

Bezpečnosť počítačov a internetu

dokument k besede organizovanej
Bratislavskou miestnou skupinou Mensy Slovensko

Mag. Martin Matuška

12. októbra 2005

Obsah

1 Úvod	1
1.1 Základné pojmy	1
1.2 Čo sa môže stať	2
1.3 Ktoré tretie osoby nás ohrozujú	2
2 Bezpečnosť počítača	2
2.1 Malware	3
2.1.1 Programy implantované u užívateľa	3
2.1.2 Pomôcky, ktoré používa útočník	3
2.2 Prevencia a obrana proti Malware	3
2.2.1 Zásady používania	4
2.2.2 Softvérové pomôcky	4
2.2.3 Hardvérové pomôcky	5
3 Nevyžiadaná pošta a zavádzanie užívateľa	5
3.1 Obsah nevyžiadanych správ	5
3.2 Typy nevyžiadanej pošty podľa média	6
3.3 Boj proti spamu	6
3.3.1 Blacklisty	6
3.3.2 Spamové filtre	6
3.4 Phishing a pharming	7
4 Bezpečnosť komunikácie	7
4.1 Únik informácií tretím osobám	7
4.2 Zabezpečenie komunikácie	8
4.3 Bezdrátové siete	9
5 Záver	9

1 Úvod

Bezpečnosť počítačov a komunikácie medzi nimi hrá v dnešnej dobe dôležitú rolu. Veľa užívateľov nie je dostatočne informovaných o rizikách, ktoré vznikajú používaním počítačov a internetu. Cieľom tejto besedy je uviesť účastníkov do problematiky, dať im krátky prehľad oboch strán boja proti zneužívaniu, ktoré sa na internete denno-denne odohráva.

1.1 Základné pojmy

Vysvetlenia nasledujúcich pojmov slúžia pre účely tohoto dokumentu.

- **Bezpečnosť počítača** je úroveň ochrany počítačového systému pred výpadkom, manipuláciou a nedovoleným prístupom.
- **Bezpečnosť dát** je úroveň ochrany dát pred zmazaním, poškodením a manipuláciou.

- **Bezpečnosť dátovej komunikácie** je ochrana prenosu dát pred odpočúvaním a manipuláciou tretími osobami.

1.2 Čo sa môže stať

Počítače, dáta a komunikáciu ohrozujú v princípe nasledujúce faktory:

- Výpadok alebo poškodenie hardwarových komponentov - môže spôsobiť stratu alebo poškodenie dát
- Nechcené škody spôsobené užívateľom - napr. neželané zmazanie dát
- Cílené škody a neželaná manipulácia spôsobená tretími osobami - vírusy, spyware, odpočúvanie komunikácie a podobne.

1.3 Ktoré tretie osoby nás ohrozujú

Média často predávajú pojem *Hacker* ako počítačového experta so zlými úmyslami.

V skutočnosti existuje ale pre týchto ľudí iné pomenovanie, tu je krátky prehľad:

- **Hacker** - je počítačový expert, zväčša dobrý programátor, ktorý hľadá bezpečnostné diery v systémoch, za účelom zlepšenia ich bezpečnosti. O nájdených nedostatkoch informuje tvorcov programov, správcov systému a verejnosť.
- **Cracker** - má rovnaké schopnosti ako hacker, používa tieto ale vo svoj prospech, často ilegálne. Sem patria aj tzv. softvéroví, filmoví a hudobní piráti, lovci čísiel kreditných kariet a iní. Medzi najčastejšie motívy patria peniaze a uznanie v komunite. Cracker robí svoju činnosť plánovane a premyslene. Medzi crackerov patria aj **pharmeri** a **phisher**, ktorých činnosť je spomenutá v kapitole 3.4.
- **Script-Kiddie** - zvykne útočiť práve na bežných užívateľov, pričom jeho znalosti internetu a programovania nezvyknú byť veľké. Jedná sa často o mládež, ktorá použije na internete dostupné nástroje na tvorbu vírusov alebo preniknutie do problematických systémov za účelom páchania škôd. Hovorí sa im aj *internetoví vandali*. Medzi najčastejšie motívy patria zábava (škodoradosť), zaháňanie frustrácie, chválenie sa. Script-Kiddie koná náhodne, pod vplyvom nálady.
- **Spammer** - Spammer je človek, ktorý organizuje alebo prevádzkuje rozposielanie nevyžiadanych správ. Túto činnosť robí pre svojich zákazníkov, ktorí jej pomocou chcú zbohatnúť. Pošta je často zavádzajúca a neprináša užívateľovi žiaden úžitok.

2 Bezpečnosť počítača

Zabezpečenie užívateľského počítača nie je jednoduchou úlohou. Ohrozujú ho tzv. škodiace programy, ktoré sú známe pod anglickým názvom **Malware**. Nasledujúce podkapitoly predstavujú rozličné typy Malware a spôsoby, ako sa proti nim brániť.

2.1 Malware

2.1.1 Programy implantované u užívateľa

Najčastejšie sa užívateľ stretne s nasledovnými druhmi Malware[1] (jednotlivé programy zvyknú zahrňovať viac typov naraz):

- **Vírus** - program napadajúci súbory a rozširujúci sa ďalším užívateľom, najčastejšie pomocou e-mailu. Na infikovanie počítača vírusom je potrebné spustiť už nainfikovaný súbor.
- **Červ** - program s funkčnosťou ako vírus, akurát sa dostane do počítača cez bezpečnostné diery bez nutnosti zásahu užívateľa
- **Trójsky kôň** - program, ktorý sa vydáva za užitočný, pričom v skutočnosti vykonáva niektoré z iných činností uvedených v tomto zozname
- **Backdoor** - program, ktorý umožní tretím osobám vstup do počítača a jeho použitie na rôzne ciele (napr. internetové útoky, rozposielanie nevyžiadanej pošty). Infikovaným počítačom sa zvykne hovoriť aj *zombie*.
- **Dialer** - program, ktorý vytáča pomocou modemu audiotextové čísla
- **Spyware** - program, ktorý zbiera a odosiela osobné a iné informácie o užívateľovi a jeho počítači tretím osobám
- **Malicious Adware** - program, ktorý zobrazuje užívateľovi reklamy alebo web-stránky bez toho, aby mal o to užívateľ záujem

2.1.2 Pomôcky, ktoré používa útočník

Medzi typy programov, ktoré používajú útočníci patria okrem iného:

- **Exploit** - software, ktoré ma za úlohu zaútočiť na jednu špeciálnu dieru v systéme, je často súčasťou červov
- **Rootkit** - programový nástroj, pomocou ktorého útočník získa kontrolu nad systémom
- **Keylogger** - program, ktorý zaznamenáva, čo bolo napísané na klávesnici

2.2 Prevencia a obrana proti Malware

Aby bola prevencia a obrana proti Malware úspešná, je potrebné kombinovať viaceré pomocné programy a tiež dodržiavať určité zásady pri používaní počítača a internetu, ktoré sú uvedené v nasledujúcej podkapitole.

2.2.1 Zásady používania

Odporúčam nasledovné kroky na zlepšenie bezpečnosti počítača:

- **aktualizovať operačný systém** - za účelom zaplátania bezpečnostných dier, napr. Windows XP podporuje automatickú bezpečnostnú aktualizáciu
- **používať antivírusový program** - pozri ďalšia podkapitola
- **nepripravovaný užívateľ** - pri Windows 2000 a XP nepoužívať prístup s administrátorskými právami, toto použiť iba na zmeny systémových nastavení alebo inštaláciu nových programov
- **bezpečné heslo** - nielen na počítač, ale aj všade na internete by mali byť používané rozličné heslá, ktoré spĺňajú určitú úroveň zložitosti (napr. obsahujú veľké aj malé písmená, čísla, nejaké znaky a majú aspoň 8 znakov). Automaty sa neustále pokúšajú nájsť prístupy s jednoduchými heslami.
- **zálohovať dôležité dáta** - pravidelné zálohovanie na externé médiá chráni pred výpadkom hardvéru, pred poškodením vírusmi a aj pred náhodným neželaným zmazaním užívateľom
- **nenavštevovať dubiózne stránky** - nenavštevovať stránky na internete, ktoré napr. otvárajú veľa okien s reklamami. Tieto stránky zvyknú inštalovať na užívateľský počítač Spyware.
- **neotvárať neznáme prílohy v pošte** - vírusy sú najčastejšie šírené prostredníctvom e-mailu, preto treba skontrolovať odosielateľa, predmet pošty a typ prílohy pred jej otvorením
- **prípadne používať alternatívne programy** - ako napr. prehliadač Mozilla Firefox a poštový program Mozilla Thunderbird. Tieto programy majú momentálne vyššiu bezpečnosť ako Internet Explorer alebo Outlook Express, je na nich podstatne menej známych útokov a pri ich používaní nie je napr. potrebné antispyswarové riešenie.

2.2.2 Softvérové pomôcky

Odporúčam používať tri základné softvérové pomôcky pre zabezpečenie užívateľského počítača - Antivirus, Antispysware a Firewall. Viacerí výrobcovia softvéru ponúkajú kombinované riešenia. Niektoré programy existujú v bezplatných verziách pre domáce použitie.

- **Antivirus** - chráni počítač pred vírusmi
Niektoré známe programy: Avast (Alwil), AVG (Grisoft), McAfee Virusscan (NAI), Norton Antivirus (Symantec), Panda Antivirus (Pandasoftware)
- **Antispysware** - čistí počítač od nežiadaneho Spyware
Niektoré známe programy: Ad-Aware (Lavasoft), Spybot S&D
- **Firewall** - chráni počítač pred červami a útokmi z internetu
Niektoré známe programy: Zonealarm (Zonelabs), Norton Firewall (Symantec), Kerio Personal Firewall (Kerio), integrovaný firewall v Microsoft Windows XP SP2

2.2.3 Hardvérové pomôcky

Medzi hardvérové pomôcky, ktoré je hodné spomenúť, patria v prvom rade domáce smerovače (Router), resp. brány (Gateway), ktoré sú použiteľné pre ADSL, káblové a pevné pripojenie na internet, majú zabudovaný firewall a mnohé z nich obsahujú aj prístupový bod pre domácu bezdrátovú sieť. Použitie týchto zariadení nie je legálne pri pripojeniach od firmy UPC.

3 Nevyžiadaná pošta a zavádzanie užívateľa

S nevyžiadanou poštou, o ktorú veľká väčšina užívateľov nemá záujem, sa dnes stretol už takmer každý užívateľ internetu. Zvykne sa jej hovoriť *spam*. Spam je pomenovanie, ktoré sa zaužívalo pre nevyžiadanú elektronickú poшту. Samostatný názov[2] pochádza od značkových mäsových konzerv SPAM (spiced ham), ktoré sa vyrábajú od roku 1936. Toto pomenovanie bolo pridelené nevyžiadanej elektronickej pošte na základe sketchu z Monty Python's Flying Circus.

V angličtine existujú dva spisovnejšie výrazy pre spam vo forme elektronickej pošty:
Unsolicited Bulk Email (UBE) - nevyžiadaná masová pošta
Unsolicited Commercial Email (UCE) - nevyžiadaná komerčná pošta

Táto kapitola sa zaoberá obsahom a formami nevyžiadanej pošty, a na záver poštou ktorá ma zaviesť užívateľa na falošné stránky.

3.1 Obsah nevyžiadaných správ

Najčastejšou rečou obsahu je angličtina, ale veľa spamu je aj v azbuke. Polovica všetkého spamu spadá obsahovo pod nasledovné kategórie[3]:

- **pre dospelých** - napríklad ponuky na viagru a iné pomôcky
- **zdravie** - napríklad prostriedky na chudnutie
- **IT** - najčastejšie predaj (nelegálnych) programov
- **osobné financie** - najšastejšie pôžicky a hypotéky (dubiózneho charakteru)
- **vzdelávanie a kurzy** - predaj akademických titulov, kurzy rozličného druhu

Medzi ďalšie druhy patria (všetko nedôveryhodné) reťazové hry, rôzne lotérie, ponuky možnosti rýchlo si zarobiť, predaj rozličných výrobkov a iné.

Medzi špeciálne kategórie patria Phishing a Pharming, kde sa niekto iný vydáva za seriózne web-stránky a touto cestou sa pokúša získať od užívateľa dôležité informácie (napr. prístup k bankovým kontám a podobne). Odkazy na tieto sú rozposielané formou spamu. Viac v kapitole 3.4.

3.2 Typy nevyžiadanej pošty podľa média

V dnešnej dobe môžeme spam zatriediť podľa použitého média na rozširovanie nasledovne[2]:

- **E-Mail Spam** - spam prostredníctvom elektronickej pošty, dnes má najčastejší výskyt a predstavuje veľkú časť celkovej e-mailovej komunikácie
- **SPIM** - instant messaging Spam, predstavuje nevyžiadané správy v Instant Messengeroch (komunikačné programy ako napríklad ICQ, MSN, AIM)
- **Usenet newsgroup Spam** - spam v diskusnej sieti Usenet (Newsgroups - poštové diskusné fóra), tu bol prvý výskyt spamu
- **Spamdexing** - špeciálne úpravy webových stránok tak, aby sa zobrazili ako prvé v internetových hľadačoch
- **Link Spam** - automatické pridávanie odkazov na web-stránky do weblogov a webových diskusných fór
- **M-Spam** - spam prostredníctvom SMS na mobilné telefóny

3.3 Boj proti spamu

Okrem právnych krokov proti rozposielačom spamu, ktorý sú často v krajinách, kde k ich prenasledovaniu nedojde sa prevádzkujú dva základné typy obrany: **blacklisty** a **spamové filtre**.

3.3.1 Blacklisty

Blacklisty sú zoznamy internetových serverov, ktoré sú na týchto označené ako servery rozposielajúce spam. Server prijímajúci poštu potom od serverov v tomto zozname akúkoľvek poštu odmieta. Toto riešenie sa používa hlavne na serveroch vo firmách, prípadne u internetových poskytovateľov.

Problematické pri tomto type filtrovania je, že do zoznamov sa môžu dostať aj servery, ktoré spam nerozposielajú.

3.3.2 Spamové filtre

Druhý spôsob je identifikácie správ obsahujúcich spam. Toto robia (dnes už celkom inteligentné) filtre (programy), ktoré na základe špeciálnych pravidiel určujú, či je pošta spam alebo nie. Medzi tieto pravidlá patria napríklad výskyt určitých slov, spôsob, akým je správa zložená a veľa ďalších. Filtre tohoto druhu podporuje dnes už veľa poštových programov, ako napr. Mozilla Thunderbird alebo The Bat, takže ich môže bežný užívateľ používať doma. Samozrejme poskytovatelia elektronickej pošty siahajú aj k tejto technológii pri filtrovaní správ na ich serveroch.

Nevýhodou tohoto riešenia je nepresnosť (aj dobré správy môžu byť označené ako spam) a tvorcovia spamu sa stále zdokonaľujú v obchádzaní týchto filtrovacích pravidiel.

3.4 Phishing a pharming

Phishing a **pharming** sú relatívne nové metódy okrádania užívateľov.

Phishing využíva metódy sociálneho inžinierstva a rozširuje sa v prvom rade e-mailom. Falšovaná správa vyzýva užívateľa, aby zmenil resp. upravil svoje osobné údaje v bankových inštitúciách alebo na webstránkach, kde sa držia finančné prostriedky, resp. záväzné objednávky. V tejto správe je ale link, ktorý ukazuje na inú web-stránku, ako je originálna webstránka spomenutej inštitúcie. Táto webstránka vyzerá a správa sa takmer úplne rovnako, užívateľ si to nevšimne. Prihlásením sa na tejto web-stránke získa nepovolaná osoba prístupové údaje a možnosť okradnúť užívateľa o finančné prostriedky.

Pharming má rovnaký efekt ako phishing, ale pracuje na inej báze. V tomto prípade je napadnutý buď internetový poskytovateľ, alebo užívateľský počítač, kde sú zmenené tzv. DNS záznamy. Touto cestou adresy web-stránok ukazujú na iné miesta, ako by mali, takže nastáva rovnaký efekt ako pri phishingu - užívateľ sa dostane na falošnú web-stránku, kde prezradí dôležité tajné informácie ako napríklad meno a heslo k bankovým operáciám.

Prevenia proti phishingu je relatívne jednoduchá, stačí preskúmať elektronickú poštu, čo prišla. Phishing zakladá totiž na tom, že užívateľ tej pošte bude naslepo veriť. Na dotyčnej pošte relatívne rýchlo poznať, že sa jedná o phishing - odkazy na falošné stránky, často nespisovný text.

S pharmingom je to už zložitejšie. Jednou z efektívnych metód je preverenie tzv. SSL-certifikátov na šifrovaných stránkach - touto cestou sa dá overiť pravosť stránky, na ktorej sa užívateľ nachádza (v typickom prehliadači sa zobrazí ikona zámku a varovanie, keď sa užívateľ nachádza na zabezpečených stránkach).

4 Bezpečnosť komunikácie

Dobré zabezpečenie samotného počítača pri používaní internetu a sietí je iba jednou stranou mince. Na druhej strane sú tu nástrahy, ktoré ohrozujú siete ako také a únik informácií, ktorý nastáva používaním internetu. Iba málo užívateľov vie, že jeho surfovanie po web-stránkach môže niekto sledovať a že zanecháva stopy, že každý e-mail, ktorý pošlú, si môže hneď niekoľko ľudí na jeho ceste k adresátovi prečítať, a informácie v ňom použiť vo svoj prospech alebo proti užívateľovi.

4.1 Únik informácií tretím osobám

Pri práci na internete a komunikáciu cez neho treba brať ohľad na to, že činnosť, ktorú na ňom užívateľ robí (napríklad surfovanie po web-stránkach, posielanie elektronickej pošty), môžu napriek dobre zabezpečenému počítaču monitorovať viaceré osoby. Medzi tieto patria:

- **Internetový poskytovateľ užívateľa** - má prístup ku všetkej komunikácii, ktorú užívateľ uskutočňuje cez internet. Ak táto nie je šifrovaná, je pre neho voľne čitateľná.
- **Správca cieľového servera** - má prístup ku komunikácii, ktorú užívateľ uskutočňuje s jedným špecifickým serverom. Ak má na tomto serveri užívateľ uložené dáta (napr.

poštovú schránku), má k tejto tiež prístup.

- **Poskytovatelia uprostred cesty** - majú prístup ku komunikácii, ktorá nimi prechádza, sem spadajú aj peeringové centrá ako napr. SIX

Pokiaľ sa crackerovi (pozri kap. 1.3) alebo inej tretej osobe podarí preniknúť do systémov niektorého z vyššie uvedených poskytovateľov či už legálne alebo nelegálne, má tiež prístup ku komunikácii.

Užívateľ je ale chránený telekomunikačným tajomstvom, takže legálne sa takto získané informácie použiť nedajú.

4.2 Zabezpečenie komunikácie

Ak si je užívateľ vedomý skutočností, ktoré su uvedené v predošlej kapitole, môže mať záujem vo vybraných situáciách viesť zabezpečenú komunikáciu. Medzi tieto patria napr. online-banking, ale v mnohých prípadoch aj korešpondencia, ktorá obsahuje dôležité, prípadne zneužitelné informácie. Tu je krátky prehľad možností zabezpečenia komunikácie:

- **Zabezpečené web servery** - v princípe všetky online-bankingy a taktiež web-stránky, kde sa odosielajú osobné informácie používajú zabezpečený HTTPS protokol. Poznať to na tom, že adresa stránky sa začína `https://` a prehliadač zvykne na zabezpečenie upozorniť oknom a ikonou zámku.
- **Zabezpečený prístup k pošte** - podobným spôsobom sa dá aj zabezpečiť prístup k čítaniu a odosielaniu elektronickej pošty (protokoly POP3S, IMAPS, SMTPS), ak to poskytovateľ podporuje
- **Šifrovanie pošty a dát** - vyššou formou ako ako zabezpečenie prístupu k pošte sú šifrovacie techniky, ktoré nebudem uvádzať. Šifrovanú poštu alebo súbor si môže otvoriť iba majiteľ príslušného kľúča.
- **Elektronické podpisovanie pošty a dát** - elektronické podpisovanie slúži k potvrdeniu originality pošty alebo súborov. Pošta alebo súbor vykážu po zmene neplatný podpis.
- **VPN** - Virtual Private Network znamená virtuálna súkromná sieť, najčastejšie sa používa pre prístup pracovníkov do firmy na diaľku cez internet alebo bezpečné prepojenie sietí v rámci internetu. Tiež sa tu používajú rôzne typy šifrovania.

V prípade zabezpečenej komunikácie má prístup k nešifrovanej forme iba odosielateľ a adresát. Útočník uprostred cesty dát musí použiť komplexné a náročne dešifrovacie techniky, ak by k týmto dátam chcel získať prístup. Efektívne majú na túto činnosť kapacity iba veľké spoločnosti a vlády. Určité typy šifrovania sa ale považujú za zatiaľ nezlomené (úmyselne nepoužívam výraz nezlomiteľné, lebo zatiaľ pre každú šifrovaciu technológiu niekedy prišiel čas zlomenia).

4.3 Bezdrátové siete

Samostatne by som sa v tejto poslednej kapitole chcel krátko venovať bezdrátovým sieťam. Bezdrátové siete majú oproti ostatným typom sietí jednu veľkú nevýhodu - prístup k signálu má v princípe hocikto z okolia a to bez toho, aby sa o tom vedelo, že odpočúva komunikáciu. Dá sa to porovnať s rozprávaním do bežnej vysielacky - každý, kto má naladený rovnaký kanál počuje, o čom sa rozprávate.

Nie je na to dokonca ani treba žiadnu špeciálnu výbavu, stačí notebook alebo malý prenosný počítač typu PDA, ktorý je vybavený bezdrátovou sieťovou kartou (WiFi), príslušné programy a know-how, ako na to.

Z tohoto dôvodu je veľmi dôležité prístup do bezdrátových sietí kontrolovať a používať najnovšie šifrovacie mechanizmy.

Veľmi demonštratívnym príkladom sú siete v rámci Bratislavy. Stretol som sa s veľmi veľa prístupovými bodmi, ktoré nepoužívajú žiadne šifrovanie. Väčšina bezdrátových sietí, čo šifrovanie používajú, šifruje pomocou technológie WEP, ktorá je už dávno prelomená a prístup do týchto sietí sa dá získať behom niekoľkých minút až hodín.

5 Záver

Svet internetu vyzerá ružovo iba na prvý pohľad. V skutočnosti sa tu skrýva veľa špinavých a nepríjemných vecí, ktorým sa uvedomelý užívateľ môže vyvarovať. Cieľom tejto besedy bolo aspoň sčasti uviesť bežného užívateľa do tejto problematiky, ukázať mu základné princípy bránenia sa. Potom sa vyvaruje nepríjemným prekvapeniam, a keď už k nejakému problémovému stavu dojde, vie sa postarať o to, aby škoda bola čo najmenšia (napr. zálohovaním dát).

Vymýšľanie nových foriem útokov a následne obrany proti nim je neustály kolotoč, ktorý sa nie a nie zastaviť. Preto je dôležité, sa priebežne informovať o nových hrozbách, spôsoboch obrany proti nim a riadiť sa pravidlami, ktoré som spomenul v tejto besede.

Referencie

- [1] Wikimedia foundation. Wikipedia project - malware [online]. Available from: <http://en.wikipedia.org/wiki/Malware>.
- [2] Wikimedia foundation. Wikipedia project - spam [online]. Available from: <http://en.wikipedia.org/wiki/Spam>.
- [3] Kaspersky Lab. Viruslist.com - about spam [online]. Available from: <http://www.viruslist.com/en/spam/info>.