Számítógépes biztonsági kultúra

SZÁMÍTÓGÉPES BIZTONSÁGI KULTÚRA

Dr. Leitold Ferenc

Veszprémi Egyetem Információs Rendszerek Tsz. - Veszprog Kft.

fleitold@veszprog.hu

BEVEZETÉS

Aki gyakran ül autóba, tisztában van vele, hogy milyen dolgokra kell odafigyelnie, hogy az utazás során a biztonságát maximalizálja. Általában mindenki el szokta vinni autóját a rendszeres átvizsgálásokra, ha észrevesszük, hogy nem fog a fék, szerelőhöz fordulunk. De vajon hasonló gondossággal járunk-e el, ha a számítógépünkről van szó? Alkalmazunk-e olyan szoftvereket, amelyek biztonságunkat szolgálják? Frissítjük-e megfelelő gyakorisággal vírusvédelmünket, tűzfalunkat? Figyeljük-e folyamatosan operációs rendszerünk javításait, melyek az újabb és újabb biztonsági réseket foltozzák be? ... és még sorolhatnánk a megválaszolandó kérdéseket.

A fentiek alapján felmerül a kérdés, hogy megbízhatunk-e számítógépünkben. Használhatjuk-e számítógépünket - megfelelő biztonsággal – például egy 50 milliós szerződés elektronikus aláírására? Megbízhatunk-e ennyire a számítógépben és a rajta futó szoftverekben?

Mit tehetünk annak érdekében, hogy az elektronikus aláírás használatának kockázatát csökkentsük, és mit tehet egy laikus számítógép használó, aki nem kíván a számítógépes biztonság rejtelmeiben elveszni, de mindennapi életében szívesen használna a technika új vívmányait?

Az alábbiakban egy rövid ízelítő erejéig néhány, a kérdéskörrel kapcsolatos aktuális problémára térünk ki, mely alátámasztja azt, hogy a jelenlegi, széles körben elterjedt számítástechnikai eszközök használata messze van a biztonságtól. Ezt főként az operációs rendszerek és a bennük rejlő temérdek biztonsági problémák okozzák. Manapság egy laikus felhasználótól, sőt számos rendszergazdától is megkövetelhetetlen, hogy az aktuális biztonsági problémákkal tisztában legyen, a javító programokat folyamatosan telepítse. De ha

ideje nagy részét mégis rászánja, még akkor sem érezheti magát tökéletes biztonságban: biztosan van (legalább még egy) javítatlan biztonsági rés. Ezt pedig egy célzott támadás esetén egy támadó bármikor ki tud használni.

BIZTONSÁGI RÉSEK

Az Internet Security Systems nemrégen nyilvánosságra hozott adatai alapján 2003 első negyedévében a cégek és vállalatok által észlelt biztonsági események száma 84 százalékkal növekedett az előző negyedévhez képest. A növekedést nagyrészt a különböző típusú Interneten terjedő féregvírusok okozták. 2003 első negyedévében természetesen beletartozik az SQL.Slammer féregvírus is, mely mindössze 376 byte méretű. A 2003 január 25-én útjára indított vírus a Microsoft SQL Szerverének már fél éve ismert biztonsági hibáját használta ki, amihez már régóta elérhető a javítás. A féreg elindítását követően néhány perc alatt körbeutazta a Földet és a fertőzés sebességére jellemző, hogy az elindulását követő percekben kevesebb, mint 9 másodpercenként megduplázta a fertőzött gépek számát.

A BIZTONSÁGI SZAKÉRTŐK VÉLEMÉNYE

A számítógép-biztonsági szakértők háromnegyede nem bízik a Microsoft termékeiben, derült ki a Forrester Research legutóbbi felméréséből [7], melynek alapkérdése: "Biztonságos lehet-e a Microsoft?". Összesen 35 számítógép-biztonsági szakértőt kérdeztek meg, melyek mindegyike olyan cégnél dolgozik, melynek legkevesebb 1 milliárd dolláros bevétele van. A válaszadók 77 százalékának kételyei vannak a Microsoft termékeinek biztonságát illetően, ezzel szemben 89 százalékuk mégis használja azokat. A Forrester elemzője szerint túl kevés cég foglalkozik Windows-rendszere biztonságával. A cégek 40 százaléka nem tervez biztonsági fejlesztéseket, és a támadást elszenvedett vállalatoknak is csak 59 százaléka változtatott a biztonsági szabályain. A Microsoft több mint egy évvel ezelőtt elindított egy programot szoftverei megbízhatóságának növelésére, de a cég szerint több évbe vagy akár egy évtizedbe is telhet, mire elérik a célt. A legnagyobb horderejű esetekben, például a Microsoft szoftvereinek biztonsági réseit kihasználó Nimda vagy SQL.Slammer vírusok támadásakor egyébként már jóval korábban hozzáférhetőek voltak a szükséges biztonsági javítások, azonban a legtöbbször a rendszergazdák nem telepítették ezeket. A legutóbbi kilenc, nagyobb biztonsági résre kiadott javítás átlagosan 305 nappal a támadások előtt megjelent, mégis csak

nagyon kevesen telepítették azokat kellő időben. Ennek szerinte az az oka, hogy a rendszergazdák nem biztosak abban, hogy egy patch nem okoz-e problémákat a már beállított rendszerekben, emellett se idejük, se eszközeik nincsenek figyelemmel kísérni a sok javítást. Amikor az SQL.Slammer féregvírus januárban terjedni kezdett, a Microsoft már régen kész volt a féreg által használt rés biztonsági javításával, hiszen azt még júliusban kiadták.

A LINUX SEM SEBEZHETETLEN

Denis Zenkin, a ***Kaspersky Lab*** munkatársa érdekes írást tett közzé az SC Magazine (Copyright © 2000 West Coast Publishing. Reprinted from SC Magazine, 161 Worcester Road, Suite 201, Framingham, MA 01701.) és az SC On-Line oldalain (*SC Magazine*, www.scmagazine.com/) *The Invulnerable Penguin* címmel. Csaknem a megszületésének és bevezetésének pillanatától kezdve folyamatosan zajlik a vita arról, hogy a vírusvédelem szempontjából milyen erős is a Linux "immunrendszere". Köztudott tény, hogy semmi sem abszolút dolog. Még a rajongóitól a "megtámadhatatlan", vírusbiztos architektúrája miatt oly sok díjat kapott Linux sem lehet tökéletesen immunis a vírusokkal szemben.

Sokan hiszik azt, hogy a Linux architektúra nem hagy semmi esélyt a vírusoknak a túlélésre. Azonban több mint lehetséges, hogy idővel fel fognak fedezni olyan réseket, amelyek lehetővé teszik, hogy rosszindulatú személyek elvégezhessék romboló tevékenységüket. Megjelenésekor a Windows NT-t is vírusmentes platformnak kiáltották ki, de ez az állítás mára ódivatú tündérmesévé vált.

A Linux rendszerek Achilles sarka az, hogy a nyílt forráskód szabadon hozzáférhető. Ez teszi lehetővé a víruskészítőknek, hogy a kernel modulok, illetve a runtime könyvtárak módosításával rosszindulatú komponenseket integráljanak bele a Linux operációs rendszer minden egyes részébe. A Linux alatt viszonylag könnyen megoldható pár perc alatt az ilyen "fejlesztés", az úgynevezett "zárt" platformoktól eltérően, ahol az ilyenfajta aktivitás létrehozása (a programkód visszafejtése és a rendszerhívások átirányítása) több hónapos kemény munkát igényel. Így az örökölt számítógépes fauna hagyományos megosztása, amely DOS vagy Windows örökség, valóságos rémálommá válhat, mivel megjelenhet egy új típusú víruskategória, amely az operációs rendszerek magjába *(a kernelbe)* épül be. Érdemes megemlíteni, hogy azokban az években, amikor az első Windows vírusokat létrehozták, egyetlen ilyen típusú vírust sem fedeztek fel. A Linuxszal ez akár már holnap is

bekövetkezhet. Ez a vírustípus minden platformon el fog terjedni, elsősorban természetesen a Linuxon, mivel ez a legnépszerűbb ilyen típusú desktop operációs rendszer.

A fertőzés módja egészen egyszerű. Ha egy vírus egyszer root jogokkal indult el egy aktív folyamatban, (többnyire a tapasztalatlan Linux felhasználók használják ezt az accountot), “megpatkolja” a kernelt vagy új modulokat hoz létre (manapság a Linux disztribúciók közül egyik sem alkalmaz digitális szignatúrákat moduljaik védelmére, azok illegális megváltoztatását megelőzendő), és betölti azokat az operatív memóriába. Ennek eredményeként a vírus a számítógép minden egyes újraindításakor aktivizálódik. A történet legfenyegetőbb eleme az, hogy egy vírus hozzáadható a rendszer funkcióihoz bármely komplexitásban, s ez pusztító incidensekhez vezethet, melyek között nem csupán adatvesztés, de a hardver sérülése is előfordulhat, valamint bizalmas információk eltulajdonítása, stb. Az ilyen típusú vírusok észlelése és fertőtlenítése, melyek beépülnek a rendszer-kernelbe, az arra még fel nem készített anti-vírus gyártóktól termékeik komoly fejlesztését igényli, beleértve akár a víruskereső motor teljes áttervezését is.

A biztonsági rések lezárására a legjobb módszer a javítócsomagok *(patch)* időnkénti telepítése. Itt ismételten megint nem a Linux a legjobb választás. A Windows, vagy bármely más "zárt" platform javítócsomagjainak telepítése nagyon egyszerű és a végfelhasználótól csak minimális erőfeszítést igényel. Általában annyi csak a tennivaló, hogy rákattintanak a javítócsomagot tartalmazó .EXE fájlra és a telepítés végén újraindítják a rendszert. Linux alatt ez sokkal komplikáltabb is lehet, mivel egy patch esetén szükség van arra, hogy a felhasználó maga fordítsa újra a forráskódot (ez nem mindig sikeres) és tovább bonyolítja a helyzetet, hogy a Linux disztribúciók közül nem sok kompatibilis teljesen a többivel. Más szavakkal a Linux az elképzelhető legagresszívebb és felhasználó-ellenes környezet.

A Linux sérthetetlenségének sűrű emlegetése és a platformot károsítani képes "in the wild" Linux vírusok hiánya csak a vírusírók kezére játszanak. A Linux fájloknál sajnos megszokott és helytelen gyakorlat, hogy az Internet gyanús forrásaiból származó fájlokat is vírusellenőrzés nélkül futtatják le. Micsoda remek vadászterület a vírusok és trójai programok számára! Az az egyetlen oka annak, hogy még eddig nem volt a Linux alatt egy, a LoveBug-hoz hasonló nagyságrendű vírusjárvány, hogy a Linux még mindig nem egy széles körben elterjedt platform és még mindig nem olyan desktop szabvány, amelyet PC-k millióin használnának világszerte az összes iparágban.

Minden ellenkező híresztelés ellenére a Linux népszerűsége ma még messze a Windows-é mögött kullog, és ezért a vírusírók figyelmét kevésbé vonja magára ez az operációs rendszer. Ez annak ellenére igaz, hogy csaknem hetente fedeznek fel új Linux vírusokat. És bár közülük sok hitvány és kontármunka, ezek a kísérletek egyre agresszívebbekké válnak, s ami sokkal rémisztőbb, közülük sok sikeres. Sajnos nyilvánvaló, hogy Linux vírusok globális járványa van a láthatáron.

ÖSSZEGZÉS

Sajnos meg kell, hogy állapítsuk, hogy nem létezik olyan PC-s környezet, melyről az Internethez történő kapcsolása mellett elmondhatjuk, hogy tökéletes biztonságban használható. Ezt főként a nem megbízható operációs rendszerek, illetve alkalmazások okozzák. Természetesen a biztonság növelése érdekében

- használhatunk célgépeket, akár minden hálózattól (Internettől) is lekapcsolhatjuk,
- használhatunk tűzfalakat, biztonsági programokat,
- alkalmazhatunk magas képzettségű rendszergazdákat, akiknek a feladata a folyamatos frissítések elvégzése.

Az viszont (jelenleg) megoldhatatlan, hogy például egy kisebb vállalkozás biztonságosan használja az Internet adta kommunikációs lehetőségeket. Különösen nagy gondot jelenthet, ha az elektronikus aláírást is alkalmazza, hiszen ennek támadása esetén már a törvénnyel kell szembesülni. Gondoljunk csak bele: egy kis ügyvédi iroda, mely használja az elektronikus aláírást egy olyan PC-n, amin valamilyen Windows fut és minden tűzfal nélkül kapcsolódik az Internetre. Egy megfelelő tudással rendelkező támadó célzottan bármikor be tud hatolni a számítógépébe és akár az ügyvéd elektronikus aláírását is meghamisíthatja.

Felmerül a kérdés: mit tehetünk? A legfontosabb az oktatás: minden felhasználónak joga van megtudni, hogy milyen veszélyek fenyegetik az elektronikus aláírás használata esetén, illetve milyen védekezési lehetőségei vannak. Természetesen ehhez megfelelő tájékoztatás is szükséges. Mindenképpen célszerű a használandó eszközöket is ellenőrizni a támadhatóság szempontjából.

FELHASZNÁLT IRODALOM

1. 2001. évi XXXV. törvény az elektronikus aláírásról

2. Virasztó Tamás: Kriptográfia és szteganográfia – avagy rövid bevezetés a rejtjelezés és az adatrejtés világába; www.wacher.hu; 2001.

3. Ködmön József: Kriptográfia; Computerbooks Kft.; 1999.

4. F. Ható Katalin: Adatbiztonság, adatvédelem; SZÁMALK Kiadó; 2000.

5. Denis Zenkin (Kaspersky Labs): The Invulnerable Penguin; SC Magazine; West Coast Publishing

6. SaveAs Kft.: Esettanulmány egy felfedezett poloska programról; www.saveas.hu; 1999.
7. www.index.hu/tech/biztonság
8. www.virushirado.hu