Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2011. éves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2011. éves jelentését, amely a év 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, többek között egy-egy cikk erejéig kitérünk a vállalati, a kormányzati és a lakossági szektorok IT és IT biztonsági kérdésköreivel.

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

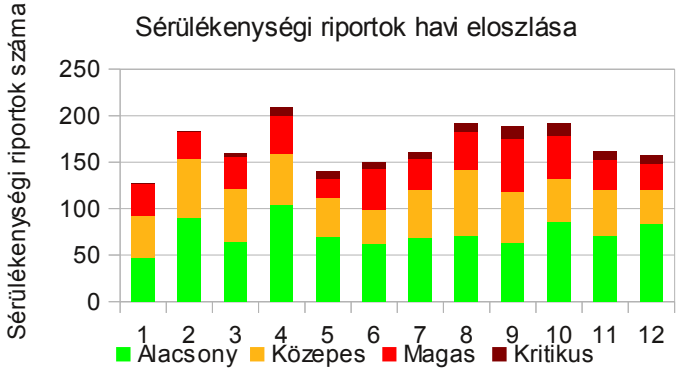
Dr. Kőhalmi Zsolt
Puskás Tivadar Közalapítvány
a kuratórium elnöke

Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

A PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ tevékenysége számokban

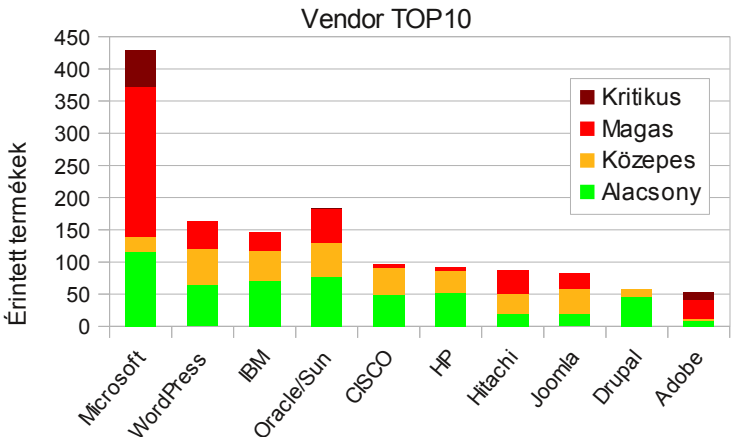
Szoftver sérülékenységek

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. során **2022 db szoftversérülékenységi információt** publikált, amelyekből 883 db alacsony, 607 db közepes, 442 db magas és 90 db kritikus kockázati besorolású.

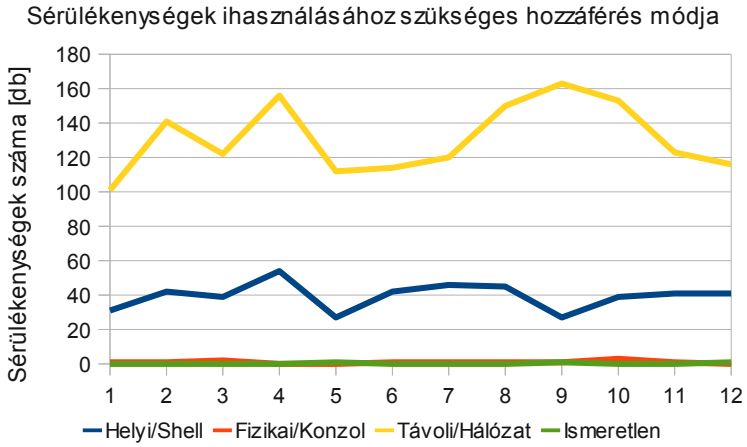
2011-ben összességében közel másfélszer több sérülékenységi publikáció került kiadásra, mint az előző évben. A képet az sem javítja, hogy a magas és/vagy kritikus sérülékenységek száma is közel 40%-kal nőtt az elmúlt év során.



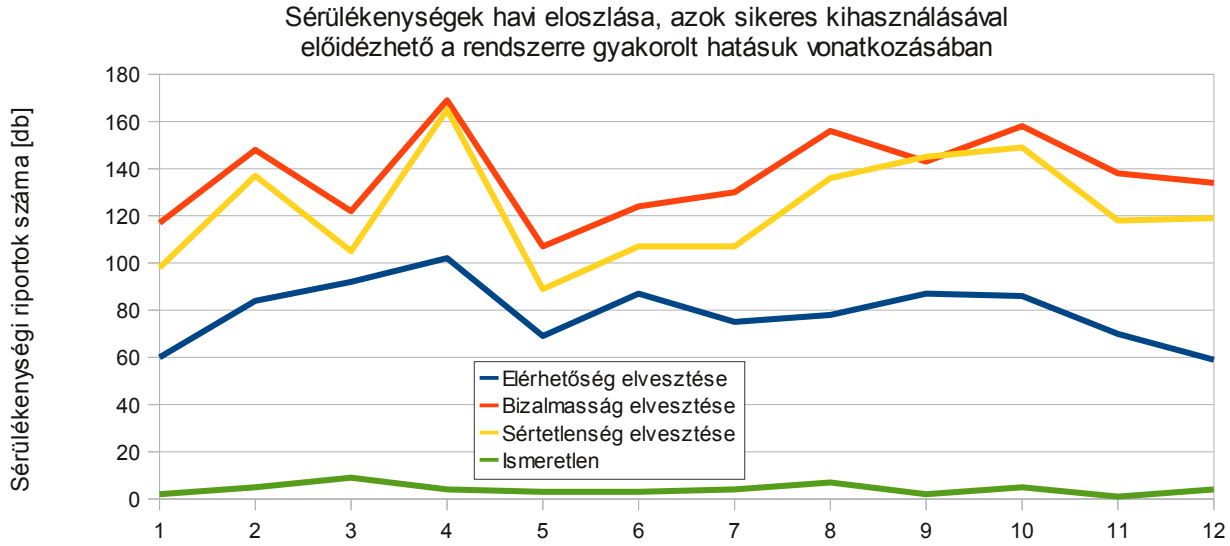
A sérülékenységi információk havi eloszlása április hónapban kimagasló értéket mutatnak, ugyanis több nagyobb szoftvergyártó cég (többek között a Microsoft, Oracle/SUN, HP és az IBM is) ebben a hónapban tette közzé legnagyobb számban a szoftversérülékenységekre kiadott javításait.

A Microsoft még mindig az első helyen teljesít a nevesített platformokhoz köthető sebezhetőségek tekintetében. A gyártó által forgalmazott termékek kétharmadára nézve a feltárt biztonsági rések magas és/vagy kritikus kockázatot jelentenek. Ez a megoszlás csak az Adobe termékek vonatkozásában ér el ennél magasabb arányt, ugyanis ezen termékekre nézve ez az arány 77%.

Továbbra is jól szembetűnik a sérülékenységek kihasználásával az interneten keresztül végrehajtható támadások lényeges súlyponteltolódása, hiszen a szükséges hozzáférések közel 80%-a ilyen. Ez azt jelzi, hogy még mindig nem lehet a távoli betörésektől védő rendszerek használatától és az aktív behatolás-jelző rendszerek használatától eltekinteni, működésük és szabály-rendszereik ellenőrzése ajánlatos minden vállalat és felhasználója számára, akár a munkahelyén, akár távolból dolgozik.



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, programjainkat, míg az elérhetőségre vonatkozó támadásokkal a gépünk rendes működését akadályozzák meg a támadók (ideértve a programjaink törlését és a gépek más célú felhasználását – zombivá változtatását is)

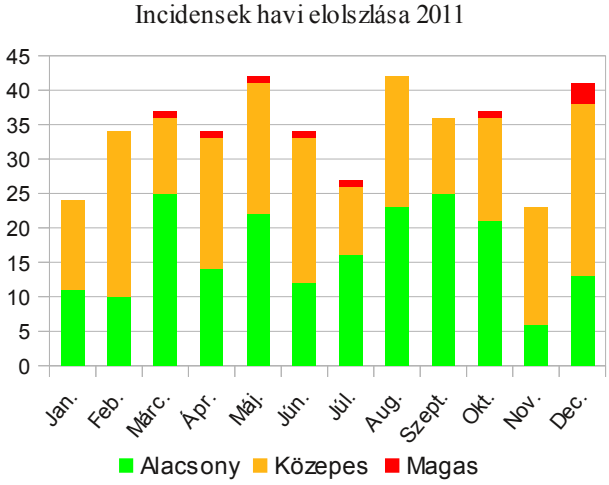


Internetbiztonsági incidensek

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-es év során összesen **411 db incidens bejelentést** regisztrált és kezelt, ebből 198 db alacsony, 201 db közepes és 41 magas kockázati besorolású. Ez közel egynegyedével több, mint az előző év folyamán volt tapasztalható.

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.



A bejelentések többnyire külföldi partner-szervezetektől érkeztek és több mint 84%-ban hazai káros tevékenységgel vagy káros tartalommal voltak összefüggésben.

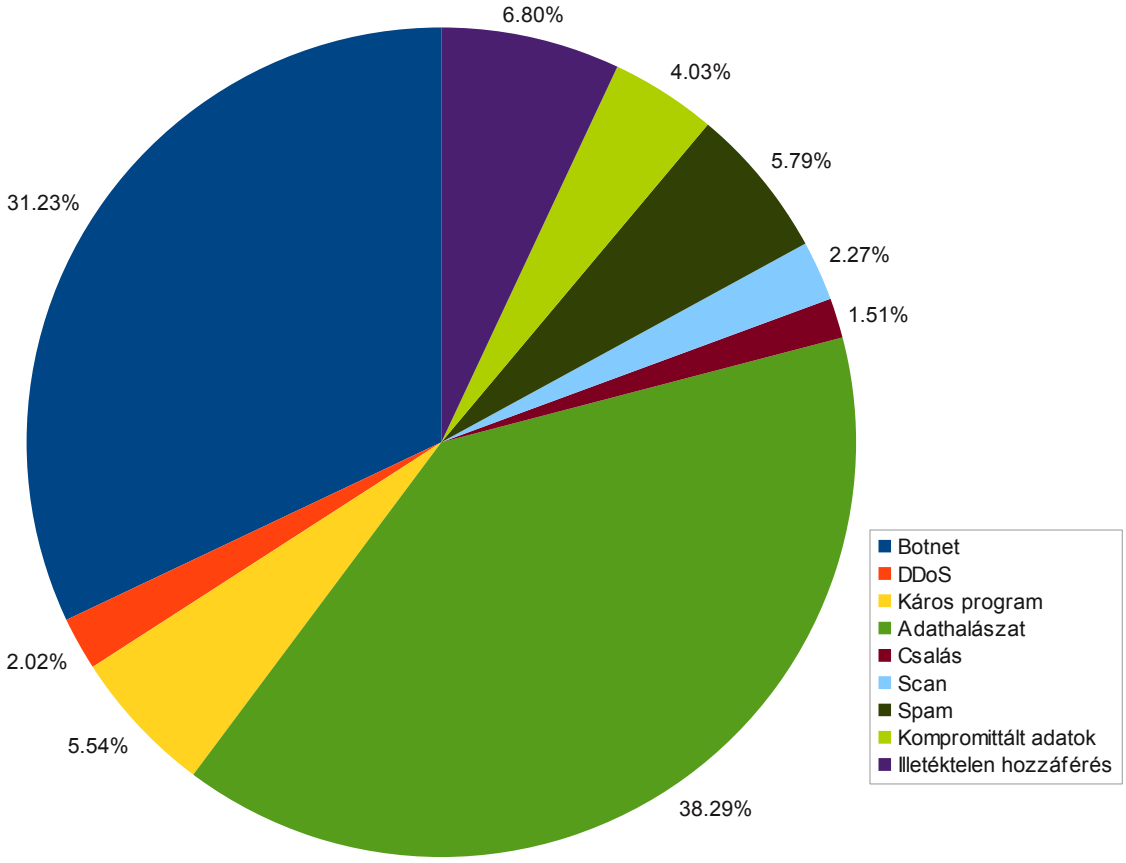
Az egyes incidensek elhárítása kapcsán összesen több, mint 180 magyar és 40 külföldi szolgáltató került bevonásra és összesen 1754 szálon folyt incidenskezelési koordináció.

2011-es év során a legnagyobb számban adathalász tevékenység (38%) és botnet hálózat részét képező számítógépek (31%) kapcsán érkeztek bejelentések. Számottevőek voltak még az illetéktelen rendszer hozzáférési kísérletek kapcsán beérkezett bejelentések, melyek mindösszesen 7%-át teszik ki az összes bejelentésnek.

Mindez azt mutatja, hogy támadók egyre nagyobb erővel igyekeznek kihasználni a felhasználók jóhiszeműségét és a botnet hálózatokon keresztül az erőforrásaikat is.

Központunk a második negyedévet követően növekedést tapasztalt a kompromittált adatokról szóló bejelentésekkel kapcsolatban, az ilyen típusú incidensbejelentések mind a harmadik és a negyedik negyedévre tehetőek és számuk az összes bejelentés 4%-át teszik ki.

Incidensek típus szerinti eloszlása



IT és biztonság a vállalati szférában

Eszközellátottság

Bár némileg eltérő adatokat közöltek, a Gartner[1] és az IDC piackutatói[2] is arra jutottak, hogy 2011-ben visszaesett a személyi számítógépek világszintű forgalma. Az okok sokrétűek a gazdasági bizonytalanságtól az alkatrészhiányig számos dolog nehezítette a gyártók dolgát.

A Gartner szerint az elmúlt év utolsó három hónapjában 92,2 millió PC fogyott, ami 1,4%-kal kevesebb, mint az egy évvel korábban mért érték. Az IDC szakértői egy kicsit több, számszerűleg 92,7 millió számítógép eladását regisztrálták, miközben náluk a 2010-es eredmény nem volt olyan nagy, mint a konkurens kutatócégnél. Így itt a mért visszaesés sem olyan jelentős, mindössze 0,2%-os.

A teljes évet vizsgálva ennek ellenére maradt még némi növekedés. A Gartner 352,8, az IDC 352,4 millió eladott eszközről adott számot, ami 0,5 és 1,6%-os expanziót mutat a cégek saját, előző éves számaival történő összevetéskor. Az elkövetkező időszakot nézve azonban bizakodók az elemzők, az IDC az év eleji botladozást követően nagy felfutást és éves szinten körülbelül 5%-os bővülést vár, míg 2013-ra kétszámjegyű, 11%-ot is.

Az időszak és általában az év vesztese egyértelműen az Egyesült Államok és az EMEA régió. Az USA-ban az IDC adatai szerint az utolsó negyedévben 6,7, míg 2011-ben közel 5%-kal kevesebb gép talált gazdára, mint az egy évvel korábbi hasonló időszakban. Ezzel minden idők második legrosszabb évén van túl az amerikai piac a növekedési mutatók alapján. Ennél rosszabb csak a dotcom válságot követő évben volt: 2001-ben 11,7%-os volt a recesszió.

Az Európát, a Közel-Keletet és Afrikát magában foglaló EMEA régió is gyengélkedett. A Gartner előzetes eredményei alapján az utolsó negyedévben 9,6%-os, miközben éves szinten 7,2%-os volt a visszaesés.

A teljes bukástól az ázsiai, azon belül is a kínai piac mentette meg a szektort. A régióban még a természeti katasztrófáktól sújtott Japán is csak szolid mínuszban zárt.

A magyar IT-ellátottságra vonatkozó megállapítások, amelyeket a 3. negyedéves jelentésben alaposan körbejártunk még mindig megállják a helyüket, nem merültek fel olyan adatok, amelyek az ott közölteket gyökeresen más megvilágításba helyeznék.

Magyarországon hardver oldalon alapvetően az asztali gépek dominanciája figyelhető meg, és még mindig van egy jól körülhatárolható, főként kisvállalati szegmens, amelyik egyáltalán nem alkalmaz informatikai megoldásokat a működésében.

Szoftver oldalon a Microsoft termékek túlsúlya figyelhető meg, a nyílt forráskódú megoldások egyelőre csak marginális, inkább másodlagos eszköz szerepet töltenek be a vállatok mintegy 10%-ánál.

Az alap szintű biztonsági megoldások (vírusvédelem, tűzfal, SPAM-védelem) lefedettsége jónak mondható, ám a magas szintű biztonsági eszközök, amelyekkel a szofisztikált kockázatokat is nagyobb eséllyel lehet semlegesíteni, még mindig nagyon alacsony arányban találhatók meg. (URL-szűrés, naplózás, megfelelő IT-biztonsági szabályzat). A legtöbb vállalatnál a biztonságnak nincsen szakképzett, sőt semmilyen személyi felelőse (61%), a leggyakrabban az informatikai team egy tagja kapja ezt a feladatot, ha foglalkoznak vele egyáltalán.

1 Gartner Group: Gartner Says Worldwide PC Shipments in Fourth Quarter of 2011 Declined 1.4 Percent; Year-End Shipments Increased 0.5 Percent, 2012.01.11.

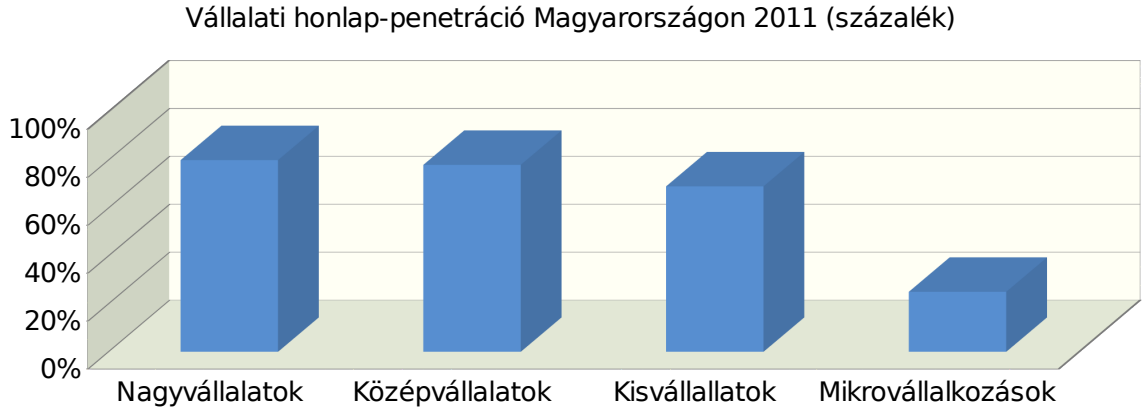
2 Gens, Frank: IDC Predictions 2012: Competing for 2020, IDC 2011. december,

Vállalati honlapok

Mivel a legtöbb potenciális sérülékenység és támadás negyedévről-negyedévre a távoli elérés kategóriájából került ki, fontos a vállalatok és az internet kapcsolatának vizsgálata. A vállalat kockázatának gyakran kitett területe maga a vállalati honlap, ha van ilyen.[3]

Lassan gyarapszik a világhálón jelenlévő hazai vállalatok száma, a lemaradó kisebb cégeknél számos tényező hátráltatja a fejlődést.

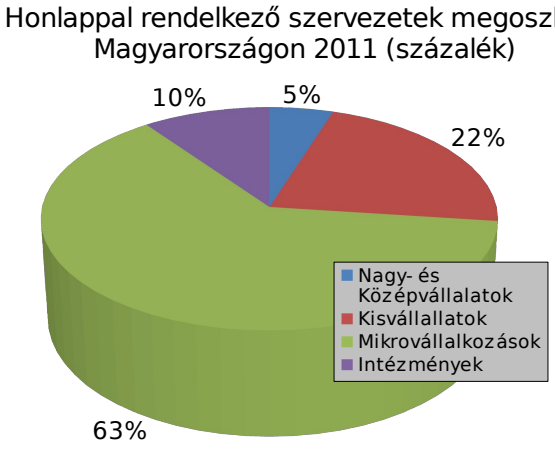
Az internetezők - immár a magyarországi lakosság több mint fele, illetve az üzleti szféra döntéshozóinak túlnyomó többsége - kiterjedt és relatíve potens piacot jelentenek a cégek számára, főként, hogy a felhasználók körében a világháló kiemelt, sokszor elsődleges vagy akár kizárólagos információforrásnak számít vásárlás vagy egyéb döntéshozatal előtt. A cégeknek üzletet hoz az internet, ebből adódik tehát, hogy a weben elvileg minden vállalatnak jelen kellene lennie. Ez azonban még közel sincs így.



A BellResearch friss kutatási eredményeiből kiderül, hogy az összes működő hazai cég mintegy harmada található meg a világhálón saját céges honlappal, illetve valamely terméke, szolgáltatása vagy részlege önálló, külön domain alatt elérhető oldalával.

Közelebbről megvizsgálva az üzleti szféra honlap-ellátottságát, meglehetősen vegyes kép rajzolódik ki. Az elmúlt évek lassú, de folyamatos növekedési ütemét követően idén már a 10 fő feletti vállalatok mintegy 70%-ának van saját honlapja (ezen belül a nagyvállalatok helyzete a legjobb, de náluk sem általános a megjelenés), ebben a körben a penetrációs mutató értéke az elmúlt három évben 10 százalékponttal nőtt. Egyéb téren is nagyok a különbségek: a 10-nél több alkalmazottat foglalkoztató budapesti cégek több mint 80%-a található meg a világhálón, míg a délkelet-magyarországi régióban csupán minden második vállalat.

Még kontrasztosabb - a számosságukat tekintve legnagyobb hányadot képviselő - mikro-vállalatok hátránya, az 1-9 fős cégeknek csupán egynegyede található meg a weben, és ez az arány az elmúlt években alig nőtt. A lemaradás mögött számos ok húzódik: a néhány fős cégek jellemzően nem marketing alapokon működnek, nem látják az internetes jelenlét hozadékát sem, hiányzik a megfelelő döntéshozói-vezetői szemlélet, a stratégia és a kompetencia, emellett relatíve kevesebb a marketingre és honlapépítésre fordítható forrás is. Sőt, a hazai mikrovállalati körben még az internet

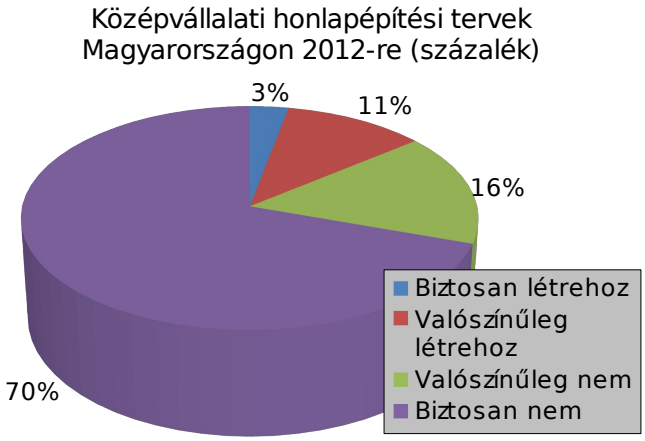


3 Bellresearch: Magyar Infokommunikációs Jelentés 2011.

használata sem általános. Sokan pedig csak addig jutnak el, hogy "honlap kell", noha az internetes jelenlét alapvető célja, hogy üzlet - bevétel és profit - legyen belőle, ahhoz pedig a weboldal létrehozása csak az első lépés.

A tartalom és a megjelenés frissen tartása és bővítése, illetve a további fejlesztések jól mutatják, mennyire tekinti egy cég stratégiai eszköznek a webes megoldásait, jelenlétét, sokat elárul tehát, hogy tízből hat hazai vállalat egyáltalán nem költött ezekre az elmúlt egy évben.

A magyar kis- és középvállalkozások az olcsó webes megoldásokat szeretik. Az átlagos magyar webfejlesztő cégek pedig nem igazán fordítanak időt és energiát az új megoldások, technológiák megismerésére, folyamatosan gyártják a hagyományos megoldásokon alapuló honlapokat. Az eredmény: weboldalak, amelyek nem érik el a kívánt célt, amiért vették őket, tudniillik semmilyen hatással sincsenek az adott vállalkozás profitabilitására, valamint biztonsági szempontból is erősen sérülékenyek, hagyományos megoldásaikkal szinte csak egy „ujjgyakorlatot” jelentenek a képzett behatolónak.

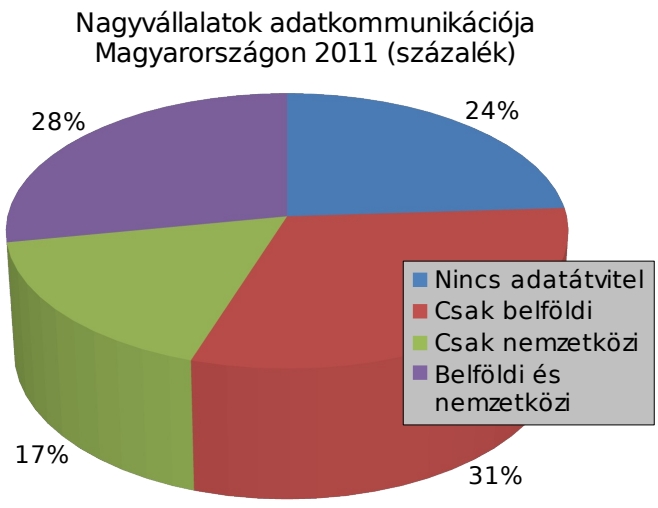


Ennek a helyzetnek tarthatatlanságát már a vállalkozói szféra is felismerte, megalakult az IVSZ online kommunikációs munkacsoportja, amelynek célja kettős: egyrészt emelni a kis- és középvállalatok tudatosságát, hogy webes jelenlétük miként javíthatja profitabilitásukat, másrészt felfelé mozdítani a webes értékláncot a hazai webfejlesztői közösség fejlesztése által.

Adatkommunikáció

Sávszélesség-bővítési igények, integráció és költségoptimalizálás mozgatja az adatkommunikációs piacot; az IP-alapú megoldások térnyerése folytatódik.

Adatkommunikációs megoldást a legalább 10 főt foglalkoztató hazai vállalatok kicsivel több mint egynegyede, a költségvetési forrásokból gazdálkodó intézményeknek pedig a 15%-a vesz igénybe - olvasható a Magyar Infokommunikációs Jelentés legfrissebb kiadásában.



A BellResearch elemzéséből[4] kiderül, hogy ezen a téren az egyes piaci szegmensek között igen jelentős különbségek mutatkoznak. Az adatátvitelben a 250 fő feletti nagyvállalatok járnak az élen, háromnegyedüknél található ilyen megoldás, míg az elterjedtségi arány a cégméret csökkenésével meredeken esik.

Az adatátviteli kapcsolatok - a teljes piacot tekintve - nagy többségükben belföldi végpontokat kötnek össze, ami alól a nagyvállalatok és a nemzetközi háttérrel rendelkező kis- és középvállalatok jelentenek kivételt, a közszférában más országba irányuló adatkommunikáció a kutatás tanúsága szerint

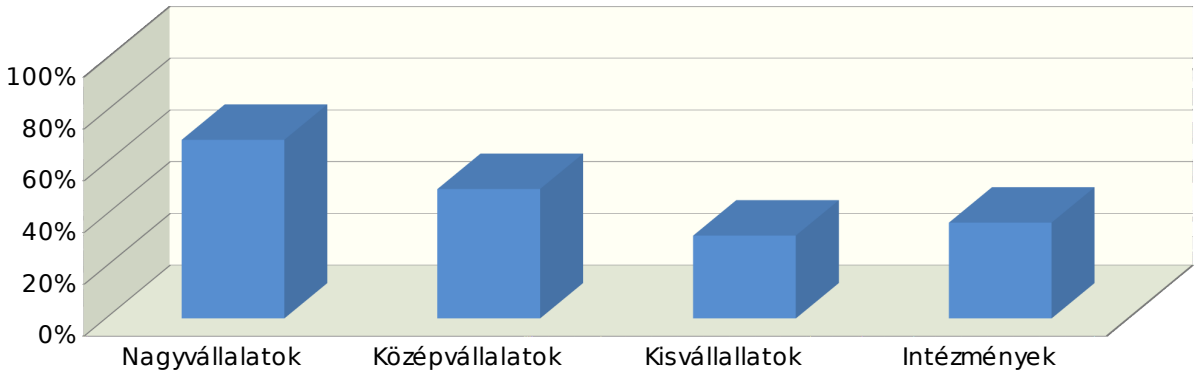
4 Bellresearch: Magyar Infokommunikációs Jelentés 2011.

csak elvétve fordul elő. A kisvállalatok nagyrészt pénzintézetekkel, illetve - jóval ritkábban - üzleti partnerekkel, beszállítókkal és alvállalkozókkal állnak kapcsolatban, míg a közép- és nagyvállalati szegmensben széles körben elterjedtek a telephelyek közötti adatkommunikációs összeköttetések is.

A kutatás a kapcsolatokat technológiai oldalról is vizsgálja. Az üzleti szegmensben - megelőzve a bérelt vonali és az egyéb (például ATM, frame relay stb.) megoldásokat - a legelterjedtebbnek már az IP alapú adatátvitel számít, amely lehet a nyilvános internet feletti vagy szolgáltatói hálózatokon létrehozott virtuális magánhálózat is. Az adatátvitel és az internet egyre erősebb konvergenciáját, illetve általában az IP alapú hálózati megoldások terjedését támasztja alá az is, hogy az adatkapcsolatokat a legtöbb hazai cégnél elektronikus levelezésre, üzleti adatok továbbítására, valamint központi adatbázisok, adattárházak és fájlok elérésére használják.

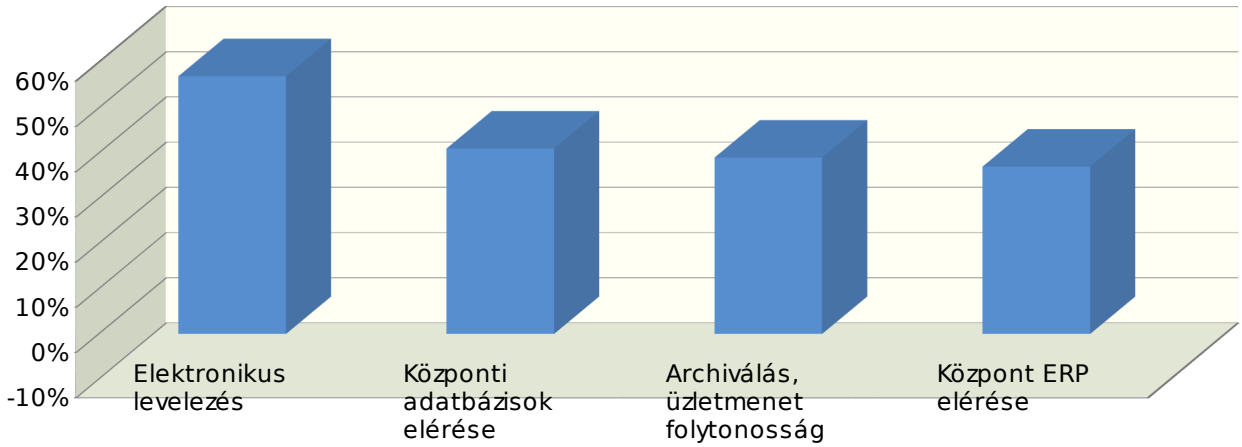
A telephelyeik között adatátviteli hálózatot fenntartó vállalatok jelentős hányada, míg a WAN-nal rendelkező intézmények túlnyomó többsége használja adathálózatát vezetékes telefonálásra, így csökkentve a beszédcélú költségeket, a telephelyek közötti hangforgalom továbbítása általában IP alapon zajlik.

Több telephelyes szervezetek Magyarországon 2011 (százalék)



A mind nagyobb fokú informatizáltság tipikusan egyre magasabb szintű hálózati fejlettséget és nagyobb adatátviteli kapacitásokat kíván, a cégeknek tehát folyamatosan növekszik a sávszélesség iránti igénye, amit a kutatásban felmért döntéshozói tervek is megerősítenek. Az integrált rendszerek bevezetése, illetve a felhőalkalmazások használata is ebbe az irányba mozdítja a piacot.

Adatátvitel használati célok a 10+ fős vállalatok körében Magyarországon 2011 (százalék)



Az üzleti igényeket kiszolgáló, integrált és intelligens távközlési és informatikai megoldásokat már nemcsak a nagyvállalati ügyfélkör, hanem a kis- és közepes cégek is egyre inkább IP alapon szeretnék igénybe venni. Az innováció ugyanis lehetővé teszi a csoportmunkát, távmunkát és ezáltal a vállalati költségek csökkentését.

Big Data

A vállalatoknak minden korábbinál részletesebb és különféle típusú adatokat kell feldolgozniuk és elemezniük, az információkhoz pedig már nem csak az üzleti döntéshozók, de akár a cég ügyfelei is hozzájuthatnak. Mindez azonban újfajta problémákat okoz a vállalati adattárházak fejlesztésében és működtetésében.[5]

Egyre több forrásból származó, exponenciálisan növekvő adatmennyiséget kell tudniuk kezelni a vállalatoknak, amelyek már nem csupán az üzleti rendszerekből, de bárhonnan - akár az internetről is - származnak. Az utóbbi időszakban újabb hívószó került elő a nemzetközi konferenciákon és cikkekben, a "Big Data" kifejezés a minden korábbinál részletesebb, sokféle típusú adatok komplex feldolgozását és elemzését fedi.

Ez alatt azonban nem csupán a nemzetközi cégek több petabájtos adattárházait kell érteni, de ebbe a témakörbe tartozik minden olyan kérdés, amely arra irányul, hogy az addig használt adatmennyiségen túl, miként lehet új típusú adatokat is kezelni. Magyarországon ugyanis már az is probléma, ha egy nagyvállalat 1 terabájtról 10 terabájtra akarja növelni az elemzési kapacitását.

Hazánkban is hamarosan vége lesz annak az egyszerű világnak, hogy csupán az értékesítési adatokat teszik be az adattárházba, és számos új típusú adatot, így például a közösségi médiából származó adatok elemzését is lehetővé kell tenni. Magyarországon is egy évtizede működnek olyan adatbányászati megoldások, amelyek az ügyfelek viselkedésének jobb megértését célozzák, ezek azonban többnyire nagyon komplex elemzési modellekkel működtek. A szakember szerint a Big Data "üzenet" része az is, hogy nagy adatmennyiségen az egyszerűbb modellek jobb eredményt hozhatnak, mint kevesebb adat részletes elemzése.

Magyarországon 1995 tájékán jelentek meg az első adattárházak, mára pedig már minden iparágban megtalálhatók; a leggyakrabban a banki, biztosítói, telekommunikációs, kormányzati és informatikai szektorban. A hazai adattárházak mérete rendkívül változó, a legnagyobbak között több mint 10 terabájtos adatbázisok találhatók. Az adattárházakat, illetve az egyes célelemzésekre kialakított adatpiacokat leggyakoribb statikus jelentések futtatására, ad-hoc elemezésekre, valamint operatív folyamatok támogatására használják.

A szakértők szerint az elmúlt 3-4 évben drámai átalakuláson ment át a piac, fél évtizede jelentek meg az első adattárház-gép (appliance) gyártók, tavaly májustól pedig a piac feltörekvő szereplőit sorban felvásárolták az IT óriások - a Sybase-t az SAP, a Greenplum-ot az EMC, a Netezza-t az IBM, a Vertica-t a HP, legutóbb az Asterdata-t pedig a Teradata kebelezte be.

A technológiai trendek közül kiemelkedik, hogy külföldön terjed a relatíve olcsón és egyszerűen használható, fürtözött szervereken futtatható nyílt forrású Hadoop keretrendszer, amelynek segítségével nagy adatmennyiségen egyszerűbb modellek segítségével futtathatók elemzések. A technológiát ma már csaknem minden óriáscég széles körben használja a hagyományos adattárháza mellett.

Óriási probléma, hogy az adatmennyiség gyorsabban nő, mint amilyen mértékben a memória ára csökken.

Az adatok mennyisége, amiatt is folyton nő, mivel például a nagy online cégek már nem csak azt elemzik, hogy mit vásárolnak az oldalaikon, hanem azt is, hogy hány kattintással, honnan jutottak el oda. Amíg az ügyfélérték a tranzakciós adatokból deríthető ki, egyre nagyobb szerep jut az ügyfélélmény elemzésére, erre az előbb említett interakciós adatokból következtethetnek. Szintén az adatmennyiség óriási mértékű növekedését vetíti előre, hogy a már néhány centért beszerezhető szenzorok egyre több termékbe, mérőórákba, járművekbe, sőt akár haszonállatokra – így például tehenekre – és akár emberekre is kerülnek, amelyek folyamatosan adatokat fognak szolgáltatni viselőjükről.

5 Mozsik, Tibor: Bele fogunk fulladni az adatok óceánjába?, Bitport 2011.05.28.

Az adatelemzési trendek közé tartozik az is, hogy a vállalatok többsége szenved attól, hogy az egyre nagyobb mennyiségű, nem strukturált – értsd: a relációs adatbázisokba, adattárházakba nem beleerőltethető – adatait, így például XML fájlokat, webes forgalmi vagy egyéb logadatokat, videókat, szöveget is elemezni tudja. Ennek következtében terjednek az olyan új elemzési modellek, mint a MapReduce, amely a hagyományos adatokkal szemben a közösségi hálózatok elemzésére, grafikus elemzésre, szövegelemzésre, vagy akár valós idejű mintakeresésre is használható.

A vállalatok nagy bajban vannak, mivel amíg a CPU teljesítmény az elmúlt 30 évben 5 milliószorosára növekedett, addig a merevlemezek sebessége mindössze ötszörösére bővült, ráadásul a kapacitás növekedésével párhuzamosan egyre romlik az adatfeldolgozási teljesítmény. Emiatt a storage iparágnak a következő 2 évben ugrásszerű fejlődésen kellene átmennie, ezt az áttörést a ma még mindig viszonylag drágának tekinthető – de a következő egy évben várhatóan fele ennyibe kerülő - flash memóriák hozhatják meg. Mivel az adatok 20%-át használják 80%-ban, ezért várhatóan a hibrid architektúrák fognak elterjedni, ahol az adatokat automatikusan lehet migrálni a memóriába, SSD-re vagy a merevlemezre aszerint, hogy milyen gyakran használt adatokról van szó.

A hagyományos információmenedzsment a stratégiai döntésekről szól, ám az új generációs információmenedzsmentben már a taktikai döntéshozatalé a főszerep. Így például egy amerikai áruházlánc aszerint változtatja, hány alkalmazottat hív be dolgozni, hogy milyen idő lesz - ha ugyanis esik az eső, kevesebben vesznek szendvicset. Mivel a legnagyobb költség a munkabér, így az ilyen jellegű taktikai elemzésekkel óriási összegeket tud megtakarítani egy vállalat.

A következő években az adatok megjelenítését, jelentések készítését lehetővé tévő üzleti intelligencia (Business Intelligence – BI) eszközök szerepe is átalakul, és egyre fontosabb szerephez jut az ügyfélintelligencia. Ez azt jelenti, hogy immár nem csak a vállalat menedzserei, de az ügyfelek is hozzáférhetnek majd bizonyos, a vállalati adattárházakból származó információkhoz.

Így például az amerikai Wels Fargo Bank már ma kínál olyan – elemző és riport eszközökkel támogatott – online szolgáltatást, amelynek keretében a kisebb pénzű ügyfelek is pénzügyi tanácsadáshoz juthatnak. Egy dél-kaliforniai áramszolgáltatónál pedig az intelligens mérőórából származó adatokat az interneten is meg lehet nézni, és olyan tippeket is lehet kapni, hogy a hűtő korszerűbbre cserélésével mennyivel csökkenthető az aktuális számlaegyenleg.

Felhő szolgáltatások

Tág gyűjtőfogalom a „cloud computing”, olyan, mint az internet. Egyrészt olyan szolgáltatások találhatók benne, mint a nyilvános e-mail, tárhely, szoftver, virtuálisgép-szolgáltatás, amilyeneket a nagy világcégek (Google, Salesforce.com, Amazon, Rackspace stb.) nyújtanak. A felhőszolgáltatásnak itthon is vannak csírái, például az infrastructure as a Service (IaaS), ilyenek a nagy távközlési cégek üzleti célú tárhely- vagy virtuálisgép-szolgáltatásai. Ez lényegében egy fizikai szerverfarmot jelent a szolgáltató telephelyén, s ezen osztoznak az ügyfelek, biztonsági paraméterekkel jól körbehatároltan.[6]

A körülhatárolás azért lényeges, mert az ügyfeleknek fontos adataik integritása, valamint hogy ki és milyen szabályok szerint férhet hozzájuk, illetve hogyan lehet megakadályozni az adatok keveredését. Az sem árt, ha a tárolóeszköz adatvesztés ellen is védett. A hálózati platformokat a szolgáltatók tipikusan úgy építik fel, hogy internetkapcsolatot csak tűzfalon keresztül lehessen létesíteni velük. Ezután következik a tárolóegységek és az adatok fizikai biztonságának kialakítása.

A tárolási platformok tárolórendszerből és szerver szintű számítási kapacitásból állnak. A tárolók biztonsága alapvetően az alkalmazott technológia és a rendszerszintű kialakítás (például redundáns megoldások) beállításaitól függ. Az egészet egy felügyeleti szoftver fogja össze, amelyben bizonyos

6 ITBusiness: Felhőben, de biztonságban, 2012.01.06.

megoldások szintén a hardveres és szoftveres biztonságot szolgálják. Úgy is fel lehet építeni a rendszert, hogy a többszörös fizikai redundanciának köszönhetően egyes tárolók és fizikai kiszolgálók kiesésekor nem vesznek el az ügyfelek adatai – sőt, a virtuális szerverek is kiesés nélkül üzemeltethetők.

A hazai szolgáltatók egyenlőre még inkább az üzleti ügyfeleket veszik célba, azok a nyilvános felhőszolgáltatások ugyanis, amilyeneket például a Google vagy az Amazon nyújt végfelhasználóknak, egyrészt nagyon magas szintű automatizálást követelnek – alacsony testre szabhatósággal –, másrészt megfelelő volumen is szükséges hozzájuk. Magyarországon ilyen szolgáltatások bevezetése még nem lenne rentábilis.

Az üzleti szegmens számára jelenleg tehát valamiféle magánfelhő (private cloud), virtualizált adatközpont kialakítása a cél. Az a biztonság egyébként, amely virtuális platformmal egyszerűen megoldható, fizikai gépekkel sokkal magasabb beruházási költséggel lenne elérhető, hiszen kettőzni kell a kiszolgálókat és a tárolókat – s még így sem lehetne elérni az elvárt üzembiztonságot.

Az ügyfelek számára az egyik fő biztonsági dilemma, hogy mennyire merjék megosztani másokkal a használt infrastruktúrát. A lakossági felhasználók viszont vígan igénybe vesznek nyilvános e-mailfiókokat és tárhelyeket (Google, Picasa, Youtube), sőt a közösségi oldalakon a világ színe elé terítik akár legbizalmasabb adataikat is (pl.: Facebook).

A hazai üzleti felhasználóknak nem kell különösképpen félteniük az előfizetők által rájuk bízott adatokat. Meglehetősen szigorúan szabályozza a magyar jog a biztonsági kérdést. Például egy cég nem tárolhatja a lakossági előfizetők adatait olyan országban, amely nem tagja az Európai Uniónak. Ugyanakkor, ha a lakosság közvetlenül vesz igénybe felhőszolgáltatást (például közösségi oldalakat), akkor a jog számára már édes mindegy, hol tanyáznak az adatok, s ezt egy szolgáltató sem hozza nyilvánosságra. Ez a szabályozatlanság is azt mutatja, hogy a jogalkotás fényévekkel marad el a technológiai fejlődés mögött.

Ugyancsak komoly lehetőségek rejtőznek a felhőből kínált biztonsági szolgáltatások terén. Piackutatók adatai szerint az információbiztonsági SaaS-piac értéke 2011-ben meghaladta az 5 milliárd dollárt, 2012-ben pedig a 6 milliárdot is felülmúlja, ennek több mint felét az üzenetek biztonságának garantálása és a biztonsági mentések adják.

A piaci szereplők marketingje szerint egy felhőszolgáltatásokat kínáló adatközpont sokkal biztonságosabb és magasabb szolgáltatási szinteket tarthat fenn, mint egy vállalaton belüli szerverterem, annál az egyszerű oknál fogva, hogy sokkal több ügyfelet szolgál ki, ezért üzemeltetője többet költhet a szükséges technológiákra.

Az adatbiztonság sérülését okozó események több mint felét vállalaton belüli felhasználó idézi elő akár szándékosan, akár véletlen hibából, felelőtlenségből, a vállalati biztonsági előírások megsértéséből adódóan. Az is gyakori, hogy a heterogén, olykor részben elavult infrastruktúra áttekinthetetlensége miatt kiskapuk maradnak a biztonsági rendszeren, olyan szolgáltatások, amelyek megkönnyítik a behatolást és adatszivárgáshoz vezetnek.

A nyilvános felhőben elérhető szolgáltatások esetében a felhasználó biztonsági adminisztrátori lehetőségei korlátozottabbak, a biztonsági előírások áthághatatlanok, mivel betartásukat a szolgáltató kikényszeríti. Ebben a tekintetben a felhőszolgáltatások magasabb biztonsági szintet adnak, mint a vállalaton belüli infrastruktúra. Az adatokhoz való hozzáférést, az egyes alrendszerek elszigetelését illetően az igényelt szolgáltatási szint és a tervezett munkatípusok határozzák meg az izoláció fokát. Egy nyilvános adatokat tartalmazó webkiszolgálónál a szigor enyhébb lehet, míg egy bérszámfejtő alkalmazás esetében sokkal komolyabb szint kérhető.

A nyilvános felhőben a legtöbb szolgáltatás szabványos, jelentős testre szabásra (beleértve a biztonsági beállításokat is) csak felár ellenében nyílik lehetőség, ha a szolgáltató ezt felkínálja egyáltalán. Ha ez nem felel meg az igényeknek, a vállalati hálózat logikai határán belül kialakított, privát felhő jelenthet megoldást.

Általános tévhit, hogy a felhő-szolgáltatásokra való átállás könnyű és zökkenőmentes. Amíg egyes munkafolyamatoknál valóban könnyű a váltás, bizonyos alkalmazások vagy üzleti igények esetében ugyancsak alapos tervezésre és gondos kivitelezésre van szükség. Sok múlik azon, hogy az egyes gyártók milyen támogatást adnak termékeikhez felhő környezetben.

A felhőszolgáltatások kapcsán a felhasználók olykor azt is feltételezik, hogy a törvényi megfelelést a szolgáltató fogja tanúsítani helyettük. Ez nincs így, viszont minden információt megadnak számukra, hogy ezt maguk megtehessék. Emellett felhasználói oldalon továbbra is biztosítani kell azt a szabályozást, amellyel például megakadályozható, hogy a felhőben levő postaládát használó alkalmazott illetékteleneknek ne adhassa ki a vállalat bizalmas információit.

A felhőszolgáltatók potenciálisan képesek arra, hogy egyes fenyegetéseket hatékonyabban kezeljenek, mint az ügyfelek önállóan. Ezzel bizonyos kockázatok csökkenni fognak felhasználói oldalon, de a felhőszolgáltatásra való áttérés új kockázatok forrásaivá is válik. Ez a kockázati profil vállalatonként más; pontos feltérképezése, a továbbra is felhasználói oldalon maradó feladatok megértése elengedhetetlen ahhoz, hogy a felhőszolgáltatások használata valóban biztonságos legyen. Tévhit azonban, hogy minél nagyobb egy szolgáltató, szolgáltatásai annál biztonságosabbak. Amíg a globális szolgáltatók egyes problémái kezelhetetlen mértékű kieséseket okozhatnak, addig a helyi vagy regionális szolgáltatók a legtöbb esetben felkészültebben, az adott ügyfélre több figyelmet fordítva, helyben adott támogatással működnek, ami nagyobb biztonságot ígér a felhőszolgáltatások felhasználóinak.

Okostelefonok – BYOD

Az okostelefonok és táblagépek elterjedésével a nagyvállalatok informatikai vezetőinél egyre égetőbb a kérdés: támogassák a dolgozók saját eszközének használatát, vagy esetleg tiltsák? Mint sok más esetben, az utóbbi itt sem túl jó választás.

A vezetők jó része hajlamos a könnyebb, biztonságosabb utat választani és inkább erővel elfojtani az ilyen kezdeményezések csíráját is. A világszinten már erősen, itthon pedig némi fáziskéséssel, de mindenképpen jelenlévő BYOD-jelenség (Bring Your Own Device, azaz "Hozd - a munkahelyre - a saját eszközödet") esetében azonban aligha lehet ezt a magatartást követni a CIO-knak, azaz az informatikai részleg vezetőinek.

2011-ben már csak a mobilok 42%-át adták a vállalatok a dolgozóknak munka célú használatra, a maradék 58%-ot olyan eszközök tették ki, melyeket a munkavállaló "civil" életében használ. Ez az arány három éven belül várhatóan egyharmad-kétharmad arányban fog elbillenni a privát mobilok javára.[7]

Természetesen a sok száz vagy akár ezer dolgozót foglalkoztató cégeknél, így sok és sokféle mobil bukkan fel, ez pedig komoly policy, házirend kidolgozását teszi szükségessé. Egyes szervezetek már itthon is rendelkeznek vállalati mobilitási stratégiával, míg mások (egyelőre) inkább teljesen tiltják az ilyen lehetőségeket – "abból baj nem lehet" alapon.

A kutatók szerint a szigor azonban több szempontból is zsákutca. Egyfelől a céges környezet konzumerizációját képtelenség rendeleti úton megállítani, és nem létezik tökéletes vállalati biztonság. Ha a dolgozók meg akarják kerülni a tiltó rendelkezéseket, meg is fogják találni ennek a módját.

Másrészt azért sem jó CIO-ként ilyen defenzív stratégiát alkalmazni, mert a jelenlegi, nehéz gazdasági körülmények között pont ennek ellenkezőjét várják el tőle. Mindent meg kell tennie az informatikai vezetőnek, hogy munkája kimutatható hasznot eredményezzen. A tiltás pedig nyilvánvalóan nem képviseli a proaktív szemléletet.

7 Gens, Frank: IDC Predictions 2012: Competing for 2020, IDC 2011. december,

A privát eszközök munkahelyi használatának engedélyezése azonban számos problémát felvet és még több kockázatot rejt magában. Ennek megfelelően a bevezetés megtervezése, a dolgozók tájékoztatása és a folyamatos ellenőrzés, finomhangolás egyaránt lényeges vetületei egy-egy vállalati BYOD-programnak.

A tiltás és a célzott szelektálás között óriási különbség van. Tehát ha bizonyos rendszerek vagy egyes termékek használata indokolatlanul sok biztonsági kérdést vet fel, vagy komoly plusz erőforrást kötne le, akkor ezek korlátozása érthető kompromisszum a vállalat szempontjából. Szintén érdemes előre rögzíteni, kik és milyen pozícióban számíthatnak arra, hogy az informatikai részleg támogatja munkavégzésüket a saját eszközükön is. Értelmetlen lenne olyanokra pazarolni az IT support munkaidejét, akiknél a munkakörüknél fogva ez nem vagy elenyésző mértékben jelentene teljesítményjavulást.

Kiemelten fontos a céges információk elérésének biztonsági feltételeit rögzíteni, és ezt a lehető legszigorúbban betartatni a dolgozókkal. A kóddal nem védett mobilok, a mindenki által elérhető, nyílt vezeték nélküli hálózatokon küldött bizalmas információk szinte garantálják, hogy nem kívánt kezekbe kerülnek belső adatok. Ebbe a körbe tartozik annak az eldöntése is, hogy a mobil eszközökön keresztül csak elérhetővé tesszük a céges anyagokat, vagy azokat szerkeszthetik és le is tölthetik saját gépükre a munkatársak.

Az egész rendszert érdemes legalább félévente egy alapos felülvizsgálatnak alávetni, és amennyiben a felgyülemlett tapasztalatok indokolttá teszik, változtatni.

Számos problémát és eddig nem létező feladatot hoz tehát magával a BYOD bevezetése, ám az "Úgysem lehet ellene mit tenni" mellett több, a vállalati működésre és eredményességre egyaránt pozitívan ható elem is felsorolható. Ha nem a vállalatnak kell beszereznie a munkára használt mobilt, tabletet, vagy akár laptopot, az önmagában óriási költségmegtakarítást hoz. Ráadásul a dolgozók többsége kifejezetten örül ennek, hiszen nem kell két mobil között váltogatva élni a mindennapjait, azaz a munkahelyi elégedettség is javul.

Biztonság

2011 igen érdekes évnek, sőt az utóbbi néhány év legmozgalmasabb időszakának bizonyult az informatikai biztonság területén. Az újonnan megjelent technológiák biztonsági vonatkozásaira jellemző, hogy a virtuális közeg egyre nagyobb hasonlóságot mutat a valósággal. Már az első negyedévben elkezdődött a váratlan támadások sorozata, ami az addig érinthetetlennek tartott vállalatok – köztük biztonsági cégek – vagy a nemzetbiztonsági jelentőséggel bíró szervezetek és infrastruktúrák ellen irányult.

A betörések mögötti összefüggések azt mutatták, hogy azokat nem feltétlenül a közvetlen haszonszerzés vagy az adott célpont elleni bosszúhadjárat motiválta. A háttérben inkább az információszerzés áll, ami a későbbi akciók sikerének feltétele; ugyanebbe a vonulatba illeszkedik a kormányok közti informatikai kémkedés egyre általánosabb gyakorlata. A trendet az aktivista csoportok (például az Anonymous) fellépése is meghatározza, ami a média főosdrában is a korábbinál sokkal nagyobb visszhangot kapott.

Technológiai szempontból a cloud szolgáltatások és a mobil eszközök rohamos terjedése bír kiemelt jelentőséggel, ami hirtelen felbukkanó kihívások elé állította a legtöbb vállalatot.

Igaz, hogy a biztonsági alapelvek változatlanok maradtak, alkalmazásuk viszont folyamatosan változott, ahogy az új problémák csak igen nehezen voltak kezelhetők a meglévő eszköztárral. 2012-ben tehát a legnagyobb kihívást minden területen a változó felhasználáshoz való igazodás fogja jelenteni, a gyártók szolgáltatásaitól és termékeitől kezdve egészen a jogi szabályozásig.

Nem meglepő, hogy az informatikai biztonságot a piaci szereplők is kiemelten kezelik, nem egy esetben külön üzletág alá szervezve a vonatkozó tevékenységeket. Folyamatosan frissítik termékeiket többek között a naplózás, behatolás-detektálás vagy alkalmazásfejlesztés területén. Mivel a támadások már jellemzően célzottak és testre szabottak, az eszközöket is kellő intelligenciával kell ellátni, ráadásul gyors megoldásokra van szükség, ami a korábbi gyakorlattal szemben a biztonsági szegmensben is felértékeli a cloud technológiák szerepét.

A kutatás eredményei szerint azért ennyire elterjedt jelenség a belső visszaélés, mert sok vezérigazgató és felső vezető nem tartja kiemelt szervezeti feladatnak ezek megakadályozását. A válaszadó szervezetek mindössze 16 százalékánál ismerték fel a vezérigazgatók és egyéb felső vezetők, hogy a belső visszaélések kiemelten magas kockázatot jelentenek.

A nemzetközi trendek Magyarországon is viszonylag gyorsan éreztetik hatásukat: az eddig megszokott, 2-3 éves késés helyett ma már a vállalati szegmensben is legfeljebb féléves eltolódásról beszélhetünk, hasonlóan a végfelhasználói újdonságok beszivárgásához. 2012 a konszolidáció éve lesz, maga a piac pedig várhatóan 3-4 komoly versenyző köré koncentrálódik.

A gazdasági helyzet a világ többi részéhez hasonlóan idehaza sem kedvez az IT-biztonsági szektornak. Csak azok a szállítók lehetnek sikeresek, akik nem csak jó, de gazdaságos megoldásokat kínálnak ügyfeleiknek, hiszen a kiadásokkal ellentétben a kihívások száma idén sem csökken.

Belső visszaélések

Több száz nagyvállalatot felölelő kutatást végeztek a belső visszaélések felmérésével kapcsolatban, amely meglehetősen lehangoló eredményeket hozott.

A Ponemone Institute felmérésében[8] [9] hétszáz vállalatot kérdeztek meg a szervezeten belüli visszaélésekről. A tapasztalatok szerint, bár a legtöbb vállalatnál léteznek szabályok a belső visszaélések ellen, azokat csak ritkán ültetik át a gyakorlatba. Az alkalmazottak tevékenységének nem megfelelő követése számos problémát okozhat, beleértve a negatív pénzügyi hatásokat, a jó hírnév csorbulását, valamint a bizalmas vagy titkos adatok eltulajdonítását.

A válaszadók több mint háromnegyed vallotta be: saját intézményük kiemelt felhasználói korábban bizonyíthatóan, vagy nagy valószínűséggel kikapcsolták, illetve módosították az ellenőrzési folyamatokat, hogy megváltoztassanak fontos adatokat, majd visszaállították a felügyeletet a nyomok eltüntetésére. Ennél is többen nyilatkoztak úgy, hogy dolgoznak szervezetükben olyanok, akik mások hitelesítési adataival visszaélve jutottak magasabb jogosultsági szinthez, illetve kijátszották a feladatkörök szétválasztására hozott szabályokat.

A felmérésben résztvevő cégek átlagosan hetente legalább egy, saját alkalmazott által elkövetett visszaélést fednek fel, miközben minden negyediknél száznál is több eset fordult elő az elmúlt 12 hónapban. A szervezeteknél közel három hónapba telik egy ilyen jellegű esemény felderítése, és legalább ugyanennyi ideig tart az okok felfedése, illetve a szervezetet érintő következmények meghatározása.

Fontos megállapítása a kutatásnak, hogy a belső vizsgálatok kétharmada során nem kerül elő olyan bizonyíték, amely felhasználható lenne az elkövető(k) ellen, így az ilyen esetek jó része büntetlenül marad, ami növeli az ismételt elkövetés esélyét. A válaszadók 52 százaléka – saját bevallása szerint – nincs birtokában olyan technológiának, amely segítene megakadályozni vagy gyorsan felismerni a belső visszaéléseket, például az informatikai erőforrásoknak a nem engedélyezett célra történő használatát.

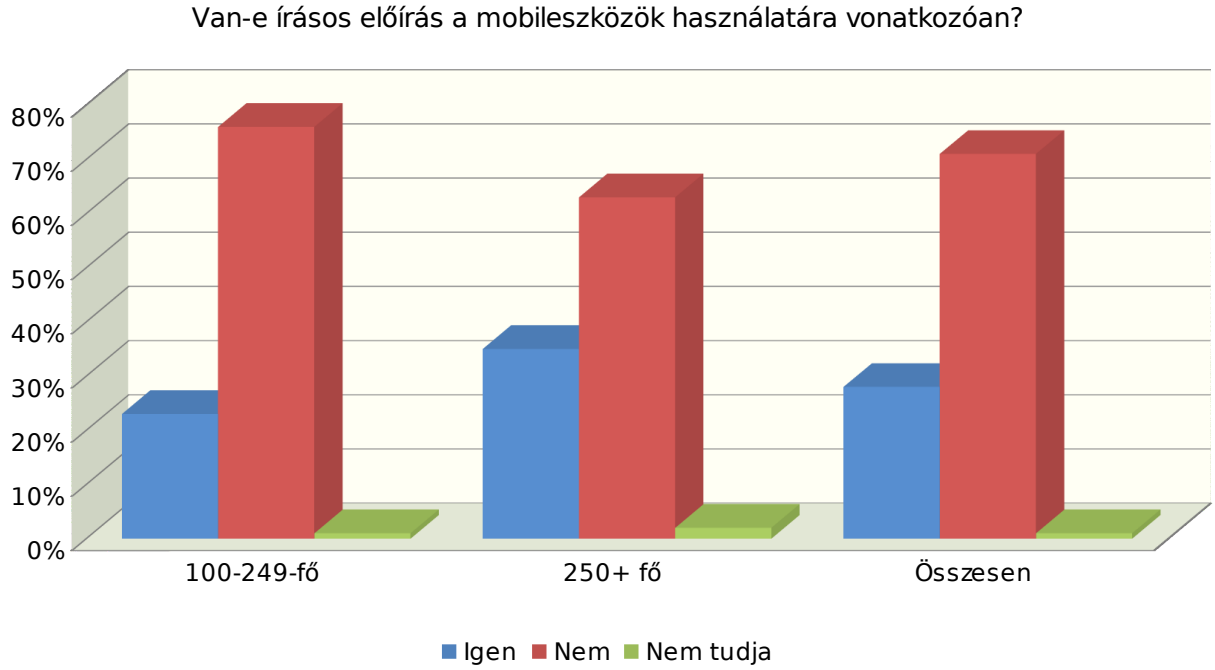
8 Ponemon Institute LLC: Second Annual Cost of Cyber Crime Study Benchmark Study of U.S. Companies, 2011 augusztus,

9 Ponemon Institute LLC - Symantec: Global costs of data breach, 2011. május

Mobilbiztonság

Bár a hazai vállalatok 71%-ánál rendelkeznek okostelefonnal az alkalmazottak, mindössze minden másodiknál alkalmaznak valamilyen megoldást a készülékek védelmére. Ezen kívül más elmaradások is jellemzik a magyar cégek mobilbiztonsági helyzetét.[10]

A vállalati informatikai infrastruktúra védelmével, a biztonsági megoldások használati mutatóival már jó ideje foglalkoznak kutatások. Még azon vállalatok esetében is, akik már valamilyen szinten gondoskodtak a mobil eszközök védelméről, jelentős elmaradások, hiányosságok tapasztalhatóak e téren.



A szakemberek szerint ugyanis hiába tartanak lépést az új eszközök megjelenésével a biztonsági megoldások, a védelem csak akkor százszázalékos, ha ezek alkalmazása mellett a biztonsági házirendeket, eljárásokat és szabályzatokat is folyamatosan frissítik és betartatják a felelősök. Már egy 2008-as Gartner elemzés kimutatta, hogy a szenzitív vállalati adatok háromnegyede elérhető digitális formában - manapság pedig ezekből egyre több vándorol át mobil eszközökre.

A felmérés szerint tízből hét vállalat már használ céges okostelefont a mindennapi munkavégzéshez, a cégek többségénél pedig az alkalmazottak is rendelkeznek magántulajdonban lévő eszközökkel, amelyeket természetesen szintén igyekeznek csatlakoztatni a belső hálózathoz, vagy épp a levelezőrendszerhez. Bár a táblagépek elterjedése még nem jelentős, Magyarországon is megfigyelhető a készülékek térnyerése, különösen a felsővezetői körökben: a kutatásban megvizsgált vállalatok hatoda már rendelkezik valamilyen tablet-tel.

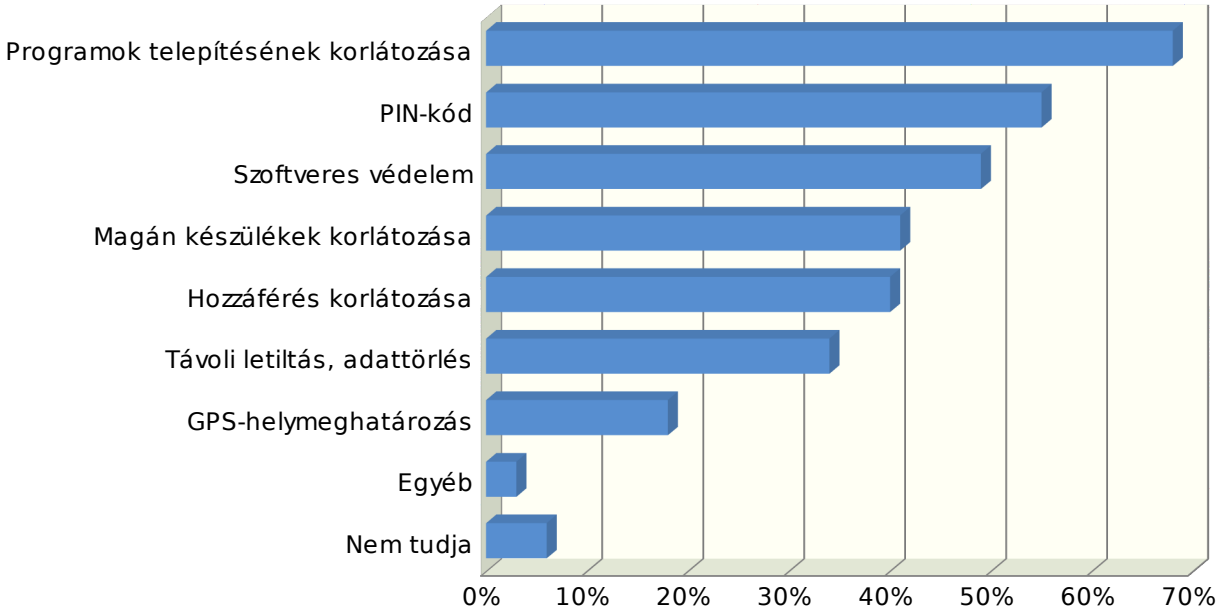
A mobil eszközök széleskörű elterjedésének ellenére a vizsgált vállalatok mindössze 40 százalékában ellenőrzik, hogy milyen tevékenységeket végeznek a munkatársak a mobilkészülékeken. Dedikált informatikai biztonsági szakértővel pedig csupán a cégek húsz százaléka rendelkezik, a többi vállalatnál az informatikai vezetőre hárul a védelem felelőssége is.

A mobil biztonsággal kapcsolatban a válaszadók többsége az adatvesztéstől tart: 69 százalékuk szerint a legnagyobb baj abból eredhet, ha valamilyen hiba vagy támadás miatt eltűnnek vagy manipulálódnak üzleti adataik. Az emberi mulasztás miatti problémákat, például a nem megengedett tartalmak letöltéséből származó károkat a válaszadók fele emelte ki fontos veszélyként, és a vírusfertőzéstől is a megkérdezettek 47 százaléka tart.

10 Bátky, Zoltán: Itthon még gyenge lábakon áll a céges mobilbiztonság, BitPort 2011.09.23.

A védelmi próbálkozások sajnos sok esetben csupán gyenge kísérletek, vagy látszatintézkedések. A legelterjedtebb még mindig a programok telepítésének tiltása, valamint a PIN kód használata. Ezek az egyszerű megoldások azonban nem jelentenek teljes körű védelmet az összes vállalati mobileszközre, valamint nem felelnek meg a vállalatok komolyabb biztonsági előírásainak, hiszen a támadások módszerei is egyre kifinomultabbá váltak.

Az okostelefonok védelmének formái a 100+ fős vállalatok körében 2011. (százalék)



A hazai gyakorlat még nemzetközi szinten is jellemző: az informatikai vezetők a gyökerénél próbálják kiirtani a veszélyeket azzal, hogy egyáltalán nem is engedik be a mobil eszközöket az irodai informatikába. Látszik azonban, hogy ez parttalan és felesleges küzdelem, az élelmes kollégák megtalálják a módot arra, hogy akár engedély nélkül is adatokat másoljanak az okostelefonok memóriakártyáira, vagy a mobilokkal rögzítsenek egy tárgyalást, így szinte felfedezhetetlen sérülékenységeket teremtve.

A megoldás tehát az, ha az eszközöket beengedjük a céges IT infrastruktúrába (Ez nem megkerülhető, mint ahogyan azt a BYOD-jelenséggel foglalkozó 2.6. alfejezetben is kifejtésre került.), de egyúttal szigorú és következetes szabályozással kezeljük az emberi tényezőt, és ehhez kapcsolódó biztonsági megoldásokkal előre befoltozzuk a lehetséges réseket.

A kormányzati szektor

Miközben a 2011-es év vége a jelentős gazdasági visszaesést hozott, a kormányzati informatikában számos pozitív fejlemény volt.[11]

Sikeresen lezárult például egy kétéves, uniós forrásokból finanszírozott fejlesztés, amely az adóhivatal számára készített úgynevezett adóalany-centrikus adatszolgáltatási modell. Bár az elnevezés kacifántos, a mögöttes tartalom éppenséggel az egyszerűsítést szolgálja: az adóalanyok (vagyis az állampolgárok és vállalkozások) végre nemcsak a NAV szempontjai alapján kérdezhetik le a rájuk vonatkozó adózási adatokat, hanem egy helyen tekinthetik meg a velük kapcsolatos adatokat és ügyeket. Így például a munkáltatók számára lehetőség nyílik arra, hogy lekérdezzék a munkavállalóik adóhatósághoz történő bejelentettségét, ezenfelül a munkavállalóknak is lehetőségük lesz megtekinteni, hogy az adóhatóságnál mely munkáltatók milyen időszakra jelentették be őket.

Az állami szektorban az informatika működési kiadásai ezen időszak alatt 15 milliárd forinttal csökkentek, és a szoftverlicenc-gazdálkodás megújítása révén is 30-50 százalékkal tudták lejjebb szorítani az ilyen jellegű kiadásokat. (Ez az összeg viszont igencsak hiányzik a magyar informatikai piacról.)

A működési költségek további lefaragását teszi lehetővé, hogy a központi államigazgatás a következő másfél év során konszolidálni kívánja informatikai rendszereit. Jelenleg 13 szerverteremből, sokszor párhuzamosan működő környezetben szolgálják ki a kormányzat informatikai igényeit. Az uniós forrásokat felhasználó, kétéves, a Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ, korábban Kopint-Datorg) munkájával megvalósuló projekt végére csak ötven (két, egymástól távol lévő adatközpontban elhelyezett) szerver marad, amelyek a hadügy és a külügy kivételével minden minisztériumot és a Miniszterelnökséget is kiszolgálják. A hardverek mellett egységesítik a szoftverrendszereket is; a bevezetendő csoportmunka-alkalmazások lehetővé teszik a távmunkát, és több mint tíz százalékkal csökkentik a papírfelhasználást.

A kormányzati gerinchálózat is változik. Tíz évig a Magyar Telekom szolgáltatta a kormányzati és közigazgatási adatbázisokat, hálózatokat és informatikai rendszereket összekapcsoló elektronikus kormányzati gerinchálózatot, ám ezt a szerződést a magyar állam felmondta.

A 2012 elején életbe lépő új modellben a fizikai infrastruktúrát a Magyar Villamos Művek – pontosabban a hozzá tartozó Mavir – biztosítja, a tulajdonában lévő nagy sebességű, eddig kihasználatlan optikai hálózat révén, a szolgáltatást pedig a NISZ nyújtja majd. A remények szerint a kormányzati célú hálózatok egységesítése, racionalizált üzemeltetése és fejlesztése jelentős költségmegtakarítást eredményez.

Biztonsági tekintetben továbbra is számos hiányossággal kell megküzdeni. Az ISACA magyar szervezete államigazgatási és önkormányzati szervezetek, oktatási és egészségügyi intézmények, pénzintézetek, távközlési vállalatok bevonásával végzett felmérést az információbiztonsági helyzetről. Az eredmények szomorúak, de nem meglepők: a megkérdezettek negyede azt sem tudja, hogy az elmúlt 12 hónap során volt-e náluk külső behatolás vagy éppen eszközlopás.

Ez talán nem is csoda annak fényében, hogy egyhatoduk sem belső, sem külső informatikai auditot nem végez a szervezetnél, több mint 60 százalékuk pedig nem foglalkozik a kockázatok felmérésével – annak ellenére, hogy olyan intézményi körről van szó, ahol sok ember érzékeny adataival dolgoznak, így különösen nagy gondot kellene fordítaniuk az információbiztonságra.

11 ITBusiness: Központosít a kormányzat, 2012. 01. 12.

Vannak azért arra utaló jelek is, hogy a szervezetek is tisztában vannak hiányosságaikkal. Erre utalhat, hogy a legfontosabb információbiztonsági törekvések között az első helyen az informatikai eszközök menedzsmentje szerepel, ezt követi a központi jogosultságkezelés, a katasztrófaelhárítási terv készítése, illetve az átfogó biztonsági szabályzat és eljárásrend készítése.

Pedig a biztonság az év vége felé közeledve is legalább olyan fontos volt, mint korábban, sőt. Magyar kutatók, a BME-n működő CrySys Adat- és Rendszerbiztonsági Laboratórium munkatársai fedeztek fel egy új kártevőt, a sokak által a Stuxnet utódjának kikiáltott Duqut. Ennek sem a kártétel a célja, hanem elsősorban adatokat és információkat – például tervezési dokumentációkat – gyűjt annak érdekében, hogy megkönnyítse egy későbbi támadás végrehajtását más szervezetek ellen. Terjesztéséhez egy addig ismeretlen – de azóta már orvosolt – sérülékenységet használtak ki a Wordben: elég volt megnyitni a fertőzött állományt, hogy a kártevő települjön a gépre.

Az elektronikus egészségügyi rendszerek (e-health) fejlesztése az amúgy kevéssé hatékony és drága egészségügy fenntarthatóságát az innováció nagymértékben segítheti, nemcsak technológiai, hanem intézményi-társadalmi vonatkozásban is.

A mind kisebb helyen elférő mind nagyobb számítási teljesítmény számtalan formában segítheti az egészség megőrzését vagy helyreállítását. Az innovációs versenyeken olyan találmányok születtek, mint például a malária felderítése egy különleges mobiltelefon-kamerával fényképezett vércsepp alapján, vagy zsebben hordható, ultrahangos vizsgálóberendezés. De például az oly sokszor elátkozott Facebook is jó eszköz lehet a manapság népbetegségnek számító depresszió felismerésére. A közösségi oldalon ugyanis minden tevékenységünk nyomot hagy, így cselekedeteinkből, preferenciáinkból, kedvenc filmjeinkből, zenéinkből leszűrhető, sőt mérhető a depresszió foka.

Elektronikus fizetések a kormányzati ügyintézésben

A valódi e-kormányzati szolgáltatások kialakulásának – akár helyi, akár országos szinten – mindeddig komoly gátja volt a megfelelő fizetési infrastruktúra hiánya. A sárga csekk alapú ügymenetre nem lehetett online szolgáltatást építeni.

Elektronikus Fizetési és Elszámolási Rendszer (EFER) működéséhez szükséges intézkedésekről döntött a kormány: október 20-án hozott határozatában előírja: haladéktalanul lehetővé kell tenni, hogy a pénzforgalmi szolgáltatók és az ügyintézést biztosító szervezetek minél gyorsabban csatlakozhassanak az EFER-hez, és átfogó hatásvizsgálat készítését is elrendelte - derül ki a Magyar Közlöny 123. számában közzétett kormányhatározatból.

A kormányhatározat szerint a nemzetgazdasági miniszternek – a Nemzeti Adó- és Vámhivatal (NAV), valamint a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala bevonásával – haladéktalanul lehetővé kell tennie a pénzforgalmi szolgáltatók minél gyorsabb csatlakozását az EFER-hez.

A kormány elrendelte továbbá, hogy 2012. január 31-ig készüljön átfogó hatásvizsgálat az elektronikus fizetés bevezetésének lehetőségéről valamennyi ágazatba tartozó – hatósági vagy nem hatósági – ügyintézés, valamint elektronikus közszolgáltatás vonatkozásában. A hatásvizsgálat elkészüléséért valamennyi miniszter felelős.

A hatásvizsgálatnak fel kell tárnia, hogy az EFER igénybevételével teljesíthető fizetés milyen ügytípusok, illetve fizetési összeghatárok esetében indokolt, összevetve az EFER igénybevételével, illetve az EFER igénybevétele nélküli fizetések felmerülő költségeit, figyelembe véve a lakosság és a vállalkozások adminisztratív terheinek csökkentésével kapcsolatos kormányzati vállalásokat.

A hatásvizsgálatok értékelése alapján a nemzetgazdasági miniszternek a közigazgatási és igazságügyi miniszter bevonásával jelentést kell készítenie a kormány részére 2012. február 29-ig. A kormány döntött arról is, hogy a jelentésben tett megállapításokban érintett miniszterek tegyék meg

a szükséges lépéseket az ügyintézést biztosító szervezetek EFER-csatlakozása érdekében, ideértve az ágazati jogszabályok felülvizsgálatát is. Ennek határideje 2012. május 1.

A Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) május 30-án jelentette be, hogy az okmányirodákban is használható központi elektronikus fizetési és elszámolási szolgáltatást hozott létre, a szolgáltatást első lépésben az okmányirodák és a NAV vette használatba. Az állampolgárok a szolgáltatás révén azonnal tudnak fizetni például ügyintézéskor az okmányirodákban.

E-egészségügy

A 2010-et megelőző néhány évben nem sok minden történt az egészségügy informatikai fejlesztése terén. A kevés eredmények egyike az uniós támogatással létrejött Intézményközi Információs Rendszer. Ennek portálján 2008 tavasza óta három hazai régióban cserélhetik ki betegadataikat a csatlakozott intézmények és háziorvosok, a páciensek pedig akár egészségügyi szolgáltatásokra is előjegyeztethetik magukat). Ugyanakkor az országos kiterjesztésre már nem került sor, s úgy tudjuk, a kedvezőtlen felhasználói visszajelzések alapján erre nem is lehet számítani.

Mára a mintegy 6 milliárd forintos hazai egészségügyi informatikai piac legnagyobb szereplője a Magyar Telekom Csoport lett, miután 2009-ben felvásárolta a kórházi alkalmazásfejlesztéssel foglalkozó International System House Kft.-t. De ez a terület a szokásosnál is jobban függ az államigazgatási költésektől.

Az általuk jegyzett projektek, fejlesztések között megtalálható az automatizált kommunikációra épülő beteginformációs rendszer, továbbá a Mobil e-Egészségügyi Asszisztens szolgáltatás is. Utóbbi egy olyan megoldás, amely okostelefonon segíti a betegek egészségügyi intézményen belüli, illetve intézmények közötti tájékozódását.

Egy másik országos fejlesztést, az elektronikus TAJ-kártya bevezetését a korábbi egészségügyi miniszter, Székely Tamás már 2010-re ígérte, a megvalósítás azonban elmaradt. Az előzetes tervek szerint a papíralapú vényeket kiváltó elektronikus receptet már 2012-ben bevezetik. Az Európai Unióban leginkább Dániában, Svédországban és Hollandiában terjedt el az e-recept, de a piacvezető Észtország, ahol alig két éve indították el a rendszert, s már az összes vény 80 százalékát elektronikusan adják ki.

Az egészségügyi ellátórendszer területi egyenlőtlenségeit szemléltető szakmai térkép is segítheti az ágazat hatékonyabbá tételét. Csakúgy, mint az országos beteg-nyilvántartási rendszer kiépítése, amelyből a jövőben az ellátók lehívhatják majd a különböző intézményekben készült felvételeket. Ez egyébként uniós kötelezettség is: bő két éven belül el kell oda jutni, hogy az úgynevezett nemzeti kapcsolattartó pontokon az érdeklődők hozzáférhessenek a más országokban nyújtott egészségügyi szolgáltatásokra vonatkozó információkhoz. Ez speciális kezelések esetén vagy ritka betegségek diagnosztizálásában segíthet.

Hasonlóan nagyszabású fejlesztés lehet a 2013-ig kiépítendő elektronikus tb-kártya, amely a betegek, a szolgáltatók és a biztosítók közötti online kapcsolat kialakítására lenne alkalmas. Ebben az időszakban valósulhatnak meg a Pólus projektek is, amelyek keretében 10 milliárd forintból 7-8 kórház építhet új integrált épülettömböket. Ehhez kapcsolódóan informatikai beruházásokat is végezhetnek, a teljes projekt összértékének 3–5 százaléka erejéig. A nagy informatikai szállítók már fokozottan készülnek ezekre a projektekre.

Áttérés a nyílt forráskódra

A Nemzeti Fejlesztési Minisztérium váratlan gyorsasággal véget vetett a Microsoft szoftverek tíz éves központi finanszírozásának a közoktatásban.[12]

Úgy tűnik, hogy az ország rohamléptekben zajló megújítása a közigazgatási informatika mezejét is gyökeresen átalakítja. A minisztérium a verseny elősegítésére hivatkozva kívánja megszüntetni az egyetlen piaci cég által fejlesztett szoftverek bérlésének támogatását, az NFM álláspontja szerint a köz- és felsőoktatási intézmények igényeit – néhány kivétellel – az ingyenesen használható, nyílt forráskódú szoftverek is képesek kielégíteni. A jövő évi költségvetés előkészítésekor a Tisztaszoftver program költségeit már nem tervezték be, így az érintett oktatási intézmények az idén júniusban kötött megállapodás értelmében 2012. március 1-ig használhatják jogszerűen a program keretében bérelt a Microsoft-szoftvereket.

A változás teljesen váratlanul érte mind a piacot, mind az intézményeket. A szoftverpiaci nyitást már régóta sürgették a szabad szoftveres közösségek, a nyílt forrás és a nyílt szabványok ügye köré csoportosuló civil szervezetek, illetve a szabad szoftverekre épített üzleti vállalkozások.

Ugyanakkor az időzítéssel kapcsolatban komoly problémák merültek fel, és a váltás gyorsasága - hiszen a szabályozás betűje szerint hónapok alatt kell a hosszú évek alatt kiépített struktúrákat teljesen új alapokra helyezni - nehéz helyzetbe hozhat sok szereplőt.

Még érdekesebb kérdés, hogy mi történik a licencek lejárta után. Vajon az iskolai rendszergazdák leporolják a sok évvel ezelőtt írt CD-ket, és a téli szünet után nekiállnak Linuxot telepíteni? Vagy a központi támogatás elmúltával immár saját erőből, a helyi büdzsé terhére lesznek kénytelenek beszerezni a szükséges licenceket, ráadásul drágábban, a központi beszerzés nyújtotta alkupozíció előnyei nélkül?

Az informatika tárgy gyakorlati érettségi vizsgáján használható szoftverek körét a vizsga lebonyolítása előtt két évvel rögzíteni kell, a szoftververziókat pedig a vizsga lebonyolítása előtt egy évvel meg kell adni. Ez tavasszal, a Microsoft-licencek lejártával szintén problémás helyzeteket eredményezhet.

A szerződéseket ugyanis be kell tartani, még akkor is, ha a másik oldalukon diákok állnak, akik adott esetben azt az ígéretet kapták, hogy a Microsoft szoftvereit használva tehetik le az érettségit. A naptári év vége sajnálatos módon nem esik egybe a tanév végével, ami nyilvánvalóan erős kötöttséget jelent az oktatási intézmények számára. A felsőfokú szakképzések (FSZ) szabályai szerint nagyon sok vizsgát csak Microsoft termékeken lehet letenni.

Még a kellő körültekintéssel megtervezett nyílt forrású migrációknak is megvannak a maguk komoly nehézségei. Nyugat-Európa úttörőinek tapasztalatai is azt mutatják, hogy az átállás költsége csak hosszabb távon térül meg, technikai szempontokból pedig komoly kihívásai vannak. A magyar közoktatás százezres nagyságrendű gépparkjának esetében ez hatványozottan igaz, nem csak a számosság, de az előkészítettség miatt is.

Nem teljesen világos, kik és milyen tudás birtokában vezénylik majd le az esetleges átállást, és hogyan képzik majd tovább – vagy éppen át – az oktatói, üzemeltetői gárdát. Persze a hosszú évekig tartó küzdelem után a szabad szoftverek ügyének támogatói most lehetőséget kapnak, hogy bizonyítsák a nyílt forrású alternatíva életképességét. Azonban a kialakult, vagy még inkább kialakított helyzetben bizonyos mértékig a bukás lehetősége reális alternatívaként van jelen. Több tapasztalat is van már a korábbi évekből, amikor felsőoktatási intézmények megpróbálkoztak ezzel az átállási folyamattal, ám végül nem lett sikeres, már csak azért sem, mert a munkerőpiacon irodai szoftverismeret címszó alatt még mindig a MS Office ismeretét várják el a munkaadók a hallgatóktól.

12 Pfeiffer, Szilárd: Így múlik ki a Tisztaszoftver program, BitPort, 2011.12.29.

A tanárok vagy diákok által igénybe vehető, szociális jellegű szoftverlicencek idejének már régen le kellett volna járnia. Válság ide vagy oda, furcsán veszi ki magát, hogy az állam bizonyos szoftvergyártók licenceit hajlandó támogatni, míg másokét nem, egyes polgárok számára igen, másoknak viszont nem. Ez különösen igaz az oktatás területén, ahol a tanárok, velük együtt pedig a diákok terelgetése olyan csőlátást alakít ki, amely a felsőoktatásból kikerülő, leendő döntéshozókon keresztül gyorsan és széles körben terjed.

Az oktatás után a közigazgatásban is át akar térni a nyílt forráskódú szoftverek használatára a kormány. Erről és az ugyancsak nyílt szabványú dokumentumformátumok előírt használatáról 2011 végén született meg a rendelet.[13]

A kormányhatározat kimondja, hogy a közigazgatásban tevékenykedő intézmények az irodai szoftverekkel előállított dokumentumokat a jövőben az egymás közötti elektronikus kommunikációjuk során kizárólag olyan dokumentumformátumban továbbíthatják, amely nyilvánosan hozzáférhető, korlátozás nélkül alkalmazható, nemzetközi szabványügyi szervezet által elfogadott szabványra épül.

Erősen ajánlott továbbá az irodai szoftverek nyílt forráskódúakra való cseréje is, miután a határozat azt is leszögezi, hogy a jövőben az egyes közigazgatási intézmények és a felügyeletük alatt álló szervek csak műszakilag vagy gazdaságilag indokolt esetben, illetve nemzetközi szerződésekből adódó kötelezettség teljesítése érdekében szerezhetnek be nem ebbe a körbe tartozó irodai szoftvereket. Az intézkedések alól csak a Honvédelmi Minisztérium és az általa irányított szervek kivételek, egyebek mellett a NATO-tagsággal együtt járó kötelezettségek miatt.

A felkészülésre itt is alig több, mint három hónap áll rendelkezésre. A minisztériumoknak március végéig kell felmérniük az ezzel kapcsolatos technikai feltételeket.

Az átállással az eddig éves szinten licencre elköltött 6 milliárd forintnak elméletileg az ötödére eshetnek vissza a dokumentumkezelő rendszerekkel kapcsolatos üzemeltetési költségek a közigazgatásban.

Az átállás, amelynek költsége minimális, nem jelenti feltétlenül az eddig széles körben használt Microsoft Office irodai szoftverek teljes lecserélését. A határozat ugyanis kétféle dokumentumszabványt is elfogad, az OpenDocument Format (ODF) mellett a Microsoft nyílt verziójú Open XML-jét is - jegyezte meg Vályi-Nagy Vilmos.

A váltás nem példa nélküli az Európai Unióban, Hollandiában például az ottani közigazgatási intézmények már 2007 óta csak az ODF dokumentumformátumot használják nyílt szabványként. Az ügyvezető szerint az átállással, 3-4 éves távlatban több tízmilliárd forintos megtakarítás érhető el.

Ahhoz azonban, hogy a folyamat minél kisebb zökkenőkkel menjen végbe, profi tervezésre és levezénylésre lesz szükség. Az átállás kritikus pontja lehet még az abban résztvevők szakmai felkészültsége is.

A nyitás tehát összességében hasznos lehet az ország számára, az alkalmazott módszerek kapcsán azonban jelentős problémák merülhetnek fel. Az biztos, hogy a jogalkotó szándéka egyelőre nem teljes mértékben belátható. Egy ekkora volumenű döntés ilyen hirtelenséggel való meghozatala jelezheti a korábbi, bebetonozott álláspontról való elmozdulás irányába mutatott elkötelezettséget, de könnyen kudarcra ítélheti a változásokat, még mielőtt azok valójában megindulnának.

13 Sági, György: Három hónap alatt kell felkészülnie a közigazgatásnak a nyílt szabványokra, BitPort 2012.01.03.

Kiber-hadviselés

Hetente százas nagyságrendű olyan informatikai biztonsági incidens történik Magyarországon is a kritikus infrastruktúrák üzemeltetésében, amely valamilyen beavatkozást igényel. A jogszabályi felhatalmazással működő szervezetek mellett nemsokára egy önkéntes mozgalom is segítheti az egyre szervezettebb kibertámadások elleni védekezést.[14]

Biztonsági szakértők szerint a közelmúlt eseményei azt sejtetik, hogy a nemzetközi kiberháború már jelenleg is zajlik. Az elmúlt években nem csak a vállalatokat érintő informatikai támadások szaporodtak el, de világszerte megsokszorozódtak az országok kritikus infrastruktúráit érő csapások is, így például az áramszolgáltatókat ért kiberincidensek száma 30 százalékkal nőtt a 2009-2010-es időszakban a korábbi évekhez képest. Számos ország megkezdte már a felkészülést az informatikai hadviselésre, így például az USA, Kína, de Irán és Észak-Korea is jelentős számú hackert foglalkoztat hadseregében.

A kibertámadások legnagyobb kockázata abban áll, hogy az akciók aránylag kis költséggel, kevés ember bevonásával végrehajthatók. Nem véletlen, hogy a vezető hatalmak kivétel nélkül hangsúlyozzák a kibervédelem fontosságát. Az Európai Unió jövőre hozza létre a nagy európai informatikai rendszerek felügyeletével foglalkozó operatív szervezetet az észtországi Tallinnban, ahol a NATO tagországok védelmét összehangoló és kutató Kibervédelmi Központ jelenleg is működik.

A kockázatok nem pusztán elméleti, hanem nagyon is valóságos lehetőségek, a károk bekövetkezése jószerével csak azon múlnak, hogy van-e érdek vagy szándék egy-egy támadás véghez viteléhez. A védelmi feladatok ellátásához ennek az oldalnak is hasonló eszközökkel és tudással kell rendelkeznie.

A magyar kibervédelmi stratégia megalkotása folyamatban van. Magyarországon két helyen, a Nemzeti Nyomozó Irodán és a BRFK-n belül is működik „internetrendőrség”, azonban a nyomozóhatóságnak nem a támadások elleni védekezés, „csupán” a számítógépes bűncselekmények felderítése a feladata.

A közelmúltban egy új civil kezdeményezés, a Önkéntes Kibervédelmi Összefogás (KIBEV) is megalakult azzal a céllal, hogy részt vállalna a hazai kibervédelemben. A megalakítás alatt álló, jelenleg még tagtoborzást végző szerveződés alapvetően a kritikus infrastruktúra üzemeltetők és auditorok képviselőiből állna, akikhez a hazai biztonsági szakma „krémje” is csatlakozhatna.

A mozgalom apropója, hogy a tavaly az iráni atomprogramot megbénító, feltehetően az USA és Izrael által készített számítógépes vírus, a Stuxnet egy új fejezetet nyitott az informatikai- és szolgáltató rendszereket (például víz- és áramellátás, közlekedés, bankszektor) érintő fenyegetettségek történetében, amire minden országnak reagálni kell.

Bár a kormányzati gerinchálózat védelme komoly kockázatcsökkentő tényező, de a kritikus infrastruktúrák védelme túlnyomórészt magáncégek kezében van, amelyek saját belátásuk szerint tesznek azok informatikai védelméért. A KIBEV egy – akár többszáz fős – szakértői „tartalékos csapatot” adhatna, amely egy esetleges országos méretű katasztrófa esetén segíteni tudna az elhárításban. Az önkéntes szerveződésre alapulva az eddigieknél lényegesen nagyobb nemzetközi kibervédelmi gyakorlatokat is lehetne szervezni hazánkban.

14 Mozsik, Tibor: Már zajlik a kiberháború?, BitPort 2011.09.12. http://www.bitport.hu/biztonsag/kiberhaboru-incidensek-cert-kibev

Lakossági felhasználók

Digitális Megújulás Cselekvési Terv névre keresztelték azt a kormányzati infokommunikációs stratégiát, amelyet december 23-án tett közzé a Nemzeti Fejlesztési Minisztérium. Ez meghatározza, hogy 2014-ig milyen elvek alapján, mely területekre fókuszálva történnek majd a kiemelt IT fejlesztések, és a kabinet milyen szabályozással kívánja elősegíteni az információs társadalom fejlődését.

Minderre azért is szükség van, mert az Európai Unió elvárásai szerint három éven belül hazánknak is el kellene érnie, hogy teljes körű legyen a szélessávú lefedettség, azaz minden településen elérhető legyen ilyen hálózat. A célok között szerepel az is, hogy 2015-re a lakosság több mint fele rendszeresen és készségszinten használja a világhálót, így az elektronikus ügyintézési szolgáltatásokat vagy éppen a webes áruházakat.

Az Európai Unió által közzétett Digitális Menetrend fő céljai

- 2013-ig a minimális szélessáv mindenki számára elérhető legyen (100 %-os lefedettség). 2020-ig 30 Mbps, vagy nagyobb sávszélességű hálózat legyen elérhető az EU teljes területén és ezen belül az európai háztartások 50 %-a rendelkezzen 100 Mbps, vagy annál gyorsabb eléréssel.
- 2015-re el kell érni, hogy a lakosság 50 %-a vásároljon online, a kkv-k 33 %-a vásároljon, vagy értékesítsen online és az e-kereskedelem 20 %-a határon átnyúló legyen.
- 2015-ig szűnjön meg a különbség a belföldi és a roaming tarifák között.
- 2015-ig a rendszeres internethasználat mutatója érje el a 75 %-ot (a jelenlegi 60 %-ról), a hátrányos helyzetűek esetében pedig a 60 %-ot.
- 2015-ig a felére kell csökkenteni azoknak a számát, akik még sosem használtak internetet.
- El kell érni, hogy a tagállami kormányzati szolgáltatásokat 2015-ig a lakosság 50 %-a használja és a legfontosabb határokon átnyúló szolgáltatások mindegyike online is legyen elérhető.
- Az infokommunikáció (IKT) területén végzett kutatás és fejlesztés kormányzati beruházások értékét a duplájára kell emelni.

A cselekvési terv 4 akciótervben 83 konkrét akciójavaslatot tartalmaz, ami teljes mértékben illeszkedik a nemrégen indult Új Széchenyi Terv prioritásaihoz.

A kormány négy éven belül 1 millióval csökkentené a „digitális írástudatlanok” számát, különös tekintettel az 50 év fölöttiekre. A széles rétegeknek szóló oktatási programok továbbfejlesztésével egy időben javítani akarják az elektronikus kormányzati szolgáltatások színvonalát, használhatóságát, és fejlesztenék az e-egészségügyet is.

Digitális írástudás

A biztonság fejlesztésének egyik legfontosabb pontja a felhasználói tudatosság fejlesztése. Ezt az otthonokban, az egyéni felhasználók szintjén kell elkezdeni. Ha itt sikerül az alapelveket megfelelően megismertetni, a biztonság tudatosságot és igényességet belenevelni a felhasználókba, akkor ezt továbbviszik a szakmai életükbe is, legyen az a vállalati szféra, a közigazgatás, vagy éppen az oktatás.

Az ország versenyképességét sokféleképpen lehet javítani, ennek egyik eszköze a digitális esélyegyenlőség megteremtése. Ez függ többek között az eszközellátottságtól, a sávszélességtől és a

közösségi internet-hozzáférési helyek számától. Ezekkel nincs komoly probléma hazánkban, az utóbbi években megfelelően felzárkóztunk.

Vannak azonban jelek, amelyek súlyos problémákat mutatnak a felszíni mutatók alatt: az EU-s pénzekből intelligens táblákkal, trendi PC-kkel, laptopokkal felszerelt iskolákba nem hívják be a nem iskolásokat, vagy az olyan internet-népszerűsítő programok, mint a Kattints rá Nagyi, a Netrekész vagy a NetX1 legfeljebb csak néhány ezer embert értek el. Márpedig, amíg ezek a programok nem tömegesednek, addig nem lehet semmi olyan hatást elérni, amely az emberek millióiban kelti fel az igényt. Ezt az igényt sokféle módon fel lelhet kelteni. Új technológiai megoldásokkal, innovatív eszközök piacra dobásával, de lehet úgy is, 'hogy például az államtól az emberek kikövetelik az elektronikus közigazgatási szolgáltatások felhasználóbarát kialakítását. A tömegigények nyomán pedig önmagát erősítő fejlődés indulhat be.

Három év alatt 10-15 milliárd forint: ekkora forrásra lenne szükség az NJSZT szerint, hogy legalább másfél millió, még „érintetlen" ember 18-20 óra alatt hozzájusson a minimális tudáshoz, azaz internet használati, elektronikus levelezési, szövegszerkesztési alapismeretekhez.

Ez az összeg elenyésző ahhoz képest, hogy ennek befektetése mekkora társadalmi és gazdasági hasznot hajtana. Mindehhez mindenekelőtt szükséges egy központi kampány az igényfelkeltéshez masszív állami részvétellel és profi reklámszakemberekkel, együttműködésben a „megszállott" kezdeményezőkkel. A terjesztésbe, képzésbe már számos intézmény, szervezet bevonható, aminek során, nem utolsósorban, munkaalkalmak is teremtődnének. Mindez a közösségi helyeken kivitelezendő: eMagyarország-pontok, könyvtárak, posták, iskolák, művelődési házak.

A kampányhoz a szervezeti háttér rendelkezésre állna, hiszen immár több mint 400 ezer ECDL-tanítványt tartanak nyilván, minőségbiztosítási rendszerrel. Ez pedig jóval komplexebb feladat, mint egy alacsonyabb szintű tudásmennyiség terítése. S finanszírozni is csak az után kellene, hogy az érintettek már megszerezték a tudást.

Másik probléma a hátrányok nehéz számszerűsítése, mérése. Ugyanis nincs mérce, amihez képest kiugorhat, hogy ezen a területen elmaradásban van Magyarország. A statisztikákban ki lehet mutatni ezt az elmaradást, de a gazdasági válsággal, végtörlesztéssel, politikai csatározásokkal terhes mindennapokban erre nagyon kevés ember figyel. Pedig a szakértők szerint már most is majdnem késő. Az idősödő népesség egyre jobban leszakad. A felnövekvő nemzedékek beleszületnek ugyan a digitális világba, de nem lesznek annak tudatos használói. Néhány év múlva már nem lesz kérdés a digitális írástudatlanság, hiszen elárasztanak minket az eszközök, és lehet, hogy kényszerből, de nem lesznek digitálisan írástudatlanok - funkcionális digitális analfabéták viszont tömegével maradnak.

Social engineering

Ismert tény, hogy minden biztonsági rendszer, csak annyira erős, amennyire a leggyengébb pontja az. A legtöbbször sajnos ez a gyenge láncszem az emberi tényező, a felhasználó, akár otthoni, akár munkahelyi környezetében.[15]

A csalók, akik célzottan a felhasználót támadják, külön területét képviselik az informatikai bűnözésnek. Védekezni ellenük nehéz, de nem lehetetlen.

Ez a fajta támadás emberi tulajdonságokat használ ki. Rengeteg tulajdonságot fel lehetne sorolni, melyeket egy támadó kihasználhat: a kíváncsiság, hiszékenység, befolyásolhatóság, figyelmetlenség csak néhány példája ezeknek. De nem kell különösebben naivnak vagy hiszékenynek lenni ahhoz, hogy valaki social engineering-támadás áldozata legyen, mert könnyen kihasználható a minden emberben meglévő segítőkészség is. Ha valaki új alkalmazottként kér valamit, szívesen segít neki bárki.

15 ITBusiness: A lélek mérnökei, 2011.12.01.

Egy támadás általában négy lépésből áll össze:

- A legelső és leghosszabb fázist a szükséges információk összegyűjtése jelenti a vállalatról, a célszemélyről vagy éppen arról, akit megszemélyesíteni akar a támadó. Az információmorzsák összeszedéséhez jó eszköz a céges honlap, a munkatársak közösségi portálokon megjelenő profiljai, különösen, ha a munkahelyüket, sőt akár a beosztásukat is beírják.
- A megfelelő tudás birtokában jöhet a második fázis, a kapcsolat kiépítése, akár mint munkatárs, akár mint külső partner.
- Ha sikerült a leendő áldozat bizalmába férkőzni, akkor jön a kapcsolat kihasználása, és az eredetileg is tervezett információ megszerzése. „Te, nem tudok bejelentkezni a gépemre, el tudnád küldeni ezt és ezt a fájlt a freemail-es címemre? Ma délig le kell adnom egy jelentést és ezek nélkül nem tudom befejezni!”
- Ezután következhet a negyedik fázis, amikor is a megszerzett információt felhasználják az eredeti céloknak megfelelően: például a konkurenciának adják a megszerzett stratégiai tervet, ügyféllistát, vagy egy social engineering-támadás során kicsalt jelszóval hozzáférnek a vállalati rendszerhez.

Auditok tapasztalatai alapján hatásos, amikor szakdolgozatot író egyetemistának adja ki magát, a támadó, mert legtöbb esetben talál olyan közép- vagy felsővezetőt, aki néhány célirányos kérdésnek köszönhetően (például egy általa tartott előadásra hivatkozva) szívesen segít a „diplomamunka elkészítésében”. De ugyanez a szituáció elképzelhető egy újságíró, riporter vagy piackutató bőrébe bújva is. Így elsősorban az épületekbe, irodákba való bejutás a cél.

A védekezés nem könnyű, meg kell húzni ugyanis a határt az egészséges bizalmatlanság és a pozitív emberi tulajdonságok megőrzése között. „Az igazság az, hogy nincs olyan technológia a világon, amely megakadályozhatja a social engineering-támadást” – mondta Kevin Mitnick, a legendás hacker. Elcsépeltnek hangzik, de ettől még igaz: a dolgozók biztonságtudatosságát kell erősíteni, ismertetni kell velük az ilyen támadási formákat. Különösen jó módszer, ha a cégvezetés social engineering auditot rendel, majd a végrehajtott – és többnyire sikeres – támadásokat példaként véve, egy biztonságtudatossági oktatás keretein belül bemutatják a dolgozóknak, hogy milyen veszélyek leselkednek rájuk, és hogyan lehet elkerülni, hogy a későbbiekben hasonló támadások áldozatává váljanak. A tapasztalatok szerint így könnyebben elfogadják a kockázatokat csökkentő szabályzatok létjogosultságát, és talán jobban be is tartják azokat.

Van néhány jó óvintézkedés, amit mindenképpen célszerű betartani a mindennapokban is. Ha ismeretlen kolléga (vagy magát kollégának mondó személy) kér valami szokatlant, akkor meg kell próbálni megbizonyosodni a hívó fél kilétéről (például megkérdezni, pontosan mely részlegen, ki a felettese), vagy visszahívni az általunk ismert belső telefonszámán, esetleg rákérdezni a kérése valódiságára a felettesénél, vagy a hívó fél által hivatkozott személynél.

Online támadások

A Symantec „Norton Cybercrime Report 2011”[16] kutatása szerint, amelyet 24 országban mintegy 12 ezer felnőtt és 5000 gyerek bevonásával végeztek, az internetes bűnözés az elmúlt évben 388 Mrd USD kárt okozott, ez az összeg megközelíti a világ teljes kábítószer kereskedelmének éves forgalmi becslését (411 Mrd USD)., az UNICEF teljes éves költségvetésének mintegy 100-szorosa.

431 millió fő válik áldozattá évente, ez másodpercenként 14 főt jelent. A felnőttek 69%-át érte már valamilyen incidens, ez a fejlődő országokban 80%-ot, a fejlettekben 65%-ot tett ki. Természetesen minél több időt tölt valaki online, annál nagyobb az áldozattá válás valószínűsége. A fiatal férfiak 75%-a volt már áldozat, az idősebbek és a nők körében ez csak 60-65%.

16 Symantec: Norton Cybercrime Report 2011, 2012.01.13.

Az internet használat csökkentése nem opció a védekezési stratégiák között, a válaszadók ¼-e azt nyilatkozta, hogy már élni sem tudna internet nélkül, 41%-uk tekinti a netet a mindennapok szerves részének. 32%-uk szerint pedig társas kapcsolataik sínylenék meg súlyosan a közösségi hálózatokról való leszakadást.

A leggyakoribb támadások a vírusok és egyéb rosszindulatú programok (58%), az online csalások a másodikak (11%), az adathalászat a harmadik (10%) és 2011-ben először, negyedikként, felkerültek a listára a mobiltelefon alapú támadások szintén 10%-kal. (pl. SMS-alapú adathalászat)

Az áldozatok 40%-a nem is a pénzét, hanem az idejét sajnálja jobban, átlagosan 10 napot (4-16 nap közötti értékek) töltöttek egy-egy támadás következményeinek elhárításával. A költségek megoszlását az alábbi ábra szemlélteti:

Ennek ellenére csak a felnőttek mintegy 41%-a rendelkezik rendszeresen frissített biztonsági szoftvermegoldással otthoni számítógépén, ez az előző év adataihoz képest 9%-os visszaesést jelent. Mobil területen még ennél is rosszabb a helyzet, mindössze a készülékek 16%-án fut valamiféle védelmi megoldás, eszközlopás esetén történő adattörlő alkalmazást pedig csak a felhasználók 13%-a használ.

Az esély, hogy egy átlagos internethasználó felnőtt internetes támadás áldozatává váljon számítások szerint 1:2,27, tehát nagyjából 44%. Érdekes adalék, hogy a statisztikák szerint, aki online áldozattá válik, az kétszer nagyobb valószínűséggel válik bűncselekmény áldozatává a való világban is, mint azok, akik online nem „égették meg magukat". Azon interjúalanyok kétharmada, akik már mindkét világban szenvedtek el támadást, azt nyilatkozták, hogy az online cselekmények miatt legalább olyan dühösek és/vagy szomorúak voltak, mint a való világban történt áldozattá válás során, ám az online esetben úgy érezték nincs kihez fordulni, nincs egy olyan intézményrendszer, ami megvédené őket.

A felnőttek 35%-a érzi csak magát teljesen biztonságban a neten, ez 2010-óta 4%-os csökkenést jelent.

Kockázati források:

- A legnagyobb kockázati faktorok a felnőtt tartalmat tartalmazó oldalak, az ilyeneket nézegetők 80%-át érte már támadás.
- A harmadik helyezett a szabad WIFI-hálózatok használata, ez esetben az arány 77%-os volt.
- A második hely érdekes megközelítést tartalmaz: azon felnőttek 78%-a, akik rendszeresen hazudnak személyes adataikról online környezetben, valótlan avatárok mögött tevékenykedve, áldozattá vált. Az ilyen felhasználók nyilván gyakrabban járnak „görbe utakon", ahol a kockázat is nagyobb. Arra a kérdésre, hogy miért kell valótlan színben feltüntetni magukat, különböző válaszok születtek:
  - Sokan mondták, hogy csak a móka kedvéért (19%),
  - mások a kényes helyzeteket akarják így elkerülni (18%),
  - megint mások csak egyszerűen jobb színben akarnak feltűnni. (14%)
- Az online szerencsejáték és a társkereső oldalak szintén a fő kockázati források között találhatók.

A családok védelme

A családok, azon belül főleg a gyerekek és a fiatalok, eredendő bizalmukkal sokkal érzékenyebbek lehetnek a social engineering típusú támadásokra. A Symantec minden évben vizsgálja a veszélyeket, amelyen az internetről, különösen a közösségi hálózatokról fenyegetik a fiatalokat. Ezt az éves „Online family report”[17] című kiadvány foglalja össze, amelyet 24 országban – köztük Magyarországon is – 10 ezer interjú (szülők, gyerekek, pedagógusok) alapján állítanak össze évről évre.

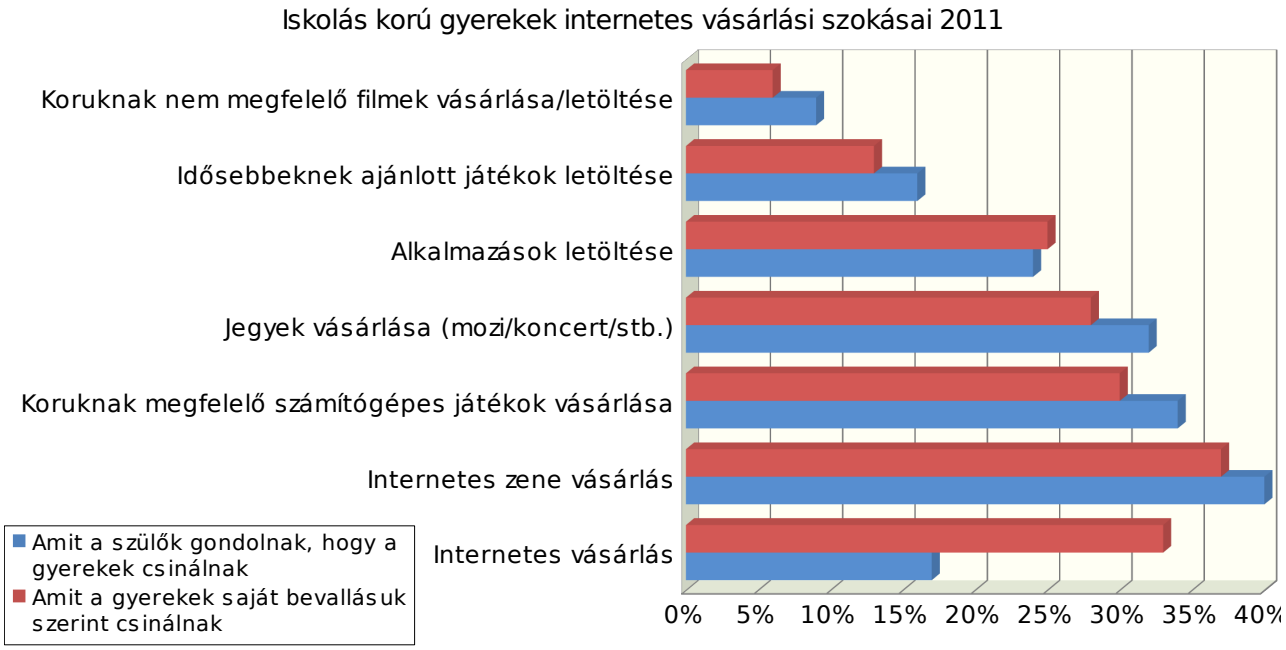
A közösségi hálózatok kiterjedt használata, a digitális világba való belenövés számos problémát, deviáns viselkedési formát idéz elő.

A egyik ilyen új fejlemény a kutatók által kiber-léprecsalás (cyberbaiting) névre keresztelt jelenség, amikor a diákok tanáraikat szándékosan kellemetlen, megalázó helyzetbe hozzák, amit mobiltelefonnal rögzítenek és azonnal meg is osztanak a közösségi oldalakon. A tanárok 21%-a tapasztalt már ilyet személyesen.

A tanárok 34%-a „barátja/ismerőse” a közösségi oldalakon diákjainak, ám 67%-uk szerint ez kockázatokat jelent a számukra. Az iskolák 51%-a semmilyen módon nem szabályozza a tanárok és diákok közösségi oldalakon történő kommunikációját, az iskolák negyedének egyáltalán semmilyen informatikai biztonsági szabályzata nincsen. A gyerekek 44%-a gondolja úgy, hogy az iskolában nem oktatják megfelelően az online biztonságot, ezzel a szülők 70%-a és a tanárok 80%-a is egyet ért.

Mindazonáltal a tanárok megkísérlik felhasználni a közösségi oldalakat, a diákok saját közegükben való elérésére, így teremtve szorosabb kapcsolatot a szükséges bizalom, motiváció, inspiráció megteremtéséhez. Ebben viszont segítségre van szükségük, hiszen ők maguk is, bár használják az online eszközöket, nagyon sok esetben digitálisan funkcionális analfabétának számítanak, tehát nem értik pontosan a rendszer működését, ezáltal pedig sokkal sebezhetőbbé válnak.

A kutatások szerint a gyerekek, mint hozzáértők, egyre szabadabban vásárolnak a neten szüleik hitelkártyáját használva. 1/3-uk teszi ezt világszerte, egynegyedük szülői engedély nélkül. A szülők mintegy 46%-a nyilatkozta, hogy valaha engedte már a gyerekét a kártyájával vásárolni a neten, 30%-uk szerint előfordult már az engedély nélküli vásárlás, 23%-uk szerint pedig a túlköltés (az engedélyezettnél nagyobb összeg felhasználása).



17 Symantec: Norton Online Family Report 2011, 2012.01.13.

Azonban nem csak negatív tapasztalatok vannak: a tudatos szülői magatartás, a megfelelően lefektetett és következetesen betartatott digitális szabályok, házirendek képesek megvédeni a fiatalokat a negatív élmények, tapasztalatok legnagyobb részétől. 82%-uk gazdagodott valamilyen negatív élménnyel, ha megszegték a szabályokat.

A biztonságtudatosság a szülők részéről folyamatosan javul az előző évekhez képest, már csak 6%-uk mondja azt, hogy fogalma sincs, hogy mit csinál a gyereke az interneten. Ez a biztonságérzet viszont némiképpen hamis, hiszen a gyerekek 17%-a (3×) szerint a szüleinek fogalma sincs, mit csinál az interneten. A szülők negyede gyanítja, hogy a gyerek markánsan másképp viselkedik a hálózaton, amikor együtt vannak a gép előtt, illetve figyelik őket, a gyerekek szerint ez 40%-ban van így. 12% kifejezetten bevallotta, hogy ha a szülők nincsenek a közelben, szánt szándékkal a tiltott tartalmak felé fordul.

Érdekes, hogy a szülők, akiknek a gyereke valamilyen negativitást tapasztalt már az interneten, 90%-ban maguk is voltak már internetes bűncselekmények áldozatai, vagyis a nem megfelelő biztonságtudatosság nagyban újra termeli önmagát. Valamint a bűnözők is gyakran kihasználják a gyerekek hiszékenységét, a valódi célpont pedig a szülő pénztárcája.

A gyerekek 62%-ának volt már valamilyen negatív tapasztalata az interneten, ebből 39%-uknak volt a lelki fejlődésükre súlyosan ható élménye. Mobilon keresztül pedig 13%-uk tapasztalt ilyesmit.

A leggyakoribb problémák:

- Ismeretlen próbál közelebbi kapcsolatot kialakítani a közösségi hálózatokon keresztül: 29%
- Erőszakos vagy pornográf képek, videók, játékok akaratlan megtekintése 28%
- Vírus letöltése a család számítógépére: 25%

Szerencsére ezek az értékek 2010 óta enyhe csökkenést mutatnak.

A szülők mintegy 45%-a fél attól, hogy gyerekük túl sok személyes, bizalmas információt adhat ki magáról, illetve a családról nem megfelelő személyeknek.

Természetesen a neten eltöltött idő és a veszélyekkel való találkozás valószínűsége szorosan összefügg:

Online eltöltött idő hetente	Negatív hatások bekövetkezése
49 óra +	88%
25-48 óra	76%
1-24 óra	60%

Kitekintés 2012-re

Az IT-iparág átalakulása

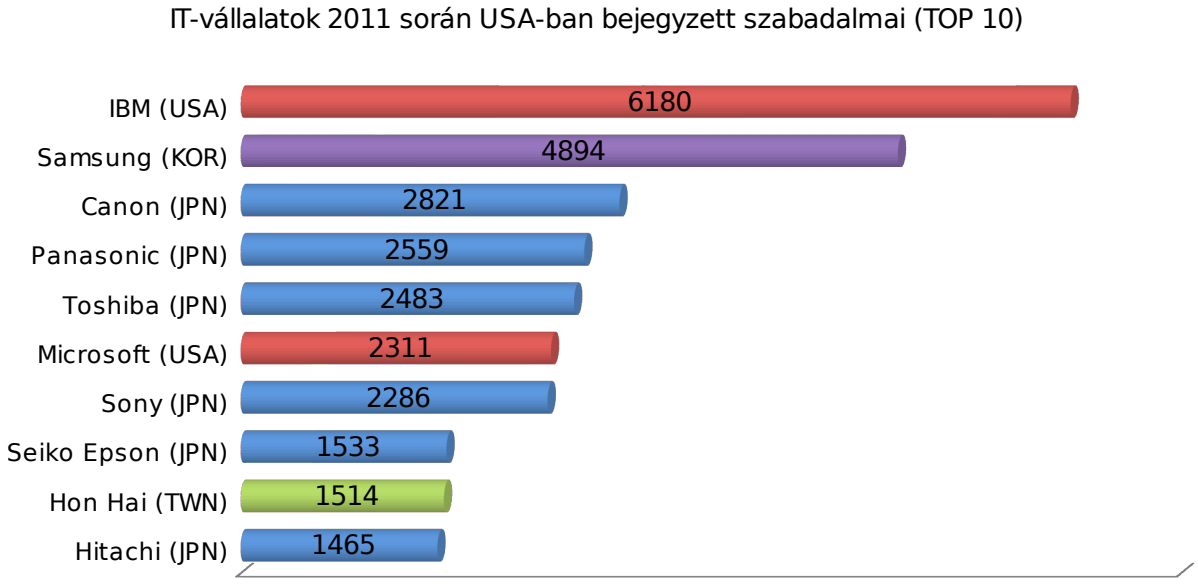
Már 2011-ben is az egyre intelligensebb mobil eszközök térnyerése jelentette az egyik legfőbb trendet az ICT területen és az egyik legfőbb kihívást az informatikai biztonság számára. Mind a lakossági, mind a vállalati szektorban megfigyelhető volt a mobilitás előretörése, ám a notebook forradalma után ez már az okostelefonok és a tabletek forradalma volt. Még a kormányzati informatika sem vonhatja ki magát a trend alól, ha lassabban is, de a mobileszközök itt is terjednek, sőt egyre többször kapnak stratégiai szerepet az oktatásban, az egészségügyben, vagy éppen az állampolgári ügyek intézésében.

A különböző kutatások és előrejelzések[18] [19] [20] [21] a következő képet festik számunkra 2012-ről:

- A világ IT-kiadásai várhatóan mintegy 7%-kal fognak emelkedni, ennek a jelentős bővülésnek a mobil eszközök és a feltörekvő piacok lesznek a motorjai.
    - Az okostelefon és tablet iparág körülbelül 2,5%-ot tesz ki ebből az értékből
    - A maradék 4,5% lesz ténylegesen az IT iparág növekedése, ennek motorjai a mobil hálózat fejlesztés, a felhő alapú technológiák, a közösségi informatika és a „big data” (extrém méretű adatbázisok kezelése) lesznek. Jelenleg az iparág ezeket nevezi a „harmadik platform”-nak, és bár az ezekre költött pénz még csak 20%-át teszi ki a teljes IT-költségvetésnek, 2020-ra a kutatók szerint a „harmadik platform” használhatja fel az erőforrások 80%-át.
    - Várhatóan a szoftver és implementációs szolgáltatások kereslet is erőteljes növekedésnek indul, ennek motorja főként Ázsia és az Egyesült Államok lesz. A kutatók az idei 2,4%-os bővüléssel szemben 6-7%-os növekedést jeleznek előre.
    - 2011 jól megmutatta azt is, mennyire sérülékeny ez a növekedés. A thaiföldi áradások katasztrofális hatása a merevlemez-iparra és ezáltal a teljes hardver forgalomra bizonyította, hogy az emelkedő trendeket bármikor, könnyen megtörheti egy vis major esemény. Ez az iparág már így is túlzott, de még inkább növekvő koncentrációjának eredménye, amely a méretgazdaságossági előnyökért cserébe feláldozza a biztonságot.
- Mint már fentebb is látható volt, a fejlődő piacok lesznek a növekedés motorjai a következő évben.
    - Kína 2012-re a világ második legnagyobb ICT-piaca lesz. Növekedése a 4,5%-os világátlaghoz képest több mint háromszoros, 14% körül várható.
    - A fejlődő országok már 28%-kal részesülnek a világ teljes IT-költségvetéséből, szemben az öt évvel ezelőtti 21%-kal. A növekedésnek pedig több mint felét ezek a régiók adják majd.
    - A fejlődő országok kereslete természetesen a kínálatot is növelni fogja ezeken a területeken. Az alacsonyabb árakon dolgozó helyi fejlesztők és szolgáltatók komoly konkurenciát jelentenek a nemzetközi IT-iparnak ezekben a régiókban. A hagyományos szállítók ezeken a piacokon csak megkülönböztetett stratégiával, különösen a költségek erőteljes visszafogásával és az igényeknek megfelelően leegyszerűsített megoldásokkal tudnak versenyben maradni.

18 Gens, Frank: IDC Predictions 2012: Competing for 2020, IDC 2011. december,
19 Ponemon Institute LLC: Second Annual Benchmark Study on Patient Privacy & Data Security, 2011. dec.
20 Ponemon Institute LLC: Second Annual Cost of Cyber Crime Study Benchmark Study of U.S. Companies, 2011 augusztus,
21 Ponemon Institute LLC - Symantec: Global costs of data breach, 2011. május

- Ázsia előretörését az alábbi ábra[22] is jól szemlélteti, eszerint már nem csak a gyártásban, de a K+F-ben is komolyan számolni kell a régióval. A TOP 10-ben 8, a TOP 50-ben pedig 25 ázsiai vállalat található. A nagyszámú szabadalom bejegyzés másik oka a töretlen fejlődésen kívül, az egyre gyakoribb jogi támadások az iparágon belül. (2011 hangos volt például az Apple és a Samsung közötti pertől.)



- A mobil eszközök és alkalmazások előretörése megállíthatatlan, alapvetően fogják átrendezni a világ IT-iparát a következő évek során.
  - Várhatóan mintegy 900 millió okos mobileszköz talál gazdára 2012-ben, szemben a 400 milliós PC (desktop+notebook) eladással. Az év során nem csak számban, de értékben is meg fogja haladni a mobil eszközök kereskedelme a PC-két (277 Mrd USD szemben a 257 Mrd USD-vel), 23%-os növekedése pedig mintegy ötszöröse a PC-ágazaténak. Bár a teljes IT-költségvetésnek csak 15%-a fog mobil eszközökre fordítódni, a növekedés 45%-át már ezek generálják a következő év során.
  - A mobil operációs rendszerek csatája is folytatódik, a döntő tényező az applikációk száma, illetve az appstore-ok minősége lesz. Az Android és az Apple ebben nagyon erős, ehhez kell felnőni a többieknek (Microsoft, RIM, stb.) Körülbelül 85 millió app letöltés várható 2012-ben, mintegy 38 Mrd USD értékben. (Ez mintegy háromszorosa a szerverek várható piacának.) Ha a Microsoft nem tud felnőni a feladathoz, várható a további piacvesztés, hiszen a mobil operációs rendszerek már a szórakoztató elektronikai berendezéseken is hódítanak, így egyre közelednek a PC-piac felé.
  - A mobil eszközök erőteljesen hatnak az internet-technológiára is, a HTML5 előretörése ennek tudható be.
  - Az app-ek egyre erőteljesebben lesznek jelen a (nagy)vállalati környezetben is, teljes integrációt biztosítva az okos eszközök és a
    - közösségi szolgáltatások (Facebook, Twitter, Forsquare, stb.),
    - adattárházak (Omniture, Flurry, Appcelerator, stb.),
    - számítási és tárolási felhők (Amazon Web Services, Windows Azure, Force.com, stb.),

22 BitPort: Nagy szám! Most is az IBM volt a szabadalmak királya, 2012.01.13.

- e-kereskedelem (PayPal, Amazon, Google, stb.)és a
- vállalati információ-rendszerek (Microsoft, SAP, Oracle, stb.) között.

- A felhő alapú technológiák jelentik a másik nagy előrelépést a hagyományos IT-hez képest. A vállalatok egyre inkább platformokban és alkalmazásokban gondolkodnak, mintsem infrastruktúra építésben.
  - A felhő üzletág mintegy 28%-kal fog növekedni, ami az iparági átlag négyszerese. 36 Mrd USD értékben költenek erre a vállalatok.
  - Az app alapú (PaaS) és az infrastruktúra alapú (IaaS) IT küzdelme folytatódni fog, egyre több komoly szereplő érdekelt mindkét üzletágban és az erőforrásokat fokozatosan csoportosítják át a felhő irányába (IBM, Microsoft, Oracle)
  - Az új alkalmazások 80%-a már a felhőn keresztül kerül majd értékesítésre, illetve felhasználásra 2012-ben.
  - Várhatóan megkezdődik a nagyvállalati információs rendszerek felhőbe költöztetése. Körülbelül az alkalmazások 2,5%-a fog nyilvános felhőkbe (pl. Amazon AWS, IBM SmartCloud Enterprise+, Fujitsu Global Cloud Platform, Microsoft Azure, and the Rackspace Cloud) költözni, ez a 2011-es 0,6%-hoz képest négyszeres növekedés. Eddig a felhő alapú technológiák fő vásárlói a B2C vállalatok voltak, a következő év a B2B éve lesz, olyan kampányok fémjelzik, mint az „SAP runs on AWS”, vagyis a mainstream vállalatirányítási rendszerek elkezdtek erőteljesen a felhő felé mozogni.
  - A kutató és IT-szolgáltató cégek is egyre nagyobb hangsúlyt helyeznek a felhőhöz kötődő fejlesztések, szolgáltatások növelésére, így a folyamat várhatóan egyre gyorsulni fog.
- A felhő elkezdi majd kiváltani a fizikai infrastruktúrát is
  - Egyre nagyobb a törekvés a nagy adattárolási és számítási kapacitást igénylő feladatok teljes felhőbe költöztetésére, ami megfelelő erősségű hálózati kapcsolat esetén feleslegessé teheti a helyhez kötötten kiépített infrastruktúrát, valamint gyökeresen megváltoztathatja az üzleti modelleket (nagy beruházások helyett használat alapú költségek). Ez a terület várhatóan 1/3-ával fog növekedni 2012 során.
  - A felhőkhöz kötődő rendszermenedzsment megoldások és szaktudás ezáltal nagyon felértékelődik, a terület 109%-kal nőtt 2010 és 91%-kal 2011 során, de bőven maradt még benne növekedési potenciál.
  - Megkezdődhet a nagy adatközpontok felhőbe költöztetése, a nagyobb adatbáziskezelők már most képesek a részben vagy egészben felhőben tárolt adatok menedzsmentjére.
- A telekommunikációs és hálózati szolgáltatók piacán is komoly átrendeződés várható, 2012-ben a mobilkommunikációra költött összeg meg fogja haladni a fix hálózati szolgáltatások részesedését a költségvetésből. Várhatóan 300 Mrd USD körülire fog növekedni, szemben a vezetékes szolgáltatások 290 Mrd USD-jával.
  - A koncentráció és konszolidáció tovább fog erősödni a mobil piacokon.
  - Várhatóan megjelennek a nyugati piacokon az ázsiai szolgáltatók (pl. China Telecom) felborítva az eddigi status quo-t.
- Az extrém méretű adatkezelési szektor („Big Data”) is erőteljesen növekedni fog, valamint komoly piaci koncentráció, felvásárlások várhatók, és így még nagyobb méreteket fognak ölteni ezek a rendszerek. Ennek jó piacot teremt, hogy a digitális tartalom teljes mennyisége

várhatóan mintegy 50%-kal növekedve el fogja érni a 2,7 ZB méretet 2012-re, 2015-re pedig a 8 ZB-t. Ennek 90%-a strukturálatlan adat, amelynek elemzése és feldolgozása nagy kihívások elé állítja e rendszerek fejlesztőit.

  - Az adatmennyiség növekedése viszont messze megelőzi a memória méretek növekedését és áruk csökkenését, így az óriási adatmennyiség feldolgozása mind nehezebbé válik. A memória technológia fejlesztése így kulcsfontosságú stratégiai céllá válik az üzletág számára.
  - Az adatbázis-kezelők várhatóan egyre több beépített analitikai funkcióval fognak rendelkezni (riporting, scoring, stb.) mindezt azért, hogy kiküszöböljék a többrétegű architektúrából eredő teljesítményveszteséget.

- Várhatóan egyre jobban elmosódik a határ a közösségi informatika és a hagyományos IT szolgáltatók között. Az IT ipar közösséget épít, míg a Facebook és társai üzletiesednek.
  - Várhatóan a nagy szállítók is lehetőséget fognak látni a közösségi megoldások fejlesztésében, a csatlakozási pontok bekerülnek a vállalatirányítási és CRM-rendszerekbe.
  - Az Oracle, a Microsoft, az IBM mind ébredeznek és bármikor berobbanhatnak a közösségi üzletbe.
  - A Facebook pedig meglehetősen agresszíven mozog abba az irányba, hogy saját B2C kereskedelmi platformot nyitva kihívja a piacvezető eBay-t.
- Rohamosan terjed az NFC-technológia, fizetésben, személyazonosításban és vezérlésben egyértelműen az NFC éve lesz 2012. A kritikus tömeget várhatóan azonban csak 2015-re éri el a terület: ekkorra már mintegy 500 millió NFC-képes okostelefon lesz forgalomban, és így robbanhat az érintés alapú technológiák piaca.
- Előtérbe kerül az intelligens otthon – intelligens város koncepció
  - Az interaktív eszközök, háztartási berendezések és szolgáltatások összekapcsolódnak a közösségi médiával. Az intelligens otthonok és háztartási berendezések már a twitteren, vagy ehhez hasonló megoldásokon keresztül lesznek vezérelhetők.
  - Az intelligens városi és közszolgáltatási funkciók már a harmadik platform (intelligens mobileszközök) technológiáit fogják alkalmazni. Ez mintegy 40 Mrd USD-os piac lesz 2012-ben.
  - Az okos város és közszolgáltatási koncepció az energiahatékonyság javítását tűzi ki célul a szükséges energia folyamatos, igényekhez igazodó elosztásával. Az épületek, elektromos járművek, kommunikációra képes háztartási berendezések új kihívást jelentenek az energia felhasználásban.
  - Az egészségügy is egyre kiterjedtebb felhasználója az IT-megoldásoknak, mind az adatnyilvántartás, mind a kezelések és orvosi berendezések egyre intelligensebbé válása, a távfelügyeleti szolgáltatások terjedése, a távoli konzílium és tanácsadás lehetősége az intelligens város koncepciók fő kihívásai közé tartoznak.
  - A közlekedési szolgáltatások szervezése is nagyban épít az interaktív eszközökre és az NFC alkalmazására.
- A pénzügyi szolgáltatók egyre markánsabban jelen lesznek a közösségi médiában, de nem csak mint hirdetők, hanem a döntéshozatali folyamatokban is egyre inkább fel fogják használni a közösségi megoldások adatait. Az ügyfélminősítés mellett a személyre szabás, az árazás, a szolgáltatásfejlesztés is profitál a közösségi információkból.

- Az elektronikus kereskedelmi üzleti modellek fejlődése a hagyományos boltokat egyre inkább kiállítóterekké változtatja, hiszen a vevőnek csak azért van rájuk szüksége, hogy a – legolcsóbb áron történő – online megrendelés előtt, egyszer kézzelfoghatóan is kapcsolatba kerülhessen a termékkel.

Az IT-biztonság trendjei

A következő év, évek legfontosabb IT-biztonsági kihívásai egyenesen deriválhatók a fenti – az iparág irányvonalait bemutató – tendenciáiból.

Előrejelzések: PWC

A PriceWaterhouseCoopers kutatása[23] szerint világszerte közel 60 milliárd angol fontnak megfelelő összegre rúgott 2011 során az informatikai biztonsági cégek értéke. Köszönhető ez többek között az állami rendeleteknek is, amelyek előírják az egyes adatvédelmi szabályok betartását, ez pedig megmagyarázza az internetes kártevők, rendszerbeli sérülékenységek ellen küzdő szervezetek gyarapodását. Olyannyira érdekessé vált ezáltal a piaci szegmens, hogy a fejlett országokban szinte marakodnak az ilyen megbízások elnyeréséért.

Sajnos Magyarországon kevés átfogó statisztika áll rendelkezésre, de egy, az USA-ban végzett kutatás kimutatta, hogy az informatikai támadások okozta károk incidensenkénti medián értéke 2011 során 6 millió USD volt, ami szélsőséges esetben a 40 millió USD-t is elérhette. Ez az előző évhez képes 56%-os emelkedést jelentett. Mintegy 72 sikeres támadást regisztráltak hetente, ez 44%-os növekedést jelent.

A legfőbb károkozók a rosszindulatú kódok bejuttatása, a DoS-támadások, az eszközlopásból eredő adatszivárgások és a távoli elérést használó WEB-ről érkező támadások voltak.

Egy támadás teljes elhárítása átlagosan mintegy 18 napot és majdnem fél millió dollárt vett igénybe, szemben az előző év 14 napos átlagával. A belső ember által segített támadások esetén a teljes helyreállítás akár 45 napot is igénybe vehetett.

Előrejelzések: McAfee

A McAfee kutatói[24] szerint 2012-ben az idén feltűnt fenyegetések lesznek az elektronikus bűnözés főszereplői, valamint várható, hogy szaporodni fognak a politikai motivációjú és az ismert személyeket érő támadások, nem lesz ritka az ipari célú támadás, de a kiberháborús demonstráció sem.

Legitim SPAM

Bár az elmúlt két évben csökkent a globális spammennyiség, de a legitim hirdetők ott, és ugyanazokkal a technikákkal folytatják, ahol a spamküldők abbahagyták, azaz email címlistákat vásárolnak olyan felhasználói címekkel, akik „beleegyeztek” a reklámok fogadásába, vagy megszűnő vállalkozások ügyfél adatbázisait használják fel. Az ilyen „legális” és úgynevezett „snowshoe” spam gyorsabb elszaporodása tapasztalható, mint például az illegális adathalászat vagy bizalmi csalások esetében.

23 PriceWaterhouseCoopers: 2012 Global State of Information Security Survey, 2012.01.15.
24 McAfee Labs: 2012 Threats predictions, 2012.01.10.

Virtuális tárcák

Mára a virtuális fizetőeszközök népszerű online fizetési módszerré váltak. Ezek az online „pénztárcák” nem kódoltak, és a tranzakciók is publikusak, ami a bűnözők szemében vonzó célponttá teszi őket. A virtuális fizetőeszközöket célzó jövőbeli támadásoknak része lesz az összes eszköz, így a spam, az adatlopás, a bűnözők komplett kisegítő rendszereket és szolgáltatásokat fognak ezek kihasználására dedikálni, hogy adatot és pénzt lophassanak a gyanútlan felhasználóktól.

Mobil eszközök

Az idei az eddigi legtöbb mobileszközöket célzó malware éve volt. A kutatók szerint a támadók jövőre továbbfejlesztik képességeiket, és a mobil banki szolgáltatások felé fordulnak. Az eddigiekben az online bankok ellen alkalmazott módszerek, mint a pillanatnyilag online lévő ügyfelek meglopása (így legitim tranzakciónak álcázva a lopást) ezentúl a mobil banki szolgáltatásokat is fenyegetik. Várható, hogy a támadók a PC-ket megkerülve egyenesen a mobil banki applikációkat fogják támadni, mert egyre többen intézik pénzügyeiket mobileszközökről.

Beágyazott rendszerek

A beágyazott rendszereket egy nagyobb rendszeren belüli specifikus funkció elvégzésére tervezték, és gyakoriak az autóiparban, az orvosi műszerekben, a GPS készülékekben, routerekben, digitális kamerákban és printerekben. Ezeket is egyre hatékonyabban lesznek képesek megtámadni a bűnözők. Ehhez a hardver réteget támadó kártékony kódokra lesz szükség, amely a támadónak lehetővé teszi az ellenőrzést és a hosszú távú hozzáférést a rendszerhez és adataihoz. A kifinomult támadók így teljesen átvehetik az irányítást a hardver felett.

Közmű-szolgáltatások

A víz, az áram, az olaj és a gáz alapvetőek a mindennapi életünkben, mégis számos ipari rendszer felkészületlen a támadásokkal szemben. Számos SCADA (ellenőrző irányítási és adatgyűjtő) rendszerrel működő környezetben hiányoznak a szigorú védelmi gyakorlatok, és amint azt a nemrégiben az USA-ban a vízművekre irányuló incidensek megmutatták, a támadók egyre gyakrabban és sikeresebben fogják kihasználni ezt a felkészületlenséget, például zsarolásra.

Virtuális politikai ellenállás

A „valódi” Anonymus csoport vagy újra feltalálja magát, vagy kihal. Emellett a digitális rendbontók és a tüntetők várhatóan összefognak majd, és közszereplőket, például politikusokat, ipari vezetőket, bírókat és rendfenntartókat fognak megcélozni eddig példátlan módon és gyakorisággal.

Kiber-hadviselés

Az országok sérülékenységének oka az, hogy egyrészt nagyban függenek számítógépes rendszereiktől, másrészt biztonsági rendszereik főleg kormányzati és katonai hálózatok védelmére fókuszálnak. Számos ország már felismerte a kritikus infrastruktúrákat, a víz, gáz, vagy energiahálózatokat fenyegető kibertámadásokban rejlő hatalmas potenciált, és azt is, hogy mennyire bonyolult védekezni ezek ellen. A szakértők szerint egyes országok, mintegy jelzésképpen, demonstrálni fogják cyberháborús képességeiket.

A felhő biztonsága

A felhasználók még mindig nem bíznak a felhőszolgáltatásokban[25], és ez a legnagyobb akadálya az elterjedésüknek. A legtöbben attól félnek, hogy a szolgáltató rendszerében valamilyen kártevő pusztít, illetve hackertámadásnak esik áldozatul, de nagyjából ugyanennyien vannak, akik a jogosulatlan hozzáféréstől, a titkosítatlan adateléréstől vagy éppen a véletlen adatszivárgástól félnek. Ugyanakkor a kutatások arra a paradox eredményre jutottak, hogy sokan pontosan azért akarnak ilyen szolgáltatásokat igénybe venni, mert így akarják javítani informatikai rendszereik és szolgáltatásaik biztonságát. Ezzel együtt nehezíti az ilyen szolgáltatások bevezetését, hogy az informatikai csapatoknak alig 20-25 %-a rendelkezik megfelelő tapasztalatokkal, mintegy felük pedig nem készült még fel kellőképpen a felhőre.

Mobil eszközök

2011 volt az első olyan év, amikor a mobiltelefonok elleni támadások igazi veszélyként jelentek meg a vállalatok és felhasználók számára[26] [27], és ez 2012-ben csak fokozódni fog, ahogy ezen eszközök egyre jobban elterjednek, mind több cég és magánszemély eszköztárában megjelenve.

Az „okos mobileszközök” használatának elterjedésével a készülékek egyre nagyobb kockázatnak vannak kitéve, különösen a mobilokat célzó rosszindulatú programok miatt, amelyek példátlan módon szaporodnak, így nőtt az adatvesztés veszélye is.

Az okostelefonok robbanásszerű terjedése a kiberbűnözők figyelmét is felkeltette, aminek eredményeként 2011-ben a mobil alapú kártevők aránya jelentősen megnőtt. Azoktól a kártevőktől kezdve, amelyek emelt díjas üzenetekkel bombáznak, egészen a rosszindulatú programokig, amelyek az információlopásra specializálódtak.

Jóllehet a felmérések szerint 2011 a külső támadások éve volt, a vezető informatikai biztonsági szakértők egyre nagyobb kockázatot látnak a belső dolgozókkal kapcsolatban. Az ok ismét a mobileszközök elterjedése, különösen a személyi mobileszközöké. A táblagépek elsősorban abból a szempontból jelentenek problémát, hogy az alkalmazottak a vállalati infrastruktúrában is használni kezdték az eszközöket gyors ütemben. Ez pedig meghaladja a szervezetek azon képességét, hogy biztosítsák és menedzseljék az eszközöket, továbbá, hogy megvédjék azokat a bizalmas információkat, amelyekhez a munkatársak hozzáférhetnek a táblagépeken keresztül.

A fő veszélyforrássá, így azok az alkalmazottak váltak, akik táblagépeikkel megkerülve a szervezet normál biztonsági protokolljait hozzáférnek a cég hálózatához és érzékeny adatokat érhetnek el. Abban az esetben pedig, ha az elkövető rosszindulatú, szigorúan bizalmas szellemi tulajdont lophat el.

A Symantec elemzése szerint a célzott támadások leggyakoribb áldozatai a kis- és középvállalkozások, ezek ugyanis nincsenek felkészülve az ilyen jellegű fenyegetések elhárítására, miközben csak a felük gondolja úgy, hogy mivel ők kisebb cégek, nincsenek veszélyben. Ez azonban szöges ellentétben áll a tapasztalatokkal. A Symantec adatai szerint az év során az összes célzott támadás 40 %-a az 500 alkalmazottnál kevesebbet foglalkoztató vállalatokra irányult, szemben azzal a 28 %-kal, amelyek kifejezetten a nagyvállalatokat célozták.

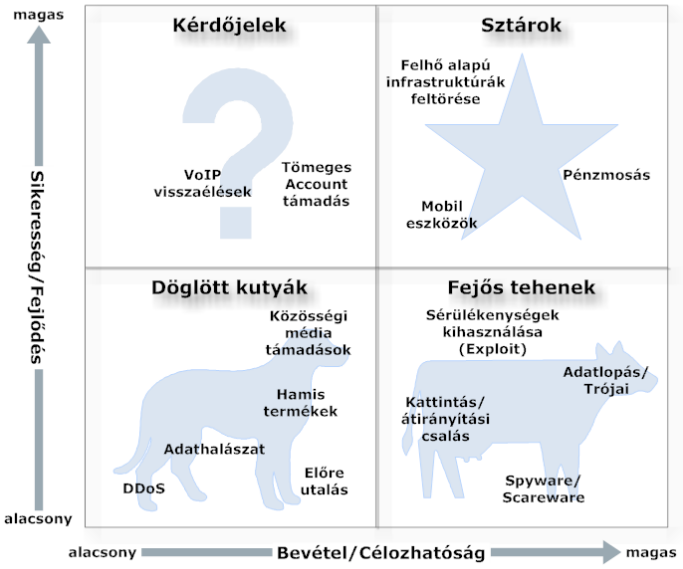
25 Schopp, Attila: Biztonság a felhőnek és a felhőből, ITBusiness, 2011.12.01.
26 Gens, Frank: IDC Predictions 2012: Competing for 2020, IDC 2011. december,
27 Schopp, Attila: Felméretlen kockázatok, ITBusiness, 2011.11.08.

Előrejelzések: Cisco

A Cisco 2011-es informatikai biztonsági jelentésében[28] beazonosította azokat a legfontosabb fenyegetéseket, amelyek 2011-során a legtöbb problémát okozták a piacon, valamint leírja a fenyegetések evolúcióját is.

A megállapításokat a BCG-mátrix mintájára készült alábbi ábra foglalja össze. Ebből is látható, hogy 2012-ben a biztonsági szakemberek számára a legfőbb kihívást 2011 „kérdőjelei és sztárjai" fogják jelenteni, ezek ellen új módszerek kidolgozására van szükség.

Cisco Kiber-bűnözési ROI-mátrix 2011



A BCG Mátrix sémát a Boston Consulting Group fejlesztette ki.

A „fejős tehenek" elleni küzdelem folytatódik, hiszen ezekkel a megoldásokkal a támadók kis befektetéssel komoly hasznot tudnak realizálni, tökéletes ellenszerüket pedig a mai napig nem sikerült megtalálni.

A „döglött kutyák" területe világosan mutatja azt a trendet, hogy a bűnözők mind professzionálisabbá válva egyre jobban a célzott támadások felé fordulnak, a nagy tömegű, alacsony hatékonyságú, bizonytalan bevételt eredményező cselekmények egyre inkább háttérbe szorulnak.

Biztonsági helyzet Magyarországon

Több mint száz szervezetre – köztük államigazgatási és önkormányzati szervezetekre, oktatási és egészségügyi intézményekre, pénzintézetekre és távközlési vállalatokra – kiterjedő felmérést végzett a BellResearch segítségével az ISACA magyar szervezete. A szervezetnek ez volt az első nagyszabású felmérése a magyar IT-biztonsági piacról.[29]

Az eredmények lesújtóak voltak, bár a kutatás során alapvetően olyan szervezeteket kérdeztek meg, amelyek sok ember érzékeny adataival dolgoznak, így különösen nagy gondot kellene fordítaniuk az információbiztonságra, a válaszokból viszont alapvető hiányosságokra derült fény. A felmérésben négy nagy témakörre összpontosítottak: információbiztonsági problémák és törekvések, biztonsági kockázatkezelés, audit, és végül a terület irányítási kérdései.

A válaszokból kiderült, hogy a megkérdezettek egyhatoda sem belső, sem külső informatikai auditot nem végez a szervezetnél. Több mint 60 százalékuk nem foglalkozik a kockázatok felmérésével, ami ebben a körben megengedhetetlenül magas arány.

Ennél is problémásabb, hogy nagyjából negyedük azt sem tudja (vagy nem akart válaszolni), hogy az elmúlt 12 hónap során volt-e náluk külső behatolás vagy éppen eszközlopás. Így viszont némi kétkedéssel kell fogadni azt az adatot is, amely szerint a szervezetek 18,4 %-ánál volt behatolási kísérlet és 27,2 %-ánál eszközlopás – könnyen lehet, hogy a valós számok ezeknél jóval magasabbak.

Arra viszont talán van esély, hogy a szervezetek tisztában vannak hiányosságaikkal. Erre utalhat, hogy a legfontosabb információbiztonsági törekvések között az első helyen az informatikai eszközök menedzsmentje szerepel, ezt követi a központi jogosultságkezelés, a katasztrófaelhárítási terv készítése, illetve az átfogó biztonsági szabályzat és eljárásrend készítése.

28 Cisco Systems: Cisco 2011 Annual Security Report, 2012. január 15.
29 Bellresearch: Magyar Infokommunikációs Jelentés 2011.

A személyazonosság ellenőrzésének jövője a billentyű leütések dinamikáján keresztül

Amikor valaki a biometriát említi, az első - és gyakran az egyetlen - dolog, ami sok embernek eszébe jut, azon fizikai jellemzők összessége, amelyek alapján az emberek egyértelműen megkülönböztethetőek: DNS, ujj és tenyér lenyomat, írisz, stb. Összességében azon fizikai jellemzők, amelyek felett nem rendelkezünk irányítással.

Amennyire hasznosak ezen jellemzők az ellenőrzéshez és azonosításhoz az életben, addig az online változat egy másik történet. Az ezen jellemzők azonosításra való felhasználásához készült technológia túl bonyolult és obstruktív az integráláshoz és a felhasználáshoz, valamint túl költséges.

Létezik a biometriának egy másik osztálya, ami hasznosnak bizonyulhat és könnyebben használható erre a célra - viselkedés biometria. A kifejezés egyértelmű: olyan biometriai jellemzőkről van szó, amelyek a személyek viselkedésével függnek össze.

Mindannyiunkra jellemző, ahogyan járunk, beszélünk, és ahogyan a számítógép billentyűzetén keresztül gépelünk (írunk). A gépelés egy olyan dolog, amit mindannyiunknak használnunk kell a számítógéppel és rajta keresztül másokkal, illetve szolgáltatásokkal történő kommunikációhoz. A gépelési stílusunk rögzítése és tárolása egyszerű és nem igényel speciális, drága eszközöket.

Nem csoda tehát, hogy számos cég kezdett olyan megoldások fejlesztésébe, amelyek a billentyű leütések dinamikáját használják a felhasználók ellenőrzésére és azonosítására, gyakran más hitelesítő tényezőkkel együtt.

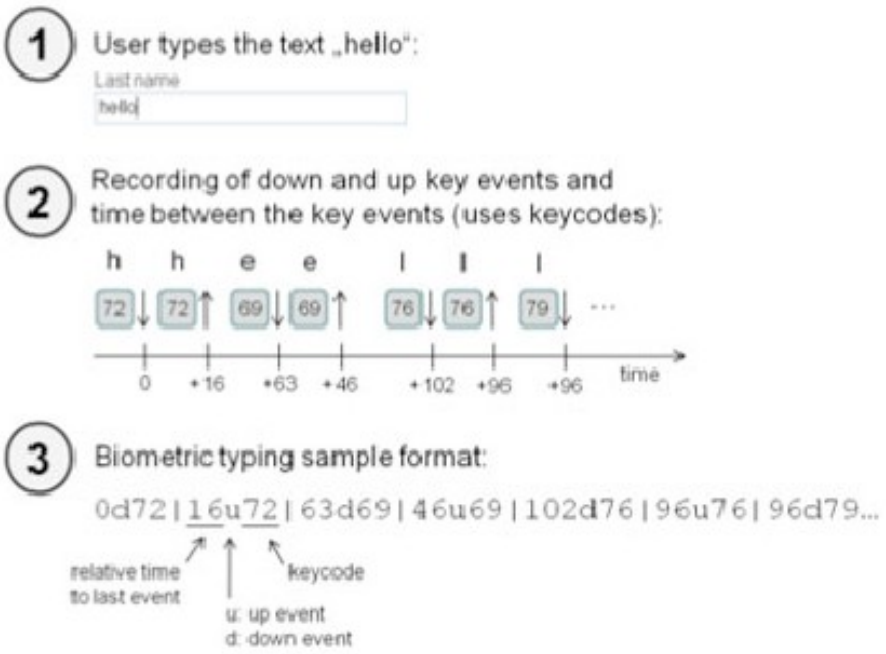
Jelenleg egyedül a TM3 Software nevű német cég az egyetlen, amely tetszőleges, a felhasználó által bevitt szöveggel működő megoldást tudott kifejleszteni. Ez azt jelenti, hogy a felhasználó munkamenetét nem kell megszakítani, sőt a felhasználó akár nincs is tudatában az azonosító és hitelesítő folyamatnak - tökéletes a csalási kísérletek megakadályozására.

A megoldás neve KeyTrac, és csak 4-5 hónapja érhető el nyilvánosan. A megoldás és maga a cég annak a munkának a közvetlen eredménye, amelyet Dr. Thomas Wölfl - CEO és cégalapító - és az ő fejlesztő és mesterséges intelligencia szakértő csapata végzett a regensburgi egyetemen.

Hogyan dolgozik a KeyTrac?

Mint minden biometrikus megoldásnál, az első lépés az adatgyűjtés, amit profilok létrehozásához használnak fel. A KeyTrac adatgyűjtő (recording) modulja integrálható egy létező űrlapba - legyen az egy regisztrációs űrlap, egy cím, banki adat, termékleírás vagy fórum hozzászólások bevitelére használatos űrlap -, vagy egy önálló alkalmazásba (e-mail programok, Office megoldások, stb.)

A modul a felhasználó gépelési módjának jellemzőit rögzíti és nem azt, amit gépel, és a begyűjtött információt biometrikus gépelési adattá alakítja.



A legjobb tulajdonsága, hogy a begyűjtött adat semmilyen személyes információt, illetve a felhasználóval kapcsolatban bármilyen következtetésre használható információt nem tartalmaz. A szöveg névtelenné válik gépelés közben és a gépelt szöveg sem a rendszer operátora sem pedig a KeyTrac által nem rekonstruálható.

Nem számít továbbá, hogy a felhasználó milyen nyelven gépel, csak az a fontos, hogy azt jól ismerje. Az sem számít, hogy milyen billentyűzetet használ, mivel minden billentyűnek van egy ún. „keycode"-ja, és a keycode maga is rögzítésre kerül, ezáltal bármely nemzeti billentyűzet használható.

Amint a billentyűleütésekkel begyűjtött adat a KeyTrac Core Engine-hez kerül, egy felhasználói profil készül belőle több kivont jellemző alapján, és egy adatbázisba kerül, ahonnan a későbbi azonosítási folyamat során felhasználásra kerül.

Az azonosítási folyamat akkor indul, amikor egy ismeretlen felhasználó egy űrlapon, vagy alkalmazásban adatot gépel. A billentyűleütési adat begyűjtésre majd átadásra kerül a KeyTrac Core Engine számára, amely a felhasználói profilokban tárolt adatokkal összeveti azt.

Amennyiben a cél annak ellenőrzése, hogy egy duplikált regisztrációról van-e szó - például, ha a felhasználó elfelejti a jelszavát és egy új hozzáférést szeretne létrehozni -, az adatot az adatbázisban tárolt összes profillal összehasonlítják. Amennyiben a cél egy lopott azonosítóval rendelkező betörő felderítése, akkor az adatot csak annak a felhasználónak a profiljával vetik össze, akinek az hozzáférési adatait a csaló használni akarja.

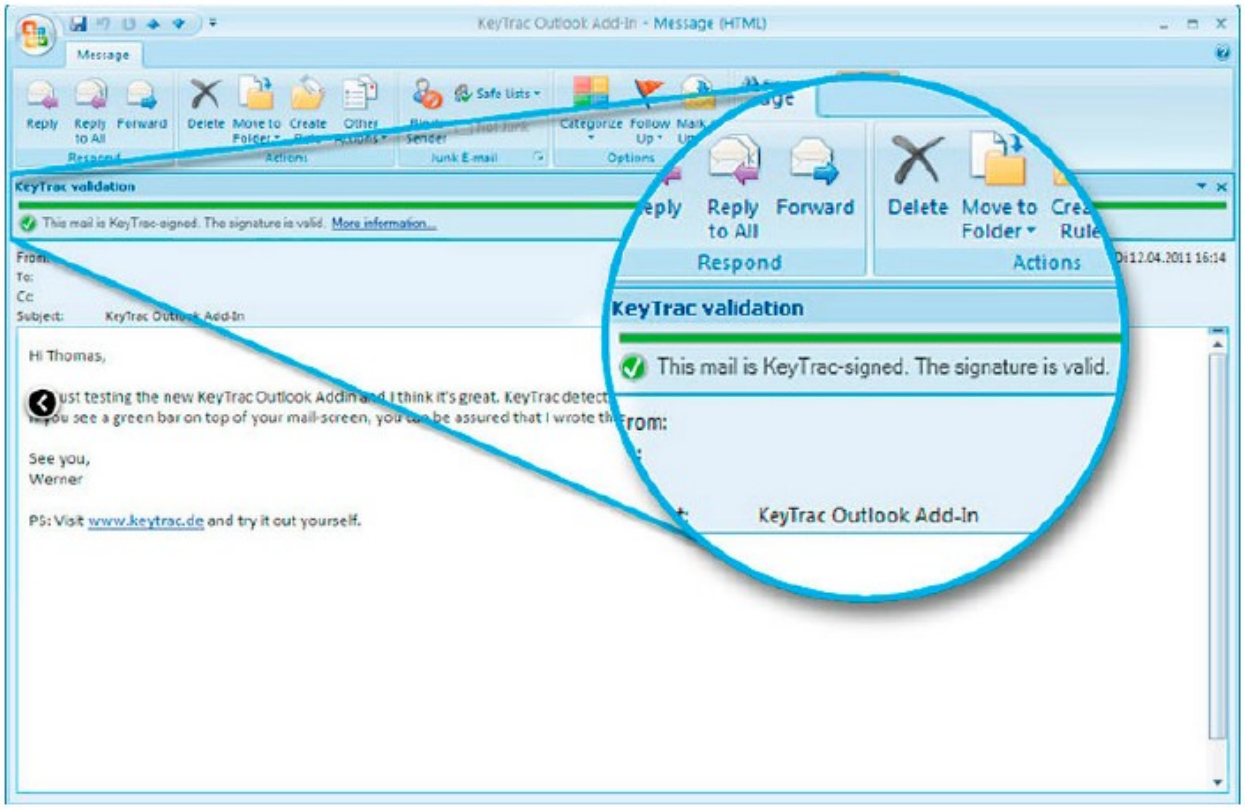
A KeyTrac által megvalósítható célok között szerepel az online csalások megakadályozása is. A csalók felismerhetők a gépelési mintájuk alapján, függetlenül attól, hogy egy ellopott bejelentkezési információt használnak, vagy új hozzáférést nyitottak hamis adatokkal.

Amennyiben felállítanak egy online csalókat és azok billentyűleütési mintáját tároló központi adatbázist, az adat összevethető ebben a speciális adatbázisban tárolt profilokkal pl. csaló tranzakciók inicializálásának megakadályozása érdekében.

Vannak más, a billentyű leütések dinamikáját használó megoldások is, de ami megkülönbözteti a KeyTrac-et más megoldásoktól, az az a tény, hogy a folyamat a felhasználó tudta nélkül végezhető vagy, hogy nem egy előre definiált szöveget kell begépelni.

„Minden más hagyományos billentyűhasználati biometrika csak a jelszavas védelem erősítéséhez vagy mindig ugyanazon, fix szöveg bevitelével történő hitelesítéshez használható," mutat rá Dr. Florian Dotzler a TM3 Software termék menedzsment vezetője. „A KeyTrac bármilyen bevitt szöveg alapján képes azonosítani a felhasználót". És ez az, ami tökéletessé teszi az elektronikus fizetéssel foglalkozó szolgáltatók, az online kereskedők és a bankok számára azt, hogy az online banki szolgáltatások biztonságosabbak legyenek.

A KeyTrac használható továbbá a feliratkozások (subscription) és felhasználói hozzáférések megosztásának megakadályozására - nagyon praktikus olyan szoftver készítők számára, akik „Software-as-a-service"-t szolgáltatnak vagy ún. „named user" licensz modellt használnak. Továbbá használható online tesztet kitöltők azonosságának ellenőrzésére, digitális dokumentum szerzőjének ellenőrzésére, vagy akár email-ek és digitális dokumentumok digitális aláírására.



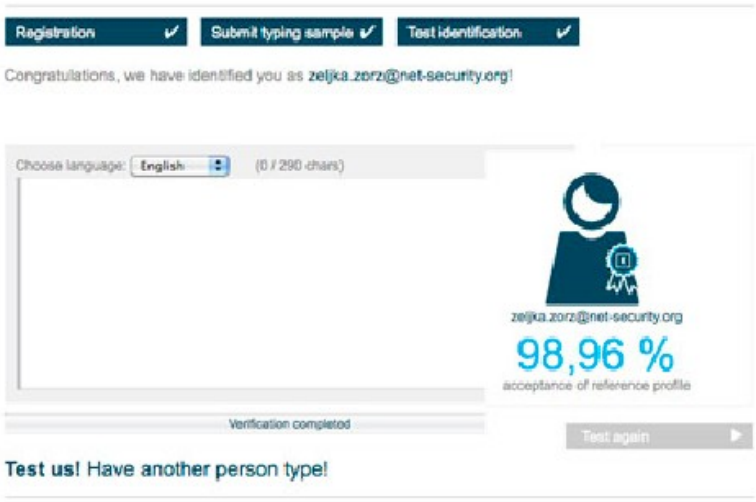
Mintha egy álom válna valóra. Tovább gondolva, a különböző KeyTrac megoldások integrációja egyszerű. „Csupán egy-két napot vesz igénybe web környezetekbe történő integrálása", magyarázza Dr. Dotzler. „Web-es környezetben csupán egy rövid Javascript-et kell tenni a web oldal fejlécébe (header) a gépelési minták rögzítése érdekében, és egy WAR-fájlt (KeyTrac core system)"

„Meglévő rendszerekbe (legacy systems) történő integrációja szintén csupán 2-3 napot igényel" teszi hozzá. „De ez függ a használati esettől".

Hatékony?

Amennyiben hitelesítésről van szó, a viselkedési metrikák általában kevésbé számítanak megbízhatónak, mint a fizikai biometrikák, mert más természetűek. A fizikai metrikák használata esetén egyértelmű válaszokat keresünk - sikerült, nem sikerült. A viselkedési biometrikák esetén inkább beszélünk statisztikákról és százalékokról.

Például, KeyTrac online demo tesztelése során, konzisztens módon azonosította a felhasználót, de sosem lehetett elérni a 100%-os elfogadottságot a referencia profil alapján.



Az gyakorlatilag lehetetlen ugyanazon személy számára is, hogy megismételje azt a mintát, amit eredetileg rögzítésre, és referenciaként tárolásra került. De a 98,96%-os valószínűség, miszerint a tesztelő az a személy, aki a referencia mintát készítette, és ez elég volt a rendszer számára, hogy „átengedje".

Nem lehet tudni, mi a beállított küszöbérték a demo verzióban, de látható volt, hogy mikor két másik felhasználót kértek fel, hogy gépeljenek valami szöveget, őket visszautasította a rendszer. És ugyanez történt, amikor az eredeti felhasználó megváltoztatta a gépelési mintáját, lelassítva, illetve rövid szünetet tartva egy szó betűi között.

A lényeg, hogy a billentyűleütések dinamikája valószínűleg nem elég pontos ahhoz, hogy egyedüli azonosító és hitelesítő módszerként használjuk, de más módszerekkel kombinálva a hiányzó összetevőt szolgáltathatja egy üzembiztos megoldáshoz.

Dr. Dotzler rámutat, hogy minden biometrikus rendszernek vannak „false positive" kimenetei, és bár ezek száma csökkenthető, de teljesen nem megszüntethető. A problémák számos módon megoldhatók a „use-case"-ektől függően.

A billentyűleütések dinamikája egy lényeges előnnyel rendelkezik más hitelesítő módszerekkel szemben: a billentyűleütések folyamatosan rögzíthetők, és ezzel detektálhatók olyan szituációk, amikor arra kényszerítenek valakit, hogy beírva a jelszót a szolgáltatásba történő bejelentkezéshez, ami után a felhasználót kényszerítő személy átveszi a billentyűzetet.

De mi a helyzet azzal a ténnyel, amikor a gépelési mód változik egy napon belül, érzelmi és fizikai állapot szerint?

„A rendszer mesterséges intelligencia algoritmusokkal dolgozik" magyarázza Dr. Dotzler. „Ezek az algoritmusok különböző jellemzőket (karakterisztikákat) tanulnak meg, amikor a felhasználó különböző billentyűzeteket használ. Ezen tanulási folyamat alatt a módszer minőségének csökkenésével lehet számolni."

De vannak módszerek a probléma megoldására. „A felhasználó számára lehet készíteni egy másik profilt (a másik billentyűzethez)” mondja. „Valamint, ha a felhasználó eltöri a kezét, a billentyűleütési dinamikája annyira megváltozik, hogy a rendszert újra kell tanítani. Kisebb sérülések nem okoznak problémát.”

Következtetés

Minden technológiának van gyenge pontja. Az RSA kompromittálódásáról szóló cikkek megmutatták, hogy még a bizonyított technológiák is, mint a SecurID tokenek, megkerülhetők, és felhasználhatók.

A mentett referencia minták, amik a KeyTrac működéséhez szükségesek, valahogyan ellophatóak,

de vajon felhasználhatók a gépelési minták újbóli megalkotására és sikeres támadások végrehajtására? Amennyiben a technológia maga hatékonynak bizonyul, és sokan fogják használni, nem lehet kétség a felől, hogy valaki megtalálja a módját, hogyan lehet ezt kijátszani.

Időközben, számos elektronikus fizető, és e-commerce szolgáltató használja a KeyTrac-et. Túl korai még megmondani, hogy ez-e a puzzle hiányzó darabkája, ami megoldja majd a digitális identitás ellenőrzést, de a lehetőségek igen ígéretesnek mutatkoznak.

Forrás: http://www.net-security.org/dl/insecure/INSECURE-Mag-31.pdf

A VirusBuster Kft. összefoglalója 2011. IT biztonsági trendjeiről

Merre haladt, milyen jelenségeket mutatott fel a nemrég lezárult esztendő folyamán az informatikai biztonság területe? Milyen új fenyegetésekkel kell számolnunk állami és szervezeti szinten, cégeknél, illetve az otthonokban?

Beszámolónkban ezekre a kérdésekre igyekszünk válaszolni, s igyekszünk rátapintani az ágazat trendvonalaira. Emellett – a VirusBuster Kft. víruslaboratóriumának észlelései alapján – áttekintést nyújtunk a 2011 leggyakoribb számítógépes károkozóiról, illetve azok legjelentősebb webes forrásairól is.

Az anyag elkészítéséhez felhasználtuk a Puskás Tivadar Közalapítványon belül működő CERT-Hungary Központ adatait, illetve a szerteágazó nemzetközi kapcsolataink révén begyűjtött információkat is. Bízunk benne, hogy összefoglalónkban mind a szervezeti, mind az egyéni felhasználók találnak számukra hasznos információt.

Túl az ötvenmillión

Dőlnek a számítógépes kártevők, az őket terjesztő spam. A tavalyi első negyedévben az ötvenmilliomodik kórokozó-mintát vehette nyilvántartásába a nemzetközileg ismert IT-biztonsági laboratórium, az AV-Test. A nevezetes szám egy PDF file-nak jutott, amely az Adobe Reader egy sérülékenységét kiaknázva próbálja megfertőzni a Windows gépeket. Ily módon a jubileumi szám nemcsak a kártevők valamikor elképzelhetetlen elszaporodásáról árulkodik, hanem arról is, hogy a számítógépes bűnözők fő célpontját már nem az operációs rendszerek vagy a böngészők, hanem a különböző cégektől származó alkalmazások jelentik.

Napjainkra a kiberbűnözés fontosabb tényezővé nőtte ki magát a világ gazdaságában, mint a kábítószer-kereskedelem. A marihuána-, a heroin- és a kokain-piacot összességében 388 milliárd dollárra becsülik. Ugyanakkor az informatikai támadások világszerte 114 milliárd dollár közvetlen kárt okoztak, amihez ha hozzávesszük a nyomozásra és helyreállításra fordított idő 274 milliárdra becsült értékét, összesen 391 milliárd dollárt kapunk. Becslések szerint minden másodpercben 14-en – napi több mint egymillióan – esnek valamilyen informatikai incidens áldozatául.

A gazdasági és politikai konfliktusok a kibertérbe is eszkalálódnak. Mind több országban lépked felfelé a kormányzati feladatok prioritási létráján az IT védelem. Mint egy szeptemberben tartott előadásában *Michael Chertoff,* az Egyesült Államok korábbi belbiztonsági minisztere kifejtette: a világháló előretörése „kétségtelenül növekvő kockázatot jelent". „Minél fejlettebb a technológia, annál inkább számíthatunk arra, hogy rendkívül veszedelmes behatolók látogatnak kiberterünkbe."

Nemcsak a nagyhatalmak vezetőit és szakértőit foglalkoztatják ilyen gondolatok. Hasonló problémákat feszegettek szeptember végén a budapesti Arena Plazában is, az immár hetedszer – és nagy sikerrel – megrendezett Informatikai Biztonság Napja (ITBN) egyes előadásain. Így nagy érdeklődés kísérte *Angyal Zoltánnak,* a Puskás Tivadar Közalapítvány hálózatbiztonsági igazgatójának, a CERT-Hungary Központ vezetőjének prezentációját. A szakember elmondta: 2010-ben szinte minden napra jutott hazánkban egy incidens. Hangsúlyozta: a biztonság területén a két legfontosabb feladat a kritikus információs infrastruktúra védelme és a nemzetközi kapcsolatok építése, illetve ápolása.

Kiemelkedő áldozatok

Hajlamosak lehetünk azt hinni, hogy a kártevők, a bűnözők igazából csak a hétköznapi átlagembert bosszantják és fosztogatják. Elvégre a nagy szervezetek és nemzetközileg ismert vezető személyiségek mögött óriási erőforrások állnak, így aztán – gondolhatnánk – őket online veszélyek biztosan nem fenyegetik.

Óriási tévedés. A tavalyi esztendő többszörösen felhívta a figyelmet arra: senki nincs biztonságban. Az adatbetörések minden fajtájára bőséggel láthattunk példát. Nem egy közülük messze túllépett a szaksajtó keretein, s bekerült a világlapok főcímei közé, sőt a tévéhíradókba is. Mikor pedig már azt hittük, hogy több ekkora botrány nem pattanhat ki – napokon belül a jött a következő.

Milyen mértékben sújtja a kiberbűnözés az egyes embert, a vállalatokat és magát az államot? Nos, némi támpontot kaphatunk az arányokat illetően *Jonathan Shaw* vezérőrnagytól, a brit védelmi minisztérium IT biztonsági programjának vezetőjétől. A tábornok október végén úgy nyilatkozott: míg a szigetország polgárainak zsebéből mintegy 3,1 milliárd font vándorolt a fekete bitvadászok kasszájába, a kormányzatot ért kárt 2,2 milliárd fontra becsülik. A cégek vesztesége 21 milliárd fontra rúg. Ez utóbbi összegből mintegy 7 milliárd fontot az ipari kémkedés számlájára írnak, s 1 milliárdot tesznek ki az ügyféladatok eltulajdonításának következményei. A hackerek leginkább a gyógyszergyárakat, a biotechnológiai, elektronikai, informatikai és vegyipari cégeket ostromolták.

A következőkben 2011 legjellegzetesebb, legnagyobb port kavart incidenseit villantjuk fel, cél- (avagy áldozati) csoportokra bontva.

Magán(?)személyek

Nem kisebb személyiség vált hackertámadás áldozatává tavaly, mint a francia elnök. Facebook lapjára a betörők helyesírási hibákkal tűzdelt üzenetet plántáltak, amely szerint *Nicolas Sarkozy* az „ország előtt álló rendkívüli körülmények miatt" úgy döntött: nem áll rajthoz az idei választáson. A szövegben egy másik Facebook lapra mutató link is volt, mely utóbbi oldal a *„Búcsú Nicolas Sarkozytól"* címet viselte.

Ennél is pikánsabb, hogy saját közösségi portálján lett hackerek áldozata *Mark Zuckerberg,* a Facebook alapító elnök-vezérigazgatója. Ismeretlenek betörtek az ifjú milliárdos Facebook lapjára, s ott azt írták: a Facebook-nak lehetővé kellene tennie, hogy a felhasználók „szociális módon" befektethessenek a cégbe, s ezzel kiváltsák a banki finanszírozást. A szerzők *Muhammed Yunus* Nobel-békedíjas közgazdász mikrohitel koncepciójára hivatkoztak, de a rövid szövegből nem derült ki, hogyan is képzelték a fejlődő világban hasznosnak bizonyult elgondolás Facebook-ra való átültetését.

A francia és az amerikai esetnek ugyanaz a – mindannyiunk által megszívlelendő – tanulsága. A szakértők ugyanis úgy nyilatkoztak: mindkét incidenst az tette lehetővé, hogy egyesek „lazán bántak" a jelszóval.

Júliusban *David Beckham* nemcsak azzal került a lapok címoldalára, hogy megszületett az első lánya. Az is bejárta a világsajtót, hogy a világhírű labdarúgó website-ját feltörték, s a látogatót egy kutyaeledel-reklámposzter elfogyasztásán fáradozó eb képe fogadta. Nem járt jobban *Lady GaGa* sem, akinek a webhelyéről csodálók ezreinek nevét és e-mail címét szippantották ki a támadók, akik bizonyítékul zsákmányuk egy részét ki is tették a site-ra.

Októberben Thaiföld röviddel korábban hivatalba lépett csinos női miniszterelnökének Twitter fiókját törte fel egy, a tettét utóbb ártatlan csínyként beállító diák.

Ugyanabban a hónapban Svédországban számos ismert személyiség – képviselő, újságíró, celeb – személyes adatai kerültek hackerkézre. Sovány vigaszul szolgálhatott a híres áldozatoknak, hogy a betörők egy füst alatt száznál több site-ra hatoltak be, s összesen 210 ezer regisztrált felhasználó adatait szerezték meg, majd tették közzé.

Nemzetközi szervezetek és nemzetállamok

Márciusban kapott szárnyra a hír: a francia pénzügyminisztérium másfélszáznál több gépébe törtek be kiberbűnözők, s állítólag más minisztériumokat is támadás ért. Az akció még 2010 decemberében kezdődött. A hackerek a nyomozás eredményei szerint a februári – Franciaország által elnökölt – G20 csúcsra vonatkozó állományokra vadásztak.

A francia nemzetbiztonsági informatikai hivatal (ANSSI) munkatársainak nem sikerült kideríteniük, hogy pontosan milyen mértékű volt a behatolás. Mindenesetre *Pailloux Patrick,* az ANSSI vezérigazgatója az esetet először megszellőztető *Paris Matchnak* úgy nyilatkozott: „ez az első támadás a francia állam ellen, s nagyságrendje ugyancsak példa nélküli".

A tettesek e-mail csatolmányba bújtatott trójai kártevőt küldtek a kiszemelt címzetteknek – többségükben a G20 csúcson dolgozó minisztériumi munkatársaknak. Megfigyelők megjegyzik, hogy az előző csúcstalálkozónak Kanada volt a házigazdája, s akkor az ottani pénzügyminisztériumot érte hasonló támadás.

Egyes elemzők Kínát gyanították az akció hátterében, bár erre nem utalt konkrét bizonyíték. Hogy ennek ellenére felmerült a gondolat, annak az az oka, hogy a csúcstalálkozó központi témája a kereskedelem kiegyensúlyozatlansága volt – márpedig ebben az ügyben az ázsiai ország ugyancsak érdekelt.

Kínát a világsajtóban nem egyszer vádolják kiberakciók szervezésével. Ám az ottani CERT 2010-et áttekintő jelentése szerint az ázsiai ország kormánya maga is a hackerek keresztтüzében állt. Az augusztusban közzétett dokumentumban az áll: az incidensek száma megközelítette a félmilliót. A támadásokat többnyire trójaiakra építették, s az országon kívülről indították – 14,7 százalékukat az Egyesült Államokból, 8 százalékukat pedig Indiából.

Röviddel később – mégpedig a brüsszeli EU-csúcstalálkozó előestéjén – behatoltak az Európai Bizottság Microsoft Exchange levelezőszerverébe. „Gyakran vesznek célba bennünket, de most nagyszabású támadás történt" – közölte a BBC-vel egy nevét elhallgató illetékes. Az uniós szakemberek azonnal reagáltak. Egy időre letiltották az e-mail és az intranet külső elérését, s a munkatársakat felszólították: változtassanak jelszót.

Alig pár nappal később az Európai Parlament lett kibertámadás áldozata.

Egy uniós tisztségviselő szerint mindkét EU-s esetben összehangolt, jól szervezett akcióról volt szó, s az elkövetők érzékeny információkat próbáltak megszerezni. „Nem tizenéves fiúk játszottak betörősdit az érintett intézményekben" – tette hozzá.

Június közepén került nyilvánosságra: kifinomult eszközökkel beférkőztek a Nemzetközi Valutaalap 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 IMF 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 a pénzügyi szervezetnél.

Ezek után nem csoda, ha a kormányok, kormányhivatalok is ostrom alatt állnak. *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.

Japánban október végén okozott botrányt, hogy kiderült: az ország parlamentjében több mint egy hónapon át kártevők garázdálkodtak, s ennek következtében közel félezer képviselő és országgyűlési munkatárs érzékeny adatai kerülhettek illetéktelen kezekbe.

Természetesen világszerte szervezik a védelmet is. Akár történelmi jelentőségűnek is mondhatjuk, hogy november elején első ízben tartott közös IT biztonsági gyakorlatot az Európai Unió és az Egyesült Államok. Nemzetbiztonsági válsághelyzeteket, a kritikus informatikai infrastruktúrát ért támadásokat szimuláltak – ezek ellen kellett védekeznie a 27 EU-tagállam és az USA csapatának. A kiberhadgyakorlatot az Európai Hálózat- és Információbiztonsági Ügynökség (European Network and Information Security Agency, ENISA) és az amerikai belbiztonsági minisztérium szervezte. A fő cél a kritikus infrastruktúra gyenge pontjainak feltárása és a gyors, hatékony reagálás fejlesztése volt.

Cégek

A nagyvállalatok elleni akciók sorát már tavasszal megnyitotta a Sony PlayStation Networkjének és Qriocity szolgáltatásának feltörése. A japán cég először csak annyit közölt: április 17-e és 19-e között hackertámadás érte a hálózatot, s emiatt lekapcsolták a rendszert – amelyet azután 23 napig nem nyitottak meg újra. A belső nyomozás arra az eredményre jutott, hogy 100 milliónál több ügyfél adatai – név, lakóhelyi és email-cím, születési idő, belépési azonosító – kerülhettek illetéktelen kezekbe. S hogy mindez mekkora kárt okozott? Nos, a Sonynál úgy kalkuláltak, hogy a veszteség elérheti a 170 millió dollárt, s ebben a becslésben még nincsenek benne az esetleges perköltségek.

Ősszel újabb – igaz, az előbbinél jóval kisebb – támadás érte a Playstation rendszert, illetve a Sony hálózatot. A betörők egyszerű nyers erő (brute force) módszerrel – felhasználónév+jelszó kombinációk próbálgatásával – dolgoztak, s Playstation Networkön 60 ezer, a Sony Online Entertainment hálózaton pedig 33 ezer fiók adataihoz fértek hozzá.

De kanyarodjunk vissza az év elejére! Még el sem csitultak a világsajtóban a tavaszi 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 2010-es 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 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 a Citigroup következett. A pénzintézet amerikai ügyfélköre körülbelül 1 százalékának adatait szerezhették meg a betörők. Akármilyen kicsiny a százalékarány, 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 adataihoz férhettek hozzá hackerek. 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.

Valószínűleg rá tudták tenni a kezüket a sötét kiberharcosok mintegy 1,29 millió Sega Pass felhasználó személyi adataira is – tudatta az érintettek elnézését kérve a japán játékóriás.

És hogy ne csak adatlopásról essék szó: októberben feltörték a Microsoft YouTube csatornáját. Így aztán a látogatót rövid ideig céges videók helyett rajzfilmek fogadták...

Minden együtt, avagy Anonymous

Külön fejezetet érdemel a kiberakciók történetében a magát Anonymousnak nevező nemzetközi hackercsoport. Az Anonymous a Szcientológiai Egyház elleni – 2008-ban végrehajtott – támadásával kezdte pályafutását, igazából azonban 2010-ben került az érdeklődés homlokterébe, amikor egymás után vette célba azokat a pénzügyi szolgáltatókat, amelyek nem engedtek adományt küldeni az amerikai diplomáciai táviratokat kiszivárogtató WikiLeaksnek.

Azóta a társaság igencsak szerteágazó tevékenységet folytatott. Céltáblájukon voltak/vannak az elnyomó rezsimek – korábban Tunézia és Egyiptom, illetve jelenleg is Szíria. Ellenségnek tekintik a tagjaikat letartóztató államok (például Spanyolország vagy Törökország) kormányát és rendőrségét. Nem kímélik az állami biztonsági szállítókat és más nagy cégeket sem.

Tavaly - egyebek mellett júliusban - megtámadták a Monsanto mezőgazdasági óriást, 8 gigabájtnyi dokumentumot emeltek el az olasz kritikus IT infrastruktúráért felelős kormányszerv, a CNAIPIC rendszeréből, betörtek egy amerikai kormányzati szállító, a Mantech hálózatába, megszerezték 45 ezer ecuadori rendőrtiszt adatait (az ottani kormány fenyegetéseit megbosszulandó), s ha ennyi nem lenne elég, lejáratható tartalmat csempésztek a szíriai hadügyminisztérium site-jára.

Mit csinált eközben az érintett országok rendőrsége? Július elején közös olasz-svájci akcióval 15 Anonymous-tagsággal vádolt hackert vettek őrizetbe. Két héttel később az Egyesült Államokban tartóztattak le 16 gyanúsítottat, akik vélhetőleg részt vettek a PayPal elleni 2010. decemberi támadásban. Ugyanakkor brit földön egy tizenévest, Hollandiában pedig négy személyt helyeztek vád alá.

Válaszul a letartóztatásokra, augusztus első napjaiban az Anonymous 10 gigabájtnyi amerikai rendőrségi adatot tett közzé. A csomagba 11 állam 76 rendőrségi site-jából kerültek személyi információk, azonosítók. Nem hiányoztak a besúgók és hitelkártyák adatai sem.

Augusztus végén aztán a brit rendőrök három letartóztatást foganatosítottak, szeptember végén pedig Amerikában emeltek vádat egy trió ellen. Ez utóbbi Anonymous-sejt akár 15 év börtönt is kaphat.

Októberben ismét a hackerek ragadták magukhoz a kezdeményezést – legalábbis a hírek terén. Áldozatuk ezúttal *Vikram Pandit,* a Citigroup vezérigazgatója volt. Az Anonymoushoz tartozó CabinCr3w becenevű csoport a nagyhatalmú üzletemberről azért tett közzé egy sor személyes információt, hogy így álljon bosszút a Wall Street ellen tüntető hackerek letartóztatásáért.

Amikor Izrael feltartóztatott két hajót, mely fedélzetén aktivistákkal Törökországból a gázai övezetbe tartott, az Anonymous a „kalózkodást” elítélő videót tett közzé, s site-jaik lebénításával fenyegette meg az izraeli biztonsági erőket. November 4-én rövid ideig azután elérhetetlen volt a Moszad és a Shin Bet hírszerző szolgálat, valamint az izraeli hadsereg webhelye. Az illetékesek cáfolták, hogy mindez támadás miatt történt volna, s hangsúlyozták: csak rendszerhibáról volt szó.

Utolsóként egy másik novemberi incidenst említünk. Az Anonymous kilőtte El Salvador kormányzati site-jait. Az elnök webhelyét akkor kapcsolták le a szakemberek, amikor egyetlen nap alatt 30 millió látogatást regisztráltak... Hasonló sorsra jutott, elosztott szolgáltatás-megtagadási (DDoS) támadás áldozatául esett a törvényhozás, a rendőrség, az igazságügyi és a munkaügyi minisztérium site-ja. Az Anonymous nemtetszését a latin-amerikai ország kormányának emberi jogi politikája váltotta ki. De mint tudjuk az Anonymous csoport azóta is aktívan és fáradhatatlanul tényked ik.

Szociális média, társadalmi kockázat

Ahogy nő a szociális média, különösen a Facebook és a Twitter szerepe mindennapi életünkben, úgy válnak ezek a szolgáltatások vonzó célponttá a kiberbűnözők szemében. Tudjuk: a Facebook diadalmenete 2011-ben tovább folytatódott. Egyetlen esztendő alatt újabb 200 millió felhasználót gyűjtött, s ezzel tábora már 800 milliósnál is nagyobb. Kell-e ennél jobb terep kártevő- vagy spamterjesztésre?

Október végén maga a Facebook jelentette: egy átlagos napon 600 ezer felhasználói fióknál próbálkoznak betöréssel vagy más, a szolgáltatás szabályaiba ütköző cselekménnyel. A Barracuda Labs felmérése szerint minden hatvanadik Facebook üzenet rosszindulatú. A kutatók azt találták, hogy a közösségi hálózatokra csatlakozók több mint 90 százaléka kapott már spam-et, s több mint felük volt már kitéve adathalász támadásnak. Minden ötödik felhasználóhoz jutott kártevő, minden hatodiknak a fiókját „vették már igénybe” spamküldésre, s 13 százalékuknak egyenesen eltérítették a fiókját vagy ellopták a jelszavát.

Ugyanakkor szakemberek azt is elismerik, hogy a mögöttünk álló esztendőben a Facebook sokat tett a kockázatok mérsékléséért. A cég igyekszik a lehető leggyorsabban reagálni az újabb és újabb fenyegetésekre. Fontos lépés például, hogy nemrég megbízták a Websense-t: fésülje át a hatalmas hálózatot és szűrje ki a rosszindulatú site-okra mutató linkeket.

Alapvető szemléletváltásról tanúskodik a számítógépes rabló-pandúr játék színpadán az, ahogyan a Facebook a rendszerét támadó, s még nevét is kifigurázó Koobface vírus ügyét kezelte. Jóllehet a történet – feltehetőleg – záró fejezete tanulmányunk zárása előtt pár nappal, azaz már 2012 januárjában kezdődött, trendjelző értéke miatt mégsem hagyhatjuk említetlenül a tavalyi év eseményeinek áttekintésekor.

Mint emlékezetes, minden 2008 júliusában kezdődött. A közösségi hálózat tagjai egy vicces vagy szexi videó megtekintésére invitáló üzeneteket kaptak. Aki a linkre kattintott, az azt olvashatta: a videó lejátszásához előbb frissítenie kell Adobe Flash pluginjét – ám a gyanútlan áldozat a következő kattintással plugin helyett a Koobface kártevőt töltötte le a gépére. Ettől a pillanattól fogva gépe zombivá vált, beépült a gyorsan növekvő Koobface botnetbe. Képernyőjét hamis antivírus programot reklámozó ajánlatok árasztották el, kereséseit pedig különböző sötét online árusokhoz irányította át a vírus. Szakértők szerint fénykorában, 2010-ben a botnetben 400-800 ezer PC működött, s a szemétszoftver eladásából, illetve a hirdetésbevételekből több millió dollárt hozott a vírusírók konyhájára.

Nos, a Facebook biztonsági csapata rendkívül hatékonyan reagált. Gyorsan beazonosították a fertőzést, folyamatosan segítették a felhasználókat, gátat vetettek a kór terjedésének, s 2011 márciusában technikailag kiiktatták a botnet „Anyahajónak" becézett vezérlőszerverét. Mindennek köszönhetően a rendszer kilenc hónapja Koobface-mentes.

Ez is óriási eredmény, ám a 2012-es fejlemények – mondhatni – szakmai paradigmaváltásról tanúskodnak. A Facebook ugyanis idén januárban úgy döntött: nyilvánosságra hozza kitartó nyomozásának eredményét, konkrétan a Koobface mögött álló bűnbanda tagjainak névsorát. „Egyrészt eddig nem mertek nyilvánosan megnevezni a vírusírókat, még ha elég sok bizonyíték is volt ellenük – mutatott rá *Szappanos Gábor,* a VirusBuster szakértője –, másrészt a lépés azért is nagy vihart kavart a biztonsági szakmában, mert még nyomozati fázisban volt az ügy, és így a bűnözők eltakaríthatták a nyomok egy részét."

Úgy tűnik azonban, elkéstek. Az öttagú társaság, melynek tagjai jómódban élnek Szentpétervárott, hiába kezdte el törölni bejegyzéseit a közösségi rendszerekből (mellesleg ezek a bejegyzések sokat segítettek a Facebook-nak a tettesek felderítésében). Hiába tüntették el Anyahajójukat az internetről. A Facebook kijelentette: „addig nem hirdetünk győzelmet a vírus felett, míg szerzőit nem állítjuk bíróság elé".

És most a közösségi hálózatok egy speciális, ugyancsak széleskörű társadalmi következményekkel járó alkalmazásáról. Emlékezetes, hogy a tavaszi arab forradalmakat jórészt a Facebook-on szervezték. Nos, a nyár végi angliai zavargások szítóinak is megvolt a maguk informatikai háttere: a Blackberry okostelefon, illetve a rajta működő (zártkörű) üzenetküldő szolgáltatás, a Messenger.

Pár éve még üzletemberi státusszimbólum volt a RIM cég kézikészüléke. Napjainkra ez a helyzet ugyancsak megváltozott: egy közelmúltban végzett felmérés szerint a brit tinédzserek 37 százalékának a Blackberry az első számú kommunikációs eszköze. Így aztán nem csoda, hogy a rendbontás által különösen sújtott Tottenham parlamenti képviselője egyenesen azt kérte a RIM-től: éjszakára állítsa le a Blackberry Messengert. Erre ugyan nem került sor, ám a cég együttérzését fejezte ki az áldozatok iránt és együttműködést ígért a hatóságoknak. Egy ilyen ígéret nagyon is jól jön a rendőröknek, hiszen a RIM átadhatja nekik – dekódolva – az üzenetforgalmat.

Mikor a szervezkedők rájöttek, a Blackberry Messengeren és a Twitteren küldött üzeneteik könnyen a hatóságoknál landolhatnak, sokan platformot váltottak. Színre lépett a Vibe, amelyben az üzenetek névtelenek, s hatósugaruk – vételi körzetük – akár 15 méterre korlátozható. Aki akarja, önmegsemmisítő szöveget is küldhet. A legrövidebb beállítható üzenet-élettartam 15 perc. Ilyen jellemzők mellett nem meglepő, hogy a Vibe gyorsan népszerűvé vált például a Wall Streeten demonstrálók körében.

Spam és botnetek

A mögöttünk álló esztendő 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.

Amy Winehouse halála után áradtak azok az üzenetek, amelyek az énekesnő kábítószerezését megörökítő videóval kecsegtettek. Gátlástalan bűnözők videofelvételt ígértek a norvégiai vérengzésről is. Nem kerülte el ez a fajta megemlékezés szeptember 11-ét sem, melynek kapcsán többek között „Bin Laden életben van", „Nyomozási eredmények", „Ledőlő tornyok" tárgyú kéretlen levelek szennyezték a világhálót.

Említhetjük azután azt a – magyar neten – új jelenséget, amelyre még tavaly tavasszal 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 – intett *Neumann Róbert,* a VirusBuster víruslaboratóriumának vezetője. – 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" – tette hozzá Neumann Róbert.

Rengeteg erőforrást leköt világszerte a kéretlen levelek, s legfőbb forrásuk, a botnetek elleni küzdelem. Mint a Commtouch világhálós fenyegetések alakulását elemző 2011-es tanulmányaiból kiderül, tavaly átlagosan naponta 114 milliárd darab spam vagy adathalász üzenet röppent ki a világhálóra.

Nagy előrelépést jelentett a spammerek elleni harcban, hogy márciusban a Microsoft vezetésével sikerült kiiktatni a Rustock botnetet. Ennek hatására azonnal 30 százalékkal esett a kéretlen levelek tömege. Júniusban az elmúlt három év legalacsonyabb spamszintjét mérték: „mindössze" napi 106 milliárdot, ami a teljes e-mail forgalomnak „csupán" háromnegyedét tette ki.

Következő táblázatunkban a zombikkal és spammel kapcsolatos legfontosabb információkat foglaltuk össze, a Commtouch jelentései alapján. Látszik, hogy India stabilan őrzi a világ legelzombisodottabb országa kétes értékű címét, a kéretlen levelek örökzölden leggyakoribb témája a gyógyszer-ajánlat, s a legtöbb spamet Gmail-fiókból küldik.

Zombik és spam a Commtouch szerint					
		2011/I. né.	2011/II. né.	2011/III. né.	2011/IV. né.
Aktivált új zombi gépek naponta [ezer]		258	377	336	209
Részesedés a világ zombi-állományából	India	17.0%	17.4%	18.8%	23.5%
	Brazília	12.0%	10.0%	7.7%	-
	Vietnám	9.0%	7.9%	8.5%	7.2%
	Oroszország	7.0%	5.3%	6.7%	6.2%
	Ukrajna	4.0%	-	-	-
	Indonézia	-	4.1%	-	-
	Pakisztán	-	-	4.9%	7.2%
	Kína	-	-	-	5.5%
Spam, ill. adathalász üzenetek száma naponta [milliárd]		149	113	93	101
Legnépszerűbb spamtémák	gyógyszer	28.0%	24.0%	29.0%	31.2%
	pénzkérő	13.0%	11.0%	6.5%	7.1%
	társkereső	12.0%	3.0%	2.3%	11.7%
	szexsegédeszköz	10.0%	12.0%	12.2%	13.9%
	pornó	6.0%	7.6%	6.4%	3.5%
	szoftver	4.0%	4.0%	2.9%	1.8%
	adathalász	3.0%	8.5%	6.7%	6.2%
	termékutánzatok	2.5%	8.4%	8.4%	14.2%
	diploma	2.0%	2.0%	5.6%	2.0%
	fogyókúra	1.5%	1.0%	5.5%	4.0%
	egyéb	18.0%	18.0%	5.4%	4.5%
Leggyakrabban spamküldésre használt domainek	gmail.com	gmail.com	gmail.com	gmail.com	gmail.com
	att.net	att.net	yahoo.com	yahoo.com	yahoogroups.com
	yahoo.com	yahoo.com	yahoogroups.com	att.net	yahoo.com
	yahoogroups.com	yahoogroups.com	googlegroups.com	yahoogroups.com	googlegroups.com
	hotmail.com	hotmail.com	hotmail.com	googlegroups.com	yahoo.com.ph
	googlegroups.com				
	yahoo.com.ph				

Kiemelkedő kártevők

Az elmúlt év kártevő-körképét vizsgálva az egyik legszembetűnőbb új jelenség az Apple eszközök elleni komolyabb támadások megjelenése. Az almás világot is elérték 2011 első felében a windowsos környezetben régóta ismert kellemetlenségek: a kártevőkészítő készletek és a hamis vírusirtók.

Ami az előbbi témát illeti, világszerte bejárta a szaksajtót a hír: földalatti fórumokon egy hacker Mac OS X-re tervezett trójaiépítő-kitet hirdetett. A Weyland-Yutani nevű, 1000 dolláros készlet segítségével számítógépes bűnözők pár kattintással készíthettek 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 hamis almás vírusirtó. Május elején több nagy napilap is beszámolt a MacDefenderként bemutatkozó rémisztőprogram (scareware) felbukkanásáról. Az utolsó negyedévben pedig az OS X-re specializált trójaiakról érkeztek jelentések.

Tavaly rajzolódott ki világosan egy másik trendvonal is, amelyre szakértők már korábban figyelmeztettek: a korszerű okostelefonok, táblagépek rohamos térhódítása mágnesként vonzza a kiberbűnözőket. „Súlyosbítja a problémát a mobil architektúrák konvergenciája és felhasználói táboruk növekedése. Az interneten 1,5 milliárdnyian vannak világszerte, a mobilosok számát viszont már 5 milliárdra teszik. A bűnözők a profitot keresik. Ha egyszer a mobiltelefonok jelentik a legnagyobb számítástechnikai platformot, akkor nyilván rendszeresen célkeresztbe kerülnek" – jellemezte a helyzetet *Patrick Traynor,* a Georgiai Műszaki Egyetem (Georgia Tech) tanára.

Júliustól novemberig több mint megötszöröződött az androidos kártevőminták száma, s ezek 55 százaléka kémprogram funkciókat is tartalmazott – állapította meg a Juniper Networks. Az elmúlt évben, különösen annak utolsó negyedében az Android platform több fertőzésére, illetve sérülékenységére is fény derült.

Csak növeli a veszélyt, hogy a magukat ingyenes Android-antivírus programként ajánló termékek többsége valójában alig nyújt védelmet. Az AV-Test.org tanulmánya szerint a legjobb díjmentesen letölthető szoftver is csak a fenyegetések 32 százalékát volt képes kiszűrni, hat másik 10 százalékot teljesített, s az egyik vizsgált program pedig éppenséggel egyetlen kártevőt sem észlelt.

Zártsága miatt az Apple iOS platformja kevésbé van veszélyben, de elemzők az iPhone, iPod és iPad felhasználókat is óvják attól, hogy hamis biztonságérzetbe ringassák magukat.

Még egy fonalat emelünk ki a kártevők végtelen kusza szövedékéből. Az olvasó jól emlékezhet a 2010-es év nagy IT biztonsági szenzációjára: az első, ipari folyamatirányító rendszereket támadó kártevőre. Az összetett funkcionalitású Stuxnet férget feltehetőleg az iráni atomprogram szabotálásának céljára fejlesztettek ki. Szakértők már akkor megjósolták, hogy a Stuxnet csak az első fecske, s további hasonló támadások várhatók. Nos, tavaly októberben színre lépett a Duqu, melyet elemzők szerint komoly fejlesztőkapacitással a Stuxnet kódjának felhasználásával építettek fel. A Duqu olyan cégek rendszereit támadta meg a világ több pontján, amelyek olajtávvezeték-vezérlőket és más kritikus infrastruktúra-elemeket gyártanak. Nyilván ennek a történetnek is lesz még folytatása...

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.

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. Alábbi táblázatunk a legaktívabb kártevő-szóró domaineket foglalja össze:

A legtöbb kártevőt szóró domainek 2011 december végén a VirusBuster észlelése szerint		
Domain	**Fájlok száma**	**Földrajzi hely**
runit.biz	1,227	Bahama-szigetek
diplomshop.ru	881	Oroszország
origin-ics.fivemillionfriends.com	750	Egyesült Államok
origin-ics.clickpotato.tv	721	Egyesült Államok
dl.dropbox.com	586	Egyesült Államok
netox.biz	500	Németország
www.screenblaze.com	262	Egyesült Államok
playsushi.com	185	Egyesült Államok
download.cpudln.com	171	Kína
s4.zip-host.ru	166	Oroszország

Az sem érdektelen, hogy a weben barangolva milyen jellegű site-okon kell leginkább fertőzéstől vagy adathalászattól tartanunk. Erre vonatkozóan a Commtouch elemzése ad eligazítást. A cég statisztikái szerint az egyes negyedévekben (gyakorisági sorrendben) a következő site-kategóriákon bújtattak meg a bűnözők előszeretettel valamilyen kártevőt:

A kártevőket leggyakrabban terjesztő site-kategóriák a Commtouch szerint				
	2011/I. né.	**2011/II. né.**	**2011/III. né.**	**2011/IV. né.**
1	parkolt domain-ek	pornó/szex	parkolt domain-ek	parkolt domain-ek
2	spam site-ok	parkolt domain-ek	portálok	portálok
3	portálok	portálok	pornó/szex	pornó/szex
4	pornó/szex	oktatás	oktatás	oktatás
5	oktatás	szórakoztatás	szórakoztatás	céges
6	szórakoztatás	céges	céges	szórakoztatás
7	céges	egészségügy	IT/technológia	áruház
8	áruház	utazás	egészségügy	egészségügy
9	divat/szépség	IT/technológia	áruház	utazás
10	IT/technológia	divat/szépség	utazás	IT/technológia

Némileg más tartalmú hálókikötők azok, amelyeken a Commtouch szerint leginkább adathalászatnak lehetünk kitéve:

Adathalászattal leggyakrabban fenyegető site-kategóriák a Commtouch szerint				
	2011/I. né.	**2011/II. né.**	**2011/III. né.**	**2011/IV. né.**
1	játék	játék	játék	játék
2	egészségügy	portálok	portálok	portálok
3	portálok	áruház	áruház	áruház
4	IT/technológia	fórum/hírcsoport	divat/szépség	oktatás
5	divat/szépség	non-profit szervezetek	oktatás	divat/szépség
6	szabadidő	divat/szépség	sport	sport
7	áruház	szabadidő	szabadidő	céges
8	sport	sport	céges	szabadidő
9	oktatás	oktatás	egészségügy	szórakoztatás
10	streaming média, letöltés	céges	szórakoztatás	ingatlan

Persze kisebb kockázattal navigálhatunk a weben, ha korszerű, biztonságos böngészőt használunk. Jó okkal indított a Microsoft kampányt az Internet Explorer immár több mint tízéves 6-os verziójának a világhálóról való kiszorítására.

„Közel félezer ki nem javított biztonsági hiba van az IE6-ban, majdnem négyszer annyi, mint az összes többi elterjedt böngészőben együttvéve – magyarázta *Szappanos Gábor,* a VirusBuster szakértője. – Tíz év alatt rengeteget változott a világ. Az internet lett a számítógépes vírusok legfontosabb támadási pontja, a böngésző pedig a kártevők legfontosabb megcélzott hordozó közegévé vált. Egy évtizeddel ezelőtt nem készítették, nem készíthették fel a böngészőket ilyen nyomás elviselésére. Azóta a Microsoft is új technológiákat alkalmaz, s ennek köszönhetően termékei – köztük az Internet Explorer frissebb kiadásai – jóval biztonságosabbak. Felelőtlenség a korábbi, elavult verziót használni.”

Nem csoda hát, hogy a Microsoft az IE 6 tizedik születésnapja alkalmából külön webhelyet állított fel a felhasználók felvilágosítására. Az „IE6 visszaszámláló” site-on (www.theie6countdown.com) láthatjuk a szoftver pillanatnyi világpiaci részesedését, sőt azt is, hogy egyes fontosabb országokban a szörfösök mekkora hányada ragadt le az IE6 mellett. Míg februárban még világszerte a felhasználók 12 százaléka szörfölt IE6-tal, december végén ez a szám örvendetes módon már csak 7,7 százalék volt. Legtöbben továbbra is Ázsiában maradtak hűek a veszedelmessé vált öreg böngészőhöz: felhasználóinak negyede kínai.

Nemcsak a böngészőt, hanem minden más alkalmazást is célszerű naprakészen tartanunk. Különösen fontos a biztonsági szoftverek és az operációs rendszer frissítése, vagy a támadások kereszttüzében álló Adobe programok – Reader/Acrobat, Flash Player – foltjainak haladéktalan feltelepítése.

Jó, ha mindig szem előtt tartjuk azt a döbbenetes számot, amelyet a Microsoft biztonsági tanulmánysorozata legfrissebb kiadásában, a Security Intelligence Report 11-es kötetében közölt. A szoftveróriás Rosszindulatú Szoftvert Eltávolító Eszköze (MSRT) által kiszűrt fertőzések 90 százaléka olyan sérülékenységet aknázott ki, amelyre már több mint egy éve rendelkezésre állt a folt...

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