Škodlivý software

Informace a data jsou to nejcennější, co se v počítači nalézá. Pro jejich zabezpečení je zapotřebí minimalizovat rizika jejich možných poškození nebo ztrát.

Zabezpečením dat v počítačích se zabývá obor informatiky nazvaný počítačová bezpečnost.

Počítačová rizika

Všeobecně můžeme počítačová rizika rozdělit na rizika vnitřní a vnější.

Vnitřní rizika se mohou projevit například kolizí programu, nechtěným smazání dat, zkratem apod. Způsobují je zejména softwarové chyby, dále hardwarové chyby a chyby uživatele.

Mezi vnější rizika patří krádež počítače, poškození vnějšími vlivy a počítačová infiltrace (tj. jakýkoliv neoprávněný vstup do počítače). Jsou důsledkem především nedostatečného fyzického zabezpečení počítače nebo absentující softwarové ochrany, firewallu atp.

Vzhledem k tomu, že současné počítače jsou obvykle připojené do sítě a k internetu, zaměříme se na rizika neautorizovaného přístupu k nim.

Malware

Pojmem malware označujeme veškerý škodlivý software. Pojem vznikl spojením anglických slov malicious software. Pokud se takový software spustí, zahájí činnost ke škodě výpočetního systému. Malware může být spuštěn přímo z počítače, do kterého byl přenesen, nebo může počítač napadnout na dálku. Mezi malware, který se spouští lokálně, patří viry, trojské koně, adware, spyware apod.

Vir

Vir je program, který parazituje na již existujícím souboru. Připojí se k programům nebo systémovým oblastem a tím je pozmění. Vir se může nekontrolovatelně replikovat, nebo – pokud je spuštěn – zahájí operace, které mohou vést k poškození, změně či zničení dat, ke stahování dalšího malware apod.

Trojský kůň (Trojan horse)

Jeho charakteristickou vlastností je, že se neumí replikovat, uživatel si jej na svůj počítač stahuje sám. Po spuštění se kód vydává za žádoucí program, ve skutečnosti provádí činnosti, které mohou být škodlivé. Jeho činnost může být vyvolána okamžitě po instalaci nebo ho může aktivovat konkrétní událost (datum).

Trojský kůň typu spyware shromažďuje informace (sniffing software) – například zaznamenává posloupnost znaků stisknutých na klávesnici nebo zablokuje software pro zabezpečení počítače. Trojský kůň typu adware může zobrazovat nevyžádanou reklamu, nahrazovat reklamní bannery vlastními apod.

Červ (Worm)

Jde o škodlivý kód, který se šíří pomocí počítačových sítí. E-mailový červ se šíří jako příloha e-mailu – posílá své kopie na e-mailové adresy uvedené v kontaktech (nebo kontakty messengeru) a u nich způsobí to samé, čímž se zahlcuje síť. Síťový červ využívá bezpečnostní díry v operačních systémech a síťovém software (např. pomocí vzdáleného přihlášení se přihlásí jako běžný uživatel a začne vydávat příkazy).

Zadní vrátka (Backdoor)

Jde o neautorizovaný vstup do počítače, díky němuž lze převzít kontrolu nad počítačem a na dálku ho ovládat. V takto infikovaném počítači tak může například někdo na dálku manipulovat s daty, nebo může otevřít CD/DVD mechaniku.

Logická bomba (Logic bomb)

Jde o skrytý kód, který je vložený do běžného programu. Může se spustit na základě nějaké události (ochrana před kopírováním, smazání aplikace po určitém počtu spuštění nebo uvedení údajů o všech členech týmu apod.). Logická bomba se může šířit pomocí počítačového viru, červa, ale i jinými způsoby.

Dialer

Vznikl v době, kdy se počítače připojovaly k internetu hlavně vytáčeným telefonním připojením. Pomocí kódu došlo k přesměrování z čísla poskytovatele připojení na číslo se zvýšeným cenovým tarifem. Obdobně fungují webové stránky, které odkazují na placené služby.

Flooder

Hackeři získají pomocí kódu kontrolu nad počítačem (takový počítač označujeme jako zombie) a generují velký síťový provoz. Od přijetí signálu od útočníka začnou všechny infikované počítače generovat zprávy a jimi zaplaví cíl. Uživatelé se na útocích podílejí jako nevědomí komplicové.

Exploit

Škodlivý kód, který využívá programátorskou chybu nebo slabé místo operačního systému či jiného software. Přes slabé místo kód proniká do systému a získává práva pro téměř libovolné operace. Tyto kódy používají white hat hackeři při testování možností průniků do systémů (v tomto případě pomáhají nalézt slabiny OS a SW).

Droopery

Drooper je malware, jehož cílem je nainstalovat virus do počítače. Protože je vir uvnitř dropperu většinou zakódován, lze vir obtížně odhalit pomocí běžných metod.

Injektor

Injektor je zvláštním druhem drooperu. Injektor instaluje kód viru do paměti počítače.

Malware podle umístění v paměti

Rezident

Škodlivý kód se umístí do paměti a díky tomu může napadat každý nově spuštěný program. V paměti zůstává až do vypnutí počítače. Tento kód sleduje, s kterými soubory se pracuje – tyto soubory může infikovat.

Nerezident

Škodlivý kód není trvale umístěný v paměti, ale aktivuje se spuštěním hostitelského programu. Poté převezme řízení a po vykonání své činnosti (rozšíří se do nenakažených souborů) vrátí řízení hostitelskému programu.

Malware podle napadené oblasti

Souborový vir

Škodlivý kód napadá spustitelné programové soubory. Může poškodit hostitelský program, který poté nemůže pracovat. Vir může napadnout spustitelné programy a poté se duplikovat, může přepsat část původního kódu svým kódem nebo se může umístit do volného místa v programu apod.

Boot vir

Napadá systémové oblasti floppy disku, HDD nebo tabulku MBR. Dnes se téměř nevyskytuje (ke svému šíření využíval floppy disky – při nastartování operačního systému se zavedl z diskety).

Malware podle projevů chování

Makrovir

Nejčastěji napadá datový soubor vytvořený pomocí kancelářské aplikace. Takový soubor obsahuje kromě dat i makra, kterými se vir šíří.

Stealth vir

Kód využívá maskování (vydává se za běžný soubor, šifruje sebe nebo infikovaná data, při pokusu o čtení infikovaného souboru vrací hodnoty, které odpovídají původnímu stavu). Patří sem také rootkity – nástroje, pomocí nichž se skrývají škodlivé kódy.

Polymorfní vir

Jde o kód, který během své replikace vytváří různé mutace. Umožňují mu to různá kódovací schémata nebo náhodné vkládání nadbytečných instrukcí.

Dopady malware

Máme-li zálohu, není problém ztráta nebo zničení souboru. Nevíme-li ale, kdy byl náš systém napadený škodlivým kódem, který vykonává činnost pomalu nebo občas, odstraňuje se škoda problematičtěji. Největší ohrožení je v současné době spojené se ztrátou osobních dat (bankovní účty, hesla do aplikací).

Zabezpečení počítače

Antivirová ochrana

Primární softwarovou ochranu dat zajišťuje antivirový software. Slouží i jako prostředek k odstraňování škodlivého kódu z výpočetnícho systému. Antivir si při prvním spuštění vytvoří databázi souborů na disků, poté běží na pozadí systému, přičemž sleduje změny v souborovém systému, kontroluje prováděné operace, prohledává soubory a testuje je na výskyt virů, které má uložené ve vlastní databázi.

Firewall

Preventivní software, který (nainstalovaný v bráně) filtruje e-mailovou korespondenci nebo může blokovat síťový provoz. Speciální firewally: proxy server, spam filtr.

Software pro auditování

Nástroje (zjm. pro správce), které umožňují monitoring aktivity v počítačovém systému, detekci škodlivého chování (např. série pokusů o přístup s nesprávným heslem). Pomocí software pro auditování lze například odhalit sniffing software (program, který zaznamenává uživatelovu aktivitu).

Zdroje

[1] BROOKSHEAR, J. Glenn. *Informatika*. Brno: Computer Press, 2013. ISBN 978-80-251-3805-2.

[2] ROUBAL, Pavel. *Informatika a výpočetní technika pro střední školy: Teoretická učebnice*. Brno: Computer Press, a. s., 2010. ISBN 978-80-251-3228-9.

[3] SZOR, Peter. *Počítačové viry – analýza útoku a obrana*. Brno: ZONER software s.r.o., 2006. ISBN 80-86815-04-8.

[4] Saferinternet.cz [online]. [cit. 2014-10-25]. Dostupné z WWW: <http://www.saferinternet.cz/>.

[5] BRAIN, Marshall a Wesley FENLON. *How stuff works: „How Computer Viruses Work*“. [online]. [cit. 2014-10-05]. Dostupné z WWW: <http://computer.howstuffworks.com/virus.htm>.

[6] Computer virus (virus). Webopedia [online]. [cit. 2014-11-05]. Dostupné z WWW: <http://www.webopedia.com/TERM/V/virus.html>.

[7] Viry.cz [online]. [cit. 2014-10-10]. Dostupné z WWW: <http://www.viry.cz/>.

[8] JUNEK, Pavel. *Zálohování a archivace dat v podnikovém prostředí - 6. díl (část 1/3), Business Continuity Management (BCM)*. [online]. [cit. 2014-10-17]. Dostupné z WWW: <http://www.zalohovani.net/zalohovani-a-archivace-dat-v-podnikovem-prostredi-6-dil-cast-13-business-continuity-management-bcm/>.

[9] HÁK, Igor. Moderní počítačové viry: třetí vydání [online]. 2005 [cit. 2014-10-16]. Dostupné z WWW: <http://viry.cz/download/kniha.pdf>.

[10] Přispěvatelé Wikipedie, Počítačová bezpečnost [online]. Wikipedie: Otevřená encyklopedie, c2014, Datum poslední revize 3. 07. 2014, 09:14 UTC, [citováno 07. 10. 2014] <http://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_bezpe%C4%8Dnost&oldid=11635583>.

[11] IT slovník [online]. [cit. 2014-10-10]. Dostupné z WWW: <http://it-slovnik.cz/>.