Információvédelem

AZ ADATÁTVITELI HÁLÓZATOKON ÁRAMLÓ ÉS A DIGITÁLIS TÖMEGTÁRAK MEMÓRIÁJÁBAN RÖGZÍTETT INFORMÁCIÓ VÉDELMÉBEN

Eiler Emil

A támadások és veszélyforrások: vírusok, kémés egyéb rosszindulatú programok. Trendek. A védekezés mai eszközei

A digitális adatátviteli hálózatok elleni támadások és a digitális tömegtárakon rögzített információ vírushatásai révén a márkák, a nyomtatott, másolt dokumentumok és a nagy értékű csomagolt termékek is veszélyeztetve lehetnek! A *CSO Computerworld Magazine* (www.csoonline.com/read/010106/) előrejelzései szerint a közeljövő meghatározó adatbiztonsági trendjei ilyen szempontból a következők:

- kevesebb számú járványszerű támadás lesz, de azok majd több és nagyobb kárt okozhatnak;
- a támadások a Microsoft operációs rendszer hátterében, rejtve, kevésbé szembetűnően zajlanak majd;
- a *Spyware* kémprogramok és a *Malware* rosszindulatú programok tevékenysége által előidézett károk fokozódnak;
- a kommunikációs és az internetes károkozásban új szereplővé lép elő az internetezésre alkalmas mobiltelefon is;
- az e-mail – károkozási szempontból – kritikus tényezővé fajul;
- a hagyományos nyomdatechnika és az elektronizáció integrációja felgyorsul, emiatt a fokozott biztonság igénye mindenhol beépül az infrastruktúrába, ami jelentős többletköltséggel jár;
- fokozódik, és már-már iparszerű méreteket ölt az internetes kalózkodás *(hacker-)* és a betörő *(cracker-)* tevékenység.

Ma még nem tudhatjuk, hogy a 2008-ban elterjedő új internetezési lehetőség (a ***web 2.0***) milyen hatással lesz a biztonságra.

Az előrejelzések szerint a számítógépeket és az általuk kezelt információtartalmat továbbra is különféle vírusok, kémprogramok és rosszindulatú szoftverek károsíthatják, de a jelenleginél nagyobb mértékben, a következők szerint.

Makrovírusok. – E-mailhoz csatolt dokumentumként terjednek. A makrókat alkalmazó Word-, Excel-állományokra fokozottan veszélyesek.

Férgek. – Szaporodásuk a vírusokhoz hasonló. E-mail-en keresztül terjednek. Céljuk a terjedés és a rombolás. Ha elindítjuk a csatolt gyanús *exe* kiterjesztésű fájlt, az a levelezőlistánk összes címzettjéhez megérkezik, és ott elkezdi a rombolást.

Trójai Faló. – Hasznos alkalmazásnak álcázza magát, miközben kártékony.

Lopakodók. – Az antivírusprogramot és az operációs rendszert is megkerülve, a gép memóriájában maradnak, majd a fájl méreteit, az operációs rendszer jellemzőit és a könyvtár struktúráját megváltoztatják.

Retrók. – A víruskereső alkalmazásokat nemcsak kijátszani, hanem hatástalanítani tudják.

Poliformok. – Bármely vírus lehet poliform, hogy nehezebben lehessen elcsípni, mivel minden fertőzéskor megváltozik a struktúrájuk. A Google kutatásai szerint, már ma is átlagban minden tizedik weboldal tartalmaz olyan rosszindulatú kódot, amely megfertőzheti a felhasználó számítógépet.

A ***Spyware kémprogram*** által végrehajtott károkozások jelentősége fokozódik. Az ilyen programok olyan módosításokat hajtanak végre a felhasználó számítógépén, amelyek

- érintik a személyes adatokat és a rendszer biztonságát is;
- a megfertőzött rendszerek erőforrásait használják fel, beleértve a telepített szoftvereket is;
- személyes információkat gyűjtenek, használnak, illetve terjesztenek.

A számítógép-tulajdonosoknak a felsorolt programok elleni védekezés újabb jelentős költséget okozhat.

A ***Malware programok*** tevékenysége bonyolultabbá válik: olyan területeken is támadás érhet

bennünket, ahol meggyőződésünk szerint eddig biztonságban voltunk, pl. a PDF-használat terén. A rosszindulatú programokat összefoglalóan *malware* vagy *vandál* programokként is emlegetik.

A mindennapi gyakorlatban az alábbi, egymástól sokszor nehezen megkülönböztethető *malware*-kategóriákat ismerhetjük meg:

- ***program típusú malware*** számítógépvírusok és programférgek: *vírusfejlesztő kitek; trójai* és *backdoor programok*; a *dialerek; dropperek*; a *kémprogramok*; *keyloggerek* és egyéb kártékony rendszerek;
- ***szöveg típusú malware***: kéretlen küldemények – *spam, hoax, holland és spanyol lottónyereménylevelek, nigériai csalások, phishing, pharming*, egyéb kártékony szöveges tartalmak.

A támadók és támadások céljai

A számítógép olyan adattár is, amelyben értékes magánjellegű és céges adatok is megtalálhatók, még ha nincs is mindenki tisztában azzal, mi minden deríthető ki egy évek óta használt számítógép merevlemezéről.

A tárolt adatokat, fájlokat az alábbi három – nem is mindig jól elválasztható – csoportra oszthatjuk.

- Az első csoportba a ***programfájlok*** sorolhatóak, beleértve az operációs rendszer és a különböző felhasználói programok fájljait. A támadások sikerességét jelentősen megnöveli, ha a támadó tudja, mi az, amit támad, hisz így fel tud készülni ellene, megkeresheti az ismert és kevésbé ismert sérülékenységeket, és nem fecsérli erejét olyan célpontokra, amelyek túl erősen védettek, vagy nem eléggé értékesek számára.
- A második csoportba a ***konfigurációs fájlok*** tartoznak, amelyek azokat a beállítási adatokat őrzik, amelyek gépünknek saját eszközeivel és a külvilággal való kapcsolattartását szabályozzák. Egy támadó számára igazi értéket a külvilággal való kapcsolattartás paraméterei – különböző felhasználói azonosítók, jelszavak, PIN-kódok, bankszámlák adatai, behívószámok stb. – jelentenek. Ha a támadó ezekhez hozzáfér, akkor visszaélhet az adatokkal, vagy úgy módosíthatja beállításainkat, hogy a megbízható és hiteles weboldalak helyett hamisított weblapokra terel.
- A harmadik adattípusba a ***felhasználói adatfájlok*** tartoznak. Ezek tartalmazzák a magán- és kereskedelmi jellegű adatainkat és levelezéseinket, marketinginformációhoz juthat, megtudja, milyen anyagokat, eszközöket szoktunk használni, milyen szoftveres, hardveres és fogyóeszköz-jellegű kiegészítőkre lehet szükségünk. Ennek hatására megszaporodhatnak a kéretlen reklámleveleink. A kereskedők a címzettek nevét általában ilyen illegális úton szerzett információk alapján válogatják ki egy vagy több címlistáról.

Aki ***kémprogram*** irtóval is rendelkezik, tapasztalhatja, hogy egy-egy ellenőrzése alkalmával 10-15 kémprogram irtására is szüksége lehet!

A védekezés aktuális és hatékony eszközei

A digitális adatátviteli hálózatokban áramló és a digitális tömegtárak memóriájában rögzített adatok elleni támadások típusai szinte naponta változnak. A lapzártánk időpontjában ezzel kapcsolatban rögzíthető konkrét megállapítások nagyon gyorsan elavulttá válnának. Szerencsére a márkás szolgáltatók szintén naponta frissítik a védelmi rendszerüket. Aki tehát biztosítja magának a szolgáltatók által felkínált megbízható automatikus védekezés lehetőségét, az úgy érezheti, hogy viszonylag magas védettsége van támadások ellen.

A HP *Compaq nx6325* noteszgépe például már ***biometrikus ujjlenyomat-érzékelővel*** és ***SmartCard író-olvasóval*** rendelkezik. Ma már egyre több ***TPM-csip hardveres modell*** is kínál védelmet a rosszindulatú hackertámadások ellen (www.dunainformkft.hu ; www.mobilx.hu; http://h41131.www4.hp.com/hu/hu/press/).

De ne feledjük! A támadók is folyamatosan fejlesztenek, ezért többnyire a legkorszerűbb eljárásokkal és eszközökkel rendelkeznek! Így aztán ebben a vég nélküli macska–egér játékban a láthatatlan, jól képzett kisegér gyakran jár *egy lépéssel* előbbre az őt üldöző macskánál.