12. Bezpečnost na internetu

Malware

Malicious Software zahrnuje kromě samotných virů spoustu dalších typů programů, jejichž výskyt v počítači je nežádoucí. Podíváme se tedy na další pojmy a typy této počítačové „havěti“ se kterou se můžeme běžně setkat.

Spyware

Spyware je program, který využívá Internetu k odesílání dat z počítače bez vědomí jeho uživatele. Narozdíl od backdooru jsou odcizovány pouze „statistická“ data jako přehled navštívených stránek či nainstalovaných programů. Tato činnost bývá odůvodňována snahou zjistit potřeby nebo zájmy uživatele a tyto informace využít pro cílenou reklamu. Nikdo však nedokáže zaručit, že informace nebo tato technologie nemůže být zneužita. Proto je spousta uživatelů rozhořčena samotnou existencí a legálností spyware. Důležitým poznatkem je, že spyware se šíří společně s řadou sharewarových programů a jejich autoři o této skutečnosti vědí. [www.viry.cz]

Adware

Obvykle jde o produkt, který znepříjemňuje práci s PC reklamou. Typickým příznakem jsou „vyskakující“ pop-up reklamní okna během surfování, společně s vnucováním stránek (např. výchozí stránka Internet Exploreru), o které nemá uživatel zájem. Část Adware je doprovázena tzv. „EULA“ - End User License Agreement – licenčním ujednáním. Uživatel tak v řadě případů musí souhlasit s instalací. Adware může být součástí některých produktů. Ačkoliv nás reklama doprovází během celé činnosti s daným programem, odměnou je větší množství funkcí, které nejsou v klasické free verzi (bez reklamy) dostupné. [www.viry.cz]

Dialer

Dialer je program, který změní způsob přístupu na Internet prostřednictvím modemu. Místo běžného telefonního čísla pro Internetové připojení přesměruje vytáčení na čísla se zvláštní tarifikací, např. 60 Kč / minutu (tzv. „žluté linky“). V některých případech se tak děje zcela nenápadně nebo dokonce automaticky, zvlášť když oběť používá špatně nastavený, popř. „děravý“ internetový prohlížeč. Dialer může být na PC vypuštěn návštěvou „nevhodné stránky“ (např. pornografické), například za využití technologie ActiveX, takže problémy mohou nastat především uživatelům Internet Exploreru. V jiném případě může jít o nenápadný spustitelný soubor (.EXE), který je nic netušícímu uživateli vnucován ke stažení klasickým dialogem (mluvíme-li o prohlížeči Internet Explorer). [www.viry.cz]

SPAM

Spam je nevyžádané masově šířené sdělení (nejčastěji reklamní) šířené internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace – např. diskuzní fóra, komentáře nebo instant messaging.

E-mailové adresy do spamových databází jsou získávány mj. pomocí robotů, které procházejí webové stránky a sbírají e-mailové adresy na nich uvedené. Také registrací na některých serverech s uvedením vaší adresy je možné přidat se na seznam pro spam. No a samozřejmě viry na PC mohou odeslat seznam vašich kontaktů nebo přímo odesílat spam z vaší adresy.

Backdoor, Zombie, Botnets

Některé viry (červy) často jako svojí další činnost instalují do PC tzv. Backdoor (zadní vrátka), které umožní k systému přístup útočníkovi. Z takto nakaženého PC může být vytvořena „zombie“ pod kontrolou autora viru. Sítě takových strojů se nazývají botnets a často jsou využívány k další nekalé činnosti jako je např. odesílání spamu nebo provádění DDoS (Distributed Denial of Service) útoků.

Hoax

Anglické slovo HOAX v překladu znamená: Falešnou zprávu, Mystifikaci, Novinářskou kachnu, Podvod, Poplašnou zprávu, Výmysl, Žert, kanadský žertík. V počítačovém světě slovem HOAX nejčastěji označujeme poplašnou zprávu, která varuje před neexistujícím nebezpečným virem nebo podobnou havětí, ale i další fámy, petice, výstrahy, pyramidové hry, řetězové dopisy apod. Jestliže zpráva obsahuje výzvu k hromadnému rozeslání na další adresy, je to s největší pravděpodobností HOAX. Takové zprávy obtěžují příjemce, zbytečně zatěžují linky a vyzrazuje informace (e-mailové adresy), čehož se dá dále využít pro spam. [www.hoax.cz]

Phishing

Phishing je činnost, při které je rozesílán email uživatelům Internetu, který se tváří, že byl odeslán z legitimní organizace (většinou finanční, banky apod.). Předmětem takového emailu je získat osobni informace uživatele, zejména pak čísla platebních karet a jejich PIN a následně jejich zneužití. Phishing email obsahuje často odkaz na stránky s formulářem, který uživatel v dobré víře vyplní a odešle. Odeslaná data vsak nekonči u bankovního či finančního ústavu, ale v rukou tvůrce phishing emailu.

Další

Kromě těchto existují i další pojmy v oblasti. Rootkit je program maskující svoji přítomnost svojí co nejhlubší infiltrací do operačního systému, keylogger (nebo jiný logger) zase zaznamenává činnost na PC a k informacím umožní přístup útočníku. Čas od času se objevují další pojmy ukazující na jiný typ či podtyp podobných programů.

Obrana:

- používat šedou kůru mozkovou
- používat antiviry, antispyware, anti….,
- používat alternativní prohlížeče, programy, OS
- nechodit na stránky s podezřelým obsahem (nelegální: sw, pornografie, cracky, ...)
- být paranoidní

Bezpečnost sítí

Dokud byly počítače pouze samostatné stanice, existovalo hlavně nebezpečí virů a to zanesených z infikovaných médií. Jsou-li však počítače připojeny do počítačové sítě nebezpečí vzrůstá a s přístupem k internetu jsme prakticky stále v potenciálním ohrožení.

Firewall

Jako obrana proti nebezpečí ze sítě existuje firewall. Hned na úvod je třeba říci, že nenahrazuje antivirový program, antispyware a další, ale v kombinaci nám dovolí mnohem lépe ochránit náš systém.
V počítačové terminologii se firewallem nazývá software či hardware (hardwarové firewally), jehož funkcí je kontrolovat (povolovat či zakazovat) komunikaci v počítačové síti na základě daných pravidel. Používá se na oddělování různých částí sítě (nejčastěji odděluje nebezpečný internet od místní sítě).

Osobní firewall je firewall určený pro ochranu pracovní stanice (tedy jednoho počítače). Jedná se tedy o software (aplikaci) s přívětivým ovládáním, tak aby s ním mohl pracovat i méně zkušený uživatel. Z funkčního hlediska pracuje velmi podobně – odděluje počítač od sítě. Navíc, díky tomu, že běží přímo na pracovní stanici, může kontrolovat komunikaci více detailněji (může kontrolovat, které aplikace komunikují) než firewall chránící celou síť (protože neběží na tomto počítači, nemá možnost zjistit, ke které aplikaci komunikace patří).

Principy:

Paketové filtry

Nejjednodušší a nejstarší forma firewallování, která spočívá v tom, že pravidla přesně uvádějí, z jaké adresy a portu na jakou adresu a port může být doručen procházející paket, tj. kontrola se provádí na třetí a čtvrté vrstvě ISO OSI.

Stavová inspekce (statefull inspection)

Mnohé útoky lze dnes rozpoznat až tehdy, když si firewally začínají všímat také vzájemných souvislostí a vztahů, a dokáží si dát "dvě a dvě dohromady". Například když si dokáží uvědomit, že najednou přichází výrazně vyšší množství individuálních požadavků než je obvyklé, což vyvolává náhlé zahlcení toho, kdo má tyto požadavky vyřizovat.

Aplikační inteligence

Firewally - se mohou nejodpovědněji (nejspolehlivěji) rozhodnout, pokud "vidí" až na aplikační vrstvu a detailně rozumí tomu, co se zde odehrává, podle jakých pravidel atd. Bez této schopnosti jsou firewally bezbranné vůči celé řadě "moderních" a čím dál tím častějších útoků, jakými jsou

například útoky červů (např. Slammer, Code Red či Nimda), útoky pomocí skriptů (cross-site scripting), vůči emailovému bombardování (mail bombing) atd. Schopnost dívat se až na úroveň aplikační vrstvy je samozřejmě nesmírně náročná na inteligenci firewallu, i na jeho výpočetní kapacitu a správu.

IDS

Nejnověji se do firewallů integrují tzv. in-line IDS (Intrusion Detection Systems – systémy pro detekci útoků). Tyto systémy pracují podobně jako antiviry a pomocí databáze signatur a heuristické analýzy jsou schopny odhalit vzorce útoků i ve zdánlivě nesouvisejících pokusech o spojení, např. skenování adresního rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod.

Ověřit si zabezpečení a popř. funkčnost firewallu je možné. Při online testech se však bude testovat váš počítač pouze máte-li veřejnou IP adresu.

netstat –abn
http://www.paranoia.cz/test/start
http://www.test.bezpecnosti.cz/

Některé SW produkty

FIREWALLY:

Sunbelt Kerio Personal Firewall (zdarma pro domácí nekomerční použití)

ZoneAlarm (zdarma pro osobní a nekomerční použití)

Comodo Firewall (aktivace zdarma, zdarma celoživotní licence)

Symantec Norton Internet Security / Personal Firewall

Agnitum Outpost Firewall Pro

Internet Security Systems BlackICE PC Protection

a další…

(http://www.matousec.com/projects/windows-personal-firewall-analysis/links.php)