Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2011. II. negyedéves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2011. második negyedéves jelentését, amely a negyedév legfontosabb IT- és hálózatbiztonsági momentumait gyűjti egybe és értékelést ad ezen technikai információk társadalmi és gazdasági hatásainak vonatkozásában az Információs Társadalomért Alapítvány közreműködésével, valamint bemutatja a VirusBuster Kft. informatikai biztonsági trendjeiről szóló összefoglalóját. A jelentésben a főszerep ismét a hálózatbiztonságé.

A jelentés betekintést nyújt az informatikai biztonság berkeibe a magyar közszféra szemszögéből mind a hardwer- és software ellátottság tekintetében, valamint a biztonság egyéb aspektusaira is kitérünk, úgy mint a nemzeti adatvagyon kérdése, az e-egészségügy, az elektronikus távoktatás és az információs terrorizmus.

Egy-egy cikk erejéig kitérünk a „szürke kalapos” hekkerek tevékenységére, az országokon átnyúló incidenskezelésben érintett felek illetékességének jogi vonzataira és a rootkit-ek érzékelésére is.

A Nemzeti Hálózatbiztonsági Központ továbbra is eredményesen működteti szakmai közönségének és partnereinek szóló IT biztonsági oldalát a Tech.cert-hungary.hu-t.

Az oldalon a látogató megtalálhatja a legfrissebb szoftversérülékenységi és riasztási információkat, valamint a TechBlog hírfolyam naponta frissülő nemzetközi hírekkel és érdekességekkel látja el a hazai olvasótábort, magyar nyelven.

Mindenkor fontos megemlítenünk, hogy a jelentésben szereplő adatok, értékek és kimutatások a PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ, mint Nemzeti Kapcsolati Pont hazai és nemzetközi kapcsolatai által szolgáltatott hiteles és aktuális információkon alapszanak.

Bízunk abban, hogy ezzel a jelentéssel egy megbízható és naprakész ismeretanyagot tart a kezében, amely hatékonyan támogatja majd az Ön munkáját és a legtöbb informatikai és internetbiztonságban érintett szervezetnek is segítséget nyújt a védelmi stratégiai felkészülésben.

A Puskás Tivadar Közalapítvány - Nemzeti Hálózatbiztonsági Központ (CERT-Hungary) nevében:

Dr. Angyal Zoltán
Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ
hálózatbiztonsági igazgató

Dr. Suba Ferenc
Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ
nemzetközi képviselő

Dr. Kőhalmi Zsolt
Puskás Tivadar Közalapítvány
a kuratórium elnöke

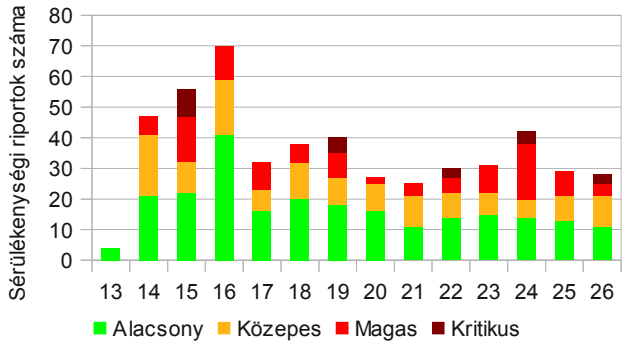
Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

Szoftver sérülékenységek

Szoftversérülékenység minden olyan szoftver gyengeség vagy hiba, amelyet kihasználva egy rosszindulatú támadó megsértheti az informatikai rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását.

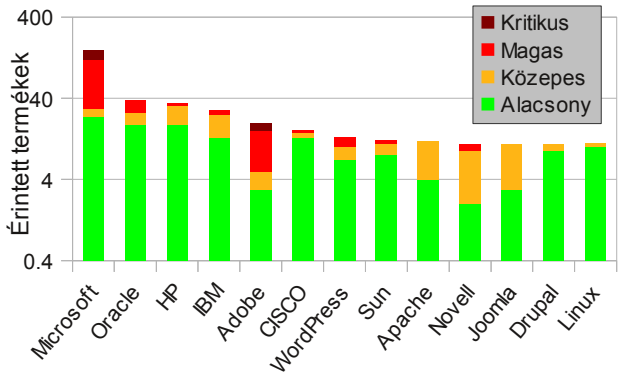
A **PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ (NHBK)** 2011. második negyedéve során **499 db szoftver-sérülékenységi információt** publikált, amelyekből 236 db alacsony, 134 db közepes, 105 db magas és 24 db kritikus kockázati besorolású.

Sérülékenységi riportok eloszlása



Az előző negyedévhez képest 6%-kal nőtt a kiadott sérülékenységi információk száma. Legnagyobb számban áprilisban kerültek kiadásra sérülékenységi információk, melyek több mint 40%-át teszik ki az összes publikációnak.

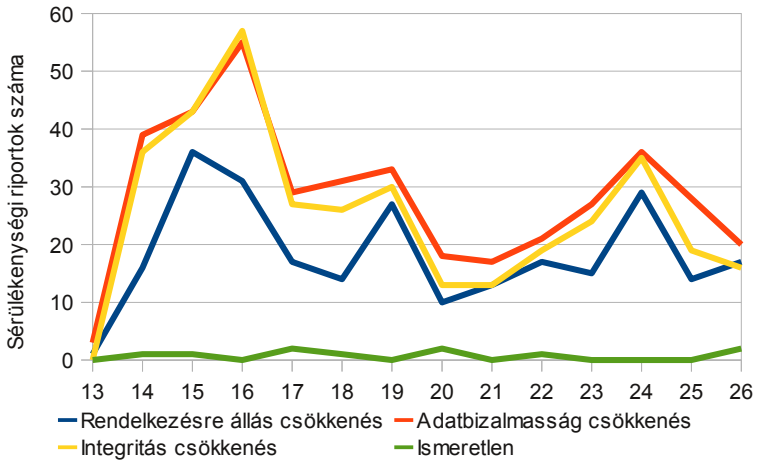
Sérülékenységi riportok a TOP10 gyártó termékeit illetően



Ahogy a grafikonon is jól látszik a sérülékenységek által érintett szoftverek kimutatásában még mindig a Microsoft áll az élen többszörös túlsúllyal az Oracle, HP és IBM trió előtt. Ugyancsak az ötödik helyen áll a kimutatásban a Adobe, de ezen termékek háromnegyede magas és vagy kritikus sérülékenység által volt érintett. Ugyanez a kimutatás a Microsoft esetében már 80%, de itt jóval nagyobb az egyes sérülékenységek által érintett rendszerek számossága, 154-ből 124 termék volt magas és vagy kritikus sérülékenység által érintett.

A sebezhetőségek értékelésénél fontos az, hogy a biztonságon belül mit fenyegetnek, azaz mit tesznek lehetővé a támadók számára. Ennek alapján a felhasználók jobban képet alkothatnak arról, hogy az egyes érintettségek kiderülése esetében milyen veszélyekkel kell szembenézni. A bizalmasságot fenyegető veszélyek kiaknázásával információt nyerhetnek a támadók a számítógépeinkről, a sértetlenség sérülésével a támadó módosíthatja adatainkat, program-jainkat, míg az elérhetőségre vonatkozó támadásokkal a gépünk rendes működését akadályozzák meg a támadók (ideértve a programjaink törlését és akár gépeink más célú felhasználását – zombi-hálózathoz csatolását).

Sérülékenységek eloszlása, azok sikeres kihasználásval előidézhető a rendszerre gyakorolt hatásuk vonatkozásában



Informatikai biztonság a közszféra szemszögéből

A közszféra, egy igen sokrétű heterogén terület, amelyben éppúgy megtalálhatók a központi és az önkormányzati hivatalok, mint az egyéb közintézmények, állami vállalatok, az oktatás, az egészségügy, stb. A közszféra stabil és akadálymentes működése jelentősen kihat a többi területre is, hiszen mind a civil szektor, mind a gazdaság működéséhez szükség van a rendszeres elektronikus interakcióra a különböző központi informatikai rendszerekkel, így kijelenthető, hogy stratégiai jelentőségű területről van szó.

IT a közszférában

A közszféra hardver-ellátottsága

Ma az intézményi feladatok jelentős részéhez legalább annyira elengedhetetlen a megfelelő informatikai háttér megléte, mint a vállalatok üzletmenetszerű működéséhez.

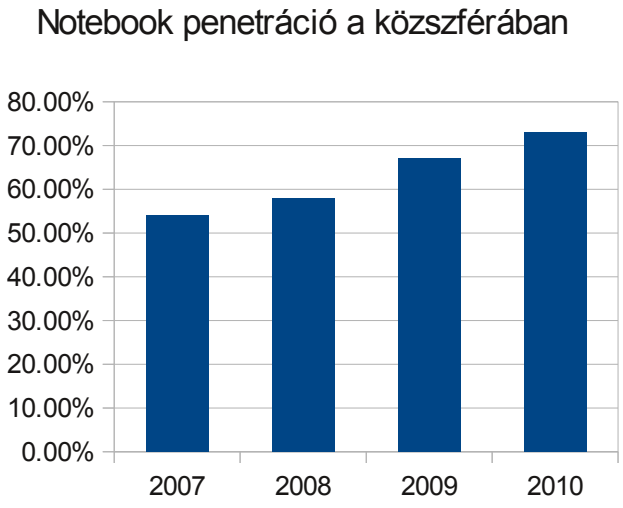
Az e-kormányzati funkciók kiteljesedésével, az így kínált szolgáltatások általánossá válásával a jövőben tovább fog növekedni az intézmények IT-rendszerekkel szembeni kitettsége. Ráadásul e szervezetek egy részénél állampolgárok nagy mennyiségű érzékeny, bizalmas adatát kezelik, így a kockázat hatványozódik.

A BellResearch elemzői a Magyar Infokommunikációs Jelentés legutóbbi adatai[1] alapján az intézmények körében trendszerű változásként leginkább a mobilitás iránti igény egyre markánsabb megjelenését emelik ki. A hazai közszféra számítógép-ellátottsága évek óta teljesnek mondható.

Az intézményi összevonások és konszolidációk következtében az állomány egyes szegmensekben csökkent ugyan, összességében azonban alig mutat elmozdulást az előző éves adatokhoz képest.

Mind a lakosság, mind a vállalatok körében évek óta megfigyelhető a hordozható számítógépek térnyerése a helyhez kötött, asztali konfigurációkkal szemben. Hála az árcsökkenésnek és a fejlett notebookokra jellemző széles körű funkcionalitásnak, ezek a kompakt eszközök a globális értékesítésben már átvették a vezető szerepet, sőt az eladásokat a legkisebb és legolcsóbb netbook-kategória reprezentánsai húzzák.

Tevékenységük jellegéből fakadóan az intézményeknél könnyebben nélkülözik a hordozhatóságból fakadó előnyöket, az itthon jellemző alulfinanszírozottságuk okán pedig nehezen fizetik meg a mobilitás - igaz, egyre csökkenő - árprémiumát. A fokozatos, de állandó változás a fentiekkel együtt is megkérdőjelezhetetlen - mutatnak rá a BellResearch kutatói. Bár ma még az intézményi installált bázis csaknem 90%-át továbbra is az asztali gépek teszik ki, a laptopok penetrációja növekszik.

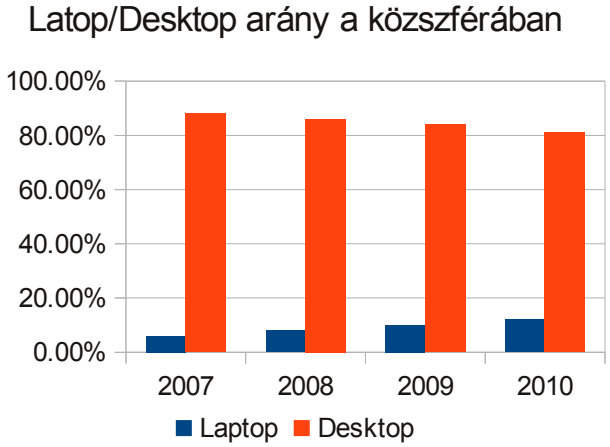


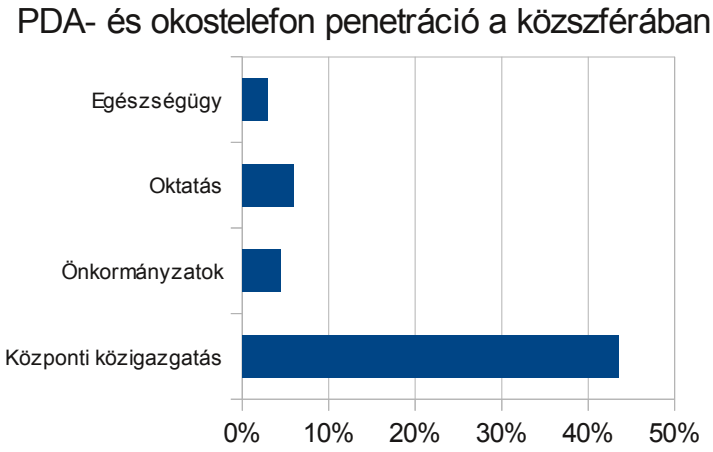
Míg a Jelentés historikus adatai szerint 2007-ben csak az intézmények valamivel több mint felében találtunk legalább egy notebookot, ma már 75%-os ez az arány. Ugyanakkor nem szabad figyelmen kívül hagyni, hogy az egyes szegmensek némileg eltérő fejlődési utat járnak be, illetve a változások eltérő szakaszában tartanak. A fejlődés az intézményi

1 Bellresearch: Magyar Infokommunikációs Jelentés 2010.

szféra "zászlóshajójának" tekinthető központi közigazgatási intézmények esetében már a belső penetráció növekedésében, azaz a notebookok részesedésének emelkedésében érhető tetten, míg az oktatási, az önkormányzati és az egészségügyi szegmensekben számos intézmény az első laptopbeszerzéseit hajtotta végre az elmúlt két-három évben.

A Jelentés adataiból kiolvasható, hogy épp annak a szegmensnek az állományában találjuk a legkevesebb hordozható pc-t, amely az új, akár mobilmegoldások legpotensebb felhasználója lehetne. Míg a szállítók prospektusairól a viziteken is érintőképernyős tablet-pc-t használó orvosok vagy távdiagnosztikát alkalmazó háziorvosok képe néz vissza, idehaza az egészségügyi intézmények hardverleltárában alig 7 %-ot tesz ki a laptopok aránya, ami alig fele az önkormányzati szegmens idevágó adatainak.





A pda-k és az okostelefonok mint személyes kommunikációs eszközök a kommunikáción túl számos funkciót biztosítanak, kétségtelen azonban, hogy az elektronikus kapcsolattartás különböző formáinak támogatásában a legerősebbek. Az állandó jelenlét és elérhetőség radikálisan lecsökkenti a reakcióidőt, hatékonyabbá téve ezzel a folyamatokat, bár növelve ezzel a munkavállalók terhelését. Az eltérő finanszírozási kereteken túl szemléletbeli különbséget is tükrözhet a gazdaság és az intézményi szféra viszonya ezekhez az eszközökhöz.

Míg azonban a vállalati kör az előnyöket felismerve évről-évre nagyobb arányban szerez be okostelefonokat és pda-kat, addig az intézményeknél jellemzően még ma is státusszimbólumként tekintenek rájuk, számottevő mértékben csak a központi költségvetési szegmensben hódítottak teret.

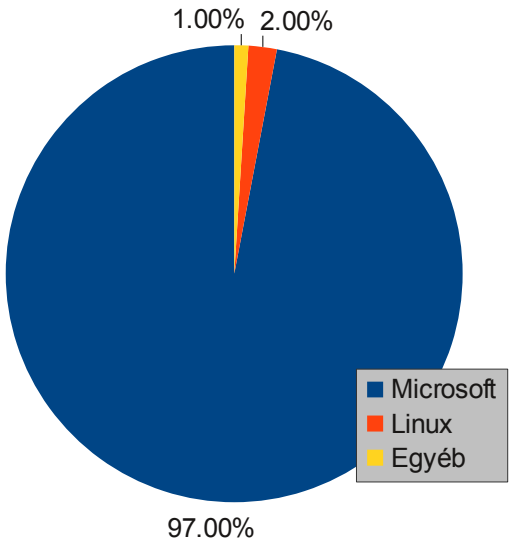
A közszféra egészét tekintve csak elvétve, a szervezetek 4-6 %-ánál alkalmaznak pda-kat vagy okostelefonokat. Így bár a mobilitás iránti igény az intézmények esetében is kétségtelenül növekszik, a következő lépcsőfoknak számító, "always on, always online" filozófia számottevő térhódítására még várni kell - mutatnak rá a BellResearch elemzői. E téren az üzleti szféráétól eltérő küldetésből és folyamatokból fakadóan az intézményi szegmens hosszú távon is valószínűleg eltérő utat jár majd be.

Szoftverek a közszférában

A termékkövetést tekintve az óvatos verziófrissítés az intézményi IT-döntéshozókat legalább annyira jellemzi, mint amennyire a vállalatok informatikai vezetőire érvényes ez az attitűd. Bár a mennyiségi licenckonstrukcióknak köszönhetően az upgrade lehetősége jellemzően adott, ma még a két generációval ezelőtti XP csaknem 90%-os részesedést ér el a windows-os pc-k bázisán. Az áttörést ebben a szegmensben a későbbiekben esetleg a Windows 7 hozhatja meg, hiszen a piacon összességében is csak korlátozott sikerességnek örvendő Vista részesedése az intézményeknél a Windows 2000-ét sem éri el.

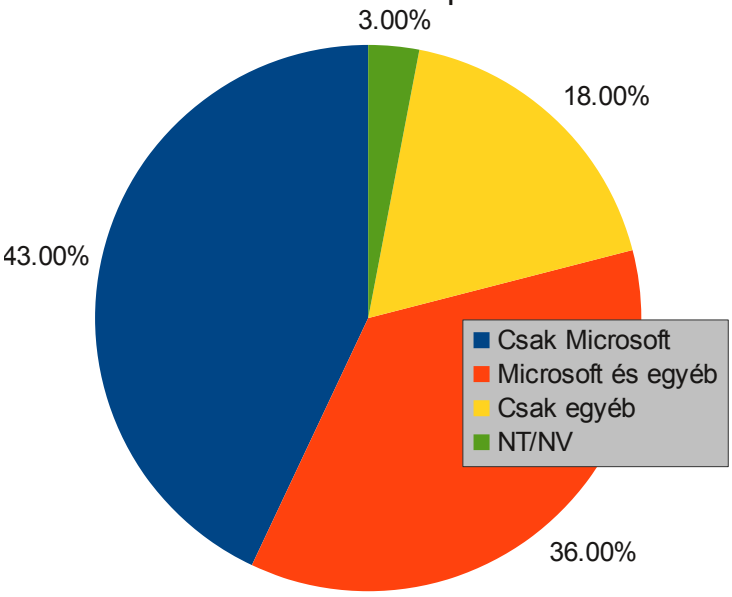
A klienseken legszélesebb körben használt alkalmazásokat egyértelműen az irodai programcsomagok jelentik. Alig akad olyan intézmény, sőt alig találunk olyan pc-t, amelyen ne futna legalább egy szövegszerkesztő vagy táblázatkezelő. Némi változás a megoldások szállítóit illetően tetten érhető. Míg korábban szinte kizárólag a Microsoft Office valamely verzióját szerezték be az irodai programokra igényt tartó szervezetek, a nyílt forráskód lassanként teret nyer. Vélhetőleg kompatibilitási okokból a Microsoft Office teljes mellőzése igencsak kevés intézményre jellemző, a vegyes használat terjed, a vizsgált entitások körében megközelíti az egyötödöt azoknak a szereplőknek a száma, amelyek más szállító termékét is alkalmazzák.

A közszféra kliensoldali operációs rendszerei



A szerverek esetében jóval heterogénebb képet mutat a szoftverleltár. Bár a Microsoft-termékek a hálózati operációs rendszerek között is a legelterjedtebbeknek számítanak, a Linux alapú megoldások jelentős teret harcoltak ki maguknak.

A közszféra szervezoldali operációs rendszerei



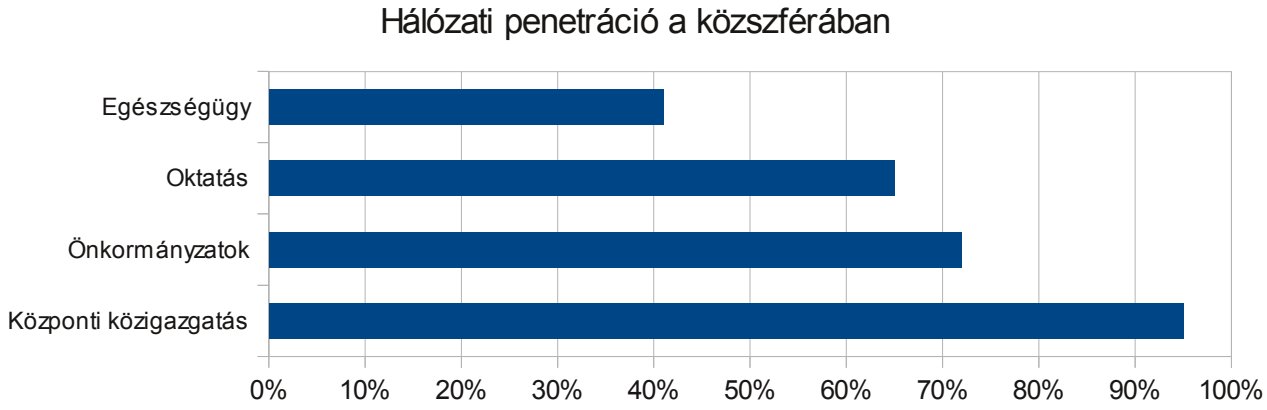
Jóllehet jelenleg többségben vannak azok a saját menedzselésű szerverrel rendelkező intézmények, amelyek kizárólag microsoftos szerveralapokon építkeznek, meghaladja az egyötödöt az olyan vizsgált entitások aránya is, amelyek kizárólag alternatív szállítók rendszereit, illetve szabad szoftvereket használnak.

Az egyes intézményi szegmentumok között e tekintetben is csak minimális eltérést találunk, vagyis nem állítható, hogy a Windows szerverek az egészségügyben vagy az oktatásban nagyobb teret kapnak, mint összességében a közszférában, a központi közigazgatási szervezetek körében az átlagosnál heterogénebb összetételű szoftverparkról beszélhetünk. A kutatók ebben részint az eltérő erőforrás-ellátottságot, részben az igények különbözőségére utaló jeleket ismernek fel. Kétségtelen, hogy az egységes eszközpark üzemeltetése jellemzően költséghatékonyabb lehet, ám nagy komplexitású megoldandó feladatok esetében mégis adódhatnak olyan feladatok, ahol - ha rendelkezésre áll a szükséges kompetencia - a specializáció hordoz jelentősebb előnyöket.

Hálózatok a közszférában

A közszféra jelentős része továbbra sem használja ki az eszközök hálózatba szervezésében, az erőforrások megosztásában rejlő potenciált.

Noha számítógépeket már évek óta gyakorlatilag valamennyi hazai intézmény alkalmaz, sőt csaknem 95 %-nál legalább két pc található, az eszközök jelentős része továbbra is szigetszerűen alkalmazott munkaállomás. A hatékonyságot nagyban fokozó, az erőforrások megosztását lehetővé tevő helyi hálózatok elterjedtsége a Magyar Infokommunikációs Jelentés adatai szerint mindössze 70 %-os.



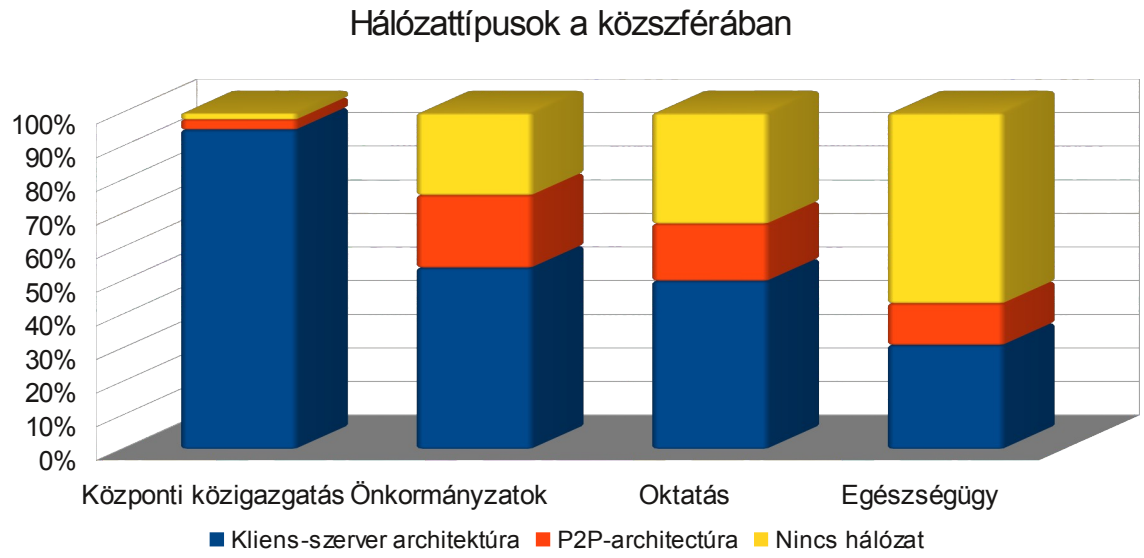
A lemaradás az egészségügyi intézményekben a legjelentősebb. Bár kétségtelen, hogy az ehhez a szegmenshez tartozó járóbeteg-, illetve szociális ellátást végző entitások körében a legmagasabb az egy munkaállomással rendelkezők súlya, az 50% alatti hálózati penetráció így is szembeötlő. Az erőforrások megosztásával elérhető hatékonyságnövekedést tehát épp az a szegmens kényszerül leginkább nélkülözni szűkös anyagi lehetőségei miatt, amelynek erre a legnagyobb szüksége lenne.

Nem kevésbé problémás az önkormányzatok vagy az oktatási intézmények helyzete sem. Ezek körében alig akad olyan intézmény, ahol ne találnánk legalább két PC-t, ehhez képest hálózati penetrációjuk messze elmarad a teljestől, pedig ahol több számítógépet is használnak, ott felmerül a fájlokhoz való közös hozzáférés, a nyomtató vagy az internetkapcsolat megosztásának igénye és még korántsem beszéltünk az integrált szoftverrendszerek használatának hiányából származó veszteségről.

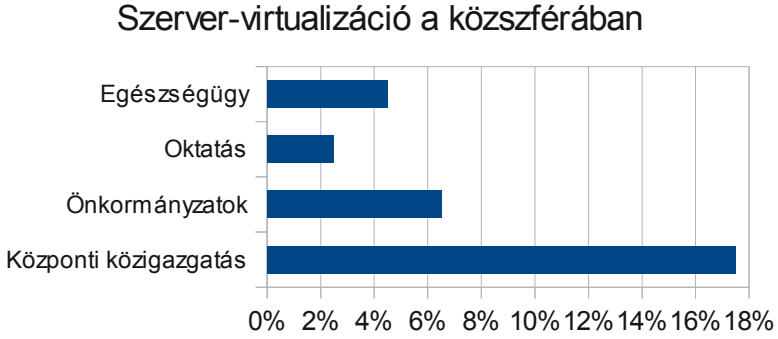
Az évente ismételt vizsgálatok ráadásul a lemaradás konzerválódására hívják fel a figyelmet a kutatók, hiszen csak kismértékű elmozdulás mutatható ki. Így digitális szakadékról nem csupán a lakosság esetében beszélhetünk, de a közszférára vonatkozóan is értelmezhető a leszakadókat az élenjáróktól elválasztó fogalom.

Az intézmények fejlettsége erőteljesen polarizált képet mutat. Azok az intézmények, amelyek hálózatot építenek ki, jellemzően szerverrel is rendelkeznek (73%), a P2P-architektúra meglehetősen ritka. A hálózati evolúció nagyobb lépcsőkre osztható, az intézményi ellátottság kissé szélsőséges képet mutat. Vagy csupán szigetszerűen alkalmazott számítógépekről beszélhetünk hálózati kapcsolat nélkül, vagy van hálózat, de ahhoz jellemzően már dedikált szerver, illetve szerverek is tartoznak.

Hardverek terén a kormányzati szektor intézményei és egyéb, jelentősebb IT-forrásokhoz hozzáférő közintézmények a nagyvállalatok hálózataihoz mérhető professzionalitással kiépített hálózattal is rendelkezhetnek, míg a kisebb/lokális intézmények esetében a leszakadás igen markáns.



A szerverek hatékonyabb kihasználását elősegítő virtualizációs technológiák terén a hazai közszféra is megtette már az első lépéseket. Jelenleg a kiszolgálóval rendelkező intézmények közül húszból egy alkalmaz ilyen megoldást. A központi költségvetési szegmens e tekintetben is élenjáró, itt csaknem minden ötödik intézmény érintett a szervervirtualizációban, ami csaknem pontosan megegyezik a nagyvállalatok idevágó adatával.



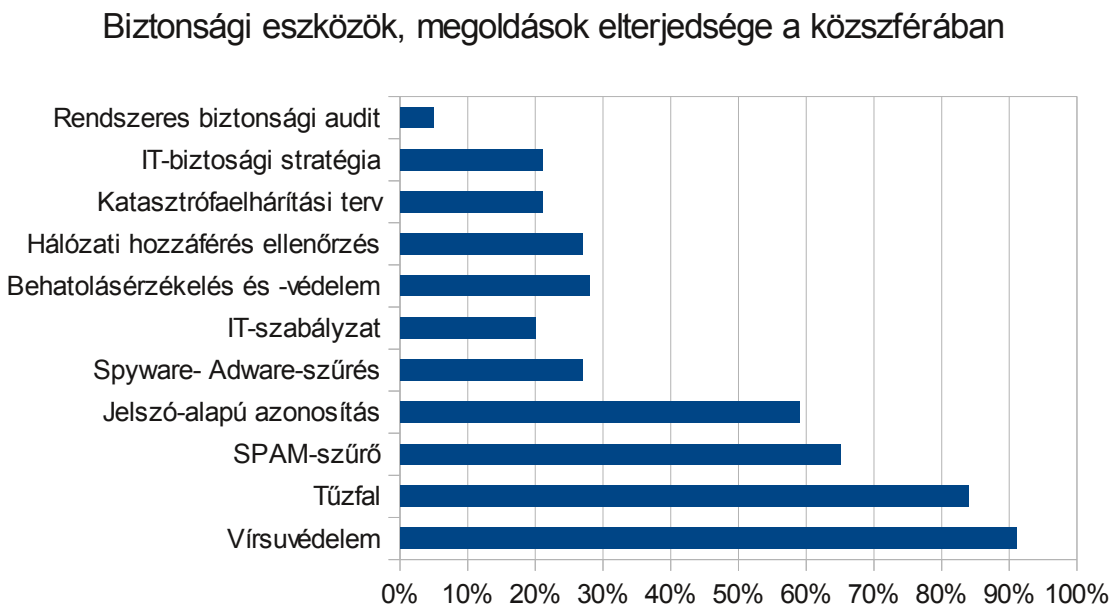
Hálózatok és szerverek tekintetében az intézményi kör tehát kettéosztott, és ez időben csak nagyon lassan változik.

IT-biztonság

Az intézmények biztonsági törekvéseit is az eszközszintű védelem jellemzi, de a vállalatokénál nagyobb arányban rendelkeznek vonatkozó szabálygyűjteménnyel és stratégiával.

Ma az intézményi feladatok jelentős részéhez legalább annyira elengedhetetlen a megfelelő informatikai háttér megléte, mint a vállalatok üzletmenetszerű működéséhez.

Az e-kormányzati funkciók kiteljesedésével, az így kínált szolgáltatások általánossá válásával a jövőben tovább fog növekedni az intézmények IT-rendszerekkel szembeni kitettsége. Ráadásul e szervezetek egy részénél állampolgárok nagy mennyiségű érzékeny, bizalmas adatát kezelik, így a kockázat hatványozódik.



Különösen nagy jelentőségű tehát, hogy milyen elgondolások szerint és milyen megoldásokra támaszkodva építik ki a hazai intézmények IT-biztonsági rendszereiket. Valamilyen IT-biztonsági megoldást már gyakorlatilag valamennyi hazai intézmény alkalmaz ugyan, de csak az alapvető eszközök (antivírus, tűzfal, levélszemét-szűrés, jelszó alapú azonosítás) elterjedtsége tekinthető kis jóindulattal megfelelőnek.

Az informatikai biztonság persze korántsem merül ki a rendszerek sebezhetőségét csökkentő szoftver- és hardverkomponensek használatában, túlmutat azokon. A kockázatok valódi mérsékléséhez stratégiai szemléletben előkészített terveken alapuló döntések sorozatára van szükség, írásba foglalt, rendszeresen felülvizsgált és következetesen betartatott szabályokra. A hardver- és szoftverkomponensek ezek megvalósulási formáiként értelmezendők.

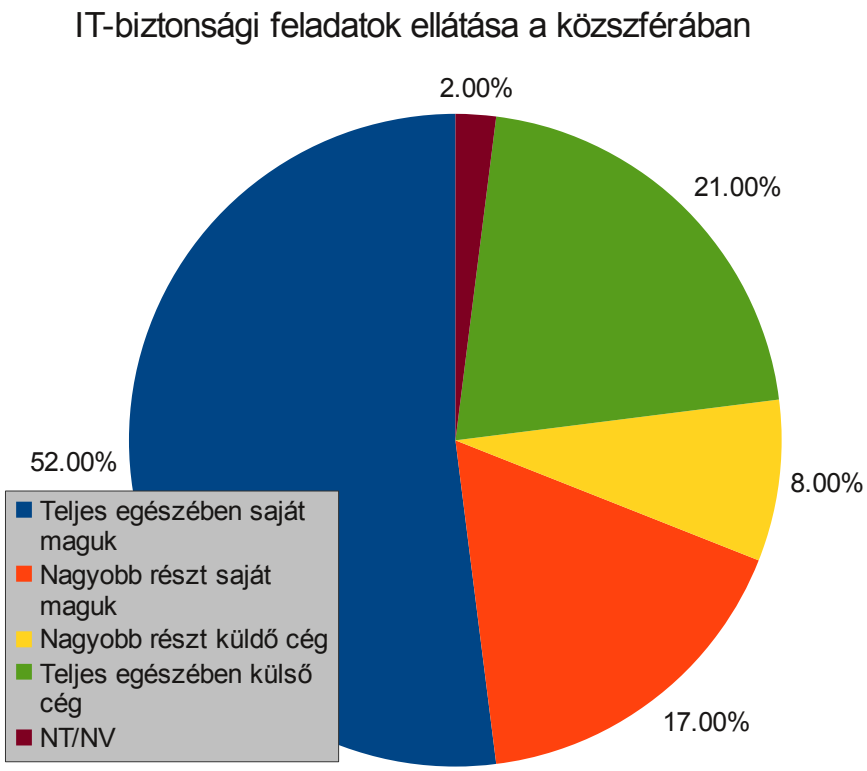
Épp a szabályozás, az IT-biztonsági stratégia és szabályok megalkotása az a terület, ahol bár az intézményi szféra mutatói - többek között jogszabályi kötelezettségeik miatt is - kedvezőbbek a vállalatok adatainál, a fejlődésnek finoman fogalmazva is igen tág tere van.

A közszféra IT-biztonsági felkészültségét tekintve meglehetősen heterogén képet mutat. Míg az olyan szofisztikáltabb megoldások, mint a fájltitkosítás vagy a behatolás-érzékelés, a központi költségvetési intézmények körében elterjedtnek tekinthetők, addig az önkormányzati, az oktatási vagy az egészségügyi intézmények biztonsági repertoárját jellemzően csak az antivírus, a tűzfal, a levélszemét-szűrés és a jelszó alapú azonosítás négyese alkotja. Különösen aggasztó, hogy biztonsági stratégiával, szabályzattal vagy katasztrófa-elhárítási tervvel a központi költségvetés alá tartozó szegmenst leszámítva csak elvétve lehet találkozni. Biztonsági audit elvégzésére pedig összességében húszból alig egyetlen intézmény vállalkozik.

Az összkép tehát, bár hosszabb távon kirajzolódnak az egyértelmű fejlődés jelei, korántsem megnyugtató. Különösen annak fényében van okunk aggodalomra, ha figyelembe vesszük egyes intézményi szereplők gazdaságra, sőt a társadalom egészére vonatkozó jelentőségét. Egy rendszerleállás, adatvesztés vagy szenzitív adatok illetéktelen kezekbe kerülése esetükben nem pusztán üzleti kockázatokat hordoz, mint a cégeknél, hanem országos jelentőséggel bír.

Az IT-biztonsági feladatok ellátásakor a közszférában elsősorban saját belső erőforrásaikra támaszkodnak: a közintézmények kevesebb mint fele von be bármilyen formában külső vállalkozót, míg a teljes kiszervezés egyáltalán nem mondható jellemzőnek.

Ennek hátterében jórészt a házon belül tartást szorgalmazó konzervatív szemlélet, valamint a forráshiány áll.



A hiányosságok ellenére a közszféra intézményeinek igen kis része tervezi, hogy komolyabb ráfordításokat allokál az IT biztonsági eszközök, módszerek fejlesztésére a következő egy évben. Különösen a biztonsági területen elmaradottabbnak számító önkormányzati szektor, egészségügy és oktatás területén sajnálatos, hogy az intézmények kevesebb, mint ötöde tervez fejlesztéseket, így e szektorok lemaradása egyre inkább konzerválódik és csak nagyon lassan közelít a vállalati szférában megszokott szintekhez.

A közszféra informatikai biztonságának egyéb aspektusai

A biztonsági komplexitás növekedése

Biztonsági szempontból a két évtizeddel ezelőtti korszak tért vissza az informatika világába – hangzott el a kijelentés az IDC áprilisi IT-biztonsági konferenciáján.[2]

Hiába a védelmi intézkedések a végfelhasználói számítógépeken, hiába vannak biztonsági eszközök a hálózatok peremén, a veszélyek már máshonnan érkeznek.

A korábbi, jól átlátható biztonsági környezetet mára káosz váltotta fel: a mobileszközök és az internetes alkalmazások, a közösségi hálózatok káosza. Ezek folyamatosan újabb és újabb biztonsági réseket nyitnak meg, ahogy ellenőrizetlen és a vállalati informatikai szakemberek számára láthatatlan csatornákon kapcsolják össze a belső hálózatot és az internetet.

Ahogy nő a függés az IT-infrastruktúrától és válik az egyre komplexebbé, úgy nő a szükséges védekezés bonyolultsága is. A legnagyobb fenyegetést a jövőben éppen ez a bonyolultság jelenti. Ma már nem a megfelelő biztonsági eszközök vagy szakemberek megtalálása az igazán nehéz, hanem sokkal inkább ezeknek az embereknek és eszközöknek a hatékony menedzselése, irányítása. Éppen ezért az egyes biztonsági eszközök szolgáltatási szintjéről, tudásáról (persze ez sem elhanyagolható szempont) a súly egyre inkább a szervezet IT-működésének menedzsmentjére, felügyeletére tevődik át.

A védekezés összetettségéből fakad egy másik fontos, ám többnyire szem elől tévesztett következtetés. Ahogy a modern államban a polgár a fizikai erőszakkal szembeni védekezést rábízza a rendőrségre, úgy kell a modern informatikai rendszerek védelmét is rábízni az erre hivatott szolgáltatókra. „A saját magunk által megvívott harc időszakának vége, mert túl sok fronton kell harcolni túl sok ellenséggel. Bizonyos csatákat át kell engednünk másoknak, akik akár a felhőben, akár kiszervezés formájában tudnak gondoskodni a biztonság bizonyos aspektusairól” – állítja Eric Domage, az IDC programigazgatója.

Az intézményeknek igazából csak három dologra kell összpontosítaniuk: legyen biztonsági politikájuk; tartsák be a jogszabályi előírásokat; és tartsák kézben a költségeket. Ami ezen túlmutat, az már mind műszaki kérdés, és mint ilyet, ki is lehet adni szolgáltatóknak. A fenti hármat viszont mindenképpen bent kell tartani a szervezetben.

A biztonsági politikát a szervezetnek magának kell kidolgoznia, neki kell döntenie arról, hogy mit akar védeni és mit nem, mit akar megengedni és mit nem.

Ehhez lehet segítséget kapni tanácsadóktól, de teljes egészében senki nem veheti le a döntést a cégvezetés válláról. Igaz ez a jogszabályi megfelelőségre is: azt sem lehet kiadni, mert a végső felelősség mindig a menedzsmentet terheli. A költségek csökkentésére, kézben tartására pedig jó módszer lehet a szállítói konszolidáció, a virtualizáció vagy az említett kiszervezés.

A mobil eszközök fokozódó szerepe

Hihetetlen ütemben zajlik a mobileszközök térnyerése: a notebookok után a netbookok váltak a mobilitás jelképévé, és biztos a tablet-ek piaci sikere is. Az egyre több funkciót ellátó okostelefonok iránt is meredeken növekszik a kereslet. Az IDC nemzetközi kutatócég adatai szerint[3], míg 2009-ben 236 ezer okostelefon talált gazdára hazánkban, addig 2011-re már közel 1 millió darab eladásával számolnak.

2 Sánta András: Egy hét az államigazgatásban, IT-Business periodikus heti-jelentések, 2011.04-06.
3 IDC Worldwide Quarterly Mobile Phone Tracker, 2011.06.09. http://www.idc.com/getdoc.jsp?containerId=prUS22871611

Ha a munkában nem is, magánemberként egyre több, a közszférában dolgozó munkavállalónál is megjelennek ezek az eszközök, széles körű kapcsolódási lehetőségeiknek köszönhetően nem ritkán a munkahelyi hálózatokra kapcsolódva, vagy töltés/menedzsment célzattal USB-porton keresztül a munkaállomásokhoz csatlakoztatva.

Az egyre nagyobb térnyerésnek örvendő mobileszközök tehát komoly biztonsági kockázatokat hordoznak, amelyek sokszor a nem biztonságos felhasználói szokásoknak és gyakorlatoknak köszönhető. A gyanútlan, hiszékeny és naiv felhasználók könnyen válhatnak visszaélések, csalások, adatlopások áldozatává. A visszaélések személyes és munkahelyi adataikat egyaránt fenyegetik. Tovább nehezíti a helyzetet, hogy az intézményi felhasználók, sőt gyakran még az információbiztonságért felelősök is elsiklanak az ilyen eszközök alkalmazásakor elengedhetetlen biztonsági szempontok felett.

A mobileszközök biztonsági kockázataival kapcsolatban legalább három – egymással szorosan összefüggő – terület érintettségét kell végiggondolni:

- az adatszivárgás elleni védekezés kérdését;
- a vezeték nélküli hálózatok (bluetooth, wifi) biztonságát;
- és azt, hogy az IT valójában a helyükön kezeli-e a mobileszközöket, hiszen mint tudjuk, ezek az eszközök valójában már teljes értékű számítógépek.

Egyre több támadás éri az okostelefonokat is: a legtöbb rosszindulatú incidens hamis hang- vagy szöveges üzenetek formájában éri el a mobilkészülékeket. Ezeknek jelenleg már több mint 500 fajtája létezik. Közös bennük, hogy ravasz módon valamilyen műveletet igyekeznek kiprovokálni - például egy program telepítését vagy működésének elfogadását -, ezért kellő óvatossággal viszonylag egyszerű védekezni ellenük. A szakértők azonban felhívják a figyelmet arra, hogy az automatizált támadások megjelenése és elterjedése várható a jövőben. A legtöbb támadást Kelet-Európában és Kínában regisztrálták egyelőre 88%-ban olyan készülékeken, amelyek a Nokia Symbian operációs rendszerével működtek. (Ezek jelentős része nem is illik bele 100%-ig a valódi okostelefon fogalomba.)

Ennek ellenére a kutatók szerint közösségformáló ereje is lenne, ha a közigazgatás elektronizálása mellett annak mobilizálása is megvalósulna. A műszaki feltételek elméletben adottak és a leendő felhasználók lelkesek – már csak a megvalósítás kellene.

Az elmúlt évek során a technológiai alapok robbanásszerűen kiforrták magukat. Az újonnan értékesített készülékek zöme már okostelefon, internetezési képességgel, GPS-szel, kamerával, letölthető alkalmazásokkal. Vagyis a lakosság körében is terjednek és nagyon népszerűek az új mobiltechnológiák, különösen, hogy az adatátvitel költségei folyamatosan csökkennek, így az egyik oldalról megvan a fogadókészség. A másik oldalról a fejlesztők dolgát könnyíti meg, hogy konszolidálódott a mezőny, és jól látszik, hogy melyik az a pár mobilplatform, amire érdemes fejleszteni.

A mobilitásnak a jövőben mind a közigazgatás belső működésében, mind az állampolgárokkal való kapcsolattartásban nagyobb szerepe lesz.

A terepen végzett munkákat kiválóan tudják segíteni a mobilalkalmazások, amelyek révén a helyszínen rögzített adatok azonnal be tudnak kerülni a központi adatbázisokba.

A másik oldal potenciáljai azonban sokkal nagyobbak: Olyan értelmes közösségi alkalmazásokat kellene fejlesztenie az államnak, amelyek rengeteg felhasználót tudnak bevonni az állammal folytatott interaktív kommunikációba. Egyébként pedig az elektronikus közszolgáltatásoknak mind a négy szintje, az egyszerű információlekéréstől a végigvitt tranzakciókig, megvalósítható mobilon is.

Konkrét példát mondva: nagyon könnyű olyan alkalmazásokat elképzelni (mint ahogy erre már vannak is külföldi megoldások), ahol az állampolgárok bejelentéseket tehetnek egy illegális szemétlerakóról vagy fakitermelésről, kátyúról, és így tovább: ehhez fotót és GPS-koordinátát is egyből lehet mellékelni. De egyébként vannak lehetőségek a gép–gép közötti mobilkommunikációban is.

Természetesen a fentebb hivatkozott biztonsági problémákat a közigazgatás minden szintjén meg kell majd oldani a szolgáltatások hosszú távon is sikeres üzemeltetéséhez.

A nemzeti adatvagyon

Szabályok

Az adatvédelem és információszabadság mindig is kulcsfontosságú területei voltak a tágabban értelmezett IT-biztonsági területnek, az állam, mint legnagyobb adatkezelő pedig még fokozottabban van kitéve támadási lehetőségeknek ezen a területen.

A 2010 végén elfogadott 2010. évi CLVII. törvény[4] a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről, majd az ez év márciusában ezt pontosító 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról, pontosan megmutatja a szektor következő néhány évének fejlődési irányait.

A rendeletben nevesített állami nyilvántartások (szám szerint 23) adatfeldolgozását a jövőben kizárólag államigazgatási szerv vagy 100%-os állami tulajdonban álló gazdasági társaság végezheti – a jogszabály ugyanis előírja, hogy a nemzeti adatvagyon védelme állami feladat, amelynek megfelelő ellátását csak az állam tudja garantálni.

A nemzeti adatvagyon részét képezik azok a jelenleg már elektronikusan vezetett nyilvántartások is, amelyek biztonságos, megbízható és hatékony működése a Magyar Köztársaság gazdasági és társadalmi rendje, valamint a közigazgatás zavartalan működése szempontjából kiemelt jelentőséggel bírnak.

A kormányrendelet többek között állami adatfeldolgozót rendel a polgárok személyi adatait és lakcímét tartalmazó nyilvántartáshoz, a központi útiokmány- és szabálysértési nyilvántartásokhoz, valamint az egészség- és nyugdíjbiztosítási nyilvántartásokhoz is. Az állam részéről adatfeldolgozói feladatokat elsősorban a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEK KH), a Kopint-Datorg Zrt. és a Földmérési és Távérzékelési Intézet (Fömi) végez majd.

A nemzeti adatvagyonról szóló törvény 2011. december 31-éig biztosít átmeneti időt arra, hogy a jelenlegi adatkezelők eleget tegyenek a benne foglaltaknak.

Indokok

Az indoklás szerint a törvény meghozatalának legfőbb indoka, hogy a nemzeti adatvagyon védelme nem megoldott – a 2010. őszén tapasztalt agrártámogatások körül kialakult anomáliák is megerősítették ebben a döntéshozókat. Továbbá az adatbázisok kezelése a korábbi években magáncégekhez került, ami természetesen biztonsági és megbízhatósági kérdéseket vethet fel nem megfelelő monitoring, felelősség-megosztás és szabályozottsági hiányosságok esetén.[5]

A jelenlegi rendszer a jogalkotók véleménye szerint nem hatékony, drága, és az ország számára számos kockázatot jelent.

4 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről

5 Mártonffy Attila: Megvan az adatvagyon 2011. 05. 08., http://www.itbusiness.hu/hetilap/business/Megvan_az_adatvagyon.html

A törvény a további visszaélések megakadályozása érdekében szűkíti az üzemeltetésre jogosultak körét, kizárva a magáncégeket. A törvény ezenkívül módosította a büntető törvénykönyvet is, és bevezette az adatnyilvántartások hozzáférését akadályozó vagy azt lehetetlenné tevőkkel szembeni büntetőjogi eljárás lehetőségét. A közérdeket nagymértékben sértő hátráltatás esetén a módosítás szerint öt évig terjedő szabadságvesztés is kiszabható.

Kritikák

A törvény szellemével a szakma alapvetően egyetért, de számos kritika hívja fel a figyelmet a megvalósítás nehézségeire, ami további kockázatoknak teheti ki ezt a területet.

A kutatók szerint a vállalati szféra teljes kizárása már csak azért sem lehetséges, mivel az új technológiák bevezetése csak a piaci szereplők segítségével lehetséges, valamint sohasem áll rendelkezésre az új fejlesztésekhez elegendő szakember az államigazgatásban, mint az már a 2010-es éves jelentésben is bemutatásra került. A szakma inkább a piaci szereplőkkel történő együttműködést támogatná, ahol a köztisztviselő informatikusok együtt dolgoztak a vállalkozó szakembereivel, az elkészült terméket később működtetésre, továbbfejlesztésre átvéve, támogatást igényelve. Ez akár együttes továbbfejlesztést is jelenthet. Ez a fajta megoldás ugyan hosszabb átfutásokat jelent – a rendelkezésre álló belső erőforrásokat gyakran kell a rövid törvényi határidők miatt átcsoportosítani – viszont biztosítja az intézményi tudás kialakulását és a piaci szereplőknek is lehetőséget ad a hosszú távú együttműködésre.

Az elmúlt néhány évben azonban, gyökeresen megváltozott a helyzet. Az új stratégia a teljes fejlesztés kiszervezése lett, azzal a feltételezéssel, hogy az elkészült terméket később az intézmény „visszaveszi”. Csakhogy a szükséges tudás ma már nem áll rendelkezésre az átvételhez.

Ez több tényezős probléma: az államigazgatási informatikusok életkora (sokan nyugdíjba mentek), a kedvezőtlen –versenyszférától elmaradó - fizetések (három éve gyakorlatilag be vannak fagyasztva a bérek, továbbá a köztisztviselőkre, kormánytisztviselőkre egy alapvetően teljesítménytől független bérrendszer működik), a folyamatos átszervezések, mind nehezítik a megfelelő minőségű és létszámú informatikai csapatok összeállítását a közintézményeknél. Sokan el is hagyták a közszférát.

De az okok közé tartozik az intézmények számára hátrányos szerződések, ill. a szerződéses pontok laza kezelése is.

Ezek után a jogalkotó motivációi érthetők: megszüntetni a kitettséget, visszaszerezni a kiszervezett egységeket, és a törvény szigorú betűit értelmezve félő, hogy átestünk a másik végletbe. A „szigorú” értelmezés szerint ugyanis, csak saját munkatársak, vagy állami vállalti alkalmazottak vehetnek részt a legfontosabb informatikai tevékenységekben azoknál az intézményeknél, melyeket a kormányrendelet a nemzeti adatvagyon egyes elemeinek tulajdonosaként felsorolt. Az intézmények jelentős része egyszerűen nem fog tudni eleget tenni a szabálynak a 2011. végi határidőig. Sokan hosszú távú szerződésekkel rendelkeznek külső szolgáltatók bevonására, de még ha ezt át is hidalják, a belső technológiai, szakértői és menedzsment erőforrások elégtelenek lehetnek a rendszerek átvételéhez és szakszerű, zökkenőmentes továbbüzemeltetéséhez, fejlesztéséhez.[6]

Ezt a problémát egyébként a döntéshozók is felismerték, mert június elején módosítási tervet nyújtottak be a törvényhez, amely szerint az illetékes miniszter előterjesztésére a közigazgatási informatika infrastruktúrájáért felelős miniszter egyedi felmentést adhat a törvényi korlátozás alól, abban az esetben, ha a korlátozás az informatikai rendszerek folyamatos működtetését, a feladatok és fejlesztések határidőben történő teljesítését veszélyezteti, vagy aránytalan költséggel járna.[7]

6 Futó Iván: A nemzeti adatvagyonról – ismét, 2011.03.07., In: eGov hírlevél, http://hirlevel.egc.hu/2011/03/07/a-nemzeti-adatvagyonrol-ismet/

7 Mártonffy Attila: Hígul a nemzeti adatvagyon-törvény?, 2011.06.06. http://www.itbusiness.hu/hirek/legfrissebb/higul_a_nemzetiadatvagyon-torveny.html

Az adatvédelmi biztos további kritikákat is megfogalmazott a joganyaggal kapcsolatban: a minősített adatnak nem minősülő adatok feldolgozásához használt informatikai rendszerre vonatkozó rendelkezés nincs összhangban a hatályban lévő joganyaggal, így ennek rendezése további jogszabály-módosítást kíván.

A biztos továbbá kiegészítené a törvény azon részét, mely szerint az elektronikus adatfeldolgozást végző a tevékenysége során bekövetkezett biztonsági eseményekről köteles lesz tájékoztatni az adatkezelőt. Véleménye szerint a törvénynek "a biztonsági események kivizsgálását, és a vizsgálat megállapításainak nyilvánosságra hozatalát is elő kellene írnia, hiszen a nemzeti adatvagyon sorsa, állapota, kezelése olyan közügy, amelyről indokolt a közvéleményt tájékoztatni".[8]

E-egészségügy

Bár a technológiák rendelkezésre állnának, az egészségügy még messze nem használja ki a lehetőségeit, Európában csakúgy, mint Magyarországon. A népesség öregedése, a szakemberhiány és a szűkös pénzforrások mind azt jelzik, hogy a régi módon nem működhet az egészségügy.

A technológiai feltételek adottak volnának, számos intézményben működik már az ügyvitelt segítő rendszer, orvosi rendszer, valamint a dolgozók és a betegek adatait egyaránt kezelő hr-rendszer – ám ezek között szinte semmilyen kapcsolat nincs, így az egészségügy egyetlen szereplőjének sincs teljes képe arról, mi is zajlik pontosan az intézményekben. Emellett kiemelt figyelmet kellene fordítani a biztonsági (adatvédelmi) kérdésekre, a dokumentumarchiválási képességekre és nem utolsósorban a mobilitásra. Az ágazat egészét jellemző probléma a közhiteles nyilvántartások, valamint a központi adattárak hiánya.

Az új kórházi tömbök létrehozását szolgáló Pólus projektek még csak az építési fázisnál tartanak, de rövidesen aktuálissá válnak az informatikai beszerzések is. Az egyébként mintegy 10 milliárd forint értékű projektekben 3-5% az informatika részesedése; ugyanakkor például Norvégiában egy zöldmezős kórházépítés esetében ez az arány legalább 6-8%.[9]

Európai szinten óriási feladatokat jelent az egészségüggyel kapcsolatos adminisztráció. Évente 500 millió pácienst kezelnek Európában, átlagosan évi tíz alkalommal; havonta 250 millió befizetést kell feldolgozni; és évente mintegy 5 milliárd vizsgálati eredményt, leletet kell(ene) megosztaniuk az egészségügyi intézményeknek. Mindehhez szükség lenne az informatika segítségére, de általánosságban is elmondható, hogy túl sok a párhuzamos rendszer, a többször meglévő adat és messze nem hatékony az adatcsere.

Minden biztató fejlemény ellenére sajnálatos módon még mindig számos - köztük jogi, politikai, kulturális és piaci - tényező hátráltatja az e-egészségügy további terjedését. Mindezeket tovább bonyolítja az eddig kifejlesztett rendszerek inkompatibilitása. Különösen a személyes adatkezelés terén, hiszen az egészségügyi adatok, a személyes adatok különleges, szenzitív csoportjába tartoznak, amelyeket csak különös körültekintéssel lehet menedzselni és a biztonságra is kiemelten kell figyelni. Nemrégiben például Németországban döntöttek úgy az illetékesek, hogy leállítják az intelligens egészségügyi kártyák bevezetését. Ezeken a chipkártyákon minden német állampolgár magával hordhatta volna egészségügyi adatait, orvosi előéletét, leleteit, a számára felírt gyógyszerek adatait, valamint társadalombiztosítási státuszát; az adatbiztonsági aggályok miatt azonban a rendszerbe állítást egyelőre elhalasztották. Nem véletlen, hogy az egészségügyi miniszterek 2010. decemberi találkozóján elfogadott közlemény is hangsúlyozza: a tagállamoknak fokozniuk kell erőfeszítéseiket, hogy a lakosság körében nőjön az e-egészségügyi szolgáltatások elfogadása és garantálható legyen az adatok biztonsága.

8 BITPORT: Titokban maradhatnak a nemzeti adatvagyonnal kapcsolatos incidensek, 2011.07.10. http://www.bitport.hu/trendek/titokban-maradhatnak-a-nemzeti-adatvagyonnal-kapcsolatos-incidensek

9 HIMSS Europe, Európai Bizottság: Európai eHealth Week összefoglaló, in: IT Business online, [Scopp Attila: E-egészségügy: a feltételek adottak] http://www.itbusiness.hu/hirek/legfrissebb/ehealth_hp.html

Elektronikus távoktatás

Az e-learning helyzetét a közép-kelet-európai régióban úgy jellemezhetjük, hogy ennek az országcsoportnak a modernizációs kihívás, az uniós csatlakozás és az információs társadalom építése halmozott feladatokat jelentenek.

Az európai integráció kétségkívül fontos szerepet játszott a nemzeti stratégiák és prioritások meghatározásában. Jelentős kormányzati programok indultak az elmúlt években az információs társadalom fejlesztésére. Ugyanakkor a fejlődés gátja – országonként eltérő mértékben és szegmensekben – a viszonylag alacsony személyes vásárlóerő, a magas telekommunikációs és számítógépárak, és a meglehetősen költségérzékeny e-learning-piac.

A régióban a fenti jelenségek az oktatási rendszerek általános finanszírozási gondjaival terheltek, és az alacsonyabb szintű technológiai ellátottság és internet-hozzáférés okozta hátrány is csak lassan számolódik fel. Az oktatási intézmények konzervativizmusa és forráshiánya, továbbá a kevéssé konszolidált piaci viszonyok tovább nehezítik a helyzetet. Az európai uniós csatlakozás modernizációs kihívását és az informatikai fejlesztéseket az emberi erőforrás-fejlesztés feladataival együtt kell megoldani.

A tendencia a konvergencia az e-learning-ben, a távoktatásban használt technológiai módszerek, a tartalomszórás technikái (modes of delivery) között. A blended learning – „kevert módszerű” – tanulás előretörése várható: az e-learning integrálódik a különböző képzésekbe, kiegészítve, és nem helyettesítve a hagyományos módszereket. Európai viszonylatban valószínűleg felértékelődnek és előtérbe kerülnek a jelentős állami kezdeményezések. Az e-learningre vonatkozó kereskedelmi prognózisok az elmúlt időszakban érezhetően túlbecsülték a szabad piac potenciálját és a fejlődés sebességét.[10]

Kiemelendő a PR és kommunikáció központi szerepe: fontos az (elektronikus) távoktatás, a nyitott szakképzés elfogadottságát, látható sikerét biztosítani professzionálisan megvalósított nagyléptékű fejlesztések, sikeres mintaprojektek megvalósításával és széles körű bemutatásával. A tevékenység hatékonyságát jelentősen növelheti a közvélemény széles körű tájékoztatása, a releváns információ terjesztése, a tudatosság növelése, a távoktatás társadalmi elfogadtatása céljából.

Az elektronikus távoktatás térhódításának az oktatási szektorban a továbbképzés, posztgraduális képzés lehet a legfőbb színtere. Az ilyen módon érintett hallgatók motivációja erős, szűkebb szakterületek irányába igyekeznek orientálódni, ugyanakkor az ország különféle szögleteiben élnek. Az elektronikus távoktatás kiváló médium egy potenciálisan jövedelmező hallgatóság elérésére, ráadásul oly módon, hogy az számukra is hatékony megoldásokat és kényelmet nyújt.

Az e-learning megoldásokkal kapcsolatosan az egyik fő biztonsági kérdés a hallgatók adataival és tevékenységével kapcsolatban rögzített információk adatvédelme, illetve a rendszerben tárolt tananyagokkal kapcsolatos hozzáférési lehetőségek szabályozása. A hozzáférés specifikációját a különböző e-learning szabványok írják le.

Az e-learning megoldások másik fő biztonsági kérdése magának a rendszernek a védelme, illetéktelen behatolók elöl. Mivel maga a webalapú oktatási rendszer az adott cég vagy szervezet meglévő hálózatába épül be, ezért a szokásos hálózattervezési szempontok figyelembe vétele mellett kell azt kialakítani. Itt kell használni tűzfalakat és más biztonsági megoldásokat, melyek garantálják a maximális biztonságot.

10 Szűcs András - Papp Lajos: Nemzetközi tapasztalatok, irányok az elektronikus távoktatásban, http://www.nive.hu/tudastar/06_papp_lajos.htm 2011.07.10.

Információs terrorizmus

Az információs terrorizmus definíciószerűen megfogalmazva: „a cyber-támadásokat és a hagyományos terrortámadásokat egyszerre alkalmazó olyan terrortevékenység amely az információs infrastruktúrákat felhasználva, a kritikus információs infrastruktúra elleni támadásokkal próbálja meg célját elérni".[11]

„Kritikus infrastruktúra alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot feltárásában."[11]

A kritikus információs infrastruktúrák alapvetően infokommunikációs rendszerek. Ezek sérülékenysége – a hathatós védelmi intézkedések, ajánlások és szabályzók ellenére – igen magas. Tovább nehezíti a kérdést, hogy sok esetben ezek az infokommunikációs rendszerek azok, amelyek a már említett kritikus infrastruktúrák közötti interdependenciát jelentik, azaz pont ezek azok a rendszerek, amelyeken keresztül infrastruktúráink összekapcsolódnak. Ez az összekapcsolódás lehet fizikai, de lehet logikai is, hiszen sok esetben az infokommunikációs rendszerek által összegyűjtött, feldolgozott, majd a megfelelő helyre eljuttatott adat vagy információ jelenti a kapcsolatot. Abban az esetben, amennyiben ezek az infokommunikációs rendszerek, azaz kritikus információs infrastruktúrák sérülnek – akár csak időlegesen, vagy akár csak lokálisan –, akkor az a kritikus infrastruktúrák működésére komoly negatív hatással van, azaz azok is működésképtelenné válhatnak. Ennek megfelelően kijelenthető, hogy a kritikus információs infrastruktúrák jelentik azokat a kulcspontokat, amelyek védelme érdekében mindent meg kell tenni, azaz a kritikus infrastruktúrák védelem területén kiemelt helyen kell kezelni ezeket a rendszereket.[11]

Szabályozási szempontból Európához hasonlóak a viszonyok Magyarországon. Jogszabályi értelemben tisztázott a terület – hiszen ami bűncselekmény, az az interneten is az –, de csak most kezdődik a stratégiai szintű gondolkodás, hogy miként lehetne biztonságossá tenni e nagyon különböző médiumokat. De azt is látni kell, hogy olykor nincs teljesen világos válasz arra, hol kezdődik az államérdek, a nemzetbiztonsági érdek, és hol a nyilvánosság és az információáramlás szabadsága – ennek talán éppen a Wikileaks a legjobb példája. Ma sok olyan információ érhető el nyilvánosan, ami az állam működésére, vezérlésére vonatkozóan teremthet potenciális támadási felületet.

Az internet-szociológusok szerint a jogi környezetnél elgondolkodtatóbb kérdés az, hogy vajon a bizalmas dokumentumok megjelentetése miként is veszélyeztethetné a demokráciát magát, mint azt jó néhány politikus szerte a világon, köztük hazánkban is kifejtette a Wikileaks-botrány kapcsán.

Elvileg okozhat (vélt vagy valós) biztonsági kockázatot, ha ellenérdekelt felek innen értesülnek olyan dolgokról, amelyek akció-szinten befolyásolják a viselkedésüket. A közlés elvileg és gyakorlatilag is sértheti egyesek személyiségi jogait, amennyiben rájuk vonatkozó információ nem kívánt módon válik nyilvánossá.

Megvalósulhat úgy is jogsértés, ha a dokumentumok adott körének titkosságát védő erős rendelkezések ismeretében és ellenére történik közlés. De mindez – az indokolt vagy indokolatlan hatósági fellépésekkel együtt is – nem a demokrácia ellenére, hanem annak részeként, azt mozgásban tartva, korrekciós mechanizmusainak működtetésével történik. A nyilvánosság határainak feszegetése – minden kellemetlensége ellenére – valójában kifejezetten a demokrácia érdekében történik.

11 Kovács László (ZMNE): Az információs terrorizmus eszköztára, In: Hadmérnök online http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html

Az Információs Terrorizmus fogalma Z. Karvalics László szerint[12] az információs technológia által nyújtott új lehetőségek destruktív felhasználását jelöli meg, az információs hadviselés (information warfare) részeként. Nincs olyan értelmezés, amely elfogadhatóvá tehetné azt a terminológiát, amely összemossa a fizikai destrukcióra kondicionált külső ellenséget az információszabadság és a kormány kontrolljának határterületein lavírozó belső „szellemi ill. modern médiamozgalommal". Ezek szervező ereje az elmúlt idő közel-keleti forradalmai során került előtérbe.

„Az Internet-polgárok már nehezen „vezethetőek meg" olyan, nemtelen eszközökkel, mint a „kellemetlen" és „nemkívánatos" jelenségeknek az elnevezésen keresztül történő ellehetetlenítése vagy a feleslegesen keltett morális pánik. A lavina hirtelen megfordul, és tisztára söpri a problémateret: miközben nem kétséges, hogy egy kiélezett világpolitikai erőtérben az erőszak folyamatos jelenléte miatt továbbra is nagy jelentősége van mindannak, hogy a nyílt és titkos csatornákon milyen információk milyen feltételekkel szerezhetőek vagy jeleníthetőek meg, a háttérben kirajzolódik egy még átfogóbb játszma és annak minden szereplője.

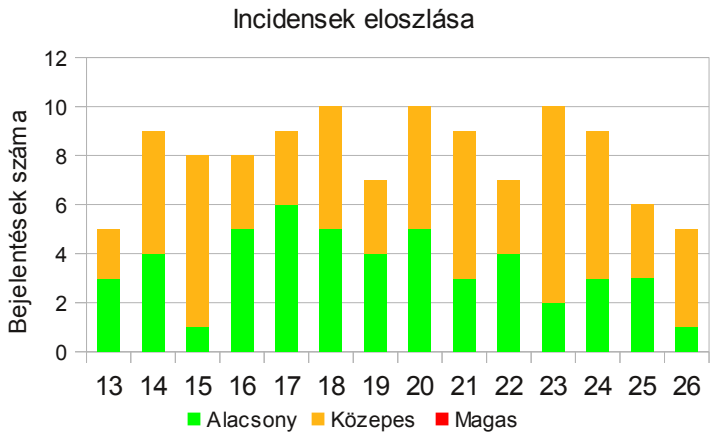
A veszély folyamatos jelenléte mellett ugyanis az információs társadalom globális színterein már jó ideje formálódik egy egészen másfajta, megismerésen és megértésen alapuló érintkezéskultúra, amely szöges ellentétben áll a képmutató, fontoskodó, titkolódzó, bizalmatlanságban fogant ipari korszakos diplomáciával. A Wikileaks-ügy valójában ennek a történetnek lesz egy fontos fejezete a jövő tankönyveiben - ha azok egyszer megírhatóak lesznek."

12 Z. Karvalics László: Az információs terrorizmus színe és visszája, 2010.12.30. http://www.pcdoktor.hu/az_informacios_terrorizmus_szine_es_visszaja

Internetbiztonsági incidensek

Internetbiztonsági incidens minden olyan biztonsági esemény, amelynek célja az információs infrastruktúrák bizalmasságának, sértetlenségének vagy rendelkezésre állásának megsértése az interneten, mint nyílt információs infrastruktúrán keresztül.

A PTA CERT-Hungary, **Nemzeti Hálózatbiztonsági Központ** a 2011. első negyedéve során összesen **112 db incidens bejelentést** regisztrált és kezelt, ebből 49 db alacsony és 63 db közepes kockázati besorolású.



A **Nemzeti Hálózatbiztonsági Központ** a hatékony incidens-kezelés érdekében **24 órás ügyeletet működtet** az év minden napján. Az ügyelet feladata az egyes incidensek kapcsán adandó válasz-intézkedések megtétele.

Hasonlóan az előző negyedévhez az incidens bejelentések túlnyomó többsége - 2011 II. negyedévében is - adathalász tevékenység és botnet hálózatok részét képező fertőzött gépek kapcsán érkezett, melyek összességében háromnegyedét teszik ki a periódusban kezelt incidenseknek leszámítva a Shadowserver Foundation-től beérkező botnet hálózatokról szóló bejelentéseket.

Nem mehetünk el szó nélkül a rendszer hozzáférési kísérletek kapcsán beérkezett bejelentések mellett sem, hiszen számos bejelentésben nem csak a rendszerekhez történő hozzáférési kísérletet jelentettek be központunkhoz, hanem azok valós kompromittálódását is, illetve az adatokhoz való illetéktelen hozzáférést is. Ezek kapcsán mindösszesen közel 200 FTP és egyéb felhasználói adat kerülhetett illetéktelen kezekbe.

A bejelentések többsége külföldi partner-szervezetektől érkeztek és több mint 85%-ban hazai káros tevékenységgel vagy káros tartalommal voltak össze-függésben. Az egyes incidensek elhárítása kapcsán összesen 184 szolgáltató került bevonásra és összesen közel 450 szálon folyt incidenskezelési koordináció.

Szürke kalapos támadás – áldás vagy átok?

Bár december még messze van, borítékolhatónak tűnik, hogy 2011 az IT-biztonsági botrányok éve lesz. Nem múlik el hét anélkül, hogy ne hallanánk komoly vállalatokat érintő biztonsági eseményekről, a hírek pedig a szaksajtó határait átlépve a széles nyilvánosságnak szóló médiában is megjelennek, egyre inkább tudatosítva a problémákat az átlagos felhasználókban is.

Nem csoda tehát, ha az egyszeri IT-biztonsági felelőst kiveri a hideg veríték, ha az általa felügyelt rendszerben rendellenességet tapasztal, nem beszélve arról az esetről, mikor egy névtelen levélben tájékoztatják egy publikus felületen tátongó hibáról - nem is olyan régen egy hazai pénzügyi tanácsadó példáján is láthattuk, hogy nem kell messzire menni egy jól irányzott zsarolásért. Azonban bármilyen hihetetlennek tűnik, a segítség néha pontosan ebben a rémisztő formában érkezik.

Itthon is gyakran előfordul, hogy a kisebb-nagyobb vállalkozásokat, állami intézményeket egy-egy jószándékú, biztonsági területen jártas felhasználójuk értesíti online rendszereik gyengeségeiről. Az érintettek egy-egy rövid e-mailben kapnak tájékoztatást a sérülékenységek jellegéről, a belőlük adódó kockázatokról és akár javításuk módjáról is, így a hibák az esetek többségében javításra is kerülhetnek.

A sebezhetőségeket feltáró szakértők – az esetek többségében inkább lelkes amatőrök - a felfedezés örömeért, a szakmai kihívás miatt keresnek biztonsági hibákat az internetre kötött rendszerekben, jutalomként a rések betömését várják. Az online szleng ezt a tevékenységet leginkább a „szürke kalapos hackelés” kifejezéssel illeti, hiszen a szerződéses keretek között zajló „fehér kalapos” megbízások törvényes kereteit elhagyva, gyakorlatilag illegálisan zajlik, mégsem célja a károkozás, az anyagi vagy üzleti haszonszerzés, mint a „fekete kalapos” esetekben.

Persze szép dolog a jó szándék, de mégis hogy jön valaki ahhoz, hogy támadást intézzen egy idegen rendszer ellen? Sokakban megfogalmazódik ez a kérdés, és a törvény betűje alá is támasztja a felháborodást. A helyzet azonban az, hogy az interneten már régóta háború zajlik, háborúban pedig nincsenek szabályok. Minden valamire való rendszergazda tudja, hogy a nap 24 órájában támadás alatt áll minden egyes online rendszer, a túlnyomó részt fekete kalapos támadók gyakorlatilag lenyomozhatatlanok, az eszközökben pedig nem válogatnak. Így nem az a kérdés, hogy fény derül-e egy biztonsági hibára, hanem az, hogy ki fedezi fel először a rést?

Ezt figyelembe véve egy szürke kalapos hacker látogatása még mindig az egyik legjobb lehetséges forgatókönyv lehet, ha a helyén tudjuk kezelni a szituációt. Ehhez mindenek előtt fel kell készülnünk a biztonsági hibajelentések fogadására, lehetőséget kell biztosítani, hogy a jelzések minél előbb eljussanak egy kompetens személyhez, aki fel tudja mérni a probléma súlyosságát, és lépéseket tud tenni a hiba elhárítása érdekében. Nagy szervezetek esetében sokszor előfordul, hogy közvetlenül csak ügyfélszolgálati, titkársági elérhetőségek állnak rendelkezésre, így az üzenetek gyakran elkeverednek, ráadásul a diszkréciót igénylő információk túl sok kézen kell, hogy keresztül fussanak. A legtöbb esetben megfelelő, ha egy webmester vagy rendszergazda közvetlen elérhetősége meg van adva az üzemeltető honlapján, nagy felhasználói táborral rendelkező vagy kiemelt biztonsági szintet igénylő szolgáltatások esetében pedig egy dedikált security@ kezdetű e-mail fiók fenntartása is ajánlott.

A beérkezett hibajelentések kiértékelése után fontos kérdéseket kell megválaszolnunk:

- Miért nem tárták fel a bejelentett hibát a hivatalos biztonsági tesztek, auditok?
- Fény derült volna-e a sebezhetőség kihasználására, ha nem érkezik bejelentés?
- Kihasználta-e más is a biztonsági rést a bejelentőn kívül?
- Előfordulhatnak-e hasonló sérülékenységek a rendszer más részeiben?

Ezek mellett kiemelten fontos egy javítási ütemterv mielőbbi meghatározása, és nem csak saját feladataink tervezhetősége miatt. Jó néhány esetben előfordult, hogy egy hibajelentés eljutott ugyan a megfelelő emberhez, erről viszont a bejelentő semmilyen visszajelzést nem kapott, így joggal feltételezhette, hogy üzenete elveszett vagy figyelmen kívül hagyták a problémát. Az ilyen esetek előbb-utóbb a sebezhetőség részleteinek publikálásához („full disclosure") vezetnek, ami nem tekinthető ugyan felelős eljárásnak, eredményeként viszont rekord sebességgel javítják a hibákat... Mivel a szivárogtató kilétének megállapítása legtöbbször reménytelen vállalkozás, a javítatlan sebezhetőség hírét pedig már sehogy sem lehet visszavonni, legjobb ha megelőzzük ezeket a helyzeteket. Ehhez legtöbbször elegendő, ha egyszerűen megosztjuk a javítási ütemterv részleteit a bejelentővel, elismerve munkáját, és biztosítva, hogy a probléma belátható időn belül megoldásra kerül.

Azt, hogy mindez nem egy naiv, utópisztikus elképzelés jól mutatja, hogy több nagy vállalat nem csak hogy üdvözli a szürke kalapos bejelentéseket, hanem külön dicsőségfalakat tart fent, vagy egyenesen pénzdíjjal ösztönzi a hibakeresést. A „hibavadász" programok eredményeként ma már több százmillió felhasználó használhatja biztonságosabban többek között a Google[13], a Mozilla[14], a Twitter[15] és a Facebook[16] szolgáltatásait is. Ezek a cégek persze amellett, hogy szeretnek a kedves, elnéző nagybácsi szerepében tetszelegni, pontosan tisztában vannak azzal is, hogy egy komplex rendszer folyamatos biztonsági tesztelése bizony nem olcsó mulatság, az internet szürke kalapos közösségének bevonásával viszont olyan lefedettségre tehetnek szert e téren, melyet másként lehetetlen lenne elérni.

Ezek pedig olyan szempontok, melyek nem csak a nagy, nemzetközi vállalatok számára lehetnek vonzóak. Szerencsére egyre több magyar szolgáltató is felismeri, hogy a felhasználói visszajelzésre nem csak a funkcionalitás vagy a használhatóság, de a biztonság területén is szükség van. Az online fenyegetések erősödése itthon is jól érezhető, kitettségünk egyre nő. Ebben a helyzetben luxus lenne megengednünk magunknak, hogy a szövetségesek között válogassunk.

Írta:

Buherátor
Kifehérített kalapos blogger
buhera.blog.hu

13 http://googleonlinesecurity.blogspot.com/2010/11/rewarding-web-application-security.html
14 http://www.mozilla.org/security/bug-bounty.html
15 https://twitter.com/about/security
16 http://www.facebook.com/security?sk=app_6009294086

Játék határok nélkül, határtalan szabadság?

Az Interneten, mint országhatárokat nem tisztelő, határok nélküli világban rendszeresen felmerül a kérdés, mégis ki, mit tehet meg, adott ügyek kapcsán melyik ország az illetékes? A Interneten megvalósuló jogsértések, legyen az hálózatbiztonsági incidens vagy jogsértő tartalom, az esetek 90-95%-ban akár több külföldi elemet is érinthetnek, így az ilyen esetekben felmerülő illetékesség[17] és hatáskör[18] kérdése különösen fontos.

Az illetékes szerv és ország meghatározásához első körben azt kell meghatároznunk, milyen cél eléréséhez keressük az illetékességgel rendelkező hatóságot.

Mik lehetnek ezek a lehetséges célok?

- A tettesek megtalálása,
- Jogsértés végleges megszüntetése
- vagy a támadás, jogsértés átmeneti megszakítása?

A különböző célkitűzésekhez különböző eljárási technikák kapcsolhatóak, értelemszerűen különböző hatékonysággal.

A tettesek megtalálása és felelősségre vonása alapvetően a büntető hatalommal és a legitim erőszak monopóliumával rendelkezőnek a kötelessége, azaz ideális esetben a jogsértés helye szerinti főhatóságnak, állami szervnek.

Joghatóság

A joghatóság az állam azon joga, hogy jogalkotással, végrehajtási cselekményekkel és bírói aktusokon keresztül egyoldalúan létrehozzon, megváltoztasson, megszüntessen jogokat és kötelezettségeket.

A joghatóság és eljárás külföldön

A joghatóságot **nemzeti hatáskör**nek (államok közötti hatáskör-megosztás) is nevezik. A joghatóság meghatározását tekintve ki kell emelnünk az alábbi fő elveket: a Területi elvet, az Állampolgársági elvet, a Védelmi elvet, és az Univerzalitás elvét.

Ezekről röviden:

Területi elv:	**Védelmi elvet**
Az állam saját területén gyakorolt joghatósága, belföldi és külföldi állampolgárok által az állam területén elkövetett cselekmények kapcsán.	Idegenek által külföldön az állam biztonságát érintő bűncselekmények felett gyakorolt joghatóság, ha az elkövetés helye szerint nem bűncselekmény.
Állampolgársági elv:	**Univerzalitás elvét**
Az adott állam hatalma polgárai felett külföldön és belföldön. Joghatóság az állampolgár külföldön elkövetett bűncselekményeivel kapcsolatban is.	Egyes bűncselekmények esetén bármely államnak joghatósága van, pl. kalózkodás.

17 Illetékesség: általában jelenti a hatóságok tevékenységének törvényileg meghatározott körét, amelyen a hatóságnak az egyes esetekben való eljárási jogosultsága is alapszik. Azt határozza meg, hogy az azonos hatáskörrel rendelkező szervek közül, melyiknek van az ügyben eljárási jogosultsága. Horizontális munkamegosztás.

18 Hatáskör: az állami szervek közötti tevékenységi kör szerinti munkamegosztást jelent. Vertikális munkamegosztás.

A joghatóság gyakorlása akkor válhat kérdésessé, ha az érintett elkövetési cselekménysor a szuverén állam területén kívüli elemet is tartalmaz.

A joghatóság főszabály szerint az államterülethez kötődik, így büntetőügyekben mind a magyar és nemzetközi büntetőjog a joghatóságot és az illetékességet az elkövetés helyéhez, azaz a jogsértés[19] megvalósulásának helyéhez köti. Az elkövetés helye egy jogsértő tartalommal bíró weboldal esetén a hosting[20] helye, azaz az oldalt tartalmazó szerver fellelhetőségi helye. Hálózatbiztonsági incidens esetén pedig a megtámadott szerver földrajzi helye.

Ugyanakkor a magyar büntetőjog kiterjeszti a magyar joghatóságot abban az esetben, ha az elkövetés valamelyik stúdiuma magyar joghatóság területén valósul meg. Egy példán szemléltetve: ha külföldön host-olnak egy Magyarországon elérhető, magyar nyelvű rasszista, idegengyűlöletre uszító oldalt amely egy Magyarországon élő kisebbség ellen irányul, és bár a hosting helye külföldön van, de ha a DNS[21] szerver Magyarországon található, akkor a magyar jog szerint fennáll a magyar joghatóság is, mivel DNS szerver működése nélkül az oldal csak korlátozottan lenne hozzáférhető, így kijelenthető, hogy a DNS szerver működése nélkül nem valósulhatna meg a jogsértés, ezért annak működése teszi lehetővé a jogsértés megvalósulását, és így magyarázható a DNS szolgáltató tettes társsá válása.

Felelősségi kérdés

Mennyiben tehetőek felelőssé azok a szolgáltatók, akik tudtukon kívül, mint szolgáltatást nyújtó felek közreműködnek egy ilyen Interneten keresztül megvalósuló támadásban, jogsértésben?

Az 2001.évi CVIII-as, Elektronikus kereskedelemről szóló törvény (továbbiakban: „Ekr tv.”) alapvetően kimondja az információs társadalommal kapcsolatban szolgáltatást nyújtok felelősségét. Azonban a törvény külön kategóriaként említi a közvetítő szolgáltatókat:

l) Közvetítő szolgáltató: az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely

la) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);

lb) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);

lc) az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);

ld) információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás);

A közvetítő szolgáltatók az Ekr.tv. 7.§ (2) bekezdése alapján alapvetően nem felelősek a rajtuk keresztül nyújtott szolgáltatásokért, bizonyos feltételek megléte teljesülése esetén. Ilyen feltételként határozza meg a törvény, hogy a közvetítő szolgáltató mindaddig nem tehető felelőssé, míg a jogsértésről nincs tudomása, arról nem értesül.

19 Jogsértés: ide tartozik valamennyi olyan magatartás és cselekmény, melynek tanúsítása vagy elkövetése a hatályos magyar jogszabályokba ütközik.

20 Hosting: webtárhely szolgáltatás, Minden felhasználó egy, a rendszer által dedikált tárhelyet foglal el, aminek nyilvános tartalma egyedi domain néven érhető el

21 DNS szerver: másnéven névszerver, fő feladata a webcímek „lefordítása", „feloldása" a hozzájuk tartozó IP-címre.

Milyen esetben, és kik tehetőek felelőssé?

Hálózatbiztonsági incidens[22]

Hálózatbiztonsági incidens esetén természetesen a támadót terheli a büntetőjogi és polgári jogi felelősség. Azonban, a támadás megszakításához, megzavarásához szükséges a közvetítő szolgáltatók, Internet szolgáltatók felelősségének bizonyos fokú megállapítása, különösen akkor, ha a támadó nem egyértelműen beazonosítható. Adott esetben egy DDOS[23] támadás kapcsán sok olyan felhasználó Internet kapcsolatának felfüggesztésére lehet szükség (botnet hálózat, zombi gép hálózatok esetén), akiknek nincs tudomásuk a támadásról. A közvetítő szolgáltatók, Internet szolgáltatók független szervezetek, ezért utasítani őket nem lehet, így mindenféle szolgáltatás korlátozásra való kötelezésükhöz jogi kötelezettségük megállapítása szükséges, vagy annak bizonyítása, hogy saját felelősségük kizárása érdekében korlátozzák a kérdéses végpontoknak nyújtott szolgáltatást. Egy támadás elhárítása érdekében ezen közvetítő pontok felelősségének megállapítása azért rendkívül fontos, hogy az egyes végpontok lekapcsolásának jogi alapot teremtsen.

Jogsértő tartalom

Itt a helyzet jogi szempontból némileg komplikáltabb, mint egy hálózatbiztonsági incidens kapcsán.

Kezdjük egy példával:

Egy domain nevet beregisztrálnak Németországban egy anonimitást biztosító domain regisztrátor cégen keresztül. A regisztrátor cég, hogy az anonimitást biztosítsa, semmilyen adatot nem kér, technikai és adminisztrációs kontaktként is magát tünteti fel. A domain valódi jogosultja Magyarországon béreli a tárhelyet, ahonnan a jogsértő tartalom elérhető, és az Egyesült Államokban bérel egy DNS szervert, ami összeköti a Németországban regisztrált domain-t a Magyarországban host-olt tartalommal, továbbá maga az oldal .com-os végződéssel kerül regisztrációra, így nem a magyar Internet Szolgáltatók Tanácsa osztotta azt ki, hanem egy nemzetközi szervezet, az ICANN.

A fent vázolt eset még az egyszerűbb esetek egyike, mivel a működtetés egyes állomásai jól behatárolhatóak, és bár az illetékesség meghatározása nem egyszerű, de még mindig egyszerűbb, mintha 5-6 szerveren keresztül futtatnák végig az oldalt a nyomok eltüntetése céljából.

A helyzetet az teszi igazán érdekessé, hogy a „weben” megvalósuló jogsértések esetén bár az elkövető általában igyekszik névtelenségbe burkolózni, a jogsértés megvalósulása „publikus”, mindenki által látható, megtalálható, és valójában ettől válik jogsértővé a cselekmény, hogy „publikusan” valósul meg.

A domain nevek nyilvánosan elérhetőek, azok kiosztásáért nemzetközi szervezetek ill. alacsonyabb szintű, de állami vagy civil szervezetek a felelősek. Ennek okán, a weboldalakon keresztül megvalósuló jogsértések esetén, mivel a jogsértés olyan végponton valósul meg ami az Internet működése okán megkövetel bizonyos szintű központi irányítást, ha más megoldás nem célravezető, legvégső esetben a domain nevek delegálói megtehetik a domain nevek felfüggesztését, vagy adott esetben visszavonását.

Magyarországon a domain nevek kiosztásáért az Internet Szolgáltatók Tanácsa a felelős (továbbiakban: „ISZT”), ők tartják karban és üzemeltetik a domain.hu-n keresztül elérhető, .hu-s

22 Hálózatbiztonsági incidens: Minden olyan esemény, ami a hálózatok és azokon működő eszközök bizalmasságát, sértetlenségét vagy rendelkezésre állását veszélyezteti, azaz minden támadás incidensnek minősül

23 Egy informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése (Denial of Service, rövidítve: DoS), történhet megosztva is, több forrásból – ekkor a támadás szokásos rövidítése a DDoS (Distributed Denial of Service).

végződésű magyarországi domain nevek adatbázisát. Nemzetközi szinten az ICANN (Internet Corporation for Assigned Names and Numbers) adja ki a legfontosabb domain nevek (gTLD, ccTLD) bejegyzéssel kapcsolatos szabályokat, és teszi lehetővé az egyes jogviták elbírálásához az általa működtetett Vitarendezési Fórumot, illetve szabályzata lehetővé teszi Választottbírósági eljárást.

Az ICANN által kezelt domainek közé tartoznak a következők: az összes .aero, .arpa, .asia, .biz, .cat, .com, .coop, .edu, .info, .int, .jobs, .mobi, .museum, .name, .net, .org, .pro, and .travel végződést igénylő weboldal, valamint a nemzeti weboldalak.

Mivel ezek a szervezetek (ICANN nemzetközi szinten, illetve az egyes nagyobb domain tartományokat kezelő szervezetek, mint pl. Afilias, ISZT) felelősek az egyes oldalak bejegyzéséért és a domain regisztrációs adatbázisban való szereplésükért, így ők adott esetben megtehetik a domain nevek felfüggesztését, vagy visszavonását, az ICANN szabályzatában és saját szabályzataikban foglaltak szerint. Félreértés ne essék, ettől még a sértő tartalom nem semmisül meg, csupán a megszokott módon elérhetetlenné válik, mivel az egyes DNS szerverek feladata, hogy a hosting szerveren megtalálható tartalom IP címét a hozzárendelt domain névvel párosítsa. Ezáltal válik elérhetővé a hosting szerveren tárolt tartalom, továbbá ennek a párosításnak a megszüntetésével érhető el a domain név felfüggesztése/visszavonása, melyet követően a böngészőben a domain név beírásával a tartalom már nem lesz elérhető. Ellenben ha az oldal IP címe alapján keresünk, bizonyos esetekben továbbra is megtalálhatjuk majd a keresett oldalt.

A domain név felfüggesztésén kívül további lehetőség még jogsértésben való segítségnyújtásért és így társettesi alakzat megvalósításáért a közvetítő szolgáltatók, illetve minden, információs társadalommal kapcsolatosan szolgáltatást nyújtók felelősségre vonása.

Felelősségük alapját megteremti a Büntető törvénykönyvről szóló 1978.évi IV-es törvény:

> *„20.§ (3) Társettesek azok, akik a szándékos bűncselekmény törvényi tényállását, egymás tevékenységéről tudva, közösen valósítják meg.”*

Természetesen mind a DNS szerverszolgáltatók, mind a hosting cégek feltüntetik a Használati Feltételeik között, hogy nem vállalnak felelősséget a szolgáltatásaik révén elérhető tartalomért és a hatályos magyar jogszabályok sem teszik a kötelezettségükké a tartalmak szűrését. Az Ekr.tv. azonban kimondja, hogy miután értesültek a rendszerükön keresztül megvalósuló jogsértésről, legyen az hálózatbiztonsági incidens vagy egy jogsértő oldal, már nem tehetik meg, hogy ne foglaljanak állást.

Mivel az értesítést követően már tud a közvetítő szolgáltató (tárhely szolgáltató, DNS szervert biztosító cég) a rajtuk keresztül megvalósuló jogsértésről, ha ezt követően is folytatódik a jogsértés, akkor ők abban már társettesként felelősségre vonhatóak, mivel az értesülést követően már szándékosan és a másik tevékenységéről tudva valósítják meg a cselekményt, ha az ellen nem tesznek semmit.

A külföldön működő közvetítő szolgáltatók felelősségre vonását teszi lehetővé az Ekr.tv. alábbi rendelkezése:

> *„1.§ a) a Magyar Köztársaság területéről nyújtott, valamint a Magyar Köztársaság területére irányuló információs társadalommal összefüggő szolgáltatásra;”*

A törvény ezen rendelkezése kiterjeszti a magyar joghatóságot mindazon külföldi szolgáltatókra is, akik tevékenysége révén Magyarországon is elérhető információs szolgáltatásért külföldről is felelősségük van. A törvény jelentősége abban áll, hogy ha amennyiben egy magyar bíróság kimondja egy pl. német tárhely szolgáltató felelősségét egy jogsértésben való közreműködését, az országok között meglévő kétoldalú egyezmények révén a német bíróság elfogadhatja a magyar bíróság ítéletének érvényességét és a német jog szerint kötelezheti az elmarasztalt felet az abban foglaltak végrehajtására.

Az Internet jellegéből adódóan az egyes folyamatok rengeteg apró részállomásra bonthatóak, ami lehetővé teszi az egyes elkövetők sikeres bujkálását. Ennek hatására és az Internet szabályozására tett kísérletek kudarcainak eredményeképpen megváltozni látszanak a klasszikus értelemben vett társadalomvédelmi eszközök. Első helyre került az online megvalósuló jogsértések minél hatékonyabb és gyorsabb megszüntetése, a támadások elhárítása, továbbá a társadalom felkészítése az Internet világában való biztonságos életvitelre, a biztonságos internetezésre.

Rootkit érzékelés kernel kód tunellezéssel

Tizenöt évvel ezelőtt az átlagos malware író olyan serdülő fiú volt, aki szerette volna felkelteni a társai figyelmét. Az elmúlt években viszont drámaian változtak meg a dolgok. A kiberbűnözőket most már nem a hírnév, a hecc, vagy a visszavágás vezérli: üzleti profitot keresnek és távol akarnak maradni a nyilvánosságtól. A pénzügyi profit eléréséhez olyan „kreációkra" van szükségük, amelyek a lehető leghosszabb ideig képesek elrejtőzni.

Ahogyan a név is sugallja, a célzott támadás egy olyan támadás, melynek célpontjai bizonyos személyek vagy szervezetek. A különlegesen kialakított kártékony szoftvereket mindössze egy maroknyi számítógép felé terjesztik, így a biztonsági vállalkozások radarjai rendkívül nehezen érzékelhetik ezeket. Különösképpen a kártékony szoftverek jelenlegi áradatakor (2010-ben több mint 12 millió malware törzs jelent meg, ami átlagosan napi 55 000 új veszélyt jelentett[24]) – teljesen olyan, mint tűt keresni a szénakazalban. Míg az offline polimorfizmust (szerver-oldali) jóval nehezebb érzékelni, mint a klasszikus változatát és az anti-anti-virus érzékelés is határozottan komplikált, mégis a lopakodás (és a rejtőzködés) végső megoldása a rootkit.

A rootkitek szofisztikált eszközök, melyek lehetővé teszik, hogy a kártékony szoftverek rejtve maradjanak. 2008-ban a legnagyobb spam botnetek több mint a fele használt kernel rootkiteket és ez a szám folyamatosan nőtt 2009-ben és 2010-ben[25] is. Valamint egyre érettebb módszerek láttak napvilágot, melyek megnehezítették az érzékelést és az eltávolítást.

Klasszikus érzékelési módszerek

A rootkitek a rejtőzködésüket általában az operációs rendszer funkcióinak felforgatásával, tipikusan a kulcsfontosságú adatstruktúrák és/vagy az operációs rendszer kódjának módosításával érik el. Így nyilvánvaló, hogy a nyomozás első lépése ezen területek óvatos vizsgálata. Kernel módban a rootkitek megváltoztathatják az olyan adatstruktúrákat, mint az IDT (Interrupt Descriptor Table), vagy az SSDT (System Service Descriptor Table). A processzor modell specifikus regiszter SYSENTER_EIP_MSR tartalmazza a 0 szinten futó kód címét, amely a kiszolgáló rendszerhívásokért felel. Általában az összes vektor az IDT/SSDT-ben és a SYSENTER_EIP_MSR-ben olyan címekre mutat, melyek az NTOSKRNL-ben azaz a Windows Kernelben találhatók. Így a triviálisan módosított adatstruktúrák egyszerű ellenőrzéssel érzékelhetők.

Az adatstruktúrák módosítása helyett a rootkitek megváltoztathatják magát a kernel kódot is. Ennek egyik jellemző módszere a végrehajtás eltérítése a malware kódján keresztül. Mivel az eltérítés

24 BitDefender report, 2010, www.bitdefender.com
25 „The top 10 spam botnets: New and improved", www.techrepublic.com, elérhető volt 2010. február hónapban

általában egyszerű elágazó utasítással történik a kártékony kezelő felé (a technika „inline patching” néven is ismert), az általános detektáló rutinok alapvető teszteket is végrehajtanak, úgy mint az elágazó instrukciók célja kívül esik-e az analizált modulon.

Mindamellett a rootkit technológia fejlődése nagyban nehezíti a detektálást: mind a Rustock.C (1. ábra) és a TDL3 (2. ábra) rootkitek a kontrollt olyan ugródeszkákon adják át, melyek a „legális” területeken helyezkednek el. Talán megállapítható az ugródeszkák valódi célja statikus analizátorral, de ha figyelembe vesszük azt, hogy ezek verzióról-verzióra változnak – nem beszélve a polimorf ugródeszkákról – a legjobb eredményt dinamikus eszközökkel érhetjük el. Megfontolandó továbbá az is, hogy az inline patch-ek már nem korlátozódnak a funkciók első bájtjaira, bárhol megtalálhatók a végrehajtási folyamatban.

```
push cs
nop
sub esp, 4
mov dword ptr [esp], _address
retf
```

1. ábra Rootkit.Rustock.C ugródeszka

```
mov eax, dword ptr [FFDF0308]
jmp dword ptr [eax+FC]
```

2. ábra Rootkit.TDL3 ugródeszka

A Cross-view széles körben elterjedt rootkit detektálási technika, mely során az operációs rendszer forrásainak „magas szintű” látványát hasonlítjuk össze az „alacsony szintű” képpel. Mivel a rootkiteket az operációs rendszer forrásainak elrejtésére használják, a detektáló eszközök összehasonlítják a magas szintű funkciók, mint például a **FindNextFileA** eredményeit az alacsony szintű funkciók kimenetelével, mint az **NTQueryFirectoryFile**, eseteg a nyers fájlrendszerrel illetve disc-elemzővel. Processzek esetén használható a magas szintű **CreateToolhelp32Snapshot** funkció, illetve alacsony szintűként az **NtQuerySystemInformation**, vagy az EPROCESS kernel struktúra elemzőjének eredménye, egy visszatérő, kétszeresen kötött lista, melyre hivatkozni lehet a **PsActiveProcessHead** kernelváltozó segítségével, vagy az exportált **PsGetCurrentProcess** függvénnyel. Egy alacsony szintű nézetet kaphatunk a PspCidTable adatstruktúrájának elemzésével, esetleg más módszerekkel, mint például a processz azonosítók brute force-olásával.

A Cross-view módszerrel járó mélyebb betekintésre való törekvés egy fajta Achilles-sarok, mivel a rootkitek mindig találnak mélyebb és mélyebb helyeket, ahol elrejtőzködhetnek. Például a TDL3 az alacsony szintű disc miniport driver-t fertőzi meg, nagyban megnehezítve a disc „valós” tartalmának megtekintését. Továbbá ugyanennek a TDL3-nak nincs szüksége saját processzre, mivel ring-3 kódot fecskendez be az svchost.exe-be és az összes saját állományát egy saját fájlrendszeren belül tárolja.

Egy rootkit érzékelő eszköz ellenőrizheti még a betöltött kód integritását (például ellenőrizheti, hogy a betöltött kód egyezik-e a diszken lévővel, az információ relokációjának alkalmazását követően). De ahogyan azt a későbbiekben láthatjuk, lehetséges a normál kódfolyam módosítása az eredeti kód egyetlen bitjének módosítása nélkül is.

Dinamikus bináris hangolás

A dinamikus bináris hangolás széles körben használatos a termékek teljesítményének értékelésekor, hibáik diagnózisában vagy egyszerűen a program viselkedésének analizálásakor. Biztonsági szempontból az ABI[26] érvényesítés kontextusában használatos egy olyan technika, mely „program shepherding”[27] néven vált ismertté. Technikai megközelítésből a dinamikus bináris hangoló keretrendszer a következő összetevőkből áll:

26 Application Binary Interface (ABI)

27 „Secure Execution via Program Shepherding”, Vladimir Kiriansky, Derek Bruening, Saman Amarasinghe, USENIX Security Symposium, 2002. augusztus

1) Kód generáló motor, amely az eredeti kódhoz „hangoló” kódot fűz hozzá. Bár a legtöbb esetben az instrukciók 1:1 arányban kerülnek másolásra, léteznek számos megemlítendő kivételek :
    a) A valószínűsíthetően támadó kódok kicserélésre kerülnek, vagy különleges hangoló kód előzi meg őket
    b) Az elágazó instrukciók kicserélődnek speciális rutinokra, melyek lehetővé teszik hogy a vezérlés visszakerüljön a hangoló motorhoz. A 3. ábra egy blokkot mutat, mely 4017F7 lineáris címnél kezdődik és a 4017FF elágazó instrukcióval végződik (így a blokk maga 401805-nél végződik) Az elágazó kondíció teljesülésekor a processzor a megfelelő címre ugrik *(a további ábrákon ez „branch taken” címkével lesz megjelölve)*, ami 401FE5; egyébként a 401805-ös címre *(az ábrákon „fall through” címkével jelölve)*. A 4. ábra a fordított alap blokkot szemlélteti; Mindenekelőtt azt láthatjuk, hogy az elágazó utasításon kívül az instrukciók egy az egyben másolásra kerültek. Azt is láthatjuk, hogy a címek könnyen kiszámíthatók fordításidőben, így már csak arra van szükség, hogy a vezérlés visszakerüljön a hangoló motorhoz, meghatározva a frissített Instrukció Pointert. Különösen fontos, hogy semmiképpen se módosítsuk a végrehajtást menetét. A „JUMP_TO_VM” makró semmilyen módon sem szennyezheti a vermet, nem módosíthatja a CPU regisztereket vagy a memória területet az adatstruktúrán kívül. Így a motor egy „shadow stack”-nek nevezett, szálankénti adatstruktúrát tart fent, mely bebillenti azokat a regisztereket, amelyeket a kód generáló motor módosíthat. Egy példa alap blokk az 5. ábrán látható.
2) Az alapblokk menedzser felelős a már lefordított alapblokkok listájának megőrzésért (alap blokk gyorsítótár), gyors visszakeresés céljából. A cache képes jelentősen növeli a végrehajtás sebességét.
3) Feltétlenül szükséges egy önmódosító kód menedzser, mivel offenzív kódokkal is számolni kell. Az önmódosító kódok kezelésének hiánya katasztrofális helyzeteket okozhat: amennyiben egy program módosítja az alapblokkot, mely már módosításra került (így már az alap blokk gyorsítótárban szerepel), könnyen előfordulhat, hogy a régi, tárolt kód kerül végrehajtásra a módosított helyett. Felhasználói módban a motor kezeli az önmódosító kódokat mégpedig úgy, hogy meggyőződik arról, hogy az alapblokkok írásvédett memória területen helyezkednek el – ha nem, akkor a memória attribútumait magunk változtatjuk meg – és elemezzük a lehetséges „Access Violation”, azaz „hozzáférés megsértése” kivételeket. Amennyiben egy írásművelet valóban módosítaná a fordított alapblokk valamelyikét, kitörüljük a gyorsítótárból és időlegesen eltávolítjuk az írásvédelmet, lehetővé téve az írásműveletet. Különösen érdekes eset az, amikor egy instrukció a saját alapblokkját módosítja – ebben az esetben újrafordítjuk az alapblokkot és megfelelően visszaállítjuk a végrehajtást.
4) A keretrendszer meglehetősen fontos részét képzi az asszinkron feladatkezelő. Jól ismert régi anti-debugging trükk a vezérlés átadására a kivétel generálás. A motor a **KiUserExceptionDispatcher** funkció hurkolásával és a paramétereinek nyomozásával kezeli ezeket a szituációkat. Az első paraméter egy **EXCEPTION_RECORD** struktúra, amely értékes információkat tartalmaz, úgy mint a kivétel kódja és a kivétel címe. Ha egy kivétel keletkezik a fordított kódon belül, akkor az ExceptionAddress tag megfelelő módosítására van szükség (így szükség van a valós és a fordított kódok közötti kapcsolatok feltérképezésére). A második paraméter a **CONTEXT** struktúra, mely a kivétellel kapcsolatos CPU regisztereket tartalmazza. Ugyanúgy mint a kivétel cím, az **Eip** tag is módosítást igényel.

```
.4017F7 43                  inc ebx
.4017F8 83 7D CC 00         cmp byte ptr [ebp-34], 00
.4017FC 89 5D B8            mov dword ptr [ebp-48], ebx
.4017FF 0F 8C E0 07 00 00   jl 401FE5
.401805
```

3. ábra Normál alap blokk (normal basic block)

```
.4017F7 43                  inc ebx
.4017F8 83 7D CC 00         cmp byte ptr [ebp-34], 00
.4017FC 89 5D B8            mov dword ptr [ebp-48], ebx
.4017FF 0F 8C E0 07 00 00   jl 401FE5
.401805
```

4. ábra Fordított alap blokk (translated basic block)

A továbbiakban szükség lesz még az asszinkron eljárás hívások (APC) és a felhasználói módú visszahívások kezelésére (amit a win32k.sys küld).

```
.3370000 43                 inc ebx
.3370001 83 7D CC 00        cmp byte ptr [ebp-34], 00
.3370005 89 5D B8           mov dword ptr [ebp-48], ebx
.3370008 0F 8C ?? ?? ?? ??  jl __branch_taken
__fall_through:
```

```
        xchg esp, dword ptr [__shadow_stack]
        pushf
        pushad
        JUMP_TO_VM (401805)
        popad
        popfd
        xchg esp, dword ptr [__shadow_stack]
        jmp dword ptr [__shadow_eip]
__branch_taken:
        […]
```

5. ábra Fordított alap blokk (verem szennyezés és regiszter módosítás nélkül)

A motor tesztelésekor a sebesség optimalizálásának lehetőségei is felmérésre kerültek:

1. A legtöbb esetben, lehetséges volt a fordított alap blokkok közvetlen kötése; ez akkor eshet meg, amikor a blokk leszármazottjának (successor) kiszámítása fordítási időben megtörténhet (6. ábra). Kezdetben a „cache_fall_trough” és a „cach_branch_taken” változók egy olyan szubrutinra mutatnak, ami megtalálja az utódokat. Az alap blokk későbbi végrehajtásai során a gyorstárazott címek használatosak.
2. Az olyan alap blokkok esetén, amikor az utódok statikus kiszámítása nem lehetséges (7. ára), az utolsó 4 utód összemérése történik. Megjegyezzük, hogy a lea/jecxz páros nem módosítja a CPU flag-eket, így nincs szükség a költséges pushfd/popfd párosra.

```
.3370000 43                inc ebx
.3370001 83 7D CC 00       cmp byte ptr [ebp-34], 00
.3370005 89 5D B8          mov dword ptr [ebp-48], ebx
.3370008 0F 8C ?? ?? ?? ??  jl __branch_taken
__fall_through:
         jmp dword ptr [_BB.cache_fall_through]
__branch_taken:
         jmp dword ptr [_BB.cache_branch_taken]
```

6. ábra Fordított alap blokk (utódok közvetlen kötésével)

```
.405B17 FF 24 95 20 5B 40 00  jmp dword ptr [405B20+edx*4]
```

7. ábra Indirekt vezérlést átadó instrukció

```
SPILL_EAX
SPILL_ECX
mov eax, dword ptr [405B20+edx*4]
lea ecx, dword ptr [eax - _real_address_1]
jecxz _1
[…]
// no match, so JUMP_TO_VM (eax)
_1:
RESTORE_EAX
RESTORE_ECX
jmp _translated_address_1
[…]
```

8. ábra Indirekt vezérlés-átadás kezelése

Normális esetben nincs szükség minden alap blokkhoz hangoló kód hozzáadására. A rootkit érzékelés szempontjából mindössze a végrehajtott kódok listájának vezetése szükséges, a valószínűsíthetően offenzív instrukciók listájára, melynek felfedezése a fordítás alatt megtörtént. Továbbá egyéb flag-ekre, mint például „szemét” (garbage) vagy ne-csinálj-semmit instrukciókra. A legtöbb művelet csak egyszer végezhető el, fordítási időben. Mindezek segítségével a hangoló motor olyan sebesség elérésére képes, ami már összemérhető a natív végrehajtással (az átlagos sebesség csökkenés mindössze 25%).

Dinamikus bináris hangolás kernel módban

A bináris hangoló motor kernel módba történő portolása fárasztó feladatnak bizonyult. Mindenekelőtt szükség volt arra, hogy a kódok analizálása ne csak PASSIVE_LEVEL, de APC vagy DPC szinteken is megtörténhessen. A cél az volt, hogy a kód generálás minden egyes aspektusa irányítható legyen, így:

a) Egy saját memóriamenedzser kifejlesztésére volt szükség. A motor memória igénye és az elérési minták igazán egyszerűek voltak: szükség volt az alap blokk struktúráinak, az alap blokk gyorstárának és a hangoló információk tárolására. Mivel a legtöbb struktúrának elérhetőnek kell lennie bármely IRQL-en futó kód számára, a memória allokáció a nem lapozott pool-ból és partíciókból inicializáció közben történik meg.

b) A hangoló motorból eltávolításra kerültek a konkurens elérési kontrollok. Felhasználói módban tetszőleges számú konkurens szál elemzésére lehet képes a motor. A helyzet kernel módban sokkal bonyolultabb, mivel elméletileg előfordulhat az, hogy a szálaknak várniuk kell a megosztott források elérésére (például az alap blokk gyorstárra). Több szál kezelése, a motor több példányával válhat lehetségessé.

c) Elméletileg a kivételek észlelése (és módosítása) megoldható az IDT különböző vektorainak hurkolásával. A motor jelenlegi implementációja nem monitorozza a kivételeket. Egy rootkit részéről lehetséges, hogy hardveres „read breakpoint”-okat alkalmazzon a saját kódjában és így érzékelje, hogy a kódjának olvasása történik. Jelenleg számos taktika megfontolása történik abból a célból, hogy az ilyen jellegű viselkedés megkerülhető legyen.

d) Az önmódosító kódok érzékelése különösen összetett kernel-módban; elméletileg használható a felhasználói módban alkalmazott megközelítés, de gyakorlatilag majdnem hogy lehetetlen az összes variáció érzékelése. A jelenlegi kernel-mód implementáció nem használja a közvetlen alap blokk kötési optimalizálást, így minden transzfer áthalad a motoron, ami felelős a checksum[28]-okkal történő módosítás-ellenőrzéséért. Amennyiben egy alap blokk saját magát módosítja (feltételezve, hogy a blokk elég nagy és a módosítás az elért soron kívül esik) a motor a régi, nem módosított kódot hajtja végre. Az ilyen jellegű viselkedés elkerülése céljából számos stratégia vehető számba.

Analízis – az MBR olvasása

Az adott tároló eszközök menedzselésében résztvevő vezérlők kollektív neve a storage stack[29]. Ha egy alkalmazás egy operációt próbál elvégezni egy tároló eszközön, a kérést először az I/O menedzser kapja meg; az I/O menedzser pedig elküldi a kérést a fájlrendszernek; a fájlrendszer lefordítja a fájl címeket kötet címekre és továbbítja a kérést a kötet menedzsernek (volume manager).

A Windows alapköteteket (egy egyszerű partíción) és dinamikus köteteket (több partíción is elhelyezkedhetnek) is támogat. Így a kötet menedzser a kezdeti I/O kérést a partíciómenedzser felé továbbítja.

Az alsó szintű vezérlők a „Class driver”-ek – melyek adott típusú eszközöket vezérelnek, mint például diszkeket vagy szalagokat, a „port driver”-ek, amelyek különleges átvitelért felelősek (Strorport SCSI-hoz vagy RAID-hez, Atapi IDE alapú eszközökhöz) és a „Miniport driver”-ek , melyeket a gyártók biztosítanak és a hardver specifikus részleteket kezelik.

Az első melléklet egy egyszerű hangoló munkamenetet szemléltet – \\.\PHISICALDRIVE0 kezelése történik, ahol a **ZwReadFile** segítségével próbálkozunk az első szektor olvasásával. Láthatjuk, hogy a hangoló motor elemzi alapblokkonként a teljes kód ösvényét.

Saját vezérlővel indult (Klup.sys) és látható, ahogyan eljutunk a **ZwReadFile**-hoz az I/O alrendszeren keresztül, míg el nem érjük a PartMgr.sys-t, amely meghívja a ClassPNP.sys-t és a Disk.sys-t. A teszt- rendszer IDE merevlemezzel rendelkezett, így a végrehajtási folyamat az Ataport.sys, az Atapi.sys és az IntelIDE.sys (miniport driver) felé haladt, majd vissza a ClassPNP-hez, a PartMgr-hez és végül a Klup.sys-hez, ahol a hangolás véget ért.

A hangolás végeztével hozzáláthatunk az elemzéshez, felhasználva a begyűjtött adatokat: a hasznos kód blokkok címeit, a tartalmát és különböző fordítással kapcsolatos statisztikákat. Láthatjuk, hogy minden egyes cím érvényes (mivel „legálisan” betöltött modulok kód szekcióihoz tartoznak) és a kód egy az egyben megegyezik a disc-en lévővel, így feltételezhetjük, hogy a kódfolyamban nem történt módosítás.

28 Checksum: Ellenőrizző összeg

29 „Microsoft Windows Internals, 4th Edition”, Mark E. Russinovich and David A. Solomon, 2004

A második melléklet hasonlóan alapvető hangoló feladatot szemléltet: egy előzetesen megnyitott kezelő használatos a \\.\PHYSICALDRIVE0-t illetően és megpróbáljuk olvasni ugyancsak a **ZwReadFile** segítségével az első szektort. A különbség az, hogy egy TDL3 rootkittel fertőzött gépen futtatjuk a motort.

Ismét a saját vezérlővel indulunk, a Klup.sys-szel, majd elérjük a **ZwReadFile**-t és a PartMgr.sys-t, amely meghívja a ClassPNP.sys-t és a Disk.sys-t. Az adott rendszer (vagy VMWare gép) egy SCSI merevlemezt szimulált, így a Storport.sys kódjának végrehajtása történik meg. Ugyanakkor láthatjuk, hogy a ClassPNP.sys végrehajtása során egy ugrás következik az „lsi_scsi.sys" forrás szekciójára, ahol egy ugródeszka van elhelyezve (2. ábra) egy gazdátlan memória területre – valóban, itt helyezkedik el a rootkit. A hangoló motor tovább dolgozik és végül eléri a Storport.sys-t, majd az lsi_scsi.sys valós kódját, majd visszatér a Klup-hoz normálisan áthaladva a ClassPNP-n és a disk.sys-en keresztül.

Az elemzés során a következő rendellenességek keltették fel a figyelmet:

- Egy ugródeszka az lsi_scsi.sys kódján kívül
- Eltérés a memória és a disc image-ek között az lsi_scsi.sys-t illetően (érdekesen nem a kód szekcióban)
- „Árva" kód végrehajtása – kód, amely nem tartozik a legálisan betöltött modulokhoz

A 9. ábra egy nagyban leegyszerűsített hurok rutint ábrázol; Észrevehető, hogy először a beviteli paramétereket ellenőrzi illetve szükségszerűen módosítja azokat. Amennyiben szükséges, átadja a vezérlést az eredeti kezelőnek és módosítja az eredeti eredményt.

```
Handler ()
{
      Check / Alter Input ()
      Call Original Handler ();
      Check / Alter Results ();
}
```

9. ábra Egyszerűsített rootkit kezelő

Rendszer fertőtlenítés

Nyilvánvalóan a fertőtlenítés legjobb módszere egy tiszta diszkről való boot-olás. Amennyiben a memória már tartalmaz egy rootkitet gátolhatja a fertőtlenítés folyamatát. Ugyanakkor a motor érdekes „live" rendszer fertőtlenítést biztosít.

A 10. ábra egy olyan alap blokkot szemléltet, amely a TDL3 hurkoló rutinjához tartozik. Egyszerűen foltozható az elágazó instrukció kondíciója (11 ábra) – bár a megoldás igen hatékony, nem igazán elegáns. Továbbá a kártékony szoftver ellenőrizheti a saját integritását checksum-ot, vagy más egyéb megoldást használva.

Egy elegáns megoldás lehet az, hogy megtartjuk a párokat vagy alap blokkokat: az eredetit és a hatástalanítottat. Jelenleg „bedrótozott" lista vagy párok használatosak, de szignatúra fájlok használata tervezett. A kódgeneráló motor egyszerű szabályt követ: amennyiben az alap blokk tökéletesen illeszkedik az eredeti blokkhoz, akkor a fordítása úgy történik, mintha ez lett volna a hatástalanított darab. Ezzel a módszerrel hatékonyan hajthatjuk végre a tiszta kódot a létező kód egyetlen bitjének módosítása nélkül, elérve a kívánt eredményt (például az írás/olvasást stb).

```
.822E3B46 8B 44 24 20         mov     eax, [esp+20h]
.822E3B4A 8B 78 60            mov     edi, [eax+60h]
.822E3B4D 80 3F 0F            cmp     byte ptr [edi], 0Fh
.822E3B50 0F 85 95 01 00 00   jnz     __Original_Handler
```

10. ábra A TDL3 hurokhoz tartozó alap blokk (eredeti)

```
.822E3B46 8B 44 24 20         mov     eax, [esp+20h]
.822E3B4A 8B 78 60            mov     edi, [eax+60h]
.822E3B4D 80 3F 0F            cmp     byte ptr [edi], 0Fh
.822E3B50 90                  nop
.822E3B51 E9 95 01 00 00      jmp     __Original_Handler
```

11. ábra A TDL3 hurokhoz tartozó alap blokk (hatástalanított)

Konklúziók

A kernel kód hangolás egy erőteljes rootkit érzékelő technológia. Bemutatásra került a **ZwReadFile** hívás egyszerű hangolása, melynek segítségével elemezhettük ez egész storage stack-et, a fájlrendszertől kezdve a kötet- és partíció menedzsereken, a port és miniport vezérlőkön keresztül az egész láncolatot. A **ZwCreateFile** segítségünkre lehet a teljes fájlrendszer filter vezérlők és a fájlrendszer vezérlők analízisében. Viszont értéktelen eszköz az olyan rootkitek érzékelésekor, melyek fájlokat vagy mappákat rejtenek el. Kevesebb mint egy tucat API hívás ellenőrzése javasolt, különösen a fájlrendszerrel, a registry-vel, a processz- és szálmenedzsmenttel kapcsolatos hívásokat tekintve. Bemutatásra került, hogy a vezérlés kiemelkedő szintje érhető el dinamikus bináris hangolással, mely segíthet az érzékelés területeinek bővítésében és elegáns fertőtlenítő modulokat is szolgáltat.

Bizonyos kernel rootkitek detektálása nem megoldott a jelenlegi motorral. Ezen rootkitek azonosítása más technológiák alkalmazásával javasolt. A **DKOM** (Direct Kernel Object Manipulation) semmilyen módon sem módosítja a kódot vagy a kód folyamot, mivel csak a kernel adatstruktúráit változtatja meg, mint például az EPROCESS listát.

Egy másik típusú rootkit, melyet „Shadow Walker”[30]-nek neveztek el, deszinkronizálja a DTLB[31]-ket az ITLB[32]-kből. Mivel az ITLB-k tartalmazzák a virtuális-fizikai fordítást a kódot illetően, és a DTLB-k tartalmazzák a virtuális-fizikai fordítást az adatot illetően, deszinkronizálva a két tartalmat, lehetővé válhat hogy az X virtuális cím végrehajtáskor kártékony kódot tartalmazzon és olvasáskor pedig tiszta kódot. Ez úgy lehetséges, hogy az X virtuális cím egy különleges fizikai oldalra mutat végrehajtáskor (az ITLB-nek megfelelően) és teljesen más fizikai oldalra mutat olvasáskor (a DTLB-nek megfelelően). Érdekes módon, ebben az esetben a dinamikus bináris hangolás a tiszta kódot hajtja végre, amit a kód generátor olvas és ez elégséges lehet a rootkit detektálásához.

A jelenlegi implementáció csak 32-bites kódok hangolására képes. Nemrég (2010 nyarán) a TDL3-at frissítették (jelenleg TDL4) és 64-bites komponenst is tartalmaz, mivel valószínű, hogy mások is követni fogják ezt a példát, ezért folyamatban van a 64-bites verzió fejlesztése.

30 „Shadow Walker – Raising the bar for rootkit detection”, Sherry Sparks, Jamie Butler, BlackHat Briefings, 2005
31 DTLB: Data Translation Look-aside Buffer
32 ITLB: Instruction Look-aside Buffer

Jelenleg a Windows Sockets Kernelen (WSK) keresztül történő hálózati hívások elemzése történik. Ennek a technikának az alkalmazásával a motor lehetővé teszi majd a legtöbb forgalom filterező kernel malware érzékelését.

Referenciák

Black Hat Europe 2011 (archives)	http://www.blackhat.com/html/bh-eu-11/bh-eu-11-archives.html
Rootkit detection via kernel code tunneling	https://media.blackhat.com/bh-eu-11/Mihai_Chiriac/BlackHat_EU_2011_Chiriac_Rootkit_detection-WP.pdf

A VirusBuster Kft. összefoglalója 2011 második negyedévének *IT biztonsági trendjeiről*

Megabetörések

Hogy az információ érték, mi sem bizonyítja jobban, mint hogy lopni próbálják. Személyi adat vagy ipari titok, netán a politika berkeiben rejtegetett terv – mindegyik iránt van kereslet, s nyilván mindegyiknek megvan az ára.

Nos, az adatbetörések minden fajtájára bőséggel láthattunk példát a mögöttünk álló negyedévben. Ráadásul több incidens olyan nagyszabású, olyan vaskos volt, hogy nemcsak a szaksajtó cikkezett róla, hanem bekerült a világlapok főcímei közé, sőt a tévéhíradókba is. Mikor pedig már azt hittük, hogy több ekkora botrány nem pattanhat ki – napokon belül jött a következő.

A sort a Sony PlayStation Networkjének és Qriocity szolgáltatásának feltörése nyitotta. A japán cég először csak annyit közölt: április 17-e és 19-e között hackertámadás érte a hálózatot, s emiatt lekapcsolták a rendszert. A hálózatot 23 napig nem nyitották meg újra... A belső nyomozás arra az eredményre jutott, hogy 100 milliónál több ügyfél adatai – név, lakóhely és email-cím, születési idő, belépési azonosító – kerülhettek illetéktelen kezekbe. S hogy mindez mekkora kárt okozott? Nos, a Sonynál arra számítanak, hogy a veszteség elérheti a 170 millió dollárt., s ebben a becslésben még nincsenek benne a perköltségek – márpedig lehet, hogy egyes áldozatok vagy áldozatcsoportok bíróságon keresnek elégtételt.

Olajat önthet a tűzre *Richard Blumenthal* amerikai szenátor nyilatkozata, aki szerint a Sony „hallatlanul keveset” tett azért, hogy értesítse a potenciális kárvallottakat. „Ha adatbetörés történik, elemi dolog, hogy az ügyfelekkel haladéktalanul tudassuk: személyi és pénzügyi adataik illetéktelen kezekbe kerülhettek-e, s ha igen, milyen mértékben” – jelentette ki. Mutatja a téma aktualitását, hogy a Consumer Reports „magatartási kódexet” tett közzé – ennek követését javasolja a szervezeteknek, hogy jobban tudjanak vigyázni az ügyfeleikre vonatkozó információra.

Mindenesetre a Sony számai így is jócskán felülmúlják a korábbi hasonló bűnesetek okozta veszteségeket. A TJX kereskedelmi lánc 2007-ben 118 millió dollárt különített el, amiért egy adatbázis-betörés során legalább 45,6 millió bankkártya adatai kerültek veszélybe. A Heartland Payment Systems pedig, ahol 100 millió kártyába pillanthattak bele a hackerek, mintegy 105 millió dolláros többletkiadásra számított.

Még el sem csitultak a világsajtóban a Sony-ügy hullámai, amikor kiderült: „jelentős és kitartó" támadás érte a Lockheed Martin hálózatát. Az óriásvállalat a Pentagon legnagyobb szállítója, világszerte 126 ezer alkalmazottat foglalkoztat, s tavalyi árbevétele 45,8 milliárd dollárra rúgott.

Az amerikai belbiztonsági és honvédelmi minisztérium egyaránt felajánlotta segítségét a Lockheed Martinnek annak felderítésére, hogy pontosan milyen kiterjedt is volt a támadás. Hírek szerint akciójukhoz a behatolók a SecureID elnevezésű beléptető készülékekről készítettek másolatot. Olyan elektronikus kód-távadókról van szó, amelyek 60 másodpercenként új számsorozatot generálnak. A készülékeket az RSA gyártotta – márpedig egy adathalász akció révén áprilisban e cég rendszerébe is behatoltak...

Szerencsére ebben a Lockheed Martin biztonsági szakemberei szinte azonnal észlelték a bajt, s hatékonyan közbe tudtak avatkozni. „A hálózat védelme és az IT-biztonság javítása érdekében tett gyors és átgondolt fellépésünknek köszönhetően rendszereinket továbbra is biztonságban tudhatjuk; egyetlen ügyfél, program vagy alkalmazott adatai sem kerültek illetéktelen kezekbe" – közölte a vállalat.

Aztán – állítólag ugyancsak májusban – a Citigroup következett. A pénzintézet amerikai ügyfélköre körülbelül 1 százalékának adatai juthattak illetéktelen kezekbe. Akármilyen kicsiny a százalékarány, már ez is akár több százezer személyt jelenthet. Születési időt, az Egyesült Államokban oly fontos társadalombiztosítási számot, kártya biztonsági kódot nem lophattak a tettesek – írta a *Financial Times,* mely elsőként közölte a hírt. Ám az érintett ügyfelek neve, számlaszáma és e-mail címe bizony ott volt a potenciálisan eltulajdonított adatok listáján.

Május végén a Honda kanadai részlegénél 283 ezer vásárló adatai kerülhettek illetéktelen kezekbe. Június elején pedig azt olvashattuk, hogy egy magát Pakisztáni Kiberhadseregnek (Pakistan Cyber Army, PCA) nevező csoport mintegy 40 ezer vásároló adatait kaparintotta meg az acer-euro.com-ról.

Ám még ezzel sem volt vége a negyedév folyamán világcégek ellen indított kiberakciók sorának. Valószínűleg hackerek kaparintották meg mintegy 1,29 millió Sega Pass felhasználó személyi adatait – tudatta az érintettek elnézését kérve a japán játékóriás.

Persze a kiberbűnözők nemcsak nagyvállalatokat, hanem kormányzati rendszereket és nemzetközi szervezetek is célba vesznek. *George Osborne* brit pénzügyminiszter például egy konferencián arról beszélt: országa kormányzati hálózataira havonta 20 ezernél több rosszindulatú e-mail érkezik. „Ellenséges titkosszolgálatok 2010-ben több száz súlyos, előre megtervezett támadást indítottak, hogy betörjenek a Pénzügyminisztérium számítógépes rendszerébe. Gyakorlatilag nem telt el nap, hogy ne próbálkoztak volna" – tette hozzá.

Hasonló adatokról számolt be *Thomas de Maiziere* német belügyminiszter: országát átlagosan két másodpercenként éri informatikai támadás, s ezek az akciók az elmúlt években mind kifinomultabbakká és célzottabbakká váltak. A német kormányzati hálózatot naponta négyszer-ötször támadják, gyakran külföldről – mondta a politikus. *Stefan Paris* belügyminisztériumi szóvivő az online kémkedés növekvő veszélyére hívta fel a figyelmet: „Németország igen fejlett technológiával, jelentős tapasztalatokkal és fontos ismeretekkel rendelkező állam, s ezeket az információkat persze mások is szeretnék megkaparintani."

„A hadsereg gyakori célpontja a kiber- és vírustámadásoknak" – jelentette ki *Hilde Lindboet,* a norvég védelmi információs infrastruktúráért felelős hivatal, az INI szóvivője, amikor májusban – egy nappal azt követően, hogy F16-os gépeik részt vettek a líbiai kormányerők bombázásában --, kiterjedt online akció indult a skandináv ország katonasága ellen.

Incidensekről szóló áttekintésünket egy igazi nagy hallal zárjuk. Június közepén került nyilvánosságra: kifinomult eszközökkel beférkőztek a Nemzetközi Valutaalap (IMF) rendszerébe. Nem sok részletet hoztak nyilvánosságra az ügyről, de annyit elismertek a szervezetnél, hogy az év folyamán korábban „igen komoly betörést" szenvedtek el. A kibertámadás hónapokon át tartott. A támadók feltörték az Alap egyik asztali gépét, ahonnan hozzá tudtak férni a rendszerekhez. „Semmi nem mutatott arra, hogy csalás céljából személyes adatokat kerestek volna" – közölték. Hogy akkor mi volt a cél? Nos, egy biztonsági szakértő szerint a feltört gépre olyan szoftvert telepítettek, amellyel egy nemzetállam „digitális belső jelenlétre" tehetett szert az IMF-nél.

Közös felelősség – kormányzati szemszögből

Ilyen súlyú incidensek láttán egyre erősödnek a hangok, amelyek központi, kormányzati beavatkozást sürgetnek, részint a polgárok, részint pedig az államérdekek – ezen belül is kiemelten az országok kritikus infrastruktúrájának – védelme érdekében.

Két éve EU-s cselekvési terv született a kritikus informatikai infrastruktúra védelmének erősítésére. Április elején az Európai Bizottság az elvégzett munkát és a hátralévő feladatokat áttekintve leszögezte, hogy a tagállamok erőfeszítései ellenére további intézkedésekre van szükség. Különösen fontos lenne a számítástechnikai katasztrófavédelmi csoportok (Computer Emergency Response Team, CERT) együttműködésének javítására.

Több feladatot is megjelölt a Bizottság a következő időszakra. 2012-ig fel kell állítani a CERT-et azokban a tagállamokban, ahol ez még nem történt meg, s a CERT-ek között jól működő hálózatot kell kialakítani. (Magyarország már régen létrehozta a maga CERT-jét. A CERT-Hungaryt – a Nemzeti Hálózatbiztonsági Központot – a Puskás Tivadar Közalapítvány működteti, s tavaly dicséretet is kapott az első pán-európai kiber-hadgyakorlaton nyújtott teljesítményéért.) A tagországok készenléti tervei alapján azután jövőre el kell készülnie egy összeurópai készenléti tervnek. Rendszeresen nemzeti szinten is kiber-hadgyakorlatokat kell szervezni. Stratégiai partneri viszonyt kell ápolni a kulcsfontosságú nem uniós országokkal, különösen az Egyesült Államokkal. Elő kell mozdítani a témáról folyó eszmecserét a különböző nemzetközi fórumokon, például a G8 keretében. Végül, de nem utolsósorban meg kell vizsgálni a feljövőben lévő – például felhő alapú – technológiák biztonságával kapcsolatos szabályozási kérdéseket.

„Európának biztonságos, ellenálló és robusztus hálózatokra és online szolgáltatásokra van szüksége. Az elmúlt két év során jelentős előrehaladást értünk el, de fokozni kell az uniós és globális szintű erőfeszítéseket a folyamatosan változó információbiztonsági fenyegetésekkel szemben" – jelentette ki *Neelie Kroes,* az Európai Bizottság digitális menetrendért felelős alelnöke.

Viviane Reding, a Bizottság elnökhelyettese, az unió igazságügyi biztosa a személyi adatok biztonságának javításáért szállt síkra. „Kötelezővé kívánom tenni az adatbetörések bejelentését. Korábban, amikor távközlési biztos voltam, ugyanezt tettem a távközlés és az internet-szolgáltatás területén. Mostani [javaslatom] azonban minden szektorra vonatkozik, tehát a banki és a pénzügyi szolgáltatásokra is" – hangoztatta. Név nélkül utalt a Sony PlayStation Network elleni akcióra, s egy nemrég végzett EU-felmérés eredményére, amely szerint a polgárok 35 százaléka nem bízik abban, ahogy a bankok védik az adataikat. „A gyakori adatbetörések könnyen alááshatják a fogyasztók online gazdaságba vetett bizalmát" – érvelt a politikus. Viviane Reding úgy nyilatkozott: az EU adatvédelmi jogszabályainak felülvizsgálatára vonatkozó javaslatok a következő hónapokban elkészülnek.

Több európai ország önállóan is lépett előre a területen. *Angela Merkel* német kancellár korábban kijelentette: a kiberhadviselés „ugyanolyan veszélyes, mint a hagyományos háború". Nyilván ennek is köszönhető, hogy Bonnban nemrég megalakult a Cyber-Abwehrzentrum, egy speciális központ, melynek feladata a kritikus infrastruktúra védelme. A szervezet a Szövetségi Információbiztonsági

Hivatal gondosan körülkerített irodatömbjében kapott helyet, s munkatársai a Szövetségi Polgári Védelmi és Katasztrófa-elhárítási Hivatalból (BKK) és a Szövetségi Alkotmányvédelmi Hivatalból (BFV) kerültek ki. Júliusban csatlakoznak hozzájuk a Szövetségi Rendőrség (Bundespolizei), a Szövetségi Hírszerző Szolgálat (BND), valamint a hadsereg (Bundeswehr) képviselői is.

Az állami kibervédelem úttörői között tartják számon Észtországot, amely 2007-ben egy elosztott szolgáltatásmegtagadási (DDoS) támadássorozat következtében kénytelen volt teljes internet-szolgáltatását leállítani. A balti köztársaság nemrég bevonta a hivatalos katonai hierarchiába a Kibervédelmi Liga elnevezésű önkéntes szervezetet, s az országban működik a NATO informatikai védelmi mintaközpontja (Center of Excellence in Cyber Defense) is.

Ausztriában most folyik egy 1600 katonából álló, több titkosszolgálati ügyosztályra kiterjedő kibervédelmi erő létrehozása. *Hans Hillen* holland védelmi miniszter nemrég kijelentette: az ország fegyveres erőinek 2011-es költségvetéséből kiberháborús célokra is juttatni kell. A brit kormány a legfenyegetőbb biztonsági kockázatok között jelölte meg a kibertámadásokat, s 650 millió fontot irányzott elő az informatikai biztonság javítására. Franciaországban azt tervezik, hogy az informatikai támadások felismeréséért és leküzdéséért felelős különböző kormányhivatalokat egyetlen egységbe vonják össze.

Eközben az óceán túlsó partján az Obama-kormányzat szövetségi törvényben szeretné szabályozni – mintegy szabványosítani --: mit és hogyan kellene közölniük a szervezeteknek adatbetörés esetén. Megjelent az Egyesült Államok informatikai támadásokra vonatkozó, régóta várt doktrínája is, a „Nemzetközi kibertér-stratégia” („The International Strategy for Cyberspace”) címet viselő tanulmány. A dokumentum olyan nemzetközi IT-biztonsági szabványok kidolgozását sürgeti, amelyek az amerikai kormányszervekre és az ország diplomáciai partnereire egyaránt vonatkoznának. Egyebek mellett segítséget helyez kilátásba azoknak a fejlődő államoknak, amelyek javítani szeretnék hálózataik biztonságát, s felszólítja a világ országait: ne nyújtsanak menedéket az internetes bűnözőknek.

Különösen nagy visszhangot váltott ki, hogy a stratégia értelmében Amerika akár katonai erővel is reagálhatna egy kibertámadásra. „Szükség esetén az Egyesült Államok a kibertérben ellene indított ellenséges akcióra ugyanúgy válaszol, mint bármilyen más, az országot érő fenyegetésre – fogalmaztak a szerzők. – Minden állam elidegeníthetetlen joga az önvédelem, és elismerjük: a kibertérben végrehajtott bizonyos ellenséges akciók szükségessé tehetik, hogy katonai szerződéses partnereink iránti kötelezettségeink értelmében lépéseket tegyünk.” „Fenntartjuk magunknak a jogot, hogy – a nemzetközi jognak megfelelően, azzal összhangban – minden szükséges eszközzel, diplomáciai, tájékoztatási, katonai és gazdasági úton egyaránt megvédjük országunkat, szövetségeseinket, partnereinket, érdekeinket” – hangsúlyozza a dokumentum, hozzátéve: katonai erőt csak a legvégső esetben alkalmaznának.

Az Egyesült Államokban egyébként – a katonai hierarchia keretében – 2009-ben alakult meg a speciális kiberparancsnokság (USCYBERCOM). Nemrég egy londoni konferencián Rhett Hernandez altábornagy, a terület vezetője úgy nyilatkozott: „világszínvonalú kiberháborús haderőt” hoznak létre.

Hasonló hangot ütöttek meg Kínában, az ottani védelmi minisztérium közelmúltban tartott sajtótájékoztatóján, ahol először hangzott el hivatalosan: az ázsiai óriás kiberháborús kommandót hozott létre. „Úgy vagyunk ezzel is, mint a ping-ponggal. Sokan játsszuk, úgyhogy nagyon jók vagyunk benne” – nyilatkozott a *The Timesnak* a kínai Népi Felszabadító Hadsereg egy volt tábornoka, utalva arra, hogy a 30 fős csapatot hatalmas tehetség-tömegből emelték ki.

Jóllehet a kommandó körülbelül két éve alakult meg, szükségességéről már több mint egy évtizede tárgyaltak a katonai vezetésben. A hadsereg hivatalos lapja azt írta: „több tízmilliót” fordítottak az ország első magas szintű katonai kiképző hálózatának kiépítésére.

A kormányhoz tartozó Kínai Fegyverzetellenőrzési és Leszerelési Szövetség egyik vezető kutatója szerint nagy előrelépés volt a Kék Hadsereg létrehozása. „Az interneten nincsenek határok, így nem tudhatjuk, melyik ország vagy szervezet lesz az ellenségünk, ki támad ránk. A Kék Hadsereg fő célja az önvédelem. Mi nem támadunk elsőként senkire" – hangsúlyozta.

Mint a katonai lap írta, nemrég komoly erőpróbából került ki győztesen a Kék Hadsereg. Egy szimulált informatikai csatában nálánál négyszer nagyobb ellenféllel kellett megküzdenie. Vírustámadások sorától, spamáradattól és titkos információ megszerzésére irányuló adatbetörésektől kellett megvédenie a kínai katonai hálózatokat.

Közös felelősség – ahogy az ipar látja

Az informatikai ágazat persze maga is igyekszik minél többet tenni a biztonság javítása érdekében. Minden érdekelt fél felismerte: igazán hatékonyan csak akkor lehet fellépni a számítógépes bűnözőkkel szemben, ha a védelmi technológiák fejlesztői, a kutatók, az operációs rendszereket és a különféle alkalmazásokat kínáló szoftverházak és az állami szervek összefognak.

„Úgy gondoljuk: attól fogva, hogy egy termék vagy szolgáltatás kikerül a piacra, a biztonság közös felelősségé válik. A biztonsági kutatók és a fejlesztőcégek együttműködése végső soron kivédi a támadásokat, s mindannyiunk számítástechnikai környezetének védelmét szolgálja" – olvasható a Microsoftnak egy, a témáról megjelent blogcikkében.

Sokat segíthet a biztonság és a bizalom javításában, ha sikerül világszerte javítani, egységesíteni, átláthatóbbá tenni az antivírus szoftverek tesztelését. Ennek jegyében alakult meg 2008-ban az AMTSO (Anti-Malware Testing Standards Organization, kb. Antivírus Tesztszabványosítási Szervezet). Büszkék lehetünk rá, hogy az alapító tagok között ott volt az egyetlen hazai antivírus-fejlesztő cég, a VirusBuster, melynek képviseletében *Szappanos Gábor* szakértő tagja az AMTSO igazgatótanácsának.

Nos, a szervezet május elején különösen érdekes dokumentummal jelentkezett. Az „Irányelvek a tesztelhetőség elősegítésére (AMTSO Guidelines on Facilitating Testability)" címet viselő anyag kidolgozását a tesztelők javasolták, s az útmutatót a gyártók a tesztközpontokkal közösen készítették el. Belőle az antivírus szoftvercégek megtudhatják, milyen egyszerű megoldásokkal könnyíthetik meg a tesztelők munkáját, hogyan tehetik alkalmasabbá termékeiket a valóban alapos, megbízható vizsgálatra. Milyen ajánlásokat tartalmaz a dokumentum? Például javaslatot tesz arra, milyen információkat naplózzanak, hogyan támogassák a tesztek automatizálását, s nem utolsósorban folyamatos párbeszédre szólítja fel az ágazat szereplőit, hogy a tesztközpontok késedelem nélkül értesüljenek a szoftverekben bekövetkezett változásokról.

„Pozitív jelzés a tesztelők számára, hogy a biztonsági termékek gyártói maguk is hozzájárulnak a tesztelés színvonalának javításához, s nem csak panaszkodnak, hogy ezt vagy azt a vizsgálatot nem tartják megfelelőnek" – értékelte a dokumentumot *Righard Zwienenberg,* az AMTSO elnöke. „Nagy öröm volt látni, hogy versenytársak és tesztelők együtt dolgoznak ezen a fontos területen egy közös célért: hogy jó és megbízható termékeket adhassunk ügyfeleink kezébe. Abban is megállapodtunk, hogy a jövőben fogyasztóbarát, a nagyközönségnek szánt oktató jellegű anyagokat is kiadunk" – tette hozzá Szappanos Gábor.

Szemetelnek, célba lőnek, rémisztgetnek

Megbízható védelmi szoftverre pedig nagy szüksége van mindenkinek, akinek a számítógépe kapcsolódik a világhálóra. A mögöttünk álló negyedév ismét igazolta: a kiberbűnözők minden érdekesebb hírt megpróbálnak kiaknázni, a piac minden rezdülésére reagálnak, mikor kivetik hálójukat.

Alig értesülhettünk például az *Osama bin Laden* elleni sikeres amerikai kommandóakcióról, a bandák máris léptek. A támadások első hulláma a Twitteren érkezett, csupán órákkal a hír bejelentése után. A terroristavezér halálából tőkét kovácsoló site-ok sorában aztán elsők között jelent meg egy spanyol hálókikötő, amely egy állítólagos Bin Laden flash videóval csalogatta kattintásra a látogatót. A lejátszó „kodeket" kért – ám a letöltött állomány valójában egy reklámprogram (adware) volt. Feltörték annak a pakisztáni férfinek a webhelyét is, aki a Twitteren elsőként számolt be az amerikai helikopterek érkezéséről. Site-ja huzamosabb ideig hamis antivírus programmal örvendeztette meg az érdeklődőt.

Említhetjük azután azt a – magyar neten – új jelenséget, amelyre a negyedév folyamán figyeltek fel a VirusBuster kutatói. Eddig csak magánszemélyeknek ígérgettek csekély előleg fejében milliós vagyont a világháló zavarosában halászó e-mailes csalók. Most viszont – kihasználva, hogy sok vállalkozás jutott nehéz helyzetbe – már cégeknek is tesznek „előnyös" ajánlatokat. „Jövedelmező üzlet", „hatalmas összegek", „projekttámogató hitel" szerepel a csalik között. A cégvezetőknek címzett – angolul vagy gépi fordítással, ragokat és szórendet zagyváló neomagyarsággal fogalmazott – üzenetek arra buzdítanak: lépjünk mielőbb kapcsolatba az állítólag pénzeszsákokon ülő feladókkal.

Mindenki tudja: kincset csak mesében szoktak osztogatni a népnek. No de mit veszíthetünk, ha mégis írunk a megadott címre? Ha csak tized százalék esélye van annak, hogy pénzhez jussunk, nem megéri elküldeni azt a két sort?

„Eszünkbe ne jusson válaszolni egy ilyen levélre – dönti el határozottan a kérdést *Szappanos Gábor,* a VirusBuster szakértője. – Csak bajunk származhat belőle. Bármi áll a válaszban, annak már puszta elküldésével megerősítjük, hogy a cím, amelyre a hitegető üzenet érkezett, használatban van. A számítógépes bűnözők felvehetik aktív címeik listájára, s ezzel önmagában hasznot hajtottunk nekik. Címünket nyilván másnak is eladják, úgyhogy garantáltan több levélszemetet fogunk kapni."

De ez még csak a kisebbik baj. Postafordultával céges vagy személyes adatokat kérhetnek tőlünk, s ha még ezt is megküldjük, könnyen visszaélhetnek velük. Ha pedig végigjátsszuk a játékukat, akkor azon kapjuk magunkat, hogy átutaltunk egy kisebb összeget egy külföldi bankszámlára – mondjuk költségtérítés, ügyintézési díj vagy előleg címén. „És ez valóban a játszma vége. Elkönyvelhetjük a veszteséget" – figyelmeztet Szappanos Gábor.

És hogyan alakul a számítógépes bűnözés világviszonylatban? Erről a Ciscónak egy nemrég közzétett tanulmányából alkothatunk képet. A cég kutatói arra az érdekes megállapításra jutottak, hogy a bandák üzleti modellje a kisebb volumenű, ám célzott akciók irányába mozdult el.

Továbbra is e-mailbe bújtatják a legtöbb támadást, ám a céltalanul, nagy tömegben árasztott levelek helyébe mindinkább a nagy pontossággal testre szabott üzenetek lépnek – derül ki a Cisco Biztonsági Hírszerző Műveleti Központjának (Security Intelligence Operations, SIO) felméréséből. Míg a bűnözők bevétele a tömeges e-mail-szórásból az elmúlt egy év alatt kevesebb, mint a harmadára apadt, a jól célzott akciók hozadéka megsokszorozódott.

A Cisco SIO becslése szerint a hagyományos, tömegével küldött levelekkel végrehajtott támadásokból 2010 júniusában még éves szinten 1 milliárd dollárt kasszírozhattak a bandák, ám 2011 júniusára ez az összeg 300 millió dollárra zsugorodott. Ennek hátterében természetesen ott áll a spamvolumen drasztikus csökkenése is: 2010 júniusában napi 300 milliárd, míg idén júniusban már „csak" napi 40 milliárd kéretlen levelet szórtak ki a spammerek.

Ugyanakkor a teljes támadástömegnek mindössze 0,2 százalékára rúgó megtervezett és rosszindulatú támadások fajlagosan nagyobb hasznot hajtottak a bűnözőknek. Alábbi táblázatukban a Cisco SIO kutatói – mértéktartóan – áldozatonként átlagosan 250 dollár veszteséggel számoltak:

Bűnözők haszna (millió dollár)	**Egy éve**	**Jelenleg**
Spam támadások	1.000	300
Megtervezett és rosszindulatú támadások	50	200
Összesen	**1.050**	**500**

Mint a Cisco SIO felmérésében részt vevő 361 szervezet válaszai mutatják, egy-egy jól célzott támadás a konkrét pénzveszteségnél lényegesen nagyobb kárt okoz. Az alábbi táblázat megfertőzött felhasználónként, dollárban kifejezve mutatja az adatokat:

Szervezet mérete	**Pénz-veszteség**	**Probléma orvoslásának költsége**	**Presztízs-veszteség**
	(egy megfertőzött felhasználóra vetítve, dollár)		
< 1.000 felhasználó	327	558	2.346
1.000 - 5.000 felhasználó	233	484	1.436
> 5,000 felhasználó	290	833	1.553

Egy ilyen, határokat nem ismerő bűnözési formával szemben csak nemzetközi együttműködéssel lehet megküzdeni. Ebből mutatott példát a negyedév folyamán az Operation Trident Tribunal, (kb. Szigony Törvényszék Hadművelet), melynek keretében amerikai vezetés mellett sok ország rendőrsége közösen vetett véget két, hamis antivírus szoftverrel (scareware-rel) üzletelő banda tevékenységének.

A hatóságok első célpontja egy olyan, több országra kiterjedő bűnszövetkezet volt, amely három év alatt mintegy 960 ezer gépet fertőzött meg, s az alaptalanul vírusokkal riogatott felhasználókból több mint 72 millió dollárt zsebelt be. Az általuk kreált probléma megoldásáért a társaság „terméke” akár 129 dollárt is kért egy-egy áldozattól. A bandára lecsapó rendőrök több mint 40 gépet, valamint több bankszámlát foglaltak le. Az elkobzott szerverek és más eszközök az Egyesült Államokon kívül Franciaországban, Hollandiában, Lettországban, Litvániában, Nagy-Britanniában, Németországban és Svédországban működtek.

„Mindössze” kétmillió dollár kárt okozott áldozatainak a másik rémisztőprogram-gyártó csoport, amely online reklámra alapozta rosszindulatú üzletét. A vádat Minnesotában emelték az ügyben, a két gyanúsítottat pedig Lettországban tartóztatták le. Ha csakugyan bűnösnek találják őket, az online csalás és összeesküvés vádpont miatt 20 évig, a számítógépes csalás vádpont okán 10 évig terjedő szabadságvesztéssel sújthatók, s emellett mindkét vádpont kapcsán akár 250-250 ezer dollár bírságot vethetnek ki rájuk. Emellett természetesen meg kell téríteniük az okozott kárt is.

Az Operation Trident Tribunalt az FBI számítógépes bűnözéssel foglalkozó részlege irányította, más amerikai szervek közreműködésével, s részt vettek a hadműveletben a brit, a ciprusi, a francia, a holland, a kanadai, a lett, a litván, a német, a román, a svéd és az ukrán hatóságok is.

Kiemelkedő kártevők

A mögöttünk álló három hónap kártevő-körképét vizsgálva a legszembetűnőbb új jelenség az Apple eszközök elleni komolyabb támadások megjelenése. Az almás világot is elérték a kártevőkészítő kitek, és sok mac-ező életét keserítették meg a windowsos környezetben régóta ismert hamis vírusirtók.

Ami az előbbi témát illeti, világszerte bejárta a szaksajtót a hír: földalatti fórumokon egy hacker Mac OS X-re tervezett trójaiépítő-készletet hirdet. A Weyland-Yutani nevű, 1000 dolláros készlet segítségével számítógépes bűnözők pár kattintással készíthetnek az Apple-gépeket támadó kártevőt. Ilyen kiteket eddig csak Windows alá ajánlottak a sötét oldal fejlesztői.

Az viszont már nemcsak a szaklapok címoldalára került ki, hogy széles körben terjedésnek indult egy almás hamis vírusirtó. Május elején több nagy napilap is beszámolt a MacDefenderként bemutatkozó rémisztőprogram (scareware) felbukkanásáról. A kártevő kísértetiesen hasonlít windowsos testvéreire. Azzal riogatja a felhasználót, hogy gépe fertőzött, s hogy hihetőbbé tegye állítását, pár percenként pornósite-okat nyit meg.

A MacDefender telepítéséhez még szükség volt a gyanútlan felhasználók jóváhagyására: a program csak úgy tud települni, ha megadják a rendszergazda jelszót. Rövidesen megjelent azonban a kártevő újabb variánsa, a MacGuard, amely kiküszöbölte ezt a kis akadályt.

Május végén az Apple Mac OS X biztonsági frissítéssel reagált a fenyegetésre. A folttal felruházott operációs rendszer felismerte és eltávolította a MacDefendert, illetve annak variánsait, tehát az utóbb megjelent MacGuardot is. Attól fogva, hogy feltelepítettük a javítócsomagot, a rendszer minden nap lekérdezi a kártevőlistát, azaz megvizsgálja, felvettek-e új kórokozót az adatbázisba.

Erre a funkcióra bizony nagy szükség volt. Órákkal az OS X verzió kibocsátása után már a neten keringett a következő kártevő-kiadás, amely megkerülte a védelmet. Tanulmányunk írásakor az utolsó fejlemény a Mac OS X 10.6.8 júniusi kibocsátása volt, amely ismét sikeresen elhárította a MacDefendert, illetve különböző, időközben született változatait, a MacGuardot, a Mac Securityt és a Mac Protectort.

Elemzők megjegyzik: az Apple-nél mindössze két éve jelent meg a kártevővédelem. Akkor a Mac OS X béta változatának csupán két almára specializált trójait kellett felismernie. Amikor tavaly áprilisban, majd idén márciusban frissítették a szoftvert, még mindig csak összesen két újabb trójai hozzáadására volt szükség...

Híven hűséges kutyájáról szóló jelmondatához – „Buster mindig éberen figyel” – a VirusBuster folyamatosan nyilvántartást vezet a hazai neten észlelt számítógépes károkozókról. A cég szakemberei kiértékelik házon belüli, illetve különböző helyeken működtetett levelezésvédő rendszereik fogását, s az adatokból hónapról hónapra toplistát készítenek, melyet a vállalat site-ján is megjelentetnek, a www.virusbuster.hu/labor/virus-toplista címen.

Mit tapasztaltak a kutatók a mögöttünk álló negyedévben? „Folytatódott a szokásos, botnetekről terjesztett trójaiak áradata. Folyamatosan bombáztak minket a hamis antivírus szoftvert telepítő kártevők. Alábbi, április-júniusi adatokat tükröző toplistánk főleg botnettel (robothálózattal) kapcsolatban álló kórokozókat tartalmaz, ám az alsóbb pozíciókban néhány IRC backdoor kártevő is megjelent” – foglalja össze *Szappanos Gábor,* a VirusBuster szakértője.

A dobogó legfelső fokán álló Backdoor.VanBot a klasszikus, robothálózatot (botnetet) építő kártevők egyike, míg az ezüstérmes Trojan.DL.Small a trójai letöltők seregébe tartozik. Ez utóbbi kórokozó egy vezérlőszerverről titkosított webcímeket olvas be, majd a megadott weblapokról állományokat – természetesen kártevőket – tölt le az áldozat gépére. A hamis antivírus programok telepítésére szakosodott Trojan.Buzus – mely korábban több hónapon át vezette a listát – a negyedévben csak a hatodik helyig vitte.

Szappanos Gábor külön felhívja a figyelmet a negyedéves toplista bronzérmesére, a Trojan.DR.TDSS-re. „Ez egy úgynevezett dropper, magyarul pottyantó – olyan program, amellyel a számítógépes bűnözők más rosszindulatú kódot juttatnak be az áldozat gépébe. Konkrétan a Trojan.DR.TDSS egy botnetekhez köthető, rendkívül veszélyes rootkit becsempészésre szolgál. Ez a fajta kártevő a legmélyebb szintű rendszerfájlokat fertőzi meg, s bizalmas adatok gyűjtésére alkalmas. Ha egy rootkit felkerül a gépre, nagyon nehéz felismerni és megszabadulni tőle” – mondja a szakértő.

És most következzék a VirusBuster kártevő-toplistája 2011 második negyedévéről:

	Kártevő	Részesedés
1.	Backdoor.VanBot	28,40%
2.	Trojan.DL.Small	21,75%
3.	Trojan.DR.TDSS	10,19%
4.	Worm.Rbot	7,53%
5.	Trojan.DL.Deliver	7,18%
6.	Trojan.Buzus	6,58%
7.	Trojan.Agent	1,34%
8.	IRC.Flood.AQ	1,17%
9.	BAT.Noshare.AD	1,10%
10.	Trojan.Sasfis	0,85%
	Egyéb:	13,90%

Az sem érdektelen, hogy a weben barangolva hol kell leginkább fertőzéstől vagy adathalászattól tartanunk. Napjaink elterjedtebb kártevőit alkotóik weboldalakon keresztül (is) folyamatos frissítik. A kártevők felismerésének biztosítása érdekében más víruslaborokhoz hasonlóan a VirusBuster is folyamatosan nyomon követi ezeket a webhelyeket. A gyakori frissítések miatt természetesen csak generikus felismerési módszerekkel kezeljük őket, az utánkövető feldolgozás nem szolgálná a felhasználók érdekeit.

Alábbi táblázatunk április-június legaktívabb kártevő-szóró domainjeit foglalja össze. Láthatóan az Egyesült Államok és Brazília megőrizte előkelő helyét a terjesztő országok között: A bűnözők továbbra is aktívan használják a fájlmegosztó oldalakat (fileave.com, dropbox,com, herosh.com). Ezek mellett a Rugo/Zango reklámprogramot (adware-t) terjesztették legintenzívebben a negyedévben. Érdekesség, hogy a táblázatban szereplő brazil oldal banki trójaiakat terjeszt.

Domain	Fájlok száma	Földrajzi hely	Kártevő
origin-ics.clickpotato.tv	1970	Egyesült Államok	Adware.Rugo
fileave.com	1100	Egyesült Államok	többféle
appbundler.net	940		Adware.Rugo
dropbox.com	678		többféle
hotbar.com	630		Adware.Rugo
screenblaze.com	588	Egyesült Államok	
uol.com	349	Brazília	többféle, elsősorban banki trójai
gabpath.com	327	Kanada	Adware.Gabpath, TrojanSpy.Bzub
p-file.su	270	Oroszország	Trojan.Qhost
herosh.com	206	Egyesült Államok	többféle

Folt hátán folt

A szoftvergyártóknak az elmúlt negyedévben is jócskán akadt vészelhárító feladatuk. Az alábbiakban csak az időszakban kibocsátott legfontosabb foltokról adunk áttekintést, időrendben.

Április

- Tizenhét biztonsági frissítést bocsátott ki menetrendszerű foltozó napján a Microsoft. A foltok összesen 64 sérülékenységet orvosoltak. A javítócsomagok közül kilenc „kritikus”, a fennmaradó nyolc „fontos” minősítést kapott. A foltok a következő szoftverekhez készültek: Windows, Office, Internet Explorer, Visual Studio, SMB, .NET Framework és GDI+.
- Biztonsági frissítésekkel jelentkezett az Apple az iOS-hez, a Mac OS-hez és a Safarihoz. Az iOS-ben és a Safariban foltot kaptak egyebek mellett a WebKit böngészőplatform hibái, melyek kiaknázásával az esetleges támadó saját kódját futtathatta az áldozat gépén.
- Frissítést bocsátott ki Flash Playeréhez az Adobe, hogy betömje a szoftver kritikus rését. A rést már támadták weblapokon, csalárd Word és Excel dokumentumokkal.
- Pár nappal a Flash Player résének betömése után a Reader 9.x, 10.x és az Acrobat X windowsos és macintoshos kiadásához is foltot bocsátott ki a gyártó.
- Megjelent az Oracle menetrendszerű foltcsomagja. A javítássor (hivatalos angol nevén Critical Patch Update, CPU) összesen 73 sérülékenységet orvosolt. Az érintett termékcsaládok listája hosszú: Database Server, Fusion Middleware, Enterprise Manager Grid Control, E-Business Suite és Supply Chain Products Suite, PeopleSoft Enterprise és JDEdwards EntepriseOne, Siebel CRM, Industry Applications, a Sun termékcsomag és végül, de nem utolsósorban az OpenOffice.
- Letölthetővé vált a Google böngészőjének új, 11-es kiadása, melyben egy sor rést is betömtek a fejlesztők – köztük nem egy „nagy kockázatot” képviselt. A Google összesen 16.500 dollár jutalmat fizetett ki a sérülékenységek bejelentőinek.
- Április legvégén készült el a Mozilla böngészőjének 4.0.1-es kiadása. Ezzel napvilágot látott a Firefox 4.0 vonal első biztonsági frissítése. Kibocsátották a fejlesztők a Firefox 3.6.17-et is, amely a browser régebbi kiadásának sérülékenységeit orvosolta.

Május

- Foltozó keddjén egy „kritikus” és egy „fontos” biztonsági frissítést bocsátott ki – három sérülékenység orvoslására – a Microsoft. A foltok a Windows-hoz és az Office-hoz készültek.
- Megjelent a Google böngészőjének 11.0.696.71 jelű változata. Karbantartási és biztonsági frissítésről volt szó. Összesen négy sérülékenységet – köztük két kritikusat – javítottak a fejlesztők.
- Mint korábban szóltunk róla, május végén biztonsági frissítést bocsátott ki Mac operációs rendszeréhez az Apple, hogy megvédje felhasználóit egy rohamosan terjedő hamis antivírus programtól.

Június

- Soron kívül betömött Flash Player-én egy rést az Adobe. A sérülékenységet már aktívan kiaknázták a bűnözők
- Megjelent az Oracle menetrendszerű Java foltcsomagja. A júniusi Java SE Critical Patch Update összesen 17 sérülékenységet orvosolt.
- Tizenhat biztonsági frissítés, összesen 34 rés betömése volt a Microsoft foltozó keddjének mérlege. A javítócsomagok közül kilenc „kritikus”, a fennmaradó hét „fontos” minősítést kapott. A foltok a következő szoftverekhez készültek: Windows, Office, Internet Explorer, .NET, SQL, Visual Studio, Silverlight és ISA.

- Flash és Shockwave Player, Reader, Acrobat, ColdFusion, LiveCycle Data Services és BlazeDS frissítés: ennyi szoftvert javított menetrendszerű foltozó napján az Adobe. Valamennyi frissítés alapvetően olyan sérülékenységeket hivatott orvosolni, amelyeket kiaknázva egy esetleges támadó a távolból magához ragadhatta a rendszer vezérlését vagy a szoftver összeomlását idézhette elő.
- Kibocsátotta az Apple a Mac OS X 10.6.8-as változatát, amely nemcsak fejlesztéseket, hanem egy sor biztonsági hibajavítást is tartalmazott. Összesen 39 rést tömött be az almás cég az új verzióval. Mint korábban említettük, védelmet nyújtott az új kiadás a hírhedt MacDefender kártevő, illetve különböző variánsai – így a MacGuard, a Mac Security és a Mac Protector ellen is.
- Pár nappal később az Apple a Java for OS X 10.5 és 10.6 összesen 11 sérülékenységét orvosolta. Közöttük olyan rések is voltak, melyeken behatolva az esetleges támadó a távolból a saját kódját futtathatta az áldozat gépén.
- Hét rést tömött be a Chrome böngészőben a Google. Közülük hat „magas”, egy pedig „közepes” kockázatot jelentett a webóriás besorolása szerint – azaz egyik sem érte el a legsúlyosabb, „kritikus” minősítést. Mint a Google közölte, a sérülékenységek bejelentői 500-tól 1000 dollárig terjedő jutalmat kapnak.

A VirusBuster Kft.-ről

Aki a VirusBustert (www.virusbuster.hu) választja üzleti partneréül, több mint húsz év szakmai tapasztalatára támaszkodhat. A nemzetközi hírnevű, ám kizárólag magyar tulajdonú, külföldi tőkebevonás nélkül működő cég a számítógépes vírus-, spamvédelmi és egyéb biztonságtechnikai megoldások úttörői közé tartozik. Az évek során a VirusBuster partneri viszonyt épített ki az ágazat számos vállalatával. Víruskereső technológiáját több vezető cég, köztük a Microsoft is beépíti termékeibe. A VirusBuster szoftverei számos nemzetközi díjat, illetve tanúsítványt nyertek, s ma már harmincnál több országban kaphatók.

Magyarországon is több nagy szervezet alapozta informatikai védelmét VirusBuster megoldásokra – köztük a Debreceni Egyetem, az Eötvös Loránd Tudományegyetem, az Invitel, a Magyar Fejlesztési Bank vagy a Magyar Televízió.

Átgondolt szoftver- és szolgáltatásfejlesztést követően 2010-ben a VirusBuster újabb piaci szegmens felé nyitott. Azt a minőséget, amely a nagyvállalatoknál bevált, s amelyet gyártófüggetlen tesztelők is sokszorosan tanúsítottak, elérhetővé tette a cég azoknak az egyéni felhasználóknak a számára is, akik nem az olcsó tömegterméket, hanem a prémium színvonalat, a valódi biztonságot keresik.

A VirusBuster világszerte elismert szakemberei rendszeres előadói hazai és nemzetközi konferenciáknak. Bozsó Julianna, a cég ügyvezető igazgatója az Informatikai Vállalkozások Szövetségétől (az IVSZ-től) 2008-ban elnyerte az „Év Informatikai Cégvezetője” díjat. A kft. 2003-ban „Év innovatív üzleti megoldása”, 2004-ben pedig „IT Reménység” díjban részesült. Két ízben is megkapta a cég az IVSZ-től a „Minősített Szoftver Exportőr” címet és 2005-ben megszerezte az MSZ EN ISO 9001:2001 szabvány szerinti minőségirányítási tanúsítványt. A vállalat webáruháza 2009-ben kiérdemelte a „Fair Business” minősítést, s ugyanebben az évben a VirusBuster Üzleti Etikai Díjat kapott.

Elérhetőségeink

Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ (PTA CERT-Hungary)

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937