Puskás Tivadar Közalapítvány

# PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2012. II. negyedéves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

# Tartalom

# Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2012. II. negyedéves jelentését, amely a negyedév legfontosabb IT- és hálózatbiztonsági momentumait gyűjti egybe és értékelést ad ezen technikai információk társadalmi és gazdasági hatásainak vonatkozásában az Információs Társadalomért Alapítvány közreműködésével, valamint bemutatja a VirusBuster Kft. informatikai biztonsági trendjeiről szóló összefoglalóját. A jelentésben a főszerep ismét a hálózatbiztonságé.

A jelentés betekintést nyújt az informatikai biztonság berkeibe. A második negyedévben a közszférát vesszük fókuszpontba IT-biztonsági szempontból, egy cikk erejéig kitérünk a bankkártyák kapcsán felmerülő biztonsági kérdésekre, valamint teszünk egy kitérőt az Egyesült Államokban az információbiztonságra, hálózatbiztonságra vonatkozó szabályozások területére is.

A Nemzeti Hálózatbiztonsági Központ továbbra is eredményesen működteti szakmai közönségének és partnereinek szóló IT biztonsági oldalát a Tech.cert-hungary.hu-t. Az oldalon a látogató megtalálhatja a legfrissebb szoftversérülékenységi és riasztási információkat, valamint a TechBlog hírfolyam naponta frissülő nemzetközi hírekkel és érdekességekkel látja el a hazai olvasótábort, magyar nyelven.

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

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

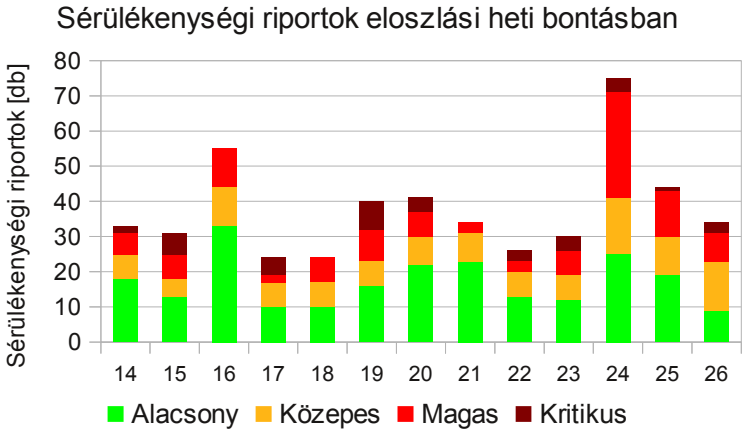
**Bódi Gábor**
Puskás Tivadar Közalapítvány
ügyvezető igazgató

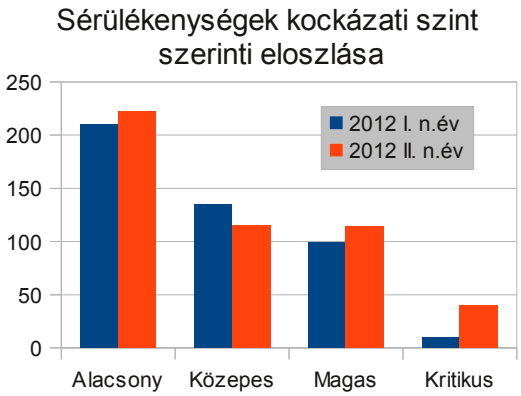
# A PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ tevékenysége számokban

## 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)** 2012 II. negyedéve során **491 db szoftversérülékenységi információt** publikált, amelyekből 223 db alacsony, 115 db közepes, 113 db magas és 40 db kritikus kockázati besorolású.

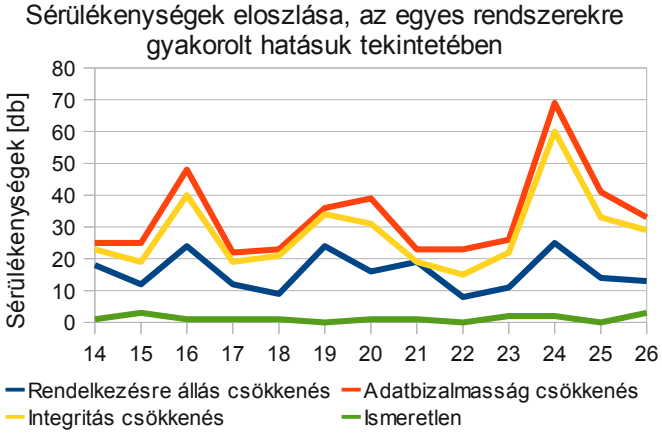



Az egész évet vizsgálva a publikált sérülékenységek számosságára, valamint az azok által érintett rendszerekre gyakorolt hatásukra fókuszálva megállapíthatjuk, hogy nem csak a mennyiség terén állunk rosszabb helyzetben, mint az előző negyedévben. Jelen periódusban igaz ugyan, hogy „csak” 8%-kal több sérülékenység került publikálásra, de a magas és a kritikus kockázati besorolású sérülékenységek jelentősen megszaporodtak. A magas kockázati besorolású sérülékenységek száma 15%-kal nőtt, míg a kritikusak számossága megnégyszereződött.

Ez többek között annak is köszönhető, hogy a negyedéveben számos SCADA (Supervisory Control and Data Acquisition) rendszereket érintő sérülékenységről adtunk tájékoztatást. Eezek közül is fontos megemlíteni az Invensys-t, amely cég SCADA rendszerekhez készít szoftvereket. A SCADA rendszereket gyakran hívják ipari vezérlő rendszereknek (ICS – indrustrial control systems), amelyek olyan számítógépes rendszerek, melyek segítségével monitorozhatóak és vezérelhetőek az infrastruktúrák és/vagy folyamatok. Az Invensys termékek kapcsán publikált sérülékenységi információk mindegyike kritikus kockázati besorolást kapott.

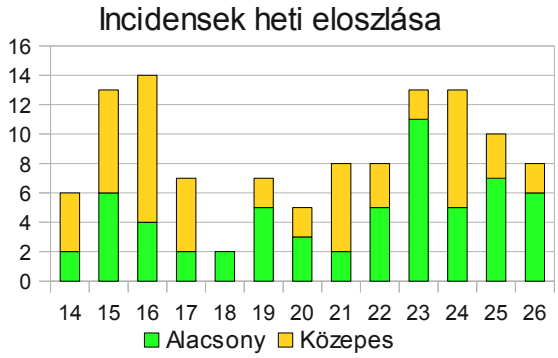
A sérülékenységek eloszlása, az egyes rendszerekre gyakorolt hatásuk tekintetében, közel ugyanazt a tendenciát követik. Legnagyobb számban az adatbizalmasság-csökkenés elő-idézésére kihasználható szoftver sérülékeny-ségekről adtunk tájékoztatást, melyek az összes jelentés 42,4%-át teszik ki. Ezt követik az integritás csökkenéssel járó sérülékenységek 35,8%-os részhányaddal. Mindezek egyenes következménye, hogy a sérülékenységek az egyes érintett rendszerek szempontjából potenciálisan legnagyobb veszélyt adatbiztonsági szempontból jelentenek.



# Internetbiztonsági incidensek

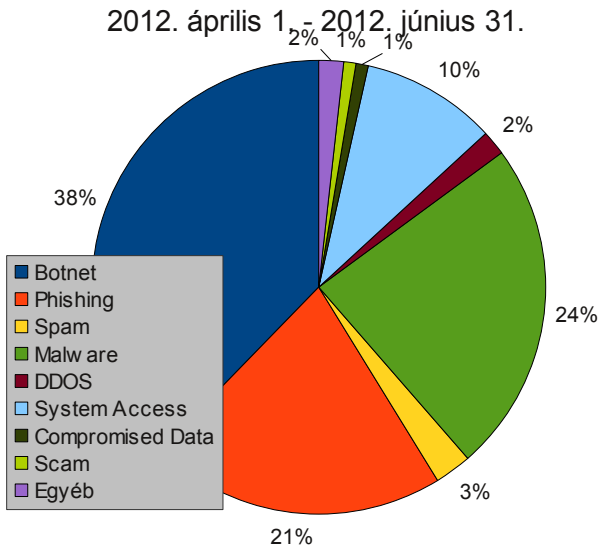
Internetbiztonsági incidens minden olyan biztonsági esemény, amelynek célja az információs infrastruktúrák bizalmasságának, sértetlenségének vagy rendelkezésre állásának megsértése az interneten, mint nyílt információs infrastruktúrán keresztül.

A PTA CERT-Hungary, **Nemzeti Hálózatbiztonsági Központ** a 2012-es év második negyedévében **114 db incidens bejelentést** regisztrált és kezelt, ebből 60 db alacsony és 54 db közepes kockázati besorolású.




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

A bejelentések többnyire külföldi partner szervezetektől érkeztek és több, mint 87%-ban hazai káros tevékenységgel vagy káros tartalommal voltak összefüggésben. Összesen 82 szolgáltató került bevonásra az egyes incidensek kezelése során és összesen 414 szálon folyt incidenskezelési koordináció.




A 2012-es év második negyedévében az incidensek típus szerinti eloszlását, a korábbi időszakokhoz hasonlóan a botnet hálózatok részét képező megfertőzött számítógépek kapcsán fogadott bejelentések vezetik közel 40%-kal, még úgy is, hogy ezek az adatok nem tartalmazzák Shadowserver Foundation-től beérkező bejelentéseket.

Az érintett időszakban nagy számban érkeztek a különböző weboldalakon elhelyezett káros szoftverek kapcsán bejelentések, melyek az incidensek 24%-át teszik ki. Az ilyen jellegű incidensek azért is érdekesek, mert több biztonsági problémára is utalhatnak, hiszen az esetek többségében ezeket a kártékony programokat az érintett weboldalak tulajdonosainak, illetve üzemeltetőinek tudta nélkül helyezik el. Ezt a bűnözők többnyire az oldal valamilyen sérülékenységének kihasználásával vagy az oldalt kiszolgáló tárhelyhez történő illetéktelen hozzáféréssel valósítják meg, így egy ilyen káros szoftverről szóló értesítés más biztonsági hibákra is felhívhatja a tulajdonosok és üzemeltetők figyelmét.

A fennmaradó 35% főként a felhasználók megtévesztésén alapuló a banki és egyéb bejelentkezési adatok megszerzését célzó, adathalász tevékenységekkel kapcsolatos, illetve az illetéktelen rendszerhozzáférések kapcsán érkezett incidens bejelentésekből tevődik össze. Az első negyedévhez képest visszaesés tapasztalható az elosztott szolgáltatás megtagadásos incidensek terén, míg a januártól áprilisig terjedő időszakban ezen bejelentések feldolgozása az incidenskezelési koordináció közel 20%-át tették ki, addig a második negyedévben ez alig több, mint 5%.

# IT a közszférában - A kormányzati informatika trendjei

## Elektronikus közigazgatás

Az elmúlt időszak jelentős fejleménye volt, hogy tavaly év végén a magyar törvényhozás módosította a KET-et, illetve idén áprilisban megjelentek a törvény végrehajtási rendeletei. A módosítás hatályon kívül helyezett több olyan szabályozást, amelyek gátolták a nyitást, illetve amelyeket ma már meghaladt a technológiai fejlődés, különösen az online ügyintézés terén.[1]

Lesznek olyan kötelező elektronikus szolgáltatások, amelyek a közigazgatási eljárásokat támogatják. Ezek később kiterjeszthetők a tipikusan nem közigazgatási hatóságnak számító szervezetekre is (bíróságra, igazságszolgáltatásra, oktatásra, stb.). Ilyen például az elektronikus aláírás, amely eddig azért nem terjedtel (Európa más országaiban sem), mert drága volt és bonyolult. A KET módosítása viszont bevezette a minősített tanúsítvány alapú, fokozott biztonságú aláírás fogalmát, ami már önmagában is olcsóbbá tenné a folyamatot.

Frissítik a már meglévő megoldásokat is. Eddig például az űrlapokat nyomtatványkitöltővel kellett kitölteni, s csak egy elektronikus csatornán (az Ügyfélkapun) keresztül lehetett elküldeni. Most az állampolgár szabadon eldöntheti, hogy melyik csatornát használja ügyintézésre: a postait, a webeset, illetve a mobilost. A polgár megválaszthatja azt is, hogy milyen módon azonosítsa őt a hatóság, s ezt egy rendelkezés-nyilvántartó adatbázis tartja majd számon. Lehetőség lesz mobiltelefon vagy akár kártya alapú azonosításra.

Ahhoz azonban, hogy ez működjön, létre kell hozni az úgynevezett összerendelési nyilvántartást, amely feloldja az eddig az elektronikus közigazgatás kiterjesztésének gátját jelentő ellentmondásos helyzetet, és egyszerre biztosítja a személyes adatok megfelelő védelmét, valamint a nyilvántartások közötti jogszerű adatkapcsolatok egyszerű kialakíthatóságát.

A kötelező állami szolgáltatásokat alapvetően három nagy állami szervezetnek kell felállítania, ezek a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEK KH), a Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ) és a Magyar Posta Zrt. Bevezetik a szabályozott elektronikus ügyintézési szolgáltatás (szeüsz) fogalmát is, amely az informatikai rendszerekről (központi rendszerről, űrlapkitöltő programról, stb.) a jól használható szolgáltatásra helyezi át a hangsúlyt, és ennek rendeli alá az informatikai rendszerek kialakítását és működtetését.

## A kormányzati informatika konszolidációja

A közigazgatás fent vázolt gazdaságosabb és rugalmasabb működését teszi lehetővé a kormányzati informatika infrastruktúrájának konszolidálása, amit főként az infrastruktúra széttagoltsága és a szervezetrendszer párhuzamosságai indokoltak. A konszolidációban máris kézzel fogható sikereket ért el a szaktárca. Ezek közül kiemelendő, hogy a közigazgatási és a Közháló keretében biztosított egyéb közösségi végpontok fenntartási költségeit több mint egymilliárd forinttal sikerült csökkenteni.

A Nemzeti Hálózatfejlesztési Projekt keretében elindult a Nemzeti Távközlési Gerinchálózaton az integrált hang- és adatszolgáltatás. Ennek jóvoltából az állam hivatalosan idén január elsejétől biztosítja a kormányzati szervek és háttérintézményeik infokommunikációs ellátását.

1 Mártonffy Attila: Parlamentáris infokommunikáció, IT-business, 2012.06.05., http://www.itbusiness.hu/Fooldal/hetilap/cimlapon/Parlamentaris_infokommunikacio.html

Annak köszönhetően, hogy a korábban az egyetlen piaci szolgáltató által működtetett Kormányzati Gerinchálózat helyett állami tulajdonú infrastruktúrára épülő hálózat szolgálja ki az igényeket, jelentős megtakarítást ért el a kormány. 20%-kal, évi mintegy kétmilliárd forinttal sikerült csökkenteni az érintett intézményi kör – körülbelül 100–120 intézmény – hálózati kiadásait.

Ami a kormányzati informatika koordinációját illeti, fontos és sikerrel végrehajtott feladat volt az együttműködés kialakítása az informatikai ágazatban hatáskörrel, jogosítvánnyal rendelkező szervezetek és intézmények között. Ennek eredményeképpen immár jobban, gyorsabban és hatékonyabban lehet képviselni az ágazat érdekeit, kezelni a napi problémákat, illetve stratégiai megoldásokat találni és ezekhez kapcsolódó fejlesztéseket megvalósítani. A koordináció másik fontos területe az intézményfelügyeleti tevékenység. Az érintett intézményi körrel jó együttműködést sikerült kialakítani a beszerzések, az informatikai üzemeltetés és a projektek kivitelezése terén. Kiépült egy olyan monitoringrendszer is, amely a KIM, az NHIT és az NFM együttműködésével támogatást nyújt az intézményeknek.[2]

## „Jó Állam” operatív programok

A kormány már két éve dolgozik az úgynevezett „Jó Állam” fejlesztési koncepció végrehajtásán, amelynek része a Magyary Zoltán nevét viselő közigazgatás-fejlesztési program. Ennek az egyik fő forrása az Államreform operatív program (ÁROP) és az Elektronikus Közigazgatási Operatív program (EKOP).[3] 2 Az államreformhoz tartozik minden, ami a szervezet- és személyzeti fejlesztéssel kapcsolatos, az e-közigazgatás keretében pedig a modern közigazgatástól elválaszthatatlan digitalizálás, elektronizálás, azonosítás, adatbázis-fejlesztés és adott esetben hardvervásárlás valósul meg. A két program között szoros az együttműködés, sok projektet párhuzamosan, két forrásból finanszíroznak.

Így történik például a járási rendszer kialakításánál, ahol a kormányhivatalok szervezetfejlesztése, illetve személyzeti továbbképzésének finanszírozása az ÁROP-ból, a kormányablakok kialakítása pedig az EKOP-ból történik.

A Magyary Zoltán programban négy fő fejlesztési területet határoztak meg: szervezet, feladat, eljárás, személyzet. A szervezetfejlesztés keretében például az állami szervezetek száma a felére csökkent. A feladatkataszter létrejötte mind az ÁROP-nak, mind az EKOP-nak köszönhető. Az eljárások digitalizálásában – az elektronikus azonosításban, az időbélyegző bevezetésében, illetve az ügyintézés internetre helyezésében – az EKOP játszik nagyobb szerepet. A személyzeti területen a képzés, valamint a nagy nyilvántartások kialakítása – például a 73 ezer kormánytisztviselő adatainak közös adatbázisba rendezése – dominál az ÁROP és az EKOP égisze alatt.[3]

A kormány fontos célja a projektek lefutásának felpörgetése. Ennek érdekében a kormány még tavaly novemberben elfogadott egy gyorsító csomagot, amely például az akciótervek nevesítése és a támogatási szerződések megkötése közötti, eredetileg 300 napot levitte 90-re. Egyszerűsödött a szerződéskötés is a döntés-előkészítő bizottság, a program-előkészítő munkacsoport és egyéb fórumok munkája során.

Lényeges momentum ebben a folyamatban, hogy lassan véget ér az Európai Unió 2007–2013-as pénzügyi ciklusa, s az érintett tárcáknál felállított munkacsoportokban már megkezdődött a 2014–2020-as periódus tervezése. Most fog eldőlni az, hogy Magyarország mekkora EU-forrásokhoz jut majd a következő hét évben, beleértve az informatikai ágazatot is.

Konkrét javaslatok az év második felében kerülnek az Európai Bizottság asztalára, s remélhetőleg az informatikai szektor nem fog rosszul járni, sőt talán még növelhetők is lesznek a keretszámai.

2 Mártonffy Attila: Parlamentáris infokommunikáció, IT-business, 2012.06.05., http://www.itbusiness.hu/Fooldal/hetilap/cimlapon/Parlamentaris_infokommunikacio.html

3 EKOP-3.1.6 Önkormányzati ASP központ felállítása, http://www.nfu.hu/doc/3459

Klasszikus probléma ugyanakkor az információtechnológiai ágazatban, hogy a projektek, legyenek azok intézményi vagy ágazati szintűek, lassan, nehézkesen indulnak el, végrehajtásuk pedig sok esetben csúszik a folyamatos változtatások miatt. Ezért a tavalyi év egyik feladata olyan, hármas eszközrendszer létrehozása volt, amelynek segítségével az intézményi kör hatékonyabban, pontosabban tervez, illetve hajt végre informatikai projekteket határidőre.

## Az EU követelményei

Magyarországon az Európai Unió megfelelő szervezetei szerint a szélessávú lefedettség mind a városi környezetben, mind a vidéki területeken jónak mondható, de az elérhetőség dacára a magyarok az uniós átlagtól elmaradó mértékben használják az infrastruktúrát. Viszont azok, akik csatlakoznak az infrastruktúrához intenzíven, az EU átlagot meghaladó mértékben használják az internetet. Mint ismert, a Digitális menetrendben megfogalmazott brüsszeli célok szerint 2013-ra a lakosság 100%-ának kell elérnie a szélessávú hálózatot. 2020-ra a hozzáférések mindegyikének legalább 30 megabit/szekundum sávszélességűnek kell lennie, a 100 megabit/szekundum feletti kapcsolatok arányának pedig el kell érnie az 50%-ot.

Hazánkban az e-ügyintézés jócskán elmarad az EU átlagától. Itthon a lakosság mindössze 35%-a intézi a közügyeit online, miközben az európai uniós átlag 41 százalék.

A vállalkozások hozzáférése az e-kormányzati szolgáltatásokhoz a leggyengébb terület, a leggyakrabban igénybe vett szolgáltatások körét pedig jobbára az online elérhető kérdőívek teszik ki. Az e-kormányzati szolgáltatásokkal kapcsolatos kihívások között szerepel, hogy meg kell teremteni a szolgáltatások nyitottságát és átláthatóságát, erősíteni kell a civil és az üzleti használatot. Ezentúl bővíteni kell a szolgáltatások körét, illetve javítani a szolgáltatások minőségét.

Ami a források felhasználását illeti, Magyarországon 124 vállalkozás összesen 27 millió eurót nyert kutatás-fejlesztésre, amely az uniós költségvetésen belül mindössze 0,7%-ot tesz ki. Ezt a jövőben növelni kell.

A következő 2014–2020 közötti költségvetési időszak Horizon 2020 elnevezésű programjában a digitális infrastruktúra fejlesztésére 9,1 milliárd euró áll majd a vállalkozások, önkormányzatok rendelkezésére.[4]

## A közszféra hardver- és szoftverellátottsága

A 2011 második negyedévében íródott közszféra jelentés és az éves jelentésben foglalt penetrációs adatok javarészt most is helytállóak, a friss adatfelvételek eredményei még nem kerültek publikálásra. A közszféra elmúlt hónapokra jellemző krónikus forráshiánya nem is nyújtott komoly teret a fejlesztéseknek. Két nagyon fontos trend okozza az infrastruktúra jelenlegi és közeljövőbeli átalakulását:

- Az első, a szabad szoftverek mind jelentősebb térnyerése a közszférában
- A második a felhő alapú, illetve központilag szolgáltatott alkalmazások fejlődése és terjedése.

## Nyílt forráskód a közszférában

Rövidesen véget ér egy korszak az állami finanszírozású intézmények szoftverellátásban. Így minden intézmény számára átláthatóbbá válnak azok a költségek, amelyek a szoftverek használatával járnak együtt az irodában vagy az oktatásban.

4 Mártonffy Attila: Parlamentáris infokommunikáció, IT-business, 2012.06.05., http://www.itbusiness.hu/Fooldal/hetilap/cimlapon/Parlamentaris_infokommunikacio.html

Az elmúlt év végén, hosszabb előkészítő munka után, kormányzati intézkedés történt a közigazgatási intézmények dokumentumhasználatát illetően. Egy kormányhatározat március 31-étől elrendeli a közigazgatási szervezetek számára a szabványoknak megfelelő dokumentumformátum használatát az egymás közti kommunikációban, illetve a szervezeteknek képeseknek kell lenniük ilyen dokumentumok fogadására külső féltől. A jogszabály rendelkezik a nyílt forráskódú irodai szoftverek használatáról is. (A határozat nem vonatkozik a Honvédelmi Minisztériumra és intézményeire.)

Egy másik bejelentés szerint a kormány március 1-jével megszünteti a Tisztaszoftver-programot a köz- és felsőoktatásban. Ez a gyakorlatban azt jelenti, hogy az állam szakít az eddigi, évtizedes, a világon egyébként példa nélküli gyakorlattal, és nem finanszírozza tovább az eddigi egyetlen szállító – a Microsoft – szoftverlicenceinek megújítását.

A két dolgot elvileg a nyílt forráskód köti össze, de nem ennek a hangsúlyozása volt a cél, hanem a költséghatékonyság és a versenysemlegesség szem előtt tartása.

2012. február elején a Free Software Foundation (FSF) magyarországi szervezete, az FSF.hu Alapítvány Szabad Út néven a nyílt forrású rendszerekre való átállást segítő portált indított, amely a LibreOffice mellett számos, infrastruktúra jellegű szoftvert is ajánl a szervezeteknek, intézményeknek.[5]

A kormányhatározat a fenti kivételtől eltekintve minden közigazgatási intézményre vonatkozik, de a félreértések elkerülése végett ez nem azt jelenti, hogy mindenhol nyílt forráskódú irodai csomagra lenne kötelező átállni. Csupán arról van szó, hogy a szabványoknak megfelelő dokumentumokat kell használni. Ahol Microsoft Office 2007 vagy frissebb verziói vannak használatban, ott nincs teendő, hiszen azok formátumai szabványosak. A 2003-as Office használói pedig megtehetik, hogy letöltik és telepítik a megfelelő fájlkonvertert.

Ez megteremti a lehetőséget arra, hogy a szervezetek költséghatékonyabb, nyílt forráskódú programokra álljanak át például akkor, amikor lejár a meglévő Microsoft nagyvállalati licencszerződése. Ilyennel egyébként már próbálkoztak, s a szervezeten belül sikerült is; viszont aránytalanul nagy erőfeszítésbe került a kommunikáció fenntartása a külső szervezetekkel.

A minisztérium március 31-étől ellenőrizni fogja a beszerzéseket ebből a szempontból is. Nem nyílt forráskódú irodai szoftver beszerzését csak abban az esetben engedélyezi, ha az műszaki, gazdasági szempontból indokolt, vagy ha nemzetközi szerződés teljesítése érdekében szükséges. Ilyen lehet, amikor a szakrendszerekkel való integráltság miatt az átállás többe kerülne, mint a zárt forráskódú szoftver licencének meghosszabbítása.

## Tisztaszoftver program az oktatásban

Ami a Tisztaszoftver-programot illeti, a felsőoktatásra vonatkozóan 2001-ben kötötte meg a kormány a Campus megállapodást, amelyet 2004-től a közoktatásra is kiterjesztett. A mostani döntés az intézmények által megvásárolt gépekre gyárilag telepített (oem) Windows operációs rendszer frissítésére, valamint a Microsoft Office licenceire vonatkozhat. A program felmondásával tehát csak az Office veszíti el jogtisztaságát, az operációs rendszer nem – legfeljebb a jövőben nem lesznek verzióváltások. Az állam egyébként a Tisztaszoftver-programra az elmúlt 10 évben mintegy 12 milliárd forintot költött, s csak tavaly kezdte szorgalmazni, hogy az oktatási intézmények vegyenek igénybe nyílt forráskódú rendszereket is. Ezzel egyidejűleg 50 ezerre korlátozták azoknak a felsőoktatási hallgatóknak a számát, akiknek a kormány finanszírozza a licenceit.

Ezzel kapcsolatban viszont sokan kételyüket fogalmazzák meg arról, hogy a közoktatási intézményekben túl rövid az átállásra engedélyezett idő, s így például veszélybe kerülhet az érettségi vagy a felvételi. A 2011-es szerződések idén március 1-jéig érvényesek, de lesz új

5 Mártonffy Attila: Tisztázott, nyílt helyzet?, IT-business, 2012.02.21., http://www.itbusiness.hu/Fooldal/hetilap/cimlapon/Tisztazott_nyilt_helyzet.html

Tisztaszoftver-szerződés, azaz az állam tovább finanszírozza az intézmények működéséhez és a feladatok ellátásához szükséges alaplicenceket. Ennek részleteit most dolgozzák ki a Microsofttal közösen. Az új szerződés nem lesz korlátlan, időtartamát egy évre tervezik. Ezután versenysemlegesség fog érvényesülni, s az iskoláknak kell kiválasztaniuk, milyen típusú licenceket akarnak tovább használni. A bérleti konstrukciót 2012 során szeretnék megszüntetni a közoktatásban, s a tárca ragaszkodik ahhoz, hogy az állam tulajdonjoggal rendelkezzen a licencekben. Amint ez megvalósul, attól kezdve az iskolák kötelezettsége lesz ezeknek a szoftvereknek a fenntartása.

## A Microsoft ellen?

A közigazgatási intézmények dolgozóinak majd 100%-a Windows-on és Office-on végzi a mindennapi feladatát. Gyakorlatilag Microsoft alapon fut a közigazgatás magja. A Nemzeti Infokommunikációs Szolgáltató Zrt. (NISZ) összesen hat minisztériumnak szolgáltat Microsoft technológiát, akik gyakorlatilag a legmodernebb szoftvereket tudják kínálni. Éppen most zajlik egy széleskörű modernizáció, amely során az XP-t és Office 2003-at Windows 7-re és Office 2010-re cserélik. A többi minisztérium is a Microsoft alkalmazásait használja, de ők maguk oldják meg a beszerzést és az üzemeltetést.[6]

A költségvetésből az informatikára köthető pénz 2012-re 40%-kal visszaesett. Uniós források tekintetében jelentős növekedés van, ám ezeket a projekteket fel kell gyorsítani, hogy az elérhető pénzeket sikeresen elkölthessük. A Microsoft sok más céggel együtt részt vesz ebben. Jelentős fejlődést hozhat például az önkormányzati privát felhő kiépítésére vonatkozó ASP projekt.

Az érintettek szerint a sajtó félremagyarázza a helyzetet, amikor a Microsoft-szoftverek nyílt forráskódú szoftverek elleni csatájaként akarja beállítani ezt a kérdést. A Microsoft szerint is megvannak az állami működésnek azok a területei, ahol a nyílt forráskódú szoftvereknek létjogosultságuk van, amely területeket szakmai érvek alapján kell meghatározni, nem hitvitákkal. Eddig is több helyen használtak nyílt forráskódú megoldásokat, sőt van olyan terület, ahol piacvezetők az ilyen szoftverek. A mostani kormányrendelet inkább csak intézményesíti az eddigi szokásjogot: „írásba adják”, hogy a tágan értelmezett magyar államigazgatásban is megvan az egyes intézményeknek a lehetőségük arra, hogy ilyen szoftvereket használjanak. Egyébként 2008 óta a Microsoft által kidolgozott office open xml (ooxml) a Nemzetközi Szabványügyi Szervezet (ISO) által elfogadott nyílt forráskódú dokumentumformátum.

A Microsoft szerint az informatikai döntéshozók felelőssége, hogy az egyes területeken azt a szoftvert használják, amely leginkább megfelel az igényeknek, és összességében a legnagyobb megtérülést adja. Vannak azonban olyan területei az állami működésnek, kitüntetetten talán éppen az oktatásban, ahol a Microsoft-szoftverek hiánya egyértelműen ártana a diákoknak, rajtuk keresztül pedig Magyarország versenyképességének. Ma már a Microsoft digitális nyelve a világ közös digitális nyelve, s ezt a piaci viszonyok alakították így. Ugyanakkor egy informatikai megoldásnak csupán egyetlen vetülete, hogy a programok forráskódját bárki vagy csak az arra illetékesek tekinthetik meg, fejthetik vissza. A licenckőltségek pedig csak töredékei egy rendszer összköltségének, ily módon egy „ingyenes” licenc bevezetése összességében sokkal drágább is lehet, mint a széles körben használt zárt forráskódú termékeké.

Egyébként az egész szoftverhelyzet olyan messzire jutott, hogy egyre nehezebb kitáncolni belőle. A technológiák ugyanis fejlődnek, terjednek, s ez egy ideig erősíti az innovációt és a társadalmi hasznosságot. Ám elérkeznek egy ponthoz, főleg ha monopolisztikus helyzet áll elő, ahonnét már gátló tényezőként lépnek fel. Jó példák erre a dokumentumformátumok, ahol ha egyeduralkodóvá válik egyetlen termék és kapcsolódó formátuma, akkor ez már akadályozza a fejlődést. Holott az informatika más területein teljesen magától értetődő a választás szabadsága, gondoljunk csak az operációs rendszerekre, köztes rétegekre vagy a szerverhardverekre. Ezért fontos most az a törekvés, hogy visszaálljon a normális helyzet, amely támogatja az innovációt, az interoperabilitást és a költséghatékonyságot. Ám mielőtt

6 Microsoft Magyarország: A Microsoft a kormányzatban; Megoldás Magazin, 2012.05. http://www.microsoft.com/hun/megoldas-magazin/2012/05/fokuszban/a-microsoft-a-kormanyzatban/

belefognánk bármilyen cserébe, erősen ajánlott előre kiszámolni, hogy megéri-e a váltás, még ha ez nem is olyan egyszerű.

Az alternatív irodai programok funkciói, felülete olyannyira hasonlít az MS Office-éhoz, hogy egy gyakorlott felhasználónak nem fog problémát okozni a különbség. Ezen kívül, a közoktatásban vélhetően kevesebb problémával, azaz kevesebb oktatási igénnyel jár majd az egyszerűbb, nyílt forráskódú rendszerre való áttérés, mint a verzióváltás az MS Office 2003-ról 2007-re. Mivel a munka és a külső kapcsolatok jellege erősen befolyásolja a szoftverhasználatot, egyébként sem várható teljes átállás a közigazgatásban – körülbelül 20%-os megmaradás még egészséges arányt jelentene.

## Kétségek

Elsőként triviálisnak tűnhet egy jelentős költségcsökkentés akkor, ha nem kell licencdíjat fizetni, hiszen nem kell megvenni a szoftvert. Ám aki egy kicsit járatos az informatikában az tudja, hogy az összes költségnek csak töredéke a licencdíj. Átlagosan 10-20 százalékkal szoktak számolni, amelyen felül van még a bevezetés, az üzemeltetés, és az esetleges fejlesztések költsége. Egy kevésbé kiforrott rendszer esetén utóbbiak drágábbak lehetnek, azaz elképzelhető, hogy a licenc megspórolása mellett rengeteg plusz költség jelenik meg egy ilyen váltással. Ha ugyanis sok esetben kell belenyúlni a rendszerbe, akkor az plusz humán erőforrást kíván, mikor már bérköltségről beszélünk.

Sok esetben ez hitvitába fajul, de léteznek független számítások, a költségérzékeny magánszektort azonban érdemes figyelni, amely nagyon megnézi, hogy mit választ: a cégek több mint 95%-a Microsoft alapokon dolgozik, azaz a tapasztalatok alapján úgy tűnik, az addicionális költségek meghaladják az ingyenes licenc előnyét.

Az a lényeges, hogy ne az eszközhöz válasszuk a feladatot. A kormányzat a kezdeti lendülete után belátta, hogy elsőként nem a technológiát kell kiválasztani, majd az alapján megvalósítani a rendszert, hanem az adott projekt esetén elsőként meg kell nézni, hogy melyik technológia megfelelő, és melyik biztosítja a legnagyobb költséghatékonyságot, s csak utána érdemes a megvalósításban gondolkodni. Ebbe a hibába egyébként már belefutott több kormányzat is a világon, amely levezényelt egy átállást, majd a plusz költségek miatt visszatértek. Ez több millió eurós veszteséget jelentett számukra, illetve az adófizetőik számára. Ez is egy intő példa volt a magyar kormány informatikai döntéshozói előtt, hogy körültekintőbben közelítsék meg a kérdést.

Komoly aggályai vannak mind az oktatási, mind a közszféra egyéb intézményeinek: kompatibilitási gondok jelentkezhetnek akkor, amikor egy elkészített, makrókkal, láb- és fejlécekkel, képletekkel tűzdelt előadást kell nagy hirtelen nyílt forráskódú programon megnyitni. A szabadon hozzáférhető irodai programokban „szétesik” a megnyitott MS-dokumentum, egészen másként mutatkozik, mint amilyennek létrehozták. Ráadásul a különböző MS Office verziók között is léteznek kompatibilitási problémák. Az ODF remélhetően mindezt ki fogja küszöbölni.[7]

A Nyílt Dokumentum Formátum Szövetség (ODFA) Magyarország ugyanakkor felhívta a figyelmet, hogy a kormányhatározat nem határozza meg egyértelműen, mi is a nyílt szabvány. Egyik kritériuma például az, hogy megvalósítható legyen, de ezt az OOXML nemigen teljesíti, hiszen mind ez idáig egyedül a Microsoft implementálta. Így jobb lett volna csak az ODF-et megjelölni egyértelmű szabványként. A másik gond az, hogy a nyílt forráskódú szoftverek kérdéskörének beemelése a nyílt szabványok közé, illetve a kettő összemosása nem szerencsés dolog, mert enélkül is elég nagy a fogalmi zavar, ami megnehezíti a tisztánlátást az átállásban a két területen.

A formátum kérdése egyébként a digitális tartalmak megőrzése tekintetében is fontos, és stratégiai döntést igényel. Nem mindegy ugyanis, hogy például 10 év múlva miként fogunk hozzáférni a digitális nemzeti adatvagyonhoz – már annak a fényében is, hogy az Európai Unió a közadatvagyonnal való gazdálkodást a nemzeti digitális stratégiák fontos részének tekinti. Ebből a szempontból pedig egyértelműen a formátum a lényeg, nem pedig a szoftver vagy az adathordozó eszköz.

7 Mártonffy Attila: Tisztázott, nyílt helyzet?, IT-business, 2012.02.21., http://www.itbusiness.hu/Fooldal/hetilap/cimlapon/Tisztazott_nyilt_helyzet.html

Persze, fontos a költséghatékonyság is, ám egy közelmúltban napvilágot látott Gartner-jelentés rámutat, hogy az általa megvizsgált cégek a nyílt formátumoknak – azok használhatósága, rugalmassága stb. miatt – inkább stratégiai, mint költséghatékonysági jelentőséget tulajdonítanak. Ez utóbbival kapcsolatban egyébként még az sem tisztázott, hogy a nyílt formátumok és szoftverek révén megtakarított pénz vajon visszaáramolhat-e a jelenleg elég alacsony szinten álló informatikai oktatásba.

A támogatók szerint azért kellenek a nyílt szabványok, mert átjárást biztosítanak a különböző rendszerek között, s ezt az együttműködést legkönnyebben és legolcsóbban nyílt szabványokkal lehet elérni. Az ODF-et már 6-7 nagy szoftverrendszer implementálta, míg az OOXML-t valójában még a Microsoft sem igazán – így aztán legfeljebb csak saját magával lehet kompatibilis. Ezért a határozatban megfogalmazott interoperabilitási kívánalomnak igazán csak az odf felel meg.

Mások is megkérdőjelezik a nyílt formátum rövid távon elérhető költséghatékonyságát. Ugyanis ha teljesen más rendszerekre térünk át a jelenlegiekről, szükséges egy bizonyos tudásbázis, szakembergárda, amely átsegíti a felhasználókat a változáson.

## Önkormányzati projektek

Egyre több önkormányzat vág bele a szabad szoftverekre való átállásba. A kormányzatot is foglalkoztatja a váltás, ám egyelőre még csak kísérleteznek, próbaprojekteket folytatnak egyes belső kormányzati szervekben, de konkrét segítséget nem nyújtanak az önkormányzatoknak. Pedig számtalan tényezőtől függhet az elérhető megtakarítás.[8]

Kellenének referenciák, mielőtt a hivatalok a már egységesen lezajlott szerveroldali átállás után a napi működésükbe integrálják a nyílt forráskódú rendszereket. Azonban nemcsak Magyarországon, hanem nemzetközi viszonylatban sem elérhetők korrekt, minden szempontra kiterjedő esettanulmányok. Emellett sokan úgy érzik, hogy a kormányzat magukra hagyja őket, és meglepő módon egymást sem nagyon segítik. Minimális közöttük az együttműködés, formális információcsere egyáltalán nincs. Ezt a hiányt szeretné pótolni egy jelenleg zajló kutatás, melynek eredményei várhatóan július elejétől nyilvánosak lesznek. (A projekt második szakasza ősszel fog megkezdődni, a közoktatási intézményeket fogja érinteni.)

A kutatócsoport olyan, nagyobb településeken található önkormányzatokat keresett meg, amelyek már megküzdöttek az átállással. Bár a felmérésben az ország minden régiója képviselteti magát, a cél nem a reprezentativitás, hanem a felmerülő problémák és megoldások alapos összegyűjtése. Példamutatóak lehetnek a Budapest XVIII. kerület és Szeged polgármesteri hivatalainak tapasztalatai. Ezek az intézmények úttörőnek számítanak a területen, és nagy elszántsággal, sikeresen építették fel nyílt rendszereiket.

Ami a félúton tartó (a kérdőívek felvétele után és a mélyinterjúk előtt álló) kutatásból már most is látszik, hogy nem egységesek a motivációk a nyílt forráskódú szoftverekre való áttérésre, és a megvalósításban is különböző utak léteznek. Jellemző tapasztalat, hogy egy vagy néhány informatikus pontos ütemterv híján és anélkül vágott bele a váltásba, hogy átlátta volna, mindez pontosan mennyi időt és munkát igényel. Ilyenkor a feladat rendszerint túlnőtt rajtuk, előbb-utóbb szinte vállalhatatlan terheket róva rájuk. Másik gyakorlat, hogy a projektbe valamilyen, piaci alapon működő informatikai szolgáltatót is bevonnak, aki tanácsadással, a szoftverek kiválasztásában, a beszerzésben, illetve a dolgozók képzésében nyújt segítséget.

Egyértelműen hasznos a felhasználók számára a nyílt forráskódú irodai programcsomag, a népszerűséget az biztosítja, hogy egyaránt fut Linux és Windows alatt, a megbízhatóságot pedig a forráskód stabilitása szavatolja. A nyílt és a hasonló funkciójú, zárt forráskódú termékek ma már egyenrangúnak tekinthetők, felhasználói táboruk egyforma nagyságú.

A szabad hozzáférésű csomagok terjedése a kis- és középvállalatok mellett különösen az önkormányzatok körében figyelhető meg. Használatuk elsajátítása nem ütközik különösebb akadályba, ezt a logikus

8 Szeli Katalin: Magányos harc a „szabadságért”, IT-business; 2012.05.30. http://www.itbusiness.hu/Fooldal/hetilap/business/Maganyos_harc_a_szabadsagert.html

elrendezésű grafikus felület is biztosítja. Átlagos felhasználás esetén kompatibilitási problémák sem merülnek fel a zárt forráskódú rendszerekkel.

A nyílt programok ár-érték aránya sokkal kedvezőbb a zártakénál, egyes vélemények szerint intézményi alkalmazásukkal legalább 50%-os megtakarítást lehet elérni – ami fontos tényező önkormányzatok esetében.

Eltérő az átállás következtében történő költségmegtakarítás megítélése az önkormányzatok részéről. Van, ahol néhány milliós nagyságrendű spórolásról számolnak be, de az is előfordul, hogy egyáltalán nem érzékelnek költségcsökkenést. Problémát jelent azonban, hogy a költségek számítására nincs egységes módszer, kérdés például, hogy milyen időtávban gondolkodnak, vagy beleértik-e például a képzést.

Egy nyílt forráskódú szoftver önmagában nem képez üzleti értéket, inkább eszköz, de hatalmas potenciállal. Ennél fogva körültekintően kell belevágni az átállási projektekbe. Ha egy szervezet azért kezdi el az átállást, mert sürgősen meg kell újítania meglevő szoftvereit, de nincs pénze rá, s úgy gondolja, a nyílt forráskódú programok segítenek a „bajban", akkor csak tűzoltást fog végezni, hosszú távon nem jut semmire. S ez nem a nyílt forráskód hibája – a költséghatékony megoldáshoz idő (és némi pénz is) kell.

Egy átállási projektben ugyanis mindenekelőtt rögzíteni kell az elvárásokat, majd meg kell vizsgálni, megvalósíthatók-e. Ez általában nem megy belső erőforrásból, mivel sok tapasztalat és nagy tudás kell hozzá. Aztán számba kell venni a szükséges kompetenciákat és erőforrásokat. Nem árt, ha azt is tudjuk, ki, mire fogja használni a szoftvert, s az új rendszert a szükséges funkciók és folyamatok alapján kell felépíteni. Ott pedig, ahol a nyílt forráskód nem tud üzleti értéket létrehozni, nem kell erőltetni bevezetését.

Az anyagi előnyök mellett a nyílt rendszerek gyorsaságát, a szervezetben folyó információáramlás felgyorsulását is kiemelték a válaszadók. A kutatás vezetője egy másik, kevésbé megfogható, pénzben ki nem fejezhető, lehetséges hozadékra is felhívja a figyelmet: a szabad szoftverekre való átállás során a szervezet – a hatékony működéshez létfontosságú – változási készségre, rugalmasságra tehet szert, amit bármilyen területen, akár egy jogszabályhoz való alkalmazkodásban is kamatoztathat.

# Felhő alapú szolgáltatások

A felhasználók azt várják az informatikai szolgáltatásoktól, hogy azonnal válaszoljanak a problémákra, legyenek interaktívak, kapcsolják össze azokat, akiket kell, valamint folyamatosan lehessen hozzájuk férni. A technológiavezérelt szolgáltatások fontosabbak, mint valaha, s ezek érvényesülését nagyban szolgálhatják a hibrid megoldások.

Az elmúlt években megváltozott a gazdasági szereplők magatartása, piaci stratégiája. Nőtt a kockázatkerülés, ami olyan új üzleti konstrukciók kiválasztására ösztönzi a döntéshozókat, amelyek gyorsan, rugalmasan indíthatóak, könnyen bővíthetők vagy csökkenthetők, és akár különösebb anyagi veszteség nélkül meg is szüntethetők.[9]

## A szükséges mozgékonyság

Eddig az intézmények a működésükhöz szükséges IT-infrastruktúrát a telephelyükön, saját tulajdonú és többnyire saját működtetésükben lévő eszközökből építették ki. A jelenlegi gazdasági-technológiai környezetben azonban előnyösebb lenne olyan, stabil anyagi és műszaki háttérrel rendelkező szolgáltatóktól igénybe venni az IT-infrastruktúrát, amelyek használatarányos szolgáltatási díj ellenében kínálják. A működési modellek közötti átállás fokozatosan történhet; hatására megjelenik a hibrid vállalati infokommunikáció, azaz amikor az on-premise (az ügyfél saját telephelyén levő) és a szolgáltatásként igénybe vett megoldások együttesen biztosítják a szükséges funkciókat.

A szolgáltatásokat pedig manapság egyre inkább a felhőből vesszük igénybe. A felhő alapú IT biztosítja a vállalatoknak a szükséges mozgékonyságot, és segít kialakítani az IT-szolgáltatások megfelelő portfólióját a releváns forrásokból. Technikai és irányítási szempontból ugyanakkor a hibrid ICT világa sokkal

9 Mártonffy Attila: Felhőkoktél, IT-business, 2012.05.15., http://www.itbusiness.hu/Fooldal/hetilap/cimlapon/Felhokoktel.html

összetettebb, mint a hagyományos. Az ICT-támogatást különböző forrásokból alakítjuk ki, saját eszközökből, nyilvános felhő-szolgáltatásokból, de egyes területeket részben vagy teljes egészében ki is szervezhetünk. Olyan munkafolyamatok jelennek meg és válnak hétköznapivá, amelyek egy része valamilyen felhőben, míg másik része saját, helyi rendszerekben fut.

## Szállítók

Számos IT-szervezet nyilvános felhő-szolgáltatásokat vesz igénybe nem kritikus megoldásként. Ilyenek például a fejlesztési és tesztalkalmazások. Szabványos szoftvereket használnak szolgáltatásként (saas) például webelemzéshez és a CRM-hez. Ez utóbbiaknak az az előnyük is megvan, hogy a mobil munkaerő könnyebben veheti igénybe őket.

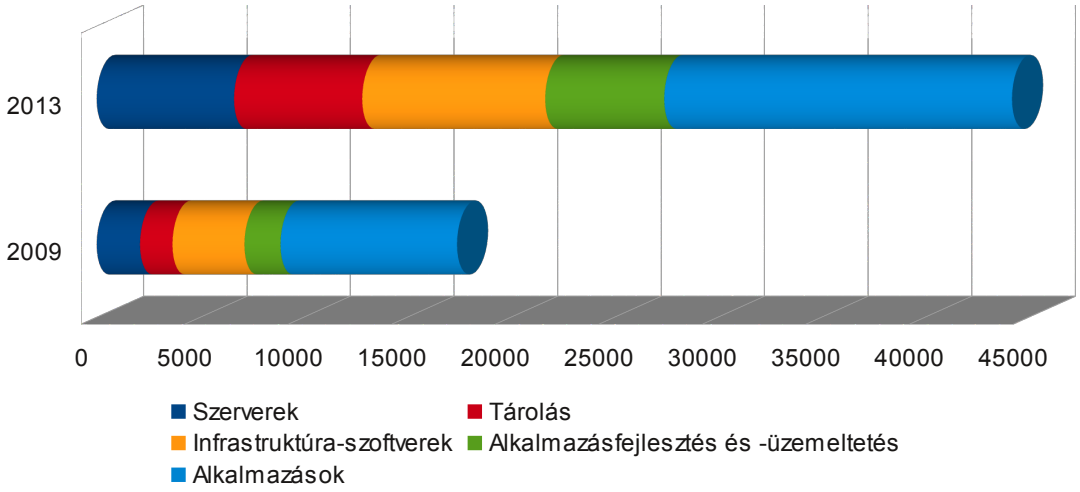
Kritikus alkalmazásokhoz és adatokhoz azonban a cégek vonakodnak nyilvános felhőből igénybe venni szolgáltatást, mivel nem tartják biztonságosnak, nem adaptálhatók a menedzsment igényeihez, vagy nem szavatolják a szünetmentes hozzáférést. Így az IT-szervezetek inkább saját, belső IT-szolgáltatásokat tartanak fent ezeknek az alkalmazásoknak az elérésére.

## Tőkeigény csökkentés

A felhő a Gartner piacelemző cég szerint átszabja az IT-architektúrákat, sőt magának az IT-nek a szerepét is megváltoztatja. A felhőszámítás ugyanis már valóság, s egy idő múlva a számítási feladatok ott futnak majd, ahol optimális: a magán- vagy nyilvános felhőben, vagy hibrid IT-környezetben. Az informatikusoknak az lesz a dolguk, hogy összeszedjék a megoldásokat az elérhető szolgáltatóktól, beleértve saját magukat is. A külső és belső szolgáltatók „gyűjteménye" megteremti a funkciók piacát – olyan funkciókét, amelyek könnyen csereberélhetők a szolgáltatási szerződésekben aszerint, hogy éppen mit követel az üzletpolitika. Ebben a forgatókönyvben az IT komplex, heterogén szállítási lánccá válik, amelyet közvetítői szerződések irányítanak.

Amikor azonban az IT-szervezetek megvizsgálják a potenciális felhőszolgáltatásokat, kiderül, hogy a piac sérülékenysége miatt nem minden felhőszolgáltatást azonos módon hoztak létre. Néhány szolgáltató kulcsrakész terméket kínál, amely esetleg helyettesítheti egyik-másik belső szoftvert. Más szolgáltatók viszont felhőszolgáltatások széles körét teszik ki az asztalra, különböző szintű biztonsággal, hozzáféréssel, árral és méretezhetőséggel. Ezek vagy megfelelnek vagy nem az alkalmazás technikai követelményeinek, az IT-megfelelés irányvonalainak vagy a cég kockázattűrő képességének.

Felhőszolgáltatások glogális bevételei terméktípusonként 2009/2013. (millió USD)




Forrás

## A felhő biztonsága

Bármennyire is elismerik az informatikusok, sőt lassan már az üzleti vezetők is a felhőszolgáltatások előnyeit, a bevezetés egyik legnagyobb akadályát továbbra is a biztonsági aggodalmak jelentik. Hiába hangoztatja minden szolgáltató, hogy nála aztán minden adat biztonságban van, egyetlen intézmény sem adja oda szívesen bizalmas, feladatkritikus vagy csak egyszerűen fontos(nak tartott) adatait egy külső szolgáltatónak, amely aztán egy ki tudja hol lévő adatközpontban, ki tudja milyen körülmények között tárolja azokat.

A számítási felhőkkel kapcsolatban az alábbi kockázati tényezőket szokták a leggyakrabban emlegetni:

- hálózati kapcsolat: ha az adatok bármilyen okból nem elérhetők, az üzletmenet leáll;
- végpontok biztonsága: a felhő könnyen elérhető mobileszközökről is, amelyek biztonságára viszont korántsem fordítunk kellő figyelmet;
- adatbiztonság: az adatoknak nemcsak folyamatosan elérhetőknek kell lenniük, hanem garantálni kell, hogy a szükséges ideig változatlan formában fenn is maradnak;
- adatvédelem: garantálni kell, hogy csak az férhet hozzá az adatokhoz, akinek erre jogosultsága van;
- ellenőrzés: a felhasználói jogosultságkezelés, az eszközök beállításai, a szabályrendszerek kialakítása több odafigyelést igényel.

A helyzet valóban ellentmondásos. Egyfelől igaz, hogy a felhőszolgáltatásokat kínáló vállalatok többsége komolyan veszi a biztonság minden aspektusát. Mivel pedig ebből élnek és hatalmas adatközpontokat üzemeltetnek, elemi érdekük, hogy a létező legjobb fizikai és informatikai védelmi rendszereket alkalmazzák.

Ennek megfelelően védelmi intézkedéseik és biztonsági szakembereik felkészültsége messze meghaladja azt, amit ügyfeleik többsége valaha is megengedhetne magának. Másfelől viszont azt sem lehet tagadni, hogy nem minden szolgáltató egyforma, mint ahogy azt sem, hogy előfordultak már adatvesztések, szolgáltatáskimaradások.

Ahogy a hagyományos informatikában, a felhőszolgáltatások esetében is a technológia, a folyamatok és az emberek hármasán múlik a biztonság. A kérdés csak az, hogy a felhasználó miként tud meggyőződni választott szolgáltatója biztonsági felkészültségéről. Ebben segíthetnek a már alakulóban lévő iparági ajánlások, mint például a CSA Guidance, de van néhány kérdés, amelyeket érdemes lehet feltenni a potenciális felhőszolgáltatónak. A válaszokból már elég jól fel lehet mérni, mennyire is veszi komolyan az információbiztonságot a szolgáltató.

A közszféra leginkább saját felhő alapú szolgáltatóközpontok létrehozásában gondolkodik. Ebben az esetben mindenképpen szem előtt kell tartani az alábbi biztonsági követelményeket.[10]

### 1. Titkosítás

Nem elég az illetéktelen hozzáférés elől jelszóval védeni az állományokat, vagy csak a mozgásban lévő adatokat titkosítani, tárolás közben pedig szabadon hagyni. A mindenre kiterjedő védelem egyik talpköve, hogy az adatot mindenkor és mindenhol (a tárolás helyén, átvitel közben és lehetőleg a felhasználó eszközén is) titkosítani kell. A titkosítatlan adatok elvesztése komoly jogi szankciókkal is járhat. Ha pedig már titkosítás, nincs értelme alább adni a 256 bites AES technológiánál, de igény szerint ennél erősebb kulcsok is elérhetők.

10 Schopp Attila: Kérdések a biztonságért; IT-business; 2012.05.07. http://www.itbusiness.hu/Fooldal/hetilap/tech/Kerdesek_a_biztonsagert.html

**2. Titkosító kulcsok**

A titkosítás nehézsége nem is annyira az adatok kódolásában rejlik, mint inkább a titkosító kulcsok kezelésében. A kulcsokat nemcsak logikailag, hanem fizikailag is el kell választani a velük titkosított adatoktól – az a legjobb, ha egy egészen másik adatközpontban tárolják őket, így nincs egyetlen gyenge pont.

Arra sem árt figyelni, hogy ugyanannak az alkalmazottnak ne legyen hozzáférése mind a kulcsokhoz, mind a titkosított adatokhoz.

**3. Redundancia**

A felhasználók elvárása, hogy minden adatuk azonnal és hiba nélkül a rendelkezésükre álljon. A szokásos szolgáltatói vállalás (99,999%-os rendelkezésre állás) az elérhetőségre jó lehet, de az adatmegőrzésnél ennél többre lehet szükség. A szokásos adattükrözés (két merevlemezen tárolják az adatot) nagyjából 99,99%-os biztonságot nyújt: várhatóan minden 10 ezer állományból elvész egy. Ha tényleg nélkülözhetetlen adatokról van szó, ragaszkodjunk ahhoz, hogy adatainkat több, egymástól távol eső adatközpontban tárolják, mindenütt legalább három példányban, és ezek között azonnali és automatikus legyen a szinkronizáció.

**4. Ellenőrzés az adatok felett**

Az ügyfélnek teljes kontrollt kell kapnia az adatai felett, legyen szó azok létrehozásáról, feltöltéséről, tárolásáról, megosztásáról és a végén a törléséről.

A szolgáltatónak garantálnia kell, hogy az ügyfél munkatársai képesek a távolból véglegesen törölni állományokat és mappákat a felhasználók eszközeiről, vagy megszüntetni egy-egy felhasználó hozzáférését az adatokhoz. A szolgáltatóval együtt fel kell készülni azokra az eshetőségekre is, amikor az adat illetéktelen kezekbe kerül.

**5. Jelszókezelés**

A gyenge, átlagos, könnyen kitalálható jelszavak minden informatikai rendszer leggyengébb pontját jelentik. Ha a felhasználóknak újabb név–jelszó párost kell megtanulniuk a felhőszolgáltatások igénybevételéhez, valószínűleg a legkisebb ellenállást választják. Akkor már jobb, ha a szolgáltatást a meglévő – és például az Active Directoryban tárolt – jelszavakkal lehet igénybe venni. Ha a felhő integrálható a már kialakított jelszó- és felhasználó-azonosítási eljárásrenddel, a kockázat csökkenthető.

**6. Adat szeparáció**

Úgy tudják hatékonyan kihasználni erőforrásaikat a felhőszolgáltatók, hogy egy fizikai szerveren több virtuális gépet alakítanak ki, és azzal több ügyfelet is kiszolgálnak. A virtuális szerverek, valamint a rajtuk futó alkalmazások és adatok csak logikailag vannak szétválasztva, ezért aztán rendkívül fontos, hogy a szolgáltató hogyan menedzseli a virtuális erőforrásokat. Senki nem szeretné, ha adatai egy másik szervezet dolgozói számára lennének elérhetők.

**7. Naplózás**

A szolgáltatónak teljes naplózást kell folytatnia minden, az ügyfelet érintő változásról, hogy a változások nyomon követhetők legyenek.

**8. Skálázhatóság**

A felhő egyik nagy előnye, hogy a szolgáltatási kapacitást az igényeknek megfelelően lehet alakítani. Ha az ügyfél a terhelés gyors növekedésére számít (akár új felhasználók, akár még több adat miatt), győződjön meg arról, hogy a szolgáltató később is képes lesz kielégíteni igényeit.

## Konkrét lépések a felhő irányába

Nemrég megjelentek az Elektronikus közigazgatás operatív program (EKOP) 2011-2013. első pályázatai, amelyek régiónként kb. 1-2 milliárd Ft-ot irányoznak elő önkormányzati zárt, ASP-alapú felhőszolgáltatások megvalósítására.[11]

A támogatást elnyerő önkormányzat létrehozza az ASP központot és vállalja önkormányzatok csatlakoztatását, akik az igénybe vett szolgáltatásokért díjat fizetnek. Minimálisan 50 település fog csatlakozni egy központhoz, amelynek a régió lakosságának legalább 30%-át le kell fednie.

A központ a csatlakozó önkormányzatok számára az alábbi alkalmazásokat szolgáltatája:

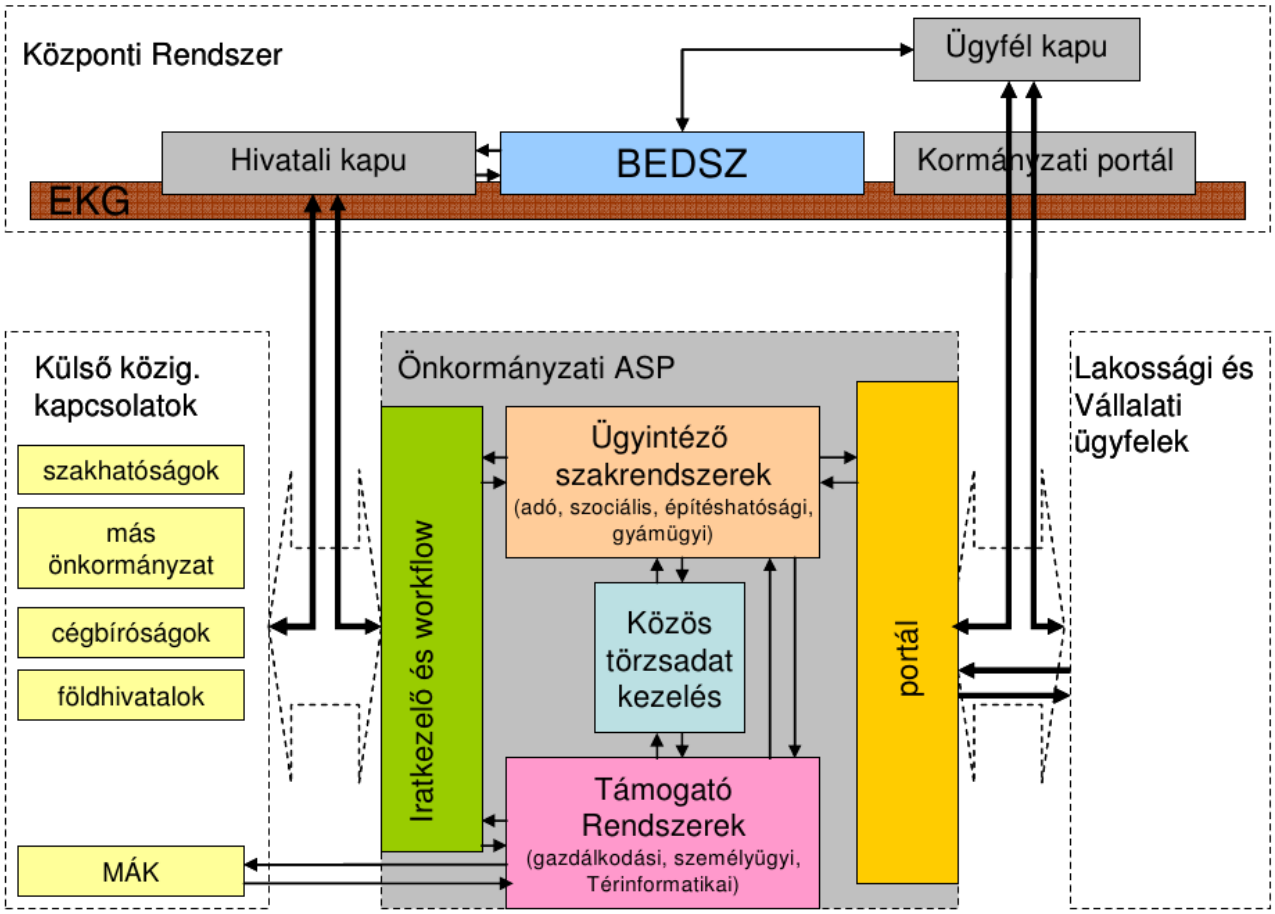
1. iratkezelő- és workflow rendszer,
2. önkormányzati portál rendszer,
3. szociális igazgatási rendszer,
4. adóügyi alkalmazás,
5. ipari és kereskedelmi igazgatási rendszer,
6. építéshatósági rendszer,
7. gazdálkodási rendszer,
8. gyámügyi rendszer,
9. testületi munka támogató rendszer.

Az új ASP-központok kialakításához természetesen teljes körű szolgáltatás-menedzsment rendszert is ki kell alakítani. Ennek tartalmaznia kell:

- Szolgáltatási szint biztosítás (SLA-k), és szolgáltatásjelentés
- Kapacitásgazdálkodás
- Rendelkezésre állás menedzsment
- IT szolgáltatásfolytonosság menedzsment
- Konfigurációkezelés
- Változáskezelés
- Kiadáskezelés
- Incidenskezelés
- Problémakezelés
- Alkalmazás és infrastruktúra üzemeltetés
- Információvédelem
- Szolgáltatásértékesítés és bevezetés

11 EKOP-3.1.6 Önkormányzati ASP központ felállítása, http://www.nfu.hu/doc/3459

Természetesen a kiépülő adatközpontoknak csatlakozniuk kell a már meglévő e-közigazgatási infrastruktúrához. Architektúrájuk a következőképpen került felvázolásra:




Az adatközpontok teljes körű tervezési, fejlesztési, megvalósítási és üzemeltetési feladatai a pályázót terhelik.

Látható tehát, hogy komoly szakértelmet és felkészültséget igénylő feladatot jelent az új struktúra kialakítása. Ám a felhőszolgáltatások valós közigazgatási megjelenése kézzelfogható közelségbe került.

## E-egészségügy

Elkelne az optimális tervezés az e-egészségügyben is. Általános vélekedés szerint – az iparvállalatokhoz, a kereskedelemhez vagy a pénzügyekhez hasonlóan – az egészségügy is olyan terület, amelyet informatikai támogatással hatékonyabbá, olcsóbbá lehet tenni. Azonban a Harvard Medical School egy korábban elvégzett felmérése szerint nincs kimutatható összefüggés a kórházak informatizáltsága és a költségek, valamint az ellátás minősége között. A jelentés megállapítja: miközben a kórházak informatikai ellátottsága folyamatosan növekedett a vizsgált években, az adminisztrációs költségek terén nem volt kimutatható csökkenés hosszabb távon sem.[12]

A hazai tapasztalatok is igazolják ezeket az eredményeket. A szakemberek szerint az egészségügy voltaképpen csodát vár, amely megold minden gondot. Az ágazat mindeddig nem igazán fogalmazta meg igényeit, inkább az informatika próbál az egészségügyre tukmálni megoldásokat. Ettől még lokális igények felmerülhetnek, ám helyi szinten nincs sok értelme a dolognak, mivel az informatika csak társadalmi szinten, átfogóan tudna segíteni.

12 Mártonffy Attila: Virtualizált egészségügy csodavárással, IT-business, 2012.02.29., http://www.itbusiness.hu/Fooldal/hetilap/kiadvanyok/BT_2012/Virtualizalt_egeszsegugy_csodavarassal.html

A célok: a kapacitások, erőforrások, költségek optimális elosztása, illetve tervezése, az alternatívák számszerűsítése – objektív, rendszerszerű döntések és megoldások kezelésével. Eredmény lenne még a várólisták rövidülése, a betegutak, a betegszállítás, a beszerzések optimalizálása, a trendek megmutatása stb. Az egészben az a szomorú, hogy mindehhez ma már minden adott.

## Az informatika szerepe

Az informatika azt is meg tudná mondani, hogy mennyire van szüksége az egészségügynek egy bizonyos egészségi állapot fenntartására. Ha valamennyi százalékkal növekedne az aránya a GDP-ben, akkor mennyivel tudna többet kihozni a rendszerből társadalmi szinten. Azaz az OEP szintjén, ahol az IT a pénzelosztás optimalizálására lenne alkalmas, ha a rendszerszerű elveket alkalmaznánk, s nem a szokásjog alapján: hogy ki mennyire képes kilobbizni a pénzeket a saját szervezetének a kasszájára.

Azért küzd már két évtizede minden egészségügyi kormányzat, hogy matematikailag kiszámítható legyen a tényleges kapacitások elosztása – ám ez rengeteg érdeket sért.

Ilyen körülmények között nem csoda, ha az ágazatnak nincsenek speciális IT-igényei. Bár szeretné mindenki azt mondani, hogy igen, mert ebből lehetne pénzt csinálni meg kompetenciát misztifikálni. Sztenderd igények léteznek sztenderd megoldásokkal, s míg más ágazatokban az informatikát elfogadják mint a tényleges működés támogatásának, mérésének és vezérlésének egyik fontos eleme, addig az egészségügyben az IT-t inkább szükséges rossznak tekintik.

Magyarországon a kórházak többségében még ma is hiányosak az adatbázisok, lassúak és korszerűtlenek a rendszerek. Az esetek túlnyomó többségében nem teszik lehetővé, hogy az adatokat strukturáltan, közvetlenül a páciensheznek rendelve tárolják. Pedig ez nagyban megkönnyítené az intézményközi információs rendszer modelljének a kialakítását a betegadatok cseréjében. Eszerint az egyes intézményi nyilvántartásokat összekötnék egymással, így a korábbi, illetve más intézményben rögzített információk lekérdezhetővé válnának.

Július elsején indul az országos online várólista-nyilvántartási rendszer, amelynek segítségével bárki nyomon követheti, hogy különböző műtétekre hányan várakoznak országszerte, az egyes térségekben, illetve adott intézményekben. A beteg választása az elsődleges és a pénz csak utána következik. Amikor az országos nyilvántartásban azt látja majd az OEP, hogy például gerincműtétre az egyik intézményben 50 nap a várakozási idő, míg egy másik intézmény listáján sokkal több beteg mellett 250 nap a várakozási idő, akkor ahhoz az intézményhez teszik a kapacitást, amelyhez a betegek ragaszkodnak.

Az OEP által kezelt új rendszerben meg tudják majd nézni azt is, hogy a várólistán tartózkodás 250 napja alatt mennyit kellett a terápiára költeni, a betegnek mennyi fájdalomcsillapítóra, gyógyszerre volt szüksége, milyen krónikus ellátásban részesült, illetve mennyi táppénzes napot vett igénybe. Az ezekre fordított költségeket összemérik a műtéti, illetve az annak elvégzéséhez szükséges költségekkel. A főosztályvezető szerint ennek eredménye az lehet, hogy az OEP-nek jobban megéri, ha az intézménynek a műtétek elvégzésére adnak többletforrást.[13]

## Telemedicina

Mivel az informatika innovatív ágazat, az egészségügyben is szeretné megtalálni a helyét, még ha nem is vehet részt az alapproblémák megoldásában. Ezért fordul például a telemedicina felé, amely sajnos, nálunk nem épül be az ellátórendszerbe.

Pedig az ellátórendszer Magyarországon (is) anyagilag egyre nehezebben birkózik meg az idősödő lakossággal s az ennek nyomán növekvő számú beteggel. Itt segíthetne a távközlésen alapuló telemedicina; ugyanis távgyógyítással költségmegtakarítás érhető el, s nem utolsósorban az orvos előbb felismerheti a kockázati tényezőket. Az új technológiai lehetőségek közé tartoznak az időskorúak, a rehabilitációra, gondozásra szorulók életét felügyelő rendszerek, de ide sorolhatók a

13 Jaksa Renáta: Az e-egészségügy helyzetének nemzetközi áttekintése, 2012.06.14. www.infoter.eu/attachment/0012/11076_jaksa_renata.pdf

járművezetők, sportolók és más szabadidős tevékenységeket végzők életfunkcióit vagy a veszélyes munkahelyeken dolgozók tevékenységét monitorozó rendszerek, sőt az intelligens épületek, intelligens otthonok is.

Egyre jelentősebb kérdésnek számít társadalmunkban a népesség elöregedése, ugyanis amíg napjainkban közel 3,2 millió nyugdíjas korú állampolgár él hazánkban, addig várhatóan ez a szám öt éven belül 4,5 millióra duzzadhat. Mivel a kórházi ellátás korlátok közé van szorítva, rövid időn belül nőni fog az igény az otthonápolásra. Először a kilencvenes évek közepén született meg a szociális igazgatásról, és a szociális ellátásról szóló törvény hazánkban, amely kitér e szolgáltatásra is. A törvényalkotás célja akkor az volt, hogy az időskorú, vagy más okok miatt gondozásra, felügyeletre szoruló személyek ápolását lehetőség szerint – költség-, és helytakarékossági megfontolásból – ne közintézményben folytassák, hanem az ellátottakat saját otthonukban gondozzák.

A telefonáló, helymeghatározó és segélykérő funkciók mellett már arra is lehetőséget nyújtanak a modern készülékek, hogy a gondozott személy bluetooth segítségével egészségügyi mérőkészülékeket (például vérnyomás-, vércukor mérő, testsúlymérleg, hőmérő, pulzoximéter, mobil ekg) csatlakoztasson a telefonhoz. Az adatok tárolásában felhőszolgáltatások nyújtanak segítséget.[13]

Az első komolyabb ilyen témájú projekt jelenleg indul MOHAnet és az osztrák gyökerekkel rendelkező – és a magyarországi idősápolásba beszállni szándékozó – Hilfswerk Hungary (HH) közös gondozásában.[14]

## Üzemeltetés

Egy ilyen korszerű rendszert egy kórház önmaga képtelen hatékonyan és megfelelő szakmai felkészültséggel üzemeltetni, ezért jó megoldás lehet az outsourcing. A kiszervezett, bérelt informatikai megoldások ráadásul már középtávon is nagy valószínűséggel kevesebbe kerülnek, mint a saját infrastruktúra fenntartása.

## E-recept, e-dokumentumok

A háziorvos a számítógépéből kinyomtatja, és a beteg, mint adatátviteli közeg, elviszi a receptet a patikába… Ez a közeljövőben elektronikussá válhat. Az e-recept egyrészt kiváltja a papírt, de a lényeg az, hogy az adatok elektronikus kezelése révén jobban lehet ellenőrizni a gyógyszerköltségeket, valamint javítani lehet a medicinák és a betegek biztonságát.

A helyzetet tovább bonyolítja, hogy a jelenlegi törvényi szabályozás értelmében a dokumentumokat 30–50 évig meg kell őrizni. Gondolható, hogy röntgen- vagy más képi diagnosztikai adatok esetében ez mekkora tárolókapacitást és informatikai infrastruktúrát igényel! Ugyanakkor egy modernizált infokommunikációs hálózat lehetővé teszi, hogy az adatokat külső adatközpontban helyezzék el. Ha pedig a kórházak mindehhez optimalizálják a saját és külső (bérelt) tárhelyek arányát, jelentősen csökkennek a beruházási költségek, illetve olcsóbbá és megbízhatóbbá válik a teljes rendszer.

Van még két papír, amit „elektronizálni” lehet. Az egyik a kórlap. Az e-kórlap bevezetésével az adatok egyből az informatikai rendszerbe kerülnének, megkönnyítve és hatékonyabbá téve a feldolgozást az egészségügyisek számára. A másik az elektronikus társadalombiztosítási azonosító jelet (e-TAJ) tartalmazó kártya. Ennek a koncepcióján már régóta rágódik a kormányzat.

Pillanatnyilag az egészségügyi ágazat úgy gondolja, hogy legjobb, ha az e-TAJ-t a Nemzeti Egységes Kártyarendszer keretében fejlesztendő állampolgári kártyára integrálja. A kártya nem hordozna egészségügyi adatot, csupán az azonosítást szolgálná.[15]

14 Deák Miklós: Forradalmasítaná az idősgondozást a MOHAnet, IT-business; 2012.05.23. http://www.itbusiness.hu/Fooldal/hirek/ict_n/mohanet_hilfswerk.html

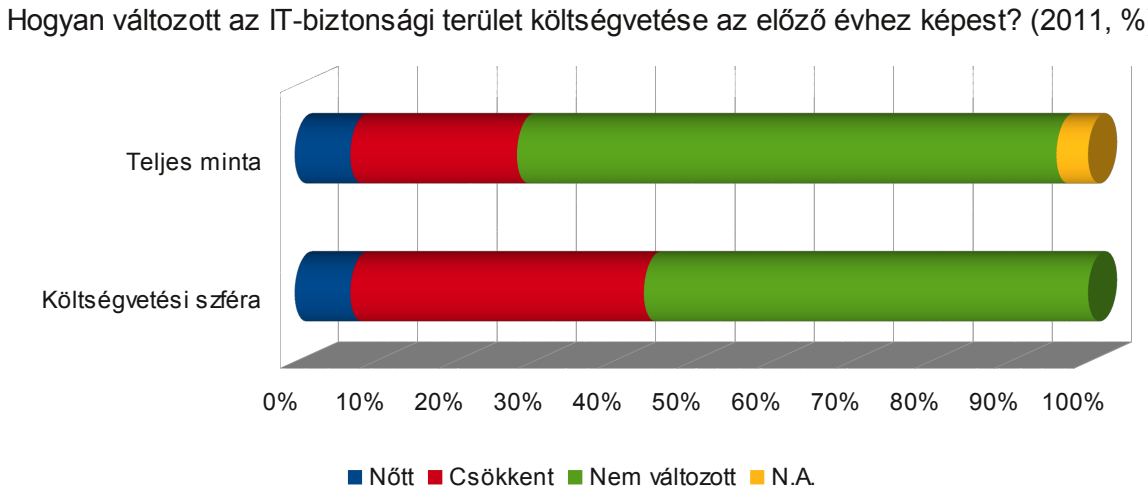
15 Jaksa Renáta: Az e-egészségügy helyzetének nemzetközi áttekintése, 2012.06.14.

# A közszféra informatikai biztonsága

## Magyarország

2011. végén az ISACA magyarországi szervezete a BellResearch kutatóintézettel közösen készített átfogó felmérést a magyar vállalati és költségvetési szféra informatikai biztonsági helyzetéről.

A tanulmányból világosan látszik, hogy a teljes mintában 21%-uknál csökkent 2011-ben az információbiztonsági terület költségvetése az előző évihez képest, míg növekedésről csak 7% számolt be. Az állami kiadások visszaszorításának következtében a költségvetési szférában még ennél is rosszabb a helyzet, az intézmények 37%-a volt kénytelen csökkenteni az IT-biztonsággal kapcsolatos kiadásait.[16]




*Forrás*

A költségvetési intézmények az átlagosnál alacsonyabb arányban rendelkeznek információbiztonsági stratégiával és katasztrófaelhárítási tervvel, kisebb hányaduknál található kifejezetten az információbiztonságért felelős vezető, az információbiztonsági területnek ritkábban kell beszámolnia tevékenységéről, mint a magánszférában, és az átlagosnál nagyobb mértékben csökkent 2011-ben az információbiztonsági költségvetésük is.

A biztonságért felelős vezetők jóval kisebb súlyát mutatja az is, hogy a költségvetési szféra intézményeinek nagy részében egyáltalán nincs rendszeres beszámoltatás az IT-biztonsággal kapcsolatban, nincsenek kitűzve a megfelelő beszámolási formák, pl. kulcs-teljesítménymutatók sem. A költségvetési szféra intézményeinek mindössze 15%-ánál jellemző a legalább havi, vagy annál rendszeresebb beszámoltatás.[17]

Az intézmények / vállalatok közel 40%-ánál történik rendszeresen mély IT kockázatfelmérés és további 34% tervezi ennek bevezetését. Ebben a kérdésben nincs jelentős különbség a költségvetési és a magánszféra között.

Komoly IT audit nehezen képzelhető el kockázatelemzés nélkül. A megfelelő IT kockázatfelmérés hiányában, amely feltárhatná, hogy milyen speciális kockázatok állnak fenn, a belső- és IT-auditorok gyakran inkább a „kényelmesebb" területekre fókuszálnak (pl. általános IT kontroll). Ezt felismerve a kockázatelemzés a belső IT auditálást végző cégek immár mintegy kétharmadánál megjelenik. Az esetek döntő többségében a kockázatelemzés tisztán kvalitatív vagy vegyes alapon történik, a tisztán kvantitatív módszertant használó kockázatelemzés viszonylag ritka. A kockázatelemzés minden előnye ellenére is lényegesen kevésbé számít elterjedtnek a költségvetési

www.infoter.eu/attachment/0012/11076_jaksa_renata.pdf

16 Bellresearch: Magyar Infokommunikációs Jelentés 2011.

17 Bellresearch: Magyar Infokommunikációs Jelentés 2011.

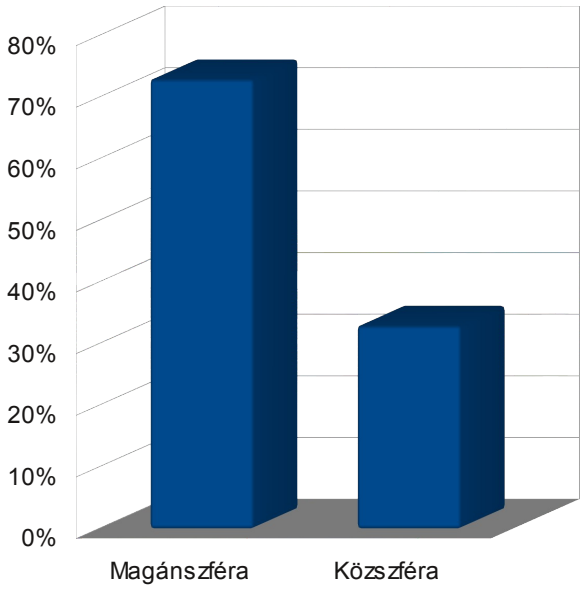
intézményeknél (33%) mint a magánszférában (73%).

Az IT-audit módszertanok sem túl korszerűek a költségvetési szférában, az általánosan használt COBIT, illetve ISO 27001 módszertanokkal szemben a költségvetési intézmények nagy részénél még mindig az ISO 20000-et alkalmazzák, ami a teljes mintában már csak 13%-os penetrációt tudhat magáénak.

A költségvetési intézmények körében kockázatelemzés céljára, a magánszférában viszont leginkább tervezésre használják az IT audit nyújtotta lehetőségeket.

Maguk az audit-folyamatok prioritásai is eltérőek. A kormányzati és a magánszféra eltérő fejlettségét jó mutatja, hogy míg a költségvetési intézmények számára a részletes audit terv kidolgozása fordul elő átlag feletti gyakorisággal, addig a magánszférában az összeférhetetlen szerepkörök elemzése fontosabb az átlagosnál.

Kockázatkezelés alkalmazása az IT-auditban 2011. (%)




*Forrás*

## Eszközök

A magyarországi nagyvállalatok és költségvetési intézmények a nemzetközi átlaghoz hasonló arányban alkalmaznak átfogó stratégiát, illetve az egyes részterületekhez kapcsolódó biztonsági terveket, azonban a konkrét megvalósítás bizonyos esetekben még elmarad ettől a szinttől. Átfogó információbiztonsági stratégiája a vállalatok/intézmények 61%-ának van (egy nemzetközi összefoglaló tanulmány szerint ez világszerte átlagosan 65%), míg például sérülékenységelemző eszközökkel csak egynegyedük rendelkezik, szemben a nemzetközi szinten átlagosan 53%-os aránnyal.[18]

Információbiztonsági stratégiával az összes vizsgált vállalat 61%-ával szemben a költségvetési szféra intézményeinek csak 56%-a rendelkezik.[18]

Hasonló különbségek figyelhetők meg a katasztrófaelhárítási tervet illetően is: a magánszférában 67% (vs. költségvetési szféra 48%).[18]

Menedzsment szintjén sem képvisel akkora jelentőséget a költségvetési intézményeknél az IT-biztonság. Az információbiztonságért felelős vezető (CISO) lényegesen ritkább a közintézményekben, mint a magánszférában (37% vs. 55%).[18]

18 ISACA-Bellresearch-KPMG: Információbiztonsági helyzetkép 2011., 2011.11.04.; http://www.kpmg.com/.../Documents/Informaciobiztonsagi-helyzetkep-2011.pdf


*Forrás*

A meglévő folyamatok, képességek mellett az idei év legfontosabb tervei, törekvései azt mutatják, hogy a vállalatok tudatában vannak az információbiztonság fontosságának – azonban jellemzően itt is elsősorban a stratégiai szintű törekvések kerültek előtérbe, míg a konkrét megvalósításra vonatkozó terveket viszonylag alacsonyabb arányban említették a válaszadók. A lista elején az IT eszköz kezelés és a központi jogosultságkezelés megvalósítása után a katasztrófaelhárítási terv és az átfogó biztonsági szabályzat elkészítése áll.

## Kapcsolat a külső szolgáltatókkal

A külső szolgáltatói kapcsolatokban a leggyakrabban alkalmazott megoldás szerint a vállalatok szerződésben, vagy külön titoktartási nyilatkozatban kötelezik szolgáltatóikat az információk védelmére. A vállalatok háromnegyed része él azzal a megoldással is, hogy csak az általuk igénybe vett szolgáltatáshoz elengedhetetlenül szükséges mértékben engednek hozzáférést a rendszereikhez. Ugyanakkor a szolgáltatók információbiztonsági szempontból való tesztelését csak a megkérdezettek 11%-a alkalmazza. Míg az első három megoldás tekintetében nincs jelentős különbség az állami és a magánszféra között, addig a tesztelés esetében szembetűnő, hogy a költségvetési intézményeknél ez a megoldás egyáltalán nem fordul elő.[19]

## IT-Irányítás

Az IT Process Institute 2009-ben közölt tanulmánya szerint az IT irányítás egy erőteljes eszköz lehet a versenyző IT prioritások egyensúlyozásában, és rávilágít arra, hogy a magasabb szintű IT irányítással rendelkező vállalatok jobb teljesítménymutatókkal bírnak. Ez jól mutatja, hogy egyre inkább elengedhetetlen az IT folyamatok és a vállalati/intézményi stratégia közötti minél szorosabb összhang kialakítása.[20]

Az eredmények azt mutatják, hogy a költségvetési szférában valamivel kisebb összhang tapasztalható az IT folyamatok és az intézményi stratégia között. A legnagyobb összhang az átlagtól

19 Bellresearch: Magyar Infokommunikációs Jelentés 2011.

20 ISACA-Bellresearch-KPMG: Információbiztonsági helyzetkép 2011., 2011.11.04.; http://www.kpmg.com/.../Informaciobiztonsagi-helyzetkep-2011.pdf

eltérően az informatikai szolgáltatási szintek biztosítása terén jelentkezik. Ezzel szemben a magánszférában kicsivel nagyobb az összhang, és a különböző folyamatok sorrendje tulajdonképpen megegyezik az átlaggal.

A vizsgált szervezetek többségében (60%) teljes mértékben, vagy legalább nagyobb részben átlátják felsővezetői szinten az IT kockázatokat. A költségvetési szférában mindez mindössze az intézmények harmadáról mondható el. A vizsgált vállalatok / intézmények méret (alkalmazottak száma) szerinti bontása alapján megfigyelhető, hogy minél nagyobb egy szervezet, annál inkább tisztában vannak a vezetők a lehetséges kockázatokkal.

A válaszadók elmondása alapján úgy tűnik, hogy a vezetőség kockázattudatossága kihat arra, hogy a meghozott döntések mennyiben támogatják az IT kockázatok hatékony menedzselését. Összességében a szervezetek 58%-a gondolja úgy, hogy legalább nagyobb részben támogatják a vezetőség döntései az IT kockázat-menedzsmentet. Ebben a vonatkozásban is megfigyelhető a költségvetési (33%) és a magánszféra (66%) közti kiugró különbség.

### Kiber-bűnözés

A kiberbűnözés nemzeti és nemzetközi viszonylatban is egyre növekvő fenyegetettséget jelent a vállalatok és a költségvetési intézmények számára egyaránt. A szakértők többsége egyetért abban, hogy ennek a biztonsági kockázatnak a csökkentése érdekében állami és vállalati szinten is átfogó biztonsági stratégiára, biztonsági eljárásrendekre van szükség. Ugyanakkor a szakértők abban is egyetértenek, hogy a hatékony stratégia önmagában nem elegendő a megfelelő biztonsági szinthez, hanem szükség van annak a proaktív megvalósítására is. A hazai intézmények, úgy tűnik, számos tekintetben nem ismerték még fel ennek fontosságát, vagy legalábbis kisebb mértékben, mint amit a nemzetközi példák mutatnak.

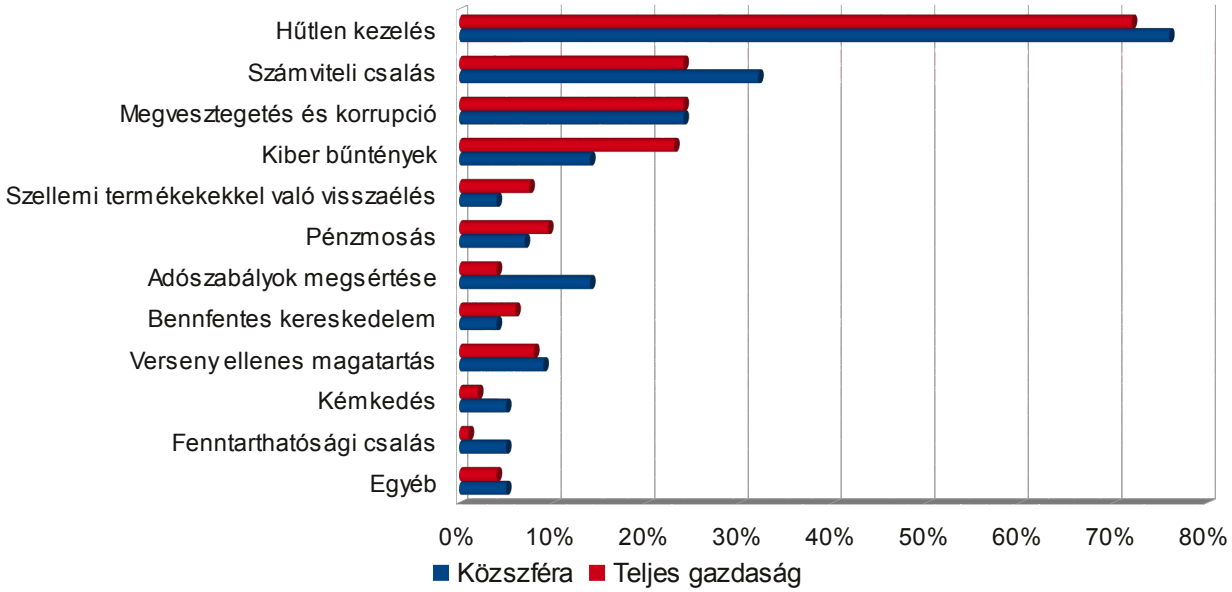
## Nemzetközi helyzet

A Pricewaterhouse Coopers 2012. elején publikálta „Fighting fraud in government” címmel globális fehérgalléros bűnözésről szóló 2011-es jelentésének a közszférát érintő résztanulmányát. A munka külön fejezetet szentel az informatikai biztonság és kiber-bűnözés fokozódó fenyegetésének a kormányzati intézmények és az állami vállalatok körében is. A tanulmány a 2009-es előző felmérést tekinti referencia állapotnak, ehhez képest teszi megállapításait. A kutatás 36 ország 184 közintézményét ölelte fel, az országok között Európán és Észak-Amerikán kívül, Ausztrália, Kelet-Ázsia, a Közel-Kelet, Afrika és Dél-Amerika is helyet kaptak, így valódi globális képet ad a téma helyzetéről.

Az első és legfontosabb megállapítás, hogy a gazdasági bűncselekmények úgy általában is sokasodnak a közszférában. Az intézmények 67%-a tapasztalt 2011-ben kevesebb, mint 10 incidenst (ez 2009-ben még 74% volt), míg azok aránya, akik 11 és 100 között eseményt észleltek, 18%-ról 24%-ra emelkedett.

Az elkövetett cselekmények közül a „nagy triász” (hűtlen kezelés, számviteli csalás és korrupció) viszi a pálmát, de 2011. végére sajnálatosan a kiber-bűntények jöttek fel a 4. helyre mind a teljes világgazdaságban előforduló, mind a közszférát érintő gazdasági bűncselekmények tekintetében. Ezt közvetlenül követi a szellemi termékekkel való visszaélés, amelynek szintén sok IT-vonatkozása van.

Bejelentett visszélések a közszférában és egyéb ágazatokban 2011.

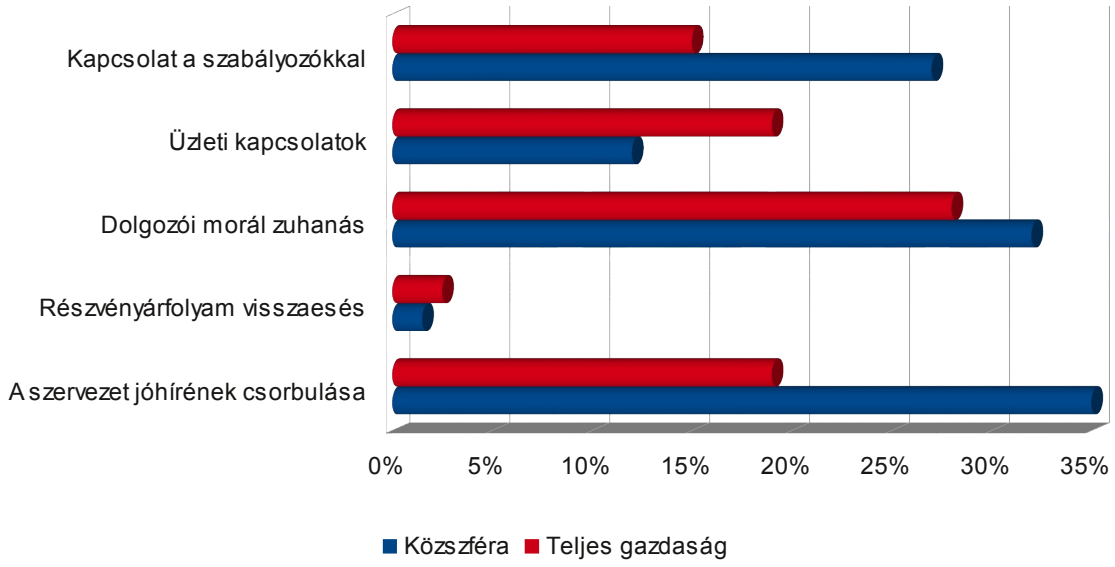



*Forrás*

Bár a közszférában a kiber-támadások fenyegetése látszólag kisebb, hiszen az intézmények 14%-át érintette csak 2011-ben ilyen támadás, a közszféra óriási adattároló feladatai, és a közelmúlt profi elkövetőkre valló támadásai kormányzati célpontok ellen azt mutatják, hogy ez a szektor is egyre vonzóbb célponttá válik.

A visszaélések kapcsán keletkező károk összetett képet mutatnak, a konkrétan pénzre váltható valódi vagyonvesztés mellett, a hatásuk megjelenhet presztízsveszteségben, a törvényhozókkal való megromló kapcsolatokban, illetve a dolgozók romló moráljában is.

A visszaélésekkel járó járulékos károk 2011.



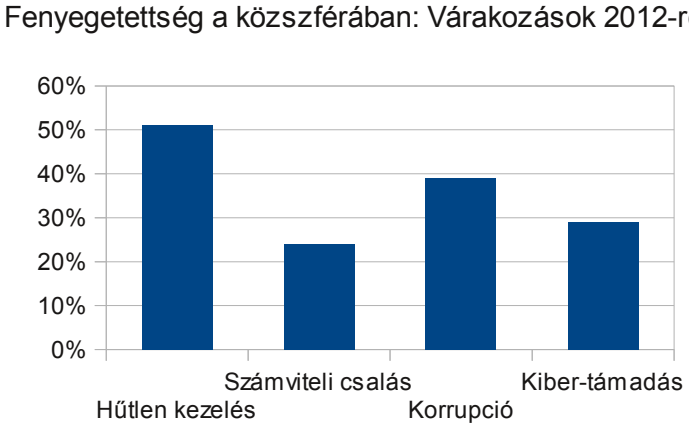

*Forrás*


Márpedig a helyes dolgozói morál fenntartása igen fontos, a 2011-es statisztikák ugyanis világosan kimutatják, hogy a fenyegetések többsége belső forrásból indul, vagy legalábbis van belső segítő ember a visszaélések körül.

Mindennek ellenére a kockázatkezelési és csalás-felderítési eszközök csak jóval korlátozottabb mértékben vannak jelen a közszféra gyakorlatában, mint azt a magánszférában megszokhattuk. Mindössze az intézmények 29%-a jelezte, hogy alkalmaznak ilyeneket és mindössze 23%-uk végez átvilágítást egy évnél sűrűbben. Ezáltal a gyorsan változó, újonnan megjelenő fenyegetésekre nem tudnak megfelelően reagálni.

*Forrás*

A felderítési eszközök fejlesztése és az audit gyakoriság növelése már csak azért is szükséges lenne, mert a közintézmények maguk is érzik fenyegetettségüket: 2012-re minden fontos területen a visszaélési kísérletek számának növekedését várják.




*Forrás*

## Kiber-bűnözés

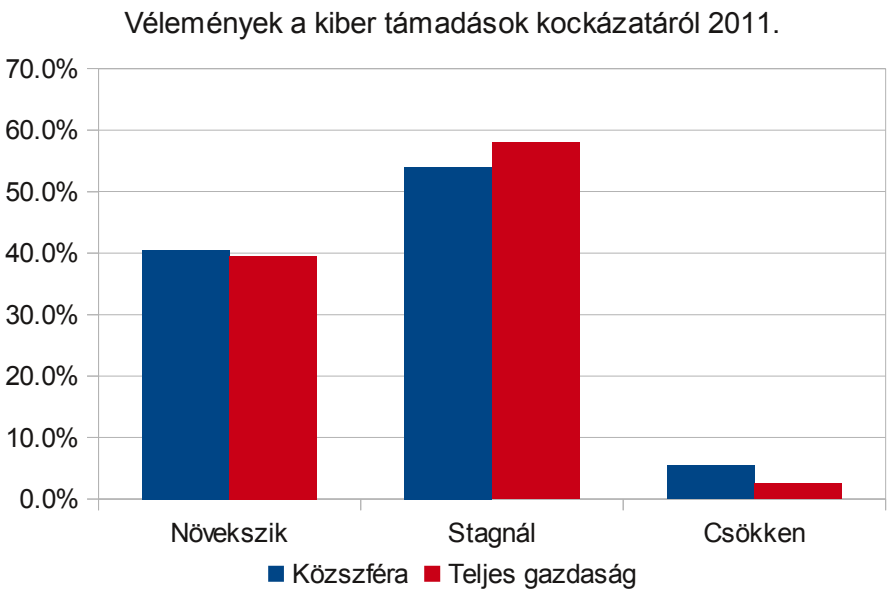
A kiber-bűnözés jelen olvasatban minden olyan gazdasági bűncselekményt lefed, amelyben központi szerepet játszanak a számítógépek és hálózatok, a vírusok terjesztésétől, az illegális fájlletöltésen vagy phishing-en keresztül, a személyes adatlopásig.

A korábbi felmérésekben nagyon alacsony volt a kiber-bűnözéssel, mint önálló kategóriával kapcsolatos észlelések száma, ez a látens kategória mégis a 4. helyre tudott előrelépni a 2011-es felmérés során.

A kiber-bűnözés elkövetési módszerei is változnak, egyre nagyobb a személyes adatlopás célzatú cselekmények aránya, erre pedig, bár 2011-ben csak az intézmények 14%-a érzékelt ilyen incidenst, eszményi célpontot nyújt a közszféra által kezelt hatalmas adatvagyon.

A fenyegetés növekedésével az érintett intézmények vezetői is kezdenek tudatára ébredni, hogy tenni kellene valamit, de ez egyelőre nagyon kevés. A nagy nyilvánosságot kapó, kirívó esetek, amelyek sajtónyilvánosságot irányítanak a közszférára, lendítik leginkább mozgásba az eseményeket. Márpedig a közszférából való adatlopásokról, pénzügyi veszteségekről szóló hírek lassan állandó szereplői a médiának.

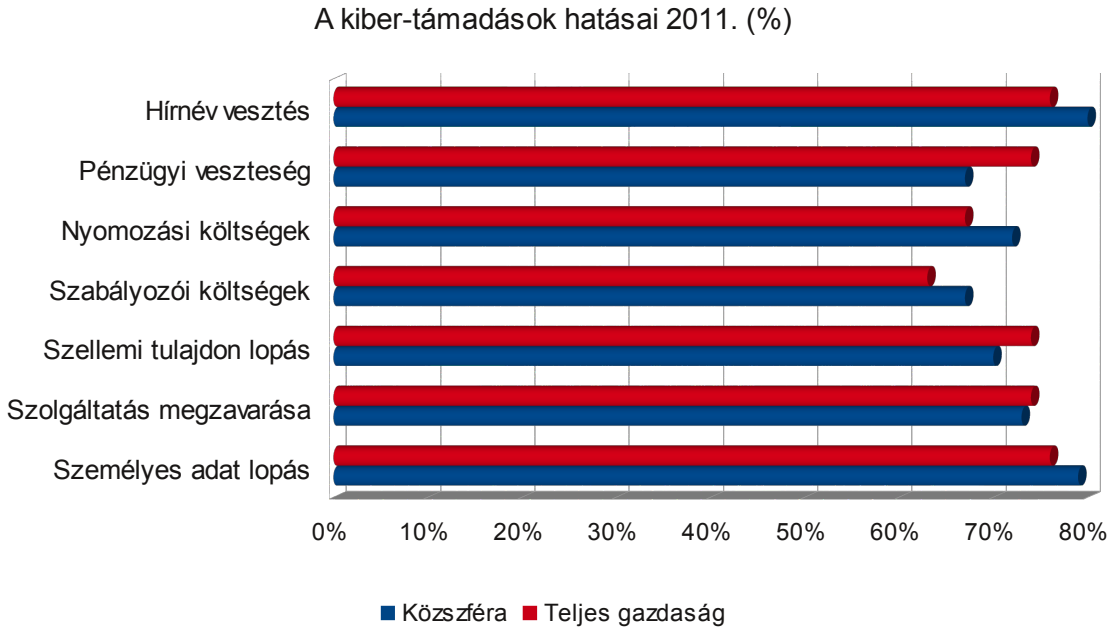
Bár a fenti ábrán az látszott, hogy a közintézményeknek mindössze 28%-a gondolja úgy, hogy 2012. során alanya lehet egy kibertámadásnak, a növekvő veszélyt ennél többen érzékelik, csökkenést pedig a legoptimistábbak sem igen vizionálnak.




A kiber-bűnözéssel kapcsolatos általános vélemény az, hogy ezt valamilyen külső, rosszindulatú harmadik fél követi el általában (hekkerek, terroristák, bűnözők), az igazság az, hogy az intézményeken belülről jövő fenyegetettség legalább akkora, mint a külső kockázat. Először azt feltételezhetjük, hogy az IT-osztályról kerülnek ki a csalók, hiszen ott van meg a támadások végrehajtásához szükséges szakértelem, de ezen kívül a biztonsági és pénzügy/számviteli területről is kerülhetnek ki belső kiber-bűnözők. Az esetek egy részében ez igaz is, de a tapasztalatok azt mutatják, hogy az olyan biztonságosnak gondolt területeket, mint a jogi vagy a HR osztály, legalább annyira védeni kell. Hiszen az általuk kezelt bizalmas információk legalább annyira értékesek, mint a többi területen.

A hatások tekintetében a közszféra az adatvesztéstől tart a legjobban, amely jelentős hírnévbeli veszteséget okoz, és nemkívánatos figyelmet irányít az ilyen közintézmények működésére, így továbbra is fontos az informatikai biztonságba való megfelelő szintű beruházás.

Anyagilag leginkább az adat vesztés/lopás és az ezzel járó károk elhárítása terheli meg a szervezetek költségvetését. Ellopott/elveszett rekordonként az adatvesztés átlagos költsége mintegy 120 USD volt 2011-ben. Egy kiber-támadás teljes költsége a szervezetben pedig átlagosan 2,7 millió USD-t tett ki.




*Forrás*

Sok szervezetben, főleg felsővezetői szinten nincsenek is tisztában a kiber-bűnözés valódi természetével és potenciáival, ez az ismerethiány pedig megbosszulja magát, a hiányos biztonsági rendszerek tervezésében. A nem egyenszilárdságú rendszerek gyenge pontjait könnyen megtalálják a támadók, földrajzi távolságuk, eltérő jogrendszerek égisze alatti működésük pedig erősen megnehezíti, gyakran lehetetlenné teszi a nyomozást és az igazságszolgáltatást.

Így, bár természetesen szükség van a támadások forrásait lenyomozni képes felderítési módszerekre és szervezetekre, a megelőzésre és az egyenszilárdságú védelem felépítésére kell helyezni az elsődleges hangsúlyt.

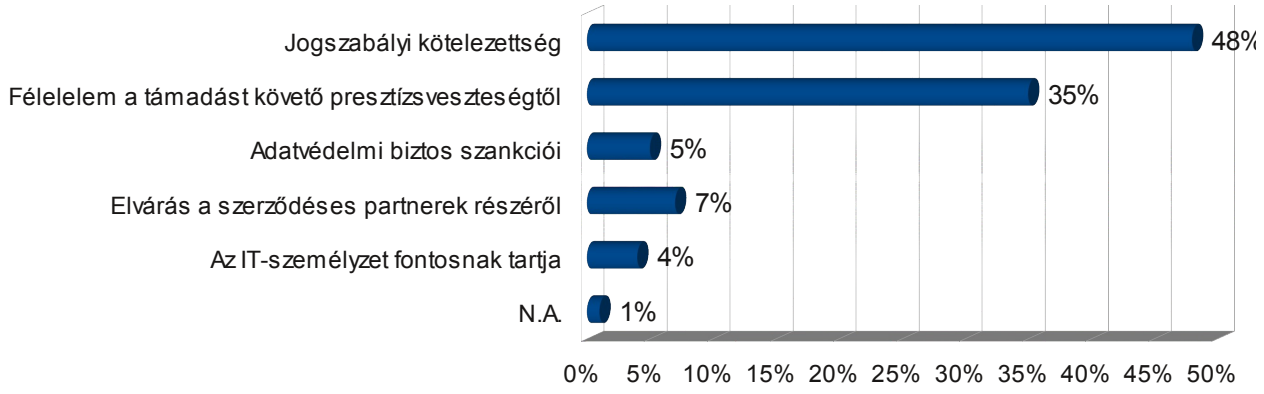
A közszféra intézményeinek mintegy fele nyilatkozott úgy, hogy megvannak a képességeik, szakértelmük a támadások felderítésére, a valóságban nagy részüknek erre nincs forrása, vagy a belső szakértelem mégsem megfelelő, így külső segítőkre kell hagyatkozniuk.

A közszféra majdnem felénél egyáltalán nincsenek olyan katasztrófa- illetve vészleállítási protokollok, amelyek kritikusak egy komoly kiber-támadás első óráinak átvészeléséhez. Nincsenek kommunikációs tervek sem, amelyek segítségével megfelelő válságkommunikáció folytatható egy ilyen esetben a média képviselőivel. Látva azt, hogy hogy mennyire fontos a jó hírnév fenntartása a közszféra szereplőinek, a fenti statisztika több mint aggasztó.

Felelősség tekintetében a megkérdezettek fele úgy értékelte, hogy a biztonsági kérdésekért az informatikai vezető (CIO) viselje a felelősséget, és mindössze 20%-uk gondolta úgy, hogy a legfelsőbb vezetés és vezető (CEO) szintjén kellene kezelni ezeket a kérdéseket. Az intézmények többi részében a legfelsőbb vezetés nem tűz rendszeresen napirendre biztonsághoz kötődő kérdéseket.

A téma megfelelő vezetői szintre emelése legtöbbször sajnos koránt sem biztonságtudatosságból, hanem a veszteségektől és a különböző külső – partneri, feljebbvalói – szankcióktól való félelemből eredeztethető. Ez pedig egyértelműen oda vezet, hogy a látványos, felelősséget fedező, áthárító, „De hát mi minden tőlünk telhetőt megtettünk!” – típusú intézkedésekre helyeződik a hangsúly a lényegi munka helyett.

A biztonsági költések fő motiváló tényezői az intézményeknél (EU, 2011, %)




*Forrás*

A tapasztalatok szerint főleg az idősebb, magasabb beosztású kollégák nem érzékelik a veszélyt és így nem helyeznek kellő hangsúlyt ezekre a kérdésekre.

Fontos, hogy a felső vezetők is elfogadják és megismerjék ezt a felelősséget, és az intézmények minden dolgozója körében biztonságtudatos, kockázatkerülő magatartást alakítsanak ki.

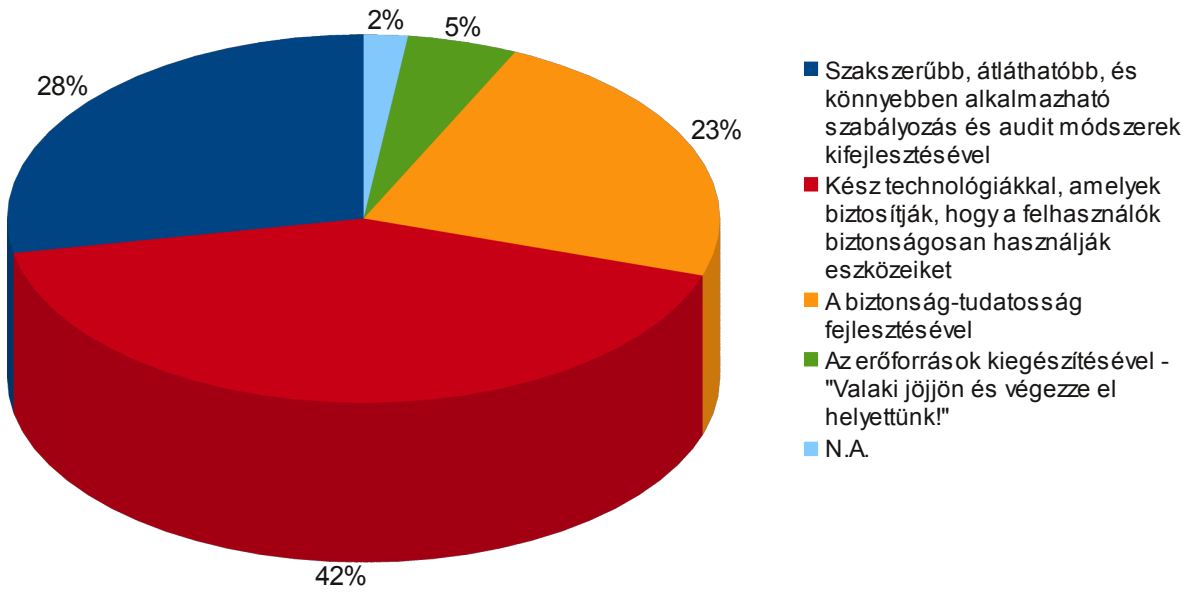
A legfontosabb tanácsok ezzel kapcsolatban:

- Vonjuk be és készítsük fel az idősebb kollégákat is
- Rendszeres IT-audittal kell tesztelni a reagálási képességet és felkészülni az újabbnál újabb támadás típusokra

- Fontos az intézmény IT-rendszerének és -kapcsolatainak teljes körű feltérképezése és biztonsági szempontú átvilágítása
- Szükség van egy gyors reagálású csapat felállítására, akik tudják, hogy támadás esetén mi a teendő, koordinálják a védekezési és helyreállítási munkát
- Már a felvételnél olyan humán erőforrást kell kiválasztani, akiben ott van a biztonságtudatosság, így az egész szervezet ellenállóbbá válik
- Egy támadás bekövetkezésekor minden rendelkezésre álló eszközzel ellen kell állni és azonnal meg kell tenni a megfelelő jogi lépéseket is a bűnelkövetők felelősségre vonására, így nagyobb lehet az elrettentő erő. (Ehhez természetesen a jogalkotókra is szükség van az ilyen cselekmények megfelelő súlyú büntetőjogi tényállássá alakításhoz.)

A közszféra szereplői számára egyre nyilvánvalóbbá válik az is, hogy saját erőforrásokkal, az ipar és a technológiai közösség segítsége nélkül nem elég erősek ebben a harcban, nincs meg az a szakértelem és technológiai szint, amely szükséges lenne a teljes körű védekezéshez.

Hogyan segítheti az IT-szféra a leghatékonyabban az intézményeket? (2011, EU, %)

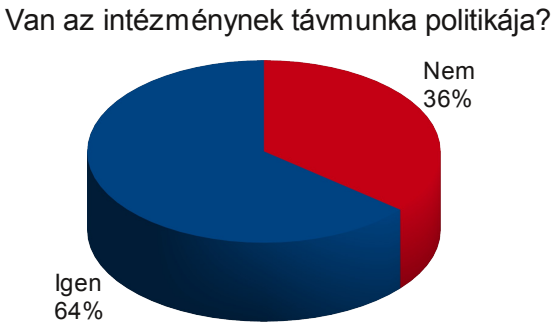



*Forrás*

Örvendetes, hogy viszonylag kevés szereplő várja a „sültgalambot”, vagyis, hogy valaki jön és megold mindent az intézmény illetékesei helyett, azonban a „csodavárás” még így is jellemző, vagyis az intézmények valami olyan technológiára vágynak, ami azonnal könnyen és gyorsan menedzselhetővé teszi számukra ezt az összetett problémát. Szerencsére sokan gondolkodnak reálisabban és a vizsgálati és tudatosságnövelő módszerektől várják a fejlődést, amely sokkal megvalósíthatóbb elképzelés.

# Mobil eszközök

A közszféra IT-biztonságának egy másik nagy fejezete az egyre szaporodó okos mobileszközök (smartphone, tablet) tömeges beáramlása a intézményi hálózatokba, többnyire megfelelő protokollok és ellenőrzés nélkül.




Forrás


A táblagépek és okostelefonok gyors és globális terjedése erős lökést adott annak a trendnek, amely eddig inkább csak az Egyesült Államokban hódított: a saját géppel végzett munkának. Amíg mindenki asztali PC-ken dolgozott, nem sok értelme lett volna az angol kifejezés (bring your own device) alapján csak byod-nak nevezett lehetőségnek, de a mobilitás – és az egyre inkább megfizethető és egyre nagyobb teljesítményű számítógépek – ezen a téren is változást hoztak. Bár Magyarországon ennek nincs hagyománya (már csak az átlagos munkavállaló anyagi lehetőségei miatt sem), egyes cégeknél és egyes munkakörök esetében azonban reális opció lehet a saját gép.

Forrás

A BYOD[21] viszont messze nem jelenti azt, hogy onnantól kezdve mindenkinek mindent szabad. Ha nem akarjuk villámgyorsan teljes káosszá züllleszteni az informatikát, bizonyos szabályrendszert előre ki kell dolgozni. Ezek értelemszerűen mindig az egyes vállalatoktól függnek, de bizonyos elemeik hasonló kérdésekre keresik a választ.

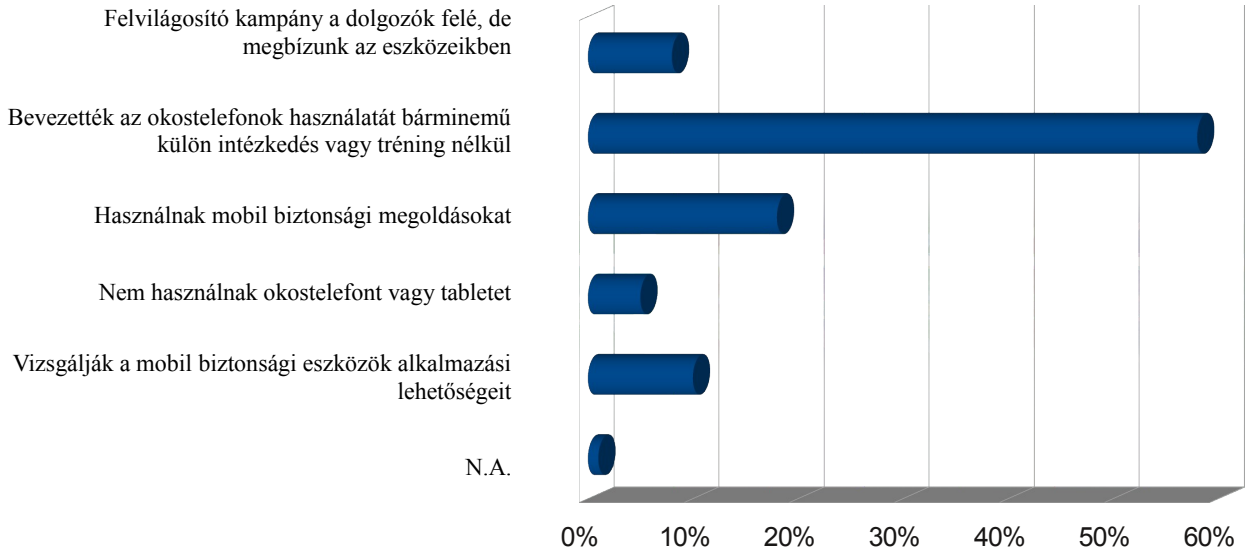
Hogyan védjék a felhasználók az eszközeiket? Milyen adatok és alkalmazások lehetnek vagy nem lehetnek a gépen? Mi legyen a géppel (és az adatokkal), ha elvész az eszköz vagy kilép a dolgozó?

Végig kell gondolni, hogy milyen platformok használatát engedélyezi (és támogatja) az intézmény. Ha laptopokról van szó, beengedi-e az infrastruktúrába az Apple gépeit; a nagyobb mobilplatformok – iOS, Android, BlackBerry, Windows Phone – közül melyik (kettő) mellett teszi le a voksát? Azt is meg kell határozni, hogy milyen adat nem lehet a gépeken – nem is annyira a felhasználó, mint inkább az intézmény védelmében. Nem jó, ha a munkára is használt gépen jogsértő anyagok vagy éppen más, céges, bizalmas információk vannak.

Szorosan kapcsolódik ehhez az engedélyezett, illetve tiltott alkalmazások köre is. A fehér- és feketelisták összeállítása viszonylag egyszerű módszer, és bár nem ad százszázalékos biztonságot, sokat tehet az informatikai környezet megóvásáért. Ezzel együtt meg kell értetni a felhasználókkal, hogy biztonsági megfontolásokból a vállalati informatikának jogában áll megtiltania bizonyos alkalmazások használatát, mint ahogy ugyanezen okból előírhatja bizonyos szoftverek meglétét (víruskereső, tűzfal, egyebek).

21 Bring Your Own Device

Milyen biztonsági megoldásokat üzemeltetnek a mobil eszközeiken? (EU, 2011, %)




Forrás

Különösen a mobileszközöknél lényeges, hogy tisztázásra kerüljön: milyen adatok kerülhetnek fel a készülékre, illetve azokról milyen vállalati erőforrások érhetők el. Meg kell határozni az érzékeny adatok körét, és hogy ezek hogyan és honnan érhetők el (csak cégen belül, vagy otthoni netkapcsolatról igen, de nyilvános hotspotról nem). Szintén dönteni kell az esetleges adatvesztés esetén követendő eljárásról is, legyen az adatlopás vagy magának a készüléknek az elvesztése. Igen lényeges, hogy minden felhasználó tudja, ilyen esetekben mit kell tennie (például azonnal bejelenteni az elveszett mobilt).

Nem elég, ha tud a munkaadó az elveszett készülékről, cselekvőképesnek is kell lennie. Erre szolgálnak a mind nagyobb választékban rendelkezésre álló mobileszköz-menedzsment (mobile device management, mdm) szoftverek, sőt, szolgáltatások. Segítségükkel nem csak központilag kezelhetők és ellenőrizhetők az eszközök, de például olyan fontos funkciók is megvalósíthatók, mint a távoli adattörlés, akár kikapcsolt állapotban.

# Kiber-hadviselés

2011. nagy változást hozott az informatikai biztonságban: általánosan megkezdődött az aktív kiberhadviselés. Néhány példa: az orosz választásokat kísérő hekkertámadások vagy az amerikai automata kémrepülő Irán feletti lelövése is egyértelműen bizonyították, hogy a kibertér hadszíntérnek minősül. Azóta fény derült a Flame létezésére, ami két éve lappang nem csak Irán és Izrael rendszereiben, de több európai országban, köztük itthon is azonosították. A magyar CrySys Labor (amely a Stuxnet tavalyi variánsát, a Duqu-t is azonosította) is elemezte a Flame-et, amely egy másik kódrészlet alapján a hazai keresztségben sKyWIper nevet kapott. A CrySys szakértői szerint akár 5-8 éve is fejlődhet a vírus, amelyről időközben kiderült, hogy az ismert célországok mellett Magyarországon is megjelent, de egyebek mellett már Ausztria vagy Oroszország fenyegetettségét is igazolták. A vírus lényegében minden olyan információt képes ismeretlen gyűjtőhelyek felé továbbítani, ami a megfertőzött gépeken megfordul: a képernyőre kiírt szövegektől a tárhelyeken lévő fájlokon át egészen a hangalapú adatokig bármi lekérhető a segítségével. A titkos irányítók akár azt is megtehetik, hogy a felhasználó tudta nélkül aktiválják a

számítógéphez kapcsolt mikrofont vagy bármilyen egyéb hangrögzítő eszközt, és felveszik a környezeti zajokat, például a gép előtt elhangzó beszélgetéseket. Eddig is több variánst azonosítottak a kártevőből, így elképzelhető, hogy mire megszületik egy általános megoldás, máris egy gyakorlatilag felismerhetetlen mutáns veszi át az előző verziók helyét. A kódkészlet például képes rá, hogy a víruskeresők megtévesztésére az érzékelt környezettől függően változtassa az általa használt fájlkiterjesztéseket. Egyes szakemberek szerint akár tíz évbe is kerülhet, míg teljesen megismerik a Flame működési mechanizmusának minden egyes elemét.[22]

De olyan kódot (ACAD/Medre) is lelepleztek, amely a fertőzött gépen tárolt és keletkező AutoCAD rajzokat továbbítja automatikusan egy adott távoli helyre.

Ezek a megoldások már egyértelműen a kémkedés és a háború eszközei.

Az előző év terméke volt az Anonymous-jelenség is: korábban ki gondolta volna, hogy politikai és ideológiai céloktól vezérelt hekkercsoportok bármit megtámadhatnak vagy ujjat mernek húzni a drogkartellekkel?

A védekezés lényegesen lassabban, de fejlődik: az illetékesek már nem dugják homokba a fejüket, és nem szimplán rendőrségi ügyként kezelik a hekkerek tevékenységét. Az angol miniszterelnök például november elején jelentette be, hogy 650 millió fontot fordítanak kibervédelemre, és a németek is felállították a kiberhadseregüket.[23]

Magyarországon egyelőre elégtelen a felkészültség, pedig az események (pl. az alkotmánybíróság honlapjának megtámadása) azt mutatják, hogy itt is bármikor bekövetkezhet egy ilyen támadás. A védekezést nem akkor kell fokozni, amikor már megtörtént a baj, hanem jóval előtte. Katonai oldalról már bejelentették egy hazai kibervédelmi stratégia készítését. Ez fontos lépés, de továbbiak is szükségesek. A kiberterroristákat és a hekkereket a jó szándék nem állítja meg: ezt csakis és kizárólag a gyakorlati védelmi intézkedések tehetik meg. Ez pedig ember és eszközigényes feladat.[24]

## Támadások a kritikus infrastruktúrák ellen

A kiberháború frontjai közül egyre nagyobb szerepet kapnak az alapvető infrastruktúrát biztosító létesítmények és szolgáltatók elleni támadások. Manapság már nem PC-s vírust írni menő, hanem megtámadni egy olajfinomítót vagy egy erőművet.

Az Egyesült Államok ipari rendszereinek biztonságával foglalkozó csoport, az ICS-CERT kutatása [25] szerint 2009-ben még csak 9 olyan esetről beszélhettünk, ahol kiberbűnözők egyértelműen valamilyen ipari létesítményt támadtak meg, tavaly már 198-ra nőtt az ellátórendszereket ért támadások száma. Mivel ezeket az intézményeket sokszor valamilyen internetes, felhő alapú rendszer vezérli, az ügyesen "megépített" kártevők a rendszerbe jutva sokkal nagyobb kárt okozhatnak egyetlen helyen, mintha egy PC-be férkőztek volna be. Ráadásul már olyan támadások is sikerrel jártak, ahol a külvilágtól elkülönített rendszerek miatt az üzemeltetők teljes biztonságban érezhették magukat.

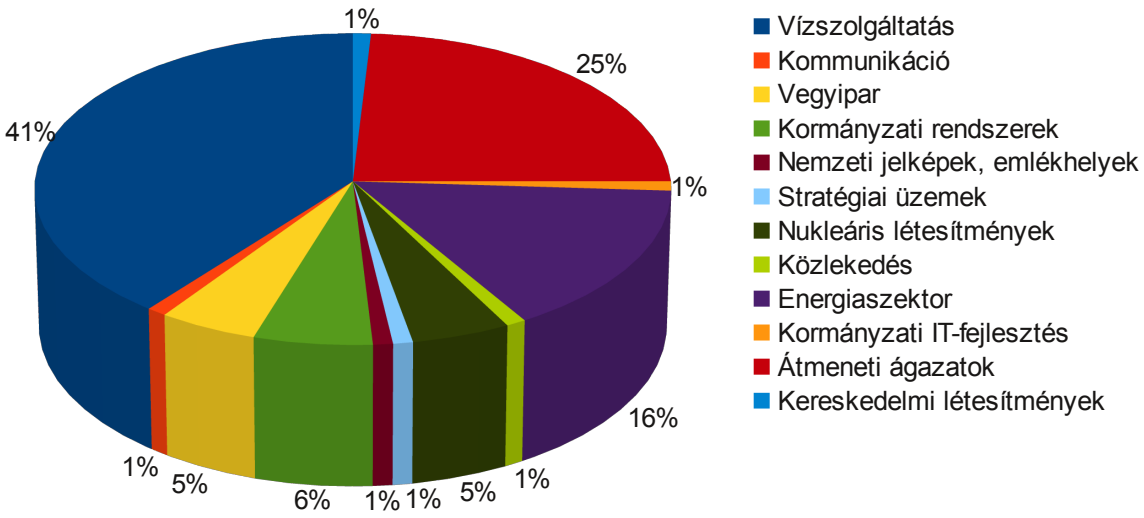
22 Symantec: Internet Security Threat Report – 2011 Trends, Volume 17. 2012.04.; http://www.symantec.com/.../b-istr_main_report_2011_21239364.en-us.pdf

23 SOPHOS Institute: Security Threat Report 2012, 2012. 06., http://www.sophos.com/en-us/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

24 Bátky Zoltán: A vírusok a kritikus infrastruktúrát célozzák, BITPORT, 2012.07.05., http://www.bitport.hu/biztonsag/a-virusok-az-alapveto-ellatorendszereket-celozzak

25 ICS-CERT: Incident Response Summary Report 2009-2011., 2012.06. http://www.us-cert.gov/.../ICS-CERT_Incident_Response_Summary_Report_09_11.pdf

Kibertámadások stratégiai üzletágak ellen az USA-ban 2011. (%)




*Forrás*

Az Egyesült Államokban a tavalyi évben a vízellátás volt a kiberbűnözők kedvenc célpontja: 81 esetben támadtak meg vízműveket, gátakat, elosztórendszereket. Energiaszolgáltatók 31 esetben kerültek célkeresztbe, de tíz olyan támadást is feljegyeztek, amely nukleáris erőművek ellen irányult.

Az ICS-CERT jelentése szerint annak ellenére, hogy kritikus fontosságú intézményekről és rendszerekről van szó, néha gyermekien egyszerű módszerekkel sikerült bejutni a védművek mögé. Kifejezetten sok olyan esetet regisztráltak, amikor alkalmazottak levelezését felhasználva, adathalászati módszerekkel szereztek információkat, jelszavakat a támadók. Tavaly már bevett szokásnak számított a fertőzött pendrive is, amellyel az Internettől teljesen elkülönített belső hálózatokba is „beinjekciózták" a hatalomátvételhez vagy épp romboláshoz szükséges károkozókat.

A kutatás egyik alapvető megállapítása, hogy bizony még a legnagyobb, legfontosabb rendszereket is csupán néhány oldalról bástyázzák körül. Többszintű tűzfalrendszerrel veszik körbe a hálózatot, miközben bárki bármilyen perifériát szabadon csatlakoztathat a gépekhez. Szofisztikált azonosítási és jogosultság-kezelési megoldásokat vezetnek be, de nem figyelik, körbeküldi-e valaki e-mailben a jelszavát. Az esetek elemzése egyértelműen bizonyítja: a kritikus rendszerek informatikai biztonsága terén akár egyetlen kis sebből is teljesen el lehet vérezni. Az egyenszilárdságú védelem megteremtése a legfontosabb feladat.

Sokan még mindig nem tanulnak az elmúlt évek tapasztalataiból. Az ICS-CERT tanulmánya megemlíti például az Echelon esetét: a vállalat többek között közműszolgáltatók számára gyárt intelligens mérőeszközöket és szenzorokat, amelyek az adatokat (elvileg) zárt internetes csatornákon küldik a fogyasztóktól a szolgáltatókhoz. A szakértői csoport néhány hete fedezte fel, hogy a távoli mérőeszközök és irányító berendezések nagy részét az interneten keresztül, alapértelmezett jelszavakkal el lehet érni. Érzékeltetésképpen képzeljük el, hogy akár egyetlen támadó lenullázhatja egy áramszolgáltató összes villanyórájának számlálóját, vagy akár tízezrek otthonában lekapcsolhatja az áramot, mindössze egyetlen „admin" jelszó felhasználásával...

Összegzésében az ICS-CERT továbbra is a kétszintű védekezés fontosságát emeli ki, melyben csupán az első szint a megfelelő biztonsági rendszerek beszerzése és telepítése. A második körben azonban az ügyvezetőtől a takarítónőig mindenkit részletesen ki kell képezni a biztonsági előírások betartására, a lehetséges fenyegetések észrevételére. Akár szakértők által szimulált kibertámadások

végigvezetésével, egyfajta "hadgyakorlattal" is meg lehet próbálkozni, amikor a sokak számára nehezen érthető fogalmak és előadások helyett élesben tapasztalhatja meg mindenki, mit okozhat egy levélben elküldött jelszó vagy egy őrizetlenül hagyott pendrive.

# A kritikus infrastruktúrák védelme

A szakértők egyetértenek abban, hogy minden, a kritikus infrastruktúrákat ért eddigi támadásban felfedezhetők bizonyos minták, szabályszerűségek. Ezek megértésével és kiküszöbölésével a veszélyek nagyban csökkenthetők. Több mint 100 incidenst vizsgálva, be kell látni, hogy a támadók nem nyílt frontális módon közelítenek a kritikus szolgáltatásokhoz, hanem mindenhol igyekeznek megtalálni azt a védelmi rést, ahol nem egyenszilárdságú a védelem.

Ezek a rések három fő hívószó köré csoportosulhatnak:

1. Emberek
2. Folyamatok
3. Technológia

## Emberek – a humán erőforrás

Közhely, hogy minden informatikai rendszer leggyengébb pontja a monitor és a szék között helyezkedik el, mégis a közszolgáltatók, intézmények személyzete nagyon sok biztonsági rés forrása lehet. A dolgozók számára természetes, hogy nap mint nap üzemeltetik azokat a berendezéseket, amelyek tömegeket látnak el, árammal, fűtéssel, ivóvízzel, közlekedési szolgáltatásokkal vagy éppen adatokkal.

Ez a megszokás sok esetben elnyomja annak átérzését, hogy milyen felelősség ezeket a folyamatokat fenntartani, és milyen kockázatok állhatnak elő, ha az irányítás rossz kezekbe kerül.

Ennek megfelelően sokszor a biztonsági szabályok sem kellően erősek és naprakészek. („A bűnözők bankot rabolnak (akár virtuálisan), mi a fenét akarna bárki egy vízműben, onnan nem lehet ellopni semmi értékeset?”)

Sokszor a szükséges tudás is hiányzik, egyszerűen az alkalmazottak nem értenek olyan szinten az IT-hoz, hogy egyáltalán felmérhessék a kockázatokat, amiket egy-egy ártatlannak látszó cselekedet (pl. egy ellenőrizetlen pendrive csatlakoztatása a zárt rendszerben üzemelő számítógépekhez) hordozhat. Ez vonatkozik a menedzsmentre, az IT-alkalmazottakra, a biztonsági személyzetre, folyamatirányítókra is.

A fentiek kivédésére, úgy tűnik, a kritikus infrastruktúrát üzemeltető szervezeteknek ki kell fejleszteni magukban az „egészséges” paranoiát: potenciális célpontként kell önmagukra tekinteniük és végiggondolni ilyen szemmel, hogy megtettek-e mindent a veszélyek elkerülése érdekében.

A legtöbb szervezetben nincsenek meg a megfelelő szabványok és protokollok, így az egyes részlegek nem tudják mérni saját kitettségüket, nem tudják megállapítani, hogy az elért biztonsági szint megfelelő-e, vagy épp ők jelentik a biztonsági rést a szervezetben. Megfelelő szabályrendszert kell kialakítani, amelyhez minden alkalmazottnak és partnernek tartania kell magát. Az ilyen szabályok legegyszerűbbjei a jelszóhasználatra és a VPN-alapú hálózati kommunikációra vonatkoznak, sok helyen már ezek is hiányosak.

Az IT-biztonság hiányosságai gyakran a megértésnek abból a hiányából erednek, hogy meg tudjuk mondani, hogyan érintik ezek a kérdések a szervezet egészét. Erre van néhány módszer, amivel a megértés növelhető:

- Hatáselemzések készítése: mi történhet egy sikeres kiber-támadás esetén, mekkora veszteség érheti ekkor az intézményt? – Ez megalapozza az IT-biztonsági költségkeret helyes meghatározását.

- Megfelelő szakemberek alkalmazása a védelem kialakításához és a támadásokra való megfelelő és gyors reagáláshoz.
- Elegendő idő és jó képzések a biztonsági ismeretek átadására.
- Szituációs gyakorlatok a szabályok alkalmazásáról, melyeken keresztül mélyebben megismerhetők a támadási módszerek. Például mi történhet egy „véletlenül talált" pendrive tartalmának céges gépen való ellenőrzésekor.
- Az IT-biztonsági rendszernek és szervezetnek az intézmény minden területén azonos erejű jogokkal kell rendelkeznie, nem hagyva így kritikus réseket.
- Folyamatos kommunikációra van szükség minden menedzserrel, alkalmazottal, technológia használóval.

## Folyamatok

A folyamatok is jelenthetnek potenciális gyenge pontot IT-biztonsági szempontból:

- Hiányoznak a megfelelő tervek a támadások megelőzésére és a támadásokra való reagáláshoz, nincsenek meg a módszerek a támadó nyomainak rögzítésére, amit át lehet adni a nyomozó hatóságoknak.
- Az IT-biztonság a legtöbbször taktikai szinten helyezkedik el a szervezetben, szükség lenne a stratégiai szintre, a kulcs tevékenységek közé emelésére.
- Nem tisztázottak a szabályok a szervezetben, nem ugyanolyan mértékben vonatkoznak mindenkire. Például teljesen tisztázottnak kell lennie, hogy a cserélhető meghajtók, vagy a saját tulajdonú mobil eszközök mely pontokon, milyen szabályokkal csatlakozhatnak az intézményi rendszerhez.
- A fenti szabályok és tervek kialakításához szükség van az iparági best-practice-ek megismerésére, a biztonság megfelelő stratégiai és technológiai támogatottságára a szervezetben, megfelelően képzett személyzetre és folyamatvezérlésre.

## Technológia

A technológia is forrása lehet természetesen a biztonsági gyengeségeknek:

- Megfelelő kockázatfelmérés és kezelés, IT-audit hiányában nem azonosítottak az IT-rendszer gyenge pontjai, így nem a megfelelő helyre csoportosítják a fejlesztési forrásokat.
- Nem megfelelő az IT-menedzsment:
    - A hálózat nincs fizikailag és logikailag szegmentálva
    - A tűzfalak rendszere nincs megfelelően kialakítva és konfigurálva
    - Kisebb célhálózatok által a hálózat felosztható olyan jól kontrollálható darabokra, amely lehetetlenné teszi, hogy a támadó egy-két lépésben átvegye az irányítást a teljes rendszer felett.
- Javítási és frissítési politika
    - A HW és SW sérülékenységek folyamatos feltérképezése és a felfedezett rések javítása
    - A javítások, frissítések teljes rendszert érintő hatásainak előzetes felmérése a működési zavarok és inkompatibilitási problémák kiküszöbölésére.
    - Visszaállítási tervek, ha egy frissítés problémákat okoz az üzemszerű működésben.

- A felhasználói hozzáférés szabályozása
    - Ellenőrizetlen felhasználói hozzáférések kiiktatása
    - Ellenőrizetlen hozzáférések korlátozása a rendszerszállítók/fejlesztők részéről
    - Erős jelszókezelési politika
- Hálózati kommunikáció
    - Forgalomszűrés és monitorozás
    - Biztonsági szempontoknak megfelelő hálózati architektúra
- Firmware
    - A beágyazott rendszereknek is támogatniuk kell a fokozatos biztonsági javítások lehetőségét
- Operációs rendszer
    - Megfelelő beépített biztonsági eszközrendszer, ennek hiányában nem menedzselhető kellőképpen a rendszer
    - A rendszer folyamatos továbbfejlesztése a szállító/fejlesztő részéről, ami lehetővé teszi a folyamatos biztonsági korszerűsítéseket, javításokat

# Néhány dolog a bankkártyák biztonságáért

A hitelkártyák használata egy kényelmes módja a mindennapi fizetésnek, beszéljünk akár egy üzletben való vagy online vásárlásról. Viszont minden egyes tranzakció kockázatot hordoz magában, attól a pillanattól kezdve, hogy a kártyát egy terminálon keresztül lehúzzák vagy annak szükséges adatai egy weboldalon keresztüli online vásárlás során megadják. Felsorolunk néhány tippet a hitelkártya műveletekkel kapcsolatban, hogy kis odafigyeléssel, hogyan csökkenthetőek a személyes adatokra leselkedő kockázatok.

## Kártyaszerződés

A kártyaszerződés megkötése során az egyik legalapvetőbb dolog a személyes adataink megadása, de most beszéljünk csak - a legtriviálisabb adatokon kívül - az email címről. A szegmentálás nevű gyakorlat a személyes adataink biztonságosabb kezelését segíti elő, mint ahogy azt Tim Rohrbaugh az Intersections Inc. alelnöke is javasolja: „Egy email címet tartson fent a megbízható oldalakkal való kapcsolattartásra, mint a pénzügyi intézetek," továbbá, „egy teljesen másikat a kevésbé megbízható oldalaknak.". Ezen kívül a közösségi oldalakban rejlő veszélyekkel is foglalkozni kell. Ezek az oldalak nagyszerűek, de a felhasználóknak óvatosnak kell lenniük annak tekintetében, hogy milyen személyüket érintő azonosító elemeket tesznek közzé. Röviden, ne adjanak meg a szükségesnél több személyes információt, mint például az édesanyja leánykori neve, az utcát ahol felnőtt vagy a kedvenc háziállatának a nevét, mivel ezek az információk egyéb weboldalak, szolgáltatások vonatkozásában „szokásosan" felhasználhatóak az „elfelejtett jelszó emlékeztető" funkciójához.

## Lehúzni vagy nem lehúzni

Egy bankkártyás fizetés során, amikor a kártya lehúzásra kerül, éber szemekkel figyelje a kártyaleolvasókat, amelyeket „megpiszkálhattak" és figyeljen a pénztárosra vagy pincérre, hogy megbizonyosodjon afelől, hogy a kártyáját nem húzták-e le még egy másik leolvasón is. Mindkettő árulkodó jele lehet annak, hogy kártyáját nem csak az aktuálisan fizetendő összeg ellentételezésére kívánják felhasználni. Ezzel kapcsolatban Andrew Schrage a Money Crashers Personal Finance chicago-i blog résztulajdonosa néhány tippel szolgál:

„A kártyaleolvasó vizsgálata során, alaposan vegye szemügyre a kártyanyílást. Ha égettnek vagy olvadtnak tűnik, ne használja. Ha a nyílás kiáll vagy szokatlan kinézetű, az szintén figyelmeztető jel. Ha a kártyanyílás színei eltérnek a leolvasó színeitől, szintén annak a jele lehet, hogy az eszközt megmahinálhatták." Online vásárlások során – a lehetőségekhez mérten legjobban - győződjenek meg róla, hogy csak megbízható viszonteladóknak adják meg adataikat, akik valamilyen tranzakciós garanciával rendelkeznek, mely védelmet nyújt baj esetén.

### A kiberbűnözők módszerei az internetes bankszámlájának megcsapolására

A kártékony szoftverek íróinak és bankjának az Ön internetes bankszámlája feletti felügyeletének harcában a bűnözőknek nagy előnyük van - jelenleg. „Ezek a fickók jóval a biztonsági közösség előtt járnak" állítja Karim Hijazi, az Unveillance cég vezérigazgatója, amely vállalati informatikai biztonsággal foglalkozik és kártékony szoftverek eltávolítására specializálódott. „Ők hibázhatnak, de mi nem. Egy hiba a részünkről súlyos következményekkel jár", viszont a bűnözők kísérletezhetnek bármely módon és módszerrel, nem számít, ha nem járnak sikerrel. Az a bank, mely csak egyszer is elveszti rendszereinek védelméért folytatott harcot, több millió dollár veszteséget szenvedhet el, nem beszélve a kompromittált felhasználói adatokról.

# Hogyan védje magát az adatszivárgásoktól

Az utóbbi időben két nagyobb adatlopás történt, amelyeket áprilisban az Epsilon jelentett be, mely több száz nagy vállalat ügyfelének adatait kezeli és a Sony, amely globális méretű szórakoztatóelektronikai játékhálózatokat üzemeltet, több mint 100 millió ember személyes adatait érintette. Ezek az emberek nagyobb eséllyel válhatnak személyazonosság lopás áldozataivá, továbbá könnyebben válhatnak célzott adathalászat (spear phishing[26]) célpontjaivá. Mégis ezek az adatszivárgások az érintettek számossága miatt kerültek a szalagcímekre. Ahogyan Bruce Schneier biztonsági szakértő rámutatott egy nem túl régi interjújában, a hálózatokat érintő adatszivárgások mindig is történtek, csendben érintve pár millió embert. „Egy hálózat sem teljesen biztonságos, az embereknek ebbe bele kell törődniük". Pesszimista, de tisztán látó mód szerint az online működő vállalatokra és szervezetekre sosem szabad támaszkodni adatvédelmi szempontból. Sosem lesznek tökéletesek, akármennyire is állítják, adatszivárgás mindig is lesz. A neve, címe és e-mail címe végül is ki fog szivárogni, táptalajt biztosítva a személyazonosság lopásoknak és más online bűnözési módszereknek.

## Használjon többféle e-mail címet

Támaszkodjon egy olyan e-mail címre, amelyet a barátokkal és családdal való kapcsolattartásra használ csak. Készítsen egy másikat levelező listákhoz, termékbemutatókhoz és más online szolgáltatásokhoz. Egyes emberek még egy harmadikat is használnak közösségi oldalakhoz, de akár használhat újat minden alkalommal, amikor feliratkozik, csatlakozik valahová. „Két pozitív oldalát látom annak, ha különböző e-mail címet használok minden egyes feliratkozáshoz" állítja Guillaume Lovet, a Fortinet felsővezetője. „Először is, ha valami kéretlen reklámlevelet (spam) vagy valami csaló e-mailt kapok bármelyik fiókomba, azonnal feltételezhetem, hogy ahová feliratkoztam az adott címmel vagy kompromittálódott vagy etikátlan módon eladásra került kéretlen reklámlevél (spam) küldő köröknek. Ezután meg lehet tenni az ide tartozó lépéseket, például leiratkozni vagy az érintett e-mail cím használatát felfüggeszteni. Másodsorban, ha a kiberbűnözők fel is törik valamelyik e-mail címemet, csak az azt érintő szolgáltatásokat kompromittálhatják (a mindenhol használatos „elfelejtett jelszó emlékeztető" funkcióval)."

## Használjon új jelszót minden bankszámlához

Nehéz lehet minden egyes különböző fiókhoz tartozó jelszót megjegyezni, de a böngészőt sem biztonságosabb megbízni ezzel a feladattal. Amennyiben a számítógépét kompromittálták, a jelszavak azonnal elérhetőek és a bankszámlái megcsapolhatóak. Jelenleg, csak a Mozilla Firefox és az Opera böngésző rendelkezik azzal a funkcióval, mely a tárolt jelszavakat titkosítani képes és egy mester jelszóval védi azokat (a Firefox ezen funkciója alapértelmezetten ki van kapcsolva). Catalin Cosoi, a romániai BitDefender elnöke hozzáteszi, az egyszerűen nem elég, hogy minden bankszámlához más jelszót használunk. Egy kitalálhatatlan jelszónak kell lennie, amennyiben azt használja jelszónak a Facebook fiókjához, hogy 'facebook_.jelszó'-t vagy például a Twitter-hez azt, hogy 'twitter_.jelszó' az önmagában nem védelem. Jó tanácsként gondoljon valami ilyesmire: 'Én vagyok a legokosabb ember ezen a bolygón'. Aztán vegye az első betűket: 'EVALEEAB'. Majd helyettesítse az 'A' betűt egy '4' betűvel és ilyesmit fog kapni: 'EV4LEE4B'. Könnyű megjegyezni és további karaktereket cserélhet ki, ezzel tovább bonyolítva a kombinációt.

## Sose adja ki a személyigazolvány számát

Sose adja ki a személyigazolvány számát vagy más Önt azonosító számot. Egy cégnek sincs szüksége ilyen információra egy tipikus tranzakcióhoz. „Ehhez hasonló információ morzsákra csak bizonyos szolgáltatások kapcsán biztonsági kérdések esetén lehet szükség, például abban az esetben,

26 olyan hamis e-mail-ek melyek állításuk szerint ismerik a címzettet

ha elfelejtette a jelszavát vagy telefonos ügyintézés során azonosítania kell magát, (például a bankkal szemben)" állítja Guillaume Lovet. Néhány vállalat a hitelkártyákat a nevek és címek összehasonlításával ellenőrzi, így ebben az esetben szükség lehet a címe megadására is. Ha valamit online vásárol, valószínűleg a valós címét szeretné megadni - hacsak nem veszi a fáradtságot, időt és anyagiakat, hogy egy postafiókot béreljen. Mindezek során számos személyes információ megadására sor kerülhet egy-egy tranzakció vagy ügyintézés során, de ha kellő körültekintéssel járunk el, minimalizálhatjuk adataink kompromittálódásának lehetőségét.

# Mobiltelefonos fizetések

## Mi az a mobil bankolás?

Egyszerűen fogalmazva, a mobil bankolás ugyanazt jelenti, amit a bankfiókjában (vagy a számítógépén) végezne, amihez az okostelefonját vagy táblagépét használja, mint például banki tranzakciók, egyenleg lekérdezések kezelése. Ezek a műveletek SMS üzeneteken, egy webböngészőn vagy egy okostelefonra telepített alkalmazáson keresztül hajthatóak végre. Mivel nem minden intézmény rendelkezik a felsorolt három módszerrel, a kiválasztott megoldás nagyban függ a bank által kezelt piaci szegmenstől. Például, bizonyos pénzügyi szervezetek a fejlődő piacokon általában az SMS szolgáltatással kezdenek, mivel ez a funkció a szerényebb képességű telefonokon is nagy eséllyel igénybe vehető.

## Mobil bankolást érintő legjobb biztonsági tippek

### *Bankolást segítő alkalmazások*

Ismét egy technológia, ami sokat fejlődött. „Az alkalmazások használata egyre növekvő tendenciát mutat a mobil bankolás terén, a rendelkezésre álló funkciók állandóan javulnak", állítja Sonia Lalli, a Juniper Research elemzője. A pénzügyi intézetekre nehezedő nyomás egyre növekszik, hogy a különböző okostelefonokhoz és táblagépekhez tartozó platformokon működő alkalmazásokat kínáljanak. A szolgáltatások nagyjából hasonlóak, a felhasználók egyszerűen ellenőrizhetik a folyószámla egyenlegüket és pénzműveleteket, számlákat fizethetnek, átutalásokat indíthatnak, közelben levő bankjegykiadó automatákat és bankfiókokat kereshetnek meg. Ám néhány bank már ennél is többre képes, például a Chase Mobile nevű alkalmazás lehetővé teszi a felhasználó számára csekkek szkennelését és letétbe helyezését az okostelefonjuk kamerájának segítségével. Továbbá pénzt utalhatnak át két Chase folyószámla között, azonnali kifizetésekhez.

### *A hétköznapi veszélyek*

A szektorban történő fejlesztések ellenére, a mobilos kereskedelem nem terjedt olyan gyorsan, mint várták, melynek fő okai a biztonsági kérdések. „A mobilos kereskedelem robbanásszerű fejlődése azt jelenti, hogy egyre több bizalmas adat kerül tárolásra egy telefonon, ami így még jobban felkelti a kiberbűnözők figyelmét, ilyen célpontok feltörésére", magyarázza Nitin Bhas, a Juniper Research elemzője. Bhas szerint az egyre növekvő kifinomultságú eszközök többféle módon gyorsítják fel az igényt a mobilbiztonság iránt. „A hackerek hozzáférhetnek az eszközökön tárolt bizalmas adatokhoz úgy mint bankszámla, mobil bankoláshoz használt PIN és átutalási kódok, hitelkártya adatok." A mobil bankolás fő veszélyei közé tartoznak a következők: eszköz elvesztése, adathalászat, kártékony szoftverek, vírusok és csalások.

### *Lopott okostelefonok*

„A legnagyobb biztonsági veszélyt azon ellopott vagy elvesztett okostelefonok jelentik, amelyek nem rendelkeznek a rajtuk tárolt adatokat érintő vagy azokat megsemmisítő védelemmel” állítja Bhas. Aki egy eszközt ellop, hozzáférhet az azon tárolt adatokhoz, mint például mobil bankoláshoz szükséges biztonsági kód vagy egyéb jelszavak.

### *Adathalászat*

A másik nagy veszélye a mobil bankolásnak az adathalászat. Az adathalászatot végző támadók általában hamis alkalmazások, e-mailek vagy SMS-ek által próbálják meg álcázni magukat. „A mobil bankolást érintő adathalászat a leggyakoribb, mivel könnyű kivitelezni és pénzzé tenni.” mondja Bhas. Gyanútlanul egy olyan weboldallal találkozhat, amely tipikus adatokat kér Öntől - felhasználói név, jelszó, az Ön hitelkártyájának adatai, mivel az oldal valódinak tűnik és úgy is működik, így Önnek nem tűnik fel semmi, de valójában az egész oldal hamis - és az adatait éppen egy támadó gyűjtötte be. Az adathalászatról több információ a PTA CERT-Hungary által készített kiadványban olvasható, amely a következő linken érhető el: http://www.cert-hungary.hu/sites/default/files/news/nhbk_adathalaszat.pdf

### *Kártékony szoftverek*

A kibertámadások másik formája az okostelefonra települt kártékony szoftverek, amelyek az Ön tudta nélkül települnek az eszközére, hogy bizalmas adatokat szivárogtassanak ki. Bizonyos alattomos kártevők még távoli hozzáférést is képesek nyújtani az Ön készülékéhez a támadók részére, melyek akár rejtett módon is képesek megfigyelni a felhasználói szokásait.”

### *Hogyan maradhatunk biztonságban*

Az első és legfontosabb, amelyet Bhas javasol, hogy valamilyen mobil biztonsági alkalmazás legyen telepítve a készülékére: „Egyre inkább nélkülözhetetlenek a mobil biztonsági szoftverek, ugyanúgy mint például asztali vagy hordozható számítógépek esetén”, mondta. Az okostelefonok és a táblagépek egyre növekvő népszerűsége miatt ez különösen fontos, mivel sok felhasználó már hozzászokott ahhoz, hogy útközben végzi el online tranzakcióit, így egyre több és több potenciálisan érzékeny adat kerül tárolásra. A Juniper legújabb felmérései azt mutatják, hogy minden 20-ból nem egészen egy okostelefon és táblagép rendelkezik csak biztonsági szoftverrel, annak ellenére, hogy a fenyegetések egyre szélesebb skálán mozognak.

Egy robusztus biztonsági csomag telepítésén túl, a felhasználóknak kerülniük kell a nem biztonságos és nem hitelesített Wi-Fi vagy privát hálózatokat. A letöltendő és telepített alkalmazások tekintetében fontos, hogy csak megbízható forrásból származó alkalmazásokat telepítsünk és/vagy APK[27]-kat töltsünk le és kellő fenntartással kezeljük a fájlmegosztó oldalakról letölthető kalózverziókat. Egy másik jó tanács, hogy alaposan vizsgáljuk meg, hogy az alkalmazások milyen jogosultságokkal fognak futni vagy milyen erőforrásokhoz, adatokhoz férhetnek hozzá. Bár az Apple és a Windows Phone meglehetősen „szigorúan” kezeli azokat az alkalmazásokat, amelyek a telepítés után a rendszer erőforrásaihoz hozzáférnek. Ettől függetlenül például az Android felhasználóknak ügyelniük kell a telepített alkalmazások funkcióira, amelyek gyanúsan túlmutatnak azon, amit az telepített alkalmazás leírása tartalmaz. Amennyiben mobil eszközére egy olyan alkalmazást telepít, amely vélhetően indokolatlanul engedélyeket kér SMS vagy MMS üzenetekhez való hozzáféréshez, gondolkozzon kicsit. Vajon miért van szüksége egy játéknak az SMS szolgáltatás hozzáféréséhez vagy ahhoz, hogy más embereket hívjon fel? Számos alkalmazás létezik, amely láthatólag nem sok mindent csinál, de a háttérben információkat küld el Önről, olyanokat mint az ismerősei nevei, privát adatai, e-mail címei és így tovább.

27 Application Package File - http://en.wikipedia.org/wiki/APK_(file_format)

A mobil bankolás lehetőségei folyamatosan bővülnek, így az ezzel járó kockázatok és a veszélyek is növekednek. A tudatosság és a fogyasztói bizalom is növekszik, de ameddig kifejlesztik az érzékeny pénzügyi információk kezelésének új módjait, addig Önnek egyre éberebbnek kell lennie, hogy a mobil bankolás kifizetődő legyen.

## Hitelkártya cégek és lehetséges adatszivárgási veszélyek

Amennyiben kiszivárgott adataink forrását kívánjuk megtalálni, elengedhetetlen a tranzakcióink megfigyelése. Több cég is fokozta a kártya mozgások megfigyelését és talán el is csíptek néhány hibát, de amennyiben élni kíván a törvény által kínált védelem lehetőségével, azért Önnek kell lépéseket tennie. Ne legyen szégyellős telefonon bejelenteni egy vélt anomáliát vagy érdeklődni egy gyanús tranzakciót illetően. Ez egy nyomós érv, amiért érdemes felhívnia a hitelkártya céget, még ha nem is feltételezi adatszivárgást. A kártya kibocsátó más cégekkel megoszthatja a személyes adatainkat így azok bármikor, bármely szerveren történő tároláskor kiszivároghatnak. Ennek hozzájárulását vonja vissza még most. Amennyiben megteszi a fenti lépéseket, sokkal jobban fogja érezni majd magát a kártya használata során. A világon ugyan semmi sem kockázatmentes, de ezáltal legalább kevésbé lesz feltűnő célpont a személyazonosság ellopását célzó támadások során.

## 10 gyakori számítógépes fenyegetés

Az erős antivírus programok és tűzfalak kiválóan védik a számítógépes rendszereinket. Azonban még ha azok naprakész frissítéssel is rendelkeznek és a tűzfalak is megfelelően konfiguráltak, még akkor is olyan alattomos veszélyek leselkednek Önre, amelyek féreg módjára „berágják” magukat a rendszerébe, amelynek következtében ellopják az adatokat és visszaélnek a számítógéppel. Ezek ellen csak úgy tehetünk, ha támaszkodunk a biztonsági és informatikai szakemberekre. Amennyiben az átlagos felhasználó nem elég éber, a világ legerősebb óvintézkedései sem állítják meg a „digitális” behatolókat, amelyek a nap végére végzetes következményekhez vezethetnek. A következőkben 10 pontban láthatja ezen fenyegetéseket, amelyek talán elkerülték a figyelmét.

### Hamis technikai támogatással kapcsolatos hívások

Lehetséges, hogy már fogadott kéretlen hívást olyan személytől, aki a Microsoft vagy valamely más nagy informatikai cég technikai támogatásával kapcsolatos képviselőjeként mutatkozott be. Viszont a hívó személy nem az akinek mondja magát. Azt követően, hogy egy, a számítógépét érintő „gyanús tevékenységről” figyelmezteti Önt, felajánlja a segítségét. Elkéri a személyes adatait, hogy elvégezhesse a munkáját, amely természetesen nem javítja meg a számítógépet. Őt csak az Ön személyes információi érdeklik. Amennyiben ehhez hasonló hívásban részesül, szakítsa meg a hívást és hívja fel azt a céget, amelynek képviselőjeként a hívó fél kiadta magát és jelentse az incidenst.

### DNS átirányítás

Az olyan internet szolgáltatók[28], mint a Time Warner Cable és az Optimum Online azt állítják, hogy segítik a DNS átirányítást, de a valóságban itt is csak a pénzről van szó. A domain név rendszer[29] átirányítás a böngésző normál viselkedését kerüli meg. Egy elérhetetlen oldal esetén a 404 "File Not Found" hibaoldal megjelenítése helyett az internet szolgáltató által választott oldal kerül megjelenítésre, amely a legtöbb esetben tele van fizetős hirdetésekkel és linkekkel. Az ártatlannak vélt műveletet a számítógépes vírusok is megtehetik, átirányítva a böngészőt egy rosszindulatú oldalra, abban a pillanatban, amikor elgépeltünk egy domain címet. Az internet szolgáltatóknál

28 ISP - Internet Service Provider
29 DNS - Domain Name System

lemondhatjuk a DNS átirányítást, így ezt követően, ha a felhasználó tudja hogy néz ki az alapértelmezett 404-es hibaoldal, könnyen kiszűrhetővé válik egy esetleges vírus által kezdeményezett átirányítás, és meg lehet tenni a szükséges lépeseket.

## Nyílt DNS feloldók

Bizonyos veszélyeket rejt néhány DNS szerver beállítása is. Egy nyílt névfeloldó[30] olyan információkat ajánlhat fel, amelyek szolgáltatására nem jogosult. Nem csak a nyílt névfeloldókat használják fel elosztott szolgáltatás megtagadás (DDoS) támadásokhoz, hanem a támadó „megmérgezheti" a DNS gyorsítótárat, ezzel hamis információt és nem megfelelő névfeloldást eredményezve, amelyet a kijavításához elengedhetetlenül fel kell tudni ismerni. Amennyiben a böngésző mérgezett DNS gyorsítótárba botlik, egy rosszindulatú szerveren található „ügynök" programok részletes információkat gyűjthetnek be a rendszerről - különösen, ha egy fontos tranzakció közepén van. Egy átlagos felhasználó hogyan tudja kezelni ezt a problémát? Hideg zuhany, de sehogy. A probléma megoldása ez esetben az internet szolgáltatón múlik.

## Hamis SSL tanúsítványok

A Secure Sockets Layer (SSL) tanúsítvány biztosítja a böngészőt afelől, hogy az éppen meglátogatott internetes oldal az, aminek mondja magát. Amennyiben a jó öreg „HTTP" helyett „HTTPS" olvasható a böngésző cím sávjában, akkor tudhatja, hogy egy biztonsági megoldást alkalmazó internetes oldalon tartózkodik, mint amikor például bejelentkezik az online banki felületre vagy egy telefonszámla online befizetésekor. A világon a legtöbb SSL tanúsítványt a kijelölt Tanúsító Hatóság[31] bocsájtja ki. De mi történik akkor, ha a böngésző és a weboldal bizalmát használják ki? Hamis SSL tanúsítványok beszerzése vagy létrehozása törvénytelen cselekedet, de ez elég gyakran megtörténik ahhoz, hogy óvatosságra intsenek. Mi sem mutatja jobban, mint az, hogy 2011-ben több alkalommal is felfedeztek hamis tanúsítványokat, amelyek Gmail-t és Google Docs-ot használó iráni állampolgárok utáni kémkedési kísérletre utaltak, mellyel kapcsolatban az F-Secure számítógépes biztonsági cég internetes oldalán az alábbi olvasható: „Valószínűleg az iráni kormány használja ezeket a technikákat, hogy figyelemmel kísérje a helyi ellenzéket".

## Munkafolyamat eltérítés

Amennyiben Ön a délutánját a laptopjával egy internetes kávézóban tölti egy nyílt Wi-Fi hálózathoz kapcsolódva, könnyen elképzelhető, hogy nem Ön az egyetlen, aki az Ön Facebook vagy Ebay fiókjába be van jelentkezve. A Mozilla Firefox böngésző egyik modulja, nevezetesen a Firesheep, lehetővé teszi a felhasználónak, hogy az azonos Wi-Fi hálózaton tartózkodó emberek böngésző tevékenységeibe betekinthessen. Amíg illetéktelen megfigyelők nem láthatnak bele a biztonságos oldalakba, addig sok internetes oldal csak a bejelentkezési felületet teszi biztonságossá. A bejelentkezést követően ez az állapot böngésző sütikkel, adatcsomagokkal kerül fenntartásra. A Firesheep azonban megengedi a felhasználóknak a böngésző sütik másolását és a műveletet követően a weboldal, ahova a felhasználó bejelentkezett nem tudja megmondani a különbséget a Ön és a másik fél között. Ezt rossz szándékú indíttatással akár törvénytelen dolgokra is fel lehet használni. Egy hasonlattal élve, a támadóknak nem kell megostromolnia a várat, amikor a vendég nyitva hagyja az ajtót.

30 open resolver
31 CA - Certificate Authorities

## Man-in-the-Middle támadások

Még a titkosított üzenetei sem lehetnek biztonságban, amíg Ön a tejeskávéját szürcsöli egy nem biztonságos hálózatot használva. A Man-in-the-Middle (MitM) támadás akkor történik, amikor a támadó lehallgatja a kommunikációt, majd a kommunikációba ékelődik, és egy eljárással saját magán keresztül továbbítja oda-vissza az üzeneteket a két jogosult fél között. Az üzeneteket váltó felek még privát titkosító kulcsot használva is azt hiszik, hogy a két oldali kommunikáció sértetlen, miközben minden üzenetük a támadóhoz kerül átirányításra, aki módosíthatja a tartalmát, mielőtt az a címzetthez kerülne továbbításra. A támadó irányítása alatt maga a titkosító kulcs is kicserélhető, miközben az érintett felek továbbra sincsenek tudtában annak, hogy folyamatosan „lehallgatják" őket.

## SQL befecskendezés

Az SQL[32] nyelvet használó adatbázisok speciálisan kialakított kérésekkel találják meg a kért adatokat, majd szolgáltatják vissza a felhasználónak. Az emberi vagy automatizált támadók olyan kéréseket küldhetnek, amelyek kihasználhatják az adatbázis gyengeségeit a lekérdezés folyamatának módosítására. Csak ebben az évben az SQL befecskendezés számos közismert adatszivárgás okozója volt, olyanoké mint a LulzSec hacker csoport által a Sony Pictures szerveréről történő állítólagos adatlopása. A probléma megoldása ismételten nem a felhasználó kezében van. „A megfelelően megtervezett szoftver kiszűrheti a meghatározott szabályokkal nem egyező bármely lekérdezést". Egy biztonsági szakember szerint tanácsos az adatbázisokat létrehozó és karbantartó személyek részéről a feketelisták helyett fehér listákat alkalmazni.

## Álcázott fájlnevek

A modern operációs rendszerek a hagyományostól eltérő nyelvektől származó karaktereket, mint az arab és héber speciális kódok alkalmazásával dolgozzák fel. Például az írás helyes megjelenítéshez ezek a kódok tartalmazzák az írás megfelelő irányát is, balról jobbra helyett, jobbról balra. Sajnos ezek az „RTL" és „LTR" parancsok speciális Unicode karakterek, amelyeket bármely szöveg tartalmazhat, így például a fájlnevek és a kiterjesztések is. Ezt kihasználva egy kártékony szoftver más kiterjesztéssel álcázhat „.exe" futtatható fájlokat. Az operációs rendszer az „álcázott" néven jeleníti meg a fájlt, amelyet azonban továbbra is futtatható fájlként kezel, így elindítva azt, a benne található programkód lefut és megfertőzi a számítógépet. Legyünk óvatosak az ismeretlen forrásokból származó fájlokkal.

## Banki trójaiak

A trójai egy rosszindulatú szoftver, amely egy ártatlan programnak álcázza magát, arra számítva, hogy letöltik vagy telepítik a rendszerre. Amint ez megtörténik titokban elkezdheti végrehajtani a kártékony tevékenységét. A hírhedt ZeuS trójai és riválisa a SpyEye az internet böngészők biztonsági réseit kihasználva „lovagolják" meg a böngésző munkamenetét, amikor például egy internetes bank oldalára történik bejelentkezés. Ezek a számítógépes kártékony szoftverek igazi szörnyetegek, ugyanis nagy óvatossággal a bankszámla egyenlegének, a tranzakciós előzmények összegeinek figyelembevételével, meghatározott összegek elutalásával igyekszik észrevétlen maradni. A pénzügyi intézetek folyamatosan növelik a biztonsági rétegeket, bevonva a nagy összegű tranzakciókat is, ilyen például az az „out-of-band" kommunikáción keresztüli megerősítés előírása - például mobil eszköz segítségével. A digitális csalók idejüket nem vesztegetve adoptálták a változtatásokat és a banki trójaiakkal képessé váltak a számlához tartozó mobiltelefonszám megváltoztatására és a megerősítési kérelem elfogására. Ez is a digitális fegyverkezési verseny egy része, amely nem mutatja a lassulás jeleit.

32 Structured Query Language

### Facebook mindenhol

Nehéz olyan személyt vagy céget találni, aki nincs a Facebook-on. Néhány kevésbé hozzáértő felhasználó számára a Facebook maga az Internet. Az olyan fejlesztésekkel, mint a Facebook Connect és Open Graph, a Facebook idézőjelesen megnyitotta kapuit bármely harmadik fél számára, aki színre szeretne lépni. Feltehetőleg már Ön is észrevette, hogy a Facebook hirdetéseket jelenít meg, amely a demográfiai adatain, a közzétett személyes információin és a azokon a tevékenységeken alapul, melyeken részt vesz. Amit talán Ön sem vett észre, hogy más oldalak is elkezdték kihasználni a Facebook-on megtalálható demográfiai adatait. Miközben az interneten böngészik és be van jelentkezve a Facebook profiljába, addig más oldalak hozzáférhetnek a nyilvánosnak beállított profil adatokhoz. Nem akarja, hogy az interneten található weboldalak kilométerekről észrevegyék? Jelentkezzen ki minden alkalommal a Facebook fiókjából.

Források:
http://www.securitynewsdaily.com/2023-5-steps-credit-card-security.html
http://www.securitynewsdaily.com/1767-banking-trojans-online-banking.html
http://www.securitynewsdaily.com/668-protect-yourself-from-data-breaches.html
http://www.securitynewsdaily.com/1993-top-mobile-banking-security-tips.html

# Az információbiztonságra, hálózatbiztonságra vonatkozó szabályozások az Egyesült Államokban

Mikor jogi szabályozásokat kutatunk, követendő példákat keresünk, és tanulni igyekszünk, célszerű mindig azon ország jogát hívnunk segítségül, ahol a kutatott területet feltalálták, vagy ahol köztudottan a legnagyobb odafigyeléssel igyekeznek alakítani rajta.

Elég csak az ARPANET-re[33] gondolnunk és máris egyértelmű, hogy információbiztonság, hálózatbiztonság valamint Internettel kapcsolatos kérdések esetén az Egyesült Államok hatályos szabályozását érdemes megvizsgálnunk, kutatnunk. Az Egyesült Államokat nevezhetjük az Internet és a hálózatbiztonság szülőbölcsőjének, és mind a mai napig élenjárónak az ezzel kapcsolatos fejlesztések, szabályozások valamint rendszerek fejlesztésében.

A kontinentális jogrendszerektől eltérve jellemző az USA jogalkotására, hogy bár jelenleg egyre sűrűbben, de viszonylag ritka, és különösen fontos esetekben nyúlnak a törvényalkotás eszközéhez. Viszonylag sok törvényből és különböző szintű jogalkotások eredményeiből tevődik össze az a jogszabály halmaz, melyet az egyes hálózatbiztonsági incidensek ill. események esetén vizsgálni kell, ha azok az Egyesült Államokban valósultak meg. Ugyanakkor a jelenleg formálás alatt lévő Európai Uniós jogszabályok kialakításánál is célszerű ezeket alapul venni, illetve tanulni belőlük.

A teljesség igénye nélkül, a következő jogszabályokról, rendelkezéseket célszerű megismerni:

- Clinger- Cohan Act (**CCA**)
- Federal Information Security Management Act (**FISMA**)
- Cyber Intelligence Sharing and Protection Act **(CISPA)**

33 http://en.wikipedia.org/wiki/ARPANET

Ezen jogszabályok vizsgálatakor fontos tisztázni: vannak, amelyek a kormányzati informatika, kormányzati szintű információbiztonságot hivatottak szabályozni (pl. CCA, FISMA), s ehhez kapcsolódnak azok jogszabályok, melyek a nemzetbiztonság, az ország kiberbiztonságának az érdekéből készülnek, készültek (CISPA).

Tekintettel ezen szabályozások összetettségére, bemutatásuk több részletben történik meg. Jelen cikkben a kormányzati rendszerek biztonságára vonatkozó szabályokat mutatjuk be.

## A kormányzati informatikára, hálózatokra, kiberbiztonságra vonatkozó szabályozások

A kormányzati és állami informatikai biztonság és irányítás területén a kormányzati ügynökségekkel és hivatalokkal kapcsolatosan, a már hatályban lévők közül, két szövetségi törvény bír meghatározó jelentőséggel az Egyesült Államokban. Az 1996-os Clinger- Cohan Act (CCA), más néven az Information Technology Management Reform Act (ITMRA), és a 2002-es Federal Information Security Management Act (FISMA), és végül 2012-ben a Cyber Intelligence Sharing and Protection Act (CISPA), mely még nem lépett hatályba.

Az Egyesült Államokban többszintű jogi szabályozás van érvényben, így jelen esetben meg kell különböztetni a szövetségi (federal law) és az adott állam (state law) törvényeit. A szövetségi törvények és az Egyesült Államok alkotmánya jelentik a legmagasabb szintet, a jelen összefoglalóban érintett törvények szövetségi törvények. Az egyes államok törvényei eltérhetnek, de nem lehetnek ellentétesek az egyes szövetségi törvényekkel.

A CCA és a FISMA is a szövetségi kormányzat ügynökségei részére ír elő kötelezettségeket és követendő szabályokat.

### A CCA

A CCA alapvető célja az volt, hogy átláthatóbbá tegye a kormányzati hivatalok beszerzéseit, meghatározza a felelősségi köröket, és kötelezővé tegye egy informatikáért felelős vezető kijelölését.

Így hát a CCA megalapította az egyes kormányzati ügynökségek informatikai beszerzésekért való felelősségét, továbbá a Kereskedelemért felelős Miniszter és a Nemzeti Szabványügyi és Technológiai Intézet feladatává tette az informatikai beszerzésekre vonatkozó szabályozások kidolgozását, és a kormányzati ügynökségek és hivatalok informatikai rendszerére vonatkozó szabályozások és biztonsági szabványok kidolgozását.

Ennek biztosítására, a kidolgozott szabályzatok és szabványok betartatása érdekében a CCA létrehozta az Informatikai Vezető pozícióját. Az Obama adminisztráció oly módon igyekszik kiterjeszteni a Informatikai Vezető hatáskörét, hogy azok ne csak a szabályzatok és szabványok betartásáért és az informatikai rendszer karbantartásáért legyenek felelősek, hanem legyen beleszólásuk erőforrások felhasználásába, és az egyes intézmények informatikai biztonságának feltételeinek kialakításába.

### A FISMA

A FISMA célja már jóval túlterjeszkedett a beszerzésekért való felelősség és az általános felelős kijelölésén. Miután a kormányzat felismerte a minőségirányítás követelményét, célszerűnek tartották törvényi szinten szabályozni. A FISMA kötelezővé tette a kormányzati ügynökségek számára az informatikai rendszereik biztonságának garantálását, fejlesztését, és dokumentálását, a követendő keretrendszer létrehozását pedig a Nemzeti Szabványügyi és Technológiai Intézet feladatává tette.

Az alábbi keretrendszereknek, szabványoknak kell megfelelniük az egyes kormányzati ügynökségeknek:

- informatikai rendszerek nyilvántartása (NIST SP 800-18)
- információk és információs rendszerek biztonsági szintek szerinti kategorizálása (FIPS PUB 199)
- minimum teljesítendő biztonsági szint (FIPS 200, NIST Special Publication 800-53)
- rendszer biztonsági terv
- kockázat kezelési terv

## A CISPA

Kijelenthető, hogy a CISPA a kiber-biztonság területén történő szabályozások egyik legjellemzőbb példája, különös tekintettel arra az irányvonalra, amit kijelöl. Az Obama adminisztráció alatt, 2011 novemberében nyújtották be ezt a javaslatot, melyet végül a kongresszus 2012 áprilisában fogadott el. A törvény alapvető célja, hogy lehetővé tegye a kormányzat és a magánszektor szereplői közötti adat illetve információ megosztást, átadást, hogy ha azt nemzetbiztonsági érdek megkívánja.

A CISPA lehetővé tenné a cégeknek, például a telekommunikációs szolgáltatóknak, hogy megosszák ügyfeleik kommunikációját az olyan kormányügynökségekkel, mint az egyre nagyobb hatalomhoz jutó Nemzetbiztonsági Ügynökség, az NSA. A jogszabály mentesíti a magáncégeket az ügyfeleik iránti felelősség alól, ha jóhiszeműen adták át az adataikat az ügynökségeknek, emiatt az ügyfelek nem perelhetik őket.

A CISPA egy korábbi verziójában a megszerzett információk „kiberbiztonsági" vagy „nemzetvédelmi" célokra történő felhasználását tette volna lehetővé a kormány számára. Ezeket a célokat a kongresszus által elfogadott változat sem nem korlátozta, sem nem törölte, hanem további két területtel bővítette: a kiberbiztonsági bűntettek nyomozása és bűnvádi eljárása során és gyermekvédelmi céllal is felhasználhatók. A meghatározás szerint kiberbiztonsági bűntettnek tekintendő minden olyan cselekmény, ami egy hálózat feltörésével, akadályoztatásával vagy leállásával vagy a CFAA (Számítógépes csalás elleni törvény, a következő cikkben kerül majd bemutatásra) megszegésével jár.

Ennek fényében a CISPA már nem csupán egy kiberbiztonsági törvény. Egyes jogászi állásfoglalások szerint ez értelmezhető úgy, hogy a kormány felhatalmazást kapna, hogy a CISPA alapján gyűjtött információt amerikai állampolgárokkal kapcsolatos nyomozásra használja, teljes mentességet élvezve a felelősségre vonás alól, illetve nem szükséges betartania az adatvédelmi törvényeket, amennyiben kijelentik, hogy a vizsgált személy „kiberbiztonsági bűntettet" követett el. Ezzel azt mondja ki, hogy az amerikai alkotmány negyedik módosítása (kiegészítése) a világhálón nem érvényes. Emellett az összegyűjtött adatokkal azt csinálnak amit akarnak, amennyiben kijelentik, hogy valakinek a testi épsége veszélyben volt, illetve, hogy az ügyben egy gyerek valamilyen módon veszélyeztetve van.

Hasznos módosítás, hogy egy hálózat vagy oldal felhasználási feltételeinek megszegése már nem számít jogosulatlan hálózathasználatnak (ennek részletes bemutatása a következő cikkben).

A CISPA még nem lépett hatályba, ehhez szükséges a Szenátus részéről való elfogadása és Obama elnök jóváhagyása is. Mindenesetre jól mutatja azt az irányt, mely felé a jelenlegi szabályozási törekvések mutatnak, és amit az Európai döntéshozók is várhatóan a jövőben követni fognak.

## Konklúzió

Ahogy fejlődött az Internet és az informatika, úgy kezdte el fokozatosan szabályozni az amerikai kormányzat is ezt a területet. Ahogyan a fenti rövid összefoglalóban is látszik, egymást követően kerültek és kerülnek szabályozás alá azok a területek, melyek mind kormányzati szempontból, mind a magánszektor szempontjából lényegesek az informatika világában, és az online biztonságunk garantálása céljából vele kapcsolatba hozhatóak.

Jelenleg mind Európában, mind Magyarországon keresik a választ ezekre a szabályozási kérdésekre. Érdekes tanulság annak felismerése, hogy szükség van a kormányzati intézményekben is egy informatikai biztonságért felelős vezető kijelölésére, továbbá annak felismerése, hogy az informatikai beszerzések és fejlesztések összehangolása milyen fontos, valamint, hogy azok előre kialakított megfelelő szabványok szerint történjenek, és ily módon lehetővé váljon a FISMA és CCA alapján az egyes kormányzati intézményekben az informatika rendszerek minőségirányításának kialakítása.

Az információbiztonság kérdése nem csupán a bankokban, és a nagy mennyiségű adatokkal foglalkozó multi cégeknél válik fontos kérdéssé. A kormányzati szerveknél koncentrálódó személyes adatok mennyisége, azok összekapcsolhatósága olyan kockázati kérdést rejt magában, melyet szükséges kormányzati szinten kezelni. Ebből kifolyólag Magyarországon is szükséges a szabályozás oly módon való kialakítása, hogy minden intézménynél legyen egy meghatározható informatikai, információbiztonsági felelős, aki gondoskodik az adott intézményben használt rendszerek minőségirányításáról. Ugyanakkor nem szabad megfeledkezni a megfelelő dokumentációs, nyilvántartási szabályok kialakításáról, és célszerű ezen esetekben a már bevált nemzetközi szabványokat alkalmazni.

Különösen érdekes kérdéseket vet fel a jövőbeni hazai és európai szabályozással kapcsolatosan a CISPA mint követendő példa, illetve, hogy követendő-e mint példa. Míg a CCA és a FISMA kapcsán egyértelműen kijelenthető, hogy szükséges azok átültetése a magyar jogi szabályozásba, addig a CISPA már egészen más kérdéseket vet fel. Bizonyos mértékig ugyanis a hatályos jogi szabályozás is lehetőséget ad a CISPA-ban meghatározott információk kikérésére, azonban jellemzően a magyar jogi szabályozásra, az nem egy törvény keretében van szabályozva, és így sérül a jogrendszer transzparenciájának követelménye. Ugyanakkor egy CISPA jellegű, önálló törvény hazai megalkotása olyan irányvonalat mutatna, ami nem feltétlenül váltaná ki a magyar társadalom támogatását, hasonlóan az amerikai társadalom reakcióihoz. Új területek szabályozását megelőzően fontos és érdemes megvizsgálni a más országokban már bevált példákat, és hazai szokásokhoz és jogrendhez illeszkedő legjobb megoldásokat átvenni. Azonban ilyenkor is vizsgálni kell azt, hogy mi a szabályozással elérendő cél, és csak a legjobb megoldásokat átvenni.

Következő cikkünkben a magánszektorra vonatkozó szabályozásokat, így a számítógépes csalás, szerzői jog, és a telekommunikációs eszközök működésére vonatkozó szabályokat fogjuk ismertetni.

## A VirusBuster Kft. összefoglalója 2012 második negyedévének IT biztonsági trendjeiről

Milyen fontos, netán trendjelző események játszódtak le tavasszal, s a nyár elején az informatikai biztonság területén? Milyen új fenyegetésekkel kell számolnunk? Mi a helyzet a kisebb-nagyobb kiberháborúságok frontjain? Hogyan igyekeznek védekezni a támadások ellen állami és szervezeti szinten?

Beszámolónkban nemcsak ezekre a kérdésekre igyekszünk válaszolni, hanem – egyebek mellett a VirusBuster Kft. víruslaboratóriumának észlelései alapján – áttekintést nyújtunk a 2012. március-június időszak 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. Reméljük, hogy összefoglalónk mind a szervezeti, mind az egyéni felhasználók számára hasznos olvasnivalónak bizonyul.

# Olimpiára (és támadásokra) készülve

Ha szökőév, akkor Olimpia. Ha 2012, akkor London. A világ szeme a ködös Albion felé fordul idén nyáron. És a világból érkező tekintetek nem feltétlenül jóindulatúak. Mi több, nemcsak a hagyományos értelemben vett terrortámadások jelentenek veszélyt. „A pekingi játékok idején 12 millió IT biztonsági incidens történt” – emlékeztetett május elején *Francis Maude,* a brit miniszterelnöki hivatalt vezető miniszter. „Speciális egység segíti majd a Londoni Olimpia kibertámadások elleni védelmét” – tette hozzá.

A világ sportolóinak nagy találkozója, ez a ritka alkalom persze csak a jéghegy csúcsa. Nemzetállamok, kormányzatok, nagy- és kisvállalatok, nemzetközi szervezetek és magánemberek egyaránt mind több és kifinomultabb támadásnak vannak kitéve.

Jól jelképezi ezt magának Francis Maude-nak a személye. A politikus ugyanis a brit Kiberbiztonsági Hivatal (Office for Cyber Security) vezetője is, s eme utóbbi minőségében mindjárt arról is beszélt: országa az informatikai behatolásokat nemrég a nemzetbiztonságot fenyegető legsúlyosabb tényezők közé – a terrorizmussal azonos kategóriába – sorolta. „Egy felmérés szerint az elmúlt egy évben minden hetedik nagy szervezet rendszerét feltörték. A nagy szervezeteket átlagosan hetente, a kisebb cégeket nagyjából havonta éri külső támadás” – jelentette ki.

A miniszter az infrastruktúra-védelem kiépítésében fontos lépésnek nevezte a brit Nemzeti Kiberbiztonsági Program beindítását. Mint mondta, az elmúlt négy évben a szigetországban 650 millió fontot fordítottak az IT támadások kivédésre, s az idei költségvetésben 400 ezer fontot különítettek el egy internetes biztonsági ismeretterjesztő kampányra.

Szinte folytatta Maude szavait *Jonathan Evans,* a brit nemzetbiztonsági szolgálat, a híres MI5 vezérigazgatója. Egy június eleji konferencián tartott előadásában elmondta: tucatnyinál több vállalat ellen indított kibertámadás ügyében nyomoznak. Közülük egy meg nem nevezett londoni cégnek 800 millió fontos kárt okoztak a behatolók.

„A sérülékenységeket a világhálón agresszíven kiaknázzák – mégpedig nemcsak bűnözők, hanem nemzetállamok is. A nagyságrendek megdöbbentőek. Ipari méretű folyamatokkal kell számolnunk. Az államilag finanszírozott kiberkémkedés és a szervezett számítógépes bűnözés ezreket foglalkoztat – figyelmeztetett Evans. – Mindez nemcsak a kormányzati információvagyon integritását, titkosságát és rendelkezésre állását veszélyezteti, hanem a vállalati szférát és a

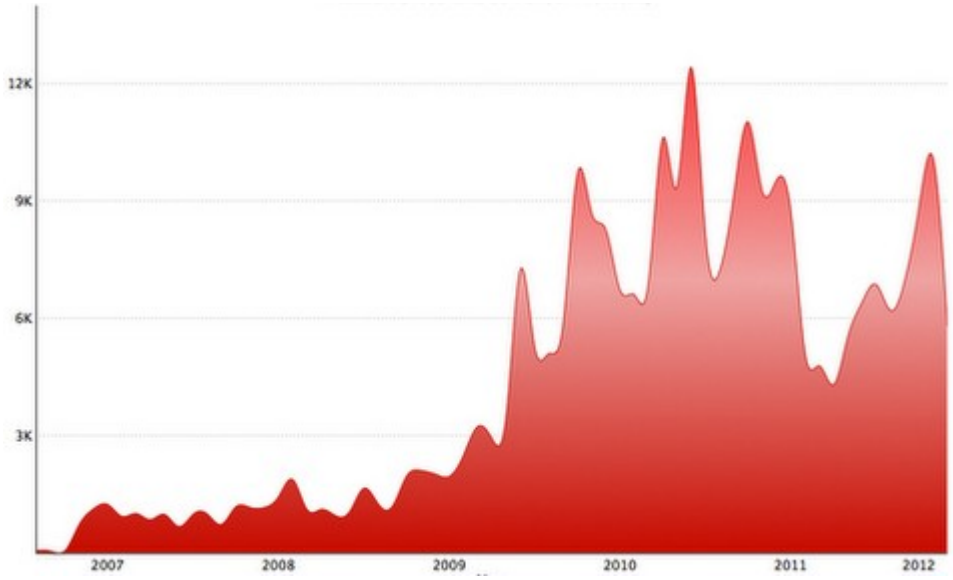
tudományos intézményeket is. Nem pusztán kormányzati titkok forognak kockán: infrastruktúránk és szellemi tulajdonunk biztonsága a tét. Márpedig ez utóbbiak jelentik jövőnk zálogát, az üzleti információ bizalmasságának megőrzése pedig létkérdés vállalataink számára."

Hogy valóságos új iparágról van szó, jelzi az Európai Parlament Polgárjogi Bizottságának áprilisi javaslata is. Az EU-s testület azt ajánlja: ne csak a magánembereket, hanem a jogi személyeket is terhelje büntetőjogi felelősség az általuk végzett vagy megrendelt kibertámadások miatt. A Google pedig nemrég azzal lepte meg a biztonsági ágazatot, hogy bejelentette: figyelmeztetni fogják a Gmail-felhasználókat, ha a fiókjukat „gyaníthatóan nemzetállam által szervezett támadás" érte.

Persze a kockázatért, a károkért nem kis részben a felhasználók – magánszemélyek és szervezetek – is felelősek. Egy-két tucat ország közel 30 millió PC-jét felölelő felmérés június végén nyilvánosságra hozott eredményei szerint a gépek 17 százalékán vagy egyáltalán nem volt védelmi szoftver, vagy ha volt is, nem működött.

Eközben pedig – mint a Google adatai az alábbi grafikonon mutatják – az idén újabb csúcsot ért el a világhálón vadászó támadó site-ok száma.

Észlelt támadó site-ok száma (ezer db)




*Forrás: Google*

Bár a védelmi szoftver működőképes és naprakész állapotban tartása nyilvánvalóan alapvető fontosságú, a védekezés hosszú távon, társadalmi szinten csak akkor lehet eredményes, ha a cégek nem hallgatják el az incidenseket – mutatott rá egy másik brit vezető. *David Willetts* tudományért és felsőoktatásért felelős miniszter hangsúlyozta: ehhez a vállalati kultúrában ugyanolyan változásra lenne szükség, mint ahogy egy évtizeddel ezelőtt a bankok változtattak a pénzügyi csalásokkal kapcsolatos korábbi titkolódzásukon.

Egyébként nem meglepő módon elsősorban továbbra is a pénzintézetek szenvedik el a legtöbb támadást. Az elosztott szolgáltatásmegtagadási (DDoS) támadások vizsgálatára szakosodott Prolexic a bankok és biztosítók körében az idei év első három hónapjában gyakorlatilag ugyanannyi támadást észlelt, mint 2011. azonos időszakában, ám a rosszindulatú adatcsomagok száma a tavalyi első negyedévben mért 14 milliárdról 1,1 billióra ugrott, s a kifinomultabb, alkalmazás-réteg elleni támadások száma 6 százalékkal emelkedett. Az akciók mind koncentráltabbak – kevesebb ideig tartanak, ám nagyobb sávszélességet kötnek le. Míg a támadások átlagos sávszélessége egy éve 5,2 Gbps volt, idén már 6,1 Gbps-sel dolgoztak a hackerek. A legtöbb támadás Kínából indult ki, de az Egyesült Államok és Oroszország „javított" korábbi helyezésén – derül ki a Prolexic jelentéséből.

Szerencsére hazánkban is megvan az érdeklődés az IT biztonság ügye iránt. Májusban már ötödször örülhettünk annak, hogy telt ház várja a NetAcademia Oktatóközpont által szervezett Ethical

Hacking konferencia előadóit. Nyitóelőadásában *Fóti Marcell,* a központ vezetője a lassan megkerülhetetlenné váló felhő alapú számítástechnika biztonsági kockázatairól beszélt. Természetesen szó esett a rendezvényen a mobil fenyegetésekről és kiberhadviselésről is.

## Harci szellem

Az informatikai eszközökkel vívott háború témája a mögöttünk álló negyedévben jóval túllépte a konferenciatermek falait. A tévéképernyők, a rádióállomások, az online és nyomtatott sajtó nagy szenzációja a minden idők legkifinomultabb kiberfegyvereként beharangozott kártevő, a Flame volt. Szakemberek már két éve ismerték a kórokozót, amely hirtelen intenzív aktivitásba kezdett a Közel-Keleten, de hazánkban is.

Mint kiderült, fegyverről beszélni nem volt alaptalan. A negyedév vége felé nagy meglepetést keltett a *New York Times* egy cikke – nem annyira a tartalmával, hanem azzal, hogy nyilvánosan szólnak a témáról. Ebben nemcsak azt a régóta hangoztatott hipotézist erősítették meg, hogy a Stuxnet féreg valójában amerikai-izraeli katonai eszköz volt, melyet az iráni atomprogram megzavarására fejlesztettek ki, hanem azt is leírták: a Flame hasonló céllal, ugyanannak az „Olimpiai játékok" fedőnevű hadműveletnek a keretében készült.

Igazából a világsajtó rohamát maguk az irániak váltották ki azzal, hogy olajipari és nukleáris rendszereik elleni kibertámadásokról, illetve azok sikeres kivédéséről adtak hírt. Hogy ezekért valóban a Flame volt-e felelős, nem tudni.

Az első nagy szenzációhullám elülte után biztonságtechnikai szakértők visszafogottabb hangot ütöttek meg a kártevővel kapcsolatban. A kód ugyan hatalmas – 20 megabájtos méretével nagyjából 40-szer akkora, mint a Stuxnet –, ám korántsem tűnt olyan veszedelmesnek és sokoldalúnak, mint azt korábban gondolták.

Akárkik is álltak a Flame mögött, megelégelték a nagy publicitást. Június első hetében kutatók azt észlelték, hogy a kártevő irányítói önmegsemmisítési parancsot adtak a kódnak.

Érdekes ága az ügynek, hogy a kórokozó alkotói olyan – súlyos – biztonsági rést használtak ki a hitelesítésben, aminek eredményeként a kártevő komponensei Microsoft által hitelesített programnak tudták álcázni magukat. Így nem csoda, hogy a szoftveróriás különös figyelmet szentelt a Flame-nek: soron kívüli biztonsági tájékoztatót és Windows-foltot bocsátott ki miatta.

Zajlott a csöndes kiber- és szópárbaj a negyedévben egy másik, régóta álló fronton is: az Egyesült Államok és Kína között. Április közepén híre kelt: tavaly júniusban a két fél állítólag titkos, békéltető célú „közös gyakorlatot" tartott a washingtoni Stratégiai és Nemzetközi Tanulmányok Központja (Center for Strategic and International Studies, CSIS), illetve a Modern Nemzetközi Kapcsolatok Kínai Intézete közvetítésével. A két delegációnak akkor előbb arra a kérdésre kellett – egymással egy időben – válaszolnia: milyen lépéseket tennének, ha egy Stuxnet jellegű kártevővel támadnák meg őket, majd pedig arról kellett nyilatkozniuk: mit tennének, ha kiderülne, a másik ország indította a támadást.

Sajtóértesülések szerint hasonló gyakorlatot terveztek idénre is, ám az Egyesült Államok szerint a kínaiak továbbra is nagy erőkkel igyekeznek amerikai katonai és más stratégiai információkhoz hozzájutni. A hadügyi szállító óriáscég, a Northrop Grumman nemrég közzétett tanulmányában azt állítja: a Kínai Néphadsereg fejlett informatikai hadviselési kapacitása konfliktus esetén „valódi veszélyt" jelent nemcsak az amerikai haderőre, hanem az ország kritikus infrastruktúrájára nézve is. A Pentagon pedig azzal vádolta Kínát, hogy az űrkutatásban elért látványos eredményeit a „sikeres kémkedésnek" köszönheti.

Kína tagadja a vádakat. Azt hangoztatja: maga is támadások áldozata. Az ázsiai ország számítástechnikai katasztrófavédelmi központja nemrég azt jelentette: míg 2010-ben 5 millió határokon kívülről indított támadás érte a kínai szerveket, tavaly ez a szám már elérte a 8,9 milliót.

A NATO egy magas rangú tábornoka ugyanakkor a Nemzetközi Kiberkonfliktus Konferencián (International Conference on Cyber Conflict, CyCon) azt hangoztatta: a katonai szervezet tervei között egyelőre nem szerepel informatikai támadó eszközök kifejlesztése. A gondolattal szemben „nagy a politikai, jogi és diplomáciai ellenállás – jelentette ki. – Hatalmas kockázat áll az esetleges haszonnal szemben." Újságírók hozzáteszik: a NATO jelenlegi akcióterve 2015-ben zárul le.

Ugyanakkor a DPA német hírügynökség június eleji híre szerint az ország hadseregének 2006. óta van IT hadviselő egysége, sőt zárt laboratóriumi körülmények között támadás-szimulációkat is végeztek. Az persze nem derül ki a jelentésből: mekkora egységről van szó, s milyen műveleteket hajtottak végre.

## Közösségi hálózatok küzdelmei

Könnyen átterjedhet az informatikai eszközökkel vívott háború vagy polgárháború a közösségi hálózatokra is – mutatott rá május közepén egy konferencián *Phillip Hallam-Barker,* a Comodo csoport elnökhelyettese és tudományos igazgatója. „Az Arab Tavasz és más hasonló társadalmi megmozdulások óta az internettel kapcsolatos döntések a legmagasabb kormánykörökhöz kerültek" – hangsúlyozta. Ami a Facebookon, a Twitteren és más közösségi hálózatokon történik, az államérdeket sérthet vagy támogathat. Következésképpen jó, ha az üzemeltetők tudják: nemcsak magányos hackerek vagy bűnszövetkezetek, hanem államok részéről is könnyen támadás érheti őket – figyelmeztetett a szakember.

Szerencsére egyelőre ilyen jellegű incidensről nem érkezett hír. „Hagyományosnak" tekinthető akciókról annál inkább. Május vége felé például két Facebook vonatkozású kártevő-kampányt is észleltek. Előbb a hálózat chat (IM) szolgáltatásán fedeztek fel egy férget. Majd olyan spamet jeleztek, amely azzal igyekezett a címzetteket rávenni a kártékony csatolmány megnyitására, hogy Facebook fiókjuk lezárásával riogatta őket.

Figyelemre méltó híre a negyedévnek egyébként, hogy a Facebook együttműködési megállapodást kötött az IT biztonsági ágazat öt nagy képviselőjével: a McAfee-vel, a Microsofttal, a TrendMicróval, Sophos-szal és a Symantec-kel. A szerződésnek két fő eleme van. A közösségi hálózat átadja URL feketelistáját biztonsági partnereinek – akik egyébként is generálják azt –, hogy még hatékonyabban védhesse felhasználóit a rosszindulatú linkektől. Másfelől a Facebookon antivírus piacteret hoztak létre, ahol az öt cég kínálhatja portékáját. Ezen kívül a gyártók cikkeket jelentetnek meg a Facebook biztonsági blogjában – ahol mellesleg magát a szerződést is bejelentették.

Biztonsági körökön messze túlnyúló publicitást azonban nem a Facebook vagy a Twitter szerzett a negyedévben a közösségi médiumok közül, hanem a LinkedIn. Június elején szakmai kapcsolatok építésének közkedvelt fórumáról mintegy 6,5 millió jelszót emeltek el, ami hatalmas visszhangot váltott ki a felhasználók és a szakma köreiben egyaránt. A tettesek egy Dropbox-hoz hasonló orosz site-on tették közzé zsákmányukat, amelyben – hangsúlyozták a LinkedIn-nél – nevek vagy e-mail címek nem szerepeltek. A cég üzenetben értesítette az áldozatokat arról, hogy jelszavukat törlik, s arról, hogyan kaphatnak helyette újat. Egyszersmind az FBI-hoz fordultak az ügyben.

Szakemberek külön szóvá tették, hogy bár a LinkedIn alkalmazott titkosítást, az nem volt kielégítő, így a jelszavak egy részét megfejthetik a hackerek. Hálózat-tagok arról számoltak be, hogy a betörést spam- és adathalászlevél-hullám követte. Június végén azután amerikai felhasználók egy csoportja beperelte a LinkedIn-t, amiért „nem gondoskodott a személyes beazonosítást lehetővé tevő információ megfelelő védelméről". Várjuk a fejleményeket...

## Anonim akciók

Szinte nem telik el hét úgy, hogy a névtelenség nevét választó hírhedt nemzetközi hackerszervezet, az Anonymous ne hallatna magáról. Április elején mindjárt azzal hívták fel magukra a figyelmet, hogy közel félezer kínai site-ot – köztük regionális kormányzati lapokat – törtek fel, saját szövegüket függesztették ki rájuk, s csatlakozásra buzdították a helybeli hackereket is.

Egy hacktivista – fedőnevén *Hardcore Charlie* – ugyanazon a héten azt állította: betört egy kínai katonai szállító, a CEIEC rendszerébe, ahonnan az afganisztáni amerikai katonai jelenléttel kapcsolatos dokumentumokat emelt el és tett közzé. A cég sietett cáfolni a hírt, ám Hardcore Charlie újabb amerikai katonai adatok megjelentetésével válaszolt, melyeket állítólag a CEIEC Vietnámnak, Ukrajnának és Oroszországnak adott át. A vállalat szerint légből kapott rágalomról van szó.

Ugyancsak április elején az Anonymous DDoS támadást mért a brit belügyminisztérium site-jára. A weblapok egy hétvégére elsötétültek... Hasonló akciót indítottak a brit miniszterelnök és az igazságügy-minisztérium site-ja ellen – mint írták, a szigetország kiadatási törvényei elleni tiltakozásul.

A következő áldozat a hivatalos Forma 1-es site volt, amelyet a Bahrainben rendezett vitatott nagydíj ürügyén kapcsolt le a hackercsoport.

Májusban nem kisebb személyiséget vettek célba, mint *Vlagyimir Putyint*. Az orosz elnök újraválasztása elleni tiltakozásul DDoS akciójukkal rövid időre leállították a kremlin.ru site-ot. A Kreml elismerte, hogy az Anonymous megfenyegette őket, s hogy támadás történt, hozzátéve: „egyelőre nem tudjuk megállapítani, hogy ki állt a támadás mögött". „Sajnos a technológiai biztonsági fenyegetések korában élünk, ám megvannak az eszközeink arra, hogy ellenálljunk nekik" – állt a nyilatkozatban.

Röviddel később az indiai elnöknek és az ország számítástechnikai katasztrófavédelmi központjának (CERT-jének) webhelye tűnt el egy időre az Anonymous DDoS kampányának csapásai alatt. Egy mezőgazdasági gépgyártó is áldozatul esett – a céget feltehetőleg csak azért vették célba, hogy ezzel is „jobb belátásra" késztessék a kormányt, amely a video- és fájlcsere portálok betiltásával váltotta ki a hacktivisták haragját.

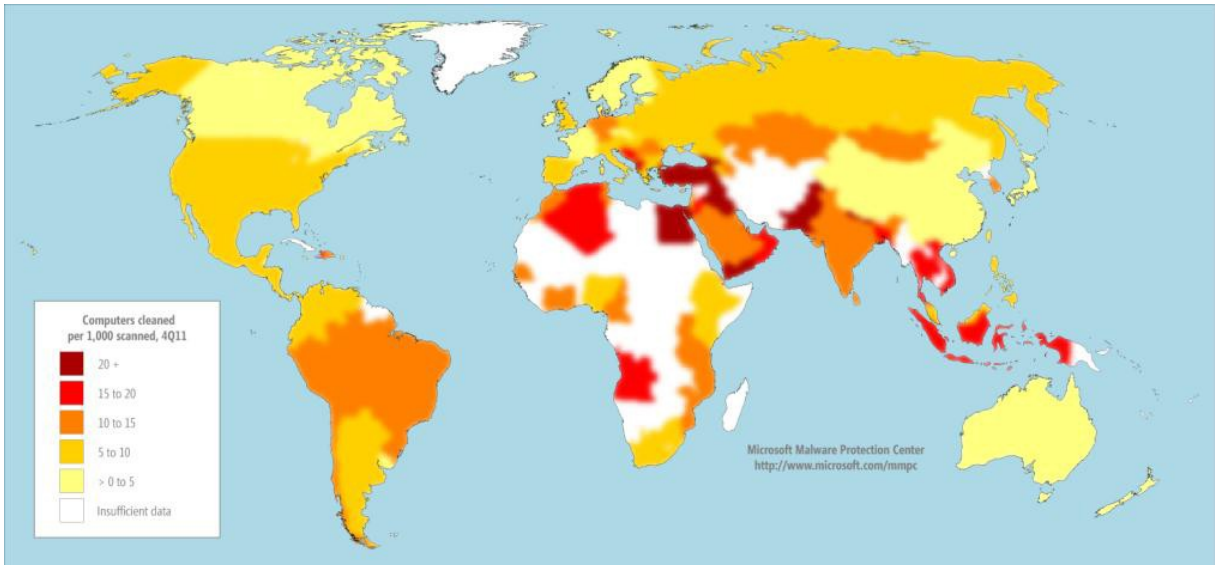
Jelentéktelennek minősítette a hackerek akcióját a következő áldozat, az amerikai igazságügyi statisztikai hivatal (US Bureau of Justice Statistics), amelytől 1,7 gigabájtnyi adatot szívtak le, s tettek közzé a támadók. A hivatal szerint csak egy publikus adatokat tároló szerverre törtek be, s website-juk mindvégig zavartalanul működött, nem beszélve az Igazságügy-minisztérium központi webhelyéről, a justice.gov-ról.

## Kiemelkedő kártevők

Az eddigiekből már nyilvánvaló: 2012 második negyedévét is átjárta a kártevők áradata. Jutott belőlük a világ minden tájára. Persze nem egyformán: a védekezési és frissítési kultúrától függően szokás szerint egyes térségekben az átlagnál jóval nagyobb a fertőzött gépek aránya.

Az alábbi térkép a Microsoft Biztonsági Kutatási Jelentésének 12. kiadásából (Security Intelligence Report, SIRv12) származik. Az anyag a feldolgozás miatt elkerülhetetlen késleltetés folytán 2011 második félévét értékeli ugyan, ám aligha valószínű, hogy a térkép az idei első negyedévben jelentősen megváltozott volna. A szoftveróriás biztonsági szakemberei azokat az adatokat értékelték ki, amelyeket a Windows Rosszindulatú Szoftvert Eltávolító Eszközétől (Malicious Software Removal Tool, MSRT) kaptak. A fertőzöttségi arányt az MSRT ezer végrehajtására során valamilyen kártevőtől megtisztított gépek átlagos számával (computers cleaned per mille, CCM) fejezik ki. A legutóbbi merítésbe világszerte 600 milliónál több gép került bele.

Fertőzött gépek aránya térségenként (CCM, 2011. II. félév)




*Forrás: Microsoft Malware Protection Center*

A Google alábbi grafikonja pedig a kártevőforrások egyikéről ad képet: a havonta felfedezett fertőzött site-ok számát mutatja. Noha lényegesen kedvezőbb a helyzet, mint három évvel ezelőtt, rózsásnak igazán nem mondható.

Fertőzött site-ok száma (ezer db)


*Forrás: Google*

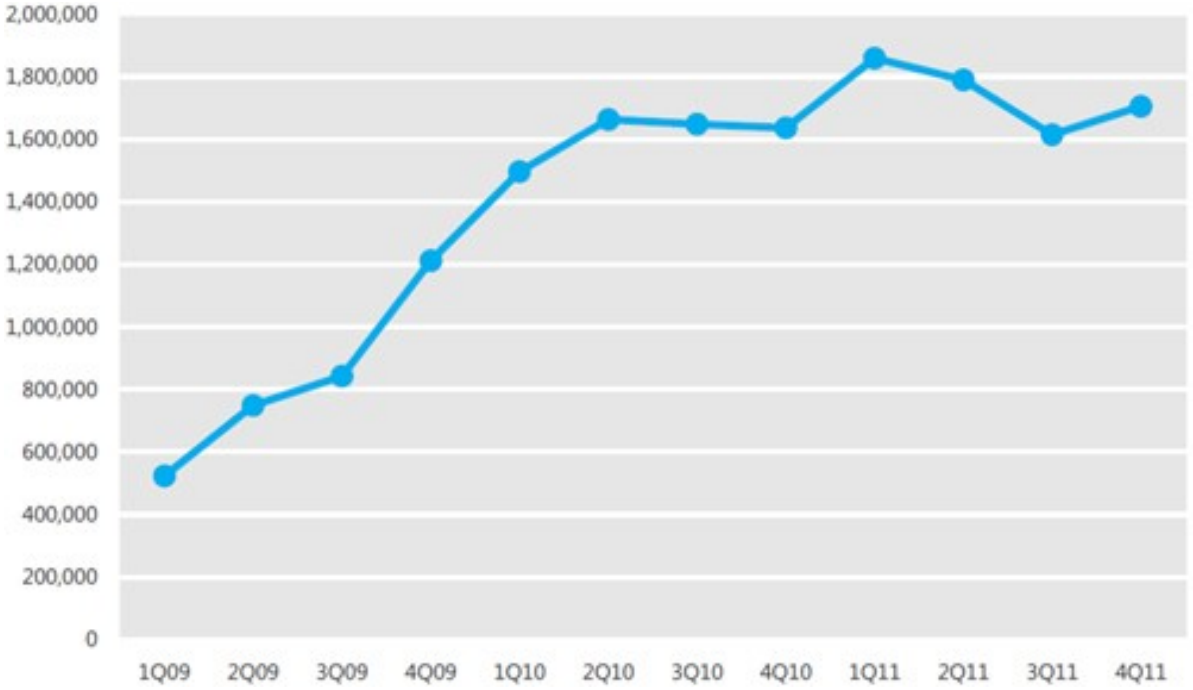
A fertőzött gépek tengerében különös figyelmet érdemelnek azok, amelyeken a DNSChanger nevű kártevő munkál. A kórokozó botnetbe szervezte a megtámadott gépet, s módosította annak DNS beállításait. Így a szörfösök automatikusan valamilyen rosszindulatú site-on landoltak. Tavaly novemberben az FBI lekapcsolta a botnet vezérlőszerverét, majd speciális DNS szervereket állított fel, amelyek a fertőzött gépek DNS-kéréseit helyesen oldották fel. A bíróság július 9-éig engedélyezte a szövetségieknek e helyettesítő szerverek üzemeltetését. Ha egy gépet nem tisztítanak meg a kártevőtől, az a határidő lejárta után DNS feloldás híján elvágja felhasználóit az internettől: sem e-mailt küldeni, sem a weben navigálni nem lehet majd rajtuk.

Amiért ennyi teret szentelünk az ügynek: a DNSChanger szakmai munkacsoport (Working Group) adatai szerint két héttel július 9-e előtt még mindig 300 ezer gép hordozta a fertőzést. Jóllehet ez jóval kevesebb, mint a járvány csúcspontján, amikor is 4 millióra tették a botnet tagjainak számát, még így is nem kevés aggodalomra ad okot a biztonsági szakemberek körében.

Talán a legaggasztóbb, hogy június vége felé közeledve az 500 legnagyobb cég (a Fortune 500) nem kevesebb, mint 12 százalékának hálózatán mutattak ki legalább egy fertőzött eszközt. A „jelentősebb" amerikai kormányszervek sem álltak sokkal jobban: körükben ez az arány 4 százalék volt.

Hasonlóan hajlamosak lennénk megfeledkezni a közelmúlt olyannyira rettegett réméről, a Conficker féregről, amely 2008 novemberében kezdett terjedni, s szerencsére nagyobb bajt nem okozott. A Microsoft már idézett Biztonsági Kutatási Jelentése azonban óvatosságra int. Mint a szerzők írják, a Conficker továbbra is olyan fenyegetés, amelyet a szervezeteknek komolyan kell venniük. Aki a részletes indoklásra kíváncsi, elolvashatja a Microsoft tanulmányában. Itt csak a kapcsolódó grafikont mutatjuk be, amely a szoftveróriás vírusirtóinak Conficker-észleléseit mutatja az idő függvényében. A telítésben ragadt görbe kiterjedt magyarázat nélkül is eléggé riasztó. Megjegyezzük: a VirusBuster statisztikáiban is folyamatosan élen járnak a Conficker-variánsok (a legutóbbi negyedévben, mint későbbi táblázatunk mutatja, a 14. helyen álltak).

Microsoft antivírus termékek Conficker-észlelései negyed-évenként, 2009-2011 között




*Forrás: Microsoft*

Mielőtt rátérnénk 2012. második három hónapjának statisztikai adataira, érdemes még pár szót szólnunk két jelenségről: a mobil és az almás kártevők mind gyakoribb felbukkanásáról. Amióta az okostelefonok milliárd darabos nagyságrendű számítástechnikai platformot alkotnak, nyilvánvalóan fokozottan vonzzák a kiberbűnözőket. Az Apple-felhasználók pedig hosszú időn át hamis biztonságérzetbe ringathatták magukat, ám egyre többször kell ráébredniük: az ő gépeik sem sebezhetetlenek.

Áprilisban két androidos trójairól érkezett hír. Az egyiket a Google hivatalos alkalmazás-áruházában, a Playben találták. Ezt a személyi adatlopót 15 alkalmazásban mutatták ki, s felfedezéséig mintegy 70 ezer – jórészt japán – felhasználó töltötte le. A másik programot nem hivatalos forrásokról terjesztették. A népszerű fotómegosztó alkalmazás, az Instagram „képében" jelent meg – egyebek között egy hivatalos Instagram site-ként tetszelgő orosz portálon.

Ugyancsak áprilisban kelt híre egy Macintoshra specializált trójainak, a Flashbacknek, amely egy Java rést kiaknázva fertőzte meg, s állította botnetbe áldozatait. Egyes becslések szerint mire az Apple befoltozta a lyukat, már hatalmas – jórészt észak-amerikai – zombihadsereg állt a Flashback gazdáinak szolgálatában. A különböző biztonsági cégek 270 és 670 ezer közé tették a tábor létszámát. Április közepén azután az almás cég megjelentette a Flashback-radírt, amellyel el lehetett távolítani a kártevőt a fertőzött gépekről.

Most pedig következzék a VirusBuster kártevő-toplistája, mely a legalább 1 százalékos részesedést elért kórokozókat tartalmazza. Mint látható, a mögöttünk álló negyedévben a magyar neten messze a leggyakoribb rosszindulatú program a Virut fájlfertőző vírus volt. Az „ezüstérmes” ZeroAccess napjaink egyik legnépszerűbb és legkellemetlenebb rootkitje.

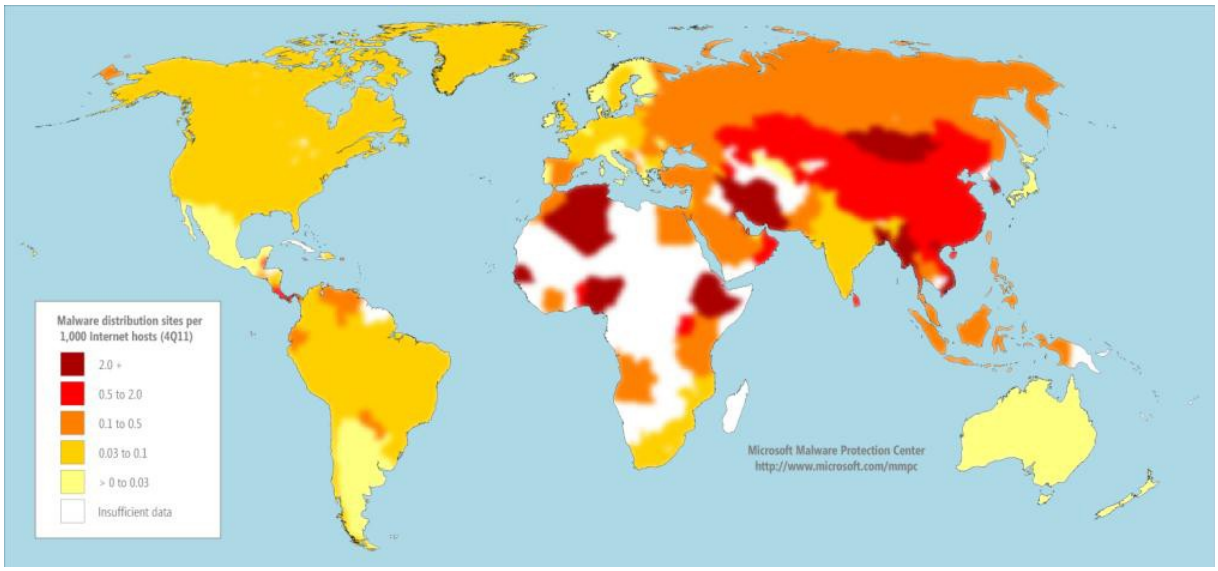
Feltűnhet az olvasónak a hatodik helyen álló Suspicious!SA elnevezés. „Ez a VirusBuster új, szabály alapú heurisztikus technológiájának (Enhanced Heuristics Detection, EHD) az eredményeit szemlélteti. Az EHD a rendszerben található futtatható állományok és környezetük tulajdonságainak az elemzésén alapul. Ennek köszönhetően sok olyan kártevőt is fel képes ismerni, amely még be sem került a víruslaborba – magyarázta Neumann Róbert, a cég víruslaboratóriumának vezetője. – Az, hogy a Suspicious!SA ilyen előkelő helyre került a táblázatban, jól tükrözi napjaink trendjeit. Az óránként, de leginkább percenként újrafordított vagy újracsomagolt kártevők korszaka még közel sem ért véget.”

A magyar net legelterjedtebb kártevői 2012 második negyedévében a VirusBuster víruslaboratóriumának észlelései szerint

| | Kártevő | Részesedés |
|---|---|---|
| 1 | Win32.Virut.Y.Gen | 36,67% |
| 2 | Rootkit.ZeroAccess.Gen.4 | 23,58% |
| 3 | Exploit.MS04-028 | 5,91% |
| 4 | Win32.Sality.BL | 5,47% |
| 5 | Trojan.PWS.Qbot | 4,66% |
| 6 | Suspicious!SA | 3,00% |
| 7 | JS.Iframe.Gen.5 | 2,96% |
| 8 | Win32.Sality.AP.Gen | 2,28% |
| 9 | Worm.Koobface | 2,21% |
| 10 | Packed/Upack | 2,07% |
| 11 | TrojanSpy.Zbot | 2,02% |
| 12 | Win32.Parite.B | 1,91% |
| 13 | I-Worm.Brontok | 1,50% |
| 14 | Worm.Conficker | 1,36% |
| 15 | Egyéb | 4,41% |

Az sem érdektelen, hogy a weben barangolva hol, mennyire kell fertőzéstől vagy adathalászattól tartanunk. Erre vonatkozóan alább megint csak a Microsoft Biztonsági Kutatási Jelentésének, illetve a Google-nak az adatai adnak támpontot.

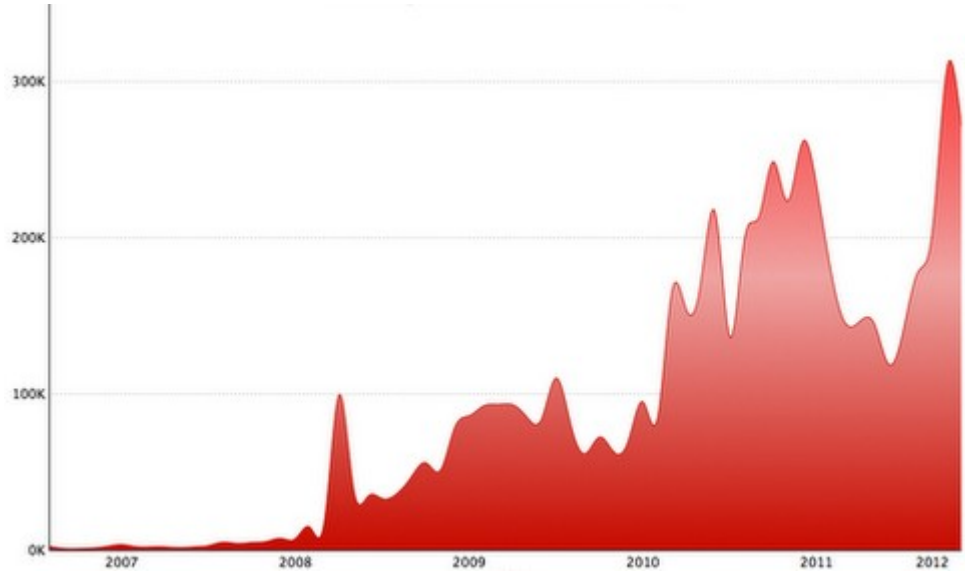
Kártevőterjesztő oldalak száma ezer hosztonként a világ egyes térségeiben (2011. II. félév)




*Forrás: Microsoft Malware Protection Center*

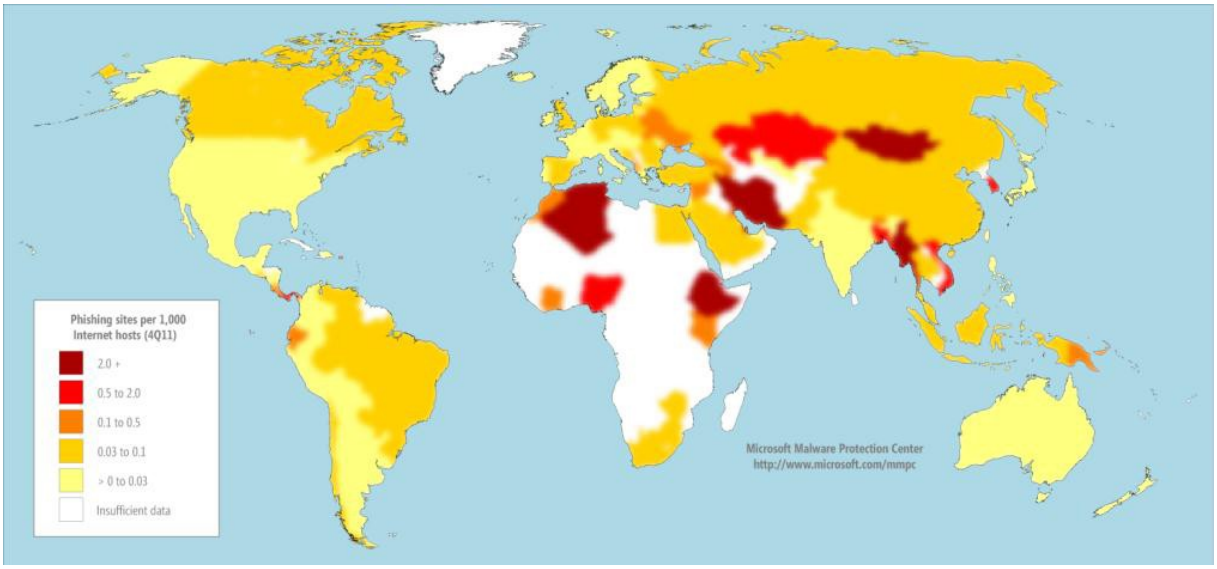
Csakúgy, mint a jelentésünkben korábban tárgyalt támadó site-ok esetében láttuk, az adathalász site-ok száma is rendkívül megugrott 2012 elején. Erről tanúskodik a Google alábbi grafikonja.

Észlelt adathalász oldalak száma (ezer db)




*Forrás: Google*

Adathalász site-ok száma ezer hosztonként a világ egyes térségeiben (2011. II. félév)



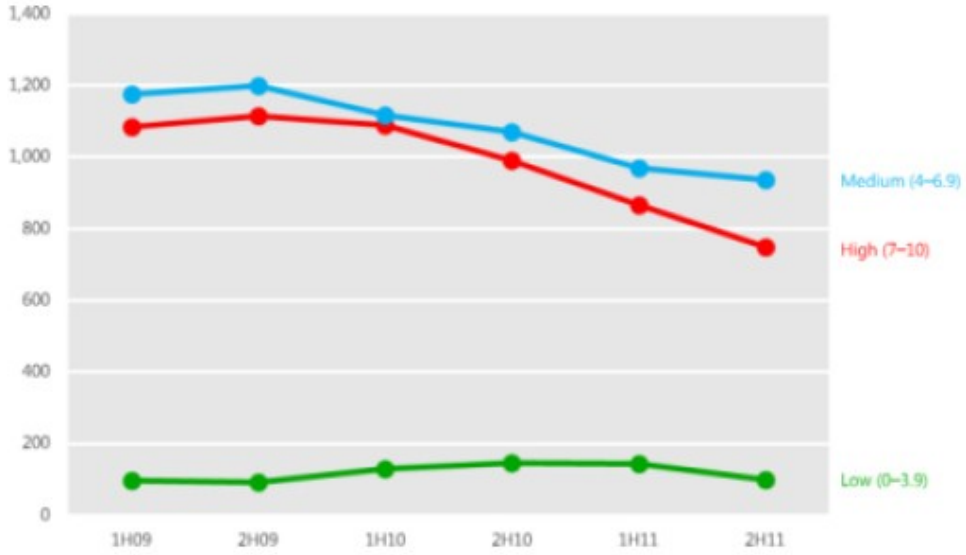

*Forrás: Microsoft Malware Protection Center*

Noha a fenti térképen Magyarországnak szerencsére még a környéke sem vöröslik, az adathalászok a magyar netezőket sem kímélték az elmúlt negyedévben. Áprilisban az OTP ügyfeleire vetették ki hálójukat a bűnözők. A pénzintézet tavasszal új online bankoló felületet vezetett be, s így az adathalászok úgy gondolhatták: sokak szemében hitelesebbnek tűnhet levelük, melyben az ügyféladatok újbóli megadását kérik. A bank közleményben figyelmeztetett (nem először): „soha nem kért és nem kér mailben ügyféladatokat”.

## Folt hátán folt

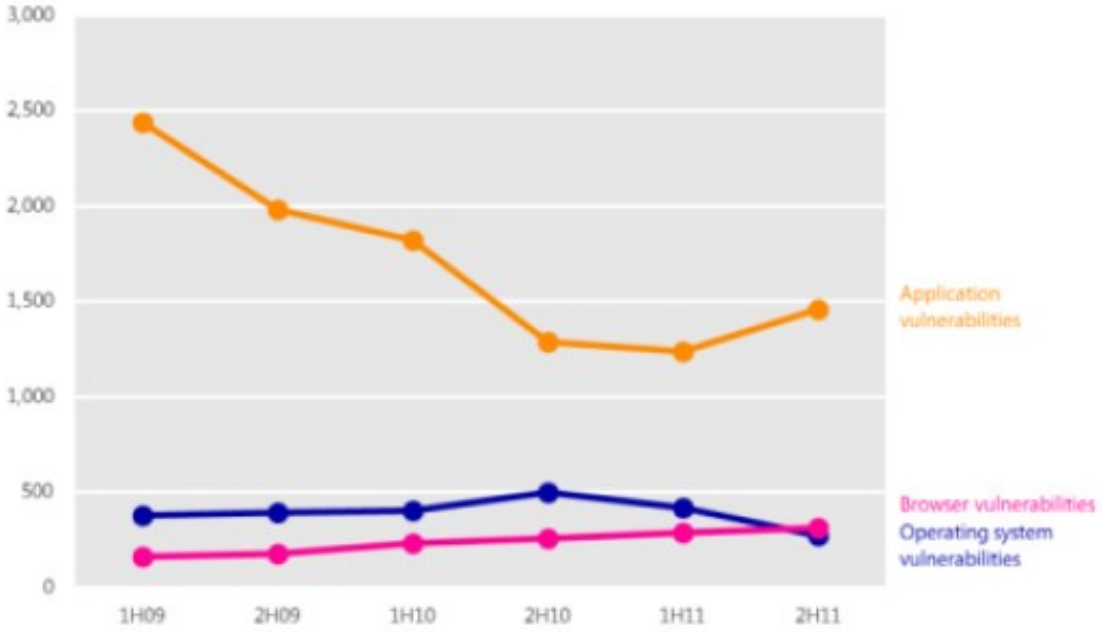
Általában elmondható, hogy a különböző szoftverekben felfedezett sérülékenységek száma, súlyossága egészében véve csökkenő tendenciát mutat. Ezt szemléltetik a Microsoft Biztonsági Kutatási Jelentésének következő ábrái.

A szoftvergyártók által újonnan bejelentett közepes (kék), nagy (piros) és kis (zöld) súlyosságú sérülékenységek számának alakulása 2009-2011 között



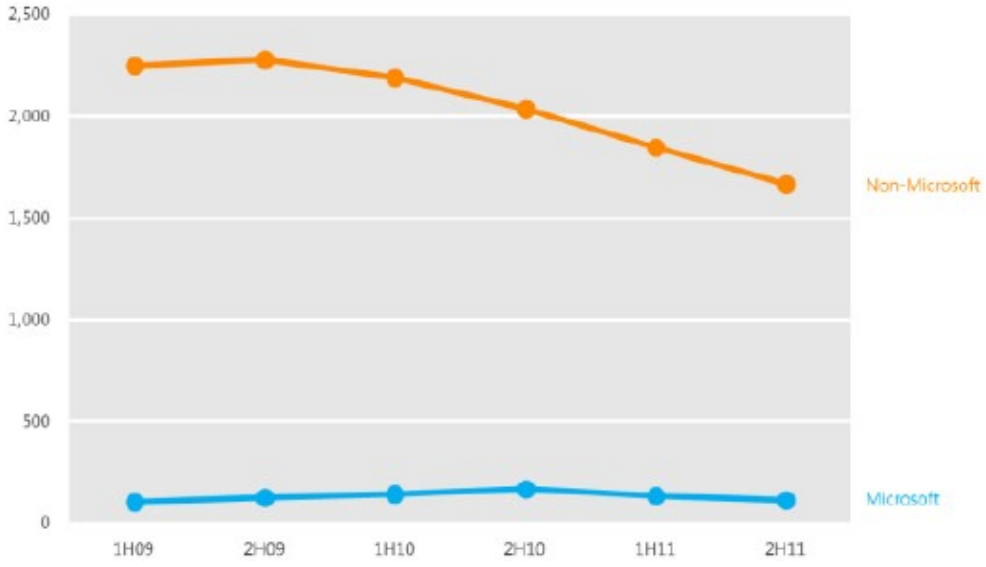

Forrás: Microsoft

Az alkalmazásokban (narancs), böngészőkben (kék) és az operációs rendszerekben jelentett sérülékenységek számának alakulása 2009-2011 között




Forrás: Microsoft

A Microsoft (kék) és a többi szoftver-gyártó (narancs) által bejelentett sérülékenységek számának alakulása 2009-2011 között




Forrás: Microsoft

A kedvezőnek mondható trend ellenére foltoznivaló 2012 második negyedévében is akadt bőven. Az is jelzés értékű, hogy a Google felemelte a legsúlyosabb sérülékenységek felfedezőinek járó díjat. Az összeghatár most 20 ezer dollár. Megjegyezzük: mióta a keresőóriás 2010-ben bevezette a hibabejelentők jutalmazását, több mint 200 kutatónak összesen mintegy 460 ezer dollárt fizetett ki.

Mint ismeretes, a Google korántsem az egyetlen cég, amely díjazza a résvadászokat. Így tesz a Mozilla, a Facebook vagy a Secunia is. A Microsoft azonban nem állt be a sorba...

Jelentésünk végén az alábbiakban hónapról hónapra haladva áttekintést adunk a negyedév folyamán kibocsátott legfontosabb biztonsági frissítésekről.

**Április**

- Havi foltozó keddjén 6 javítócsomagot bocsátott ki a Microsoft. Közülük 4 kritikus, 2 pedig fontos besorolást kapott. A foltok többek között a Windows Common Controlshoz és az Internet Explorerhez készültek, s összesen 11 hibát orvosoltak. A javítócsomagok megjelentetése alkalmából a Microsoft felhívta felhasználói figyelmét: két év múlva, 2014 áprilisában megszűnik a Windows XP és az Office 2003 támogatása.
- Google Chrome-ba integrált Flash Playerének frissítésével indította a negyedévet az Adobe. Pár nappal később megjelent a cég háromhavonta, a Microsoft foltozó keddjeire időzített menetrendszerű Reader és Acrobat biztonsági javítás-sora is.
- Menetrendszerű negyedéves biztonsági frissítési napján számos termékében összesen 88 hibát javított az Oracle. Az adatbázis-kezelőn kívül foltot kapott egyebek mellett az Application Server, az E-Business Suite, a Peoplesoft Enterprise család és az Oracle Sun Product Suite.
- Betömött egy olyan Hotmail-rést a Microsoft, amelyet kiaknázva hackerek kizárhatták a felhasználókat saját mail fiókjukból. Bár a hibát már korábban ismerték, a foltozást megelőzően felerősödtek a rá irányuló támadások. Két háttér-információ: hackerek az utóbbi időben 20 dollárért vállalták egy Hotmail-fiók feltörését, s a levelező rendszert 2010-ben egy felmérés szerint 364 milliónyian használták.

**Május**

- Rendszeres havi frissítési ciklusa keretében a Microsoft összesen 7 – 3 kritikus és 4 fontos besorolású – javítócsomaggal jelentkezett. Az érintett termékek: Windows, Office, Silverlight és a .NET keretrendszer, melyekben együttvéve 23 rést tömtek be.
- Windows, Macintosh, Linux és Android platformon egyaránt kritikus hibát javított Flash Playerében az Adobe. Kutatók azt jelentették: a sérülékenységet Internet Explorer alatt már kiaknázták a hackerek. Néhány nap elteltével az Adobe a Shockwave Playerhez is biztonsági frissítést bocsátott ki.
- Kritikus frissítéssel 17 rést tömött be a QuickTime 7.7.2-en az Apple.
- Új, 19-es Chrome-verzióval jelentkezett a Google. A friss változat 20 biztonsági problémát – köztük 8 súlyosat – is orvosolt.
- Megjelent a PHP 5.4.3-as és 5.3.13-as változata, amellyel a fejlesztők egy támadási hullámot védtek ki.

**Június**

- A negyedév utolsó foltozó keddjén 7 biztonsági frissítés látott napvilágot a Microsoftnál. Kritikus minősítést 3, fontosat 4 frissítés kapott. Az összesen 26 folt a Windows, az Internet Explorer, a Dynamics AX, a Lync és a .NET keretrendszer réseire került. Egyszersmind a szoftveróriás közölte: egy új automatizmus segítségével naponta vizsgálja felhasználói gépén a biztonsági tanúsítványok érvényességét.
- A hónap elején megjelent a folt az Adobe Illustrator és Photoshop korábban jelzett sérülékenységeire. Ismételten lyukat kellett tömnie az Adobe-nak a Flash Player különböző változataiban is.
- iOS biztonsági útmutatót jelentetett meg az Apple.
- A hónap végén ismét feljebb lépett a Google Chrome verziószámlálója. A 20-as változat 20 sérülékenységet orvosolt, melyek közül egyiket sem minősítették súlyosnak.

***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.

# 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