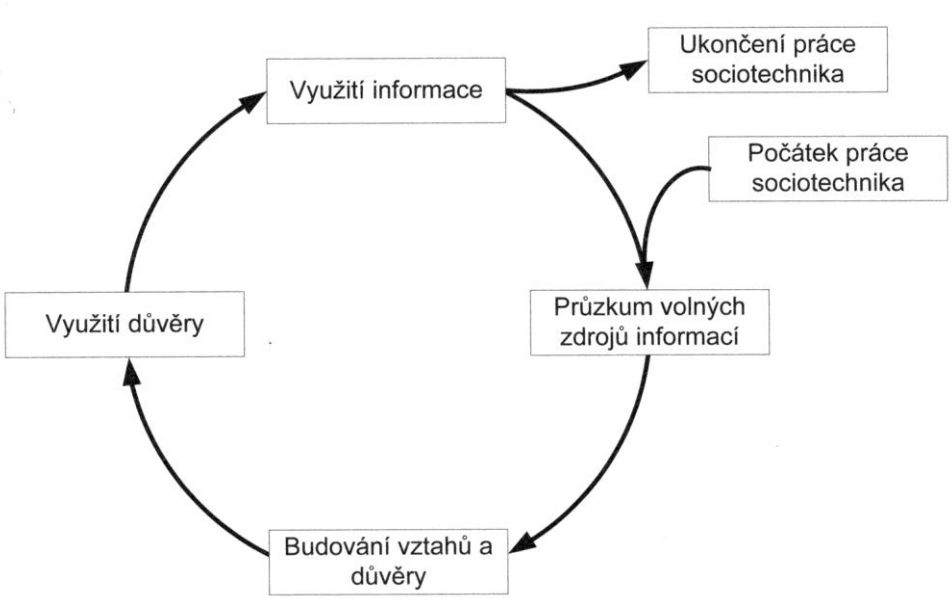
[18] Cílovým systémem je míněna napadená organizace
[19] Míněn segment počítačové sítě

5.3 PRŮNIKY ZALOŽENÉ NA SOCIOTECHNICKÝCH METODÁCH

Mitnick a Simon (12) definují sociotechniku jako ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využít lidi, se kterými hovoří, případně dodatečné prostředky, aby získal potřebné informace.

Obdobně k Mitnikově a Simonově definici říká pseudonym Harl citovaný v (3): Na světě neexistuje žádný počítačový systém, který by nebyl závislý na lidech. To znamená, že bezpečnostní slabina je univerzální, nezávislá na platformě, síti či druhu vybavení. Kdokoliv, kdo má přístup k jakékoli části systému, fyzicky či elektronicky, představuje potenciální bezpečnostní ohrožení.

Obecné schéma sociotechnického útoku naznačuje obrázek číslo 8. Zobrazený cyklus se může opakovat, kdy získaná informace se použije v dalším kroku útoku.



Obrázek číslo 8 – publikováno v (3)

5.3.1 PŘÍPRAVA ÚTOKU

5.3.1.1 Získávání informací

Cílem sociotechnika je získat takový rozsah informací o terči svého útoku, který mu umožní vystupovat ve zvolené roli. Zájem útočníka začíná od veřejně dostupných informací (sídlo firmy, zveřejněné kontaktní údaje) k informacím běžně nezveřejňovaným (jako je seznam zaměstnanců, jejich pracovní pozice, e-maily a telefony, přezdívky, firemní žargon a slang). Informace vedou k vytypování konkrétní osoby, vůči které bude veden sociotechnický útok. Dalším krokem tedy bude vyzískání znalostí o jejích povahových rysech, zázemí a kontaktech. Tyto znalosti pak vedou k volbě konkrétní komunikační strategie.

5.3.1.1.1 Otevřené zdroje

Jsou takové zdroje informací, které jsou dostupné veřejnosti a (s výjimkou autorských práv) není přístup k nim omezován. Patří sem Informace, které o osobě potenciální oběť sama zveřejňuje (firemní webové stránky), aplikace typu Yellow Pages, ale i speciálněji zaměřené nástroje typu who.is, ripe.net apod. Při zadání dotazu na populární server zprávy.idnes.cz do databáze je možné zjistit jméno osoby odpovědné za provoz internetových komunikací, její e-mail, telefon i kontaktní adresu – viz příloha 11.5.

5.3.1.1.2 Nelegální a pololegální zdroje informací

Do této kategorie lze zařadit informace takové, které jsou ve zdrojích otevřených nedostupné. Jejich získávání je na hraně zákonného jednání a často je lze označit jako podvod či krádež.

Na základě informací z otevřených zdrojů může sociotechnik zkoušet získávat další informace pod tzv. falešnou vlajkou – může se například vydávat za pracovníka servisní firmy, o které získal informace z internetu.

Velmi účinnou metodou je prohledávání odpadků – díky nízkému bezpečnostnímu povědomí ve většině firem mají odpadky vysokou informační hodnotu. V odpadu lze nalézt telefonní seznamy, faktury s čísly bankovních účtů,

zdrojové kódy programového vybavení, ale i paměťová media s rekonstruovatelným obsahem. Příklad viz příloha 11.6.

5.3.1.2 Budování důvěry

Po získání potřebných informací je nutné zvolit vhodnou komunikační strategii spočívající jednak ve výběru komunikačního prostředku a stylu komunikace.

Komunikačním prostředkem může být:

- telefon
- e-mail
- dopis
- osobní kontakt

Styl komunikace:

- důvěrný (přítel – přítel)
- oficiální – partnerský (obchodní jednání)
- oficiální – nadřízený (z pozice autority, nadřízeného)
- oficiální – podřízený (v submisivní roli, uklizečky, opraváře, poslíčka)

5.3.2 METODY SOCIOTECHNICKÉHO PŘESVĚDČOVÁNÍ

- altruismus – dobrý pocit z vědomí nezištné pomoci druhému „v nouzi“
- strach – vyvolání pocitu strachu z konkrétní události vede ke snížení ostražitosti vůči tomu, kdo nabízí pomoc s řešením této situace
- morální povinnost – oběť je přesvědčována, že se děje bezpráví, které lze odvrátit akcí sociotechnikem požadovanou
- přenesení odpovědnosti – sociotechnik ujistí cílovou osobu, že odpovědnost za jím požadovanou akci nese třetí osoba, případně sociotechnik sám. Pro tuto situaci je vhodný styl komunikace z pozice autority.
- důvěra

- Možnost povýšení – pokud si cílová osoba připustí, že splnění sociotechnikovy žádosti povede potěšení nadřízeného, zvýší se její ochota požadavek splnit

5.3.3 FORMY ÚTOKU

5.3.3.1 Telefonní útoky

Patří k oblíbeným a účinným technikám používaných sociotechniky. Umožňují zakrýt podobu volajícího či věrohodně předstírat jinou identitu. Prvním cílem těchto útoků bývají help-desky organizací. Jejich pracovníci jsou přímo školeni k poskytování informací a z titulu své funkce se snaží vyhovět.

5.3.3.2 Útoky z prostředí internetu

5.3.3.2.1 Typ nigerijské dopisy

Jedná se o podvodné e-maily, často je předpokládána interaktivní komunikace, kdy tím, že oběť na dopis odpoví, potvrdí útočníkovi funkčnost získané e-mailové adresy. Následuje většinou výměna několika dopisů zakončená žádostí o nějakou formu finanční pomoci či transakce.

5.3.3.2.2 Phishing

V češtině se občas používá termín rybaření. Cílem phishingu je získání citlivých neveřejných informací – nejčastějším cílem jsou čísla kreditních karet a přihlašovací údaje k účtům internetového bankovnictví. Oběti jsou vyzývány k zaslání požadovaných dat zpět e-mailem, nebo e-mail obsahuje odkaz na stránky snažící se napodobit stránky oficiální instituce. Autoři podvodných mailů počítají s tím, že díky velkému množství rozesílaných e-mailů i nízké procento získaných údajů může být zajímavé. Průzkum provedený OIKT České zemědělské univerzity popsaný v (13) ukazuje, že po dobu funkčnosti „podvodných“ stránek 9,87% studentů zadalo korektní přihlašovací údaje. To představuje 2 253 získaných přihlašovacích údajů. není bez zajímavosti 13% „nachytaných“ studentů oboru IT. Odborná erudice tedy není účinnou obranou před sociotechnickým útokem. Souhrn dat z průzkumu prezentuje tabulka číslo 3.

Ročník	I	II	III	IV	V	Celkem
Počet studentů	8250	5250	4066	2944	2312	22822
Zachycených ID	734	595	427	226	271	2253
Procento	8,90%	11,33%	10,50%	7,68%	11,72%	9,87%
Studenti IT	370	341	278	130	145	1264
Zachycených ID	32	45	31	15	19	142
Procento	8,65%	13,20%	11,15%	11,54%	13,10%	11,23%

tabulka číslo 3 – zdroj dat (13)

5.3.3.2.3 Pharming

Je technologie na pomezí útoku sociotechnického a technologického. Při pharmingu je přesměrována komunikace oběti z původního serveru na server podvodný, opět s cílem vylákat důvěrná data, tedy přihlašovací údaje apod. Nejčastěji je útok realizován napadením serveru DNS a nahrazením IP adresy originálního serveru adresou serveru podvodného. Tato technologie se používá při plošné akci. Alternativou je modifikace souboru lmhost přímo na počítači oběti – což je vhodné pro bodový cílený útok.

5.3.4 OBRANA PROTI SOCIOTECHNICKÝM ÚTOKŮM

5.3.4.1 Klasifikace dat

Podmínkou úspěšné obrany proti jakémukoli útoku je definování možných cílů, stanovení jejich hodnoty pro organizaci a odhad škod, které organizace utrpí, bude-li útok úspěšný. Tato definice umožní cíle kategorizovat podle jejich hodnoty a následně zvolit jejich vhodnou a přiměřenou obranu soustředěnou na skutečné hodnoty. Cílem sociotechnického útoku jsou informace. Mitnick a Simon v (12) rozdělují informace do čtyř kategorií:

- Veřejná – informace volně přístupná i subjektům mimo organizaci
- Vnitřní – informace přístupná pouze zaměstnancům organizace
- Soukromá – informace personální
- Tajná – informace je v rámci organizace poskytována jen osobám s potřebou jejich znalosti

Oproti tomu český zákon zabývající se ochranou utajovaných informací, Zákon 412/2005 Sb. (14), klasifikuje informace výhradně podle ohrožení, jaké by jejich kompromitace měla pro zájmy České republiky jako státu. Dle litery Zákona (14) se informace dělí na:

- Přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,
- Tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,
- Důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,
- Vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.

K tomu lze dodat ještě zákonem nezmiňovanou, leč potřebnou kategorii

- Neutajované informace

Zákonná klasifikace ovšem nic neříká o praktickém významu konkrétní informace pro organizaci. i kompromitace informace s nízkým stupněm utajení může přímo organizaci způsobit značnou újmu. Příkladem může být únik neutajované informace z Policie ČR o tom, že registrační značky služebních vozidel začínají kombinací 1A57. Zákon porušen nebyl, praktické dopady ovšem byly značné. Zákon 412/2005 navíc pod hrozbou sankce zakazuje zařazovat informace do jiného stupně utajení, než informaci přísluší[20].

Vzhledem k tomu, že nakládání s informacemi legislativně upravují i další zákonné normy, například zákon o svobodném přístupu k informacím (15) a zákon na ochranu osobních údajů (16), je pro organizaci vhodné stanovit vlastní klasifikaci informací a způsob nakládání s jednotlivými kategoriemi. Klasifikace musí splňovat tato kritéria:

[20] Paradoxně tedy i do stupně vyššího. Legislativce k tomu vedla snaha zabránit „přeutajování“ a následným vyšším nákladům na ochranu těchto informací

- jednoznačná – nelze dopustit dvojí výklad pravidel
- jednoduchá – omezený počet kategorií, snadná rozeznatelnost, kam má být informace zařazena
- jednotlivé kategorie musí mít jasně definované způsoby nakládání s informací

Na rozdíl od dělení pospaného v (12), postačí pro běžný provoz, při respektování zákonných omezení popsaných výše, tyto kategorie:

5.3.4.1.1 Veřejná informace

Informace této kategorie lze poskytovat a zveřejňovat bez jakéhokoli omezení – sem patří základní informace o organizaci, kontaktní údaje pro veřejnost

5.3.4.1.2 Interní informace

Informace tohoto typu se standardně nezveřejňují, jsou ale k dispozici zaměstnancům organizace bez dalšího omezení. Do této kategorie musí být zařazeny zejména:

- seznamy telefonních čísel a e-mailových adres
- detailní organizační struktura organizace včetně personálního obsazení jednotlivých funkcí
- bezpečnostní politika a její aplikace – systém ostrahy či ochrany objektů, prokazování oprávněnosti ke vstupu, mechanismy zabezpečení informačních a komunikačních systémů
- systém interních norem a předpisů

Způsob poskytování informací kategorie Interní subjektům mimo organizaci musí být upraven vnitřním právním předpisem, který stanoví co, kdy, komu a jak může být poskytnuto. Nejsou-li u konkrétní informace stanovena uvedená pravidla, nezveřejňuje se. Příkladem typů informací, u kterých je vhodné tato pravidla stanovit jsou telefonní čísla přímo dovolatelných linek či internetové e-mailové adresy, jež se poskytují rodinným příslušníkům nebo obchodním partnerům.

Interní informace musí být uloženy a zpracovávány tak, aby byly ochráněny před kompromitací. Nesmí být umístěny na veřejně přístupných místech jako je recepce či návštěvní místnosti a nezveřejňují se na internetových webových stránkách.

5.3.4.1.3 Registrované informace

Představují nejvyšší kategorii informací, které jsou poskytovány jen těm zaměstnancům, kteří je pro svou práci bezpodmínečně potřebuji (již zmíněná zásada need-to-know). Každá entita informace musí mít své jednoznačné označení, být evidovaná a její předání protokolované.

Kopie registrovaných informací se mohou pořizovat výjimečně, pouze na základě interní právní normy. S kopií takovéto informace musí být zacházeno jako s originálem, tedy musí být evidovaná jako další entita informace a o její existenci musí být protokolárně vyrozuměn autor informace.

Pokud je zapotřebí informaci zlikvidovat, je nutné použít zařízení na fyzické ničení nosiče informací[21], je-li informace ve formě datového záznamu, použít vhodný programový prostředek pro neobnovitelné smazání informace. Zničení registrované informace je nutné protokolovat.

Registrované informace je možné přenášet na nosičích vyhrazených k tomuto účelu a pouze po zabezpečených telefonních či datových linkách, v případě telefonního hovoru či faxového přenosu navíc pouze případě, kdy není pochybnosti o identitě příjemce informace.

Registrované informace se subjektům mimo organizaci neposkytují krom případů, kdy tak stanoví zákon. Prozrazení informace této kategorie, ztrátu, neoprávněné zničení jejího nosiče či chybnou manipulaci s ní je nutné postihovat jako hrubé porušení pracovní kázně podle příslušných právních norem. i tyto skutečnosti je nutné protokolovat.

[21] Nosičem informace je myšlen papír, kompaktní disk apod.

Uvedené postupy garantují, že je vždy dohledatelné, kdo se s informací seznámil, kde se její konkrétní exemplář nachází včetně mapy jeho pohybu, eventuálně zda a jak byla zničen.

Vzhledem k vysoké míře diskomfortu při práci s touto kategorií informace a její vysoké administrativní náročnosti je vhodné do této kategorie zahrnovat pouze informace, u kterých je to nezbytně nutné a jejichž kompromitace by způsobila organizaci vážnou újmu. Patří sem například:

- know-how
- podklady pro strategické rozhodování
- osobní údaje a údaje o zdravotním stavu
- kritické bezpečnostní údaje (přístupová hesla a kódy, kryptografické prostředky a klíče)

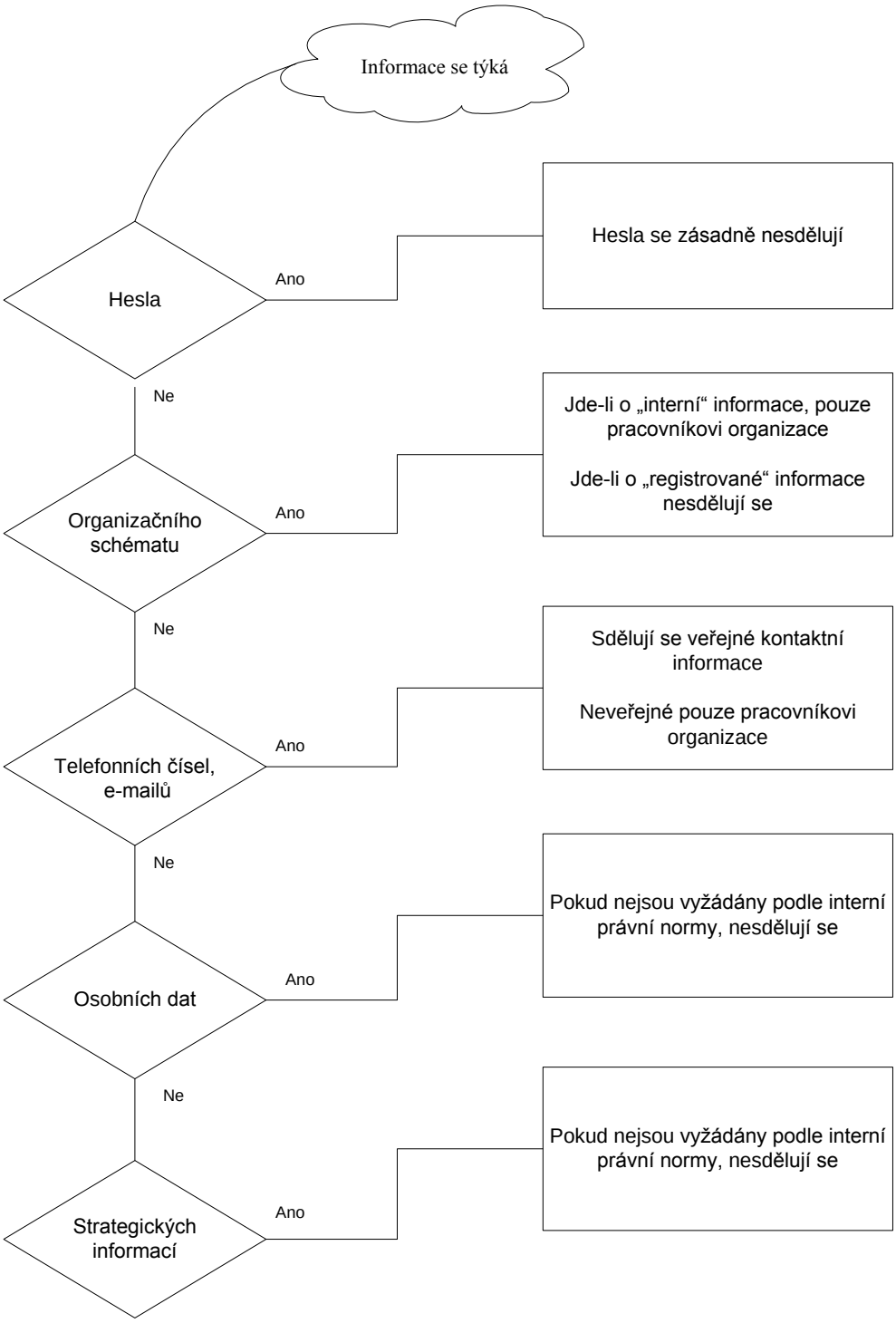
Registrované informace se ukládají v pouze k tomuto účelu zřízených úložištích (trezory, trezorové a serverové místnosti). Fyzický přístup k těmto informacím musí být zaznamenáván (fyzické bezpečnosti se věnuje kapitola 3.1), práce s nimi v informačním systému musí být logována (popsáno v kapitole 6).

5.3.4.1.4 Obecné zásady

Každý nosič informace musí nést označení kategorie informace. Na nosiči mohou být informace kategorie stejné nebo nižší, než pro kterou je nosič určen[22]. Není-li kategorie vyznačena, přepokládá se kategorie Interní informace. Pokud používané informace spadají do kompetence zákona 412/2005 Sb. (14), použije se pro práci s nimi restriktivnější alternativa (neporušuje-li zákon).

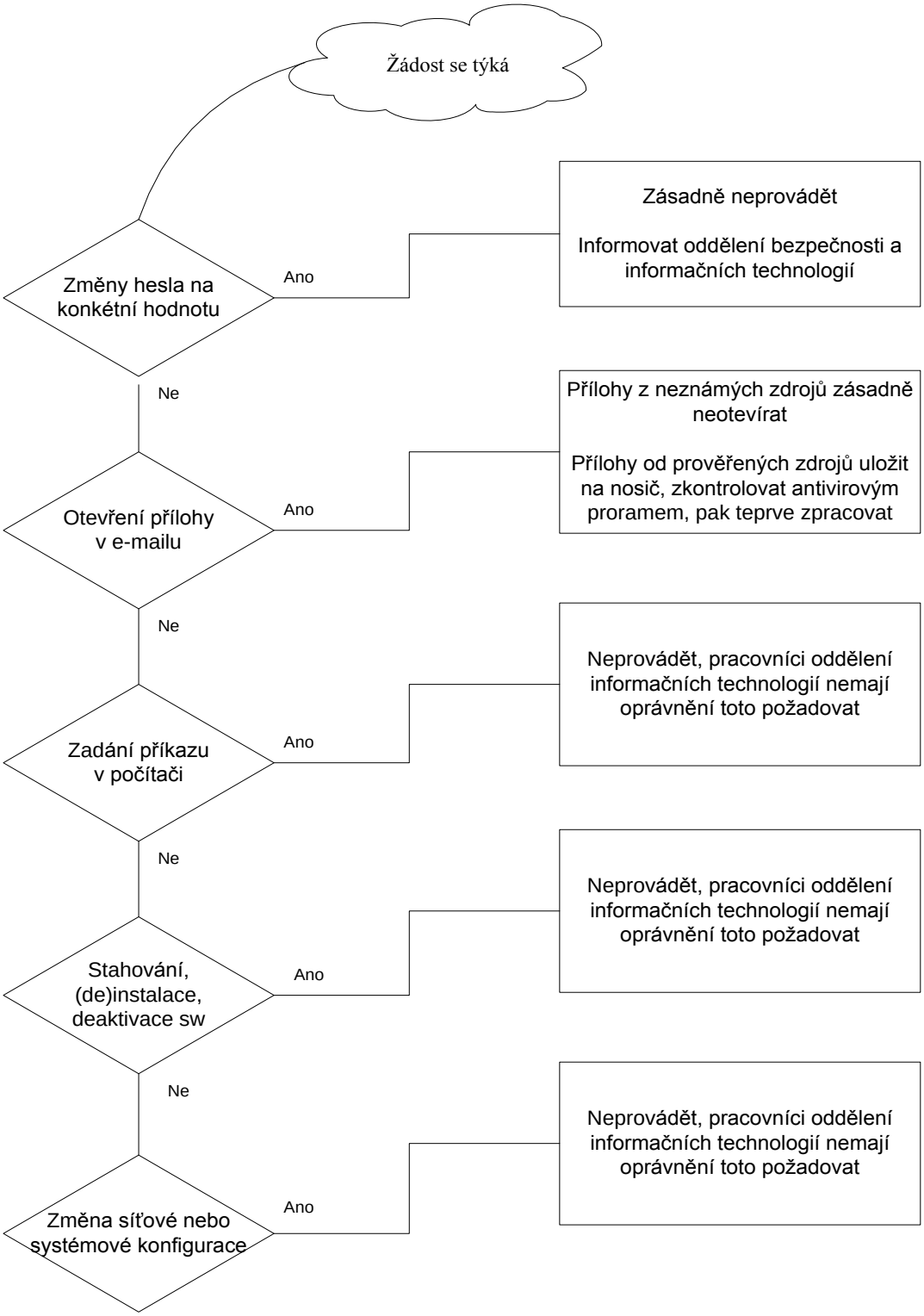
[22] Tedy na CD s označením INTERNÍ mohou být informace interní a veřejné, nikoliv však registrované.

5.3.4.2 Reakce na žádost o informace



.

5.3.4.3 Žádost o provedení činnosti



6 TECHNICKÉ ZABEZPEČENÍ INFORMAČNÍCH SYSTÉMŮ

Představuje komplex technických zařízení, programového vybavení, organizačních metod a postupů, které zaručují integritu a důvěrnost zpracovávaných dat. Je nutné při tom dbát na to, aby zabezpečení informačního systému nesnižovalo (příliš) komfort práce s ním, což by uživatele vedlo k tomu, že budou data zpracovávat mimo zabezpečený systém se všemi riziky z toho vyplývajícími.[23]

6.1 PŘÍSTUPOVÁ PRÁVA A UŽIVATELSKÉ ÚČTY

Jsou základním prvkem, na základě kterého je možné pracovat s uloženými daty. V ideálním případě by rozsah přístupových práv měl pokrývat oprávněné potřeby uživatele.

6.1.1 GESTOR DAT

Data v organizaci jsou členěna a zpracovávána podle problematik k tomu určenými organizačními jednotkami. Odpovědnost za přístup k datům leží tedy na vedoucím organizační jednotky a on je tím, kdo má plná přístupová práva ke svěřeným datům a kdo přístupová práva k nim nastavuje jednotlivým uživatelům. Je gestorem dat. Každý gestor dat musí mít vytvořený speciální účet odlišný od svého standardního, který používá výhradně pro správu dat.

6.1.2 SPRÁVCE INFORMAČNÍHO SYSTÉMU

Úkolem správce informačního systému je udržování systému v chodu, ale nikoli odpovědnost za správu dat. Správce IS musí mít přístup ke konfiguraci systému a síťových prvků, ale k uživatelským datům či datům uložených v databázích mít nesmí. Každý správce IS musí mít vytvořený speciální účet odlišný od svého standardního, který používá výhradně pro správu informačního systému.

[23] Fráze, že nejbezpečnější počítač je vypnutý počítač neplatí, jak píše Mitnick v (12), šikovný sociotechnik dokáže přesvědčit uživatele, aby ho zapnul

6.1.3 BEZPEČNOSTNÍ SPRÁVCE

Úkolem bezpečnostního správce ve vztahu k informačnímu systému je dozor nad dodržováním provozních předpisů a řešení bezpečnostních incidentů. Tomu odpovídají i přístupová práva, kdy bezpečnostní správce potřebuje mít přístup k systémovým a bezpečnostním logům a k informacím o nastavení přístupových práv k jednotlivým objektům a uživatelům IS. Přístup k obsahu dat mít nesmí. Každý bezpečnostní správce musí mít vytvořený speciální účet odlišný od svého standardního, který používá výhradně pro účely bezpečnostní správy.

6.1.4 PRIVILEGOVANÝ ÚČET

Při provozu informačního systému mohou nastat nestandardní stavy, kdy oprávnění výše popsaných speciálních účtů nepostačují k provedení požadovaných informací. Pro tento případ je vytvořen účet se všemi oprávněními, která systém poskytuje[24]. Pro práci s privilegovaným účtem by (vzhledem k jeho oprávněním) měla být vynutitelná účast alespoň dvou osob. To je vynutitelné buď systémem více hesel (Lotus Domino) nebo děleným heslem[25]. Po ukončení zásahu je vhodné hesla změnit. Hesla k privilegovanému účtu by měla být uložena v oddělených zapečetěných obálkách u nejvýše postaveného vedoucího pracovníka organizace. O použití privilegovaného účtu se musí sepsat záznam v kategorii registrovaná informace.

6.2 ZABEZPEČENÍ SERVERŮ

Servery jsou klíčovým prvkem informačního systému. Slouží k autentizaci uživatelů, jsou na nich uložena uživatelská data a provozovány síťové aplikace včetně databází. Kompromitace serveru znamená ohrožení většiny aktivit organizace. Kromě fyzického zabezpečení serveru (řešeno v kapitole 3.1) je nutné server zabezpečit na systémové úrovni – tedy autentizací oprávněného uživatele. K tomu se užívá jméno

[24] V MS-Windows účet Administrator, v unixových systémech uživatel root, Lotus Domino Full Access Administrator.
[25] Dělené heslo – každý oprávněný uživatel zná pouze část hesla. Při jeho zadání se tedy musí sejít příslušný počet osob.

a heslo, optimální je doplnění této dvojice autentizacím předmětem (tokenem, čipovou kartou) nebo biometrickým snímačem (otisk prstu, rozpoznání tváře či rohovky).

6.3 ZABEZPEČENÍ STANIC

Problematika zabezpečení stanic se od serverů mírně odlišuje. Stanice nejsou umístěny ve specializovaných prostorách (serverovnách) s řízeným přístupem. Je tedy vhodné je alespoň neumísťovat do prostor veřejně přístupných. V současnosti je většina stanic vybavena pevným diskem a z toho plyne riziko, že se na tomto disku mohou nacházet citlivá data nebo můžou na něj být instalovány špionážní programy zachytávající hesla nebo informace. Kromě autentizace oprávněného uživatele jménem, heslem, předmětem či biometrií, je nutné ochránit počítač před neoprávněným zapnutím a nahráním operačního systému z neautorizovaného media, což lze učinit vynucením zadání hesla v BIOSu stanice. Reziduální citlivá data na pevném disku by měla být po odhlášení bezpečně mazána včetně stránkovacího souboru nebo by měl být pevný disk chráněný šifrováním svého obsahu v reálném čase. Skříň stanic by měla být zapečetěna či zaplombována, aby byl zřejmý pokus o neautorizované vniknutí a tyto ochranné prvky by měly být uživateli průběžně a bezpečnostním správcem pravidelně kontrolovány.

6.4 ZABEZPEČENÍ EXTERNÍCH DATOVÝCH KOMUNIKACÍ

Pokud je nutné propojit více objektů organizace sítěmi procházejícími veřejným prostorem, musí být tyto spoje chráněné proti neoprávněnému přístupu – odposlechu datové, hlasové či faxové komunikace. Jedinou spolehlivou ochranou je šifrování. Je-li spojení zajištěno pronajatou linkou nebo vlastním soukromým kanálem (mikrovlnný spoj), může se pro zabezpečení tohoto spoje nasadit linkový šifrátor, v případě spojení přes internet je optimálním řešení nasazení technologie VPN[26]. Schéma sítě VPN je v příloze 11.8.

[26] VPN - virtual private network – je technologie umožňující propojit informační systémy skrze nedůvěryhodné prostředí, jako je internet

6.5 ZABEZPEČENÍ ELEKTRONICKÉ POŠTY

Standardy e-mailové komunikace s žádným zabezpečením nepočítají. Elektronickou poštu tak, jak ji většina uživatelů používá, lze přirovnat k pohledu pošty klasické. Komukoli se dostane do rukou, může si ji přečíst. Chceme-li používat e-mail k přenosu informací kategorie Interní či Registrované je nutné použít další zabezpečení. Obdobně jako u externích datových komunikací je jedinou spolehlivou metodou šifrování. Je možné použít buď proprietární systémy jako Lotus Notes nebo použít volně dostupné programy typu OpenPGP, pracující na principu kryptografie s veřejným klíčem, které umožňují šifrovat buď tělo zprávy nebo připojené soubory v běžných e-mailových klientech[27]. Výhodou proprietárních systémů je jejich robustnost, bezpečnost a odolnost vůči lidským chybám, nevýhodou je vyšší cena a nutnost vybavit klienty elektronické pošty všechny účastníky komunikačního řetězce. Výhodou otevřených standardů je globální dostupnost a rozšířenost.

[27] Microsoft Outlook, Mozilla Thunderbird

7 MANAGEMENT A BEZPEČNOSTNÍ POLITIKA ORGANIZACE

7.1 BEZPEČNOSTNÍ POLITIKA ORGANIZACE

Bezpečnostní politika organizace zahrnuje veškeré aktivity vedoucí k ochraně aktiv (tedy i informací) organizace i jejích pracovníků. Je realizována formou definovaných instrukcí v podobě interních právních norem, které určují chování zaměstnanců při ochraně. Úkolem bezpečnostní politiky je ex ante předcházet bezpečnostním incidentům, určit pravidla chování, pokud bezpečnostní incident nastane a následně stanovit postupy při likvidaci následků a vyšetřování příčin incidentu.

Jak píší Marek a Dastych v (17), je výhodné vytvářet bezpečnostní politiky jako více provázaných hierarchických dokumentů, které na své úrovni řeší vždy příslušné oblasti bezpečnosti. Na nejvyšší úrovni se bezpečnostní politika formuluje velmi obecně a vzniká tak dokument, jenž bude platný dlouhou dobu bez nutnosti jakékoli novelizace. Na něj navazují další, oborově orientované politiky, týkající se bezpečnosti oblastí informačních technologií, personální, ekonomické či fyzické bezpečnosti. Na nejnižším žebříčku jsou dokumenty konkrétně popisující ochranu například serverů nebo elektronické pošty. Tato vrstva dokumentů je aktualizovaná poměrně často díky krátkému životnímu cyklu technologií i často překotnému vývoji v oblasti IT.

7.2 ÚLOHA MANAGEMENTU VE FORMULOVÁNÍ A PROSAZOVÁNÍ BEZPEČNOSTNÍ POLITIKY ORGANIZACE

Při formulování bezpečnostní politiky je nutné hledat odpovědi na tři základní otázky.

- Jaká aktiva organizace chránit
- Jaká potenciální rizika těmto aktivům hrozí
- Pokud k předpokládaným útokům dojde, jaké škody hrozí

- Jak aktiva zabezpečit
- Jaké náklady si vyžádá zabezpečení jednotlivých aktiv

Zodpovězení těchto základních otázek ukáže, která aktiva je nutno chránit a zda budou navržená ochranná opatření rentabilní, zohlední-li se náklady na ochranu s výnosy a ztrátami aktiv.

Nutnou podmínkou úspěšné aplikace bezpečnostních politik je jejich bezvýhradná podpora pracovníky nejvyšších stupňů vedení organizace. Vedení musí dát jednoznačně a zřetelně najevo svou angažovanost a v dodržování stanovených pravidel jít demonstrativně příkladem. Jak říkají Mitnick se Simonem v (12), pracovníci si musejí být vědomi, že vedení vykazuje silnou víru, že bezpečnost informací je pro fungování firmy nezbytná, že ochrana obchodních informací je nutná pro udržení pozice na trhu a že úspěch programu závisí na individuálním postoji každého zaměstnance.

7.3 BUDOVÁNÍ BEZPEČNOSTNÍ KULTURY ORGANIZACE

Bezpečnostní kultura tvoří nadstavbu bezpečnostních politik. Na rozdíl od nich ji nelze popsat jazykem právních norem. Rozvinutost bezpečnostní kultury určuje to, jak jednotliví zaměstnanci organizace, nejvyšším vedením počínaje a řadovými pracovníky konče mají, jak píše Edwards v (18), vštípeny bezpečnostní návyky a zda se s nimi ztotožnili.

Edukativní činnost organizace se musí zaměřit i na jednotlivé bezpečnostní politiky a při školení zaměstnanců jim nejen odpřednášet obsah interních předpisů, ale zasadit ho širokého kontextu a vysvětlit i důvody, které tvůrce přepisů vedly k jejich konkrétní formulaci. Součástí školení musí být i vytvoření povědomí každého zaměstnance o tom, že se mohou stát terčem manipulativního jednání útočníků a osvětlit jim metody, které útočníci mohou použít. S těmito znalostmi se zvyšuje šance, že případný útok zaměstnanci rozeznají a ubrání se mu. Je také nutné zaměstnancům vysvětlovat, jaká aktiva je třeba chránit a proč, ale také pojmenovat důsledky, jaké by pro organizaci, ale i pro ně samotné mělo, pokud by tato aktiva byla

napadena. Je nutné školení pravidelně opakovat a při té příležitosti zaměstnance informovat o novinkách v bezpečnostní oblasti a otevřeně referovat i o případných bezpečnostních incidentech a jejich důsledcích.

Dobrý školitel musí apelovat na zaměstnance, aby potlačili přirozenou zvídavost a dobrovolně vyžadovali pouze ty informace, které pro svou práci potřebují. V textu několikrát zmiňovaná zásada need-to-know nepatří do rejstříku „tajných“ služeb, ale je nedílnou součástí zdravé bezpečnostní kultury. Přijetí či nepřijetí zásad bezpečnostní kultury dokumentuje situace, kdy jeden pracovník v přítomnosti druhého zadává přihlašovací heslo do systému. Pokud druhý pracovník automaticky odvrátí pohled od klávesnice, a ten, jenž zadává heslo, se tomu nepodivuje, je zřejmé, že se oba pohybují v prostředí s vysokou bezpečnostní kulturou.

8 MOTIVACE UŽIVATELŮ A SPRÁVCŮ IS

Po zformování bezpečnostní politiky organizace je nutné vhodným způsobem přesvědčit zaměstnance k tomu, aby přijatá pravidla respektovali. Jednou z cest jsou kvalitní a opakovaná školení v bezpečnostních problematikách. Dále je nutné zaměstnance pozitivně i negativně motivovat k žádoucímu chování.

8.1 MOTIVACE UŽIVATELE

Běžný uživatel má práva v informačním systému sice omezená, ale tento fakt nikterak nesnižuje hodnotu informací, se kterými pracuje. Před nerespektováním pravidel stanovených interními předpisy neodradí uživatele ani tak výše sankcí jako jejich neodvratitelnost. Dodržování bezpečnostních předpisů by mělo být považováno za standardní součást pracovní disciplíny a nemělo by být zvláště odměňováno.

Odměněno by mělo být takové chování, které vedlo k rozpoznání a nahlášení nebo přímo k odvrácení technologického či sociotechnického útoku na organizaci. Na druhé straně ale pravidla musí vyloučit stav, kdy se budou uživatelé vzájemně udávat. Postačí, bude-li bezpečnostní politika takovéto jednání označit za stav, kdy uživatel mohl přímo odvrátit nebezpečí (upozorněním chybujícího či vlastním zásahem), ale on toto jednání neodvrátil. Zmíněné pravidlo a jeho důsledné dodržování zvyšuje kulturu nejen bezpečnostní.

Sankcionováno by mělo být jednání, které interní předpisy porušuje. Systém trestů by měl být dán předem a musí odrážet nebezpečnost jednání uživatele. Je nutné odlišovat náhodné a ojedinělé opomenutí, kdy postačí zaměstnanci jeho chování vytknout bez záznamu v jeho personálních materiálech od jednání, které vede k přímému a eventuálně i úmyslnému ohrožení aktiv organizace.

Případy, kdy dojde k selhání pracovníka a jeho potrestání, ale i případy opačné, kdy se podařilo odvrátit útok na organizaci, by měly být se zveřejnitelnými detaily publikovány v rámci organizace.

8.2 MOTIVACE SPRÁVCE IS

Pro správce informačních systémů platí vše, co bylo řečeno o motivaci uživatele. Správcům IS musí být vedením organizace zdůrazňováno, že jejich primární úlohou je starost o chod a rozvoj systémů, ale data samotná jsou jim zapovězena. Vzhledem k tomu, že správci IS disponují v rámci organizace unikátními znalostmi, je pro vedení těžké vyhodnotit kvalitu odváděné práce ve všech jejích aspektech. Možným řešením je pravidelně pořádaná anketa mezi uživateli IS zaměřená na spokojenost s fungováním IS.

8.3 MOTIVACE BEZPEČNOSTNÍHO SPRÁVCE

V organizaci s vyspělou bezpečnostní kulturou představuje bezpečnostní správce uznávanou autoritu v oblasti bezpečnosti, na kterou je možné se kdykoli obrátit s konzultací a žádostí o radu v dané problematice, nikoli člověka, který čeká na chybu druhého, aby ji mohl zneužít ve prospěch své kariéry. Platí zde se zvýšenou měrou, co bylo řečeno u běžného uživatele, tedy je nutné odlišovat náhodné a ojedinělé opomenutí, kdy postačí zaměstnanci jeho chování vytknout bez záznamu v jeho personálních materiálech od jednání, které vede k přímému a eventuálně i úmyslnému ohrožení aktiv organizace.

9 ZÁVĚR

Cílem práce bylo identifikovat a definovat aktivity ohrožující informační a komunikační systémy, popsat a analyzovat druhy průniků do těchto systémů a navrhnout možnosti obrany proti popsaným útokům.

Byly popsány tři základní oblasti, na které útoky mohou směřovat – samotné stroje, zařízení a objekty dislokace, funkční technologie (databáze, operační a bezpečnostní systémy) a člověk, jako nositel klíčových informací nutných pro přístup do informačních systémů

Podařilo se charakterizovat základní kategorie útočníků (hackerská komunita, nespokojení zaměstnanci, zločinci a teroristé) a popsat základní motivy jejich jednání.

Charakterizovány byly základní typy útoků (technologický, sociotechnický) a zevrubně byly navrhnuty metody proti těmto útokům.

Ze shromážděných poznatků bylo možno zodpovědět otázku, zda s rostoucí úrovní technické ochrany vliv lidské bytosti na bezpečnost informačních systémů klesá. Odpověď na ni je jednoznačně záporná. Člověk se svými dobrými i špatnými povahovými vlastnostmi zůstává nejslabším článkem i nejsofistikovanějších bezpečnostních opatření, otevřený psychické manipulaci.

Sumarizované znalosti v této práci umožnily naplnit i sekundární cíl, jímž bylo formulovat interní právní normu pro ochranu před sociotechnickými útoky, a kategorizovat data organizace dle citlivosti. Uvedené návrhy norem jsou uvedeny v přílohách této práce.

10 SEZNAM LITERATURY

1. **MAJEROVÁ, V. a MAJER, M.** *Empirický výzkum v sociologii venkova a zemědělství, část II.* Praha : Česká zemědělská univerzita, 2007. str. 274. ISBN: 978-80-213-1671-3. s. 180.

2. *Zákon č. 40/1964 Sb., Občanský zákoník.*

3. **JÍROVSKÝ, V.** *Kybernetická kriminalita.* Praha : Grada, 2007. str. 288. ISBN: 978-80-247-1561-2.

4. **HARRIS, S., HARPER, A. a EAGLE, CH.** *Manuál hackera.* [překl.] T. Znamenáček. Praha : Grada, 2008. str. 400. ISBN: 978-80-247-1346-5. s. 29.

5. **MCCLURE, S., SCAMBRAY, J. a KURTZ, G.** *Hacking bez záhad. 5. vydání. Praha: Grada 2007. 520s.* [překl.] T. Znamenáček. Praha : Grada, 2007. str. 520. ISBN: 978-80-247-1502-5.

6. Slovníkové útoky a útok silou. *Power to serve...* [Online] 9. 11. 2007. [Citace: 21. 2. 2009.] http://www.dusatko.org/node/63.

7. Národní bezpečnostní úřad. [Online] 24. 10. 2008. [Citace: 17. 11. 2008.] http://www.nbu.cz.

8. **MAZEL, M.** Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a Internetu včetně návrhu řešení. *Ministerstvo vnitra ČR.* [Online] 25. 8. 2006. [Citace: 21. 2. 2009.] http://web.mvcr.cz/archiv2008/dokument/2006/informacni.doc. s. 3-5.

9. Personalis 2006 - ICT Forum. *ICT Forum.* [Online] 27. 9. 2006. [Citace: 12. 1. 2009.] http://www.personalis.cz/filemanager/files/file.php?file=3990.

10. **FOLTIN, P. a ŘEHÁK, D.** Důvody realizace a formy terorismu. *Obrana a strategie.* [Online] 11. 7. 2005. [Citace: 10. 2. 2009.] http//:www.defenceandstrategy.eu/filemanager/files/file.php?file=6291. ISSN: 1802-7199. s. 35-36.

11. Dynamic Graphs of Code Red worm. *CAIDA.* [Online] 2. 8. 2001. [Citace: 27. 12. 2008.] http://www.caida.org/dynamic/analysis/security/code-red/index.html.

12. **MITNICK, K. a SIMON, W.** *Umění klamu.* [překl.] L. VAŠATA. Praha : Helion S.A., 2003. str. 348. ISBN: 83-7361-210-6.

13. **ŠUP, L.** Podpora uživatelů - OIKT. *OIKT.* [Online] 27. 2. 2009. [Citace: 28. 2. 2009.] http://www.oikt.czu.cz/?dl=1&f=7078.

14. *Zákon č. 412/2005 Sb., O ochraně utajovaných informací a o bezpečnostní způsobilosti.*

15. *Zákon 106/199 Sb., O svobodném přístupu k informacím .*

16. *Zákon č. 101/2000 Sb., O ochraně osobních údajů.*

17. **MAREK, R. a DASTYCH, J.** Bezpečnostní politika v organizaci. *SystemOnLine.* [Online] 1.. 4. 2003. [Citace: 22. 1. 2009.] http://www.systemonline.cz/clanky/bezpecnostni-politika-v-organizaci.htm. ISSN 1802-615X.

18. How to Build a Culture of Security. *ITsecurity.* [Online] 16. 6. 2007. [Citace: 21. 2 2009.] http://www.itsecurity.com/features/culture-of-security-071607/.

19. eMAG. *eMag.cz, technologický magazín.* [Online] 27. 1. 2009. [Citace: 28. 1. 2009.] http://www.emag.cz/novozelandan-objevil-v-mp3-prehravaci-tajne-udaje-o-americke-armade/. ISSN: 1802-4238.

20. Jak zjistit heslo na Seznam E-mail. *La Trine.* [Online] 25. 9. 2005. [Citace: 15. 12. 2008.] http://latrine.dgx.cz/jak-zjistit-heslo-na-seznam-e-mail.

21. *Connect!* Brno : Computer Press, 2004 - . ISSN: 1211-3985.

22. *Vyhláška č. 523/2005 Sb., O bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.*

23. *Hackin9: IT Security Magazine.* Varšava : Software-Wydawnictvo, 2005 - 2008. ISSN 1214-7710.

24. Úřad pro ochranu osobních údajů. [Online] 02. 11. 2008. [Citace: 17. 11. 2008.] http://www.uoou.cz.

25. **STAUDEK, J. a HANÁČEK, P.** Bezpečnost informačních systémů. *Archiv stránek bývalého ministerstva informatiky.* [Online] 28. 2. 2002. [Citace: 17. 11. 2008.] http://aplikace.mvcr.cz/archiv2008/micr/files/479/uvis_bezpecnost_20000701.pdf.

26. **Winkler, I. S.** CASE STUDY OF INDUSTRIAL ESPIONAGE THROUGH. *The Computer Security Division.* [Online] 26. 9. 1996. [Citace: 12. 2. 2008.] http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper040/WINKLER.PDF.

27. **WENSTROM, M.** *Zabezpečení sítí Cisco.* [překl.] D. Krásenský. Brno : Computer Press, 2003. str. 784. ISBN: 80-7226-952-6. s. 36.

11 PŘÍLOHY

11.1 POKYN BEZPEČNOSTNÍHO ŘEDITELE K OCHRANĚ PROTI SOCIOTECHNICKÝM ÚTOKŮM

Směrnice bezpečnostního ředitele organizace
o ochraně proti sociotechnickým útokům.

Preambule

Hlavním důvodem vydání této směrnice je omezit na minimum riziko úspěšně provedeného sociotechnického útoku zaměřeného na získání dat z informačního systému nebo přístupu do něho. Hlavním znakem sociotechnického útoku je skutečnost, že útočník předstírá identitu osoby vlastnící požadovaná oprávnění nebo se snaží psychologickou manipulací přimět zaměstnance k provedení nepovolených činností.

Čl. 1

Úvodní ustanovení

1) Tato směrnice upravuje povinnosti zaměstnance organizace při práci s informačním systémem.
2) Tato směrnice je doplňkem Směrnice ředitele organizace Bezpečnostní politika organizace číslo 101/2005.
3) Tato směrnice je závazná pro všechny zaměstnance organizace. Její porušení je klasifikováno jako závažné porušení pracovní kázně podle Zákoníku práce.

Čl. 2

Základní pojmy

4) Uživatel – zaměstnanec organizace, který má zřízen účet v informačním systému a je oprávněn s tímto systémem pracovat
5) Správce IS – zaměstnanec oddělení komunikačních a informačních systémů (dále jen OKIS), který má oprávnění ke správě KIS
6) Bezpečnostní správce – zaměstnanec oddělení bezpečnostního ředitele (dále jen OBŘ, který odpovídá za bezpečnostní režim KIS
7) Gestor informací – vedoucí odboru nebo samostatného oddělení, který je odpovědný za data své organizační jednotky uložená v informačním systému
8) Sociotechnický útok – jednání, mající za cíl zmanipulovat napadenou osobu k provedení činností, jejichž výsledkem je neoprávněný prospěch
9) Útočník – osoba nebo skupina osob provádějící sociotechnický útok
10) Hodnověrná osoba – osoba, u které je zaměstnanci bez jakýchkoli pochybností známa její identita a pracovní zařazení
11) Ověřená osoba – osoba, u které je zaměstnanci nadřízeným pracovníkem nebo bezpečnostním ředitelem potvrzena její identita a pracovní zařazení
12) Neověřená osoba – osoba, u které není zaměstnanci známa její identita a pracovní zařazení nebo nebylo možné tyto údaje ověřit
13) Úkon – poskytnutí informace nebo provedení činnosti
14) Žadatel – osoba žádající o provedení úkonu

Čl. 3

Ověřování totožnosti

1) U hodnověrné osoby není zapotřebí totožnost ověřovat
2) U ověřené osoby je povinnost ověřovat její pracovní zařazení při každé žádosti o úkon, identita se ověřuje v případě pochyb
3) U neověřené osoby se identita a pracovní zařazení ověřuje vždy

Čl. 4

Vyhovění žádosti o úkon

1) Žádosti o úkon lze vyhovět, je-li žádající osoba hodnověrná a povaha úkonu odpovídá jejímu pracovnímu zařazení a uživatel nemá žádné pochyby
2) U osoby ověřené je nutné před vyhověním žádosti o úkon ověřit její pracovní zařazení. Je-li toto ověření kladné a uživatel nemá žádné pochyby, úkon se provede
3) U neověřené osoby je nutné ověřit její identitu a pracovní zařazení. Je-li toto ověření kladné a uživatel nemá žádné pochyby, úkon se provede
4) V ostatních případech se žádosti o úkon nevyhoví. Jsou-li požadovány úkony týkající se informací kategorie Registrované, o zamítnutí úkonu se vyhotoví záznam do formuláře ZOOÚ-1, vzor v příloze a odešle se bezpečnostnímu řediteli

Čl. 5

Závěrečná a přechodná ustanovení

1) Tato směrnice nabývá účinnosti dnem 1. dubna 2009

Příloha – formulář ZOOÚ-1

ZOOÚ-1 Záznam o odmítnutí úkonu kategorie REGISTROVANÉ	
EČI.:	V Praze, dne:_____
Úkon:	
Uživatel:	Žadatel:

11.2 SMĚRNICE BEZPEČNOSTNÍHO ŘEDITELE O KLASIFIKACI INFORMACÍ

Směrnice bezpečnostního ředitele organizace o klasifikaci informací

Preambule

Hlavním důvodem vydání této směrnice je vymezit kategorie informací podle následků, jaké by mělo jejich neoprávněné zveřejnění či zničení. Tato kategorizace umožní snížit náklady na ochranu informací tím, že pozornost bude soustředěna na omezenou kategorii nejcennějších informací.

Čl. 1

Úvodní ustanovení

2) Tato směrnice upravuje povinnosti zaměstnance organizace při práci informacemi.
3) Tato směrnice je doplňkem Směrnice ředitele organizace Bezpečnostní politika organizace číslo 101/2005.
4) Tato směrnice je závazná pro všechny zaměstnance organizace. Její porušení je klasifikováno jako závažné porušení pracovní kázně podle Zákoníku práce.

Čl. 2

Základní pojmy

1) Uživatel – zaměstnanec organizace, který má zřízen účet v informačním systému a je oprávněn s tímto systémem pracovat.

2) Správce IS – zaměstnanec oddělení komunikačních a informačních systémů (dále jen OKIS), který má oprávnění ke správě KIS.
3) Bezpečnostní správce – zaměstnanec oddělení bezpečnostního ředitele (dále jen OBŘ, který odpovídá za bezpečnostní režim KIS.
4) Gestor informací – vedoucí odboru nebo samostatného oddělení, který je odpovědný za data své organizační jednotky uložená v informačním systému.
5) Úkon – poskytnutí informace nebo provedení činnosti.
6) Žadatel – osoba žádající o provedení úkonu.
7) Informace – uspořádaná množina dat, má nehmotnou podobu, vždy je uložena na nosiči.
8) Entita informace – informace se může vyskytovat ve více než jednom vyhotovení, každé jednotlivé vyhotovení představuje entita.
9) Nosič – medium, na kterém je informace uložena (například papír, pevný disk, kompaktní disk).
10) Úložiště – prostor pro ukládání nosičů s informacemi.
11) EČREI – evidenční číslo registrované entity informace.

Čl. 3

Kategorie informací

1) Jsou stanoveny tři kategorie informací – VEŘEJNÉ, INTERNÍ, REGISTROVANÉ.
2) Kategorie VEŘEJNÉ: Informace této kategorie lze poskytovat a zveřejňovat bez jakéhokoli omezení – sem patří základní informace o organizaci, kontaktní údaje pro veřejnost.
3) Kategorie INTERNÍ: Informace této kategorie se standardně nezveřejňují. Zaměstnancům organizace jsou k dispozici bez dalšího omezení. Poskytnutí těchto informací subjektům mimo organizaci je možné pouze na základě vnitřních směrnic, jednorázového nebo dlouhodobého povolení gestora informací. Interní informace musí být uloženy a zpracovávány tak, aby byly ochráněny před kompromitací. Nesmí být umístěny na veřejně přístupných

místech jako je recepce či návštěvní místnosti a nezveřejňují se na internetových webových stránkách. Do této kategorie jsou zařazeny zejména:

- seznamy telefonních čísel a e-mailových adres
- detailní organizační struktura organizace včetně personálního obsazení jednotlivých funkcí
- bezpečnostní politika a její aplikace – systém ostrahy či ochrany objektů, prokazování oprávněnosti ke vstupu, mechanismy zabezpečení informačních a komunikačních systémů
- systém interních norem a předpisů
- Interní informace musí být uloženy a zpracovávány tak, aby byly ochráněny před kompromitací. Nesmí být umístěny na veřejně přístupných místech jako je recepce či návštěvní místnosti a nezveřejňují se na internetových webových stránkách

4) Kategorie REGISTROVANÉ: Do této kategorie patří informace, jejichž kompromitace by způsobila organizaci vážnou újmu. Způsoby manipulace a ukládání registrovaných informací upravuje článek 5 této směrnice. Do této kategorie patří:
   - technologické know-how
   - podklady pro strategické rozhodování vedení
   - informace o vztazích s partnerskými organizacemi
   - osobní údaje a údaje o zdravotním stavu
   - kritické bezpečnostní údaje (přístupová hesla a kódy, kryptografické prostředky a klíče)

Č4.

Evidenční číslo registrované informace

1) Evidenční číslo registrované informace slouží k jednoznačné identifikaci entity informace po celou dobu její existence.
2) Při označení informace se uvádí kódem EČRI.

3) Evidence je vedena v Protokolu informací.
4) Každá organizační jednotka vede vlastní protokol.
5) Informacím, vedených v informačním systému přiděluje EČRI systém automaticky, jejich evidence je soustředěna na OKIS.
6) Pokud je informace, vedená v informačním systému, převedena na nosič mimo IS (vytištěna, kopírována na CD) je zaevidována s novým EČRI na příslušné OJ.
7) Tvar EČRI Rxxx/rok – OJ – n/m
   - xxx – označuje pořadové číslo informace za kalendářní rok
   - rok - rok, kdy byla informace zaevidována
   - OJ – organizační jednotka, která informaci zaevidovala
   - n – pořadové číslo entity dané informace
   - m – počet entit dané informace

     Příklad – R007/2009-OKIS-2/3 označuje druhou entitu ze tří informace vzniklé na OKIS v roce 2009 a zaevidované pod pořadovým číslem sedm.

Čl. 5

Manipulace s informacemi kategorie REGISTROVANÉ

1) Registrované informace se ukládají v úložištích k tomuto účelu zřízených.
2) Fyzický přístup k těmto úložištím musí být zaznamenáván.
3) Práce s registrovanými informacemi v informačním systému musí být logována.
4) Předání registrované informace musí být protokolované v Předávací knize, předání registrované informace v IS je evidováno v rámci IS.
5) Kopie registrovaných informací se mohou pořizovat výjimečně, pouze na základě interní právní normy. S kopií takovéto informace musí být zacházeno jako s originálem, tedy musí být evidovaná jako další entita informace a o její existenci musí být protokolárně vyrozuměn autor informace.
6) Pokud je zapotřebí informaci zlikvidovat, je nutné použít zařízení na fyzické ničení nosiče informací, je-li informace ve formě datového záznamu, použít

vhodný programový prostředek pro neobnovitelné smazání informace. Zničení registrované informace je nutné zaznamenat v Protokolu informací.

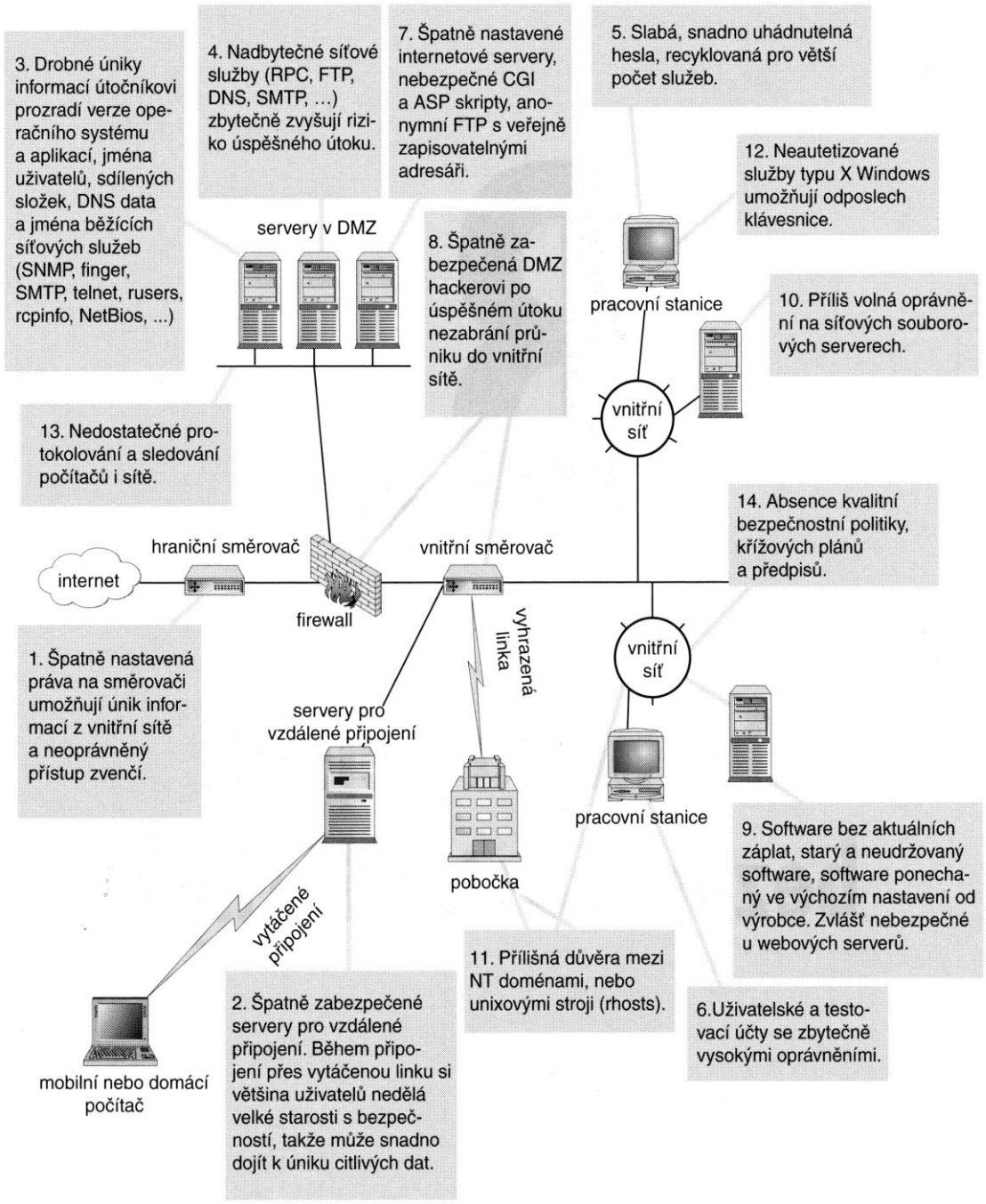
7) Registrované informace je možné přenášet na nosičích vyhrazených k tomuto účelu a pouze po zabezpečených telefonních či datových linkách, v případě telefonního hovoru či faxového přenosu navíc pouze případě, kdy není pochybnosti o identitě příjemce informace a o jeho oprávnění registrovanou informaci přijmout.
8) Registrované informace se subjektům mimo organizaci neposkytují krom případů, kdy tak stanoví zákon.
9) Prozrazení informace této kategorie, ztrátu, neoprávněné zničení jejího nosiče či chybnou manipulaci s ní je nutné postihovat jako hrubé porušení pracovní kázně podle příslušných právních norem. I tyto skutečnosti se evidují v Protokolu informací.

Čl. 5

Závěrečná a přechodná ustanovení

1) Tato směrnice nabývá účinnosti dnem 1. dubna 2009

11.3 14 ČASTÝCH BEZPEČNOSTNÍCH CHYB



Obrázek č – citováno v (5)

11.4 SEZNAM NEJČASTĚJI POUŽÍVANÝCH PORTŮ

Služba/aplikace	Port/protokol
echo	7/tcp
systat	11/tcp
chargen	19/tcp
ftp-data	21/tcp
ssh	22/tcp
telnet	23/tcp
smtp	25/tcp
nameserver	42/tcp
whois	43/tcp
tacacs	49/udp
xns-time	52/tcp
xns-time	52/udp
dns-lookup	53/udp
dns-zone	53/tcp
whois++	63/tcp/udp
oracle-sqlnet	66/tcp
bootps	67/tcp/udp
bootpc	68/tcp/udp
tftp	69/udp
gopher	70/tcp/udp
finger	79/tcp
http	80/tcp
náhradní port webového serveru	81/tcp
kerberos nebo náhradní port webového serveru	88/tcp
pop2	109/tcp
pop3	110/tcp
sunrpc	111/tcp
sqlserv	118/tcp
nntp	119/tcp
ntp	123/tcp/udp
ntrpc-or-dce (epmap)	135/tcp/udp
netbios-ns	137/tcp/udp
netbios-dgm	138/tcp/udp
netbios	139/tcp
imap	143/tcp
snmp	161/udp
snmp-trap	162/udp
xdmcp	177/tcp/udp
bgp	179/tcp
snmp-checkpoint	256/tcp
snmp-checkpoint	257/tcp
snmp-checkpoint	258/tcp
snmp-checkpoint	259/tcp
ldap	389/tcp
netware-ip	396/tcp
timbuktu	407/tcp
https/ssl	443/tcp
ms-smb-alternate	445/tcp/udp
ipsec-internet-key-exchange (ike)	500/udp

Služba/aplikace	Port/protokol
exec	512/tcp
rlogin	513/tcp
rwho	513/udp
rshell	514/tcp
syslog	514/udp
printer	515/tcp
printer	515/udp
talk	517/tcp/udp
ntalk	518/tcp/udp
route/rip/ripv2	520/udp
netware-ncp	524/tcp
irc-serv	529/tcp/udp
uucp	540/tcp/udp
klogin	543/tcp/udp
mount	645/udp
remotelypossible	799/tcp
rsync	873/tcp
samba-swat	901/tcp
w2k rpc služby	1024–1030/tcp/udp
socks	1080/tcp
kpop	1109/tcp
bmc-patrol-db	1313/tcp
notes	1352/tcp
timbuktu-srv1	1417–1420/tcp/udp
ms-sql	1433/tcp
citrix	1494/tcp
sybase-sql-anywhere	1498/tcp
funkproxy	1505/tcp/udp
ingres-lock	1524/tcp
oracle-srv	1525/tcp
oracle-tli	1527/tcp
pptp	1723/tcp
winsock-proxy	1745/tcp
radius	1812/udp
remotely-anywhere	2000/tcp
cisco-mgmt	2001/tcp
nfs	2049/tcp
compaq-web	2301/tcp
sybase	2368/tcp
openview	2447/tcp
realsecure	2998/tcp
nessusd	3001/tcp
ccmail	3264/tcp/udp
ms-active-dir-global-catalog	3268/tcp/udp
bmc-patrol-agent	3300/tcp
mysql	3306/tcp
ssql	3351/tcp
ms-termserv	3389/tcp
cisco-mgmt	4001/tcp

Služba/aplikace	Port/protokol
nfs-lockd	4045/tcp
rwhois	4321/tcp/udp
postgress	5432/tcp
secured	5500/udp
pcanywhere	5631/tcp
vnc	5800/tcp
vnc-java	5900/tcp
xwindow	6000/tcp
cisco-mgmt	6001/tcp
arcserve	6050/tcp
apc	6549/tcp
irc	6667/tcp
font-service	7100/tcp/udp
web	8000/tcp
web	8001/tcp
web	8002/tcp
web	8080/tcp
blackice-icecap	8081/tcp
cisco-xremote	9001/tcp
jetdirect	9100/tcp
dragon-ids	9111/tcp
iss system scanner agent	9991/tcp
iss system scanner konzole	9992/tcp
stel	10005/tcp
netbus	12345/tcp
snmp-checkpoint	18210/tcp
snmp-checkpoint	18211/tcp
snmp-checkpoint	18186/tcp
snmp-checkpoint	18190/tcp
snmp-checkpoint	18191/tcp
snmp-checkpoint	18192/tcp
trinoo_bcast	27444/tcp
trinoo_master	27665/tcp
quake	27960/udp
backorifice	31337/udp
rpc-solaris	32771/tcp
snmp-solaris	32780/udp
reachout	43188/tcp
bo2k	54320/tcp
bo2k	54321/udp
netprowler-manager	61440/tcp
pcanywhere-def	65301/tcp

Tabulka číslo – citováno z (5)

Celkový počet portů přesahuje číslo sto třicet tisíc (2x 65 535 portů pro TCP a UDP protokoly). Redukovaný seznam s běžně používanými aplikacemi a jejich porty zachycuje tabulka číslo

11.5 VÝPIS INFORMACÍ Z WWW.RIP.NET

```
% This is the RIPE Whois query server #1.
% The objects are in RPSL format.
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html
% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.
% Information related to '194.79.52.0 - 194.79.55.255'
inetnum:        194.79.52.0 - 194.79.55.255
netname:        MAFRA-CZ
descr:          MAFRA, a.s.
country:        CZ
org:            ORG-MA149-RIPE
admin-c:        JC607-RIPE
tech-c:         JC607-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-HM-PI-MNT
mnt-by:         MAFRA-MNT
mnt-lower:      RIPE-NCC-HM-PI-MNT
mnt-routes:     MAFRA-MNT
mnt-domains:    MAFRA-MNT
source:         RIPE # Filtered
organisation:   ORG-MA149-RIPE
org-name:       MAFRA
org-type:       OTHER
address:        Karla Englise 519/11
address:        Praha 5
address:        150 00
address:        Czech Republic
phone:          +420 2 22062600
fax-no:         +420 2 22062616
e-mail:         Jaroslav.Cerveny@mafra.cz
admin-c:        JC607-RIPE
mnt-ref:        MAFRA-MNT
mnt-by:         MAFRA-MNT
source:         RIPE # Filtered
person:         Jaroslav Cerveny
address:        MAFRA, a. s.
address:        Karla Englise 519/11
address:        Prague 5
address:        150 00
address:        Czech Republic
phone:          +420 225062600
fax-no:         +420 225066000
e-mail:         jaroslav.cerveny@mafra.cz
nic-hdl:        JC607-RIPE
source:         RIPE # Filtered
% Information related to '194.79.52.0/22AS38952'
route:          194.79.52.0/22
descr:          MAFRA
origin:         AS38952
mnt-by:         MAFRA-MNT
source:         RIPE # Filtered
```

11.6 PŘÍKLAD ÚNIKU DAT

Novozélanďan objevil v MP3 přehrávači tajné údaje o americké armádě

Novozélanďan Chis Ogle objevil v MP3 přehrávači, který si zakoupil v charitativní akci, soubory s citlivými údaji o amerických vojácích. Některé z nich dokonce obsahovaly upozornění, že zveřejnění jejich obsahu zakazují americké federální zákony, informuje v úterý televize TV One News.

Devětadvacetiletý Ogle vypověděl, že přehrávač zakoupil za 18 dolarů v americké Oklahomě a jeho obsah zjistil poté, co MP3 připojil ke svému počítači. Soubory na přehrávači obsahovaly mimo jiné jména a stále aktuální telefonní čísla velkého počtu vojáků, z nichž několik sloužilo v Afghánistánu nebo v Iráku. Na MP3 byly uloženy dokonce detailní informace o některých amerických základnách v Afghánistánu.

Novozélanďan v přehrávači objevil také čísla sociálních pojistek či záznamy o těhotných ženách v armádě.

Americké velvyslanectví na Novém Zélandu se k případu odmítlo vyjádřit.

Podobný únik informací byl zaznamenán v roce 2006 v Afghánistánu, když američtí vyšetřovatelé nakupovali v obchodech zpět USB klíče, které z vojenské základny Bagrám ukradli místní zaměstnanci. Klíče obsahovaly utajované vojenské informace včetně map či zpráv tajných služeb s podrobnostmi o akcích islamistického hnutí Taliban a teroristické sítě Al-Káida.

Citováno z (17)

11.7 PRAKTICKÝ PŘÍKLAD PHISHINGU

Uveřejněno v (18)

Text e-mailu

Jak zjistit heslo na Seznam E-mail

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 e-mail), ten jej vyhodnotí a pošle zpět odpověď. Administrátoři Seznamu to používají při práci „v terénu". Teď prozradím přesný tvar e-mailu, kterým lze získat heslo k jakékoliv schránce na Seznam E-mail.

E-mail 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 e-mail* `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 e-mail s heslem ke schránce.*

Doplněno o pár hodin později:

Asi bych měl nejprve vysvětlit záměrný dvojsmysl v prvním odstavci. Neuvažoval jsem nad tím, jestli má bezpečnostní díru Seznam, ale jestli ji má naše hlava. Jestli se skutečně najde dost jedinců, kteří po přečtení jakéhosi pochybného textu dobrovolně svěří cenné údaje cizí osobě. a právě to jsem vyzkoušel.

Nachytal se za tu krátkou chvíli vůbec někdo?

E-mailů přišlo několik desítek! *V 8:58 mi napsali z Helpdesku Seznamu žádost o stažení článku a schránku zablokovali (čest jejich pohotové reakci). Bohužel tím zrušili i velmi důležitou funkci celého experimentu, automatickou odpověď ve znění:*

Člověče, příště se zamysli, než uděláš takovou hloupost a pošleš někomu cizímu své vlastní heslo.

Pěkný den a více opatrnosti přeje dgx

Což mě velice mrzí – spousta lidí tak možná stále netuší, čeho se vlastně dopustili. Jen doufám, že si přečtou tuto část článku.

Poznámka: všechny e-maily se automaticky mazaly, přístupové údaje jsem neviděl a ani mě nezajímají.

11.8 SCHÉMA SÍTĚ VPN