

Projekt č. 3

Ochrana proti počítačovým virům a spamu

Jméno: Vladimír Kudělka
Třída: 7. AK
Datum: 5.1. 2003

Hned ze začátku rozdělím tento projekt na dvě témata, protože se jedná o dvě odlišné problematiky internetového světa. Viry mohou mít velmi drtivý dopad a zanechat komplikace každému uživateli a spam zase narušuje soukromí uživatelů. Oba problémy také spadají do e-mailové části. Každopádně existuje několik účinných obran a ty se zde budu snažit prezentovat.

Viry a ochrana proti nim

Co je to tedy počítačový virus? Virus je program, který má škodit. Například první generace virů škodila tím, že se z ničeho nic aktivovala a něco se zobrazilo na monitoru. Viry dnes, jsou na takové technické úrovni, že formátují pevné disky, kradou data uživatelům a posílají je přes internet jinam, obcházejí různé rezidentní ochrany antivirových programů, takže se obtížně hledají a ničí. Dá se říci, že viry se stávají stále vychytralejšími a bohužel i zákeřnějšími, proto je také kladen větší důraz na antivirovou ochranu. Co nám mohou viry způsobit:

Blokování místa. Vir musí být někde uložen, a to buď v paměti nebo na pevném disku (nebo na obou místech).

Zpomalení práce systému. Vir pro svou "činnost" potřebuje část pracovních systémů počítače, které tak "krade" jiným programům.

Nestabilita systému. Viry nejsou testované pro různé počítače a konfigurace hardware a software, a tak systém může často bez zjevné příčiny "zatuhnout".

Krádež dat. Oblíbená kratochvíle především e-mailových virů, které čas od času odešlou elektronickou poštou náhodnému či předem určenému příjemci data z počítače.

Šifrování dat. Některé viry se projevují tak, že zašifrují data na pevném disku, která berou jako "rukojmí" a za šifrovací klíč mohou požadovat finanční obnos na příslušné konto, nebo jen svoje nesmazání ze systému.

Zničení dat. To je snad jedna z nejhorších věcí, která vás může potkat, pokud pravidelně nezálohujete data.

Osobně jsem se ještě se závažným virovým napadením neseťkal a vždy šlo o rychlou a lehkou léčbu. V poslední době jde především o viry zvané Trojský kůň. Trojský kůň je škodlivý program, který není schopen vlastního samostatného šíření. Původní trojské koně byly nejčastěji programem, který předstíral, že se jedná o nějakou užitečnou aplikaci (třeba o novou verzi populární utility) a ve skutečnosti jeho spuštění vedlo ke smazání obsahu disku nebo jeho části. Dnes jsou nejčastější trojské koně typu BackDoor, které zprostředkovávají vzdálený přístup k zasaženému počítači a PSW (Password Stealer), které se snaží sesbírat nejrůznější privátní údaje uživatele a odeslat je na internet. Pro odstranění obvykle stačí smazat spustitelné soubory, které si na počítači trojský kůň vytvoří. Pokud je takový program spuštěn, tak je bohužel jeho .EXE podoba na disku chráněna operačním systémem před smazáním, ale to není dvakrát složitá situace.

Celkově můžeme viry rozdělit do čtyř základních skupin a to podle podle sektoru napadení nebo různých vlastností:

Boot viry - mohou infikovat BOOT sektor disku nebo diskety a BOOT, MBR (master boot record) nebo FAT tabulku disku. Tyto viry se mnohdy šíří přes BOOT sektor disket. Stačí, když si infikovanou disketu necháte před zapnutím počítače v disketové mechanice a máme infikovaný i počítač, tato disketa nemusí být ani systémová, tedy z níž jde spustit operační systém. Proto bych doporučil nastavit si v Setupu počítače funkci nekontrolovat disketu při startu počítače. Máte-li infikovaný BOOT sektor diskety a neinfikovanou operační paměť, zasuňte infikovanou disketu a napište v příkazové řádce příkaz `sys c: a:` (ne obráceně!) a BOOT diskety budete mít v pořádku, použitím příkazu `format a: /y` jste dosáhli stejného výsledku. Máte-li infikovaný systémové oblasti disku, svěřte obnovu raději odborníkovi. K obnově se používají nástroje SYS, FDISK nebo opravné prostředky antivirového programu.

Souborové viry - infikují vybrané soubory na disku, disketě, zip disku a dalších médiích. Objevíte-li vir ve vašem souboru, např. s příponou Exe, Com, Bat, Dll, můžete s ním udělat několik věcí: Funkcí opravit, léčit, obnovit, dokáže-li to antivirový program nebo ho ihned nahradit souborem ze zálohy, který je v pořádku. Pak ještě existuje varianta smazat nebo přejmenovat ho na Ex_, Co_, Ba_, Dl_, aby nebylo možno ho ani omylem spustit nebo aktivovat, vždy je však potřeba uvědomit si, v jakém adresáři je a k jakému účelu soubor slouží.

Multipartitní viry - infikují jak soubory, tak i systémové oblasti, v případě infekce je nutno postupovat jako u bootových virů.

Makro viry - infikují textové dokumenty typu Word a Excel, v případě infekce tímto typem viru je dobré použít antivirový program nebo soubor smazat.

Škodlivost virů a jejich typy již byly charakterizovány, ale jak se tomu všemu vyhnout? Určitě je lepší prevence než řešení vzniklého problému a mnohdy vyjde právě prevence na menší úsilí či finanční obnos než vzniklá škoda. Nejběžnější prevenci, ale i léčbou je využití antivirových programů. Mezi ty nejkvalitnější patří:

Norton Antivirus

Norton AntiVirus je již dlouhou dobu považován za jeden z nejlepších antivirů vůbec. Program pochopitelně dokáže provádět antivirovou kontrolu celého systému na povel nebo podle předem stanoveného plánu. Všechny testy si můžete přesně nakonfigurovat, vybrání adresářů, které chcete kontrolovat, přípon, na které dávat pozor. Dokáže automaticky kontrolovat stahované soubory, přílohy emailů a otevírané soubory. Zcela jasně největší problém všech antivirů je, že si musíte stále stahovat nové definice virů. Norton AntiVirus obsahuje funkci LiveUpdate, která automaticky kontroluje po Internetu, zda máte nejnovější definice, a nabídne vám stažení aktuálních.

AVG

Nejznámější český antivirový program! Systém AVG je velmi sofistikovaný softwarový prostředek na ochranu vašeho počítače a dat před nebezpečím počítačových virů. Obsahuje všechny důležité součásti jako rezidentní štít, kontrola pošty v Outlook Express a samozřejmě také jednorázové testy diskového prostoru.

BitDefender

BitDefender je antivirový systém se vším, co má takový systém mít. Obsahuje rezidentní ochranu, plánované testy, automatickou aktualizaci. Samozřejmostí je také ochrana před emailovými viry, která pracuje nezávisle na klientovi, který používáte. Součástí programu je také osobní firewall pro ochranu před nechtěným vstupem do vašeho počítače.

Osobně využívám AVG a jsem spokojený. Myslím, že program je spolehlivý a obsahuje rozsáhlou a bohužel stále rostoucí databázi virů, která je řešena aktualizacemi díky internetu. Tato ochrana je podle mě alespoň z části dostačující co se osobního domácího počítače týče. Vyhledávání a zneškodnění zatím neznámých virů bych přenechal osobě zasvěcené do této problematiky. V nouzi bych se však pokusil o smazání daného souboru (v tom lepším případě) a nebo formátováním disku a reinstalaci celého počítačového softwaru.

Podobně bych řešil i antivirovou ochranu ve firemním prostředí, kde by byl základem spolehlivý antivirový program a opatrnost při vybírání nevyžádaných e-mailů.

Spam a ochrana proti němu

Co je spam? Podle českého zákoníku je to každý nevyžádaný reklamní email. Jde téměř vždy o zakázanou nevyžádanou reklamu.

Podle § 2 odst. 1 písm. e) zákona č. 138/2002 Sb. (dále jen zákon o regulaci reklamy) platí následující:

"Zakazuje se šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje."

Zákaz tak platí pouze při splnění všech následujících podmínek:

1. musí jít o reklamu
2. tato reklama musí být nevyžádaná
3. musí dojít k obtěžování adresáta
4. nebo k výdajům adresáta

Sám musím uznat, že tato problematika se mě dotýkala více než viry. Mám totiž zavedené přijímání e-mailů na mobil a to za určitý poplatek. Platím tedy za každý přijatý e-mail. Postupem času došlo i na spam a denně mně začaly chodit zhruba 3 e-maily. To, že mě to obtěžuje časově jsem ještě toleroval, ale platit za to. Naštěstí jsem vše vyřešil antispamovými filtry, které jsou dnes již standartem každé společnosti, která provozuje poskytování e-mailových schránek. V mém případě bylo vše jednodušší, protože se jednalo o spam stále ze stejných adres, které jsem lehce vypsal do antispamové sekce e-mailové schránky a dnes se setkám se spammem velmi zřídka (1 do měsíce).

Ne vždy je ovšem boj se spammem tak jednoduchý a tak existuje spousta programů pro boj se spammem. Za zmínku stojí například:

Aldo's SPAM Cleaner

Za pomoci programu Aldo's SPAM Cleaner ušetříte čas, neboť nebudete muset stahovat z poštovního serveru nepotřebnou poštu. Můžete tak odfiltrovat spam, zavirované emaily či nechtěné zprávy. A to dříve, než si je stáhnete pomocí POP3 do svého počítače. Sami si můžete definovat, jaký druh zpráv má být vymazán. Můžete k tomu využít filtr slov, sousloví, odesílatelů nebo domén. Aldo's SPAM Cleaner vám ušetří čas i peníze.

MailWasher

Velice dobrý nástroj pro boj s nevyžádanou obtěžující poštou. Využívá k jejímu rozeznání jak heuristických metod, tak filtrů založených na vlastních i externích (ORDB, SpamCop) blacklistech. Samozřejmostí je i použití nadefinovatelného whitelistu. Vedle základní možnosti odstranění spamu jej můžete poslat zpět v takovém formátu, že to vypadá, že vaše e-mailová adresa neexistuje (tzv. bouncing). Dále program dokáže odhalit možné viry obsažené v e-mailu a řetězové dopisy. V neposlední řadě je třeba zmínit možnost zobrazení náhledu dopisu před jeho stažením.

SpamGunner

SpamGunner je anti-spamový program určený běžným uživatelům a malým podnikům. Dokáže kontrolovat několik různých emailových účtů najednou a odstraní poštu, která obsahuje reklamu. Filtr je možné nastavit podle odesílatele, předmětu, země původu, velikosti, přílohy nebo textu v obsahu zprávy. Dále SpamGunner chrání uživatele před emailovými viry. Součástí programu jsou tzv. Divoké karty (Wildcards), díky kterým již žádný spam neunikne. Nejen pro uživatele s pomalejším připojením nabízí SpamGunner možnost identifikování velkých příloh emailů ještě před stažením do počítače, urychlí tak práci s internetem.

Pokud však nechcete zacházet až k používání antispamových programů, je zde pár rad jako prevence:

Skrývání své adresy

Spamové útoky rozšiřuje uvedení vaší e-mailové adresy na některé z internetových stránek, odkud jí pak stačí zkopírovat a odesílat spamové e-maily. Proto je možné nahradit povinné znaky jako je zavináč a tečky slovy. Adresu v.kudelka@centrum.cz lze tedy zapsat jako v.kudelka /zavináč/ centrum.cz.

Rozvážné používání e-mailové schránky

Dalším způsobem jak spam potlačit je zřízení více e-mailových schránek. Jednu využívat čistě na korespondenci s prověřenými osobami či společnostmi a druhou při vyplňování nepodstatných registrací, ze kterých spam většinou vzniká.

Použité zdroje:

www.svetsiti.cz, www.cdr.cz, www.viry.cz, www.avg.cz, www.stahuj.cz