

Virusveszély és egyéb kockázatok.

Telbisz Ferenc

1. Bevezetés

Jelen írás nem kíván tudományos alaposságú elemzést adni az informatikai kockázatokról, még kevésbé részletes útmutatást adni ezek elkerülésére. Csupán szeretné a figyelmet felhívni néhány jelenségre, és néhány ötletet adni a kockázatok csökkentésére. Az alább elmondandók nem tekinthetők egyetlen szervezet hivatalos véleményének sem, amelyekkel a szerző kapcsolatban áll, de reméli, hogy minden olvasója komolyan mérlegelni fogja az itt elmondottakat.

2. Számítógépes betörések és vírusok

A számítógépek mindig is ki voltak téve támadásoknak. Ezt a veszélyt a zárt géptermi üzemeltetés idején, amikor legfeljebb helyi terminálokat használtak, viszonylag könnyen kézben lehetett tartani a hozzáférési hely ellenőrzésével. A veszély nagymértékben megnőtt a távoli terminálok megjelenésével, és még inkább a gépek hálózatba kapcsolásával, amikor a támadó a hálózati névtelenség mögé bújhatott.

A korai támadások motívumai meglehetősen racionálisak voltak, a támadók vagy az erőforrások (CPU, háttértárak) jogosulatlan használatára törekedtek, vagy a gépen tárolt információkhoz akartak hozzáférni, bár több "hacker" is volt, akik ezt a támadások, betörési kísérletek intellektuális kihívásának a kedvéért csinálták. Ezekben a betörési kísérletekben mindig nagy szerepe volt a személyes akcióknak, személyes részvételnek, valójában a betörő (hacker) és a rendszergazda (sysman) párharcai voltak, volt bennük valami a rabló-pandúr játék romantikájából. Egy ilyen akció sorozat igen élvezetes leírása megtalálható Cliff Stoll: "Cuckoo's Egg" című könyvében.

Noha a betörési kísérletek ma is folynak, a vírusokkal megjelent az informatikában is "korunk hőse", a terrorista. A cél immár nem az erőforrások, információk megszerzése, hanem az erőforrások tönkretétele, de legjobb esetben is a békés felhasználó gyötrése, esetleg valamilyen demonstráció érdekében. Mindez azonban igen komoly veszélyt, kockázatot is jelent. Az év elején jelentkezett HAPPY99 és az újabb Melissa vírus jó alkalom arra, hogy elgondolkodjunk, végre felébredjünk és észrevegyük a nyilvánvaló veszély súlyát.

3. A vírusok és a Microsoft

A szándék szerint a felhasználók kényelmét szolgáló, de átgondolatlan és valójában nem is igazán szükséges lehetőségeket nyújtó fejlesztések is segítik a vírusgyártókat. Ilyen kockázati helyzetek kialakításában igen jelentős a Microsoft szerepe is. Mindkét fentebb említett vírus Microsoft szoftver eszközökre épült, és különösen a Melissa Microsoft rendszerkomponensen keresztül (levelező rendszer) támadt, okozott igazán számottevő

kárt. Elkészítésük aligha lett volna lehetséges a Microsoft implicit, bár nyilvánvalóan nem szándékolt segítsége nélkül.

A Microsoft a mai napig nem vetett igazán számot avval, hogy már nem "home computerek"-re, kezdetleges PC-kre fejleszt, amelyek mai szemmel visszanezve – kissé eltúlozva – lényegében szuperkalkulátoroknak, intelligens írógépeknek vagy játéklatformoknak voltak tekinthetők. A PC-k mai utódai komoly teljesítménnyel rendelkeznek, sőt szerver szerepkörben is használják őket. Ehhez képest meglehetősen kockázatos, hogy a Windows változatok (3.1x, 95, 98, NT) adatvédelme enyhén szólva is meglehetősen hiányos, jószerével nem is létezik. Nemhogy a rosszindulatú felhasználókkal szemben nem nyújt jószerével semmilyen védelmet, de a figyelmetlen vagy tapasztalatlan felhasználót sem védi a saját hibáitól. Megdöbbentő, hogy teljesen "mezei" felhasználó által elindított programok minden akadály nélkül beleírhatnak a rendszer területére mind a memóriában, mind a háttértáron. Ez még a többfelhasználós NT szervereken is így van. (A hálózat felől van valamelyes védelem.) És mit mondjunk arról, hogy egy NT munkaállomáson a lokális hálózaton kiejáratott file-oknál defaultként minden felhasználónak jogosultsága van írásra, olvasásra, törlésre. A Microsoft szoftver fejlesztőinél vajmi kevés nyomát látjuk annak, ami a számítástudomány, a "software engineering", az operációs rendszerek készítésének régóta bevett elveihez és gyakorlatához tartozik.

Mindkét említett támadásnak lényeges eszköze volt a Winword-be beépített makró lehetőség, ami a védelem említett hiánya következtében tud hatékonyan működni. A Winword – és valamennyire az Excel makro is – olyan lehetőség, amire alig-alig van egy felhasználónak szüksége, és csak a kifejezetten gyakorlottabb felhasználó szánja rá magát makró írásra. Viszont ilyen módon még az a felhasználó is elindítja a makróval megvalósított "programokat", aki egyébként csak a kész programokat (szövegszerkesztő, táblázatkezelő, stb.) futtatná. Ezeket a makró programokat készen kaphatja egy-egy levélhez csatolva. Szinte tálcán van felkínálva mindenkinek a támadási eszköz és lehetőség, ne csodálkozzunk, ha van, aki felhasználja.

Az Office 98 esetében a makróvírusnak további rombolási lehetősége is van a korábbi Office változatokhoz képest. Minden adatállomány lényeges attribútuma létrehozásának vagy az utolsó módosításának az időpontja. A makró vírussal fertőzött, és ezért módosított file-t – nyilván a "szórakozott" felhasználó rosszul értelmezett védelmében –akkor is menti a Winword, ha a kilépéskor ezt kifejezetten ellenezzük, ilyen módon meghamisítva a file keltezését. Ez viszont igen veszélyes, kellemetlen és valódi ügyvitelnél semmiképpen nem megengedhető, az ügyvitel hitelességét veszélyezteti.

4. A szoftver követés kockázata

Az újabb szoftver verziók bevezetése is jelenthet kockázatot. Ez abban áll, hogy az újabb változat (esetleg csak vélt, vagy az adott környezetben nem is szükséges) jobb funkcionalitása által elérhető haszon nincs arányban a szoftver beszerzési költségével, a hozzá szükséges hardver bővítéssel, tanulási, stb. ráfordítással. Nem véletlen, hanem nagyon is racionális gazdasági megfontolás következménye az, hogy azokban az országokban, ahol az informatika nálunk előbb terjedt el, a magyarországinál jóval nagyobb arányban használnak régebbi szoftver verziókat. (Pl. az Egyesült Államokban, Angliában a Windows 3.11 még mindig kiterjedten használt a Windows 95, 98 mellett.)

Bár többé kevésbé a legtöbb szoftver gyártóra áll, de a Microsoft cég esetében különösen igaz, hogy a fejlesztések "eredménye" már régóta nemcsak elsősorban újabb funkciók kialakítása, vagy a mindenhol – így természetesen a Microsoft programokban is – bőven meglévő programhibák kijavítása, hanem az, hogy újabb és újabb szoftver verziók megvásárlására kényszeríti a felhasználókat. Ebben egyik leghatékonyabb "eszköz" az új változatokkal együtt az egyre újabb, egymással inkompatibilis adatstruktúrák bevezetése – lényegében a valós funkciók kiterjesztése nélkül – amivel az új szoftvert megvásárló kisebbség kényszeríti a többit is az új változatok beszerzésére. Az újabb, az előbbitől eltérő felhasználói interface is azt sugallja, hogy valóban valami újról van szó, mivel az eddig megszokott műveleteket is csak másként tudjuk elvégezni.

Az addig egységes szoftver platformon jól működő együtt dolgozó csoportok munkája felborul, szétesik csak azért, mert néhányan áttérnek az új, funkcionálisan semmiképpen nem is indokolt változatra. A probléma nem csak az, hogy a különböző verziókban megszerkesztett és elmentett dokumentumok egymással nem kompatibilisek. A kompatibilitás érdekében a korábbi verzió szerint elmentett dokumentum immár arra is alkalmatlanná válik, hogy az elmentő a következő lépésben saját maga folytassa a munkát, mert az elmentett és újra betöltött dokumentum külön "bűvészkedés" nélkül nem alkalmas a továbbírásra, gyakorlatilag előbb újra kell formázni. A változatok közötti inkompatibilitás eredménye, hogy éppen a bonyolultabb struktúrájú, nagy dokumentumoknál nehéz a szövegszerkesztő szolgáltatásait kihasználni, és gyakorlatilag még mindibb kényelmesebb a korábbi változatoknál egyedül lehetséges kézi szerkesztéshez visszatérni. De így mit érnek az új lehetőségek? (Míg a Winword esetében egyszerű volt a 2-esről a 6-os változatra való átállás, a továbblépés már korántsem ilyen egyszerű. Különösen kellemetlen inkompatibilitási terület a fejezetszámozás és a számozott listák összekapcsolása az Office 98-nál.)

A nagyobb felhasználók számára külön is van ennek a "belső" inkompatibilitásnak kellemetlen következménye. Lehetetlen az új változatokra való fokozatos áttérés, ez a belső munkarend veszélyeztetése nélkül csak úgy lehetséges, ha minden gépen egyszerre történik meg az átállás, ami még egy nagy felhasználó számára sem elhanyagolható, egyszerre fellépő nagy költséget jelent. Vagy alternatívaként marad hosszú időre bezárva lenni a régebbi változatba. (Sok nagy cég valóban ezt az utat választja.)

A szabványosítás célja az, hogy a különböző gyártók termékeit egymással símán össze lehessen kapcsolni, egymással símán együtt tudjanak működni. A megbízható, jó termékek gyártói szívesen veszik ezt, mert így a felhasználókat fokozatosan a saját termékeikre szoktathatják át, az áttérés senkinek sem jelent törést. Láthatóan a Microsoft felfogása a szabványokról is meglehetősen különös, amikor a szabványosodó rendszereknek (Java, HTML) elkészíti a Microsoft verzióját. Ilyen módon, tekintve termékeinek elterjedtségét, a kompatibilitás és kommunikáció érdekében sokan kénytelenek a Microsoft termékeket is megvásárolni. Nem véletlen, hogy pl. a Java ügye bíróság elé is került, és a bíróság is elmarasztalta a Microsoft-ot.

5. Adatvédelem

Bizonyára sokan elgondolkoztak már azon, hogy ugyanazon winword formátumú file két változatának a hosszát összehasonlítva az egyiké többszöröse lehet a másiknak.

Ennek oka abban van, hogy a mentés "fast save" opcióval, vagy anélkül történt. Ez ennyiben csak a háttértár gazdaságos használatát érinti. Aki azonban más programmal beletekint a változatokba, ennél nagyobb meglepetésben is részesülhet. A file-ban jobb esetben csak információs "szemét" található, de az is előfordulhat, hogy más adatállományok kisebb-nagyobb töredékeit fedezi fel benne. Noha a Microsoft mára már felszámolta ezt a súlyos adatvédelmi hiányosságot, de aki valaha valakinek elektronikus formában átadott bármilyen dokumentumot, nem kell föltétlenül sokáig keresnie annak okát, hogy milyen módon kerülhettek bizalmas (cég)információk mások birtokába.

6. Néhány védekezési ötlet

Mindenképpen szükséges azok ellen az illetéktelen, káros beavatkozások ellen védekezni, amit a memóriavédelemnek a Microsoft rendszerekben található hiánya tesz lehetővé. Munkaállomásként egy Windows operációs rendszerű PC kellő óvatossággal még elviselhető kockázatot jelent, de szerverként általában megengedhetetlen biztonsági kockázat. Pedig ezeknek a gépeknek megfelelő hardvere van a biztonságos működéshez, mint azt a Linux használata is bizonyítja. Egy tűzfalal védett hálózatban, ahol a tűzfalon belül csak "megbízható" felhasználók vannak, akik a szerverre közvetlenül nem jelentkezhetnek be, csak a kívülről jól védett hálózaton keresztül érhetik el az adatállományait, egy NT szerver még jó szolgálatot tehet, de nyíltabb helyen alkalmazva ezeket a szervereket, a veszély túl nagymértékű. *Ha PC szervert akarunk használni, lehetőleg ne használjunk Microsoft szoftvert, a Unix (Linux) alapúak sokkal védhetőbbek.*

Mindenképpen *szükséges a vírusok elleni védekezés* is, mert ezek a jószándékú, mit sem sejtő felhasználókon keresztül is működhetnek. Hogyan, mi módon védhetjük magunkat, gépeinket, adatállományainkat? A Microsoft szövegszerkesztők, táblázatkezelők elterjedtsége, kellemes és jól használható volta mellett aligha lehetséges ezek kiiktatása. A makrók működését még nem támogató Winword2-höz sem igen lehet már visszatérni. De azt megtehetjük, hogy a makrók ellen lehetőleg védekezünk. Mivel ezek a normal.dot file-be kerülnek elmentésre, legyen azonnal gyanús, ha a kilépéskor a "normal.dot file changed, save it?" üzenetet kapjuk. Válaszunk legyen határozott "No", és azonnal kezdjük nyomozásba, virustakarításba. Szükséges a vírusvédő eszközök állandó és rendszeres használata, mind a munkaállomásokon, mind a szervereken. Sajnos, ezen eszközök vásárlási költségein kívül további költséget jelent az is, hogy erősebb és ezért drágább gépekre van szükség (CPU sebesség, memória).

Mivel a Microsoft szoftver elterjedtsége miatt a hackerek bőséges sikert remélnek, egyéb feladatokra (levelezés, web navigáció) lehetőleg ne a Microsoft eszközöket használjuk (Bár a vírusok ezeken keresztül is megérkezhetnek, az eddigi tapasztalatok szerint kisebb az esélye annak, hogy a hálózaton keresztül mi is terjesztőiké váljunk.) Nagyon jó alternatív eszközök vannak, és az esetlegesen csak a Microsoft eszközökben megtalálható újdonságok nem érik meg a kockázatot. Várjuk meg, amíg az újdonság letisztul.

Fontoljuk meg azt is alaposan, mielőtt új verziójú (Microsoft vagy egyéb) szoftvert telepítenénk, hogy szükséges-e az, milyen következményei lesznek a munkánkra, adatvédelmünkre, kooperációinkra, esetleges jelentős hardver bővítést is szükségessé téve.

Vigyázat, a Microsoft szoftver használata különösen komoly biztonsági, (és esetleg eredményességi) kockázat! Szerencsére, az eddigi kiterjedtebb vírustámadások többé-kevésbé ártalmatlanok voltak, mivel nem okoztak lényeges, nem helyrehozható károkat, hanem elsősorban a levelező rendszerekben okoztak forgalmi dugókat, bosszúságot. – Esetleg a szerzőik talán csak demonstrálni akartak? – De még elgondolni is rossz, hogy egy valóban rosszindulatú támadó mi mindent érhetne el ilyen módon, ezekkel az eszközökkel. Erre is volt már precedens, szintén Microsoft eszközre építve, de ennek ismertetését biztonsági okokból ezúttal mellőzzük.

7. Zárszó

Az itt elmondottak elsősorban a Microsoft szoftver kockázataival foglalkoztak. Ennek jó oka a Microsoft termékek nem ok nélküli igen nagy elterjedtsége, és az, hogy ennek ellenére ezen termékek az átlagosnál és elvárhatónál kevésbé védettek. A két tényező együtt különösen komoly kockázat növelő. De bár a statisztika szerint ezek a kockázatok nagyon sok felhasználót érintenek, természetesen a más gépeket is érintő direkt támadásokra is fel kell készülni.

Budapest, 1999. május 6.