Zneužitelnost internetu a jeho vliv na oprávněné zájmy

Internet exploitability and it influences to the legitimate interests

Dmitriy Volkov

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Abstrakt

Tato bakalářská práce posuzuje všechny možné druhy internetových hrozeb dle cílů útoků. Odhadují se průměrný škody způsobené různými druhy útoků a navrhují se způsoby ochrany. Praktická část práce je zaměřená na podrobnou analýzu internet-útoků na dobrou pověst podniku či produktu/služby, protože obrana proti těmto útokům je nejslabší a nepropracovaná. Navrhují se také možné způsoby ochrany a prevence. Na závěr záměr zpracování komplexního manuálu pro obranu proti útokům na dobrou pověst a image firmy.

Klíčová slova: web-útoky, ochrana dobré pověsti.

Abstract

This work considers every possible kind of Internet threats, classifying them due to the attack purpose. There are estimated possible damages from each kind of Internet attacks and offered the ways of protection. The practical part of work is a detailed analysis of Internet attacks on the good story of a brand, because defense against these attacks is the weakest and unexamined. Also there is offered possible methods of protection and prevention. In conclusion, the intention for the further work on creation of a universal manual for defense against attacks on the reputation and image company.

Keywords: web attack, protection of reputation.

Poděkování

Děkuji tímto panu JUDr. Františku Brabcovi za odborné vedení, poskytnuté materiály a cenné rady. Dále děkuji PhDr. Vladislavu Böhmovi za pomoc ve výběru tématu a průběžné konzultace. Bez jejich pomoci by tato bakalářská práce nemohla vzniknout.

Neodvolatelná prohlášení

- Beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve zněni pozdějších právních předpisů, bez ohledu na výsledek obhajoby.
- Beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce.
- Byl jsem seznámen s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3.
- Beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- Beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše).
- Beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům.
- Beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti muže být důvodem k neobhájení práce.

Prohlašuji, že

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor;
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Praze .....

podpis bakaláře

Obsah :

II. PRAKTICKÁ ČÁST

3. Zkoumání útoků na dobrou pověst a zajištění obrany

Úvod

Hlavní cíl této bakalářské práce je definovat a klasifikovat všechny možné (resp. známé) typy útoků na oprávněné zájmy s pomocí internetu. Všechny druhy hrozb na internetu shromáždíme do čtyř skupin podle konečných cílů útočníka:

- útoky, které mají za cíl narušit funkčnost software a hardware;
- útoky, které mají za cíl dosáhnout poruchy webové stránky;
- útoky, které mají za cíl krádež obchodních informací a osobních údajů;
- útoky, které mají za cíl poškodit dobrou pověst firmy, poškodit vnímání kvality služb nebo produktu.

Současné webové útoky nespolehají jenom na zranitelnost softwaru, ale častěji používají lidský a sociální faktor. Proto se v této práci podíváme na útoky nejen z hlediska technického, ale také z hlediska psychologického a sociálního.

Detailně prozkoumáme webové útoky na dobrou pověst, které jsou specifické tím, že se proti nim není možné bránit pouze technickými metodami, a tudíž vyžadují mnohem komplexnější obranu.

Dále s pomocí statistických údajů zjistíme výši škod způsobených různými druhy útoků a sestavíme formuli pro odhad možných ztrát, způsobených internetovými útoky na dobrou pověst.

Dále probereme současné právní předpisy s touto problematikou souvísející.

I.TEORETICKÁ ČÁST

1. Analytická část: Výhody a hrozby internetu pro podnikání

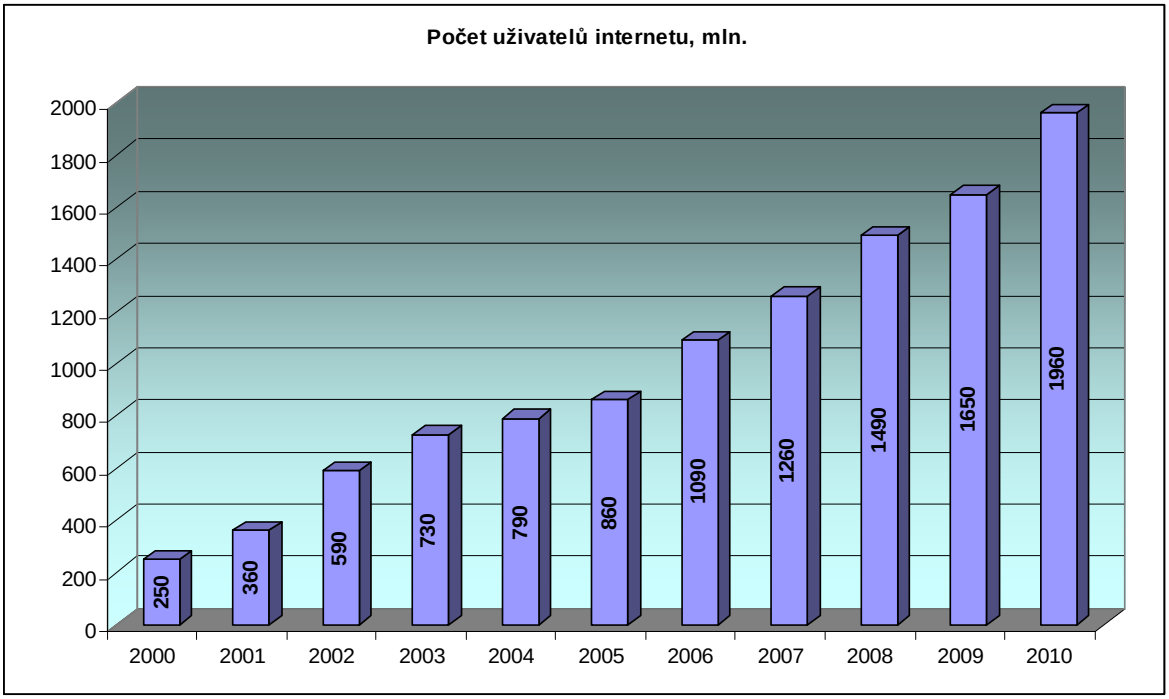
1.1. Internet v dnešní době – nejdynamičtěji se rovíjející oblast současnosti

Zdokonalení výpočetní techniky umožňuje zvýšení rychlosti připojení k internetu a snižuje náklady na jeho použití.

Internet se proto stal největším přístupným zdrojem informací ve světě. Jeho ohromnou výhodou je globálnost a rychlost přenosu informace. Přes internet se dnes komunikuje, v síti internetu se hledají potřebné informace, za pomoci internetu se obchoduje, provádějí se bankovní transakce, řídí se obchodní procesy, tvoří umělecká díla, rozšiřují politické názory apod. Prostřednictvím internetu se ale také krade, podvádí, manipuluje atd. Internet zkrátka v dobrém i ve zlém zasahuje do všech oblastí lidské činnosti, jako jsou ekonomika, kultura, sociální oblast.

Internet ale svět take hluboce mění. Například povinný systém komunikace pomocí datových schránek nejenom usnadnil veřejným institucím komunikaci s fyzickými a právnickými osobami, ale de facto způsobí, že kdo nebude umět pracovat s internetem, bude společensky stejně diskvalifikovaný, jako kdyby neuměl číst, psát a počítat. Podobně se mění tradiční média. Jejich zpravodajská funkce zaniká, protože aktuální zprávy z celého světa snadněji a rychleji dostaneme na zpravodajských portálech. A je otázka, zda jejich role analytiků a komentátorů se také v dohledné době nepřenese na internet.

V roce 2011 počet uživatelů internetu překročil dvě miliardy [3], a to znamená, že téměř každý třetí obyvatel planety Země používá internet. Dle údajů NetMonitoring v únoru 2011 bylo v České republice registrováno 5,86 milionu uživatelů internetu [4]. Jinými slovy více než polovina populace ČR aktivně používá internet. Navíc tato statistika nebere v úvahu pasivní uživatele internetu, kteří využívají internetové služby různých mobilních operátorů.



Obrázek č. 1: Dynamika růstu počtu uživatelů internetu na světě

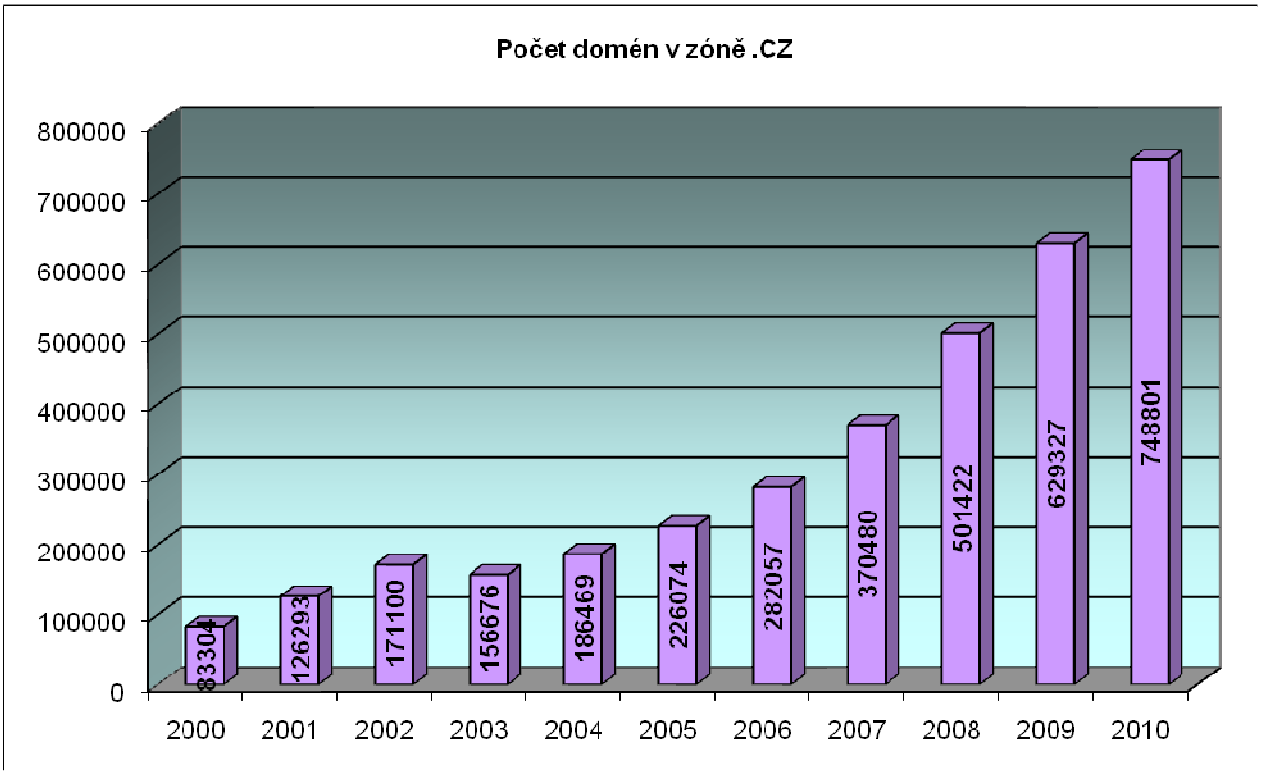
1.2. Výhody internetu pro podnikání

Nyní si dost těžko představíte společnost, která při své práci nepoužívá internet. S pomocí internetu se dnes běžně řídí pracovní procesy a spravují finance. Většina firem má své vlastní webové stránky. Některé z nich jsou pouze on-line vizitkou, nicméně, většina moderních webů nabízí svým návštěvníkům nejen statické informace o společnosti, ale i řadu služeb, které umožňují třeba i nákup online.

Všeobecně jsou známa jména zahraničních korporací, jejichž činnost je postavena výhradně na internetových technologiích. Jako příklady lze uvést Gogole, Facebook, AOL, Yahoo... Z českých připomeňme víceúčelový portál Seznam, zpravodajské portály Aktuálně.cz, Novinky, iDnes, iHNed apod.

S růstem počtu uživatelů internetu roste také počet webových stránek. Podle analýzy společnosti Netcraft, počet aktivně fungujících stránek v celosvětové síti v únoru 2011 byl více než 273 milionů. [5] V souvislosti s počtem registrovaných domén v zóně .CZ můžeme také přibližně sledovat růst podnikatelské činnosti na českém internetu (samozřejmě je otázka, do jaké míry jsou růst počtu domén a růst podnikatelské činnosti v nějaké vzájemné korelaci - může jít

pouze o "dohánění" počtu domén, o české mutace zahraničních domén atd.). Počet domén v dubnu 2011 byl 793.521. [6] Dynamiku růstu ukazuje níže uvedený diagram:



Obrázek č. 2: Dynamika růstu registrovaných domén v zóně .CZ

1.3. Internetové hrozby a analýza ztrát způsobených webovými útoky

Internet je ale také velice nebezpečným prostředím. Útoky vedené přes internet mohou způsobit nejen "tolerovatelné" ztráty (podobně jako když obchodníci počítají s určitým procentem krádeží zboží), ale dokonce přivést ke zhroucení celého podniku či vážnému narušení chodu státu.

Čerstvá zpráva «Cost of Cyber Crime Study», poskytnutá Ponemon Institute, jasně ukazuje, jak velkou škodu trpí společností v reálném pracovním prostředí.

Celkem se studie zúčastnilo 45 velkých amerických společností s počtem 500 až 100.000 zaměstnanců. Bylo zjištěno, že průměrné škody způsobené různými druhy počítačových útoků jsou téměř 3,8 milionů dolarů ročně. Tato částka zahrnuje náklady na vyšetřování a likvidaci následků mimořádné události, přímé finanční ztráty, ztráty v důsledku přerušení práce zaměstnanců a dislokací podnikových procesů, ušlý zisk, atd. Mimo toho existuje potenciální

riziko, že incident se stane veřejně známým, a tím bude poškozena dobrá pověst organizace, což její ztráty ještě dale prohloubí.

Během čtyřtýdenní studie 80 % podniků přežilo útoky virů, červů a trojských koni. 73 % firem byly napadeny „phišery“ a sociálními inženýry, ve kterých se útočníci se snažili uvést do omylu uživatele nebo správce serveru. Ve 62 % případů případů došlo ke ztrátám spojeným s únikem obchodních informací a osobních údajů. 29 % všech útoků bylo spojeno se zaváděním škodlivého kódu a snahou přípojit počítač do botnetu.

"Nejnákladnější" (ve smyslu způsobující nejvyšší škody) útoky jsou dnes vedeny na firemní webové stránky korporací, u nichž každoroční ztráta v průměru činí 1 milion dolarů. Lze můžeme sledovat výrazný růst počtu útoků, využívajících techniky sociálního inženýrství, a růst počtu kombinovaných útoků, nacílených na dobrou pověst podníku. Přičemž rozsah škod způsobených takovým chytře provedeným útokem nelze určit definitivně, jelikož důsledky poškozené pověsti na dlouhou dobu zkracují příjmy společnosti. [7]

2. Metodická část – Klasifikace útoků na internetu dle jejích cílů

Máme-li se internetovým útokům bránit, musíme vědět, jaké útoky hrozí, čím jsou charakteristické, co mohou způsobit a jaké jsou jejich silné a slabé stránky… Jinak řečeno, abychom se v možných útocích orientovali, musíme je vhodně roztřídit.

Pro účely této práce se autoru jako nevýhodnější jeví, klasifikovat a systematizovat útoky na internetu především dle konečného cíle útočníka. Takové rozlišení umožní přesněji definovat předmět útoku, a tím pádem vyvíjet efektivní metody jeho obrany.

2.1. Interní sítě, hardware a software

Toto je nejstarší druh útoků, cílem kterých je zavést do počítačů škodlivé programy, které porušují stabilitu práce, způsobují selhání zařízení, vyvolávají závady na software a také přispívají ke zničení důležitých informací.

Od objevení prvních počítačových virů uplynulo více než 50 let. Za tuto dobu bylo vyvinuto ohromné množství druhů a způsobů infikování výpočetní techniky a programového zabezpečení. Všechny spojuje to, že zneužívají zranitelná místa v software. Není možné nabídnout jedinou klasifikaci a jednoznačně určit metody obrany, protože každý účinný virus, červ nebo trojský kůň je kreativní dílo, které zhodnocuje “zkušenosti” všech dosavadních útočníků a přináší nové metody, prorážející obranu vyvinutou proti dosavadním útočníkům. Tvůrci virů, červů a trojských koní a vývojáři antivirových softwarů jsou mezi sebou v nekonečné válce.

Pro jakous takous orientaci zde nabídneme víceméně stabilní klasifikaci typů škodlivých programů a způsobů vniknutí těchto programů do počítačů a počítačových sítí.

2.1.1. Viry

Počítačové viry jsou speciální počítačové programy, jejichž charakteristickým rysem je schopnost k reprodukci. Škodlivé viry mohou bez vědomí uživatele provádět různé svévolné akce, včetně způsobení škody na software a/nebo na počítači. [8]

Viry jsou schopny proniknout v RAM (rezidentní viry). Takové viry mohou kontrolovat a převzít všechny operace, které provádí systém: rozbít a zcela zablokovat interakci s uživatelem, poškodit soubory a programy, apod. [9]

Přepisovací viry se vyznačují tím, že mažou informace, které se nacházejí v infikovaných souborech, a tím je dělají zcela nebo zčásti nevhodné k prečtení. [9]

Některé viry pronikají v boot-sektory disku (boot-viry). Oni neinfikují soubory, ale disky, a znemožňují spuštění systému nebo jej spustí nesprávně. [9]

Viry se mohou skrývat i v dokumentech jako makra (makroviry). Uživatel otevře soubor, který považuje za bezpečný, ale přitom automaticky dává svolení ke spuštění viru. Důsledky mohou být katastrofální. [9]

Některé viry se mohou schovávat pod rouškou obrazových souborů, skrytí v archivu apod.

Hodně moderních virů se kóduje nebo se schová pomocí různých algoritmů a šifrovacích klíčů. To jim umožňuje skrýt se před skenery (programy na vyhledávání virů). Před provedením svého úkolu se virus sám dekóduje a začne produkovat určité destruktivní akce. Jakmile virus „udělá to, co má“, znovu se skryje a zůstane pro antivirový software neviditelný.

2.1.2. Červi

Červ je program podobný viru. Je také schopen autoreprodukce a může systému způsobit škody. Nicméně červ není virus sám o sobě, protože pro své rozmnožování nemusí napadnout další soubory. [9]

Červi jsou nejrozšířenějším typem škodlivého software, které je distribuováno internetem, obvykle pomocí protokolu http, chatování nebo prostřednictvím e-mailu. Červi pronikají do počítače oběti bez zásahu uživatele. Aby pronikly do počítače, červy používají takzvané "díry" (zranitelnosti) v software operačních systémů. Zranitelnosti jsou chyby a nedodělky v software, které umožňují vzdáleně nahrát a spustit zdrojový kód, v důsledku kterého se virus dostane do operačního systému.

Červi mohou existovat samy o sobě, bez poškození souborů, ale množí se obrovskou rychlostí, a tím způsobují zahlcení. Zničení souborů tak způsobují jaksi nepřímo. Mohou sledovat i jiné cíle, např. rozesílání spamu nebo organizaci DDoS- útoků.

2.1.3. Trojany (trojské koně)

Trojský kůň pracuje stejně jako jeho jmenovec mytologický, slavný dřevěný kůň, v němž se ukryli řečtí vojáci, aby nenápadně pronikli do Tróji. Zdají se být neškodnými programy, které se dostanou do počítače libovolným kanálem. Obvykle tak, že je uživatel počítače sám do

počítače pustí (tvůrci jim proto dávají atraktivní názvy nebo vlastnosti, aby uživatele uvedli v omyl). Když je ale program je spuštěn, v počítači se nainstalují jiné, již opravdu škodlivé programy.

Trojské koně se n začátku vůbec nemusejí jakkoliv projevovat, a tím pádem jsou neviditelné pro antivirový software, který kontroluje nové soubory. Když však začnou působit, mohou totálně zničit počítačový systém. Trojské koně jsou ale schopné provést nejen přímé destruktivní akce, jako například poškodit a smazat potřebné soubory nebo poškodit řádné fungování sytému, ale také mohou krást a předávat dál citlivé informace. [9]

Jako příklad destruktivního působení trojských koní můžeme uvést:

- Zničení informací. Konktrétní výběr objektů a způsobů zničení záleží na záměrech tvůrce takovéhoto pragramu a na možnostech hardwaru.
- Zachycení a předání informace. Většinou jde o krádež přihlašovacích údajů a hesel. Může se provádět cestou zachycení symbolů bezprostředně v klávesnici, nebo během jejich přenášení po síti.
- Cílevědomá modifikace kódů programů, o který se pachatel zajímá. Zpravidla jsou to programy, které realizují funkce zabezpečení a ochrany.

Moderní internet se hemží různými viry, červy či trojskými koni a stát se obětí takového útoku je velmi jednoduché, obzvlášť pokud surfujete na internetu bez kvalitního antivirového programu a správně nakonfigurovaného zabezpečení systému (tzv. firewall - ovládá porty a filtruje pakety přenášené po síti). Kromě toho je velmi důležité mít nejnovější verzi antivirového softwaru, který obsahuje aktuální databáze.

2.1.4. Technické prostředky útoku

Nicméně, poškození hardwaru a softwaru mohou být nejen výsledkem působení škodlivého software. Jsou také různé technické nástroje, které vedou k selhání řádného fungování hardwaru a softwaru. Stručně prozkoumáme ty hlavní.

- UDP Storm – používá se v případě, že oběť otevřel minimálně dva porty UDP, z nichž každý odesílá odesílateli nějakou odpověď. Pak je možné uměle vytvořit situaci, kdy porty začínají nekonečně odpovídat jeden druhému, což snižuje produktivitu.
- UDP Bomb – UDP paket s neplatnou oblastí služebních dat. Údaje mohou být jakkoliv narušené, např. nekorektní délka pole, struktura... To vše může vést k havárii.

- Land – záměna adresy odesilatele za adresu příjemce (stejně tak se zaměňuje číslo portu odesilatele za číslo portu příjemce). V tomto případě nastává selhání routeru, protože se on bude snažit navázat kontakt sám se sebou.
- Puke – vymyšlená odpověď ICMP unreachable (chyba smazaného systému), což může vést k odpojení klienta od serveru.
- Fake unreachable – vymyšlená zpráva, že balíček/soubor nelze doručit (nedostupný), která způsobí, že si server „myslí“, že klient má poruchu, a přestane pakety dodávat na místo určení. To může způsobit, že server klienta vypne. [10]

Existuje mnoho dalších možností, jak vyřadit software či hardware z řádného provozu. Účinné ochrany lze dosáhnout pouze s pomoci správného nastavení sítě (výběr správné topologie a instalace routerů). Také by měly být prováděny pravidelné preventivní údržby hardwaru a neustálé sledování vnitřní sítě.

2.2. Útoky na webové stránky a web-servery

Jak již bylo zmíněno, největší finanční škody přinášejí útoky na firemní webové stránky. Není to nijak překvapující, protože pro mnoho současných organizací nejsou webové stránky jenom internetovou vizitkou, ale jsou také důležitým a zpravidla dnes již nejdůležitějším marketingovým nástrojem.

Útoky na webové stránky, na rozdíl od útoků výše zmíněných, vždy mají konkrétní cíl a jsou vždy předem plánované. Jinak řečeno, útočníci nejenom "rozptylují" viry po internetu v naději, že nakazí co nejvíce nezabezpečených počítačů, ale cíleně útočí na konkretní webový uzel. Konečným cílem útočníků může být jak získání neoprávněného přístupu k citlivým obchodním informacím obsažených na webových stránkách, ale také celkové selhání řádného fungování webového serveru. [2]

Jeden z největších známých útoků na bankovní servery byl uskutečněn v roce 1994 počítačovým programátorem z Petrohradu, Vladimirem Levinem. Jemu se podařilo proniknout do vnitřní sítě banky Citibank a převést na své účty 10,7 milionu dolarů. [11]

Přestože banky vydávají obrovské částky na zabezpečení svých počítačových sítí, které obsahují "peníze v elektronické podobě", útoky s cílem rychle zbohatnout pořád pokračují. Jeden z posledních úspěšných útoků se stal 8. listopadu 2008, když se dosud neznámí hackeři nabourali

do bankovního počítačového systému RBS WorldPay. Hackeři pronikli do systému mzdových účtů a ukradli informace potřebné k vytvoření klonů debetních karet. V závěru se jim podařilo s pomoci zprostředkovaelů vybrat z ATM až 9 milionů dolarů.

Stejnou škodu způsobují i destruktivní útoky na firemní webové stránky. V tomto případě útočníci neusilují o neoprávněné proniknutí do zabezpečeného počítačového systému, aby pak ukradli nebo zničili informace. Cílem tohoto útoku je paralyzovat práci určitého webového serveru. Nejnebezpečnější formou těchto útoků jsou DDoS útoky (Distributed Denial of Service – Distribuované odmítnutí služby). První zprávy o těchto metodách se objevily na začátku roku 2000, kdy se útočníkům podařilo zcela ochromit největší on-line prodejce: Amazon.com, buy.com, ebay.com. Finanční ztráty jsou odhadované na několik miliard dolarů. Jde nejenom o ušlý zisk, ale také o náklady spojene s obnovením provozu a s prořízením nového vybavení a nového zabezpečení. Tyto útoky jsou u hackerů stále velmi oblíbené, protože jsou jednoduché na relizaci a zaručují anonymitu pachatele.

Ale i organizace, které na internetu přímo neobchodují, také mohou utpět obrovské ztráty způsobené poruchami firemních stránek. Jeden z posledních velkých útoků se stal 30. března 2011. Byl to útok na populární blog "Live Journal" (livejournal.com). V důsledku toho musela společnost vrátit peníze majitelům placených účtů a poskytnout jim další bonusy, jen aby udržela loajalitu uživatelů. [12]

Ztráty způsobené nedostupností firemní webové stránky mohou být značné i v případě malých podniků, protože mohou mít za následek přímou ztrátu potenciálních zákazníků (při nedostupnosti stránek), narušení on-line komunikace se stávajícími zákazníky, negativní dopad na image podniku a snížení pozice ve vyhledávacích systémech.

Existuje ohromné množství útoků na weby a servery - dle počtu použitvaných skriptů serverového softwaru. „Pachatel-odborník“ zaprvé prozkoumá webovou stránku, server, nainstalované skripty a hledá chyby, z jejichž pomocí by mohl získat neoprávněný přístup nebo narušit provoz webové stránky. Dále jsou uvedeny nejběžnější a nejnebezpečnější typy útoků na webové stránky.

2.2.1. Útoky na CGI

Hodně webových stránek používají CGI-skripty, které umožňují těmto stránkám komunikovat s návštěvníky a poskytnout uživatelům další služby a možnosti. Programátoři ne

vždy vytvářejí vlastní skripty tak, aby kontrolovali hodnoty, které uživatelé zadávají, a proto jsou zde možnosti využití těchto přehlédnutí pro různé účely.

Rozsah této bakalářské práce neumožňuje nám proniknout do problematiky psaní bezpečných kódů, a tak jen chci říci, že přinejmenším potřebujeme filtrovat všechny služební symboly od přijatých dat. [9]

2.2.2. SQL Injection (SQL injekce)

Jsou-li uživatelem uvedená data použita ve vygenerovaných SQL požadavcích bez ověření, útočník je schopen zadat informace, které mu umožní získat veškeré informace z databází SQL. Například na SQL dotaz: "SELECT login, password FROM members where email='admin@site.com OR login LIKE '%admin%';“ nechráněný systém poskytne útočníkovi přihlašovací údaje včetně hesla, pokud login obsahuje „admin“. [9]

2.2.3. Hijacking Pages

Cílem útoku je přinutit server přeposlat pachateli webovou stránku, která byla určena jinému uživateli, tím pádem může útočník získat důležité informace, které jsou určené jiným uživatelům. Může to být číslo účtu nebo vydané heslo. K provedení útoku musí mít útočník TCP spojení s proxy serverem, TCP spojení mezi obětí a proxy serverem a TCP spojení mezi webovým serverem a proxy serverem. [9]

2.2.4. Include Bug

To je často se vyskytující zranitelnost. Pro zjednodušení přidávání nových stránek na webu nebo pro jiné účely se ve skriptech používá funkce include($ file);, kde $ file se zadává uživatelem nebo je uveden v odkazu. Po tom, namísto funkce include (); se vkládá obsah uvedeného souboru. Pokud soubory nejsou administrativně chráněny před přečtením protokolu HTTP, můžete dostat obsah jakékoli souboru umístěného na serveru, včetně těch, které obsahují hesla. [9]

2.2.5. Flood (Flůd)

Útok spojený s velkým počtem obvykle nesmyslných nebo ve špatném formátu zformovaných žádostí na webový server nebo síťový hardware. V důsledku takového útoku

dochází k selhání systému, neboť dojde k vyčerpání systémových prostředků procesoru, paměti nebo komunikačních kanálů.

Bránit se proti tomuto útoku je snadné, stačí včas určit zdroj (IP-adresu) fludu zakázat přijímání od něj paketů

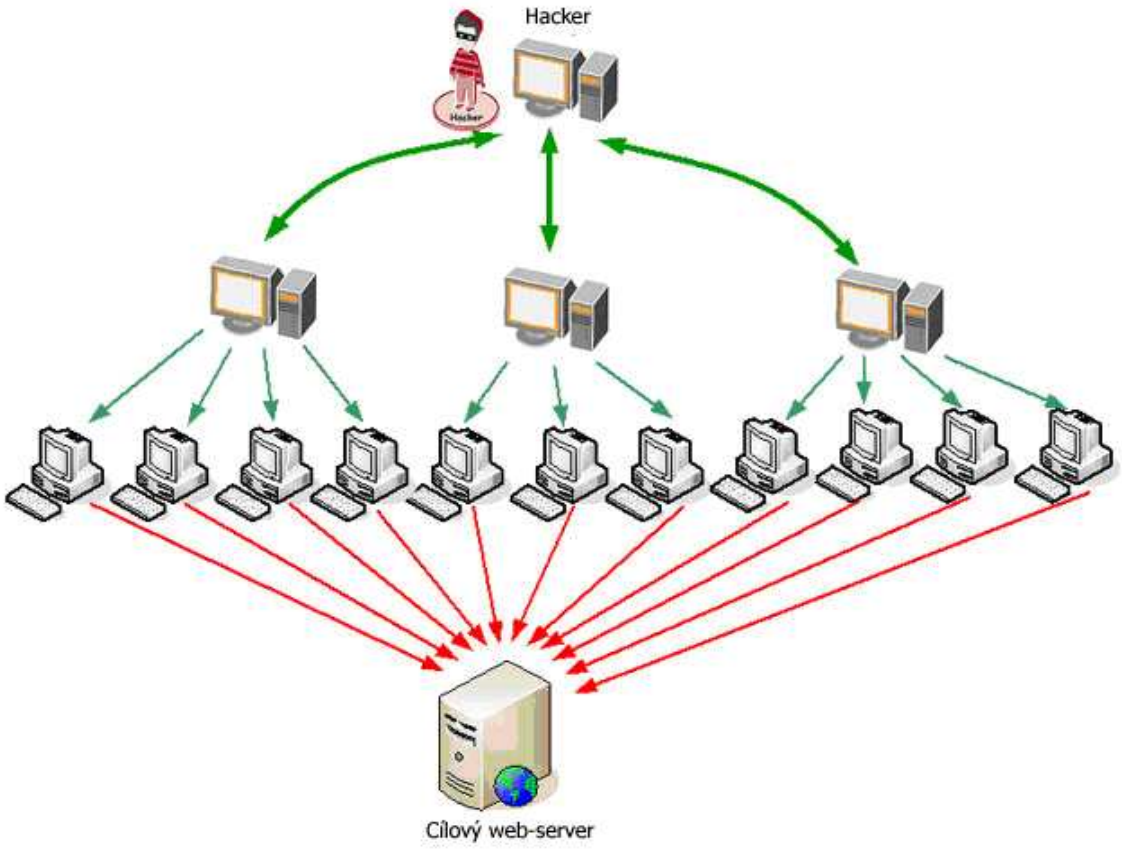
2.2.6. Distributed Denial Of Service Attack (DDoS-útok)

Tento útok je dle důsledků obdobný fludu, ale čelit mu je mnohem náročnější, protože zdrojů fludu je obrovské množství.

Schematicky útok DDoS vypadá přiblížně takto: na server padá obrovské množství falešných žádostí z více počítačů z různých částí světa. Jako výsledek, server vynakládá všechny své zdroje na zpracování těchto žádostí, a tím pádem je prakticky nepřístupný pro běžné uživatele. Ale hlavní je, že uživatelé počítačů, které posílají falešné požadavky, dokonce ani nemusí tušit, že jejich počítače na dálku využívají i hackeři. Programy, které pro tyto účeli hackeři nainstalovali do počítačů, obvykle nazýváme "zombie". Existuje mnoho způsobů zneužití jiných počítačů, začínající proniknutím do nechráněné sítě a končící používáním trojských koni. Možná, že tato fáze přípravy je pro útočníka nejvíce časově náročná.

K útokům DDoS se nejčastěji používá trojhladinová architektura, která se nazývá "cluster DDoS". Tato hierarchická struktura obsahuje:

- řídicí konsola (může jich být i několik), tj. ten počítač, ze kterého útočník určuje cílový webový server a vysílá signál k zahájení útoku;
- hlavní počítače, které dostávají signál o útoku z řídicích konzol a předávají je „agentům-zombie“
- agenti - to jsou bezprostředně bot-počítače, které svými požadavky útočí na cílový web-server.



Obrázek č. 3: Schéma DDoS-útoku

(Dostupný z URL: http://www.pcweek.ru/upload/iblock/a9e/ddos-1l.jpg)

Vystopovat takovou strukturu v opačném směru je prakticky nemožné. Jediné, co oběť může určit, je adresa některého agenta. Speciální akce v nejlepším případě přivedou k hlavnímu počítači. Ale jak je známo, bot-agenti a hlavně počítače samy jsou také obětmi v této situaci a jsou "zkompromitované". Tato struktura prakticky neumožňuje vystopovat adresu počítače, který útok zorganizoval.

Dnes specialisté v oblasti bezpečnosti informace rozlišují tyto druhy DDoS-útoků:

- UDP flood – zaslání na adresu cílové stanice hromady paketů UDP (User Datagram Protocol). UDP má větší prioritu než TCP. S pomoci velkého množství UDP-paketů různých velikostí nastává přetížení komunikačních kanálů, poté server přestane reagovat v protokolu TCP. Avšak aplikace, které používají tento typ útoků, lze snadno odhalit, protože během výměny mezi hlavním počítačem a agenty jsou používány nezašifrované protokoly TCP a UDP. Proto s útoky tohoto druhu můžeme poměrně úspěšně bojovat. [13]

- TCP flood – zaslání na adresu oběti hromady TPC-souborů, což také způsobuje zablokování síťových zdrojů. [13]
- TCP SYN flood – odeslání velkého počtu žádostí o inicializaci TCP-spojení na cílový server, který v důsledku toho útoku musí vynaložit všechny své prostředky na sledování těchto částečně otevřených spojení. [13]
- ICMP flood – ping-žádosti ICMP (Internet Control Message Protocol), na zpracování kterých je zapotřebu delší doba, v důsledku čeho server není k dispozici běžným uživatelům. [13]
- Smurf-útok – chytrý trik, během kterého se rozesílají soubory s použitím ping-dotazů ICMP s uvedením falešné zdrojové adresy, která se ukáže být terčem útoku.

Samozřejmě, že nejnebezpečnější jsou programy, které zároveň používají několik typů výše uvedených útoků.

Univerzální způsoby ochrany proti webovým útokům neexistují, ale lze uvést obecná doporučení pro snížení rizika a minimalizování škod. Patří sem například taková opatření, jako správná konfigurace funkce anti-spoofing a anti-DoS na serverových routerech a firewallech. Tyto vlastnosti omezují počet napůl otevřených kanálů, což nedovoluje přetížení systému.

Na úrovni serveru je žádoucí, aby výstup konzole serveru byl i na jinou IP-adresu dle SSH-protokolu, a to pro získání možnosti vzdáleného restartu serveru. Další velmi efektivní metodou ochrany serveru v boji proti DDoS útokům je přesměrování IP-adresy.

Programy a skripty webových stránek musejí vykonávat pouze funkce, které jsou nezbytné pro interakci s uživatelem, a všechny další možnosti musejí být vypnuté.

2.3. Krádež obchodních informací a osobních údajů pomoci internetu

Jedná se o velmi širokou škálu útoků s pomocí souhrnu technických a psychologických technik zaměřených na získání neoprávněného přístupu k utajovaným informacím, jako např. k důležitým obchodním informacím, k osobním účtům, k bankovním účtům, k e-mailům, atd.

2.3.1. Brute force (hádání hesla hrubou silou)

Metoda pro získání přístupu k neveřejným zdrojům cestou vyzkoušení všech možných kombinací uživatelských jmen a hesel. Jako "pracovníci" se používají programy sestavené z různých kryptografických algoritmů. Složitost hledání všech možných kombinací závisí na počtu všech eventuálních alternativ. Pokud je počet těchto variant velmi velký, jejich kompletní vyzkoušení může trvat bez výsledku několik let či dokonce staletí. [2]

Příklad délky výběru hesla

Počet symbolů	**Počet alternativ**	**Čas odhadnutí**
1	36	Míň než vteřina
2	1296	Míň než vteřina
3	46 656	Míň než vteřina
4	1 679 616	17 vteřin
5	60 466 176	10 vteřin
6	2 176 782 336	6 hodin
7	78 364 164 096	9 dnů
8	$2{,}821\,109\,9 \times 10^{12}$	11 měsíců
9	$1{,}015\,599\,5 \times 10^{14}$	32 let
10	$3{,}656\,158\,4 \times 10^{15}$	1 162 let
11	$1{,}316\,217\,0 \times 10^{17}$	41 823 let
12	$4{,}738\,381\,3 \times 10^{18}$	1 505 615 let

Jak vidíme z této tabulky, stačí používat hesla s 8 a více symboly, abychom se dostatečně ochránili proti možném odhadnutí hesla programovými metodami. Také lze zvětšit počet alternativ - znaky pro heslo lze vybírat nejen z abecedy s malými písmeny, ale i s velkými, doplnit čísly a dalšími znaky z klávesnice…

2.3.2. Key-loggers

Speciální programy, které sledují stisky kláves a posílají tuto informaci na předem určenou adresu. Útočníci infikují počítač oběti programem, který zachytne a útočníkovi odešle všechny znaky, které nabírá oběť na klávesnici, a to včetně hesel.

Nicméně, většina moderních antivirových programů si s problémy tohoto druhu umí úspěšně poradit a zabraňuje takovémuto úniku informací.

2.3.3. Phishing (Fišing)

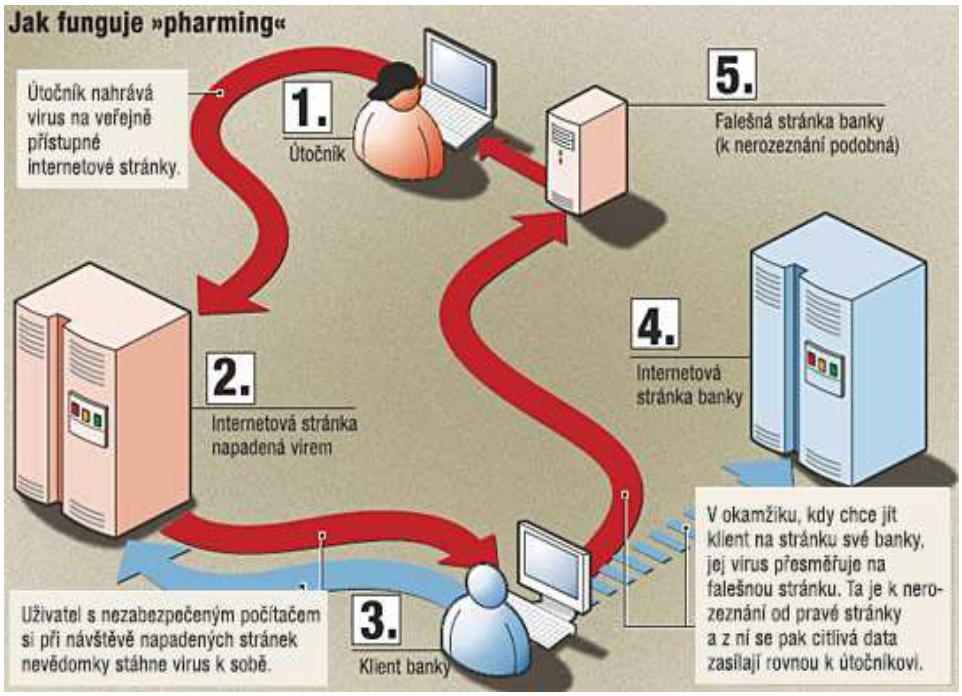
Phishing je technologie internetových podvodů, spočívající v odcizení důvěrných osobních údajů, jako jsou hesla, údaje bankovních a identifikačních karet atd. [14] Podstata phishingu je následující: Podvodník vytvoří webovou stránku, která je velice podobná jiné webové stránce, a tím pádem uvede do omylu uživatele, který se domnívá, že je na stránce původní. Pak stačí pod vhodnou záminkou uživatele požádat o identifikaci, o sdělení hesla či jiné důvěrné informace, a on často vyhoví. Je třeba zdůraznit, že všechny tyto akce vykonává oběť naprosto dobrovolně a netuší, co ve skutečnosti dělá. Používají se zde techniky sociálního inženýrství. K dnešnímu dni můžeme vyčlenit 3 typy phishingu:

- Emailový. Je nejstarší. Na email se odesílá dopis s požadavkem poskytnout nějaké údaje. Když uživatel přejde na odkaz, který mu byl v dopise zaslaný, dostane se na phishingový web, který, i když je vizuálně naprosto shodný s původním webem, je určen pouze pro odcizení důvěrných dat obětí.
- Online phishing. Tato metoda je postavena na kopírování nějakého webu, který umožňuje on-line komunikaci a placení (nejčastěji jde o e-shopy). Opět se používají shodné webové adresy a design. Dále vše pokračuje velice jednoduchou cestou. Oběť, jež se dostane do podobného „e-shopu“, se rozhodne si něco koupit. Počet obětí bude dostatečně velký, protože ceny v takovém "neexistujícím" obchodě budou nízké, a všechna podezření jsou rozptýlena vzhledem k „dobrému jménu“ původního e-shopu. Při nákupu zboží se oběť registruje a zadává údaje své platební karty.
- Kombinovaný. Podstatou této metody je, že se vytvářejí falešné webové stránky nějaké organizace, které pak lákají potenciální oběti. Je jim navrhnuto navštívit určité webové stránky a osobně tam provést nějaké operace. Zpravidla jsou zde použity psychologické metody ovlivnění uživatele.

2.3.4. Pharming

Mechanismus pharmingu v sobě kombinuje phishing a standardní metodu virové infekce. Oběť si otevře nevyžádanou e-mailovou zprávu nebo navštíví nějaký webový server. V obou případech tam čeká spustitelný program - virus. Přitom se poškozuje soubor hosts, do kterého se vpisují falešné IP adresy pro konkrétní URL. V důsledku toho se aktivuje mechanismus přesměrování, a když uživatel zadává například URL své banky, tak je přesměrován na jeden

z falešných webů, na kterém zadá své přihlašovací údaje. Ani ten nejzkušenější uživatel nemá nejmenší ponětí, že se nachází na falešné stránce. [15]



Obrázek č. 4: Schéma Pharmingu

(Dostupný z URL: http://ihned.cz/attachment.php/160/14175160/iAajmMtovJu68nRLxFeW2sDpOkSUV9lC/pharming-pc-540.jpg)

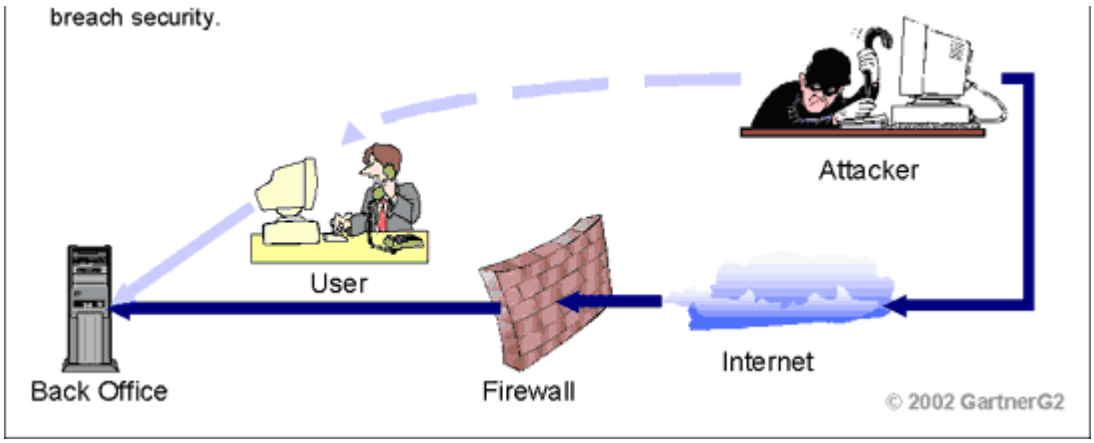
2.3.5. Sociální inženýrství

To je celkem chytrá kombinace technických a psychologických technik zaměřených na získání neoprávněného přístupu k osobním údajům a obchodním informacím. Útočník využívá lidskou důvěřivost, nedbalost a nepozornost jako klíč k prolomení jinak nepřístupné obrany utajovaných informací. Informovanost společnosti o tomto jevu je nyní nízká a zatím neexistuje žádný široce využívaný vzdělávací nástroj pro efektivní vzdělávání lidí v této záležitosti, a tak jsou tyto metody velmi nebezpečné.

V roce 1995 byl nejhledanější počítačový kriminálník Kevin Mitnick zatčen za počítačovou kriminalitu, která mu vynesla 4 roky vězení. Jeho nejrozšířenějším polem působnosti týkajícím se infiltrace bylo právě sociální inženýrství.

Sociální inženýrství je přehlížená bezpečnostní hrozba a firmy jsou v tomto ohledu velmi zranitelné. Největším nebezpečím je, že podniky nejen přehlížejí daný problém, ale je tu i nedostatek společenské pozornosti a nedostatek znalostí o sociálním inženýrství jako fenoménu. [16]

Důvod, proč je tak těžké se bránit sociálnímu inženýrství, spočívá ve faktu, že sociální inženýr útočí na nejslabší článek zabezpečení firmy, a to na lidský faktor. V podstatě to znamená, že zkušený sociální inženýr může získat přístup ke kterémukoli požadovanému systému informací, přestože hardwarový i softwarový ochranný mechanismus, který má chránit systém nebo informace, je řádné implementován a kontrolován. Proto je sociální inženýrství v podstatě o hledání způsobu nebo prostředku, jak obejít technologii (nebo software) založenou na ochranném mechanismu, prostým manipulováním lidí, kteří mají přístup k požadovanému systému informací. Tento obrázek ukazuje, jak sociální inženýr používá lidi, aby se zmocnil požadovaných informací. [16]



Obrázek č. 5: Cesta sociálního inženýra

(Dostupný z URL: http://www.gartner.com/it/products/research/images/b_security.jpg)

Způsob, jakým sociální inženýr používá sociální dovednosti místo tradičního hackování softwaru a hardwaru, aby získal přístup k cílové informaci, by si zasloužil samostatnou práci. Sociální inženýrství je obvykle děleno do dvou rozdílných kategorií, jmenovitě podvod založený na technice nebo počítači a podvod založený na lidské spolupráci. Uveďme zjednodušenou ukázku postupu:

Útočník nejprve získává základní informace, například shromažďuje údaje o zaměstnanci cílové firmy, třeba pomocí jednoduchého telefonního hovoru, nebo tím, že pronikne do organizace jako nový zaměstnanec.

Útočník pak může zavolat zaměstnancům společnosti (pod záminkou technických služeb) a požádat je o sdělení hesla, například s odkazem na potřebu vyřešit drobné problémy v počítačovém systému. Jde samozřejmě o trik, jehož nejúčinnějšími zbraněmi jsou příjemný hlas a herecké schopnosti. A nejúčinnější obranou je prostě neodpovědět, ale kto to zvládne?

Útočník se přitom mohl tvářit jako technik dodavatelské společnosti, kterému bylo voláno na telefon technické podpory. Chtěl přece působit ve prospěch zaměstnance dané společnosti, zjevně hodně znal… A sehrál třeba scénku, že z důvodu hackerského útoku změnil přístupové heslo a chce nové sdělit příslušnému zaměstnanci. A aby si byl jistý, že to heslo sděluje tomu pravému, ptá se na to, zda zná heslo… Nebo sehraje jinou scénku, například kontroluje, zda zaměstnanec své heslo nezapomněl… Autor nemá k dispozici průzkumy, kolik procent lidí by obstálo a „potřebnou“ informaci nesdělilo, domnívá se však, že by to bylo procento velmi malé.

Podobných příběhů lze vymyslet spoustu. Například se „technik“ dodavatelské organizace zeptá, proč dotyčný pracovník nedorazil na důležitou schůzku, že mu to vedoucí slíbil oznámit… Ale oni teď jsou na smluveném místě s potřebnou technikou a čekají, aby jim dotyčný „napsal“ heslo… Když tedy on nyní na místě není, ať ho řekne s tím, že zatím začnou s prací, a až za hodinku dorazí, tak heslo změní na nové.

Potřebná jména zaměstnanců lze zjistit několika telefonáty na podnikovou ústředku, jindy jsou k dispozici přímo na webových stránkách společnosti a v dalších veřejně dostupných zdrojích informací (zprávy, reklamy atd.). Jiné zdroje vstupních informací jsou již na hraně či za hrnaou zákona, například analýza takzvaných virtuálních odpadků a virtuálních stop, analýza obsahu ukradeného přenosného počítače nebo paměťového média…

Pokusme se uvedené příklady zobecnit: Zkušený sociální inženýr nejprve provádí analýzu bezpečnostních opatření firmy a nalézá jejich slabiny. Podle této analýzy vytváří scénář útoku, který v různé míře může v sobě kombinovat lidské a technické faktory. Je to zřejmé, i bez příkladů to každý snadno pochopí, že?

Nejefektivnnějším mechanismem obrany proti sociálnímu inženýrství je důkladná znalost hrozícího nebezpečí, metod a způsobů socialních inženýrů a trvalá pozornost věnovaná zaměstnancům, kteří mají přístup k důležité citlivé informaci.

2.4. Útoky na dobrou pověst společnosti a obhájení kvality produktu pomoci internetu

Využívání prostředků masové informace ke konkurenční válce má historii počítanou na staletí, počínaje možná již kouřovými signály a konče internetem (samozřejmě jen prozatím). Metody konkurenčního boje můžeme rozdělit na legální a nezákonné, na morální a nemorální. Základní legální metodou využívání prostředků masové informace k získání výhody oproti konkurentům je reklama. I když reklama se také někdy může stát nezákonnou, zejména když zadavatelé reklamy v zájmu získání klientů použijí všemožná „chytráctví“ včetně různě upravených polopravd i vyslovených lží. Z tohoto důvodu vznikly a více či méně fungují zákony a morální kodexy, které se snaží reklamu regulovat. [1]

Prostředky masové informace lze naopak využívat i jako nástroj „antireklamy“, kdy se peníze zadavatele reklamy nevkládají do vychvalování vlastního produktu a vlastního podniku, ale do šíření informací, které poškozují image a reputaci podniků konkurentů.

Je jasné, že jak legální, tak nelegální postupy mohou, jsou-li uplatněny zkušenými specialisty na reklamu a PR, dát firmě zákazníka opravdu značné konkurenční výhody.

Na internet se dnes můžeme dívat jako na součást prostředků masové informace. Je zřejmé, že oproti dřívějším mediím má řadu nesporných výhod:

- Na internetu si lidé najdou to, co potřebují, a ne to, s čím se náhodně setkají v tradičních médiích. To pozitivně ovlivňuje loajalitu a zvyšuje důvěru k informacím, které získávají na internetu.
- Internetová reklama je aktuální a přístupná dlouhá léta.
- Internet umožňuje operativnější umístění reklamy na více místech a zobrazuje se vícekrát.
- Internet nemá žádné geografické a politické hranice.
- Cena reklamního kontaktu s cílovou skupinou je vždy nepochybně nižší než u tradičních medií.
- Existují a úspěšně se používají mechanismy demonstrace internetové reklamy pouze těm uživatelům, pro které tato reklama může být zajímavá (Google AddWords, Seznam Sklik atd.)

Proto výdaje na internetovou reklamu stale rostou a mají zvyšující se význam v marketingových rozpočtech. Již dnes podíl internetové reklamy činí v průměru 5,4 % celkových výdajů na reklamu ve světě. [17] Přitom je třeba brát v úvahu, že náklady na televizní reklamu jsou sta a lecky i tisíce krát větší než náklady na obdobnou účinnou reklamu v síti. Předpovědi vývoje trhu reklamy pro příští desetiletí jednoznačně potvrzují rychlý růst internetové reklamy na pozadí mírného poklesu tradiční reklamy.

Kromě toho, kvalitně provedená reklama nebo antireklama se šíří lavinovitě – jeden uživatel ji zasílá dalšímu a ten zase dál. V moderním internetu lze doporučení nebo nedoporučení výrobků a služeb šířit nejen „klasicky“ zveřejněním na podnikových webových stránkách, rozesíláním e-mailem nebo chatem, ale i mnohem rychleji a do více směrů na fórech a v internetových sociálních sítích, jako jsou facebook, twiter, livejournal apod.

Tyto výhody internetu se s úspěchem používají i v nelegálních metodách konkurenčního boje. V tom případě se velmi uplatní další zvláštnost internetu, kterou je možnost zůstat v anonymitě nebo dokonce pod cizím jménem. To nabízí široké pole možností pro očernění reputace konkurentů a očernění kvality jejich výrobků a služeb. [1] Velké problémy působí zejména dlouhodobost „života“ informace. V době, kdy internet nebyl v každé kavárně a informace se šířily pouze tiskem, se i pomluva za krátký čas „vypařila“. Jenže v hlubinách internetu lze relativně snadno najít pomluvy, lži a polopravdy, které tam někdo uložil již před mnoha lety. A ovlivňují chování zákazníků, dodavatelů, úředníků…

Jestliže proti prvním třem druhům internetových útoků (které již byly zmíněny dříve) existují a stále se rozvíjejí technické prostředky obrany, jestliže hackerství a zpronevěra obchodních informací podléhají ve většině civilizovaných zemí trestní odpovědnosti, tak bohužel útoky na reputaci a image většinou zůstávají nepotrestané. Přitom takové útoky přinášejí zpravidla nenapravitelnou škodu dobrému jménu podniku, která se prakticky bezprostředně projeví v obrovských finančních ztrátách a která podnik může dovést až k bankrotu.

Praktická část této práce proto sestává z mnohostranného popisu možných internetových útoků na image a dobrou pověst, odvození originálního postupu pro ocenění možných škod a jejich porovnání s konkurencí, a sestavení metody identifikace útočníka nebo jeho společníků. A také nabízí přehled hlavních zákonů, které mohou v tuzemsku pomoci při obraně proti takovým útokům. Na závěr bude navržen další možný postup pro hlubší poznání dané problematiky a orientační návrh pravidel a metod obrany před internetovými útoky na image a reputaci.

II. PRAKTICKÁ ČÁST

3. Zkoumaní útoků na dobrou pověst a zjištění způsobů obrany

3.1. Monitoring internetu

Základním úkolem obrany proti internetovým útokům na image a reputaci podniků je, takový útok odhalit co nejdříve. Jakmile se informace začne lavinovitě šířit, je jakákoliv obrana velmi ztížená a spíše než o obranu by už šlo pouze o zmírňování škod.

Jako preventivní opatření postačuje, věnovat se analýze rizika těchto útoků jen zhruba jednou týdně, přičemž zpravidla postačuje, budeme-li se vyhledávání útoků věnovat tak nanejvýš jednu až dvě hodiny.

Vyhledávání se provádí jednoduše, do vyhledávačů (seznam, google) vložíme název podniku či název produktu (výrobku nebo služby) a sledujeme, jaké informace budou zobrazeny. Nejspíše najdeme vlastní webovou stránku a internetové obchody (pokud nabízejí naši produkci). Ale možná najdeme i stránky s informacemi, které mohou škodit.

Pokud weby se škodlivými informacemi, budou umístěny na prvních pěti místech ve výsledcích hledání, můžeme předpokládat, že 99 % uživatelů zadávajících ve vyhledavačích název firmy nebo její produkt navštíví tyto weby a seznámí se s informacemi na nich umístěnými. Proto je velmi důležitá propagace vlastní webové stránky a také publikování článků s informacemi pozitivně ovlivňujícími image a reputaci daného podniku. Tímto postupem lze vytvořit buffer „pozitivní zóny“, které budou umístěny na prvních místech ve výsledcích hledání potřebných informací o podniku.

Pokud se zobrazí velké množství odkazů, výběr zúžíme tak, že vyhledáváme současně dvě slova - k názvu podniku či produktu přidáme slovo, které může charakterizovat postoj klientů k naší nabídce. Vhodná jsou například slova podvod, kvalita, reklamace, zkušenost…

Kromě toho má smysl se seznámit se statistickými údaji, jak časté jsou požadavky na „název firmy“ či „název produktu“. Současné vyhledávače tuto informaci sbírají a poskytují ji široké veřejnosti. Pro seznam.cz je to velice jednoduché, stačí zadat svůj požadavek ve vyhledávači a vedle výsledků vyhledávání zmačknout „Statistika dotazu“. Nebo zde lze také uvést následující URL: http://search.seznam.cz/stats?collocation=NÁZEV

Google takovou statistiku nabízí svým registrovaným uživatelům. Registrovaný uživatel ve svém účtu AddWords vybere Přehledy a nástroje > Návrhy klíčových slov. V otevřeném

formuláři si uvede požadavek, který ho zajímá, vybere region a dostane průměrné měsíční statistické údaje ohledně daného požadavku.

Statistické údaje požadavků, které obsahují název firmy/produktu, přibližně ukazují, kolik lidí, kteří znají název firmy/produktu, se zajimalo o doplňujicí informace pomocí internetu.

Vedle toho se vyplatí vyptat se u dobrých zákazníků a partnerů, aby nás informovali, kdyby se setkali s nějakými negativními informacemi o našem podniku či produktu. Ideální je, když od nich získáme přímo odkaz na webovou stránku, kde ty informace objevili.

Jakmile zjistíme, že se počet útoků zvyšuje nad přijatelnou mez, je nutné zvýšit frekvenci sledování těchto útoků, aby se na každý dalo včas správně reagovat.

3.2. Metoda posouzení škodlivosti informace

Vedle frekvence útoků musíme posoudit i míru jejich škodlivosti. Škodlivost je dána jednak škodlivým obsahem (fakta), jednak vnímáním tohoto obsahu (účinek) a dále rozsahem jeho rozšíření (dosah).

Míra škodlivosti pak určuje, nakolik je nutno se problému věnovat. Obrana musí být efektivní. Jinak řečeno, kdyby náklady na obranu měly být vyšší než způsobené škody, tak by obrana jistě vůbec neměla smysl. Ale v praxi je situace složitější. Je nutno si uvědomit, že ekonomickou škodou je i samotná obrana. Škodou totiž de facto je jak zisk, který podniku ujde v jeho obchodní činnosti, tak náklady, které vynaloží na svoji obranu. [1]

Je proto zapotřebí jednotlivé škody posoudit opravdu komplexně.

Samozřejmě jistě nikdo nepochybuje, že pokud negativní informace odradí část potenciálních zákazníků, tak se přímo úměrně sníží zisk. Skutečnost však je horší. Neplatí, že když o třetinu klesne počet zákazníků, tak o třetinu klesne zisk. Zisk klesne mnohem více, protože fixní náklady nezávisejí na odbytu.

Škodou však je i to, když dodavatelé začnou mít pocit, že náš podnik je v tísni a začnou požadovat platby předem. Škodou je v takovém případě rozdíl v časové ceně peněz. Nejlépe si to lze představit tak, jako by si podnik musel u banky půjčit potřebnou částku za běžný úrok – škodou je tento úrok.

Škodou jsou i náklady na zaučení pracovníků, které bylo nutno propustit z důvodu snížení výroby, a vyplacené zákonné odstupné. Ale i náklady na zaučení pracovníků, kteří z podniku odejdou sami, protože jim lidé v jejich okolí vyčítají, že pracují pro tak negativní podnik…

Škodou jsou i náklady na obranu – sem patří i mzdy, nájem kanceláří, pořizovací a provozní náklady technického vybavení…

Podle konkrétních podmínek konkrétního podniku se jistě objeví i možné škody další. Při tomto chápání škody je zřejmé, že jakýkoliv útok představuje jen a pouze škodu. Jediné, co můžeme, je škody minimalizovat. Měřítkem úspěchu je, zda míra škod (například poměr celková škoda / zisk + celková škoda) je nižší než u konkurence.

V tomto případě pomíjíme škody společenské, jako je zvýšená nezaměstnanost v důsledku propuštění zaměstnanců, ztráta důvěry ve schopnost státu chránit občany a podniky apod.

Nicméně, toto jsou ekonomické otázky, jejichž zodpovězení není cílem této práce. Zde pouze navrhneme zjednodušenou metodu výpočtu potenciálních ztrát způsobených publikací škodlivých informaci na internetu, které poškozují dobrou pověst a image podniku čí název produktu (výrobku nebo služby). Pro posouzení efektivnosti obrany to postačuje.

V praxi však zdaleka nestačí znát výši škody. Abychom škodu mohli v budoucnu snížit, potřebuje vědět, která informace (včetně taho, jak je zpracovaná a jak a kde je zveřejněná) působí škodlivěji a která méně. Platí-li i zde Parettův zákon, vyplatí se odhalit těch 20 % zveřejněných informací, které způsobily 80 % škod.

Škodlivým obsahem je jakákoliv informace (jak lživá, tak pravdivá), která může poškodit image a reputaci podniku. Podstatná ovšem není sama informace, ale to, jak je vnímána a jak je šířena.

Přestože je útok vedený zvnějšku, někdy se může podařit informaci otočit v náš prospěch. Pokud si zákazník veřejně stěžuje na nekvalitní výrobek, můžeme jej do dvou dnů v reklamaci opravit nebo vyměnit, a se zákazníkem dohodnout, že doplní informaci o tom, jak promptně byla jeho reklamace vyřízena. Pokud si návštěvník pivnice stěžuje na hrubiána číšníka, můžeme jinými cestami šířit informaci, jak je naše pivnice svérázná a jak nabízí zážitky, které v nudné restauraci nenajdeme…

Obvykle je ale takové „překlopení“ negativní informace v pozitivní nemožné. Je to zejména tehdy, když informace obsahuje polopravdy a lži a když je podána se silným emocionálním nábojem. Například takovýto reálný výrok, zvěřejněný na internetu o jedné nebankovní úvěrové společnosti: „Jsou to hrozný podvodníci. Půjčili mi podělaných sto tisíc. Udělali ze mne neplatiče

a jejich exekutor mi v dražbě prodal zastavený byt za milion.“ Na tomto vyjádření lze ukázat obvyklé postupy při formulování negativních informací. Autor označuje osočenou osobu negativním názvem (je to „podvodník“), působení zesiluje emocionálně negativními přívlastky („hrozný“), zaměňuje příčinu za následek („udělali ze mne neplatiče“, ačkoliv neplatiče ze sebe dlužník udělal sám) a zkresluje škody (byt byl sice prodán za milión, avšak věřitel samozřejmě dostal pouze svůj oprávněný nárok a zbytek dostal dlužník - on to ale vnímá jako ztrátu bydlení), přitom apeluje na city a na sklon lidí věřit všemožným teoriím o komplotech (naznačuje cosi jako „mají svého exekutora a ten zařídil, aby mne okradli o milion“). [18]

Lze změřit účinek takové informace, tj. jak tato informace působí? Částečně ano. V úvahu připadají zejména dvě metody, měřením důsledků a měřením vnímání. V prvním případě můžeme porovnat počet zákazníků, obrat či jinou vhodnou veličinu před zveřejněním takové informace a po určité době po zveřejnění. Problémem této metody je, že pokles počtu zákazníků nemusí záviset jen na této jedné škodlivé informaci. Ve druhém případě můžeme provést jednoduchý průzkum některou z metod, které se používají při sociologických průzkumech (na reprezentativním vzorku osob, které patří co cílové skupiny, provedeme dotazování, jak na ně informace působí). Můžeme tak zjistit, jaká část cílové skupiny informaci nekriticky podlehne, jaká se jí nedá ovlivnit, protože ji bude chápat jako výlev neplatiče, a jaká si začne vše prověřovat ještě z jiných zdrojů. V tomto druhém případě pak zjištěnou míru účinku musíme přepočítat podle toho, jaká se vnímaná serióznost místa, kde je informace zveřejněna. Tato druhá metoda je samozřejmě teoreticky mnohem správnější než první. [2] V praxi to však pravděpodobně vyjde nastejno, protože nakonec vždy půjde o hrubé odhady, jen ve druhém případě dražší.

Mezi základní parametry, které mají vliv na celkovou škodlivost informace, patří ještě její dosah, její rozšíření. Můžeme sledovat, na kolika různých místech byla škodlivá informace rozmístěna, jaká je návštěvnost takových míst a jaký je podíl cílové skupiny na celkové návštěvnosti. V neposlední řadě je zapotřebí sledovat časové řady všech sledovaných hodnot.

Posouzením všech těchto údajů můžeme kvalifikovaně odhadnout, kde vznikají největší škody, a můžeme se soustředit na jejich eliminaci.

3.3. Šíření škodlivé informace z hlediska porušení nebo nesplnění zákonů

Z hlediska platných zákonů je důležité identifikovat, kdo škodlivou informaci zveřejňuje. Zda konkurent, nebo někdo jiný (nekonkurent - zpravidla klient). Pro účely této části práce budeme předpokládat, že útok je veden na právnickou osobu (dále též osočená osoba).

Zveřejňuje-li negativní informaci nekonkurent, půjde o porušení dobrého jména osočené právnické osoby. Ta ochranu nalezne zejména v následujících ustanoveních občanského zákoníku:

Obecné klauzule jsou v § 3, odst. 1, a v § 415: Výkon práv a povinností vyplývajících z občanskoprávních vztahů nesmí bez právního důvodu zasahovat do práv a oprávněných zájmů jiných a nesmí být v rozporu s dobrými mravy. Každý je povinen počínat si tak, aby nedocházelo ke škodám na zdraví, na majetku, na přírodě a životním prostředí. [19]

Tématu této práce se konkrétně týká § 19b, odst. 2, spolu s odst. 3: Při neoprávněném zásahu do dobré pověsti právnické osoby je možné se domáhat u soudu, aby se zasahující zdržel dalšího zásahu a odstranil závadný stav; je možné se též domáhat přiměřeného zadostiučinění, které může být požadováno i v penězích. [19]

Zásahem do dobrého jména právnické osoby může vzniknout škoda. V takovém případě se lze domáhat její náhrady podle § 420 a násl, občanského zákoníku. Podle § 442 se hradí skutečná škoda i to, co poškozenému ušlo (ušlý zisk). Škoda se zpravidla hradí v penězích; požádá-li však o to poškozený a je-li to možné a účelné, hradí se škoda uvedením do předešlého stavu. [19]

Pro úplnost poznamenejme, že v případě podnikající fyzické osoby by šlo o neoprávněný zásah do její osobnosti, která je chráněna jinými ustanoveními občanského zákoníku.

Zveřejňuje-li negativní informaci konkurent, může jít také buď o porušení dobrého jména osočené právnické osoby, nebo o porušení ustanovení obchodního zákoníku o nekalé soutěži:

§ 44, odst. 1: Nekalou soutěží je jednání v hospodářské soutěži nebo v hospodářském styku, které je v rozporu s dobrými mravy soutěže a je způsobilé přivodit újmu jiným soutěžitelům, spotřebitelům nebo dalším zákazníkům. Nekalá soutěž se zakazuje. [20]

V případech studovaných v této práci přichází do úvahy zejména porušení § 45 (klamavá reklama) a porušení § 50 (zlehčování).

§ 45: Klamavou reklamou je šíření údajů o vlastním nebo cizím podniku, jeho výrobcích či výkonech, které je způsobilé vyvolat klamnou představu a zjednat tím vlastnímu nebo cizímu podniku v hospodářské soutěži nebo v hospodářském styku prospěch na úkor jiných soutěžitelů,

spotřebitelů nebo dalších zákazníků. Klamavým je i údaj sám o sobě pravdivý, jestliže vzhledem k okolnostem a souvislostem, za nichž byl učiněn, může uvést v omyl. Za šíření údajů se považuje sdělení mluveným nebo psaným slovem, tiskem, vyobrazením, fotografií, rozhlasem, televizí či jiným sdělovacím prostředkem. [20]

§ 50: Zlehčováním je jednání, jímž soutěžitel uvede nebo rozšiřuje o poměrech, výrobcích nebo výkonech jiného soutěžitele nepravdivé údaje způsobilé tomuto soutěžiteli přivodit újmu. Zlehčováním je i uvedení a rozšiřování pravdivých údajů o poměrech, výrobcích či výkonech jiného soutěžitele, pokud jsou způsobilé tomuto soutěžiteli přivodit újmu. Nekalou soutěží však není, byl-li soutěžitel k takovému jednání okolnostmi donucen (oprávněná obrana). [20]

Právní prostředky ochrany proti nekalé soutěži jsou pak uvedeny v § 53: Osoby, jejichž práva byla nekalou soutěží porušena nebo ohrožena, mohou se proti rušiteli domáhat, aby se tohoto jednání zdržel a odstranil závadný stav. Dále mohou požadovat přiměřené zadostiučinění, které může být poskytnuto i v penězích, náhradu škody a vydání bezdůvodného obohacení. [20]

Porovnáme-li výčet možností obrany u nekalosoutěžního jednání a u zásahu do dobré pověsti právnické osoby, je zřejmé, že nekalosoutěžní jednání je na obranu proti jednání konkurenta „výhodnější“, protože nabízí více možností nápravy. Ale skutečnost bude v praxi stejně tristní. Než je soudem rozhodnuto a než je rozhodnutí vymoženo, osočená společnost bude nejspíš nevratně poškozena a ani vymožené zadostiučinění jí její pozici na trhu nevrátí. Ale ještě pravděpodobněji se stane, že škůdce včas připraví situaci tak, aby nemusel nic zaplatit (úpadek).

V praxi navíc obvykle nelze odlišit, zda negativní informace šíří konkurent či nespokojený klient, neboť i informace šířené konkurentem jsou zpravidla zveřejňovány anonymně (pod smyšleným jménem) a tváří se jako názor poškozených klientů. Jak jsme ale ukázali, odlišení má zásadní význam pro případnou obranu, pokud bychom ji chtěli vést na úrovni původce škodlivé informace.

Nabízí se však ještě jedna cesta. Vzhledem k tomu, že škodlivé informace zpravidla nezvěřejňuje a nešíří konkrétní osoba, ale nějaké medium (tisk, rozhlas, televize, internetový server), platné zákony na ně přenášejí část odpovědnosti.

Odpovědnost za obsah tištěného média nese vydavatel (§ 4 tiskového zákona č. 40/2000 Sb.) a osočená osoba se může domáhat odpovědi a dodatečného sdělení (§ 10 - 15). Ochranu poskytuje soud. Je zapotřebí ještě uvést, že tištěná média dle § 16 tiskového zákona chrání zdroj informací. Jinak řečeno, osočené osobě jsou zde kladeny překážky při určení, zda původcem negativní informace je konkurent či nekonkurent. Obdobně je řešena ochrana osob osočených v televizním nebo rozhlasovém vysílání, konkrétně zákonem č. 231/2001 Sb. o provozování

rozhlasového a televizního vysílání a o změně dalších zákonů, a to zejména v hlavě II. I zde jde o právo na odpověď a dodatečné sdělení (§ 35 - 40), i zde se osočená osoba bude potýkat s ochranou zdroje informace (§ 41). [21]

U elektronických médií je ochrana práv osočovaných osob řešena zákonem o některých službách informační společnosti č. 480/2004 Sb. Klíčový je § 5, podle kterého poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele jen, a) mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo b) dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.

Situace se dále komplikuje, je-li poskytovatel služby reálně či formálně v zahraničí. Informaci o protiprávnosti zveřejněných negativních informací obvykle nelze zaslat poštou jako český dopis. Narážíme na problém doručování písemností, kdy místní orgány zpravidla vyžadují specifický způsob doručení (obvykle musí jít o doručení prostřednictvím soudů a písemnosti musejí být v místním jazyce).

V neposlední řadě problémy při ochraně dobrého jména jistě vytušíme také v tom, že hranice mezi „klasickými médii“ (tisk, rozhlas, televize) a „novými médii“ (servery, chaty atd.) je dnes dosti nejasná, neboť obsah tištěných médií bývá překlápěn na webové stránky, rozhlasové i televizní vysílání bývá také dostupné prostřednictvím internetu…

Trestní odpovědnost je velmi diskutabilní. Dokonce se může zdát, že poškozením dobrého jména nedochází k trestnému činu, i když je způsobená škoda velmi vysoká. [22]

Trestní zákoník (zákon č. 40/2009 Sb.) zná několik trestných činů, které by se mohly při vhodné interpretaci týkat poškození dobré pověsti osočené právnické osoby.

Konkrétně § 181 o poškození cizích práv ustanovuje, že „kdo jinému způsobí vážnou újmu na právech tím, že a) uvede někoho v omyl, nebo b) využije něčího omylu, bude potrestán...“ Přirozená interpretace zní, že kdosi někomu způsobí vážnou újmu tím, že toho někoho uvede v omyl. Čili přímý vztah škůdce a poškozený. Potřebná interpretace by ale byla, že kdosi (zveřejňovatel negativní informace) způsobí újmu osočené osobě tím, že její potenciální klienty uvede v omyl… Autorovi této práce není známo, že by uvedené ujednání bylo takto vykládáno. [23]

Dále by mohl přijít v úvahu § 184 o pomluvě, že „kdo o jiném sdělí nepravdivý údaj, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu, bude potrestán…“. [23] Přirozená interpretace zní, že pomluvena může být pouze fyzická osoba, kterou lze poškodit v zaměstnání, které lze narušit rodinné vztahy apod. Potřebná interpretace by ale byla, že kdo o jiném (o osočené právnické osobě) sdělí nepravdivý údaj, který je způsobilý způsobit mu jinou vážnou újmu… Autorovi této práce není známo, že by uvedené ujednání bylo takto vykládáno.

Pro případ, že by šiřitel negativních informací byl odsouzen k náhradě škody a k zaplacení zadostiučinění, ale ten by s předstihem převedl majetek na jinou osobu a sám skončil v úpadku, by se jistě dala uplatnit například ustanovení trestního zákoníku o podvodu či předlužení, ale v praxi se tak asi nestane. A to jak z důvodu promlčení, tak prostě proto, že je to jen další zátěž osočené osoby a ta si takový postup rozmyslí jako neefektivní.

Je zřejmé, že jediný jasný trestný čin dotýkající se předmětu této práce je obsažen v § 248 o porušení předpisů o pravidlech hospodářské soutěže. Toto ustanovení trestního zákoníku v odst. 1 uvádí, že „kdo poruší právní předpis o nekalé soutěži tím, že se při účasti v hospodářské soutěži dopustí a) klamavé reklamy, /…/ f) zlehčování, /…/, a způsobí tím ve větším rozsahu újmu jiným soutěžitelům nebo spotřebitelům nebo opatří tím sobě nebo jinému ve větším rozsahu neoprávněné výhody, bude potrestán…“ [23]

3.4. Praktický případ

Autor této práce spolupracuje s úvěrovou společností 1. faktorská s.r.o., o které se na různých serverech šíří v podstatě stejné negativní informace. Nezřídka opravdu jeden nespokojený klient zveřejňuje naprosto identický text (kopíruje jej na různé servery). Společnost z analýzy zveřejněného textu zjistila, kdo je jeho pravděpodobným původcem, ale bohužel to nelze průkazně dokázat. Dotyčný se zpočátku dopustil chyby a v prvním příspěvku uvedl své pravé iniciály, dále iniciály právníka a požádal „ostatní poškozené“, aby se sním spojili, a uvedl spojení. Společnost se dopustila chyby a vyzvala ho, aby se tohoto jednání zdržel a závadný příspěvek odstranil. On tak neučinil, ale objevil se nový člověk s vymyšleným jménem, který stejným stylem píše stejné texty a z některých detailů lze vyvodit, že jde o stále stejného nespokojeného klienta. Tímto krokem se společnost fakticky zbavila šance, dosáhnout v brzké době odstranění jeho pomlouvačných příspěvků.

Společnost se proto nakonec rozhodla, že se nebude pokoušet o náhradu škody od viníka (tím spíše, že jde o důchodce), ale že využije částečný přenos odpovědnosti na provozovatele serverů, kde dotyčný své texty zveřejňuje.

Společnost proto nejprve provozovatele uvedených serverů podle zákona č. 480/2004 Sb., (zákon o některých službách informační společnosti) doporučeným dopisem upozornila:

„V rámci diskusních příspěvků umístěných na internetové adrese (URL) http://www.***.cz je publikována řada nepravdivých tvrzení týkajících se naší společnosti, která jsou způsobilá značnou měrou poškodit naši vážnost a způsobit nám značné škody, a která tak představují neoprávněný zásah do naší dobré pověsti ve smyslu ustanovení § 19b odst. 3 zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.

Z ustanovení § 5 odst. 1 písm. b) zákona o některých službách informační společnosti vyplývá, že pokud se poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, prokazatelně dozví o protiprávní povaze obsahu, je povinen neprodleně učinit veškeré možné kroky, které po něm lze požadovat, vedoucí k odstranění či znepřístupnění takovéhoto obsahu.

Doručením této výzvy jste tedy prokazatelně informováni o protiprávním obsahu uvedených příspěvků, a tím na Vás přechází odpovědnost za jejich obsah a povinnost je odstranit či alespoň znepřístupnit.

S ohledem na shora uvedené skutečnosti Vás tímto vyzýváme, abyste příspěvky (které byly publikovány ze strany uživatelů Vašich služeb) z Vašich webových stránek neprodleně odstranil nebo alespoň znepřístupnil. Nebude-li této naší výzvě vyhověno, budeme nuceni domáhat se ochrany své dobré pověsti všemi dostupnými právními prostředky.“

Protože žádný z provozovatelů dotčených serverů nevyhověl, společnost podala (v podstatě opět shodné) Návrhy na vydání předběžného opatření ve věci ochrany dobré pověsti právnické osoby:

„Je zřejmé, že uveřejněné příspěvky mají velmi závažný negativní dopad na dobrou pověst žalobce. Žalobci v důsledku protiprávního jednání žalovaného spočívajícího v uveřejňování závadných příspěvků nepochybně vznikla značná újma, přičemž je možné dokonce říci, že je takovým jednáním bezprostředně ohroženo podnikání žalobce, neboť žalobce nabízí své služby a vyhledává nové zákazníky hlavně právě prostřednictvím internetu. Ohledně rozsahu poškození svých práv si žalobce dovoluje poukázat na počet shlédnutí předmětných diskusních příspěvků,

když např. na internetových stránkách www.***.cz je u citovaného diskusního příspěvku uvedeno, že byl od doby svého uveřejnění přečten již 9.195x.

Vzhledem k tomu, že předmětné diskusní příspěvky jsou stále zcela přístupné, je důvodné se domnívat, že celková újma způsobená žalobci bude dále narůstat.

Žalobce má za to, že vzhledem k povaze zásahů do jeho práv je zapotřebí rychlé a účinné ochrany těchto práv, když nelze vyčkávat do doby, než bude meritorně rozhodnuto ve věci samé, neboť jen včasným poskytnutím ochrany práv žalobce je možné zabránit dalším nepříznivým následkům protiprávního jednání žalovaného. Dle žalobce je tak v tomto případě nepochybně naplněn předpoklad naléhavosti (nezbytnosti) úpravy poměrů předběžným opatřením. Navrhovaným předběžným opatřením by soud nepředjímal pravomocné rozhodnutí ve věci samé, neboť v případě vyhovění návrhu na vydání předběžného opatření by se jednalo pouze o dočasné, nikoliv trvalé odstranění části obsahu webových stránek. Žalobce v této souvislosti odkazuje na rozhodnutí Vrchního soudu v Praze ze dne 16.06.1995, sp. zn.: 3 Cmo 1952/94, podle kterého: „Zásada, že není přípustné, aby již předběžným opatřením dosáhl oprávněný toho, čeho lze dosáhnout až pravomocným rozsudkem ve věci po proběhlém řízení (a dokazování), se nepoužije v případech předběžného opatření směřujícího k zákazu určitého jednání a žaloby o zdržení se tohoto jednání, jež naplňuje znaky jednání nekalé soutěže. Rozhodné je zde hledisko zabránění vzniku, popř. rozšiřování újmy dotčeného účastníka.“ Žalobce má za to, že tyto závěry lze vztáhnout na jeho případ, když institut ochrany dobré pověsti právnické osoby je velmi příbuzný institutu ochrany proti nekalosoutěžnímu jednání, a rovněž nároky, které lze uplatňovat, jsou velmi podobné.“

Je zajímavé, jak různě se příslušné soudy zachovaly, ačkoliv návrh byl fakticky tentýž (měnili se jen provozovatelé serverů):

- Krajský soud v Ústí nad Labem samosoudcem JUDr. Michalem Mědílkem návrhu nevyhověl, neboť prý nebyly splněny všechny náležitosti takového návrhu.
- Krajský soud v Ostravě samosoudkyní JUDr. Annou Řehákovou druhému návrhu vyhověl. Soud přisvědčil žalobci, „že jím popsaná situace v návrhu na nařízení předběžného opatření, osvědčená k návrhu připojenými listinami, vyžaduje zatímní úpravu poměrů účastníků ve smyslu § 74 odst. 1 o.s.ř.“ Soud proto návrhu vyhověl s tím, že podle ustanovení § 169 odst. 2 o.s.ř. se upouští od jeho odůvodnění.
- Krajský soud v Hradci Králové - pobočce Pardubice samosoudkyní Ing. Mgr. Evou Poláčkovou návrh zamítnul. Soud se „musel zabývat a zabýval otázkou svobody projevu uživatelů vyjadřovat své názory, a jednak na druhé straně intenzitou bezprostředního

> ohrožení, zamezení vzniku škody či jiné újmy na straně žalobce. /…/ Žalobce požadoval tímto návrhem odstranit dosud publikovaná vyjádření z webových stránek, aby bylo zamezeno újmě a ohrožení jeho podnikání, musí si být ale též vědom skutečnosti, že neovlivní případné další příspěvky týkající se žalobce. /…/ Soud má za to, že vyjádření uživatelů o žalobci neobsahují naprosto hrubá a vulgární vyjádření, kdy by soud zvažoval a neviděl by jediný důvod pro upřednostnění svobody projevu před naprosto zjevným překročením hranic a mezí obecně uznávaných pravidel slušnosti, a neodstraněním ve výroku citovaného diskusního příspěvku. Soud chápe, že vyjádření uživatelů o žalobci se tomuto nelíbí a nesouhlasí s nimi, ale soud v tomto případě na základě shora uvedeného i vzhledem ke konkrétním okolnostem musí dát zamítnutím návrhu na vydání předběžného opatření přednost svobodě projevu, právu vyjadřovat názory s tím, že v daném případě nebylo prokázáno, že je třeba, aby byly zatímně upraveny poměry účastníků."

Uvedený příklad ukazuje, jak obtížné je bránit se zveřejňování negativních informací, a jak obtížné je zastavit způsobované škody.

Pardubická soudkyně zjevně vůbec nechápe, jaké škody tyto pomluvy působí. Mnoho potenciálních klientů si krátce před podpisem smlouvy úvěr rozmyslelo právě s poukazem na to, že se dočetli o „podvodných praktikách mafiánů z 1. faktorské". Přitom společnost 1. faktorská je bezpochyby jedna s nejslušnějších nebankovních úvěrových společností na českém trhu (jedny z nejnižších úroků, žádné poplatky, záruka tříměsíčního odkladu splátek v případě osobních potíží atd.) a jistě se nemýlím, když se domnívám, že zájemce o úvěr skončil v tenatech mnohem horší úvěrové společnosti. Soudkyně tím v první řadě ublížila těmto potenciálním klientům.

Společnost 1. faktorská se přitom setkala i s takovým jednáním, kdy si potenciální klient z Moravy nechá připravit všechny smlouvy (vytíží tím na několik hodin člověka z obchodního oddělení a člověka z právního oddělení) a nechá si je vysokoškolsky vzdělaným makléřem přivézt na prezentaci a na podpis přes půlku republiky k sobě domů (to je bezplatná služba této společnosti). A doma tomu makéři oznámí, že si to rozmyslel. Už před několika dny. Ale neřekl to, protože chtěl společnost potrestat, neboť si přečetl, že to jsou podvodníci…

Společnost 1. faktorská měla v prvních 3/4 roku 2010 přibližně 250 nových klientů. Po spuštění kampaně dvou klientů měla za poslední čtvrtletí pouze cca 50 nových klientů. Tj. ztratila přibližně 35 klientů, které by asi měla, kdyby tato kampaň nebyla spuštěna. Průměrný příjem (tržba) od jednoho klienta činí 150.000,-- Kč, tj. ztráta na tržbách jen za jedno čtvrtletí je více než 5.000.000,-- Kč (to není zisk, ale tržba; průměrný zisk na klienta mi není znám).

Uvedené pomluvy jsou na internetu stále k vidění a počet nových klientů stále mírně, ale vytrvale klesá.

Za zmínku stojí i skutečnost, že mnozí klienti, kteří až dosud řádně spláceli, se šířenými pomluvami polekali a rozhodli se úvěr předčasně splatit. I v tomto případě se jistě nemýlím, když se domnívám, že tito klienti si na výplatu úvěru půjčili u mnohem horší úvěrové společnosti, za vyšší úrok a při tvrdších podmínkách splácení. Tato pardubická soudkyně tak ublížila i těmto dosud spokojeným klientům.

Pokud sečteme všechny uvedené škody, snad budete s autorem této práce souhlasit, že pouhé pochopení soudkyně, že se šířené lži společnosti 1. faktorská nelíbí, je zcela neadekvátní škodám, které svým rozhodnutím způsobila.

3.5. Způsoby zjištění autora a osob podílejících se na šíření informace

V uvedeném praktickém případu byla zmínka o tom, že se společnosti 1. faktorská podařilo zjistit jednoho z autorů nejvíce pomlouvačných zpráv. Problematice jejich zjišťování se nyní budeme věnovat hlouběji.

Před tím, než začneme rozvíjet účinné metody obrany proti internetovým útokům na pověst a image firmy, je nutné určit osoby odpovědné za tyto útoky. Vzhledem k takové vlastnosti internetu, jako je anonymita uživatelů, zjištění osob není jednoduché. Ale můžeme navrhnout některé způsoby, které mohou pomoci identifikovat útočníky nebo spolupachatele útočníků.

Samozřejmě, pokud škodlivé informace jsou zveřejněny na stránkách konkurentů, nebo na osobním účtě na Facebook, není již nutné určovat odpovědnou osobu, protože útočník je známý a je jasné, proti komu se bránit. Tato kapitola popisuje metodiku pro určení osoby odpovědné za případ, kdy škodlivé informace jsou umístěny na neutrálním webu jako jsou fóra, analytické stránky, falešné účty na Facebook a další.

3.5.1. Analýza zveřejněného textu

Někdy lze ze zveřejněné škodlivé informace autora jednoznačně identifikovat. Stačí jen důkladně se s obsahem textu seznámit. Pokud se ve škodlivém textu podrobně popisuje nějaká ojedinělá situace, je možné určit autora na základě těchto údajů a okolností této situace. Nebo

situace nebyla až tak ojedinělá, ale jejím filtrováním přes další zjištěné informace se ojedinělou stane (situace se sice stala vícekrát, ale autor škodlivého textu uvedle své křestní jméno, a to již autora přesně identifikovalo)

Nicméně takové jednoduché zjištění bude dosti vzácné. Kromě toho bude neprokazatelné, pokud celá věc půjde k soudu. Soudu asi nebude stačit tvrzení, že v našem hotelu v posledním roce na pokoji 13 byl jeden jediný klient, kdy praskla žárovka a sklo z ní něco poničilo. Soud bude chtít prokázat, že opravdu nikdo jiný takový nebyl. Ale jak prokážete, že něco nebylo? Jinak řečeno, naše jistota bude pro ostatní nejistotou, a může nám sloužit nanejvýš jako prvotní poznatek o útočníku.

Ve většině případů identifikovat autora textu škodlivé informace není možné. Ale pro uspěšnou obranu proti útokům na dobrou pověst nám zpravidla stačí určit kontakní údaje vlastníka či provozovatele domény nebo hostingu. Dle § 5 bodu „b" zákona o některých službách informační společnosti č. 480/2004 Sb., poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem (čili majitel webové stránky, majitel domény nebo hostingu), odpovídá za obsah informací uložených na žádost uživatele, když se prokazatelně dozví o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele. A musí neprodleně učinit veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací. [22]

Proto lze otázku o určení autora škodlivé informace přeformulovat na otázku určení osob odpovědných za zveřejnění škodlivé informace. Na tuto druhou otázku lze odpověď najít mnohem jednodušeji.

3.5.2. Analýza webové stránky

Informace o provozovateli webu často bývá uváděna přímo na webu na stránce „O nás" či „Kontakt". Je ale pravdou, že webové stránky, vytvořené speciálně pro šíření pomluv, údaje o provozovatelích neposkytují.

Někdy lze provozovatele „pomlouvačné webové stránky" zjistit z nepřímých náznaků. Typickým případem je, když web poskytující prostor pro kritiku hotelových služeb sice provozuje „bílý kůň" (nastrčený bezdomovec), ale ve skutečnosti je z pozadí řízen vlivným konkurentem. Pokud je na takovém webu podezřele málo kritiky hotelů konkurenta, můžete vytušit, odkud vítr vane.

Weby někdy umožňují korespondencí přes své komunikační rozhraní. I to může být cesta ke zjištění vlastníka nebo provozovatele.

Speciálním případem analýzy webové stránky je analýza cizích webových stránek. Když k nalezení provozovatele na dané webové stránce nic nepomáhá, tak se někdy vyplatí porozhlédnout po celém internetovém prostoru. Vlastník webové stránky třeba v době jejího počátku poskytl reklamní rozhovor, a ten je v hlubinách internetu stále ještě k přečtení. A i když se třeba vlastník změnil, tak ten nový by měl něco vědět o tom minulém. Jindy zjistíte, že v minulosti již po majiteli pátralo více lidí, a někdo z nich ho třeba nalezl. A tak podobně. Chce to jen čas a kreativitu při hledání.

3.5.3. Technické možnosti zjištění majitelů webu / domeny / hostingu

Ale praxe ukazuje, že většina fór, které jsou speciálně navrženy pro pomluvy, nezahrnují kontaktní informace, stejně jako nezahrnují informace o majiteli tohoto webu. V takovýchto případech můžeme zjistit majitele domény, který je buď vlastníkem webu, nebo předal práva pro správu webu třetí straně. V každém případě, vlastník domény se vpředu popsaným postupem může stát osobou odpovědnou za obsah textů na webových stránkách na určité doméně.

Kontakty na hostingovou společnost webu, která obsahuje pomlouvačné informace, také mohou být užitečné. Velcí poskytovatelé hostingu pečují o svou pověst a nechtějí být spojováni se soudními jednáními ohledně protiprávních informací zveřejněných na svých serverech.

Na internetu je ohromné množstvi užitečných služeb, které umožňují zjistit podrobnou informaci o doménách (WHOIS služba), jako například jsou:

- http://whois.domaintools.com/
- http://www.whois.net/whois/
- http://www.domena.cz/whois.html

Pomoci těchto služb jsme schopni zjistit informaci o vlastníkovi domény, o jejím registrátoru a o datu registrace doménových jmen, či o hostingu webových stránek (DNS záznamy ukazují na adresu hostingu).

Také mohou být užitečné informace o IP adrese domény, které lze nalézt pomocí následujících služeb:

- http://domaintoip.com
- http://whois.czechlinux.info

Všechny výše uvedené služby nám umožňují identifikovat osoby, které jsou odpovědné za šíření škodlivých informací (nebo nám umožní identifikovat osoby, které znají osoby odpovědné za šíření škodlivých informací), což je nepochybně velmi důležité pro úspěšnou obranu proti útokům na dobrou pověst podniku nebo na jeho produkty.

Závěr: Systematizace možností obrany a záměr na pokračování práce

Je zřejmé, že internet je fenomén, se kterým si společnost neví příliš rady. Přinesl mnoho pozitiv, ale také nová rizika, které zdaleka nejsou jen teoretická. Škody, vzniklé jeho využitím (či vlastně zneužitím) jsou naprosto mimořádné, a přitom jen těžko měřitelné.

Rozsáhlé jsou jak útoky na technické prostředí, tj. na hardware i software (například viry, trojské koně…), tak krádeže informací a jejich následné zneužití (phishing, sociální inženýrství…), i šíření informací škodících image a dobré pověsti (a následné ztráty, například na zisku). Narůstají také obavy z možného zneužití informací zveřejňovaných na komunitních serverech (zde nejde o krádež, neboť původně byly informace zveřejněny dobrovolně).

Možnosti obrany jsou jen omezené, tak jako ostatně u většiny možných útoků i v jiných oblastech života společnosti.

1) Osvěta. Výchova k obezřetnému chování v síti.

2) Obrana za využití technických prostředků (antivirové programy, firewolly, šifrování …).

3) Zpracování krizových postupů pro případ úspěšného útoku a jejich technické zajištění (duplikace uložených informací, náhradní servery…).

4) Proti škodám vznikajícím ze šíření škodlivých informací lze užít řadu specifických metod, legálních i nelegálních, například:

- připojování odpovědí, komentářů (pokud to je umožněno)
- ředění informací (zřízení podobně orientovaných webových stránek, kde je sice prostor pro hanění všech, ale s řízením informací o sobě, takže jde de facto o hanění konkurence)
- právní postupy vůči poskytovatelům informačních služeb, pokud je založena jejich odpovědnost
- právní postupy vůči šiřitelům škodlivých informací, pokud se je podaří jednoznačně identifikovat
- technické útoky na servery poskytující prostor šiřitelům škodlivých informací.

Při přípravě této práce se ukázalo, že zatímco ochraně proti útokům na technické prostředí a ochraně proti krádežím a zneužívání informací se věnuje velká pozornost, útokům na image a reputaci jen velmi malá. Z praxe vím, že v této oblasti také vznikají mimořádně velké škody, a přesto vlastně neexistují účinné možnosti ochrany. Další práce by se proto měla zaměřit tímto

směrem. Jejím obsahem by měla být analýza toho, jak škodlivé informace působí, a jak změřit ekonomické škody, které v jejich důsledku vznikají. Dále by měla shrnout možné metody obrany. A nakonec by měla na modelovém případě vytvořit manuál účinných reakcí na vybrané možné situace.

Použitá literatura

[1] BRABEC, František. *Technologie detektivních cinností.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíne, 2009. 160 s.

[2] BRABEC, František. *Konkurencní zpravodajství.* Prezentace pro konference Tovek, 2003. 20 s.

[3] Statistická data z serveru Internet World Stats: http://www.internetworldstats.com

[4] Statistická data z serveru NetMonitor - SPIR - Mediaresearch & Gemius: http://www.netmonitor.cz

[5] Statistická data z serveru Netcraft: http://www.netcraft.com

[6] Statistická data z serveru IGNUM s.r.o.: http://www.domena.cz/statistics.html

[7] Statistická data z serveru Ponemon Institute: http://www.ponemon.org

[8] Hanák, I.: Moderní počítačové viry. 2. vyd. Brno, Computer press, a. s. 2001. ISBN 80-7226-402-8

[9] Stuart McClure, Saumil Shah and Shreeraj Shah: Web Hacking: Attacks and Defense. Addison-Wesley, 2002. ISBN 0201761769

[10] N. G. Miloslavskaja, A. I. Tolstoj: Интрасети: обнаружение вторжений. Учебное пособие для вузов. (Intranet: detekce průniku. Učebnice pro vysoký školy). Moskva. 2001

[11] Článek Levin's Case, the Missing Chin. Provider.net.ru: http://www.providernet.ru/article.37.php

[12] Článek Hackerův útok na LiveJournal: http://www.digit.ru/internet/20110330/381433796.html

[13] Wikipedia, článek Denial of Service: http://cs.wikipedia.org/wiki/Denial_of_Service

[14] Wikipedia, článek Phishing: http://en.wikipedia.org/wiki/Phishing

[15] Článek Rhybaření střídá pharming: http://www.lupa.cz/clanky/rhybareni-strida-pharming

[16] Hermansson M. & Ravne R.: Fighting Social Engineering. University of Stockholm / Royal Institute of Technology, March 2005.

[17] Statistická data a prognóz ze serveru Magnaglobal: http://www.magnaglobal.com

[18] Realní příklád web-útoku na dobrou pověst, zveřejní na web-stránce: http://www.podvodnefirmy.cz

[19] Občanský zákoník ČR

[20] Obchodní zákoník ČR

[21] Tiskoví zákon č. 40/2000 Sb.

[22] Zákon o některých službách informační společnosti č. 480/2004 Sb.

[23] Trestní zákoník ČR