Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2012. éves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető

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

A jelentés betekintést nyújt az informatikai biztonság berkeibe, összefoglaló jelleggel. Többek között szót ejtünk a lakossági-, vállalati- és a kormányzati szektorokat érintő IT-biztonsági trendekről. Szemezgetünk az év során nyilvánosságra került kiberbiztonsági incidensek, malware fertőzések, valamint egyéb IT- és adatbiztonságot érintő hírek sokaságából.

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, információk 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

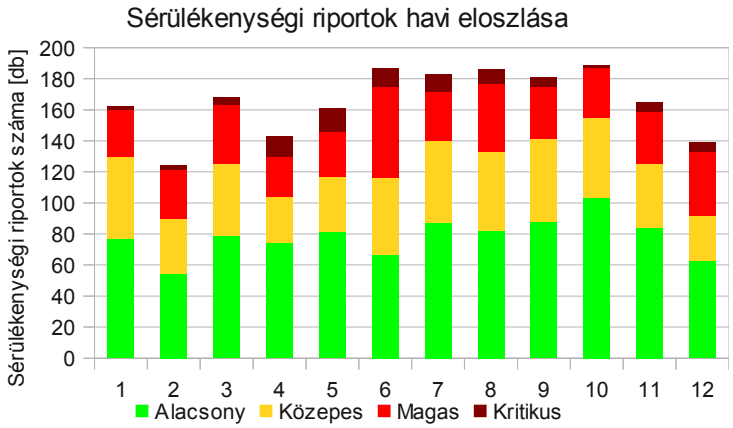
Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

A PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ tevékenysége számokban

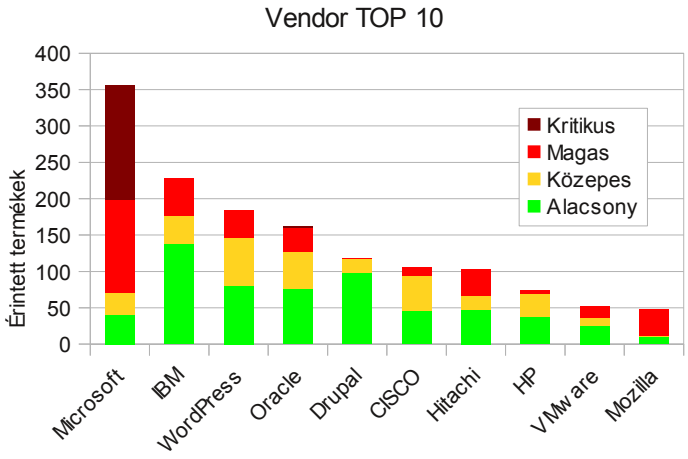
Szoftver sérülékenységek

Szoftver sérülékenység 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. során **1988 db szoftver sérülékenységi információt** publikált, amelyekből 939 db alacsony, 529 db közepes, 430 db magas és 90 db kritikus kockázati besorolású.

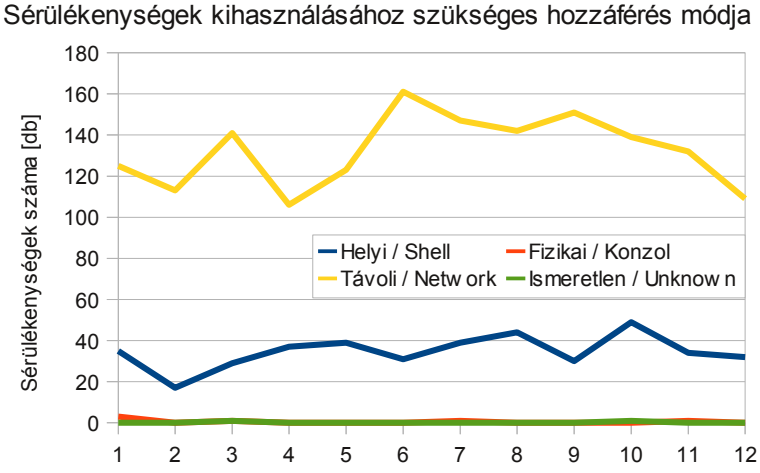


2012-ben összességében közel ugyanannyi sérülékenységi publikáció került kiadásra, mint az előző évben. A magas és/vagy kritikus sérülékenységek száma is közel ugyanannyi, mint az elmúlt év során (26%).

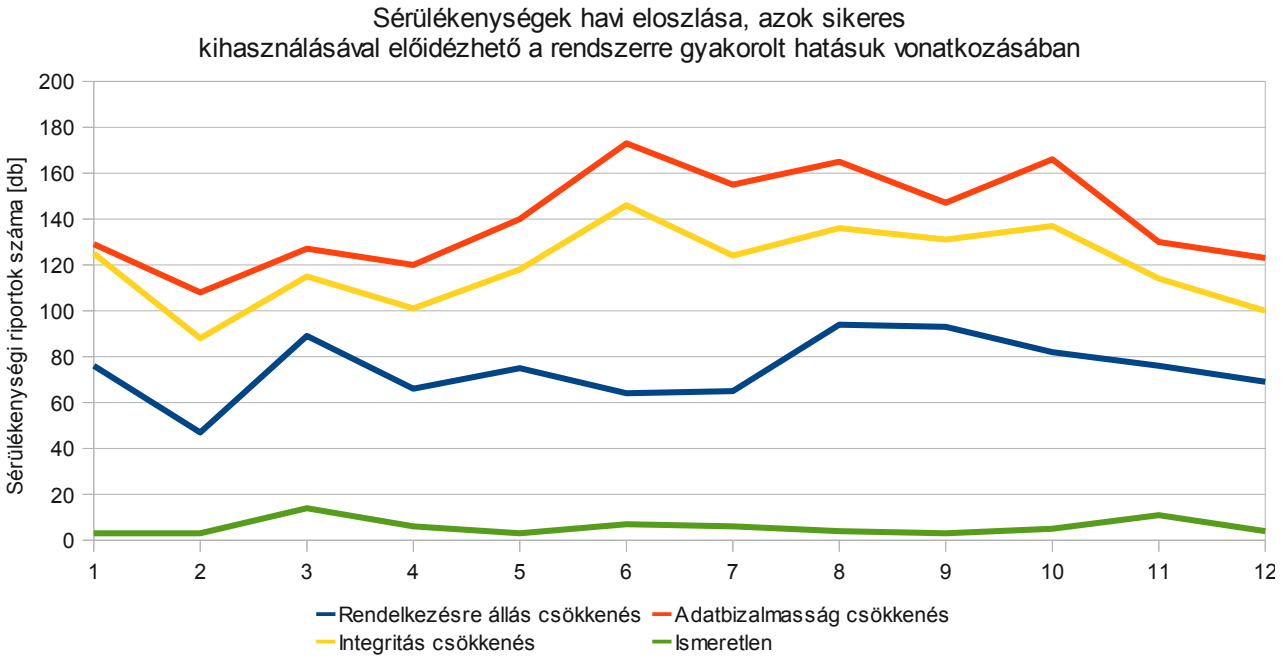


A sérülékenységi információk havi eloszlása a III. negyedév hónapjaiban a legmagasabbak, ugyanis a nagyobb szoftvergyártó cégek, mint a a Microsoft, Oracle/SUN, HP és az IBM ezekben a hónapokban tették közzé legnagyobb számban a szoftver sérülékenységekre kiadott javításaikat.

A nagyobb szoftvergyártó cégek előre kijelölt időpontokban hozzák nyilvánosságra szoftvereik sérülékenységét javító frissítéseiket. A Microsoft termékeit 2012-ben 55%-kal több szoftver sérülékenység érintette, mint például a második helyen található IBM termékeit. A Microsoft által forgalmazott termékek 80%-ára nézve a feltárt biztonsági rések magas és/vagy kritikus kockázatot jelentenek. Ez a megoszlás a Mozilla termékek vonatkozásában is igen magas értéket képvisel, ugyanis ezen termékekre nézve ez az arány 75%. A kiberbűnözők által az interneten keresztül kihasználható sérülékenységek közel 80%-ához nem szükséges helyi vagy fizikai hozzáférés, azaz távolról kihasználhatóak. Ez az arányszám a vállalatok számára azt jelenti, hogy továbbra is kiemelt figyelmet kell fordítani az újonnan megjelenő szoftver sérülékenységek mielőbbi javítására,



amellyel a lehetséges kockázatok csökkenthetőek. A 2012-es évben több alkalommal is olyan kritikus Zero-day sérülékenységek kerültek nyilvánosságra, amelyek megmozgatták mind a hazai, mind a nemzetközi IT közösséget, nem csak a sérülékenység létezéséről, hanem arról is, hogy az egyes gyártók milyen sikerességgel foltozták be ezeket. A 2012-es évben nyilvánosságra hozott sérülékenységek nagy számban érintették a CMS (Content Management System), azaz tartalomkezelő rendszereket is, mind core szinten, mind pedig a hozzájuk tartozó bővítmények szintjén.



Internetbiztonsági incidensek

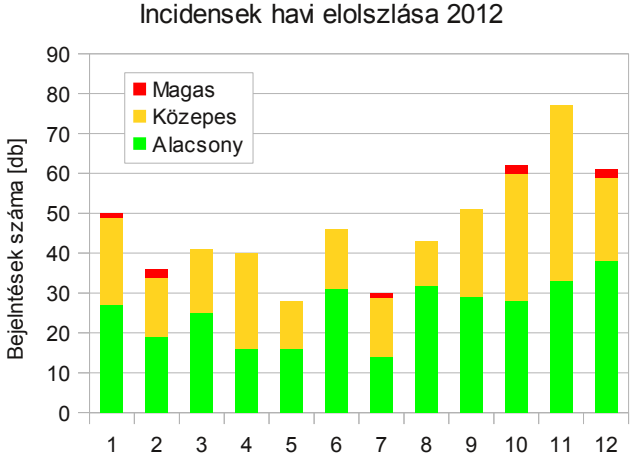
Internetbiztonsági incidens minden olyan biztonsági esemény, amelynek célja az információs infrastruktúrák bizalmasságának, sértetlenségének vagy rendelkezésre állásának megsértése az interneten, mint nyílt információs infrastruktúrán keresztül.

A PTA CERT-Hungary, **Nemzeti Hálózatbiztonsági Központ** a 2012-es év során összesen **565 db incidens bejelentést** regisztrált és kezelt, ebből 308 db alacsony, 249 db közepes és 8 magas kockázati besorolású. Ez közel egyharmadával több, mint az előző év folyamán volt tapasztalható.

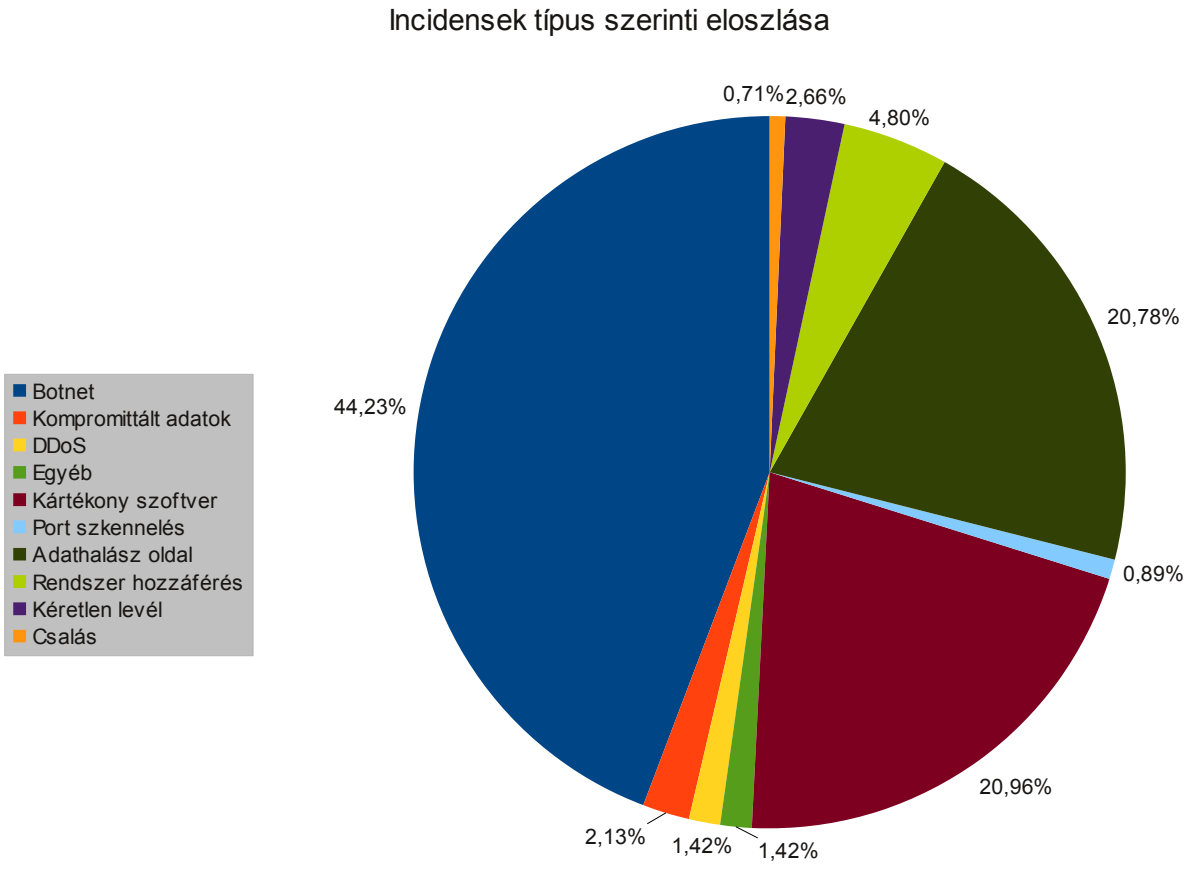
A **Nemzeti Hálózatbiztonsági Központ** a hatékony incidens-kezelés érdekében **24 órás ügyeletet működtet** az év minden napján. Az ügyelet feladata az egyes incidensek kapcsán adandó válasz-intézkedések megtétele.

A bejelentések többnyire külföldi partner-szervezetektől érkeztek és több mint 89%-ban hazai káros tevékenységgel vagy káros tartalommal voltak összefüggésben.

Az egyes incidensek elhárítása kapcsán összesen közel 90 magyar és 40 külföldi szolgáltató került bevonásra és összesen közel 2200 szálon folyt incidenskezelési koordináció.



2012-es év során a legnagyobb számban botnet hálózat részét képező számítógépek (44%) és adathalász tevékenység (21%), valamint kártékony szoftver (20%) kapcsán érkeztek bejelentések, valamint több alkalommal érkeztek olyan bejelentések, amelyek népszerű tartalomkezelő rendszerek sérülékenységeivel voltak kapcsolatosak. Az adatok alapján megállapítható, hogy a kiberbűnözők igyekeznek kihasználni a népszerű tartalomkezelő rendszerekben talált szoftver sérülékenységeket céljaik megvalósítása végett, így minden felhasználó és vállalat számára javasolt ezen rendszereik folyamatos ellenőrzése és frissítése. A tartalomkezelő rendszerek mellett érdemes megemlíteni a botnet-ekhez kapcsolódó incidens bejelentéseket is, amelyekből az következik, hogy az Internetet használó felhasználók számítógépei, még mindig nagy számban fertőzöttek valamilyen kártékony szoftverrel. Ennek következményeként gépüket botnet hálózathoz kapcsolták, amelyet a kiberbűnözők több célra is felhasználhatnak, az egyszerű kéretlen levelek küldésén keresztül egészen más weboldalak és/vagy rendszer elleni támadásig. Ezt a feltevést támasztja alá a 2012-es évben megnövekedett kártékony szoftver bejelentések száma is, ami a 2011-es évhez képest több mint 500%-kal nőtt meg. Napjainkban mivel egyre több felhasználó használja az internetet asztali vagy hordozható számítógépen, táblagépen vagy okostelefonon keresztül, és mivel egyre több szolgáltatás érhető el online is, így a kiberbűnözők egyre nagyobb hangsúlyt fektetnek az adathalászatra, amivel felhasználói hozzáférések szerezhetőek meg, ami nem egy esetben akár (komoly) anyagi kárt is okozva a felhasználónak.



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

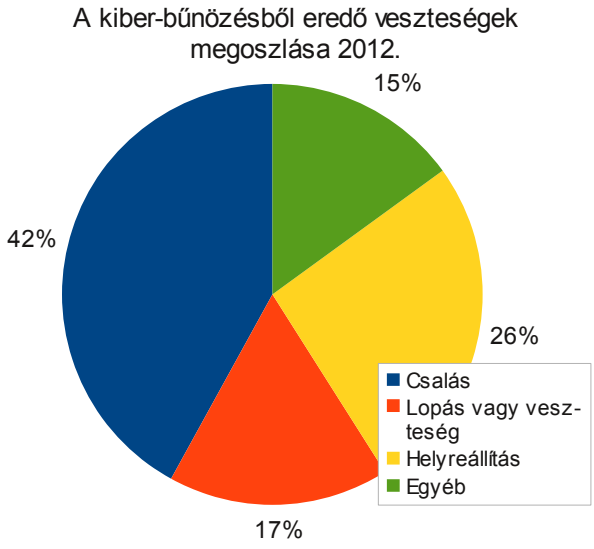
2012. tapasztalatai – Szektorális összefoglalók

Lakossági szektor

Az internetes csalók az elmúlt évben világméretekben nem kevesebb, mint 110 milliárd dollárt zsebelhettek be a világháló még mindig nagyszámú gyanútlan felhasználóit megkárosítva.

Kiberbűnözés

A Norton immáron negyedik éve készíti globális kiberbűnözési tanulmányait, melyek átfogó képet adnak a netes csalásokról és az új technológiák alkalmazásának biztonsági következményeiről. Az idei felmérés[1] több mint 13 ezer ember megkérdezésével készült 24 országban - Magyarország ezúttal nem volt része a kutatásnak. A Norton ezúttal is beárazta a kiberbűnözést: a csalók globálisan 110 milliárd dollárra tehettek szert ebben az „ágazatban" az utóbbi 12 hónapban, ez felhasználónként átlagosan 197 dollárt jelent, ami egy négytagú magyar család havi élelmiszerkiadása.

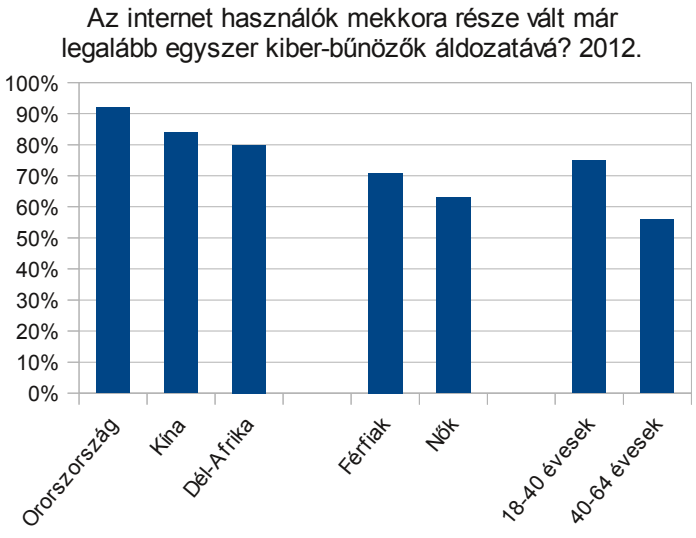


Forrás: Symantec: Norton Cybercrime Report 2012

A tanulmány megállapítja, hogy naponta legalább másfél millió áldozatot szed a kiberbűnözés. Az elmúlt egy évben globálisan 556 millióra volt tehető a felnőtt károsultak száma, ami több mint az Európai Unió teljes lakossága. Ez nagyjából másodpercenként 18 áldozatot jelent világszerte. A szakértők csak azokat sorolják az áldozatok közé, akik nemcsak kapnak például adathalászatot rejtő elektronikus levelet, hanem arra aktívan reagálnak is.

Életükben az internethasználó felnőttek legalább 2/3-a vált már legalább egyszer kiberbűntény áldozatává, 2012 során pedig világszerte az internethasználó felnőttek 46%-át érte malware, vírus, hack, csalás, átverés vagy lopás típusú sikeres támadás. Jellemzően inkább a férfiak, illetve a fiatalabb korosztály válik áldozattá.

A nők és az idősebbek eredendően bizalmatlanabbak, illetve az idősebbek kevesebbet használják a legnagyobb kockázatot közvetítő közösségi site-okat, illetve az okostelefonok tekintetében is jobban le vannak maradva, illetve megfontoltabban telepítenek applikációkat.

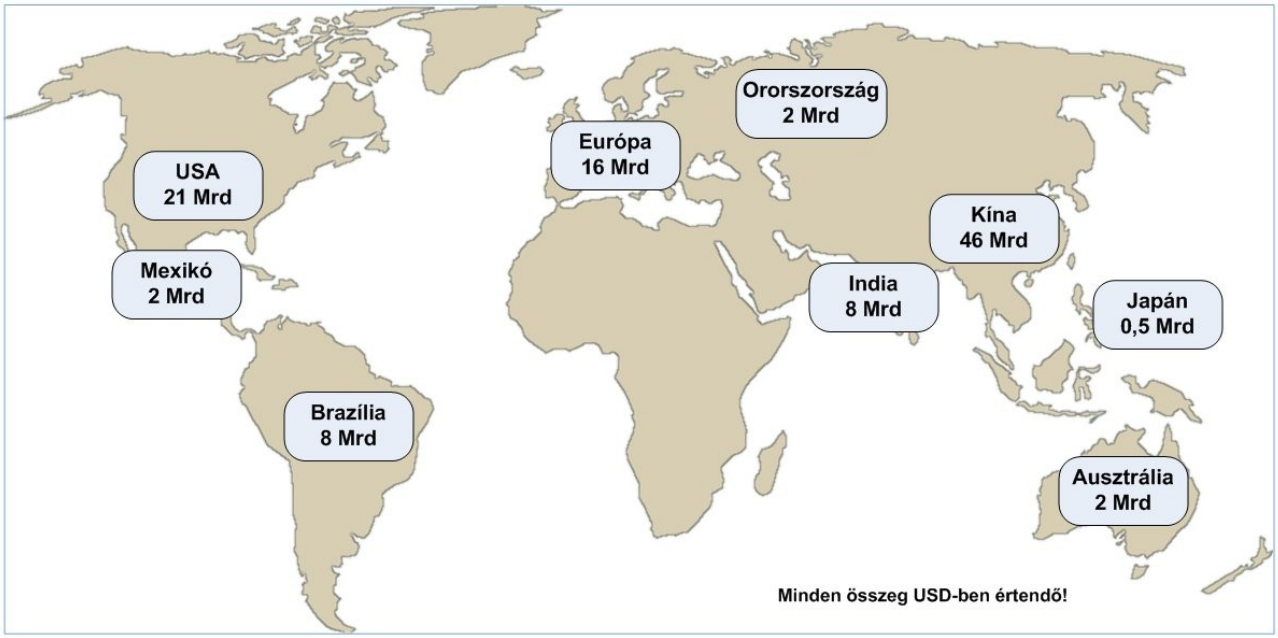


Forrás: Symantec: Norton Cybercrime Report 2012

1 Symantec: Norton Cybercrime Report 2012; 2012.09.05.

Ha az internetes bűntények által okozott károk földrajzi eloszlását vizsgáljuk, nem meglepő, hogy a legnagyobb lélekszámú, egyben ugrásszerűen, kicsit „vadnyugati" módon fejlődő Kína a legtöbb csalás helyszíne, utána a legnagyobb internethasználó régiók, az USA és Európa következnek.

A kiberbűnözésből eredő károk világszerte 2012.



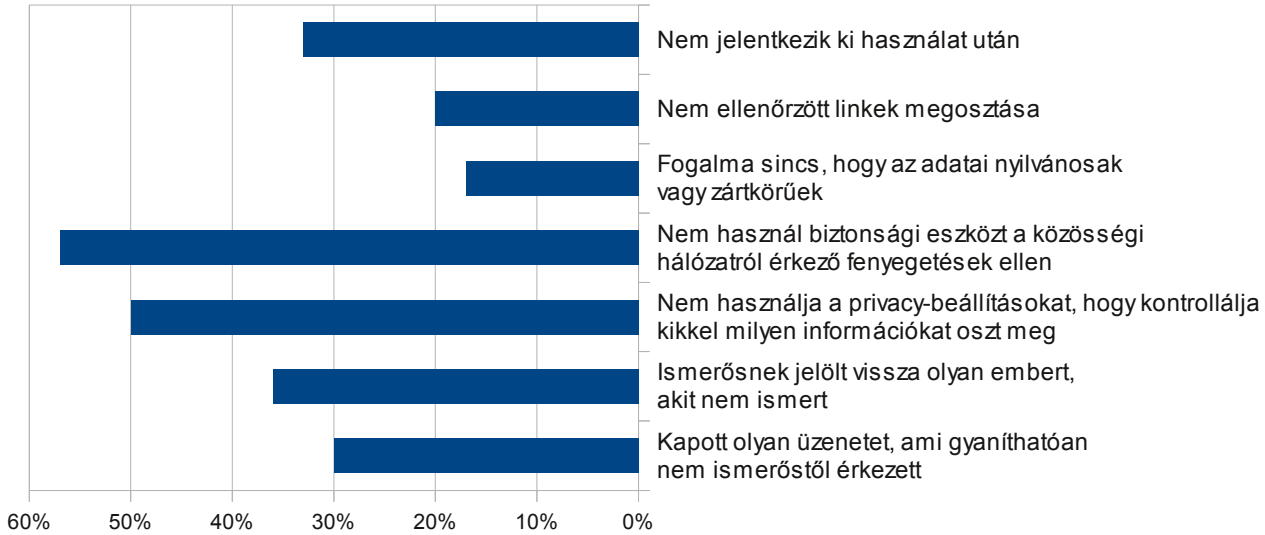
Forrás: Symantec: Norton Cybercrime Report 2012

Közösségi oldalak

Felgyorsult a kiberbűnözés új formáinak, a mobilos és közösségi támadásoknak a terjedése. A világhálón barangolóknak már az egyötöde kerül ilyen módon kapcsolatba a netes csalókkal. Ezen belül a közösségi oldalak felhasználói közül már 39% vált valamilyen módon áldozatukká, vagy úgy, hogy feltörték a profiljukat és a nevükben használták az oldalukat (18%), vagy úgy, hogy bedőltek a közösségi hálózatokon terjedő átveréseknek, hamis linkeknek (10%).

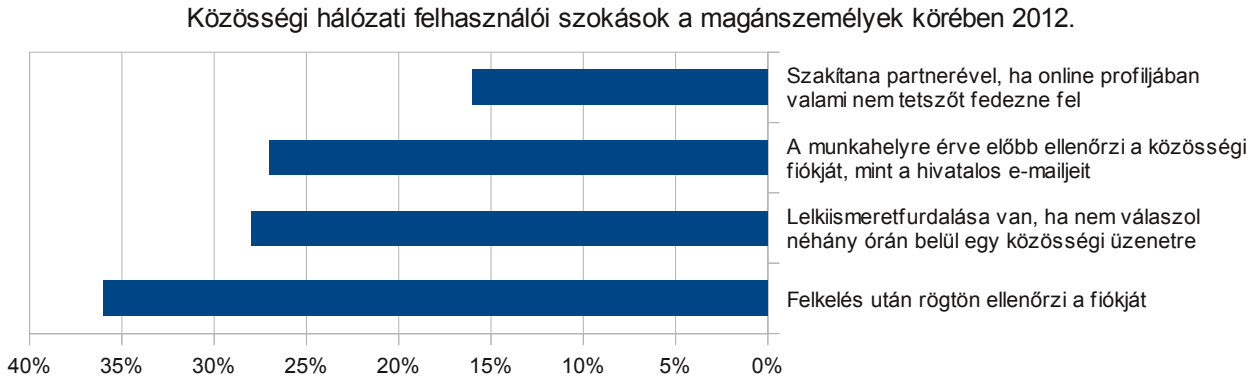
A felhasználók ¾-e úgy gondolja, hogy kiberbűnözők is erőteljesen jelen vannak a közösségi oldalakon, mégsem tesznek meg mindent a biztonság fokozása érdekében.

Kockázatos viselkedés közösségi hálózatokon a magánszemélyek körében 2012.



Forrás: Symantec: Norton Cybercrime Report 2012

A közösségi hálózatok egyébként is egyre aktívabb szerepet töltenek be a felhasználók életében. Körülbelül egyharmaduk kifejezetten „függőnek” tekinthető, de a fiatal felnőttekre általánosan jellemző ez a kapcsolattartási forma, amelyhez való folyamatos (gyakorlatilag 24 órás) hozzáférésről már nem is akarnak lemondani. Ennek lehetőségét a mobilnet képes okostelefonok még csak fokozták, de a munkahelyi hálózatokon is egyre fokozottabb biztonsági problémát jelentenek a közösségi hálózatokon továbbított fájlok-linkek, nem is beszélve az elvesztegetett munkaidőről. Ahogyan az majd a vállalatokkal foglalkozó részben látható lesz, a vállalatok komoly korlátozásokkal próbálják mindezt megelőzni, de a saját tulajdonú, mobilinternetre kapcsolódó eszközökkel nem sok mindent tehetnek a kategorikus és drasztikus tiltáson kívül, ez viszont a munkamorál és a munkahatékonyság – hiszen ezek az eszközök a munkát is hatékonyabbá tehetik – rovására megy.



Forrás: Symantec: Norton Cybercrime Report 2012

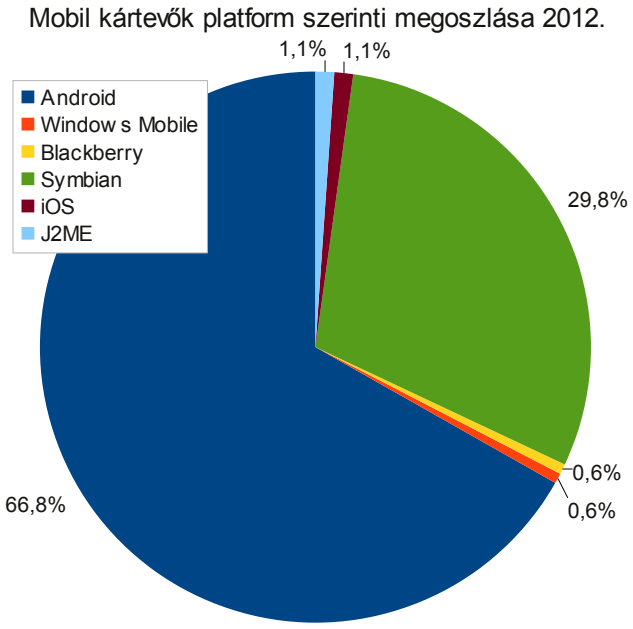
Mobil eszközök

A felnőtt internethasználók 2/3-a már mobilinterneten keresztül is kapcsolatban áll a világhálóval. Az elmúlt évben a mobil kártevők száma megkétszereződött. Különösen veszélyeztetett az Android platform. Az F-Secure Mobile Threat Report 2012. 3. negyedévi jelentése szerint összesen 51 447 egyedi androidos kártevőt és 42 új kártevő-családot regisztráltak.

Nem csak a kártevők jelentenek fenyegetést, a felnőtt lakosság 35%-a vesztett már el mobiltelefont (vagy ellopták tőle). Az okos készülékekkel ez azt is jelenti, hogy levelezésünk, kontakt- és egyéb személyes adatok is könnyen illetéktelen kezekbe kerülnek.

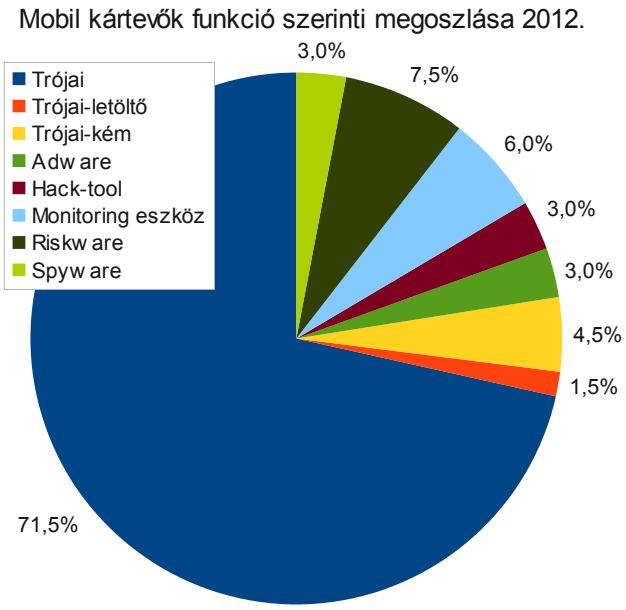
A felhasználók 2/3-a semmilyen védelmi megoldást nem használ mobil készülékén, 44%-uk nem is tud arról, hogy léteznek és szükségesek ilyen alkalmazások.

Úgy tűnik, ami annak idején a Windows volt az asztali gépeknél, most az Android lesz a mobil eszközöknél. Az androidos készülékek értékesítésének robbanásszerű növekedése ugyanis magával hozta azt is, hogy a kártevők is erre a platformra jelennek meg legnagyobb számban.



Forrás: F-Secure: Mobile Threat Report 2012Q3

Ebben a negyedévben a két legjellemzőbb fenyegetettség a profitszerzés céljából indított SMS-küldő aktivitások és a fertőzött készülékről történő információlopás volt. A növekedés azért is figyelemre méltó, mert közben bevezették a Google Bouncert, a Google Play Store (korábban Android Market) biztonsági megoldását. A Google Bouncernek az a feladata, hogy a Play Store-ban lévő alkalmazásokat átvizsgálja, hogy tartalmaznak-e kártékony kódot. A Google szerint a Bouncer hatására 40 százalékot csökkent a malware fertőzések száma, biztonságtechnológiai konferenciákon már igazolták, hogy a védelme kijátszható. Az F-Secure szerint azonban nem ez a jelentősen megnövekedett fertőzöttség alapvető oka, sokkal inkább az androidos készülékek terjedésének természetes mellékhatása. Különösen igaz ez Oroszországra és Kínára, ahol világszinten messze a legmagasabb az Android piaci részesedése - Oroszországban meghaladja a 80 százalékot.



Forrás: F-Secure: Mobile Threat Report 2012Q3

A harmadik negyedévben iOS 6-ra frissülő iOS platform összesen 197 sérülékenység javítását is tartalmazza. Ugyanakkor tény, hogy eltekintve a FinSpy esetétől ebben a negyedévben az iOS platformon egyetlen említésre érdemes kártevő volt, az Androidot is fertőző Fidall, amely a fertőzött eszközön található kapcsolat információkat juttatja el egy távoli szerverre, majd spam SMS-eket küld az adott telefonszámokra, amelyek az app letöltését elindító linket tartalmazzák.

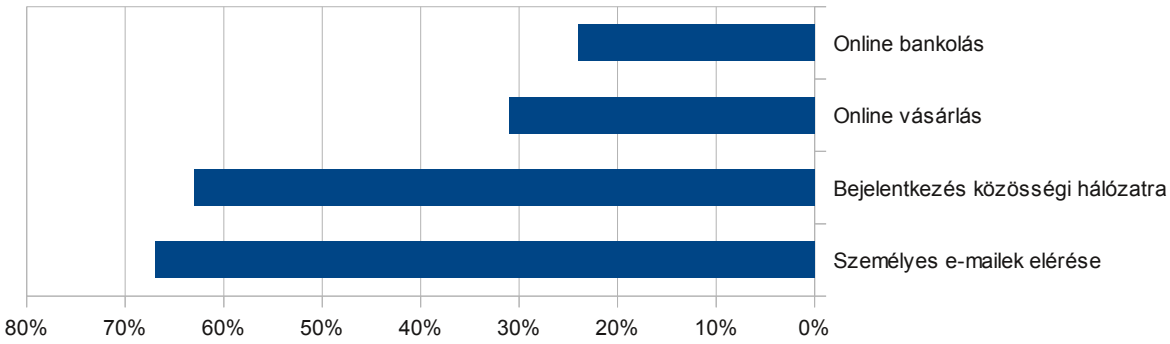
A Balckberry sem maradt tiszta. Ezen a platformon a Zitmo (a Zeus malware mobil verziója) egy új változatát azonosították. A bankoló kártevő célja ellopni azt a mobiltelefonra küldött tranzakció-hitelesítő számot, amelyet a bankok küldenek ügyfeleiknek az online tranzakciók jóváhagyásához. A Zitmo kártevő kinyeri az SMS-ből az adott számsort, és továbbítja azt egy távoli szerverre, így a bűnözők SMS-ben jóváhagyott utalásokat tudnak indítani. A FinSpy-nak is van Blacberry-n futó változata (ahogy andorid-os és Windows Mobile-os is). Ez a kórokozó képernyőképeket készít a fertőzött készülékről, megjegyzi a valós vagy virtuális billentyűzeten történő leütéseket, befolyásolja a Skype kommunikációt, követi az eszköz helyzetét, valamint figyeli az SMS-eket és hanghívásokat.

Annak ellenére, hogy a Symbian fejlesztése leállt, a fejlődő országokban még mindig népszerű támadási célpont. Ott ugyanis még nagyon magas a piaci részesedése. 2012 harmadik negyedévében még mindig 21 új víruscsaládot és változatot fedeztek fel rá, ami 17%-os növekedés a második negyedévhez képest. Tipikus Symbian károkozó az a trójai, amely rendszerfrissítésnek vagy legális programnak álcázza magát. A legtöbb kártevő Kínából származik, és általában profitszerzési céllal készülnek. A legtöbbjük (például a Fakepatch.A és a Foliur.A) SMS-küldő aktivitásokhoz kapcsolható, jellemzően emelt díjas számokra küldött üzenetekkel vagy prémiumszolgáltatásokra történő regisztrációval károsítják meg a telefon tulajdonosát.

A mobiltelefon-felhasználók közel egyharmada kapott szöveges üzeneteket ismeretlen számokról, amelyek arra kérték, hogy kattintson egy linkre, vagy tárcsázzon egy ismeretlen számot egy hangposta üzenet eléréséhez. Egy év alatt a mobilos sebezhetőségek száma csaknem megduplázódott. Ráadásul a WiFi-vel ellátott okostelefonok szinte kiáltanak azért, hogy a tulajdonos használja ki a nyilvánosan hozzáférhető, ingyenes hotspot-okat, ahol adatforgalmi díj nélkül intézheti online teendőit, vagy fogyaszthat tartalmat mobilján. A felnőtt felhasználók 2/3-a

rendszeresen csatlakozik okostelefonjával szabad, nem biztonságos WiFi hálózatokra, 53%-uk pedig meg van győződve róla, hogy a csatlakozás ilyen módja teljesen biztonságos. A felhasználók az okostelefonok elterjedése óta, ha lehet, még óvatlanabbak a nyilvános hálózatokon, a telefonon elérhető internetkapcsolatot pedig sok, több-kevesebb kockázatot rejtő tevékenységre használják nem biztonságos környezetben is.

Kockázatos felhasználói magatartások nem biztonságos WIFI-kapcsolat esetén 2012.



Forrás: F-Secure: Mobile Threat Report 2012Q3

A legtöbb internetező legfeljebb néhány alaplépésre hajlandó védelme érdekében, többségük vagy egyáltalán nem használ jelszavakat, vagy csak a legegyszerűbbeket, amiket ráadásul nem változtat rendszeresen. A személyes email fiókok pedig gyakran az összes létező kulcsfontosságú információt tartalmazzák. A kiberbűnözők nem csak a bejövő levelekhez nyernek hozzáférést, de megváltoztathatják a felhasználó jelszavait az általa látogatott oldalakon: egyszerűen használják az „elfelejtett jelszó” funkciót, elfogják az emaileket és kizárják a gyanútlan felhasználót saját fiókjából. Összetett jelszavakkal és rendszeres jelszóváltoztatással lehet ez ellen a legkönnyebben védekezni.

A megkérdezettek bő harmada még azt sem ellenőrzi, hogy a böngésző címsorában van-e a nagyobb biztonságot jelző lakat szimbólum, mielőtt érzékeny információkat adna meg az oldalon, beleértve a banki adatait. A felhasználók 40%-a azzal sincs tisztában, hogy a gépére telepedő kártevők ma már diszkrét módon is tudnak működni, megnehezítve a gép fertőzöttségének a felismerését.

A rosszindulatú programokat terjesztőknek ugyanis ma már nem a bosszantás, hanem az illegális jövedelemszerzés a célja, amit inkább az segít elő, ha minél tovább észrevétlenek maradhatnak.

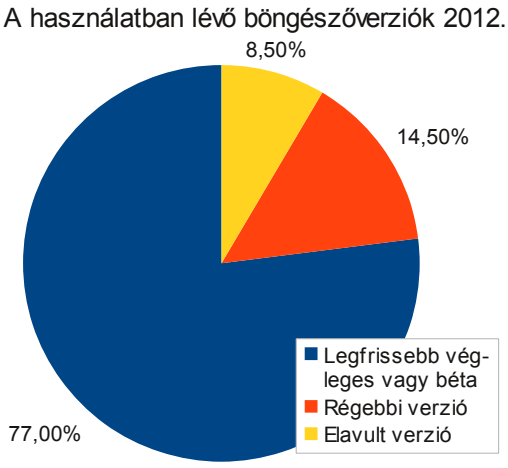
Böngészők

Súlyos biztonsági problémát jelentenek az elavult böngészők, a felhasználók mégsem frissítenek kellő időben.

A webböngészők a legszélesebb körben használt számítógépes szoftverek, amelyek majdnem minden számítógépen megtalálhatók, ezért nem meglepő, hogy a kiberbűnözők legtöbb támadása még mindig a böngészőkön keresztül érkezik, kihasználva azok sérülékenységeit. Rendkívül fontos, hogy a felhasználók választott böngészői mindig naprakészek legyenek és tartalmazzák a legújabb biztonsági javításokat és védelmi funkciókat. A felhőalapú Kaspersky Security Network által összegyűjtött több millió felhasználó névtelen adatai segítségével a Kaspersky Lab elemzést készített a böngészőhasználati szokásokról.[2]

A kutatás riasztó képet mutat: bár a legtöbb felhasználó már egy hónapon belül frissíti böngészőjét, negyedük még mindig nem tesz ennek eleget. Ez azt jelenti, hogy több millió potenciálisan veszélyeztetett számítógép folyamatosan ki van téve a kiberbűnözők támadásainak. Ez is alátámasztja, hogy mindenkinek szüksége van megfelelő biztonsági szoftverre, amely akár percek alatt képes reagálni és védekezni az új fenyegetések ellen.

2 Kaspersky Lab: Global Web Browser Usage and Security Trends; 2012. november



A felhasználók több mint ötöde (23%-a) használ elavult vagy régi böngészőt, ami jelentős problémákat okoz az online biztonság területén.

A felhasználóknak több mint egy hónap kell ahhoz, hogy frissítsenek egy újonnan megjelent biztonságosabb verzióra. A kiberbűnözők a böngészők ismert sebezhetőségeit akár pár órán belül képesek megtalálni.

Forrás: Kaspersky Lab: Global Web Browser Usage and Security Trends; 2012. november

Az Internet Explorer a legnépszerűbb böngésző 37,8%-kal, amit szorosan követ a Google Chrome 36,5%-kal és végül a harmadik helyen a Firefox áll 19,5%-os aránnyal.

A 2012 végén a legfrissebb verzióval rendelkező felhasználók aránya a következőképpen oszlik el: Internet Explorer 80,2%, Chrome 79,2%, Opera 78,1% és Firefox 66,1%.

Az átmeneti idő, amíg a felhasználók frissítik a böngészőiket: a Chrome-nál átlagosan 32 nap, az Opera-nál 30 nap, végül a Firefox-nál átlagosan 27 nap.

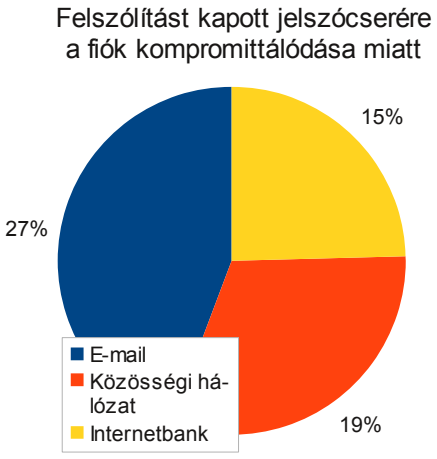
Forrás: Kaspersky Lab: Global Web Browser Usage and Security Trends; 2012. november

Ahogy a fentebb említettek is mutatják, a felhasználók 23%-a nem telepítette a böngészője frissítéseit vagy legújabb verzióját. Kétharmaduk (14,5%) a böngésző egyik előző verzióját használja, a maradék pedig elavult kiadást. Ez azt is jelenti, hogy csaknem minden tizedik internethasználó elavult webböngészőn keresztül fér hozzá banki adataihoz és személyes információhoz is. Bár az internetezők többsége szorgalmasan frissíti böngészőjét, de még mindig több tízmillióra tehető azoknak a felhasználóknak a száma, akik nem frissítik ezeket a kritikus alkalmazásokat.

Jelszavak

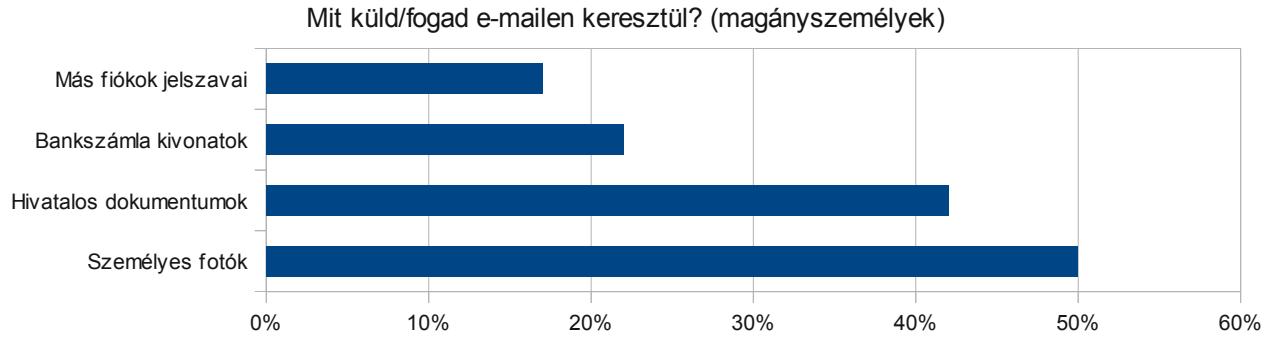
Továbbra is súlyos probléma a jelszavak kérdése, bár a felhasználók nagy része fontos személyes adatokat és tartalmakat védelmez jelszavaival, 40% mégsem választ kellőképpen komplex jelszót és nem is változtatja rendszeresen.

A felhasználók 46%-a már kapott felszólítást szolgáltatójától, hogy változtasson jelszót fiókja valós vagy feltehető kompromittálódása miatt. Ez egyaránt előfordul email szolgáltatóknál, közösségi hálózatokon, de ami még kritikusabb, netbanki hozzáférések esetében is.



Forrás: Symantec: Norton Cybercrime Report 2012

Különösen az email fiókokhoz tartozó jelszavak fontosak, a bűnözők ugyanis még mindig ezeken keresztül juthatnak hozzá a legkönnyebben a fontos személyes és üzleti információkhoz.



Forrás: Symantec: Norton Cybercrime Report 2012

Adathalászat

Az adatlopásnak még mindig az a manapság már elavultnak számító módszere a leggyakoribb, hogy a felhasználót ráveszik, kattintson egy fertőzött weboldalra, vagy nyisson meg egy emailben érkező csatolmányt. A Kaspersky Lab[3] azt vizsgálta, hogy a felhasználók tudják-e azonosítani az adathalász üzeneteket vagy a hamis weboldalakat.

Minden hatodik megkérdezett vallotta be, hogy gyanús oldalakon is gond nélkül megadta személyes vagy pénzügyi adatait.

Az adathalász üzenetek túlnyomó többsége emailben vagy a közösségi oldalakon keresztül érkezik, ugyanis ezeket a kommunikációs csatornákat szinte mindenki használja. A számítógép-használók 86%-a nézi email-jeit rendszeresen, 73% kommunikál a közösségi oldalakon, 54%-uk pedig rendszeresen folytat internetes csevegéseket az okostelefonján. A kiberbűnözők célja az, hogy hozzáférést szerezzenek a felhasználók közösség oldalainak fiókjaihoz, de végső soron a felhasználótól annak online banki, a fizetési szolgáltatásokhoz kapcsolódó vagy az online áruházi bejelentkezési adatait szeretnék megszerezni.

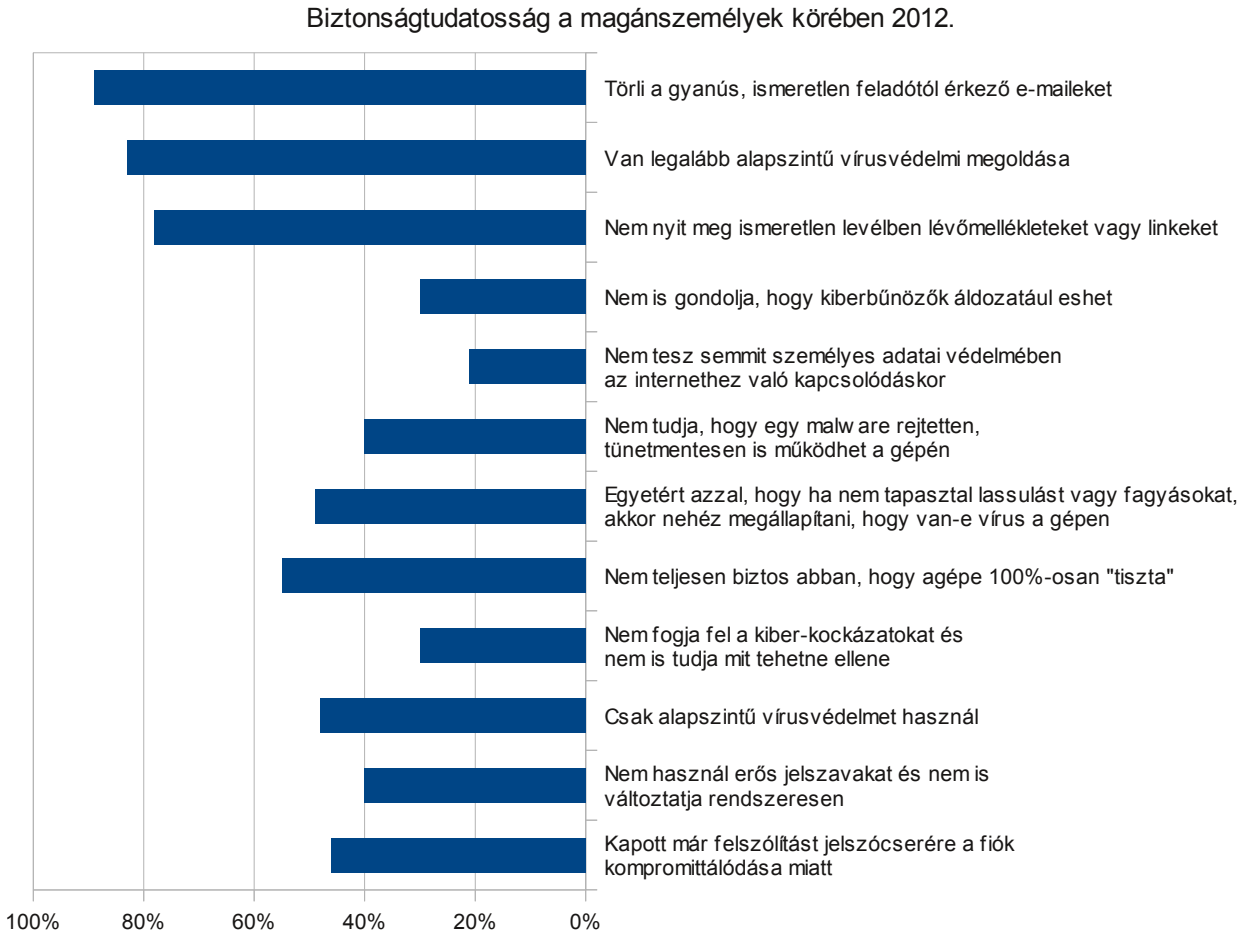
Az esélyük, hogy sikerrel is járnak, jó: a felhasználók fele ugyanis nem ismeri fel az adathalász üzenetet vagy a hamis weboldalt. A felhasználók 47%-a kapott már gyanús linkeket vagy csatolmányokat tartalmazó üzeneteket, 29%-uk pedig kapott már egy bank nevében levelet (közösségi oldalon, másik szolgáltató stb.), amelyben bizalmas információkat kértek tőle. 26%-uk azt is elismerte, hogy fertőződött már meg a számítógépe egy üzenet mellékletének megnyitása következtében, 13%-uk pedig megadta személyes vagy pénzügyi adatait gyanús oldalakon.

Ezeket az adatokat érdemes összevetni azzal, hogy a Kaspersky Lab szerint például csak ez év júniusában az adathalász üzenetek 68%-a személyes információk megszerzését célozta. Bár az információbiztonsági cégek az ilyen veszélyek ellen is próbálnak hatékony eszközöket fejleszteni, a legnagyobb tanulság az lehet, hogy a szervezeteken belül – különösen a saját eszközök elszaporodása miatt – egyre fontosabb a biztonságtudatosságra nevelés, valamint a biztonsági előírások maradéktalan bevasalása.

3 Kaspersky Lab: Perception and knowledge of IT threats: the consumer's point of view; 2012.08.29.

Biztonságtudatosság

A felhasználók IT-biztonsági felkészültségét összességében vizsgálva, felfedezhető a fejlődés néhány fontos jele, például, hogy a legtöbb felhasználó ma már olvasatlanul törli az ismeretlen feladótól származó emaileket, 4/5-ük használ legalább valamilyen alapszintű vírusvédelmi megoldást és nem nyit meg gyanús emailekhez fűzött csatolmányokat, linkeket. Az alapszintű biztonságtudatosság tehát erősödik, noha bőven van még fejleszteni való, például a potenciális vészhelyzetre való mentális felkészülés, az adatvédelem, illetve az erőteljesebb technikai felkészültség területén.



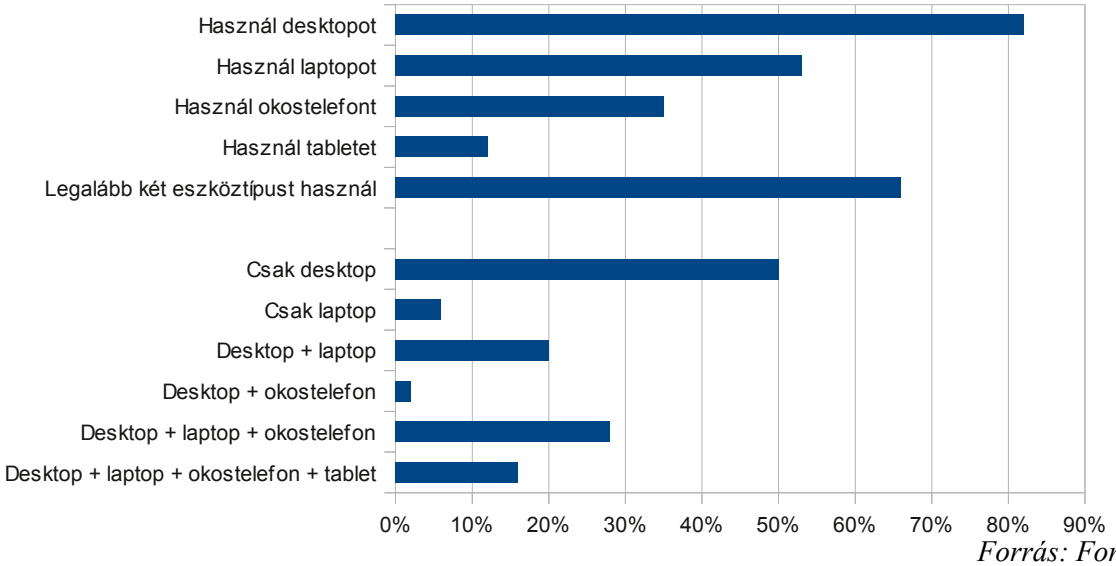
Forrás: Symantec: Norton Cybercrime Report 2012

A vállalati szektor

IT-eszközhasználat

A vállalatok egyre erőteljesebben haladnak a mobilitás irányában, a Forrester legújabb kutatása szerint[4] az alkalmazottak 66%-a legalább kétféle IT-eszközt használ munkája során naponta: a desktop-ok és laptopok mellett, az okostelefonok és a tablet-ek is egyre gyakrabban tűnnek fel a hivatalos vállalati IT-repertoárban. Az alkalmazottak 82%-a még mindig főként desktop-on dolgozik, de a vállalatok 55%-a úgy nyilatkozott, hogy a jövőben erősíteni tervezi az okostelefonok használatát a munkaeszközök között, 52%-uk pedig a tablet-ek bevonását is szükségesnek tartotta.

IT-eszközhasználat vállalati környezetben Észak-Amerika és Európa 2012.

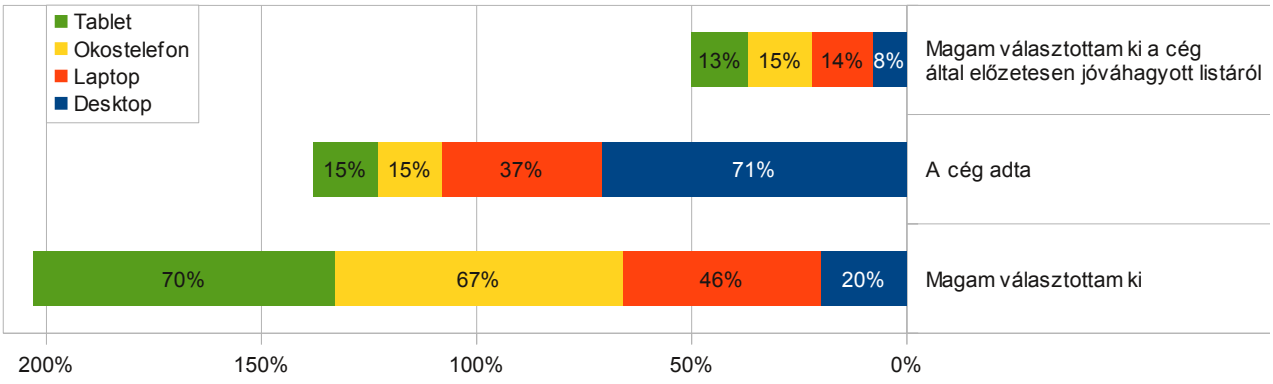


Forrás: Forrester[4]

Egyre több szervezet támogatja a saját tulajdonú eszközökön végzett munkát. Ez a jelenség a BYOD (bring your own device), amely az egyre újabb és munkára egyre sokoldalúbban használható mobileszközök fejlődésével valamint a foglalkoztatási szerkezet átalakulásával, az egyre nagyobb arányban alkalmazott távmunka, rugalmas munkavégzési hely előretörésével erősödött fel.

A szervezetek többsége mindazonáltal próbál valamiféle kontrollt gyakorolni az alkalmazottak által használt eszközök hardveres és szoftveres összetételére, bár az újabb „kütyük” esetében egyre gyakrabban szabadjára engedik alkalmazottaikat a választáskor.

Hogyan választotta ki munkára használt IT-eszközét?
Vállalati környezetben Észak-Amerika és Európa 2012.



Forrás: Forrester[4]

4 Perez, Sarah: Forrester: 66% Of Employees Use 2 Or More Devices At Work, 12% Use Tablets; Techcrunch. com; 2012.10.10.

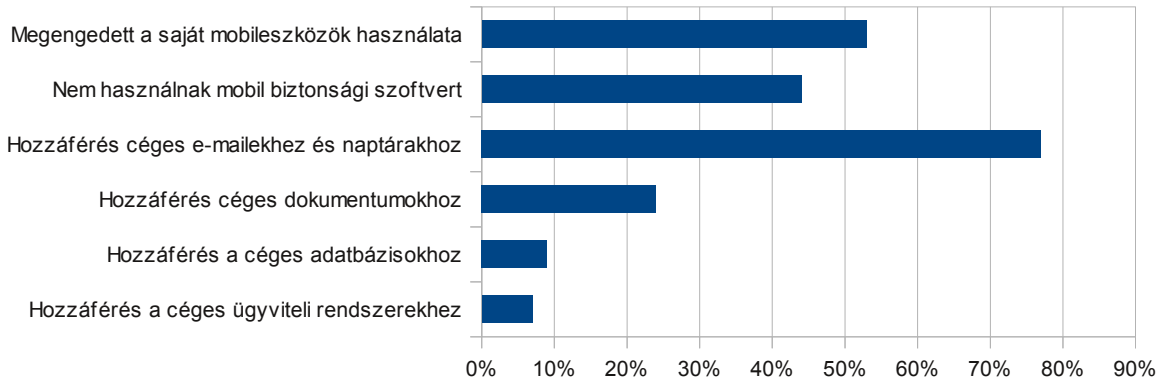
A vállalatok leginkább a totális engedékenység és a totális tiltás végletei között ingadoznak, viszonylag kevés az olyan vállalat, ahol előzetesen tanulmányozva a piacon található eszközöket, összeállítanak egy listát a vállalati hálózatban biztonságosan beilleszthető, jobban menedzselhető eszközökről, amelyek így egyfajta kontrollált szabadságot adnak az alkalmazottaknak a választáskor.

Mobil eszközök

A mobileszközök elterjedése és a közösségi média terjedése a vállalati környezetben lényegesen befolyásolja az idei IT-biztonsági trendeket. Az infrastruktúrák védelme szempontjából a végpontok védelme, a kiberbűnözés visszaszorítása és a sérülékeny mobilplatformok lefedése a legfontosabb feladat.

Az „okos" eszközök elterjedése átfogóbb védelmi eszközök kialakítására ösztökélte az IT-biztonsági szakembereket. A Forrester 2012. évi tanulmányának[4] számai szerint az alkalmazottak 53%-a a saját mobileszközét használja vállalati környezetben.

Mobileszközök vállalati környezetben 2012. Észak-Amerika és Európa 2012.

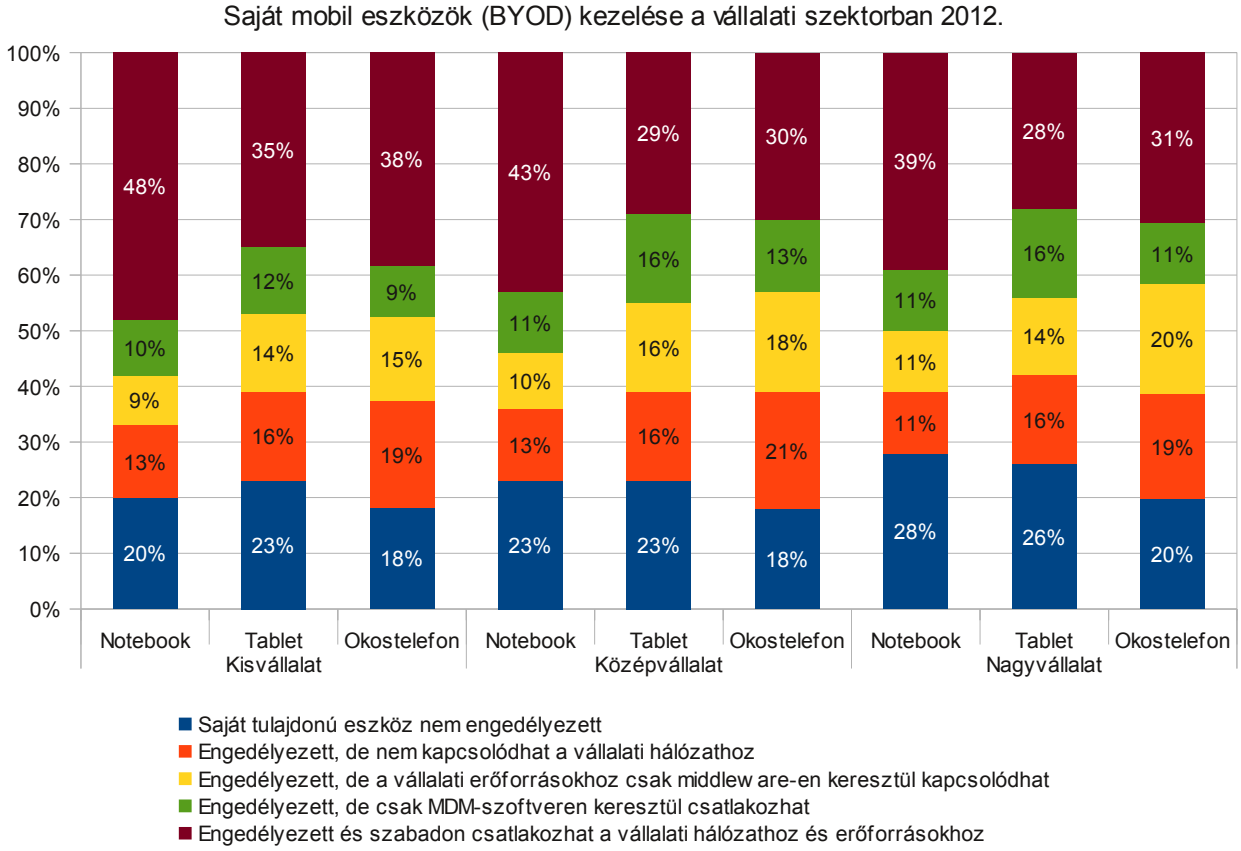


Forrás: Kaspersky[5]

Az elemzők szerint az elkövetkező három évben a vállalatok ellenállását megtörve a saját mobilkészülékek használata lehet az általános házirend a legtöbb cégnél. A BYOD (bring your own device – használd a sajátod) trend jól cseng, de miatta sebezhetővé váltak a vállalatok informatikai rendszerei. A nem megfelelően konfigurált mobileszközök rést nyitnak a vállalat hálózatán, a belső adatok egyszerűen „megkerülik" a tűzfalat, védelem nélkül szabadon járnak ki-be.

A saját mobileszközök használatához való hozzáállás vállalati mérettől, típustól függően is jelentős változatosságot mutat, a Kaspersky Lab a 2012-es évet áttekintő adatgyűjtése szerint[5] a liberalizmus a vállalati méret növekedésével fokozatosan csökken és a vállalati rendszergazdák szívesebben engednek be jól ismert technológiára épülő saját tulajdonú eszközöket, pl. laptopokat a céges hálózatba, mint a sok esetben ismeretlen és kevéssé jól menedzselhető tablet-eket, okostelefonokat.

5 Kaspersky Lab: Global IT Security Risks: 2012; 2012. december



Forrás: Kaspersky[5]

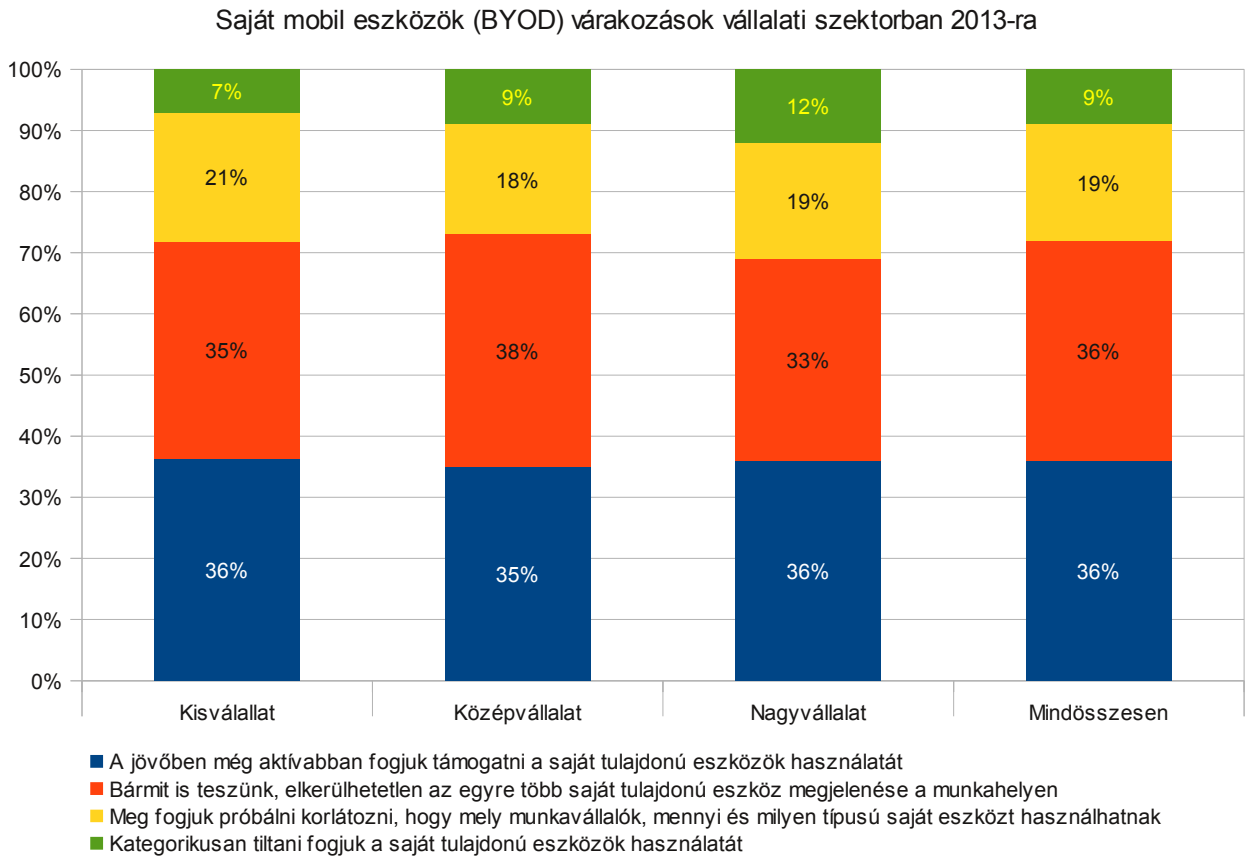
A magán-mobileszközök vállalati környezetbe kerülése folyamatos küzdelem a felhasználók és az IT között. Az IT-szakemberek által prezentált kódfeltöréses esettanulmányok – hogyan lehet az iPad-eket feltörni, védelmeiket megkerülni – miatt felvetődik a kérdés: valóban iPad-en kell tárolni a céges információkat?

A Gartner legfrissebb, 2013-ra vonatkozó előrejelzése[6] alátámasztja a fentieket, miszerint a jövő évi trendek egyik meghatározó IT-védelmi koncepciója a végpontvédelem (endpoint security) lesz. Ebből a szempontból az egyik legfontosabb feladattá vált a mobil infrastruktúra és az azon keresztüli adatforgalom védelme. További feladat az elveszített vagy ellopott laptopokon, mobiltelefonokon, tablet-eken tárolt titkos céges adatok védelme (például távoli törléssel). Miután az értékes adatok leginkább a végponti eszközökön: laptopokon, iPad-eken, okostelefonokon stb. tárolódnak, a megfelelő védelmet ezekre kell alkalmazni. Ez nemcsak a vírusvédelmet, hanem a végpontbiztonságra vonatkozó irányelvek készítését és betartását is jelenti. A szakértők javasolják továbbá a különböző biztonsági zónák kialakítását, így több védelmi réteg képezhető. A nagyon kritikus adatok tárolására pedig helyi titkosítást javasolnak.

Már 2012-ben robbanásszerű növekedést lehetett érzékelni a mobiltelefonon keresztüli támadások számában. Először az Android platformon fedeztek fel biztonsági rést, de nem elképzelhetetlen, hogy az Apple termékek is áldozatul esnek majd. Van olyan androidos kémprogram, amely a GSM kommunikáció szervizkódjait használja ki. A biztonsági hibák lehetőséget adnak arra, hogy illetéktelenek a mobiltelefon adatait távolról töröljék.

2013-ban valószínűleg a mobiltelefonok elleni támadások még gyakoribbá válnak. Sok felhasználó még a PIN-kód védelmét sem veszi igénybe, titkosítatlanul tárolják az adatokat, nem is mentik azokat.

6 Messmer, Ellen: Gartner: Growth in cloud computing to shape 2013 security trends; networkworld.com; 2012.12.06.



Forrás: Kaspersky[5]

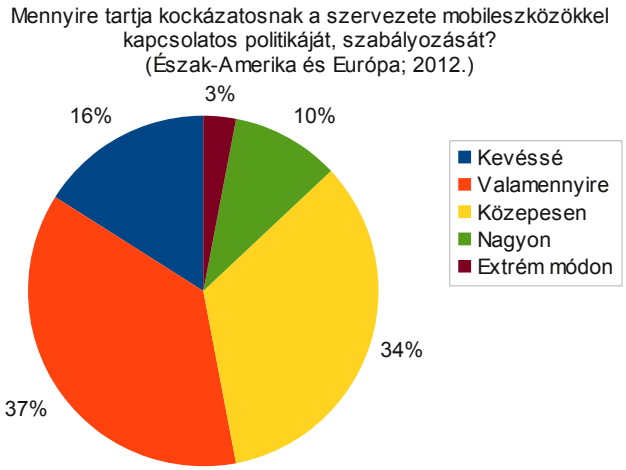
A saját eszközök térnyerésével párhuzamosan a vállalatok 18%-a rendelkezik már belső applikáció tárral, ahonnan az alkalmazottak a Google Play vagy az Appstore rendszereken megismert módon tölthetik le a munkájukhoz szükséges vállalati alkalmazásokat: pl. értékesítés, helpdesk, ellátási lánc, logisztika, készletmenedzsment, stb. Más szervezetek a nagy megoldásszállítók nyilvános applikáció letöltőközpontjaiban helyezik el a vállalat specifikus alkalmazásokat is.

A Gemalto friss kutatása[7] szerint az IT-vezetők (CIO) közel fele (48%) nyilatkozott úgy, hogy biztonsági kérdésekben nála van a döntő szó, a vállalatok ötödénél (20%) az első számú vezető (CEO) asztalán dől el ez a téma is. Ennél is érdekesebb az adat, miszerint a legalább 100 főt foglalkoztató vállalatok hatodánál a dolgozókra van bízva, hogy munkájuk során biztonságosan használják az informatikai eszközöket, szoftvereket. Talán nem meglepő, hogy az önálló gondolkodásban élen járó Skandináviában ugyanez az arány majdnem kétszer akkora, mint a fenti átlag.

A CIO-k persze akár akarják, akár nem, kénytelenek fokozatosan teret engedni a kollégáknak. Ezt egyfelől az indokolja, hogy az IT-használatban egyre jártasabb emberek kerülnek a cégekhez, akik fiatal koruk óta ezen technológiákat használják, így idősebb kollégáikkal szemben nem csak igénylik, de ideális esetben kezelni is tudják a szabadság jelentette kockázatokat. Másrészt a munkahelyekre egyre nagyobb számban benyomakodó konzumer eszközök is ebbe az irányba terelik a vállalati biztonsági politikát.

7 Gemalto: Are CIOs Losing the Battle for Secure Network Access?; 2012. szeptember

Úgy tűnik, tisztában vannak ezzel a problémával maguk a CIO-k is, hiszen elsöprő többségük nyilatkozott úgy, hogy potenciális veszélyt jelent a cégre nézve és nincs megnyugtatóan kontrollálva a BYOD. Mégis, a megkérdezettek mindössze 17%-ánál van érvényben céges policy a saját eszközök vállalati használatáról.



Forrás: Gemalto[7]

Láthatóan az az elképzelés is mély gyökerekkel bír a CIO-k fejében, hogy a biztonság és a felhasználóbarát környezet egymással ellentétes fogalmak. E kettős közül egyértelműen elsőbbséget élvez az authentikáció és biztonság. Az informatikai vezetők 85%-a nem tűrne meg semmiféle olyan új, a céges mobilitást és a munka könnyebbé tételét célzó változtatást, ami a biztonsági kockázatok növekedésével járna.

A tanulmány egyik legmeghökkentőbb része a felhasználói beléptetéssel kapcsolatos. Az IT-s topmenedzserek majdnem fele nyilatkozott úgy, hogy egy egyszerű azonosító és jelszó elégséges védelmet jelent a céges hálózat és alkalmazások számára. A kérdésre, hogy miért nem alkalmaznak többszintű, nagyobb biztonságot szavatoló rendszert a leggyakoribb válasz a pénzhiány volt. Ennek viszont némileg ellentmond az a megállapítás, hogy az utóbbi években tapasztalt, többször nagy médiavisszhangot kiváltó adatlopási és adatszivárgási ügyek miatt a CIO-k több mint fele nagyobb összeget különített el költségvetéséből a védelmi kiadásokra.

A Gartner biztonsági szegmensre koncentráló előrejelzése[8] azt mutatja, hogy a részterület dinamikusabban, 8,4%-kal fog bővülni. Ezekre idén összesen 60 milliárd dollár értékben költenek a vállalatok és a végfelhasználók. Bár sokáig úgy látszott, az IT-biztonsági termékek iránti keresletet még a nehéz gazdasági helyzet sem tudja jelentősen visszavetni, de az elmúlt időszakban volt néhány rosszabb éve ennek a szegmensnek is. Azonban mind az idei, mind a közeljövőre vonatkozó előrejelzések azt mutatják, hogy a szektor a bizonytalan piaci környezet ellenére egészséges növekedést tud felmutatni. Számítások szerint 2016-ban az összbevétel elérheti a 84 milliárdos szintet.

A pozitív változást alátámasztja a Gartner informatikai vezetők körében végzett átfogó kérdőíves kutatása[9] is. Ebben rákérdeztek arra is, várhatóan miként alakulnak jövőre a vállalati biztonsági büdzsék. A válaszadók fele stagnálásról számolt be, ám 45%-uk növekedést prognosztizált. Az arányok régiós szinten némi eltérést mutattak, a dinamikusan fejlődő területeken – mint például Brazília, India, Kína – ennél is magasabb volt a növekedést várók száma.

A biztonsági piacon belül a legnagyobb fejlődést idén a szolgáltatások tudják felmutatni, míg a szoftvereké a második legjobban bővülő terület. Ez egyben azt is jelenti, hogy a hálózati eszközök és egyéb fizikai termékek szegmensében a teljes piac átlaga alatt marad a növekedés.

A fentiek konklúziója az, hogy a teljes körű kontroll illúzió napjainkban. A 21. századi felhasználók használni fogják saját mobil eszközeiket munka célokra, szoftvereket töltenek le, amelyekről úgy érzik, szükséges a munkájukhoz és úgy fogják gondolni, biztonságosan jártak el. Ezek azok a kihívások, amelyekre az IT vezetőknek fel kell készülniük és hatékony válaszokat kell találniuk.

8 BITPORT: Cégen belül nehezen adható el az IT-biztonság; Bitport.hu; 2012.12.11.
9 BITPORT: A fenyegetettség megnyitja a pénztárcákat a biztonsági piacon; 2012.09.14.

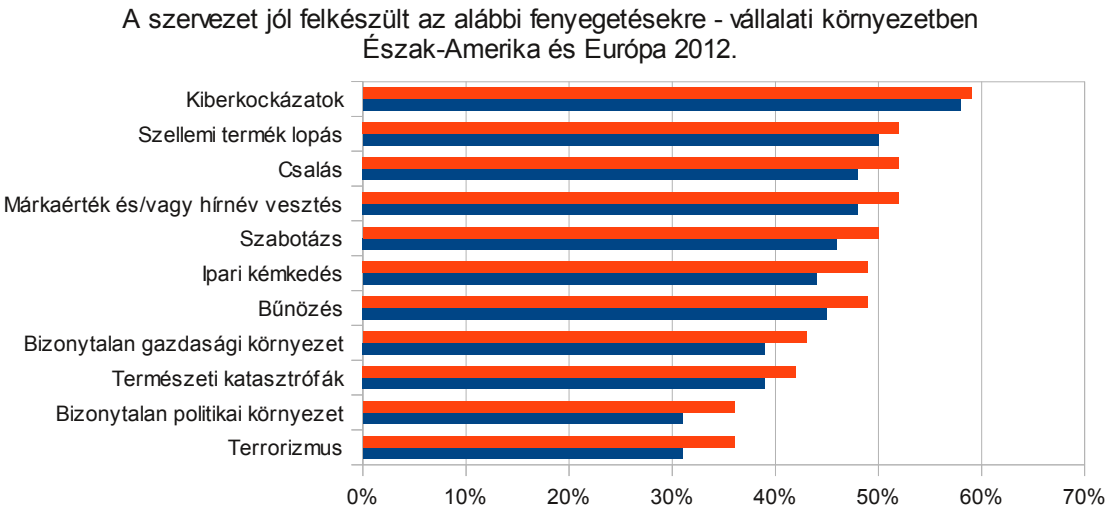
A jövő mobil-biztonsági stratégiai irányait feltérképezve több kutató véleményeit összevetve az alábbi ütemterv bontakozik ki, mint legvalószínűbb forgatókönyv:

- 2014-ben a vállalkozások 85%-a engedi meg munkatársainak, hogy saját mobileszközeiken SaaS szolgáltatásokat használjanak.
- 2015-ben a cégek 50%-a engedi meg munkatársainak, hogy saját mobileszközeiket használják.
- 2015 év végéig 50%-ban a felhasználók személyi adataikat a közösségi hálózatokon tartják.
- 2016 év végéig a vállalkozások több mint 30%-a fog használni távoli eléréshez hitelesítést.
- 2016-ban a vállalkozások 80%-a igényli az SSO (single sign on) technológiát.
- 2016-ban a rosszindulatú szoftverek célpontjai az operációs rendszerek lesznek.
- 2017-re a végfelhasználók több mint 50%-a használ alkalmazásboltból származó védelmi szoftvereket.

Nemzetközi IT-biztonság

A globális információbiztonsági incidensek növekedése, a csökkentett büdzsék és a biztonságvédelmi programok elhanyagolása oda vezetett, hogy manapság a vállalatoknak egyre több olyan biztonsági kockázattal kell szembesülniük, melyeket a belső szakértők nem látnak át, és emiatt nem is tudják konzisztensen kezelni. Az IT-vezetők többsége ennek ellenére biztos abban, hogy mindent megtesz a megfelelő IT-biztonság elérése érdekében. Meglehet, túlzott az optimizmusuk, hiszen egyre több akadályozó tényezővel kell(ene) számolniuk – legalábbis erre az eredményre jutott a PwC, a CIO Magazine és a CSO Magazine által közösen végzett 2013-as Globális információbiztonsági felmérés.[10]

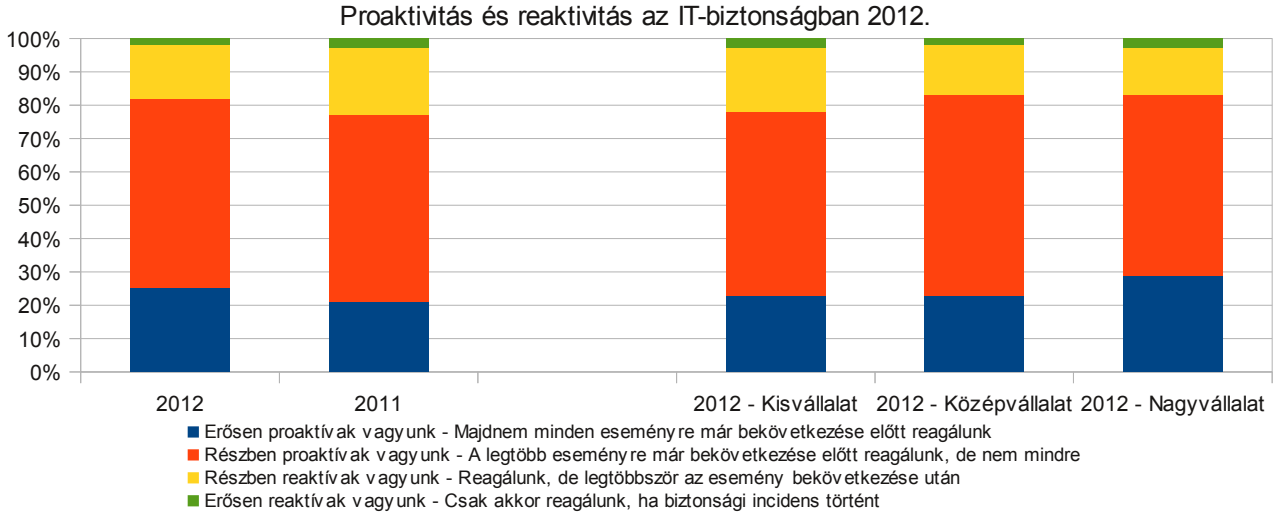
A vállalatok bő kétharmada úgy véli, sikerült beépíteni a vállalati kultúrába a hatékony információbiztonsági viselkedést, ráadásul több mint 70%-uk biztos abban is, hogy a valós információbiztonsági tevékenységeik valóban hatékonyak. Magabiztosságukat táplálja az is, hogy a a válaszadók közel fele (42%) saját vállalkozását az információvédelmi stratégiák és implementációk éllovasának tekinti. Ha azonban ezt összevetjük azzal, hogy a felmérés készítői szerint mindössze 8%-uk értékelhető valójában piacvezetőnek az információbiztonság szempontjából, erősen megkérdőjelezhető a vállalatok magabiztossága.



Forrás: Kaspersky[5]

10 PriceWaterhouseCoopers: The Global State of Information Security® Survey 2013; 2012. november

A vállalatok nagy többsége felkészültsége mellett reakciókészségét is igen jóra értékeli. A szakemberek szerint ezek az eredmények is túlzóak némiképpen, de az tény, hogy az elmúlt évek során sikerült a proaktivitás fontosságát egyre nagyobb mértékben megértetni és elfogadtatni a szervezetek IT- és pénzügyi vezetésével, így a felkészültség valóban javuló tendenciát mutat.

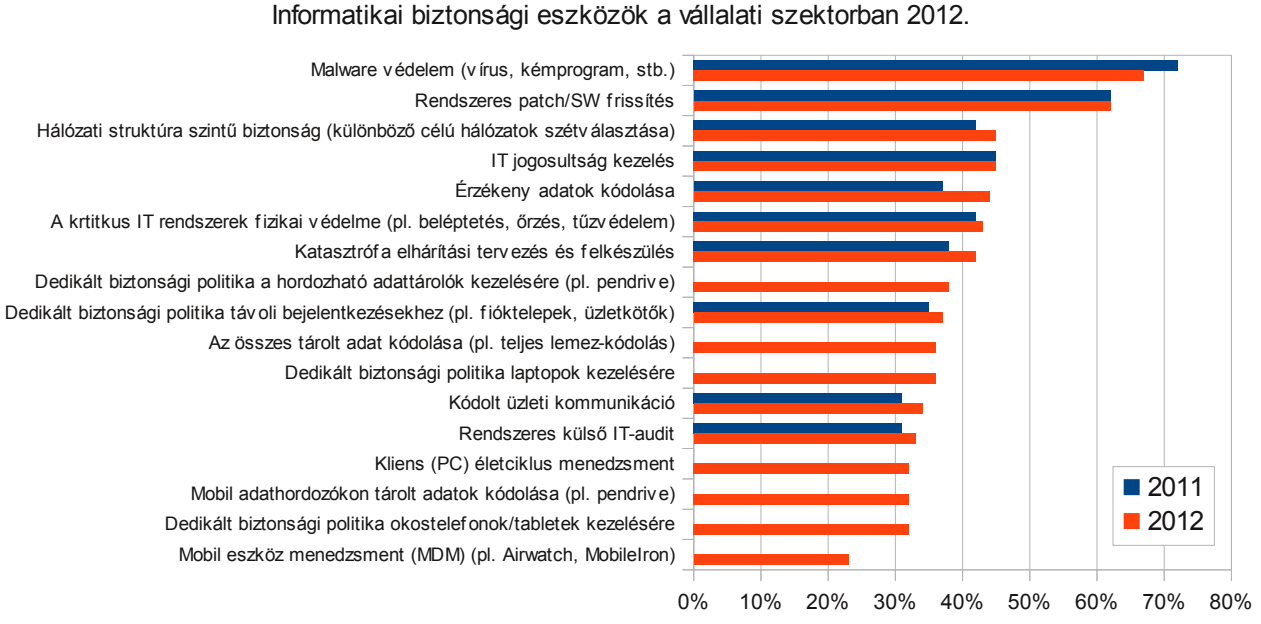


Forrás: Kaspersky[5]

Igazán felkészültnek azok a cégek minősülnek, ahol van vezető információbiztonsági menedzser, aki folyamatosan informálja a felsővezetést, van egy átfogó információbiztonsági stratégia, mérték és értékelték az elmúlt év információbiztonsági intézkedéseinek hatékonyságát, valamint tudatában vannak a felmerült biztonságkockázati eseményeknek.

Eszközrendszerét tekintve a vállalati IT-biztonságban majdnem minden vállalat tisztában van az alapvető biztonsági intézkedések fontosságával, alkalmazzák is ezeket, a legújabb idők jellemző kihívásaira (BYOD, cloud, adatszivárgás, stb.) viszont sokan még mindig nem, vagy csak nagyon alap szinten reagálnak.

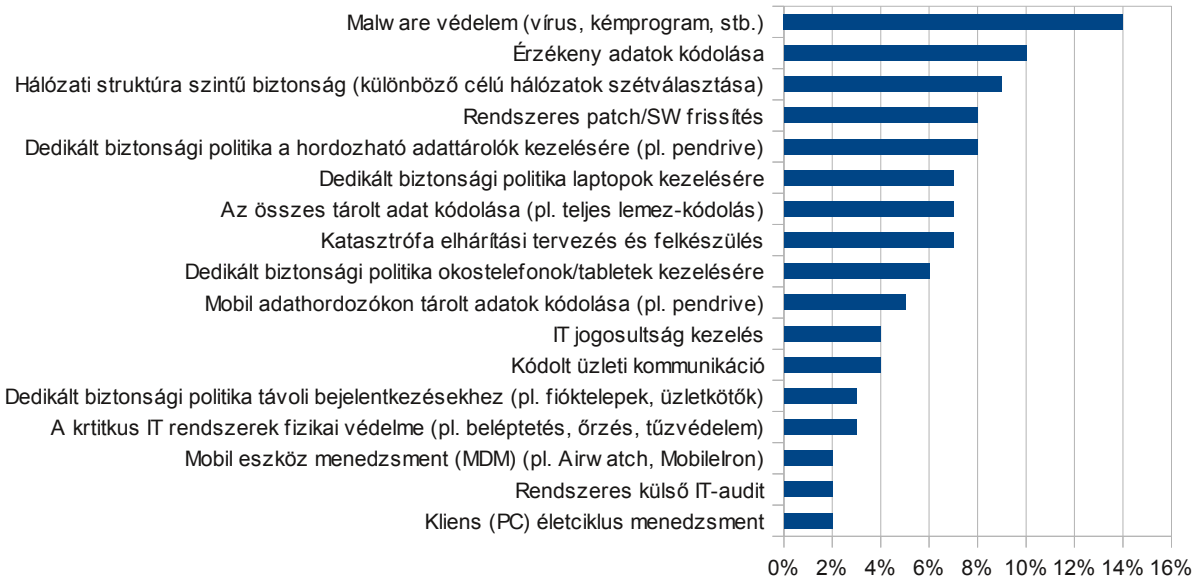
A működőképes biztonsági előírások kialakítását az is nehezíti, hogy egyre kevesebb védelmi eszközt használnak a vállalatoknál. Például a rosszindulatú kódokat, spyware-eket, adware-eket felismerő eszközöket használók aránya a 2008-as 84%-os tetőzés után 2012-ben 67%-ra esett vissza. Behatolásvédelmi eszközöket pedig régebben a válaszadók kétharmada alkalmazott, ma azonban már csak fele.



Forrás: Kaspersky[5]

Még mindig az antivírus programok a legnépszerűbb biztonsági eszközök a külső fenyegetések ellen, ám az IT-szakemberek egyre inkább rájönnek, hogy a rosszindulatú programok blokkolása nem ad teljes körű védelmet a szervezetnek. A szakemberek 14%-a úgy gondolta, hogy a jövőben a vírusvédelem mellett más biztonsági területek fejlesztése is elengedhetetlen, különösen az adattitkosítás és a helyi hálózatok területén.

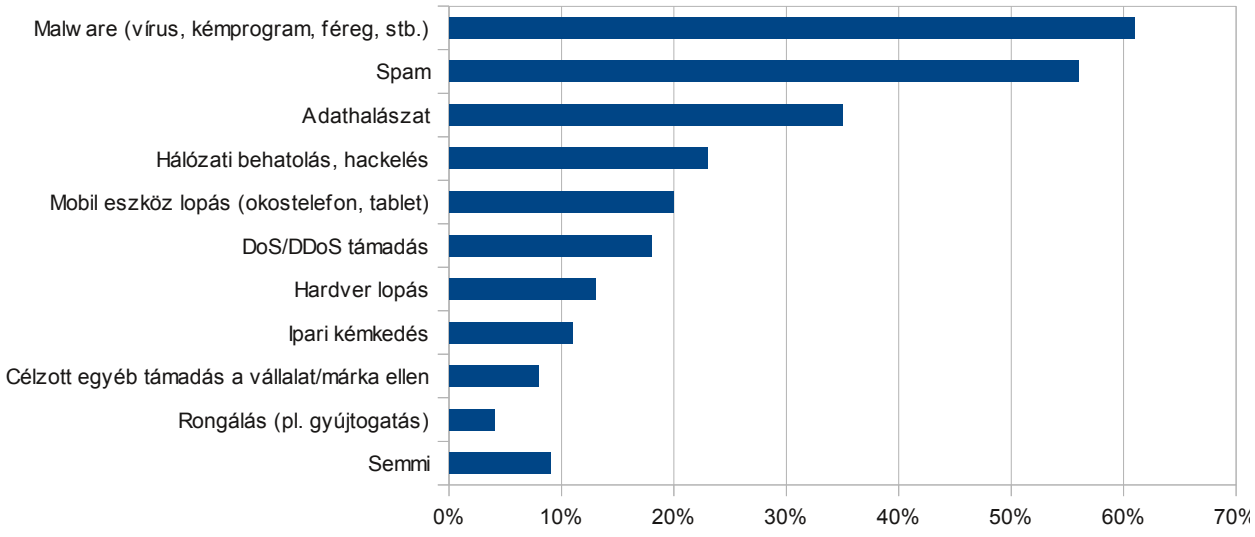
Fejlesztésre szoruló IT-biztonsági megoldások a vállalati szektorban 2013.
IT vezetők %-a említette



Forrás: Kaspersky[5]

Bár egyre több válaszadó (idén 13%) számol be 50 vagy még több információbiztonsági incidensről, kevesebb mint a felük (45%) számol azzal, hogy a biztonságra fordítható büdzséjük nő a következő 12 hónapban. 2010-ben még 52%-uk, 2011-ben pedig 51%-uk számolt a büdzsé növelésével. Úgy tűnik, hogy bár több tényező is befolyásolja az információbiztonsági büdzsé alakulását, a legnagyobb hatással a gazdasági környezet alakulása van rá, az információvédelemmel kapcsolatos aggodalmak csak a sokadik helyen szerepelnek. Érdekes ellenmondást mutat a felmérés: bár a felső vezetés tisztában van a probléma súlyával, a válaszadók fele, a biztonságért felelős vezetőknek pedig a 86%-a épp őket tartja az információbiztonsági fejlesztések legfőbb akadályának.

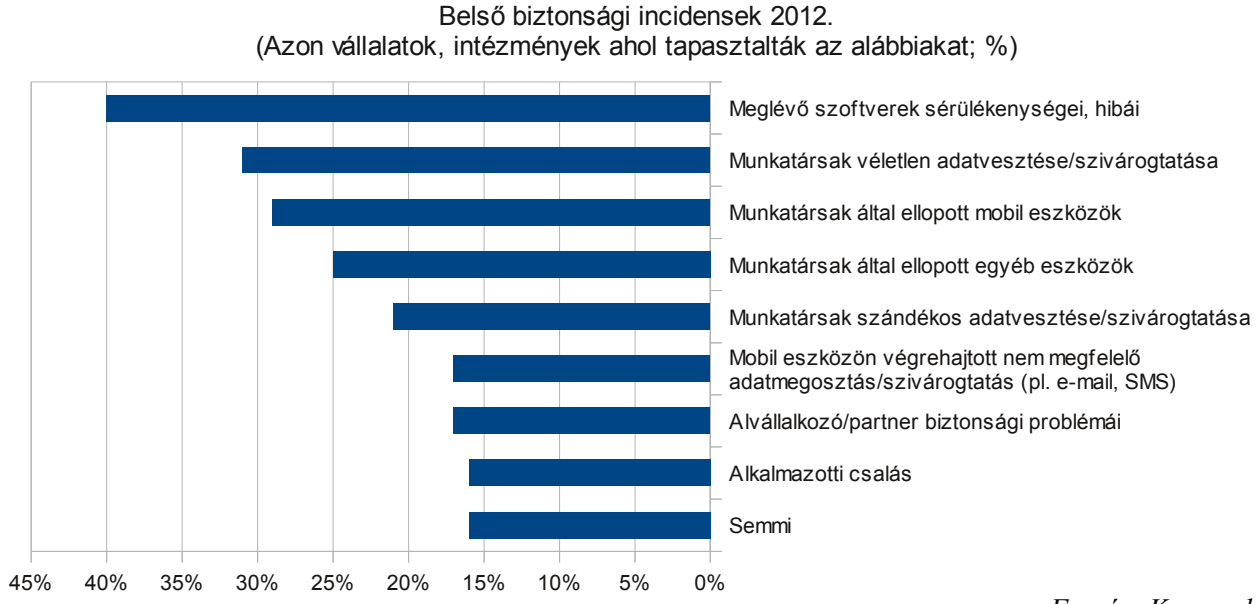
Külső biztonsági incidensek 2012.
(Azon vállalatok intézmények ahol tapasztalták az alábbiakat; %)



Forrás: Kaspersky[5]

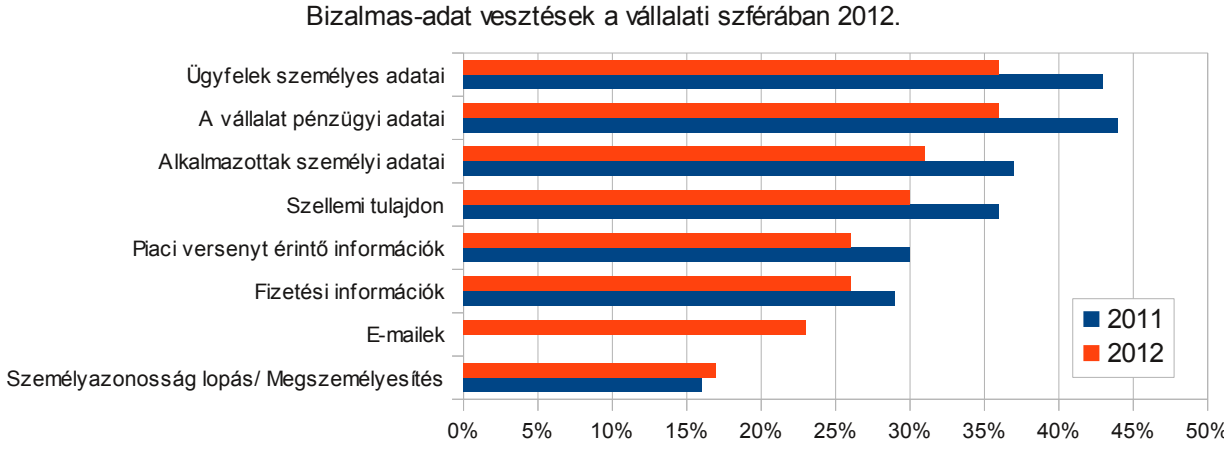
Az általánosnak mondható külső biztonsági incidensek mellett, amire általában a szervezetek IT-szakemberei, biztonsági megoldásai fel vannak készülve, egyre nagyobb szerepet töltenek be a belülről jövő problémák. Ezek megfelelő kezelése, felderítése és kivédése teljesen másfajta szemléletet igényel a vállalat részéről. Megfelelő kezelésükre jóval kevesebb cégnek állnak rendelkezésre a megfelelő protokollok.

A big data korszak beköszöntével lazul a cégeknél az adatok felügyelete. Miközben a válaszadók 80%-a szerint fontos az ügyfelek és az alkalmazottak adatainak biztonsága, azt már sokkal kevesebben tudják, valójában mit is hordoznak ezek az adatok, és hogy hol tárolják őket a vállalati rendszerben. A vállalatok kevesebb mint 35%-a rendelkezik megfelelő ügyfél- és alkalmazotti adatokat tartalmazó adatleltárral, és csupán 31%-uknál van megfelelően nyilvántartva, hogy hol tárolják ezeket az adatokat, illetve hogy a tárolt adatokra milyen törvénykezés vonatkozik.



Forrás: Kaspersky[5]

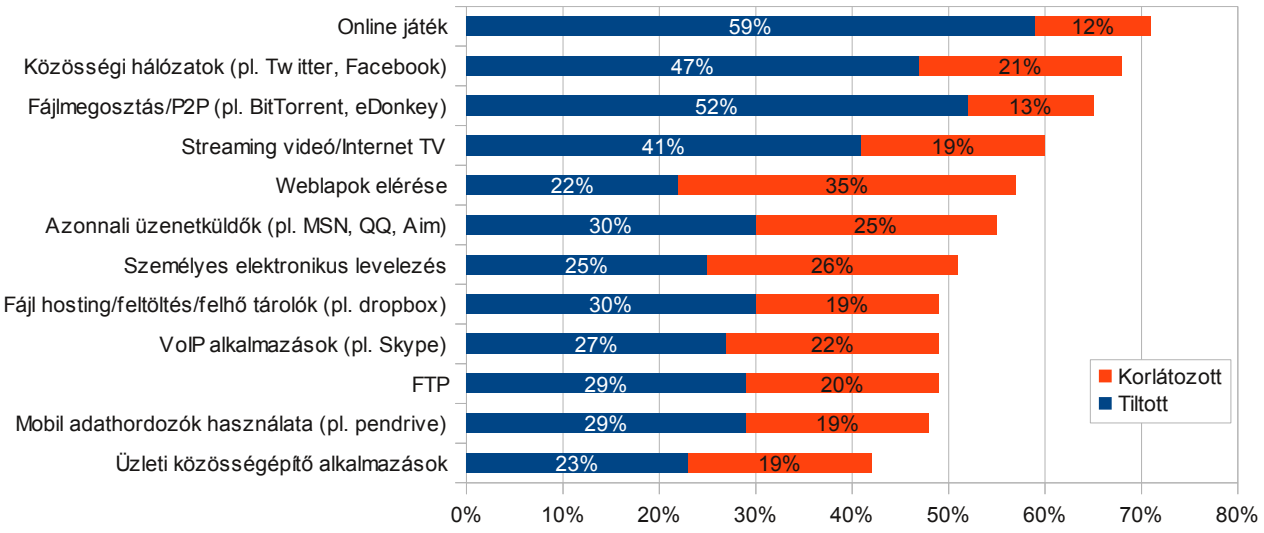
Az adatszivárgás a fenti incidensek, kockázatok egyik igen súlyos, az utóbbi időben és a jövőre nézve egyre gyakoribb következménye. A támadások – legyen az külső vagy belső – nagy többsége manapság éppen az adatok megszerzése, kiszivárogtatása érdekében történik, mégpedig igen pontosan célzottan és tudatosan. Ennek ellenére az adatvédelem területe az egyik legkevésbé jól szervezett, legkevésbé világos koncepciókkal és stratégiákkal rendelkező terület az IT-biztonság területén. Léteznek kifejezetten adatszivárgás elleni (DLP – Data Leakage Protection) megoldások, ám a vállalatok mintegy harmada ezek bevezetését túl komplikált feladatnak tartja, de a többiek sem túlzottan előrehaladottak az ilyen projektek területén.



Forrás: Kaspersky[5]

A belső és külső fenyegetések legyőzése érdekében és a vállalat produktivitását növelendő, az informatikai osztályok nagyon sok esetben tiltanak, illetve korlátoznak bizonyos felhasználói magatartásokat. A legfontosabb ilyen tevékenységek, az online játékok, a közösségi oldalak, a filemegosztók, illetve az online videomegosztó portálok, de bizonyos weboldalak korlátozása is elterjedt a vállalati körben. Az eredmények azt mutatják, hogy a vállalatok a produktivitást (munkaidőrabló alkalmazások, tevékenységek korlátozása) sokkal fontosabbnak tartják, mint az IT-biztonság szempontjából valóban fenyegető viselkedés (mobil adathordozók, FTP, felhő-tárhelyek) korlátozását.

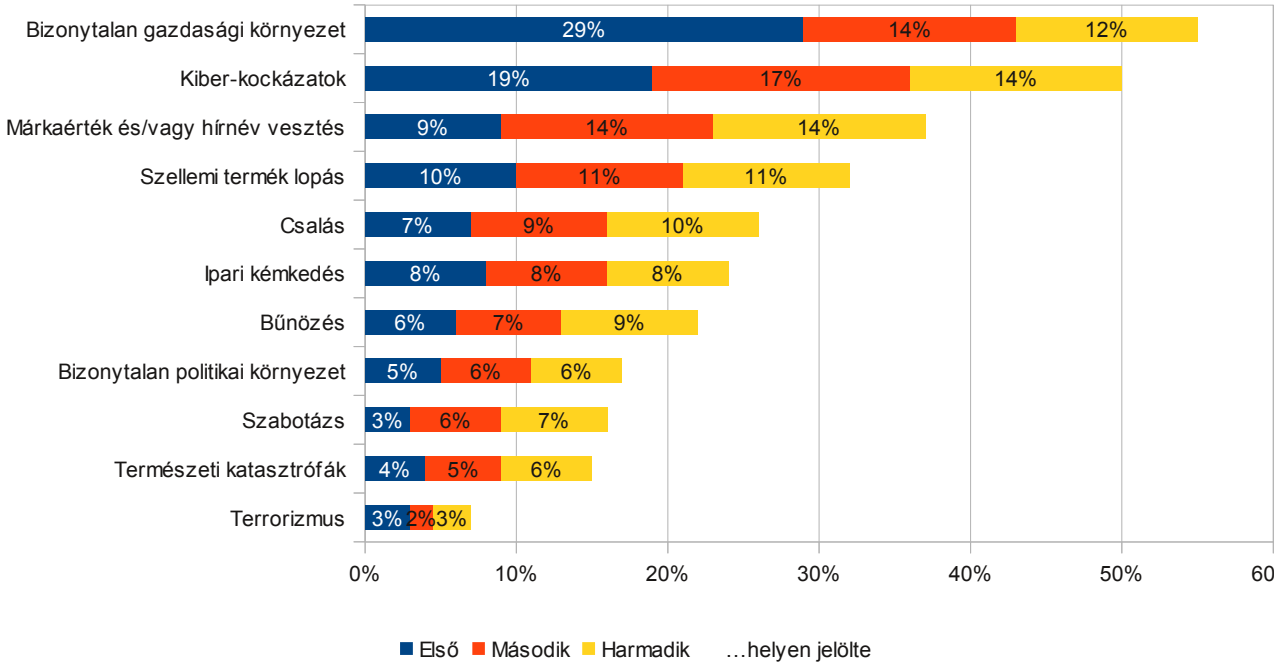
Tiltott vagy korlátozott tevékenységek a vállalati szektorban 2012. (%)



Forrás: Kaspersky[5]

A kockázatokat tekintve az IT-vezetők azzal is egyre inkább tisztában vannak, hogy nem csak a biztonsági incidensek érinthetik rosszul a vállalatot. Bár ott van a TOP3 kockázati tényező között, a gazdasági bizonytalanság és a vállalat hírnevének megtartása legalább ennyire fontos szempontok az IT-stratégia tervezésekor.

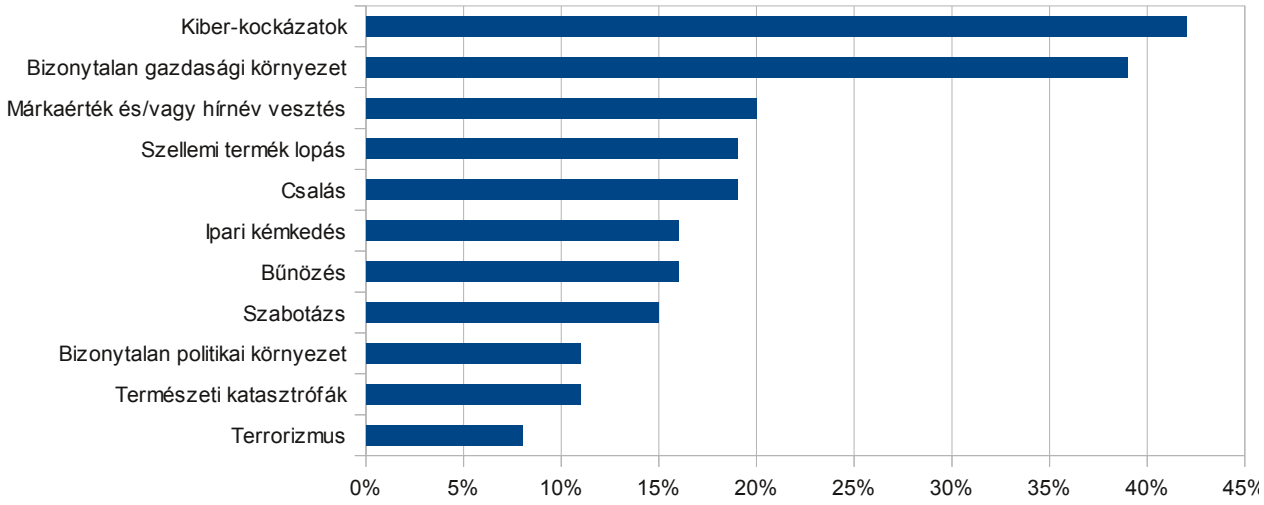
2012 során legkritikusabbra értékelt kockázatok a vállalati és állami szférában



Forrás: Kaspersky[5]

A válságból való kilábalást és az IT-büdzsék fokozatos erősödését mutatja, hogy a jövőre nézve viszont egyértelműen a védekezés, a biztonsági incidensek elhárítása a IT-szakemberek fő prioritása.

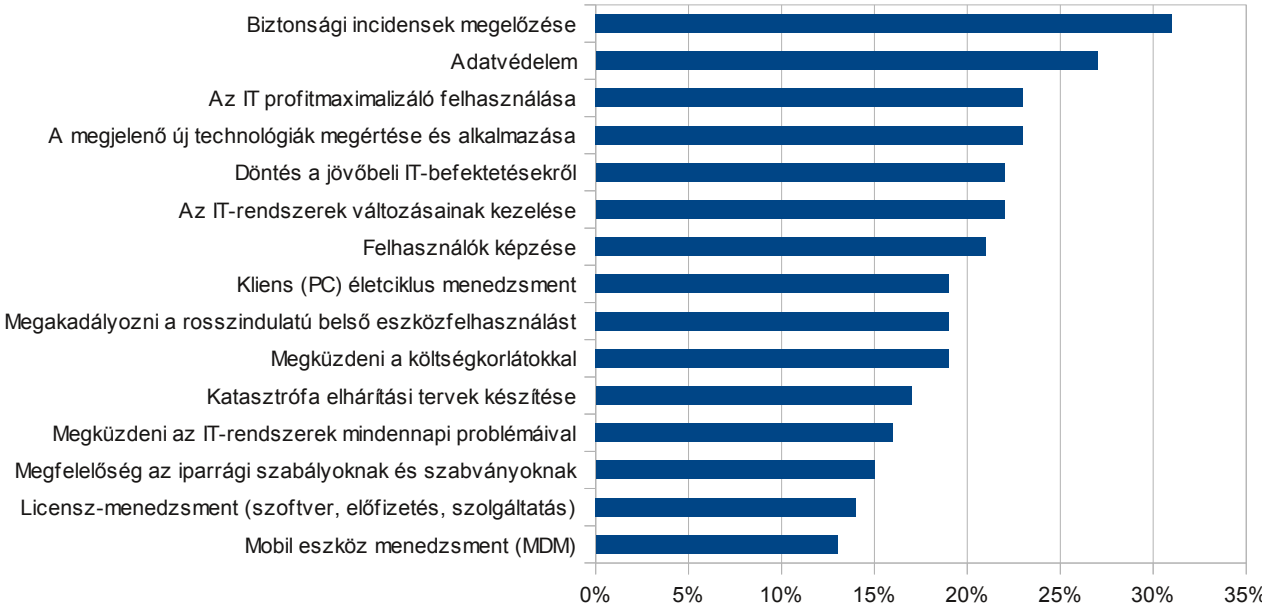
2013-as várakozások alapján legkritikusabbra értékelt kockázatok a vállalati és állami szférában



Forrás: Kaspersky[5]

Az IT-szakemberekre ezen általános problémák kezelésén túl nagyon is konkrét kihívások várnak a következő évben. A biztonság fenntartásán túl az elsődleges prioritás az IT-biztonsági terület ésszerű, minél inkább profitmaximalizáló forrásfelhasználásának biztosítása. A vállalatok pénzügyi vezetői a válság tapasztalataiból okulva még erőteljesebben figyelnek a ROI megfelelő alakulására, de természetesen a biztonsági-stratégiai területen is vannak még tennivalók.

Az IT-szakemberekre váró legfontosabb kihívások 2013-ban



Forrás: Kaspersky[5]

Érdekes kérdés annak körbejárása, hogy ezek a hiányosságok miért maradhattak fenn éveken keresztül, miért nem tudnak a szervezetek kellő hatékonyságú IT-biztonságot felépíteni. AZ IT-szakemberek ennek okait részben anyagi, nagyobb részt viszont szervezési, kommunikációs, HR és ellátási láncbeli problémákkal indokolták.

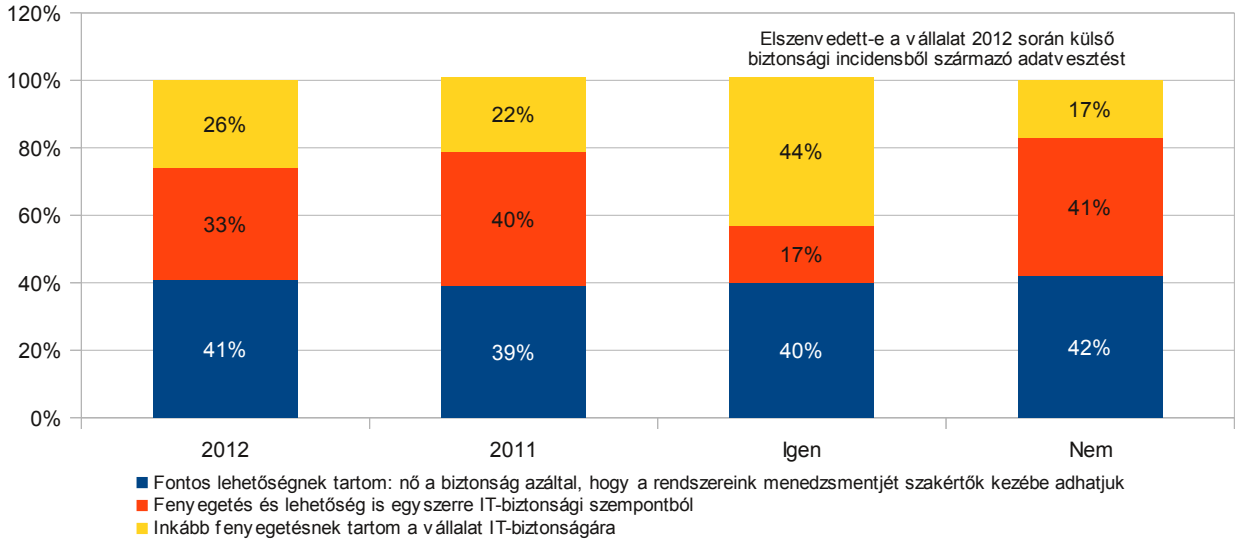
Akadályok az erőteljesebb IT-biztonság előtt 2012.

Forrás: Kaspersky[5]

Ahogy az az előző alfejezetben is látható volt, a mobileszközök biztonsági szempontú kezelése szintén kritikus pontja a vállalati infrastruktúrának. A közösségi média, a mobilkészülékek és a felhő szolgáltatások megjelenése cégen kívül és belül sokkal gyorsabban zajlik, mint az ezeket védő technológiák adaptációja. A BYOD szemlélet rohamos terjedését minden kutatás igazolja: a fogyasztók 88%-a használja ugyanazt a mobil készülékét munkára és személyes célokra, ugyanakkor a vállalatoknak mindössze 45%-ának van információbiztonsági stratégiája ezekre a személyes készülékekre vonatkozóan, és még kevesebben (37%) védekeznek is a nem kívánatos szoftverek ellen.

Az elmúlt évekhez képest érzékelhetően emelkedett azon cégek száma, akik információbiztonsági szabályokat és eljárásokat alakítanak ki a mobilkészülékek, közösségi média, és felhőszolgáltatások alkalmazottak által történő használatára. Az arányuk azonban még mindig alacsony: a válaszadók 44%-ának van mobil biztonsági stratégiája, de kevesebb mint 40%-uk alakított ki külön stratégiát a közösségi médiára és a felhőre.

A felhőszolgáltatásokkal szembeni attitűdök a vállalati szektorban 2012.



Forrás: Cisco[11]

11 Cisco: Global Cloud Index; 2012. október

A költségcsökkentés, a biztonság növelése, a kockázatkezelés és az adatok mennyiségének növekedése okozza a legnagyobb problémát. Emiatt közeljövőnkben a globális adatforgalom fele a felhőkbe kerülhet.

2014-re az adatközpontok számítási kapacitásának több mint fele felhő alapú lesz, a globális felhőforgalom 2015-re pedig a 12-szeresére: évi 1,6 zettabájtra nő. Pedig még sok számítástechnikai szakember számára nem tiszta, hogy a meglévő infrastruktúra keretei között hogyan helyezzék át alkalmazásaikat a felhőbe, derült ki egy a Cisco által készített felmérésből[11], amelyet 13 ország (Ausztrália, Brazília, Egyesült Államok, Egyesült Királyság, Franciaország, India, Japán, Kanada, Kína, Mexikó, Németország, Oroszország, Spanyolország) több mint 1300 informatikai döntéshozójának részvételével végeztek.

Többek között a felhőbe helyezhető alkalmazások, hálózati kihívások és akadályok, illetve az adatbiztonság kérdéseit vizsgálták. A résztvevők 39%-a tart továbbra is a privát vagy nyilvános felhők bevezetésével járó hálózati kihívásoktól. A megkérdezettek 72 %-a az adatbiztonságot tartja aggályosnak, 67% az elérhetőség és a megbízhatóság miatt aggódott.

A tanulmány szerint az alkalmazások számítási felhőbe történő áthelyezésének a kulcsa a hálózat fejlesztése. Ennek előfeltételének pedig a virtualizált adatközpontot és a felhőszolgáltatóval való szolgáltatásszint-megállapodást emelték ki.

IT-biztonság Magyarországon

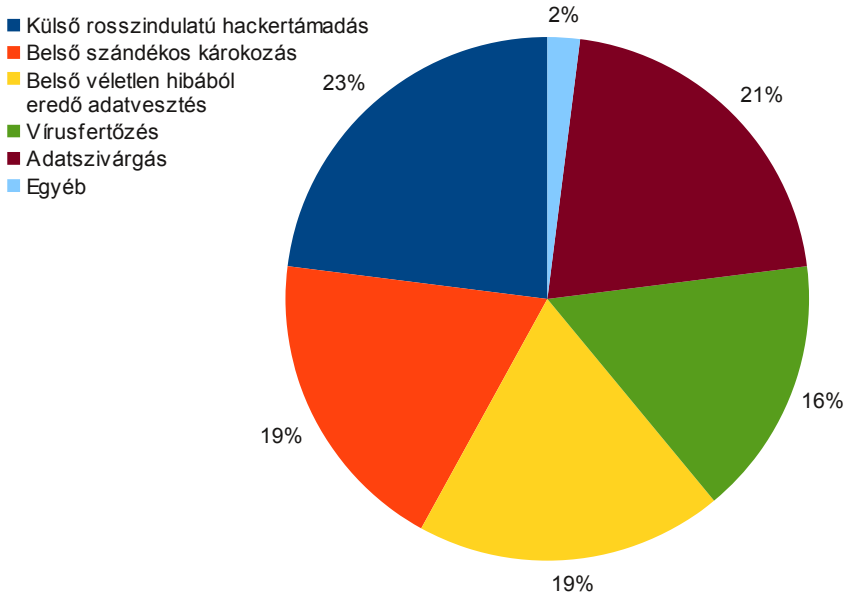
A számítógépes bűnözői csoportok nemcsak egyre prominensebb áldozatokat ejtenek világszerte, hanem a tapasztalatok szerint a támadások száma is sűrűsödik, a célba vett vállalkozások köre pedig lényegesen bővül azóta, hogy a szervezett bűnözés felfedezte magának ezt a jelentős, illegális jövedelemforrást.

Tévedés azt hinni, hogy a támadásoknak Magyarországon működő cégek nem lehetnek célpontjai, vagy hogy a bűnözők bizonyos vállalatméret alatt nem látnak fantáziát egy-egy célpontban. A támadások felépítése és a célpontok kiválasztása szinte minden esetben tudatos, a döntő szempont pedig a megszerezhető adatok „piaci” értéke.

Bár sokan érzik a fenyegetések legkritikusabb formájának a külső támadásokat (hacker-támadás, vírusok), a válaszadók többsége (59%) szerint ennél is nagyobb fenyegetést jelentenek a cégen belüli, emberi tényezők.

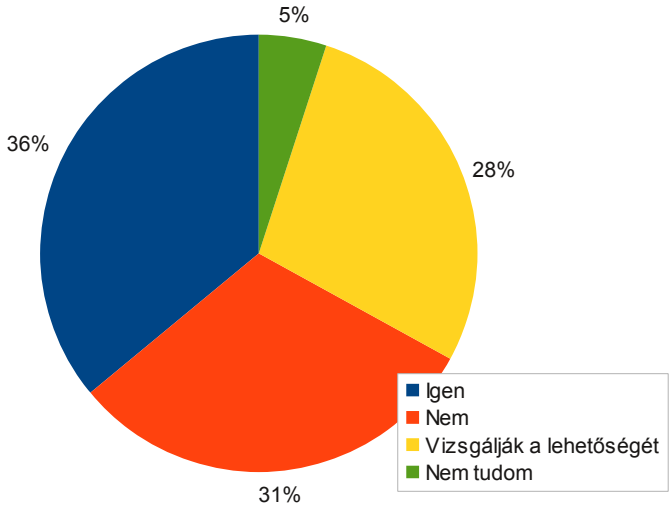
Ilyen belső tényező lehet az akár véletlen hibából adódó, akár szándékos károkozás, de az adatszivárgás is, amelynek csatornái (és sokszor vétlen eszközei) szinte kivétel nélkül a saját alkalmazottak, még ha az értékes üzleti adatok megszerzésére irányuló támadás jó eséllyel a cégen kívülről indul is. A felsorolt fenyegetések mindegyik típusa valós veszélyt jelent a vállalati, üzleti adatok biztonságára nézve.

A legkritikusabbank ítélt IT-fenyegetések a magyarországi vállalatok esetében 2012.



Forrás: CDSys[12]

Felhő technológiák alkalmazása a magyar vállalati szektorban 2012.



A felhőalapú technológiák terjedésére utal, hogy a válaszadók 36%-a alkalmazza, további 28%-ukat pedig komolyan foglalkoztatja a cloud computing alkalmazása saját cégénél. Sok cég esetében viszont eleve fel sem merül az igény, 23%-uk pedig a felhőalapú rendszerekkel összefüggő biztonsági kihívások miatt teljesen elzárkózik a technológia alkalmazásától. Hátráltathatja a cloud-ra épülő modellek és szolgáltatások széles körű terjedését az a 2011 decemberében megalkotott törvény is, amely korlátozza az adatok más félnek történő kiadását.

Forrás: CDSys[12]

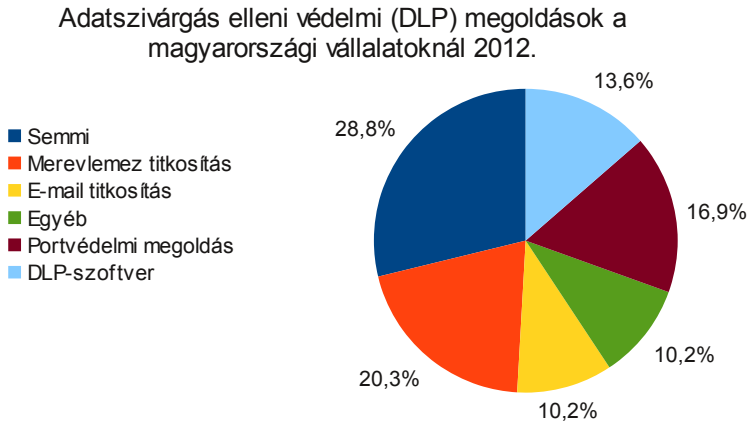
Egyre erősödő tendencia, hogy a munkavállalók saját mobil eszközeikről szeretnének hozzáférni a vállalati hálózathoz, vagy elérni a céges alkalmazásokat. Ez komoly biztonsági kihívásokat rejt magában, és felkészülést igényel a cégek részéről. Mindenekelőtt le kell fektetni a mobileszközök használatának pontos irányelveit a vállalaton belül, és ezeket tudatosítani kell az érintett munkatársakban is. A hozzáférést biztosító platformok egységesítésén kívül az adatbiztonsági kérdésekre is megnyugtató válaszokat kell találni.

A hazai vállalatok informatikai biztonsága egyelőre nem tud megfelelő választ adni a felmerülő biztonsági kihívásokra, illetve a cégek döntő többsége még felbecsülni sem tudja, hogy mekkora kár éri a vállalatot egy adatszivárgási incidens alkalmával.

12 CDSys: Milliós adatszivárgási károk Magyarországon; 2012.12.05.

A magyarországi IT-vezetők 70%-a már hallott valamilyen adatszivárgás elleni védelemről, ugyanakkor a válaszadók közel harmadánál nem használnak semmiféle adatvédelmi megoldást. A cégeknél használt adatvédelmi megoldások közül a merevlemez titkosítás a legelterjedtebb (20%), amelyet a portvédelmi megoldás követ (17%), DLP szoftvert csak mintegy 14% használ.

Forrás: CDSys[12]



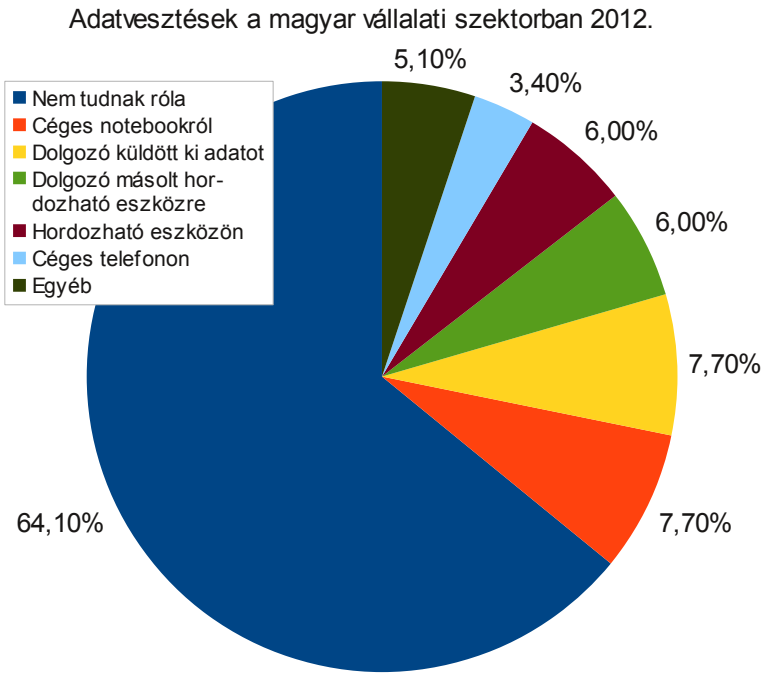
A vállalatok több mint felénél osztályozva vannak az adatok, de jelentős részben a dolgozók saját maguk osztályozzák a cég adatait, ami biztonsági szempontból aggályos. Közel 15%-nál semmiféle osztályozás nincs, azaz a dolgozók és a vezetők nem mindig tudják megállapítani, hogy melyik adat a bizalmas és melyik nem. Az adatok használatának szabályozása, illetve az ezekhez kapcsolódó oktatás csak a cégek felénél jellemző, 23%-nál csak szabályozás van, oktatás nincs, a válaszadók ötödénél pedig se szabályozás, se oktatás nincs.

A vállalatok 45%-ánál használnak dolgozói tulajdonú hordozható, vagy asztali számítógépet, amelyeknek csupán 30%-án van ugyanolyan szintű védelem, mint a vállalatnál, és a gépek 15%-án semmiféle védelmi megoldás nincs. Manapság kulcsfontosságú téma, a mobileszközök védelme. A tapasztalt az, hogy a vállalatok felénél használnak okostelefont és táblagépet és ezek negyede a munkavállalók tulajdonában van. A dolgozók tulajdonában lévő okostelefonok aránya nagyobb, de a magántulajdonú táblagépek is kezdenek elterjedni vállalati környezetben, ami kritikus tényező lehet az adatszivárgás elleni védelemben.

A vállalatok több mint felénél nincs kétfaktoros azonosítás, ahol van, ott a fizikai tokenes azonosítás a legelterjedtebb megoldás, amelyet a szoftveres azonosítás követ.

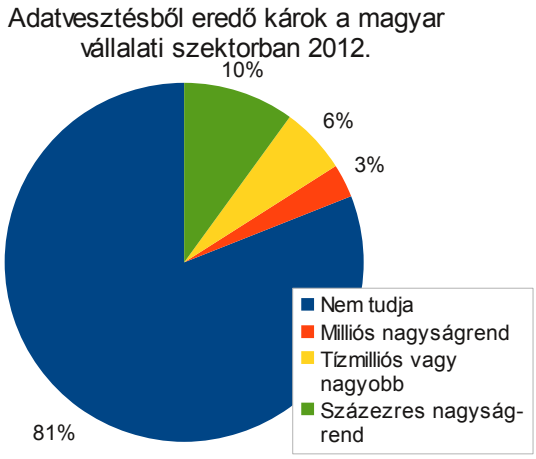
A vállalatok dolgozói közel 65%-ának nincs tudomása adatszivárgási incidensekről, ami természetesen nem azt jelenti, hogy ezek az esetek nem léteznek, inkább arról van szó, hogy a legtöbb esetben a vállalat maga sem észleli ezeket, illetve a legtöbb felfedezett incidenst a vezetőség igyekszik titokban tartani.

A leggyakoribb adatszivárgási esetekben a munkavállaló küldött ki bizalmas adatokat emailben, vagy más módon hálózaton keresztül, de ugyanilyen gyakoriságú az elveszett laptopok okozta adatvesztés is. Ugyancsak gyakori az elveszett céges hordozható eszközök által bekövetkezett adatszivárgás, illetve a saját használatra, a dolgozó által hordozható eszközre kimásolt anyagok aránya.



Forrás: CDSys[12]

A vállalatok 81%-a megbecsülni sem tudja, hogy mekkora kár érhette a cégét egy adatszivárgási esemény kapcsán. Ahol mégis, ott a százezres nagyságú kár a leggyakoribb, ugyanakkor a tízmillió forint feletti veszteség gyakoribb, mint a milliós kár.



Forrás: CDSys[12]

Kijelenthető, hogy a vállalatoknál nincs egységes koncepció az előforduló adatszivárgási esetek kezelésére. Egyharmaduk csak az incidens után hoz szabályokat, 30% utólagosan oktatja a munkavállalókat, 12% fegyelmi eljárásokat indít, és alig egytizedük tesz jogi lépéseket. Aggasztó, hogy csupán a válaszadók alig több mint felének van tudomása arról, hogy az új adatvédelmi törvény kapcsán milyen védelmi kötelezettségeknek kell eleget tenniük és milyen szankciókkal jár ezek elmulasztása. IT biztonsági vezető a cégek 12%-nál van, informatikai vezető a 35%-nál van alkalmazásban, és a vállalatok 40%-nál van mindkettő, illetve 13%-nál egyik sincs.

Forrás: CDSys[12]

Összegzésként elmondható, hogy a vállalatok nagy része már hallott valamilyen adatszivárgás elleni megoldásról, de 30%-a a cégeknek semmiféle adatvédelmi megoldást nem használ. Az adatok megfelelő osztályzása is problémás, mivel hiába használ a többség valamilyen adatosztályozást, az adatok bizalmas jellegének megállapítását zömében maguk a munkavállalók végzik, ami nem minden esetben jelent hatékony megoldást, ráadásul a bekövetkezett adatszivárgási incidensek nagy része továbbra is belső eredetű. Sajnos az adatvédelmi szabályozás kialakítása és a megfelelő oktatás is csak a cégek felénél jellemző, illetve aggodalomra adhat okot a mobileszközök, ezen belül a dolgozói tulajdonú készülékek elterjedése a vállalati környezetben. Ahogy a CDSYS felméréséből[12] kiderül a vállalatok munkatársai nincsenek tisztában az adatszivárgás okozta károk mértékével, és az ismert többmilliós nagyságrendű károkat okozó adatszivárgások mértéke arra enged következtetni, hogy a nem ismert adatszivárgási esetek összege jóval nagyobb lehet. A vállalatoknak tehát érdemes lehet elgondolkozni a megfelelő IT biztonsági szabályzatok bevezetésén és betartatásán, az alkalmazottak folyamatos biztonsági képzésén, illetve egy hatékony adatszivárgás elleni megoldás bevezetésén.

Államigazgatás

IT-biztonság

A régi technológiák nem szívódnak fel, de az új fenyegetések, a kedvezőtlen gazdasági folyamatok és a felhőalapú szolgáltatási modellek a biztonsági iparágat is átalakítják.

A kutatásokban a bevált preventív intézkedések közül tízből kilencen jelölték meg a tűzfal- és UTM-eszközök alkalmazását, míg 85%-ban az antivírus, anti-spyware vagy anti-spam típusú megoldások használatáról, 65%-ban pedig a hálózati hozzáférés menedzseléséről számoltak be. A válaszokból az is kiderült, hogy az elkövetkező tizenkét hónapban idehaza a hálózatbiztonság, a jogosultságkezelés és a mobil eszközök biztonsága kapja majd a legnagyobb figyelmet a kormányzati informatikában.

Az informatikai biztonság területén az új technológiák és felhasználói trendek mellett a támadások volumenét és összetettségét tekintve tapasztalhatók a legjelentősebb változások. Jóllehet a kibertámadások karakterisztikái jelentősen átalakultak az utóbbi időben, a velük szemben alkalmazott módszerek, illetve az IT szervezetek által alkalmazott „legjobb gyakorlatok” (best practice) nem változtak túl sokat.

Ez elsősorban az incidensek időtartamára vonatkozik. A legtöbb esetben semmi gond a támadás előtti (biztonsági audit, sebezhetőség-vizsgálat, behatolás-tesztelés stb.) és a támadás utáni (forensic vizsgálatok, megelőző események elemzése stb.) intézkedésekkel, ám ezek önmagukban csak a rövid ideig tartó próbálkozások esetében érnek valamit, mivel abból a feltételezésből indulnak ki, hogy az incidensek között, pláne a fenti eljárások során, a rendszerek nem állnak folyamatos támadás alatt.

A megoldást a szakember a szervezeti IT részlegen belül létrehozott, állandó készültségben lévő "kiberháborús irányítóközpont" felállításában látja, amely képes "tűz alatt" is elemezni a helyzetet, áthangolni a védelmet, meghatározni a támadási mintákat, és arra kényszeríteni a behatolókat, hogy felhagyjanak az akcióval. Ezeket a készségeket mielőbb adaptálni kell, sőt a különböző cégeknél működő központoknak egymással is érdemes kommunikálniuk, hogy sikeresek legyenek a kibertámadások legújabb hullámával szemben.

Az új trendek a globális recesszióval vagy éppen a cloud alapú kiszolgálási modellel karöltve a teljes szoftverpiacot, így a biztonsági iparágat is jelentősen átalakítják. Az IDC júliusi előrejelzése szerint a szolgáltatásként kínált szoftverek (SaaS) értékesítései modellje már ebben az évben is 7 milliárd dollárt szívott el a hagyományos szoftverlicencek piacáról, az árak pedig ezzel arányosan a következő években is tovább csökkennek majd. A teljes piac azonban folyamatosan erősödik, hiszen a kiberbiztonságra központi szerep hárul az üzletmenet folytonosságának biztosítása, illetve az ügyfelek bizalmának megtartása szempontjából.

Az előrejelzések szerint öt év múlva már az állami szektor és a közművek adják majd a kiberbiztonsági piac legnagyobb, 30%-os önálló szeletét, másrészt folyamatosan növekszik az érdeklődés a menedzselt biztonság, valamint a tanácsadás iránt. Az ügyfelek nem feltétlenül antivírust, tűzfalat vagy más konkrét terméket vásárolnak, hanem egy-egy adott problémára keresnek teljeskörű megoldást, ami a gyártók és az értéknövelt viszonteladók számára is új lehetőségeket tartogat, bár mindenképpen a disztribúciós csatornák átalakítását feltételezi.

A jövő olyan kiszolgálási modelleket tartogat, amelyek révén mindenki úgy veheti igénybe a biztonsági készségeket, ahogy manapság például az iTunes rendszerét használja. A terebélyes és átláthatatlan infrastruktúra adminisztrációs szempontból is olyan megközelítést igényel, mint amilyen mondjuk a megbízhatóság-alapú elemzések alkalmazása, figyelembe véve akár az egyedi felhasználói szokásokat is, de a sokak szerint túlhaladott termékek – mint az antivírusok – ideje sem járt le, legfeljebb a technológiák „átméretezésére” lesz szükség.

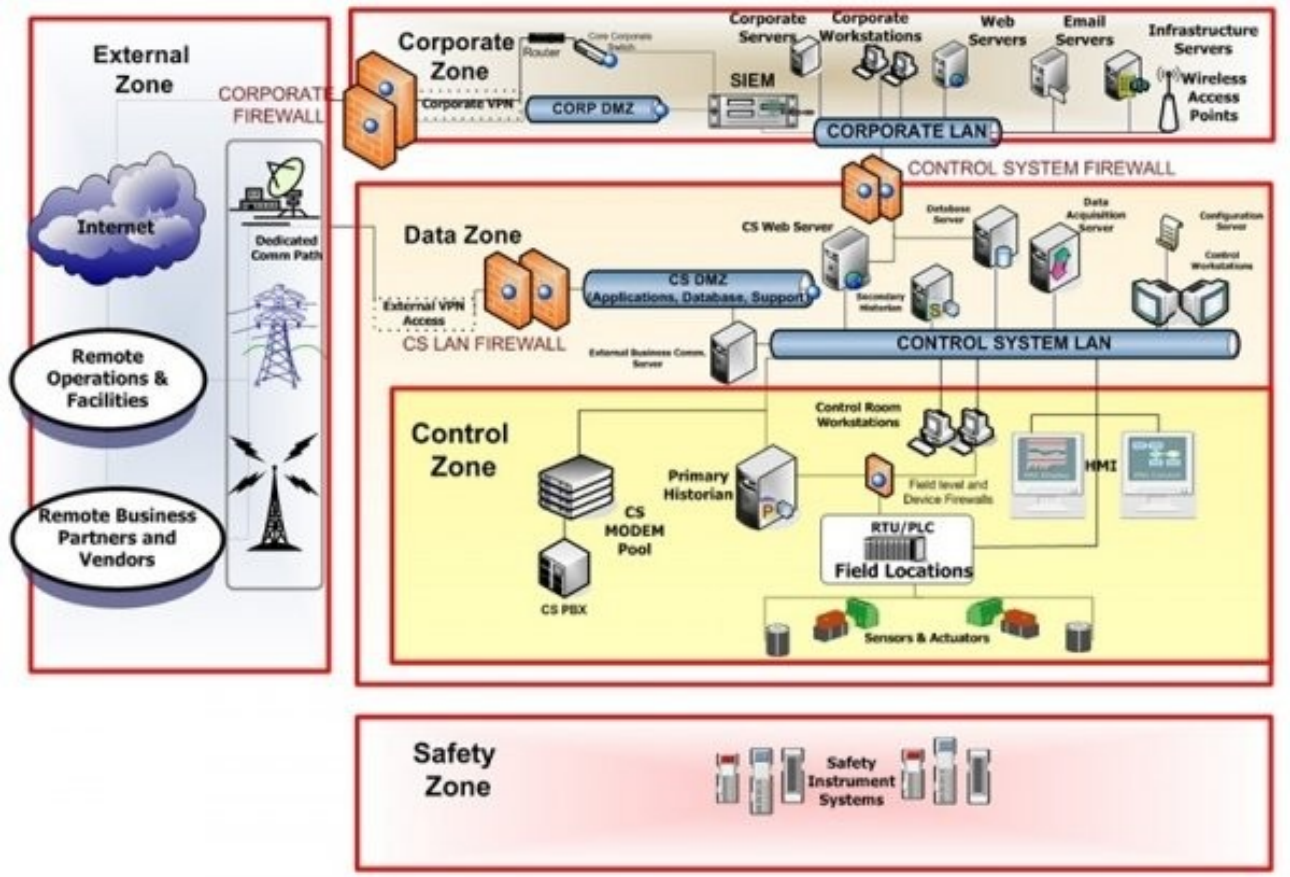
Ahogy az informatikai biztonság határterületei egyre jobban elmosódnak, olyan egységes platformok kialakulására lehet számítani, ahol könnyű az éppen szükséges dolgokat letölteni vagy engedélyezni, másokat pedig ugyanígy felfüggeszteni vagy tiltani is lehet. A mélyülő konvergencia jegyében a hagyományos eszközök az antivírustól a behatolás-megelőző rendszerekig (IPS) ezeken az egységes platformokon futnak, ami nem az egyes technológiák vagy a régi gyártók eltűnésével, inkább a kategóriák átalakulásával jár majd.

Kritikus infrastruktúrák

2012-ben minden korábbinál többször bizonyosodott be, hogy az ipari rendszerek és a kritikus infrastruktúrák is kiszolgáltatottak a kibertámadásokkal szemben.

Az amerikai Belbiztonsági Minisztérium irányítása alatt működő ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) szervezet 2012-re vonatkozó felmérése[13] mind a kritikus infrastruktúrák, mind az ipari vezérlő-, felügyeleti és adatgyűjtő rendszerek ellen elkövetett jelentős támadásokat górcső alá vette. A nyilvánosságra került információk tanúsága szerint tavaly 198 olyan regisztrált biztonsági incidens történt, amelyek ilyen rendszerek, infrastruktúrák esetében következtek be.

Védelmi architektúra szegmentálással



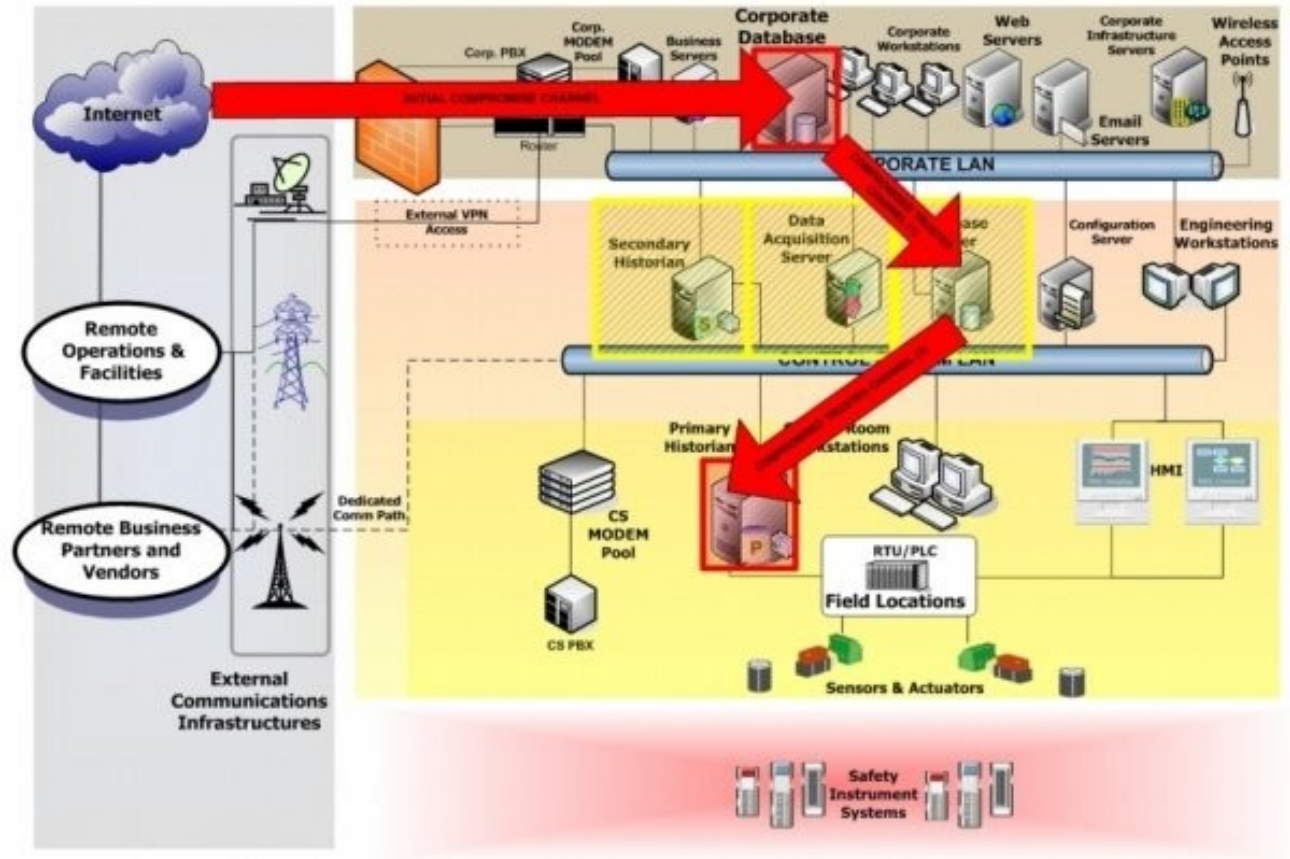
Forrás: ICS-CERT[13]

A napvilágra került biztonsági események 40%-a energetikai vállalatok, szolgáltatók informatikai hálózatát sújtotta. A második legtöbbször célkeresztbe állított rendszereknek pedig a vízellátásban kulcsfontosságú szerepet betöltő infrastruktúrák számítottak. Ezek mellett viszonylag gyakran szúrtak szemet a támadóknak az olajipari és a földgázzal foglalkozó vállalatok is. Sok akció a kiberbűnözés szempontjából sikeresnek bizonyult, hiszen az elkövetőknek - többségében SCADA-rendszereken keresztül - sikerült titkos, bizalmas információkhoz hozzáférniük.

13 ICS-CERT: Monthly Monitor Oct-Dec 2012.; 2012. október

Az ICS-CERT külön kitért a nukleáris létesítmények elleni célzott támadásokra. A szervezet összesen hat bejelentést kapott az atomenergetikai szektor egyes szereplőitől. Ezen esetek kapcsán feltételezhető volt, hogy kritikus informatikai infrastruktúrák kompromittálódtak. A nagyon szigorú és alapos kivizsgálások során bebizonyosodott, hogy a támadóknak nem sikerült manipulálniuk e rendszereket, és nem tudtak vezérlést biztosító hálózatokhoz hozzáférést szerezni. Ennek ellenére ezek a nukleáris létesítmények elleni támadási kísérletek is jelentős mértékben felhívják a figyelmet a kockázatokra. Különösen igaz mindez a Stuxnet korábbi megjelenése óta, amikor beigazolódott, hogy akár egyetlen kártékony program is komoly veszélyforrást jelenthet az ilyen kulcsfontosságú rendszerekre nézve.

Egy lehetséges támadás



Forrás: ICS-CERT[13]

Tavaly többször lehetett hallani olyan biztonsági hírekről, amelyek ipari vezérlőrendszerek, illetve SCADA kapcsán feltárt sérülékenységekről számoltak be. Novemberben egyes SCADA rendszerek esetében sebezhetőségek derültek ki, melyek elsősorban adatlopásra adhatnak lehetőséget a támadók számára. Egy héttel később pedig 23 biztonsági rést sikerült kimutatni ipari vezérlésre alkalmas szoftverekben. A legérdekesebb, hogy ezeket a sérülékenységeket milyen könnyen fel lehetett tárni. Aki sok időt tölt vállalati és egyéni felhasználók számára fejlesztett szoftverek auditálásával, annak a SCADA rendkívül könnyű feladatnak számít.

Az ICS-CERT jelentésében összesen 171 ismert sebezhetőségről számoltak be. Ezek legnagyobb része puffertúlcsordulási hibákra volt visszavezethető. Emellett paraméterellenőrzési, XSS (Cross-site Scripting) és authentikációs rendellenességek is viszonylag nagyobb számban akadtak. Érdekes megemlíteni, hogy e kritikus infrastruktúrák esetében hét alkalommal került fény olyan (hard-coded) jelszavakra, amelyeket a fejlesztők "égettek" a kódokba.

Az ICS-CERT szerint azonban nem kizárólag a sérülékenységek számának növekedése okoz problémát. Komoly gond az is, hogy a fejlesztők nem egyszer nagyon lassan orvosolják a biztonsági hiányosságokat, ami pedig azt eredményezi, hogy hosszú ideig maradhatnak kiszolgáltatottak e rendszerek.

Ezért a szervezet bevezette, hogy a fejlesztők értesítését követő 45. napon közzéteszi a sebezhetőségek technikai részleteit, és ezzel próbálja arra sarkallni a gyártókat, hogy minél hamarabb dolgozzák ki a szükséges patch-eket.

Az internet felől is elérhető vezérlőrendszerek

Forrás: ICS-CERT[13]

Az ICS-CERT hangsúlyozta, hogy nem kizárólag fejlesztői oldalon vannak hiányosságok. Az üzemeltetőknek is sokkal nagyobb odafigyelést kellene fordítaniuk a kritikus infrastruktúrák védelmére. Egy vizsgálat során ugyanis kiderült, hogy legalább 20 ezer olyan ipari és szolgáltatói rendszer érhető el az internet felől, amelyek ezáltal fokozottan ki vannak téve a támadásoknak.

A biztonsági szervezet 63 további CERT-tel működik együtt annak érdekében, hogy az internet felől is elérhető kritikus infrastruktúrák és ipari rendszerek számát csökkenteni lehessen, illetve mód nyíljon az üzemeltetők tájékoztatására.

E-egészségügy

Forrás már van, a technológia és a piaci szereplők ugrásra készen várják, hogy modernizálódjon az egészségügy. Hiányzik azonban az egységes és átfogó stratégia.

Mobiltechnológia, analitika és üzleti intelligencia, számítógép, szerver- és adattároló-virtualizáció, számítási felhő, illetve az IT-menedzsment eszközei lesznek az egészségügyi szolgáltatók legfontosabb technológiai prioritásai világszerte az elkövetkező években – jósolja a Gartner. Az okos eszközök elterjedésével az eHealth-, valamint az egészségügyi informatika mobil ágazata, az mHealth-megoldások értékes terápiát adhatnak a meglehetősen súlyos állapotban levő magyar egészségügynek.

Az mHealth robbanásának előjele lehet, hogy más országokban, például az Egyesült Államokban, az Obama-kormányzat egy sor intézkedés segítségével ösztönzi az egészségügyet, hogy vegye igénybe az informatikát, a mobiltechnológiát és a korszerű eszközöket. Angliában pedig a patikák és a műszergyártók egyedi megoldásokat és szolgáltatásokat kínálnak – és értékesítenek is.

A tématerületen dolgozó szakemberek tapasztalatai szerint a magyar egészségügy elavult, korszerűtlen, részrehajló, alacsony hatékonyságú és veszteséges. Ugyanannyit költünk az egészségügyre, mint a nálunk jóval gazdagabb országok, Japán, Dánia vagy Nagy-Britannia. Mégis úgy tűnik, hogy az egészségügy hazai trendjei nem az anyagi ráfordítások mértéke, hanem ezek intelligens felhasználásának hiánya miatt alakulnak kedvezőtlen irányba. Az eHealth hazai programjainak fejlesztése évek óta folyik, ezeken belül az mHealth-megoldások nemrég kerültek előtérbe. Kormányzati tájékoztatásra lenne szükség, hogy milyen mHealth-projekteket szeretne az állam megvalósítani, és igény lenne a központosított fejlesztésre és összefogásra.

Optimizmusra ad okot, hogy a közelmúltban jelentette be az Emberi Erőforrások Minisztériuma: a kormány 12 milliárd forintnyi összeget fordít a következő hónapokban az egészségügyi ágazat informatikai fejlesztéseire. Az elsősorban uniós forrásokból több mint 17 projekt valósulhat meg, köztük számos eHealth-megoldás, például a különböző rendszerekben és intézményeknél található egészségügyi adatok adatbázisainak összekapcsolása, amit közel 20 éve nem sikerült megoldani. Milliárdos nagyságrendű összeget fordítanak többek között az országos egészségmonitorozási és kapacitástérkép adatbázis- és alkalmazásfejlesztésre („Katéter” és „Mónika” projektek), a Nemzeti Egészségügyi Informatikai Rendszer bevezetését támogató módszertani és humánerőforrás fejlesztésre, a kora gyermekkori programmal kapcsolatos feladatokra és az egészségügyi szolgáltatók akkreditációs rendszerének megvalósítására is. Infrastruktúra-fejlesztésre mintegy 3,63 milliárd forint áll majd rendelkezésre.

Az ellátórendszer szereplői mellett az egészségügyi informatika területén tevékenykedő IT-cégek is régóta várnak erre a lehetőségre, mivel a magyar egészségügy minden szinten átfogó reformot igényel és ennek a reformnak a leghatékonyabb eszköze lehet az eHealth, illetve rajta keresztül az mHealth megszilárdítása.

A projektek prioritásai közé tartoznak többek között:

- d2d (doctor-to-doctor): orvosok közötti elektronikus kapcsolat, amely egy konkrét beteg gyógyításával vagy valamilyen terápiával összefüggő elektronikus információcserét feltételez.
- p2a (patient-to-administration): az állampolgár (nem csak a betegek) és az állam (illetve az állami egészségügyet működtető közintézmények, hivatalok) közötti kommunikációs csatornák összessége.
- h2a (hospital-to-adminstration): azaz az egészségügyi szolgáltatók és az állami egészségügyi adminisztráció, közfinanszírozó közötti relációk.

Magyarországon létjogosultságuk van a fejlesztéseknek és az új rendszereknek, a korábbi vezetékes iparhoz képest a mobiltechnológia sokkal több lehetőséget kínál, segíti a kritikus helyzetek megoldását is. Például nem ritka eset, hogy a leletek több száz kilométert utaznak a konzíliumra, ilyenkor a technológia (például videó-telefon) használata gyorsítaná a diagnosztizálási folyamatot. Az egészségügy modernizálásához jól hasznosíthatók a tablet-ek és okostelefonok is, amelyek egyre nagyobb számban terjednek el az egészségügyi ellátásban – valójában minden területen jól lehetne használni őket.

Szerencsére több hazai példa is akad, ahol sikerült új fejlesztéseket megvalósítani. A magángyógyszerészek nagyon komoly lehetőséget látnak az mHealth-ben. Gyógyszerész gondozási program keretében üzleti alapokra helyezték a telemedicinát, amely 50 patikában már elérhető, s nemsokára call center szolgáltatást is mögé tesznek. A mobiltechnológia biztosítja, hogy újabb szolgáltatásokat lehessen beépíteni. Ebben a modernizációs folyamatban a távközlési és mobilszolgáltatók szerepe is jelentős.

Európai és hazai viszonylatban csupán 5 évvel ezelőtt kezdtek el a telemedicina területtel foglalkozni a távközlési cégek. Ennek eredményeképpen a Telenor-nál többek között köztes egészségügyi réteg kialakításán dolgoznak.

Ezen a rétegen végzik a beérkező adatok feldolgozását. Egyebek mellett a háziorvosi szinttől fölfelé terjedő egészségügyi ellátólánc protokolljai is fejlesztés alatt állnak.

Kiváló teszterepnek bizonyult Szabolcs-Szatmár-Bereg megye, ahol az idősebb betegeket szerelték fel mHealth-megoldásokkal – annyira kedvező volt a modern technológia fogadtatása, hogy a tesztidő lejárta után nehéz volt visszaszerezni az eszközöket az idős emberektől.

Látható, hogy bizonyos részterületeken már kimutatható a siker, viszont akkor működik normálisan és zavarmentesen az e-Egészségügy egy országban, ha több szegmens szereplője kapcsolódik be, ha egyre több megoldás születik az egyenletes fejlődés érdekében. Ezeket piac hiányában az államnak kell megteremtenie, vagy a piaci sajátosságok miatt szabályoznia kell.

Az egyik legfontosabb az elektronikus (digitális) aláírás kérdésköre, ami az egészségügyben a személyes adatok védelme érdekében valamennyi szereplő közös érdeke. Központi megoldás nélkül azonban nehezen elképzelhető a továbblépés. Ennek hiányában nem nagyon van értelme az elektronikus taj-kártya-, e-recept, e-lelet- és más hasonló projekteknek sem, mert a felhasználhatóság szempontjából inkább párhuzamosságot okoz, semmint az ügyintézést gyorsítaná, élőmunkát váltana ki vagy papírt takarítana meg.

Ezért lenne fontos, hogy műszakilag egyértelmű, időtávlatában megfelelően szakaszolt, logikus sorrendbe egymásra épülő e-egészségügyi stratégiát fogadna el az ágazat, amelyben megfelelő egyensúlyban szerepelne a műszaki megvalósíthatóság, a pénzügyi finanszírozhatóság, az orvosszakmai relevancia és az egészségpolitikai koncepció támogatása. Ehhez ma Magyarországon a feltételek adottak, de a megvalósításhoz új gondolkodásmód szükséges.

Amíg nincs egységes, átfogó eHealth-stratégia, addig hiába beszélünk a mobiltechnológia lehetőségeiről.

Hiába kezelhető a BYOD trend biztonsági kérdése Android, iOS platformon elérhető ingyenes biztonsági alkalmazásokkal, ha a szigetszerű fejlesztéseket, projekteket nem kapcsolják össze. Segítené a fejlődést az is, ha az orvosok nagyobb számban állnának az eHealth- és az mHealth-megoldások mellé.

Pedig az egészségügyet azért is érdemes mobilizálni, mivel hatékonyabb és nem mellesleg kiváló költségcsökkentő megoldás. Segítségével kiváltható bizonyos ellátási folyamatok helyhez kötöttsége (például a fekvőbeteg-ellátásban). A mobil technológia előrefutott és a lehetőség mindenki számára rendelkezésre áll, továbbá már kezdenek megjelenni az egészségügy-specifikus mobileszközök is a piacon.

A távközlési cégek az mHealth bonyolultabb részfeladatait kapták meg, mégpedig az azonosítást, amelynek a banki rendszerekhez hasonló biztonsági követelményeknek kell eleget tennie. Az egészségügyi ellátórendszer része a biztonság, amelynek a kórház épületén belül és a falakon kívül is ugyanazt a szintet kell biztosítania. Ezenkívül a nagy mennyiségű adatok tárolása miatt keresnek minket. A kérésekre olyan hibrid megoldáshalmazzal válaszoltunk, hogy csak bizonyos adatok jelennek meg az eszközökön és egy böngészőhöz hasonló módszerrel szekvenciálisan kell lekérni az adatokat.

Technológiailag a távközlési cégek felkészültek az igényekre, viszont a kórházi kiszolgáló rendszereket még nem alakították át. A modernizáció ott is elakad, hogy az egészségügyben használt telefonok több mint 90%-a még olcsó, hagyományos készülék, s csupán 3-4%-uk okos eszköz. Emiatt az az új technológiákra fogékony orvosok a saját „smart” készüléküket használják (ez a BYOD trend), ami felveti a biztonsági autentikáció kérdését. Az intézményvezetők pedig nehezen döntenek a költséges beruházások mellett.

Kevés szó esik a felhő alapú egészségügyi rendszerekről. A szakértők szerint leginkább azokban a fejlődő országokban terjedhetnek majd el, ahol a gyors és hatékony ellátást rövid időn belül akarják kiépíteni.

Nagy számosságú lakossági célcsoport határozható meg Magyarországon: a 33–38 éves kismamák – akik kimondottan a telemedicinára és az mHealth-re fókuszálnak –, valamint a 40–45 éves menedzser férfiak, akik valamilyen egészségügyi problémával küzdenek, nincsenek pénzügyileg korlátozva és időhiány miatt a leggyorsabb egészségügyi megoldásokat keresik. E két korcsoportot tekintik az mHealth innovátorainak, emiatt az ipar kiemelten fókuszál rájuk. A harmadik szegmens a krónikus betegségben szenvedő idős emberek, akik a modern eszközök segítségével interakcióba tudnak kerülni orvosukkal. Az mHealth leghatékonyabban az idősebb generáció problémáját tudja megoldani.

Magyarország azon kevés országok egyike, ahol sok szereplő tevékenykedik az egészségügyi informatika területén. Ezek a piaci szereplők nagyon is komolyan veszik az üzleti lehetőségeket az mHealth-megoldásokban.

Magyarország az informatikában és a mérnöki képzésben is erős. Komoly múltat tudhatunk magunk mögött a gyártásban és az összeszerelésben, az elmúlt 30 évben fontos, tapasztalt cégek jöttek létre. Számos mHealth-minialkalmazás jött létre, amelyek hatékonyan működnek. Az orvostársadalom is nyitottabb, ha szakértőként és tanácsadóként vehet részt a projektekben – ahogy a világ más országaiban. Tehát a kompetenciák rendelkezésre állnak. Ahhoz, hogy a megvalósítás is teljesüljön, az mHealth és eHealth fejlesztésében a különböző tudományoknak együtt kell dolgozniuk: a jognak, az orvostudománynak, a műszertechnológiának, az informatikának. Fontos, hogy összhangban legyenek. Külföldtől megtanulhatjuk, hogyan kell kooperálni egymással.

A Washington Post tanulmánya[14] szerint az eddigi „sláger-területek” mellé az egészségügyi rendszerek is felkerülnek a hacker-ek céltáblájára.

Az elmúlt években felgyorsult a különféle egészségügyi rendszerek átállása online környezetekre, ami persze egyrészt jó dolog. Könnyebb és helyfüggetlenebb lehetőségek állnak a páciensek és orvosok rendelkezésére például a kommunikáció, saját adataik karbantartása, az intézmények közötti adatáramlás terén. Viszont, mint köztudott, ahogy valami az internetre kerül és bármilyen kicsi értéket is képvisel, azonnal megtámadják.

Az orvosi adatok igenis sokféleképpen jelenthetnek pénzt rosszindulatú támadók számára is. A legegyszerűbb felhasználási mód, ha az idáig csupán véletlenszerű témákat (főként potencianövelőket) használó levélszemét-küldőknek az orvosi rendszerekbe bejutó hackerek sokkal célzottabb elérést nyújtó adatbázisokat tudnak majd eladni. Ha valakiről olyan adat szerepel egy feltörhető adatbankban, mely szerint erős asztmája van, könnyen olyan levelek áraszthatják el, amelyekben saját betegségére kínálnak olcsóbbnak vagy épp hatékonyabbnak kikiáltott (ám közel sem hivatalos forrásból származó) gyógyszereket.

Ez még ráadásul csak a legkevésbé ártó felhasználási mód: egyes egészségügyi rendszerek feltörése után akár visszaélhetnek társadalombiztosítási adatainkkal is, és még sok egyéb formában keseríthetik meg betegek vagy épp orvosok életét.

A legnagyobb veszélyforrásnak épp a rendszerek újdonsága számít. Míg például a banki webes megoldások esetén évek teltek el az első próbálkozások óta, így volt idő kitapasztalni a sérülékenységeket és védekezni ellenük, az egészségügyi megoldások biztonsága nagyon sok kívánnivalót hagy maga után.

Az Egyesült Államok nemzetvédelmi hivatala szintén idén ívta fel a figyelmet arra, hogy a webbel „érintkező” rendszerek közül az egészségügyi megoldások számítanak biztonsági szempontból a leginkább kiforratlannak. Sokszor ráadásul a felhasználók is hozzájárulnak a sérülékenység növeléséhez, hiszen az orvosok és egészségügyi dolgozók gyakran nem rendelkeznek megfelelő informatikai tapasztalatokkal. Épp ezért nem kevés példa akad már emailben továbbított bizalmas adatokra, könnyen elérhető online archívumokban tárolt ügyfél-adatbázisra és egyebekre.

14 O’Harrow Jr., Robert: Health-care sector vulnerable to hackers, researchers say; The Washington Post; 2012.12.25.

Jó példa lehet a Chicago-i Egyetem orvosi központjának esete: itt az orvosok egy iPad-en használható alkalmazást használatnak a páciensek kezelésekor, amely a betegek adatait egy teljesen hagyományos Dropbox fiókból nyeri, amely csupán egy felhasználónevet és jelszót kér. Az orvosoknak a kórház minden esetben biztosított egy .pdf fájlt a tablet-eken, amelyekben mindenféle titkosítás nélkül le volt írva a belépéshez szükséges információ, így ellopott, elveszett iPad-ekről azonnal a teljes adatbázishoz hozzá lehetett férni.

Az ehhez hasonló esetekben elég az odafigyelés, a más területeken szerzett biztonsági tapasztalatok átvétele. Emellett azonban a saját tervezésű rendszerek, újfajta egészségügyi megoldások üzembe helyezésekor is nagy figyelmet kell fordítani a lehetséges biztonsági rések eltorlaszolására, valamint a felhasználók képzésére.

Várakozások 2013-ra

Már az előző fejezetben is számos helyen megjelennek az egyes szektorok, IT-biztonsági területek 2013-ra, esetenként még távolabbra mutató előrejelzései, várakozásai.

Ebben a fejezetben ezek leglényegesebb, közös pontjai kerülnek összefoglalásra, vagyis, hogy melyek a legfontosabb, legkritikusabb területei a közeljövő IT-biztonságának.

Az előrejelzések a legfontosabb IT-biztonsággal foglalkozó kutató cégek felméréseiből táplálkoznak, például a F-secure[15], Gdata[16], Symantec[17], Kaspersky[18], IDC[6], Gartner[6], Sophos [19] elemzései kerültek felhasználásra.

Felhő

A Gartner előrejelzése szerint 2015-re a globális vállalati IT-biztonság 15%-a a felhőből fog futni, a kulcsterületek egyértelműen a ma is kurrensnek számító azonnali üzenetküldés, web-biztonság és a távolról való sérülékenységi vizsgálatok lesznek. Ugyanakkor a várakozások szerint a felhő alapú biztonsági technológiák várhatóan nyitni fognak az adat szivárgás megelőzése, titkosítás és hitelesítés irányába is, hiszen ezen területek biztonsága meglehetősen erőforrás intenzív, amelyet a felhő alapú infrastruktúrák sokkal hatékonyabban tudnak majd biztosítani.

A felhő alapú biztonsági fejlesztések felgyorsulása várhatóan néhány hagyományos biztonsági terület üzleti visszaesését fogja jelenteni, amelyet jelenleg a nagy viszonteladók biztosítanak partnereik számára, de a trendek alapján sokkal komplexebb, szervezettebb biztonsági rendszerek kialakulása várható.

Az előrejelzések szerint a hagyományos tűzfal/VPN piac 20%-a már virtualizált környezetben, felhőszolgáltatóktól fog üzemelni 2015-re.

Természetesen a hagyományos biztonsági vállalkozások sem nézik tétlenül piacaik szűkülését, hatalmas felvásárlási hullám indult meg a felhő alapú biztonsággal foglalkozó startup cégek körében, amely az új ötletek és technológiák tőkeerősebb piaci szereplőnél való koncentrációját vetíti előre.

15 F-Secure: Mobile Threat Report 2012Q3; 2012.09.30.
16 GData: IT security trends in 2013: cyber war not on the horizon; 2012.12.17.
17 Haley, Kevin: Top 5 Security Predictions for 2013 from Symantec; 2012.11.08.
18 Kaspersky Lab: Perception and knowledge of IT threats: the consumer's point of view; 2012.08.29.
19 Sophos: Sophos Unveils Thirteen IT Security Trends For 2013; 2012.12.27.

BYOD – BYOA

Aki hatékonyabb és gyorsabb tud lenni konkurenseinél, az győztesen kerülhet ki a válságból – ezt az ügyviteli szoftvereket fejlesztő vállalatok is érzik. Mint ahogyan azt is, hogy a mobiltelefonok és táblagépek egyre inkább helyet szorítanak maguknak a vállalati környezetben.

A cég számára előny, hogy így jelentős anyagi befektetést kerülhet el azzal, hogy az alkalmazottaknak nem kell megvásárolni a munkavégzésükhöz szükséges berendezések egy részét, azonban a vállalati levelezéshez, adatbázisokhoz és belső hálózatokhoz való hozzáférés ilyen bizonytalan forrásokból adatvédelmi és biztonsági szempontból több mint aggályos.

A jelenség a legtöbb vállalatvezetőt kétségekkel tölti el, a legfrissebb kutatások szerint azonban kénytelenek lesznek alkalmazkodni ehhez a jelenséghez – még a fenntartások ellenére is. Ma már számos megoldás áll a vállalatok rendelkezésére, amelyek segítségével ezek a biztonsági kockázatok jelentősen csökkenthetők vagy akár meg is szüntethetők, így a BYOD rohamos elterjedésére számíthatunk a közeljövőben.

A munkavállaló szempontjából mindenképpen előnyös, hogy egy általa választott és kedvelt technológiai és hardverkörnyezetben dolgozhat, sőt ehhez gyakran a BYOA (Bring Your Own App – hozd a saját alkalmazásodat) szemlélet is társul, ami lehetővé teszi hogy olyan alkalmazásokat futtasson, amelyek a munkavégzést hatékonyan segítik, de a vállalati szoftverparknak egyébként nem képzik részét. Az alkalmazottnak viszont kényelmetlenséget okozhat, hogy a hivatalos adatok védelme a privát tartalmak elérését is megnehezíti, valamint az is előfordulhat, hogy saját számítógépe fölött elveszti a teljes körű irányítást.

A technikai háttér megteremtésén túl mindenekelőtt azt követeli meg a BYOD, hogy a saját eszközök használatát engedélyező vállalat pontos, végrehajtható – és az IT-startégiához szervesen illeszkedő – BYOD-stratégiát dolgozzon ki, mert csak így tudja egyensúlyban tartani a kockázatokat és a várható üzleti előnyöket.

Egy BYOD stratégiába az alábbi elemeket célszerű belevenni:

- pontosan definiált hozzáférési szabályok mind a dolgozókra, mind az eszközeikre vonatkozóan;
- pontos előírások az IT-biztonságra és a vállalati adatok kezelésére vonatkozóan;
- titkosítási és adattárolási előírások;
- a mobil eszközök használatának szabályozása üzleti utak, illetve bármilyen, vállalaton kívüli helyszín alkalmával, különös tekintettel a külföldi utazásokra;
- általános szoftverhasználati szabályok;
- lincence-jogi előírások;
- a beszerzési támogatás szabályozása.

Kémkedés és terrorizmus

2013-ban és a következő években az országok, szervezetek és az egyéni felhasználók konfliktusai várhatóan központi szerepet kapnak majd a kibertérben. Az online kémkedés nagyon hatékony eszköze lehet az illegális információszerzésnek, hiszen gyakran felderítetlen marad, és könnyen letagadható. Az elmúlt két évben több ország is az online kémkedés áldozatául esett, mert nem voltak megfelelően felkészülve a fenyegetésre. Ez a trend várhatóan idén is meghatározó lesz, és az egymással szemben álló nemzetek, vagy hacker-ek szervezett csoportjai továbbra is az információtechnológiát használják majd célpontjaik érzékeny adatainak eltulajdonítására, vagy teljes számítógépes rendszerek elpusztítására.

A Symantec előrejelzése szerint egyre több egyéni felhasználót és nem kormányzati szervezetet is érhetnek támadások a jövőben. Ilyen célpontok lehetnek például azok a szervezetek és egyének, akik nyíltan kiállnak valamely politikai ügy, vagy kisebbségi csoport mellett. Ma ilyen támadásokat akkor tapasztalhatunk hacktivista csoportok részéről, amikor egy egyén vagy vállalat konfliktusba kerül velük.

Online zsarolás

Miközben a bűnözői csoportok érezhetően egyre kevesebb fantáziát látnak a hamis vírusölő programok terjesztésében, az illegális pénzszerzés érdekében közülük többen egy új, a korábbinál lényegesen durvább módszerhez folyamodnak. Ennek eszköze az úgynevezett ransomware, vagyis az online zsarolás, aminek során a bűnözők valamilyen fenyegetéssel próbálnak pénzt, „váltságdíjat" kicsikarni a felhasználóból, miután előzőleg használhatatlanná vagy elérhetetlenné tették az adatait.

A ransomware túllép az áldozatok megtévesztésén: megfélemlíti és zaklatja őket. Míg ezzel az "üzleti modellel" már korábban is próbálkoztak néhányan, a módszer eddig nem tudott elterjedni, mert a kiberbűnözők nem találtak hatékony módszert az áldozatoktól kizsarolt pénz begyűjtésére. Időközben azonban a bűnözők rájöttek, hogy az online fizetési csatornákat erre a célra is használni tudják, így a korábbi üres fenyegetőzéssel szemben ma a zsarolókat is komolyabban kell venni. Súlyosbítja a helyzetet, hogy mivel nem szükséges többé cselhez folyamodniuk azért, hogy célpontjaiktól kicsalják a pénzüket, várhatóan a zsarolási módszereik is egyre aljasabbak lesznek.

A Symantec várakozásai szerint 2013-ban a támadók még professzionálisabb módszereket (például az eredetihez megszólalásig hasonlító weboldalakat) használnak majd az információszerzésre és zsarolásra, egyre terjednek az áldozatok érzelmeire ható fenyegetések, miközben a bűnözők egyre inkább megnehezítik majd az értékes személyes adatok visszaállítását.

Mobil kártevők

A tablet-ek és okostelefonok terjedésük és sikerességük, valamint kiforratlan biztonsági protokolljaik okán továbbra is a támadók fontos célpontjai maradnak főként adatlopási célzattal. A windows phone növekvő piaci részesedése várhatóan erre a platformra is ráirányítja a támadók figyelmét, valamint az iOS zártsága ellenére a támadók nem tesznek le arról, hogy az Apple eszközeire is beférkőzzenek.

A rosszindulatú mobilhirdetések, más néven madware-ek nem csak a felhasználói élményt zavarják, de felfedhetik a kiberbűnözők előtt a felhasználó tartózkodási helyét, elérhetőségeit, vagy az általa használt eszköz azonosítására alkalmas információkat. A madware - mely alkalmazások letöltésekor kerül a felhasználók eszközeire – gyakran felugró figyelmeztetéseket küld, váratlanul ikonokat ad hozzá a nyitóoldalhoz, megváltoztatja a böngésző-beállításokat, miközben személyes adatokat gyűjt.

A legagresszívebb madware-eket tartalmazó alkalmazások száma 210%-kal növekedett az elmúlt kilenc hónapban. A tartózkodási helyre és az adott eszközre vonatkozó információkat a hirdetési hálózatok törvényesen használhatják, mert ennek köszönhetően személyre szóló hirdetéseket tudnak szolgáltatni. Mivel a jövőben várhatóan egyre több vállalat fog mobilhirdetéseket alkalmazni bevételei növelése érdekében, ezzel a növekedéssel párhuzamosan a madware-ek további terjedésére is számít a Symantec.

A kiberbűnözők jellemzően mindenhol jelen vannak, ahol a felhasználók is, így a mobil eszközökön, illetve a felhőben tárolt adatok várhatóan 2013-ban is a támadások kiemelt célpontjai lesznek. Tovább növeli a kockázatokat, hogy az alkalmazottak a vállalati hálózatokat védelem nélküli mobileszközökön keresztül használják, és olyan adatokkal dolgoznak, melyeket aztán más felhőkben is tárolnak.

Várhatóan nő idén a mobileszközökön található adatok megszerzésére irányuló támadások veszélye, ezzel párhuzamosan a malware-ek is elszaporodhatnak a felhasználók eszközein, amennyiben szabadon tölthetnek le alkalmazásokat a telefonjukra.

Egyes malware-ek a támadások korábbi, ismert módjait alkalmazzák, például az eszközökről történő adatlopást. A malware-ek más fajtái ugyanakkor emelt díjas SMS-eket is képesek küldeni az áldozat mobiljáról, amiből természetesen bűnözők profitálnak. A mobileszközök egyre komolyabb értéket képviselnek, mivel a mobilszolgáltatók és a kereskedelem egyre nagyobb arányban vált a mobilfizetésre, és folyamatosan bővül az így igénybe vehető szolgáltatások sora is. A Symantec várakozásai szerint emiatt a bűnözők is egyre gyakrabban alkalmaznak majd malware-t a fizetési információk eltérítésére és megszerzésére mindenhol, ahol a mobileszközöket fizetésre használják a tulajdonosaik. Megkönnyíti a bűnözők dolgát, hogy sok felhasználó egyelőre nem ismeri elég jól az egyes fizetési rendszereket, nincs elegendő tapasztalatuk ilyen technológiákkal.

Közösségi oldalak

A fogyasztók általában megbíznak a közösségi oldalakban és sokszor gondolkodás nélkül megosztják a nyilvánossággal személyes adataikat, játékkrediteket, ajándékokat vesznek maguknak, vagy barátaiknak. Az ajándékvásárlás és -küldés lehetőségének megteremtésével a közösségi oldalakat üzemeltető vállalkozások komoly bevételekhez jutnak, ami a kiberbűnözők érdeklődését is felkeltette. A Symantec szakértői szerint idén nőni fog az olyan rosszindulatú támadások száma, melyek az ismert közösségi oldalak hamisított, megtévesztésre alkalmas verzióin keresztül próbálják megszerezni a felhasználók fizetési adatait, illetve egyéb értékes, személyes információkat. A csali lehet egy ajándékról érkező hamis értesítés vagy email, amelyben postacímet, vagy más személyes információt kérnek a felhasználóktól, amennyiben hozzá szeretnének jutni az ajándékhoz.

A Mac támadása

A Macintosh platform az eddigiekben zártsága és relatíve kis felhasználói létszáma miatt elkerülte a támadók figyelmét, ám ez a helyzet az Apple termékek népszerűsödésével várhatóan változni fog. Az előrejelzések szerint a Mac kártevői is túl vannak a tesztelési fázison és bevetésre készen állnak az új évben.

Okos TV-k

Az okos TV technológiával a nappalikba költöznek a mikrofonnal, és webkamerával ellátott számítógépek, amelyek biztonságára sem a gyártók, sem a felhasználók nem ügyelnek. Ezek az eszközök is a támadók célpontjaivá válhatnak. A támadások fő csapásiránya egyrészt a kéretlen üzenetek reklámok közvetítése lehet, de ami sokkal fontosabb, hogy a kamera és a mikrofon feletti irányítás megszerzésével kémkedésre kiválóan alkalmas platform jön létre. Ezt a támadók módosított firmware-ek interneten keresztüli feltöltésével tudják elérni.

Sérülékenységek

A támadók egyre gyorsabban és hatékonyabban használják ki az egyes szoftvertermékek, komponensek, böngészők sérülékenységeit. a sérülékenységek kihasználására alkalmas készleteket már az interneten keresztül is értékesítik, így kihasználásukban az informatikailag kevésbé képzett támadók is hatékonyan részt tudnak venni. Leginkább a régi Java verziók és a már ismert biztonsági rések engednek szabad teret az ilyen, „instant” támadásoknak, a friss sérülékenységeket pedig gyorsan integrálják a készletekbe, folyamatosan napra készen tartva azokat.

Biztonság tudatosság

A Symantec várakozásai alapján 2013-ban továbbra is az online csatornákon kell majd a leginkább ébernek lennie a felhasználóknak. A technológiákhoz és az internethez való hozzáférés korábban érintetlen piacokon is megfizethetőbbé vált, így minden vállalati online stratégiának része kell, hogy legyen a fogyasztók IT-biztonságra való nevelése. A kiberbűnözők gyorsabban alkalmazkodnak a változó technológiákhoz, mint ahogy velük a vállalatok és egyéb szervezetek lépést tudnak tartani. Éppen ezért fontos, hogy a sikeres üzleti működés és a vállalat jó hírnevének megőrzése érdekében a cégek a megfelelő információbiztonsági alapokkal és irányelvekkel rendelkezzenek. Ez a feltétele annak, hogy a vállalatok képesek legyenek megvédeni a rájuk bízott értékes felhasználói adatokat.

2012. dióhéjban

A 2012-es év sem volt híján olyan incidenseknek, amelyek hazai és nemzetközi szinten is „nagy port kavartak”. Jelen összeállítás (a CERT-Hungary Tech-Blog cikkei alapján) több témakörre bontva eleveníti fel 2012. „legemlékezetesebb” informatikai eseményeit, amelyek több esetben is kapcsolatban állnak Magyarországgal, így a magyar felhasználókkal.

Január

Adatvédelem, adatlopás

- Több Internetes oldalon is elterjedt az a hír, hogy face.book.hu és a facebook.hu weboldalak megnyitásakor káros kód kerül a felhasználók számítógépére. Szerencsére ez nem történt meg, mindazonáltal felmerült annak a lehetősége, hogy azoknak a felhasználóneve és jelszava, akik a fenti két domain-en keresztül használták a Facebook-ot, illetéktelen kezekbe került, mivel a két oldal nem a Facebook tulajdonában van, hanem "közvetítőként" volt szerepe a forgalomban, így a begépelt adatok egy harmadik fél rendszerén haladtak át. Arról pontos adatok nincsenek, hogy hány felhasználó adta meg hozzáférési adatait a weboldalon keresztül. Az viszont mindenképp elmondható, hogy a felhasználók nem kellő elővigyázatossággal jártak el.

Kibertámadások

- Már rögtön január első napjaiban közzé tette az Internet Storm Center (ISC) azon jelentését, mely szerint a Lilupophilupop SQL befecskendezéses támadás sorozat elérte az 1 millió áldozatot. Egy hónap alatt ennyi weboldal esett áldozatul a támadásnak, amely automatikusan és gyorsan változik, ezért nehéz ellene védekezni.
- Indiai hacker-ek szerezték meg a Notron Antivírus forráskódját. A világ első, kizárólag Interneten megtalálható boltja a Zappos januárban alaphelyzetbe állította mind a 24 millió felhasználó jelszavát, miután egy támadónak sikerült megszereznie az ügyfelek email címét és nevét.

- Az Anonymous hacker csoport is folyamatosan a média középpontjába volt. Így már januárban a US-CERT-nek több különböző forrás is megerősítette, hogy a hackercsoport egy összehangolt elosztott szolgáltatás megtagadásos támadásra készül amerikai kormányzati ügynökségek és a szórakoztatóiparban érdekelt cégek weboldalai ellen. A támadások célja a MegaUpload fájlmegosztó lekapcsolása és az online kalózkodás visszaszorítására törekvő törvénytervezetek, a SOPA (Stop Online Piracy Act) és a PIPA (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act) elleni tiltakozás. Az AFP hírügynökség jelentése szerint január végén a litván nemzeti bank rendszerét érte kibertámadás, de a hackereknek nem sikerült legyűrniük a bank rendszerét.

Február

Adatvédelem, adatlopás

- Tovább gyűrűzött a Wikileaks ügy egy újabb meglepő ténnyel, mely szerint a Wikileaks portál olyan, a Stratfor-tól ellopott email-eket hozott nyilvánosságra, amelyek bizonyítják, hogy amerikai ügyészek a "privát titkosszolgálat" segítségével próbáltak meg vádat emelni Julian Assange, a Wikileaks alapítója ellen.

Malware

- Az FBI 2011 novemberében az ”Operation Ghost Click” fedőnevű akcióban lecsapott azokra a bűnözőkre, akik a DNSChanger nevű trójait készítették. A közel 100 országban mintegy 4 millió fertőzésért felelős trójai onnan kapta a nevét, hogy megváltoztatta az áldozatuk számítógépén a DNS szerverek címét, így tetszőlegesen át tudták irányítani a kereséseket. Az FBI mindezek ellenére egészen 2012. július 9-ig üzemeltette a szervereket, hogy az áldozatoknak legyen idejük megtisztítani a számítógépüket a fertőzéstől.
- Februárban a biztonsági szakértők a Zeus/Spyeye banki trójai új variánsára hívták fel a figyelmet, amely a szokásos C&C szerverek helyett P2P architektúrát használ a botnet vezérlésére, amely sokkal ellenállóbbá teszi azt a lekapcsolás ellen. Ezenkívül a készítők UDP protokollra váltottak a TCP helyett, amely nehezíti a forgalom nyomon követését.
- Johnathan Norman, az Alert Logic biztonsági cég vezetője februárban a Pastbin-en hozta nyilvánosságra azt az exploit kódot, amely segítségével össze lehet omlasztani a távoli hozzáférést lehetővé tevő pcAnywhere szolgáltatást.

Kibertámadások

- Az Adobe Reader egy korábban javított sérülékenységét kihasználó PDF dokumentumokkal követtek el támadást kínai hacker-ek számos nyugati cég, többek között nagy amerikai védelmi beszállítók ellen.
- A VeriSign tanúsítvány kibocsátót februárban számos támadás érte, amely kétségeket ébresztett az általuk kiadott tanúsítványok hitelességével kapcsolatban, mert a hírek szerint az adminisztrátorok sikeresen elhárítottak egy támadást, amely a rendszereik ellen irányult, de a legfelső vezetés csak később értesült a dologról.
- Február 13-án, péntek éjszaka, vélhetően egy elosztott szolgáltatás megtagadásos (DDoS) támadás eredményeképpen órákra elérhetetlenné vált a CIA weboldala. Az első értesülések szerint a támadást az Anonymous csoport követte el és ezt látszott megerősíteni egy Anonymous-hoz kapcsolható Twitter hozzáférésen megjelent "CIA Tango Down" üzenet is. Még ebben a hónapban az Anonymous hackercsoporthoz tartozó támadók elosztott szolgáltatás megtagadásos támadást (DDoS) indítottak a NASDAQ hivatalos oldala ellen is, amely a támadás hatására ideiglenesen elérhetetlenné vált.

- A hónapban Magyarországot érintő hírt közölt a média, ami arról szólt, hogy egy magyar hacker 30 hónap letöltendő börtönbüntetést kapott egy maryland-i bíróságon. A 26 éves Németh Attila bűne az volt, hogy betört Marriott International hotelhálózat rendszerébe és azzal zsarolta a céget, hogy nyilvánosságra hozza az adatokat, ha a hotel nem ad neki 150 ezer dolláros fizetéssel munkát Európában, ingyenes repülőjegyet és szobát bárhova is megy.
- Február közepén ismét az Anonymous került középpontba, akik március 31-ére azt ígérték, hogy romba döntik az egész Internetet azzal, hogy a root DNS szervereket fogják támadni. Az akció oka a Wall Street mohósága és az Internetet korlátozni akaró törvénytervezetek.

Március

Adatvédelem, adatlopás

- A NASA bemutatta azon jelentését, amelyben 13 olyan betörés elemzése volt található, amelyek 2011 során irányultak a NASA rendszerek ellen. Ezek közül az egyik támadás kiinduló pontja Kína volt, amely bizonyos kritikus rendszerek irányításának teljes átvételével végződött, továbbá a támadás során a Jet Propulsion (Sugárhajtás) Laboratory alkalmazottainak felhasználói adatbázisát is sikerült megszereznie a támadónak. Ez még nem minden, ugyanis egy olyan másik eset is történt, amikor olyan laptop tűnt el, amely a Nemzetközi Űrállomás (ISS) parancs és vezérlési kódjait tartalmazta.
- A hónapban a kínai hatóságok letartóztattak egy férfit, akit azzal gyanúsítanak, hogy betört a Kínai Szoftverfejlesztői Hálózatba (Chinese Software Developer Network - CSDN), és onnan 6 millió felhasználó adatait lopta el és hozta nyilvánosságra, amelyek közt felhasználónevek, jelszavak és email címek voltak.
- Az év során többször a média célkeresztjébe került az, hogy a munkáltatók a leendő munkavállaló Facebook profilját ellenőrzik, sőt esetlegesen még a hozzáférési adatokat is elkérik. Ezen okból a Facebook egy közleményt adott ki, amelyben nyilvánosan is elítéli azt az Egyesült Államokban egyre terjedő trendet, amikor egy munkáltató a felvételi elbeszélgetés során megkéri a jelöltet, hogy adja meg a közösségi oldalhoz tartozó belépési adatait, hogy a HR-es kollégák a felvételiző nem publikus információit és tevékenységeit is megtekinthessék. A munkáltatók azzal mentegetőznek, hogy a cég érdekeit védve nem akarnak olyan embert felvenni, aki rombolja a vállalatról kialakított képet. Az év folyamán több amerikai szövetségi államban is hoztak törvényt az ilyen típusú adatkérések tilalmáról.

Kibertámadás

- Egy orosz biztonsági szakértő olyan sérülékenységet fedezett fel a GitHub-on, amelyet kihasználva egy támadó korlátlan hozzáférést szerezhet egy felhasználó tárolójához. A sérülékenységet a Ruby on Rails egy hibája okozta.
- A márciusi patch kedden a Microsoft javította a Remote Desktop (távoli asztali kapcsolat) sérülékenységét, amelyet addigra már aktívan kihasználtak, miután nyilvánosságra került az ezt kihasználó exploit kód. A későbbi vizsgálatok kiderítették, hogy a kód a biztonsági sérülékenységek javítását célzó Microsoft Active Protection Program (MAPP) révén szivárgott ki az egyik kínai partner cégtől, akit később kizártak a kezdeményezésből.
- A PayPal sem úszta meg incidens mentesen, ugyanis a weboldalán találtak egy sérülékenységet, amit kihasználva a támadónak lehetősége volt megszerezni a felhasználók adatait. Ezt követően a vállalat hamar kijavította a hibát.

- Talán a hónap „meglepetés” híre volt, hogy Ausztráliában kitiltották a kínai Huawei óriást az ország közbeszerzési eljárásaiból, mivel a kormány attól tart, hogy a kínai titkosszolgálatoknak hozzáférésük van a cég által gyártott rendszerekhez. Az év folyamán az Egyesült Államok is hasonló indokkal a Huawei mellett a ZTE-t is ugyanilyen módon büntette.

Április

Adatvédelem, adatlopás

- Április elején az atlantai székhelyű Global Payments rendszereit feltörő támadók 1,5 millió felhasználó bizalmas adatait szerezték meg.
- Az Egyesült Királyságban készült felmérés szerint a legnépszerűbb weboldalakon átlagosan 14 nyomkövető süti (tracking cookie) van, amelyeket a felhasználó az oldal megtekintése közben letölt. A felmérés azt is megállapította, hogy a sütik kétharmada nem az oldal készítőjétől, hanem harmadik féltől származik. A felmérés azért kapott nagy visszhangot, mert alig 1 hónappal az Európai Uniós Privacy Directive - az EU online személyiségi jogokkal foglalkozó irányelve - életbe lépése előtt került nyilvánosságra. Az irányelv kimondja, hogy engedélyt kell kérniük az oldalaknak, mielőtt követni kezdik a felhasználót.

Malware

- Az ukrán hatóságok leállították a VX Heavens fórumot, azzal az indokkal, hogy olyan információkat terjesztenek, amelyet bűnözők fel tudnak használni káros szoftverek készítésére, illetve sokan az oldal segítségével adták és vették ezeket a kódokat.
- Áprilisban jelentek meg az első hírek a Darkshell-ről, ami egy olyan botnet hálózat, amely elosztott szolgáltatás megtagadás támadásokat tud végrehajtani (DDoS). A célpontjai elsősorban kínai weboldalak. Az új variánsba nagyon sok olyan megoldást építettek be, amely megnehezíti a debug-olást, a kód elemzését.

Kibertámadások

- Április rögtön az előző hónap Anonymous eseményétől volt hangos, ugyanis annak ellenére, hogy az Anonymous bejelentette, mégsem állt le az Internet március 31-én, azaz elmaradt a világ minden pontjára meghirdetett DDoS támadás, amely a root DNS szervereket vette volna célba.
- A hónap közepén egy iráni biztonsági szakértő 3 millió iráni állampolgár bankszámla adatait hozta nyilvánosságra, miután egy komoly sérülékenységet fedezett fel az iráni bankrendszerben. Először az érintett bankok számára küldte el 1000 ügyfél adatait, hogy alátámassza az állításait, majd amikor erre nem reagáltak, minden megszerzett adatot feltett az Internetre.
- Támadás érte az iráni Olajipari Minisztérium számítógép hálózatát is, amelynek hatására az Iszlám Köztársaság megelőző jelleggel lekapcsolta a fő olajexport terminálját az internetről. A támadók sikeresen töröltek bizonyos adatokat, de a minisztérium rendelkezett adatmentéssel.
- A whitec0de.com blog jelentése szerint egy hacker fórum felhasználója azt hirdeti, hogy mindössze 20 dollárért bármilyen Hotmail fiókot percek alatt feltör, és ha lehet hinni a híreszteléseknek tartotta is a szavát.

Május

Adatvédelem, adatlopás

- A nagy gyártók is követnek el gyermeteg hibákat, mint például az Apple. Az OS X Lion rendszerben bekapcsolva maradt a FileVault debug opciója, amelynek következtében a felhasználók jelszava egyszerű szövegként tárolva jelent meg a napló állományokban. Magyarországon az Apple OS X aránya nem olyan számottevő - mint Amerikában - de képzeljék el, ha egy ilyen eset egy nagyobb szoftvergyártó cég rendszerével történne...
- Május 14-én jelent meg az Internet Crime Complaint Center felhívása, mely szerint az internetezők sehol sincsenek biztonságban. A felhívás leginkább azoknak az felhasználóknak szólt, akik a hotelekben elérhető ingyenes WiFi-t használják. A hackerek betörnek a WiFi hálózatba és módosíthatják a vendégek adatforgalmát úgy, hogy egy ártalmatlan, frissítést ajánló felugró ablak jelenjen meg a képernyőn. Amikor a gyanútlan áldozat elfogadja a frissítést, akkor egy káros szoftver települ a rendszerére, így a támadó akár bizalmas adatokhoz is hozzáférhet.

Malware

- Május 17-én a Google Chrome telepítőjének olyan verziója vált elérhetővé, amelybe a hacker-ek egy trójait csomagoltak, így a böngésző telepítésekor lefut a káros szoftver, és megfertőzi az áldozat rendszerét.
- Május 13-án fertőzési adatok jelentek meg a Bredolab botnetről, mely szerint összesen 30 millió számítógépet fertőzött meg. Az zombi számítógépek irányítója havi 100 ezer eurót is keresett azzal, hogy bérbe adta a hálózatot más bűnözőknek és képes volt akár napi 3 milliárd spam-et is küldeni. Georg Avanesov-ot végül 4 év börtönre ítélték.
- Az Iráni Nemzeti CERT (MAHER) egy újabb kifinomult kártevőt fedezett fel, amelyet a Kaspersky Lab-nál Flamer-nek, a Budapesti Műszaki és Gazdaságtudományi Egyetemen működő CrySys Labor által pedig sKyWIper-nek neveztek el. A CrySys labor munkatársai komoly szerepet játszottak a káros kód tevékenységének megfejtésében, amely minden korábban ismertnél nagyobb és összetettebb volt. A bejelentés pillanatában 43 modult ismertek, a kód körülbelül 20 MB-ot foglalt el. A bővítmények következtében rendkívül széleskörűen lehetett felhasználni, számos feladatot volt képes ellátni. A későbbi elemzések kimutatták, hogy egy gyenge Microsoft tanúsítványt is felhasznált a terjedéséhez, amelyet titkosítási szakértők úgy jellemeztek, hogy alig néhány olyan ember van a világon, aki képes ilyen minőségű és összetettségű kódot készíteni. A Flamer/sKyWIper elsősorban a Közel-Keleten és Kelet-Európában terjedt el.

Kibertámadások

- A PHP script nyelv egy nem javított sérülékenysége miatt világszerte tömegesen veszélyeztetettek voltak a weboldalak, amelyet kihasználva a támadók távolról átvehetik az irányítást a szerverek felett. A kód futtatási sérülékenység csak akkor érintette a weboldalt, ha az common gateway interface (CGI) módban volt. A PHP FastCGI-t használók nem voltak érintettek a sérülékenységben.
- Egy Kanadában élő Anonymous hacker Christopher “Commander X” Doyon egy eléggé hihetetlennek tűnő üzentet hozott nyilvánosságra: az Anonymous hozzáfér az Egyesült Államok minden titkos adatbázisához, ráadásul nem is kellett feltörniük ezeket a rendszereket, mivel azok üzemeltetői adtak hozzáférést nekik.
- Egy iráni hacker csoport azt állította, hogy sikeresen feltörte a NASA egyik szerverét, és onnan adatokat szereztek. A NASA elismerte a támadás tényét, de a későbbi vizsgálatok szerint nem történt adatlopás.

- Az Anonymous állítása szerint betört az Igazságügyi Hivatal (Bureau of Justice) weboldalára, és 1,7 GB adatot szereztek meg onnan, belső levelezést és adatbázis dump-ot egyaránt. Az összegyűjtött adatokat a Pirate Bay torrent oldal segítségével letölthetővé tették.
- Az orosz Anonymous célkeresztjébe kerültek a Kreml és a Szövetségi Biztonsági Szolgálat (Russian Federal Security Service - FSB) weboldalai, amelyeket elosztott szolgáltatás megtagadásos támadásokkal (DDoS -Distributed Denial of Service) tettek elérhetetlenné.
- Egy masszív elosztott szolgáltatás megtagadásos támadás (DDoS) következtében, amely Kínából indult, az 1,4 millió oldalt kiszolgáló egyesült királyságbeli 123-reg nevű szolgáltató elérhetetlenné vált.

Június

Adatvédelem, adatlopás

- Egy orosz fórumon 6,5 millió LinkedIn felhasználó jelszavát, illetve annak titkosított verzióját hozták nyilvánosságra. Különböző hiányosságok miatt a jelszavakat könnyen vissza lehetett fejteni. Az utólag megjelent hírek szerint a felhasználók elég komoly hányada nem vette komolyan a biztonságos jelszóra vonatkozó ajánlásokat, mivel a leggyakoribb jelszó a "Link" volt. Ezen kívül számos esetben fordultak elő a "work" és a "job" jelszavak is.
- Az online játékosokat sem felejtették el a kiberbűnözők, egy június 11-én megjelent cikk szerint a népszerű League of Legends című játék félmillió felhasználója kapott értesítést arról, hogy azonnal változtassa meg a jelszavát, mivel illetéktelenek fértek hozzá, email címeik és több más bizalmas adattal együtt. A hírek szerint pénzügyi információk nem kerültek ki a rendszerből.

Malware

- További elemzések láttak napvilágot a Flamer kémszoftverről, melyek szerint szoros kapcsolat van a 2009-ben felfedezett Stuxnet és a mostani káros szoftver között.
- A hónapban egy újonnan felfedezett javítatlan Microsoft XML Core Services sérülékenységet kihasználva, feltört weboldalakon keresztül káros kódot terjesztettek. A fertőzéshez elegendő volt, ha a felhasználó meglátogatott egy olyan kompromittált weboldalt, ahonnan káros tartalmú oldalt töltött le, az pedig kihasználta a szoftver sérülékenységét, és további káros szoftvereket töltött le.
- Június 27-én jelent meg az a cikk, amely a Zeus trójai újabb variánsának felfedezéséről szólt, amely már képes saját adatforgalmát titkosítani, hogy megnehezítse a felismerést.

Kibertámadások

- Az Operation High Roller-nek elnevezett akció keretén belül a bűnözők káros szoftverek segítségével tehetős emberek bankszámlájáról emeltek le komoly összegeket. A támadásban a Zeus-SpyEye káros szoftvereket használták, legalább 60 bank ellen és körülbelül 60-80 millió euró kárt okoztak.
- A London Internet Exchange-t (LINX) egy nagyobb kimaradás sújtotta, amit megfigyelők szerint egy elosztott szolgáltatás megtagadásos támadás (Distributed Denial of Service - DDoS) idézett elő. (A non-profit szervezet biztosítja a főbb brit internet szolgáltatók számára a peering-et, ennek következtében pedig mind a cégeket, mind azok ügyfeleit érintette a leállás.) A LINX Network Community a Twitter-en megerősített a kimaradás tényét.

Július

Adatvédelem, adatlopás

- Olaszországban letartóztatták egy korábban bezárt fájlcserélő weboldal adminisztrátorát, aki az oldal működése alatt nagyjából fél millió eurót keresett, majd ezután eladta a körülbelül 300 ezer felhasználó személyes adatait tartalmazó adatbázist.
- A Yahoo-t sem kímélték a hacker-ek, 450 ezer felhasználó email címe és a hozzá tartozó titkosítatlan jelszó került nyilvánosságra. A támadók a Yahoo egyik aldomain-jének SQL befecskendezéses sérülékenységét használták ki. A nyilvánosságra került jelszavak között a "password" és az "123456" voltak a leggyakoribbak.
- Az Android Forums 1 millió felhasználója volt kénytelen jelszót változtatni, mivel az oldal adminisztrátorai észrevették, hogy illetéktelenek hozzáfértek az adatbázishoz. A hírek szerint nem volt bizonyított, de elképzelhető, hogy a támadók letöltötték a teljes felhasználói adatbázist, amelyben email címek, titkosított jelszavak és egyéb információk is voltak.
- Az NVIDIA nehezen vallotta be, hogy tévedtek, ugyanis azt állították, hogy a korábbi betörés alkalmával ellopott felhasználói adatok titkosítottak voltak, ezért nem érheti kár a felhasználókat. Azonban kiderült, hogy ez nem igaz, legalábbis a károkozás része, mivel a betörő(k) szerint semmilyen nehézséget nem jelentett visszafejteni a titkosítást.
- A Microsoft is egy bejelentéssel élt a hónapban, mégpedig, hogy augusztustól blokkolni fog minden olyan adatforgalmat, amely 1024 bitnél kisebb SSL kulcsot használ. A lépésre azért volt szükség, mert az 512 bites vagy annál rövidebb kulcsok már nem jelentenek megfelelő biztonságot az adatok titkosításában.

Malware

- Leálltak a DNSChanger trójai által használt, FBI által működtetett DNS szerverek. A hatóságok szerint még ekkor körülbelül 260-300 ezer felhasználó ezeket a szervereket használta, amely azt jelenti, hogy több mint fél évvel a szerverek lefoglalása után is rengeteg fertőzött gép volt. Több Internet szolgáltató, azért hogy az ügyfelek ne szakadjanak le a netről ezután, a káros DNS szerverek felé irányuló kéréseket a saját DNS szervereikre irányította át.

Kibertámadások

- Óriási erőfeszítéssel készültek fel a 2012-es Londoni Olimpiai játékokra a biztonsági szakértők, akik úgy vélték, hogy akár napi 14 millió kísérlettel is számolniuk kell az amatőröktől kezdve a hacktivistákon keresztül a profi hacker-ekig és jól vizsgáztak.

Augusztus

Adatvédelem, adatlopás

- A Microsoft úgy döntött, hogy az Internet Explorer következő verziójában bekapcsolja a "do not track" opciót, amelynek célja, hogy a weboldalak ne kövessék a felhasználót az internetes barangolás idején. A lépés komoly vitákat gerjesztett, például az Apache webszerver készítői olyan javítást adtak ki a termékükhöz, amely figyelmen kívül hagyja az IE alapértelmezett beállítását.

Malware

- A ZeuS-in-the-Mobile (Zitmo) azt bizonyítja, hogy a számítógépes káros szoftverek készítői követik a trendeket és a mobil eszközök (okostelefonok, tablet-ek) terjedésével ők is lépést tartanak. Bár a Zitmo nem újdonság, de korábban a Blackberry készülékeken még nem voltak jelen. Júliusban egy újabb kifinomult és összetett káros szoftvert fedeztek fel, amely a szakértők egybehangzó állítása szerint a Stuxnet készítőinek kézjegyét viseli magán. A Gauss káros szoftver szintén a Közel-Keleten terjedt el, és elsősorban banki és egyéb felhasználói adatokat gyűjt. Beépül a böngészőbe, és megfigyeli az adatforgalmat, valamint egyéb adatokat gyűjt a számítógépről.
- Augusztusban került napvilágra, hogy az FBI nevében próbál meg pénzt kiszedni az áldozatokból a Reveton nevű ransomware, amely blokkolja a számítógép használatát és olyan figyelmeztetést ad, miszerint az FBI a törvények megsértése miatt zárolta azt. A zárolást csak fizetés ellenében hajlandó feloldani.
- Egy újabb ransomware bukkant fel, ezúttal Európában, elsősorban Hollandiában. A Dorifel névre keresztelt kártevő szintén zárolja a felhasználó számítógépét, illetve titkosítja a rajta lévő fájlokat. A Dorifel adathalász email-ek segítségével terjed, a benne lévő hivatkozásokra kattintva káros szoftver települ az áldozat rendszerére, viszont érdekes módon nem követel pénzt.
- A Zeus újra visszaköszönt ugyanis nyilvánosságra került a Citadel, ami egy új Zeus variáns, amely feltört weboldalak látogatóit fertőzi meg, majd titkosítja a dokumentumokat.
- Újabb információk jelentek meg a júliusban felfedezett Crisis malware-ról, a hírek szerint a Windows-os verzió képes arra, hogy megfertőzze a VMware virtuális gép képfájljait is. A káros szoftver telepítője egy olyan Java (jar) állomány, amely a VeriSign által kiadott digitális aláírással hitelesíti magát. A káros szoftver social engineering támadásokkal terjed, vagyis email vagy azonnali üzenetben próbálja meg rávenni az áldozatot, hogy nyisson meg egy káros tartalmú hivatkozást.
- 2012 júliusában az Oracle Java megkezdte vesszőfutását az első nyilvánosságra került 0-day sérülékenységgel. Ha a felhasználó a legfrissebb JRE-t és Firefox böngészőt használva meglátogatott egy speciálisan erre a célra készített weboldalt, akkor egy Dropper.MsPMs nevű program települt a számítógépére, amely kapcsolatba lépett egy C&C szerverrel, és további káros programokat is tudott telepíteni. Ezzel kapcsolatban a lengyel Security Explorations nevű cég bejelentette, hogy a most felfedezett sérülékenységet több másikkal együtt már áprilisban továbbították az Orcale-nek, ennek ellenére a júliusban kiadott frissítésekben nem javították azt.

Kibertámadások

- Egy friss felmérés szerint az SQL befecskendezéses támadások a legelterjedtebbek a hacker-ek közt. 2012 második negyedévében 69%-kal több ilyen támadást regisztráltak, mint az év első 3 hónapjában. Az adatok négy főbb támadási típus elterjedtségét mutatják: cross-stie scripting (XSS/CSS), könyvtár bejárásos támadás (directory traversal), SQL befecskendezés (SQL injection) és cross-site request forgery (XSRF/CSRF).
- Kínai hacker-ek törtek be az Európai Tanács rendszereibe, és onnan bizalmas információkat szereztek meg, amely az aktuális görögországi pénzügyi csomag részleteit tartalmazták, illetve az Európa Tanács elnökének, Herman Van Rompuy-nak a teljes levelezéséhez is hozzájutottak.
- A Saudi Arabian Oil Co (Saudi Aramco) lekapcsolta a számítógépes hálózatát válaszul egy komoly vírus fertőzésre, ennek ellenére az állami tulajdonú vállalat azt állította, hogy az incidens nem érintette az olaj kitermelést.

Szeptember

Adatvédelem, adatlopás

- A Microsoft 16 karakterben határozta meg a Hotmail fiókok maximális jelszavát, az ennél hosszabb jelszavakat a rendszer automatikusan csonkolja. Ez felvetette azt a kérdést, hogy vajon a Microsoft egyszerű szövegben tárolja-e a jelszót, vagy pedig csak az első 16 karakterből képzi a hash-t.

Malware

- Adam Gowdiak, biztonsági szakértő a Security Explorations vezetője bejelentette, hogy a napokkal korábban soron kívül kiadott Java frissítésben egy újabb sérülékenységet talált. Elmondása szerint a mostani sérülékenység az áprilisban felfedezettekkel áll kapcsolatban és segítségével ki lehet törni a sandbox-ból és tetszőleges programot lehet telepíteni.

- A kártékony szoftverek a Linux rendszereket sem kímélték. A Wirenet trójai a Linnux és OS X rendszereket vették célba, és a fertőzött rendszerekből, a népszerű programokból (Firefox, Chrome, Thunderbird, Seamonkey, Pidgin) próbálta meg ellopni a felhasználóneveket és jelszavakat, illetve továbbítani azokat egy C&C szervernek.

- A fenyegetések mellett jó hírt is hozott a július, ugyanis a Microsoft bejelentette, hogy szövetségi bírósági jóváhagyással átvette az irányítást a Nitol botnet hálózat felett. A malware elsősorban Kínában terjedt el, ahol a hamis Windows verziókba építik be a bűnözők, így az már az operációs rendszer telepítésekor felkerül a rendszerre.

- A hónap közepén ismét a Java kapta a főszerepet, mert Eric Romang biztonsági szakértő az elhíresült Java 0-day sérülékenységek után kutatott, amikor belefutott néhány gyanús fájlba. Az állományok elemzésekor kiderült, hogy egy korábban ismeretlen Internet Explorer 0-day sérülékenységbe futott bele, amely a teljesen naprakész Internet Explorer 7 és 8 verzióján is működött. Az exploit 2 html fájlból és egy Flash videóból állt.

Kibertámadások

- Jelentések szerint a Perzsa-öbölben, Katarban székelő folyékony földgáz (liquified natural gas - LNG) szolgáltató RasGas-t egy azonosítatlan vírus támadta meg, amely miatt sem a vállalat weboldala, sem pedig az email szerverei nem voltak elérhetőek.

- Biztonsági kutatók egy olyan spam-ben terjedő káros szoftverre hívták fel a figyelmet, amely egy 3 évvel ezelőtt felfedezett sérülékenységet használ ki. A célzott támadásokkal a katonai repülőgépet gyártó vállalatokat vették célba. Amennyiben a spam címzettje megnyitja a csatolmányként érkező káros tartalmú PDF állományt - amiben egy meghívó található egy védelmi ipari eseményre - akkor a háttérben lefut egy olyan program, amely képes kihasználni a régebbi kiadású Adobe Acrobat és Adobe Reader programok egy sérülékenységét.

- Szeptemberben DDoS támadás ért számos amerikai bankot, amelyet az Izz ad-Din al-Qassam Cyber Fighters nevű csoport a Mohamed prófétát gúnyoló film miatt, a tiltakozás eszközének szán és amit addig folytatnak, ameddig nem távolítják el a filmet mindenhonnan. Az Egyesült Államok kormánya szerint a támadás mögött Irán állt.

Október

Adatvédelem, adatlopás

- A felhasználó első (és gyakran az egyetlen) biztonsági szintje a jelszó. Ezért rendkívül fontos, hogy betartsuk az erre vonatkozó alapvető előírásokat. A jelszó legyen minél hosszabb, de legalább 8 karakter! Legyen benne kisbetű, nagybetű, szám, írásjel! Időnként változtassuk meg, és ne használjuk ugyanazt a jelszót több szolgáltatás igénybevételénél! Ehhez képest, amikor a SplashData nyilvánosságra hozta a 2012-es évben hacker-ek által ellopott, majd bemutatott jelszavakat, az komoly hasonlóságot mutatott az előző évi listával. Sajnos az emberek nagy százaléka még mindig elegendőnek tartja a "password", az "123456" vagy az "12345678" jelszó használatát.

- Októberben látott napvilágot az a hír is, mely szerint a Közbeszerzési Hatóság nevében gyűjtöttek adatokat arra jogosulatlanok. A csalók hamisított levélpapír, aláírás és bélyegzőlenyomatok felhasználásával kerestek meg embereket, hogy adatokat szerezzenek tőlük egy Európai Uniós adatgyűjtésre hivatkozva.

Malware

- A káros szoftverek írói senkire nincsenek tekintettel, ahogy azt bizonyítja a Rovio nevű cég Angry Birds című, hatalmas sikert elért játékának folytatása is. A Bad Piggies is óriási népszerűségre tett szert néhány nap alatt, amit kihasználva a bűnözők újracsomagolták a játékot, csak éppen káros szoftvert is adtak mellé, amellyel kéretlen reklámokat jelenítettek meg az áldozatok rendszerén.

- Októberben derült fény arra, hogy egy legálisnak tűnő orosz vállalat, amely proxy szolgáltatást nyújtott világszerte, a Backdoor.Proxybox nevű káros szoftvert terjesztett az ügyfelei között. A botnet olyan nagy volt, hogy időszaktól függetlenül legalább 40 ezer zombi PC-t tudott munkába állítani, és ezt a botnet gazdái úgy használták ki, hogy bérbe adták a hálózatot más bűnözők számára.

- Az elmúlt években a világ megismerhette a Conficker nevű malwaret és ezzel kapcsolatban jelent meg újabb hír, ami szerint a Conficker annak ellenére is aktív, hogy a C&C szerverei már nem elérhetőek, a készítők pedig nem adnak ki újabb verziókat. Mindezeket figyelembe véve meglepő, hogy a Microsoft még most is a 2. legelterjedtebb kártevőként tartja számon, amely a Windows-os tartományokban okoz fertőzést.

- Októberben a Közel-Keleten újabb, a Flame rokonaként azonosított kártevő bukkant fel. A miniFlame vagy mások által "SPE" vagy "John" néven ismertté vált malware működhet önállóan is, de a Gauss vagy Flame kémszoftverek egyik moduljaként is használható.

- A hónapban megjelent Trend Micro felmérés szerint a Google Play-en elérhető alkalmazások felmérése során olyan ingyenes Flash Playert fedeztek fel, amely képes reklámokat megjeleníteni, ezenkívül adatokat is gyűjtenek (telefonszám, IMEI szám, naptári bejegyzések, stb.).

- A hónap végén egy újabb hír látott napvilágot a botnetek világából, ugyanis a Kindsight Security Lab felmérése szerint a harmadik negyedévben a ZeroAccess botnet felelt az otthoni számítógépek megfertőzésének 29%-áért. A készítők a nehezebb észlelés miatt TCP-ről UDP-re változtatták a kommunikációs protokollt.

Kibertámadások

- Az Adobe bejelentette, hogy hacker-ek feltörték a kódok aláírására használt rendszert, hogy azzal a saját malware-üket az Adobe aláírásával hitelesítsék. A szoftveróriás szerint legalább két káros programot írtak alá az érvényes Adobe tanúsítvánnyal.
- Október elsején a Fehér Ház elismerte, hogy az egyik számítógépes hálózatukat kibertámadás érte, de állításuk szerint nem szivárgott ki semmilyen bizalmas információ a rendszerből, amelyet a Fehér Ház Katonai Hivatala használ (White House Military Office).
- Letartóztatták Andrej N. Sabelnyikovot, akit azzal vádoltak, hogy a Kelihos botnet fejlesztője és irányítója volt. Az orosz C++ programozó végül megállapodott a Microsoft-tal, de a részleteket nem hozták nyilvánosságra.
- A hónap végén feltörték az izraeli rendőrség hálózatát. Erre a következtetésre jutott egy vizsgálat, amelyet azután indítottak, hogy gyanús fájlokat találtak egy szerveren. A rendőrség vezetése ezután a teljes hálózat leállítását rendelte el a teljes kivizsgálás idejére.
- Az amerikai bankok ellen irányuló szeptemberi támadássorozatban egy nagyon kifinomult eszközt használtak az elkövetők. A Prolexic Technologies októberben nyilvánosságra hozott álláspotja szerint az elosztott szolgáltatás megtagadásos támadás (DDoS) mögött egy "itsoknoproblembro" nevű program állt, amely segítségével több nagy bankot is megbénítottak ideiglenesen.
- Október közepén, saját magukat iszlamista hacktivistáknak nevező hacker-ek újabb kibertámadásokat hajtottak végre egyesült államokbeli nagy bankok ellen, és legalább két esetben meg tudták zavarni azok működését.

November

Adatvédelem, adatlopás

- Ha a felhasználó megfelelő erősségű jelszót használ, illetve ha betartja a munkahely által előírt, jelszavakra vonatkozó szabályait, még akkor is történhetnek problémák, ahogy például a dél-karolinai Szövetségi Adóhivatalban, ahonnan 3,8 millió állampolgár és 700 ezer vállalkozás adatait lopták el. A nyomozás kiderítette, hogy még augusztus folyamán több, káros tartalmú email érkezett a hivatalba és legalább egy alkalmazott rákattintott a benne lévő hivatkozásra, így egy káros szoftverrel a támadó megszerezte az illető felhasználónevét és jelszavát, ez pedig sok millió adat ellopásához vezetett. Az elkészült jelentés két komoly, emberi hibára mutatott rá. Az alkalmazott több helyen is ugyanazt a jelszót használta, így például a bizalmas adatok eléréséhez, valamint a munkaadó nem titkosította az adatbázist.
- Egy belga cikk szerint a Titkosszolgálat számos munkatársa saját magát buktatta le a Facebook vagy LinkedIn profilja segítségével. A titkosszolgálatok munkatársai általában nem szokták reklámozni, hogy mi a munkahelyük, de valamiért ezt elfelejtik, amint egy közösségi oldalra tévednek. A cikk rámutat arra, hogy Oroszországnak és Kínának több ezer olyan kiképzett embere van, akiknek a feladatuk kimondottan a közösségi oldalak figyelése, hogy onnan információkat szerezzenek.

Malware

- A Java egyik „ironikus” előnye - amely a mottója is egyben (write once, run anywhere) - a káros szoftverek esetén a hátrányává válik. Októberben jelentek meg először hírek a Jacksbot nevű távoli hozzáférést lehetővé tevő trójairól (RAT - remote access trojan), amely a Windows mellett a Linux és a Mac rendszereken is fut. A tényleges károkozást végző kód nem Java-ban készült, az csak dropper-ként szolgál, amely letölti a tényleges malware-t.

- A káros szoftverek gyakran feltört weboldalokon keresztül terjednek, ahogy azt az Opera böngésző esete is példázta. Hacker-ek feltörték a böngésző gyártó egyik weboldalát, és ott egy reklámba ágyazott script segítségével átirányították a látogatókat egy olyan oldalra, amely megfertőzte a számítógépeiket.

- November 20-án megjelent a Symantec jelentése, amelyben kifejtették, hogy a hacker-ek számára nagyon fontos, hogy az általuk készített káros szoftver egyáltalán ne, vagy minél később "bukjon le". Ennek érdekében fejlett technológiákat használnak, hogy az antivírus cégek és a biztonsági szakértők nehezebben ismerjék fel a fertőzést okozó kódokat. Mivel a Symantec 2011-es jelentése szerint 400 millió új káros program jelent meg, belátható, hogy képtelenség ezt a hatalmas mennyiséget kézzel átvizsgálni. Ehelyett automatizált rendszereket használnak a kutatók, hogy felismerjék a malware-eket. Azok viszont úgy védekeznek, hogy felismerik, ha virtualizált környezetben, automata rendszereken futnak, ezért tétlenül várnak és nem csinálnak olyan műveleteket, amelyekkel magunkra vonhatnák a szakemberek figyelmét.

- November végén újabb Java 0-day sérülékenységet fedeztek fel, amit egy feketepiaci fórumon 5 számjegyű összegért árultak. A sérülékenység a legfrissebb verziót érinti, de a korábbi 6-os kiadást nem.

Kibertámadások

- A "Project Blackstar" akció során a GhostShell hacktivista csoport 2,5 millió, többek között az orosz politika, oktatás és rendőrség szerv tagjait érintő adatot tett közzé. A csoport ezzel a lépéssel szeretné felhívni a figyelmet az orosz állam visszaéléseire, a korrupcióra és a társadalmi egyenlőtlenségekre.

- A Pentagon legnagyobb beszállítója a Lockheed Martin októberben kiadott közleményében felhívta a figyelmet arra, hogy drámaian megnőtt a hálózatuk ellen végrehajtott behatolási próbálkozások száma, illetve azok kifinomultsága és emiatt felveszik a kapcsolatot a partnereikkel, hogy segítsenek azoknak biztonságosabbá tenni a saját rendszereiket.

- Novemberben került nyilvánosságra egy döbbenetesen egyszerű módszer, amivel bármely Skype fiók felett át lehetett venni az uralmat. A Microsoft a probléma javításáig letiltotta a jelszó emlékeztetők küldését, amely a problémát okozta.

- Az Egyesült Államok egy amerikai és izraeli együttműködésben készült kémszoftvert használt arra, hogy betörjön a francia elnöki irodába, adta hírül a l'Express magazin az ország kiberhadviselési ügynökségére hivatkozva. Az újság szerint a köztársasági elnök számos közeli munkatársának számítógépét - köztük volt a személyzeti főnök Xavier Musca is - törték fel májusban és a fertőzés a hírhedt Flame nyomait viseli magán. Az Egyesült Államok határozottan tagadta a vádakat.

December

Adatvédelem, adatlopás

- A felelőtlen felhasználói viselkedésre mutat rá egy felmérés, amely megállapította, hogy a bizalmas adatokat tartalmazó állományokat akkor töltik fel valamilyen nyilvános fájlmegosztó (cloud) szolgáltatásba, ha az kifejezetten tiltva van. A felmérés szerint az alkalmazottak 20%-a használja a Dropbox-ot vagy más hasonló szolgáltatást. Ha a vállalati szabályzat kimondottan tiltja az ilyen cselekvést, az alkalmazottak fele akkor is ragaszkodik ehhez a módszerhez és a cégvezetőkre ez ugyanúgy igaz, mint az alkalmazottakra.

- December 6-án került nyilvánosságra az a cikk, mely szerint az adatlopások kiterjedtsége azt is mutatja, hogy egyre gyakrabban válnak gyerekek is áldozattá. Egy amerikai tanulmány szerint minden 40. háztartásban történt már olyan eset, amikor a kiskorú gyermek személyes adatait ellopva (az összes adat közül leginkább a gyerekek társadalom biztosítási száma van kitéve veszélynek), a bűnözők számlákat nyithattak, hitelkártyát szerezhettek vagy pénzmosásra használhatták. A szakértők szerint könnyebb egy gyerek adatait felhasználva létrehozni egy tiszta pénzügyi profilt. A jelentés ezen kívül rámutat arra is, hogy a szegényebb családok nagyobb veszélynek vannak kitéve.

Malware

- Az ünnepek előtt jelent meg az a hír, mely szerint 36 millió eurós kárt okoztak az Eurograbber káros szoftver segítségével. A Check Point és a Versafe kutatói azonosították azt a malware-t, amely több nyugat-európai országban 30 ezer felhasználót károsított meg, jellemzően 500 és 250000 euró közti összegekkel.
- Manapság már nem csak a számítógépeket veszélyeztetik a káros szoftverek. Egy decemberben nyilvánosságra került jelentés bemutatja, hogyan fertőztek meg világszerte több száz, számítógépre csatlakoztatott POS (point-of-sale) rendszert, amelyekkel bankkártyás fizetést lehetett végezni. A Dexter névre keresztelt káros szoftver az összegyűjtött adatokat elküldte egy C&C szervernek, ahol szétválogatták azokat, hogy hozzájussanak a kártya-adatokhoz. A káros szoftvert felfedező szakértő szerint, ha a megfertőzött kereskedők használtak volna titkosítást a POS terminál és a banki rendszer közötti adatátvitelben, akkor valószínűleg megelőzhető lett volna az adatlopás.

Kibertámadások

- A németországi illetőségű 50Hertz áramszolgáltatót ért kibertámadás megbénította a vállalat kommunikációját, de támadásban az áramszolgáltatás nem került veszélybe. Az incidens egy botnet által végrehajtott szolgáltatás megtagadásos támadás (DDoS - Distributed Denial of Service) volt, amely öt napon át tartott és amelyben másodpercenként több ezer kérés érkezett a rendszerhez, így idővel teljesen lefoglalta annak erőforrásait és a vállalat internetes, valamint email kapcsolata összeomlott. Bár a támadók ismeretlenek, az IP címeket vissza lehetett követni Oroszországba és Ukrajnába.

Nem a 2012-es év eseményeihez kapcsolódóan, de mindenképp meg kell említeni a „Vörös Október” névre keresztelt kiberkémkedési kampányt és az ehhez köthető Rocra kártékony szoftvert, amit célzott email támadással terjesztenek. 2013. január 14-én hozta nyilvánosságra a Kaspersky Lab azon jelentését, amelyben egy olyan új kiberkémkedési akciót azonosított, amely diplomáciai, kormányzati és tudományos kutatással foglalkozó szervezeteket támad világszerte legalább öt éve. A támadássorozat elsődlegesen a kelet-európai országokat, a korábbi Szovjetunió tagjait és Közép-Ázsiát célozza, de széles körben előfordulnak incidensek, beleértve Nyugat-Európát és Észak-Amerikát is. A támadók célja, hogy érzékeny adatokat tartalmazó dokumentumokat lopjanak a szervezetektől, köztük geopolitikai információkat, számítógépes rendszerek hozzáféréséhez szükséges hitelesítéseket és személyes adatokat mobil eszközökről és hálózati berendezésekről. A Vörös Október bűnözői saját kártevőt fejlesztettek ki, amit a Kaspersky Lab “Rocra” néven azonosított. Ennek a kártékony programnak saját, egyedi moduláris felépítése van rosszindulatú bővítményekkel, adatlopásra specializált modulokkal és úgynevezett „backdoor” trójai programokkal, amik jogosulatlan hozzáférést biztosítanak a rendszerhez és így lehetővé teszik további kártevők telepítését vagy a rendszerekhez való hozzáférést és személyes adatok lopását.

IT biztonság trendjei 2012

Ismét lezárult egy év, ráadásul nem is akármilyen. Volt Olimpia Londonban, elnökválasztás Amerikában, Sandy hurrikán az Egyesült Államok keleti partvidékén. Folytatódtak a feszültségek a Közel-Keleten, a gazdasági nehézségek a világ több térségében, például az eurózónában.

Vajon hogyan tükröződött ez az eseményekben és problémákban gazdag esztendő az informatikai biztonság területén? Milyen fenyegetések jelentkeztek állami és szervezeti szinten, a cégeknél, illetve az otthonokban? Milyen trendvonalakat húzhatunk?

Ezekre – és hasonló – kérdésekre igyekszünk válaszolni. Sorra vesszük 2012. leggyakoribb számítógépes kártevőit, a weben bujkáló fenyegetések jellemző forrásait. Górcső alá vesszük a botnetek, a spam és az adathalászat alakulását, s azt is, hogy a nagy szoftvergyártók hogyan foltozták termékeiket, hogy megvédjék őket a hacker-ek támadásaitól.

Válságban is virágzásban?

Jóllehet a világ számos térségében hanyatlott vagy legalábbis stagnált a gazdaság 2012-ben, az IT biztonsági piacot nem érte el a többi szektort sújtó betegség. Az év adatainak összesítésére még várnunk kell, de a Gartner elemzői szeptemberi tanulmányukban úgy becsülték: 2012-ben 8,4 százalékkal bővülhet az IT biztonsági világpiac. A szakemberek a 2011-es 55 milliárd dollár után a mögöttünk álló esztendőre 60 milliárd dolláros összforgalmat prognosztizáltak. Felmérésük szerint az informatikai vezetők 45 százaléka az előző évinél nagyobb, 50 százalékuk pedig szinten maradó biztonsági költségvetéssel kalkulált tavaly. A növekedés az előttünk álló években sem áll meg: a Gartner 2016-ra 86 milliárd dolláros volument ígér.

Miközben ezek a számok az ágazat beszállítói szempontjából kétségtelenül örvendetesek, kérdés: helyénvaló-e virágzásról beszélnünk, hiszen a biztonsági kiadások folyamatos növelését a kockázatok fokozódása teszi szükségessé.

A kibertámadások egyre növekvő – éves szinten több százmilliárd dollárnyi – kárt okoznak a szervezeteknek és magánszemélyeknek. Hogy a Symantec adatait idézzük: 12 hónap alatt a számítógépes bűncselekmények világszerte mintegy 110 milliárd dollárt vettek ki a fogyasztók zsebéből.

Mint a cég 2012. évi, szeptemberben közzétett *Norton Kiberbűnözési Jelentéséből (Norton Cybercrime Report)* kiderül, a vizsgált 24 országban minden másodpercben 18 felnőtt esik informatikai bűncselekmény áldozatául. Ez napról napra másfél millió embert jelent. Egy-egy eset átlagosan 197 dollár közvetlen pénzügyi veszteséget okoz. Ebből az összegből a Symantec számítása szerint egy hétig lehetne etetni egy négytagú családot. Egyetlen esztendő leforgása alatt összesen 556 millió embert károsítottak meg a kiberbűnözők – többet az Európai Unió teljes lélekszámánál. Ez az 556 millió fő a világ internetező felnőtt népességének 46 százaléka.

Tavaly februári adatok szerint hazánkban is 900 ezer körül jár azoknak a száma, akik elszenvedtek már valamilyen számítógépes támadást. A közvetlen anyagi kár 7 milliárd forint, s 14 milliárd forintra becsülik a kiesett idő értékét. És persze a világon mindenhol vannak pénzben ki nem fejezhető károk is. Ráadásul az imént csak az egyének elleni akciókról szóltunk – a vállalatok, szervezetek, netán nemzetállamok ellen elkövetett támadások sokkal nagyobb anyagi és erkölcsi veszteségeket okozhatnak.

Már-már közhelynek számít, hogy a kiberbűnözés önálló iparággá nőtte ki magát. Ha belegondolunk, nem is csodálkozhatunk ezen. Óriási bevételek vonzzák a hackereket a sötét oldalra. A Sophos például szeptember végén úgy becsülte: a ZeroAccess botnet gazdái, ha teljes kapacitással működtették több mint egymillió gépből álló zombi-hadseregüket, akkor klikkcsalásból vagy digitális pénz (Bitcoin-) vadászatból naponta több mint 100 ezer dollár bevételre tehettek szert.

A feketepiacon mind fejlettebb kártevőkészítő készletek kaphatók, s még az árusítás módja is követi a legális szoftverkereskedelem legújabb megoldásait. A hírhedt Blackhole kit készítői például nemcsak új verzióval rukkoltak ki, hanem bérleti (SaaS, software as a service) konstrukcióban kínálják portékájukat.

És ahogy egy valódi iparághoz illik, már évek óta nemcsak magánvállalkozások tevékenykednek a kiberalvilágban sem. Az utóbbi években jól megfigyelhető, hogy mind gyakrabban nemzetállamok vagy általuk támogatott szervezetek indítanak rejtett akciókat – akár információszerzés, akár szabotázs céljából gazdasági, politikai vagy ideológiai alapon. Tavaly ismét sűrűn lehettünk tanúi például a közel-keleti feszültségek kibertéri megnyilvánulásainak. Multinacionális óriásbankok, fontos ipari létesítmények kerültek a támadások célkeresztjébe.

A bűnözők malmára hajtja a vizet, hogy még a fejlett országokban is sok az olyan cég, amely nincs tisztában a valós IT biztonsági kockázatokkal, s következésképpen nem rendelkezik megfelelő védelemmel sem. A Kaspersky Lab megbízásából tavaly júliusban a B2B International 22 országban összesen 3300 vezető beosztású, az IT biztonsági stratégiáért felelős szakembert kérdezett meg a cégüknél uralkodó állapotokról. Az eredmények aggasztóak: a vállalatok körülbelül fele nincs tudatában annak, milyen fenyegetésekkel kell napi szinten szembenéznie. Az Egyesült Államokban még rosszabbnak bizonyult ez az arány. Márpedig, mint *Eugene Kaspersky,* a Kaspersky Lab alapító-ügyvezetője az adatok novemberi közzétételekor hangsúlyozta: „A számítógépes bűnözők feldúlhatják mindennapi üzleti környezetünket. Világszerte gátat állíthatnak a fejlődés útjába, gazdasági, sőt politikai összeomlást idézhetnek elő.”

Magyarországon a HP végzett hasonló felmérést. Az IT óriás többek között arra használta ki a szakterület két nagy sikerű hazai rendezvényét, az Informatikai Biztonság Napját (az ITBN-t) és a Hacktivityt, hogy kérdőíven tudakozódjék a cégek biztonsági felkészültségéről. Nos, az eredmények nagyjából egybevágnak a nemzetközi tapasztalatokkal. A válaszadó szakembereknek mindössze 52 százaléka gondolta úgy, hogy vállalata felkészülten tudna fogadni egy jelentősebb hackertámadást. Informatikai kockázatkezelési stratégiát pedig csak a cégek 47 százalékánál dolgoztak ki.

Az pedig feltehetőleg főként egyéni és kisvállalati felhasználóknál nyit tág kaput a bűnözők előtt, hogy a weben leggyakrabban használt szoftvert, a böngészőt sokan egyáltalán nem, vagy csak jókora késéssel frissítik. A Kaspersky Lab felhő alapú rendszerének, a Kaspersky Security Networknek az adatait elemezve a biztonsági cég novemberben megállapította: a felhasználók 23 százaléka nem böngészője legfrissebb kiadásával dolgozik. 14,5 százalékuk az utolsó előtti verzióval, 8,5 százalékuk pedig még annál is régebbi változattal szörföl. Ugyanakkor a bűnözők akár már órákkal egy-egy sérülékenység felfedezése után támadást indíthatnak böngészőnk ellen...

Egy esztendő eseményei

Tanulságos, hogy a világ egyik vezető IT biztonsági cége mit emel ki a 2012-es év szakmai híreinek hatalmas kazlából. Nos, a Kaspersky Lab éves vissza- és előretekintésében a következőket vette fel a mögöttünk álló esztendő legfontosabb, trendjelző fejleményeinek tízes toplistájára.

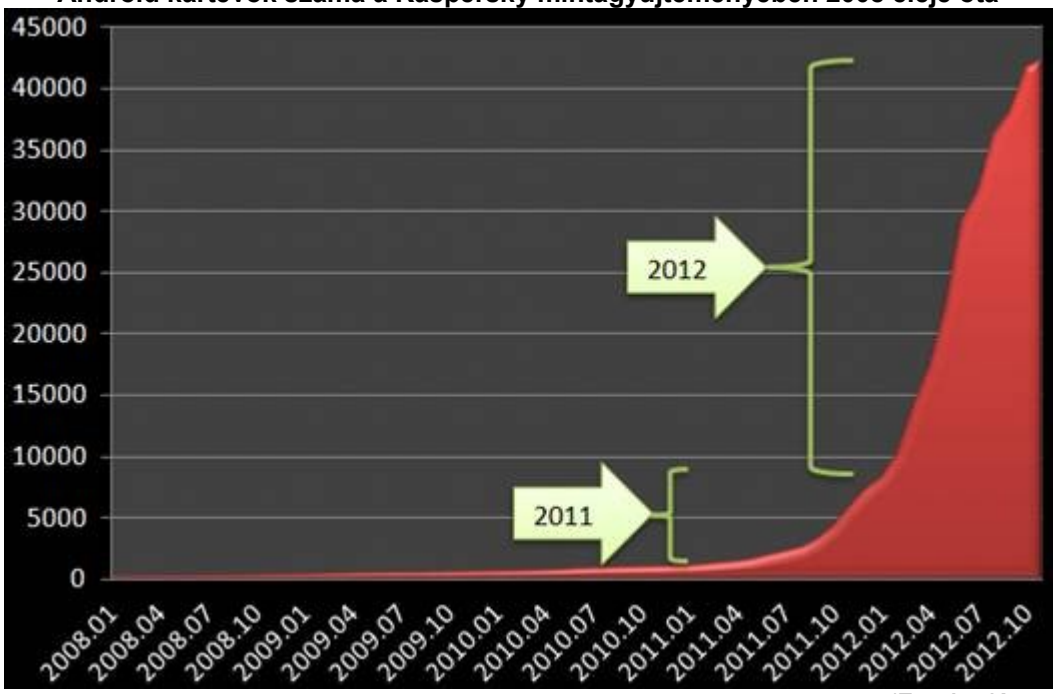
Kifinomult kártevők a Mac OS X ellen

Szakértők nem először mutatnak rá: a Mac-tulajdonosok biztonságérzete nemcsak hamis, de veszélyes is, hiszen megfelelő védekezés hiányában még nagyobb a kár, ha a nem várt támadás bekövetkezik. Íme, a legújabb figyelmeztetés: minden idők legnagyobb Mac-fertőzése, a Flashback/Flashfake trójai tavaly több mint 700 ezer Mac OS X-es rendszerre terjedt ki. Jóllehet a kártevő 2011 végén vált ismertté, igazi járványt tavaly okozott.

Az Android platform fenyegetettségének robbanásszerű növekedése

Ha egyszer a világszerte újonnan értékesített okostelefonok több mint kétharmada Android alapú, s ráadásul nyílt operációs rendszerről van szó, nem csoda, hogy a platform a hacker-ek közkedvelt céltáblájává vált. A Kaspersky-nél egyedül 2012 júniusában 7 ezer új Android kártevőt azonosítottak. Tavaly összesen 35 ezer kórokozóval gyarapodott a cég androidos mintagyűjteménye – hatszor annyival, mint 2011-ben. A trend idén se igen fog változni.

Android kártevők száma a Kaspersky mintagyűjteményében 2008 eleje óta



(Forrás: Kaspersky Lab)

Flame és Gauss: Folytatódnak az államilag támogatott kiberhadműveletek

A tévéképernyők, a rádióállomások, az online és nyomtatott sajtó egyik nagy szenzációja volt tavaly a minden idők legkifinomultabb kiberfegyvereként beharangozott kártevő, a Flame. A *New York Times* nemcsak azt a régóta hangoztatott hipotézist erősítette meg, hogy a korábban elhíresült Stuxnet féreg valójában amerikai-izraeli katonai eszköz volt, melyet az iráni atomprogram megzavarására fejlesztettek ki, hanem azt is állította: a Flame hasonló céllal, ugyanannak az „Olimpiai játékok" fedőnevű hadműveletnek a keretében készült.

Az első nagy hírverés 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 utóbb korántsem tűnt olyan veszedelmesnek és sokoldalúnak, mint azt korábban gondolták. Mindenesetre a Flame alkotói megelégelhették a nagy publicitást: június első hetében kutatók azt észlelték, hogy önmegsemmisítési parancsot adtak a kódnak.

Ugyanakkor a Kaspersky tanulmánya rámutat: a Flame esete felhívja a figyelmet arra, hogy egy-egy összetett kártevő akár évekig is tevékenykedhet észrevétlenül. Kutatók szerint a Flame projekt akár öt éven át is futhatott „a háttérben".

Nem sokkal a Flame után jelentették be egy kifinomult, feltehetőleg szintén állami támogatással kifejlesztett trójai, a Gauss felfedezését. Ez a kártevő a Közel-Keleten, elsősorban Libanonban vadászott online banki belépőkre.

Mindezek alapján valószínű, hogy a geopolitikai konfliktusoknak nagyobb informatikai vetületük van, mintsem gondolnánk.

LinkedIn és DropBox: Nagyszabású jelszólopások népszerű webes szolgáltatásoknál

Június elején ismeretlen tettesek közel 6,5 millió jelszót emeltek el a LinkedIn-ről, a szakmai kapcsolatok építésének világszerte közkedvelt fórumáról. Az eset hatalmas visszhangot váltott ki a felhasználók köreiben és IT biztonsági berkekben egyaránt. A hacker-ek egy orosz oldalon tették közzé zsákmányukat. 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 megfejthették a támadók. 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".

Hasonló incidens történt a DropBox felhőalapú file-tároló rendszernél, a Last.fm online médiaszolgáltatónál és a Gamigo ingyenes német játéksite-nál. Az utóbbi támadást tavaly márciusban követték el, majd a hacke-reknek a jelek szerint sikerült feltörniük a titkosítást: négy hónappal a betörés után 11 millió jelszót tettek közzé, 8,2 millió email cím társaságában. A feltört fiókok közül 3 milliót amerikai, 2,4 milliót német, 1,3 milliót pedig francia felhasználók hoztak létre.

Elmondhatjuk tehát: mind vonzóbb hacker-célponttá válnak a nagy online szolgáltatók. Tekintettel arra, hogy sajnos a felhasználók nagy része több helyen is ugyanazzal a jelszóval operál, a megszerzett belépőkkel a támadók sokfelé próbálkozhatnak, busás zsákmány reményében.

Adobe tanúsítványok hacker-kézen

Már 2011-ben nagy port kavart két tanúsítványkezelő elleni támadás: márciusban a Comodo, júniusban a Diginotar nevű cég volt az áldozat. Tavaly szeptemberben azután két olyan rosszindulatú programot fedeztek fel, amelyek érvényes Adobe kódtanúsítvánnyal álcázták magukat. Trendjelző – mutatnak rá a Kaspersky-nél --, hogy a hacker-eknek egy ekkora cég biztonsági háttere, az Adobe által használt speciális titkosító eszköz (hardware security module, HSM) sem jelentett akadályt.

Sérülékeny Java

A Kaspersky Lab felmérése szerint tavaly a második negyedévben a felhasználók 30 százalékának gépén régi, sebezhető Java változat működött. Ezzel a Java bízvást kiérdemelte a legelterjedtebb sérülékeny szoftver címet.

A Macintoshok körében dúló, *2.1.* pontban idézett Flashback járványt is egy nulladik napi Java sérülékenység váltotta ki. Válaszul az Apple merész lépésre szánta el magát: Mac OS X felhasználók millióinak a gépén letiltotta a Javát. Augusztusban egy másik nulladik napi Java rést kezdtek el tömegesen támadni a hacker-ek, világszerte több millió fertőzést okozva. Külön figyelemre méltó, hogy ez utóbbi sérülékenységet a már említett Blackhole kit segítségével aknázták ki.

Hálózati eszközök elleni támadások

Hardver is jelenthet legalább akkora biztonsági kockázatot, mint a nem frissített szoftver.

Mint a brazil CERT megállapította, a félkontinensnyi országban 4,5 millió DSL modemet törtek fel a hacker-ek. Októberben a Kaspersky Lab egy szakembere bemutatta: egyetlen firmware sérülékenységet kiaknázva, két rosszindulatú szkript és 40 rosszindulatú DNS szerver segítségével hónapokon át hat különböző gyártó modemeit tartották hatalmukban a támadók.

Sérülékenységet fedeztek fel Huawei router-ekben is. Az amerikai kormány egyenesen kémkedési kockázat miatt indított vizsgálatot az ügyben.

A DNSChanger helyettesítő szerverek lezárása

Tavaly július elején megkülönböztetett figyelem irányult azokra a gépekre, amelyek korábban a DNSChanger kártevőnek estek áldozatul. A kórokozó botnet-be szervezte a megtámadott gépeket (melyek számát a járvány csúcspontján 4 millióra becsülték), s módosította azok DNS beállításait. Így a szörfösök automatikusan valamilyen rosszindulatú site-on landoltak. 2011 novemberében az FBI lekapcsolta a botnet vezérlőszerverét, majd speciális DNS szervereket állított fel, amelyek a fertőzött gépek DNS-kéréseit helyesen oldották fel. A bíróság 2012. július 9-éig engedélyezte a szövetségieknek e helyettesítő szerverek üzemeltetését. Ha egy gépet a határidőre nem tisztítottak volna meg a kártevőtől, az DNS feloldás híján elvágta volna felhasználóit az internettől: sem email-t küldeni, sem a weben navigálni nem lehetett volna többé rajtuk.

Mindez azért keltett nagy aggodalmat, mert a DNSChanger szakmai munkacsoport (Working Group) felmérése szerint június végén még mindig 300 ezer gép hordozta a fertőzést, s félő volt, hogy ezek július 9-ével egy csapásra elvesztik internet-kapcsolatukat. Szerencsére azonban ügyfelei érdekében számos internetszolgáltató saját helyettesítő DNS szervert állított üzembe, s végül is nem következett be olyan tömeges leállás, amelytől többen is tartottak.

A történet példa értékű: kormányzat és a magánszektor együttesen, eredményesen lépett fel a kiberbűnözéssel szemben.

Shamoon és Wiper: Veszedelmes kártevők

Két kártevőt külön kiemel a tavaly felbukkant kórokozók sorából a Kaspersky Lab elemzése. Mindkettőt vállalatok működésének megbénítására tervezték. A Shamoon akkor híresült el, amikor augusztusban nem kevesebb, mint 30 ezer számítógépet tett tönkre a Saudi Aramco-nál, a világ egyik legnagyobb olajvállalatánál. A Shamoon tervezési koncepcióját látták felbukkanni a szakemberek a Wiper-nek keresztelt kártevő esetében is. Mindkét támadással kapcsolatban rengeteg még az ismeretlen tényező: nem tudni, pontosan hogyan fertőződtek meg a gépek, s főként, hogy kik álltak az akciók hátterében.

Ma(h)di kiberkémkedési akció

Madi vagy *Mahdi* az iszlám vallás megváltója. Összeállításunkban azért szerepel, mert egy rosszindulatú kódban gyakran előfordult ez a szó, s így a támadást elemző Kaspersky és Seculert szakértői ezt a nevet adták a kártevőnek.

A kórokozó 2011 második és a tavalyi év első felében szedte áldozatait, elsősorban Iránban, Izraelben és Afganisztánban, de a világ más tájain is. Nem volt különösebben kifinomult kártevő, ám ügyes csalijának köszönhetően mégis széles körű fertőzést okozott.

Megjelenése egyrészt aláhúzza: milyen erőteljes kiberkémkedési tevékenység folyik a Közel-Keleten, másfelől azt is bizonyítja: nemcsak egy nemzetállam korlátlan költségvetéséből, hanem kis pénzből is lehet sikeres kiberhadműveletet indítani.

És ami jön...

Mindaz, amit az elmúlt esztendő főbb jelenségeiről elmondtunk, már előrevetíti, mire számíthatunk az idén. Nyilván folytatódik, sőt fokozódik a kiberkémkedés, kiberhadviselés és -szabotázs, a nemzetállamok által nemzetállamok ellen indított informatikai hadműveletek sora. Újabb országok fejlesztenek ki kiberháborús eszközöket. Számíthatunk arra is, hogy a kormányok saját polgáraikkal – például bűnügyek gyanúsítottjaival – szemben is mind gyakrabban alkalmaznak – legalábbis ellentmondásosnak minősíthető – megfigyelő rendszereket.

Különösen a közösségi hálózatok széleskörű használata, az ellenük irányuló akciók következtében szűkülhet-sérülhet az egyén digitális magánszférája, adatainak biztonsága. A személyi adatok feketepiaci értéke nő, ugyanakkor többen veszthetik el bizalmukat az online szolgáltatások iránt. Fokozódó ostrom alá kerülnek a számítástechnikai felhők, amelyeket hatalmas és értékes adattartalmuk rendkívül kívánatossá tesz a kiberbűnözők számára.

Mint korábban rámutattunk, minden valószínűség szerint folytatódik az Andorid platform ellen indított akciók számának rohamos növekedése. Továbbra is a hacker-ek célkeresztjében marad a Java, miközben az Adobe Reader és Flash már nem olyan vonzó számukra, hiszen ezeket a szoftvereket automatikus mechanizmus frissíti.

A Kaspersky Lab az alábbi tízpontos előrejelzést állította össze a 2013-ra várható fontosabb IT biztonsági jelenségekről:

- Tovább szaporodnak a célzott támadások.
- Folytatódik a hacktivizmus, vagyis az ideológiai alapon álló hackertevékenység.
- Több lesz a nemzetállam által pénzelt kibertámadás.
- „Legális” IT megfigyelési eszközöket alkalmaznak kormányzati támogatással.
- Támadásokra kerül sor a felhő alapú infrastruktúra ellen.
- Szűkül a digitális magánszféra.
- Továbbra is ingatag lesz a bizalom az online szolgáltatások és a digitális hatósági funkciók iránt.
- Mind több kártevő irányul a Mac OS X és a mobil eszközök ellen.
- A számítógépes bűnözők továbbra is elsősorban sérülékenységek kiaknázásával igyekeznek elérni céljukat.
- Sok áldozatot szednek a „váltságdíjat” követelő és a titkosítással zsaroló kártevők.

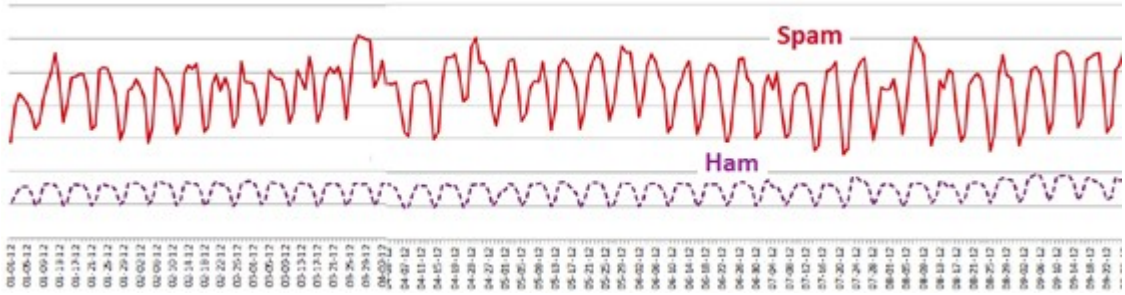
Spam és botnetek

A kártevők terjesztésének, az adathalászatnak az egyik fő eszköze a spam. A kéretlen levelek száma, a valódi emailekhez (szakzsargonban ham-hez) viszonyított aránya azonban ettől függetlenül is fontos jellemzője digitális környezetünk állapotának.

Lássuk hát, hogyan is állt a világ spam dolgában a tavalyi esztendőben! Erről a Commtouch negyedévenként kiadott *Internetes fenyegetés-trendjelentéséből (Internet Threats Trend Report)* igyekszünk képet adni.

A Commtouch két grafikonjából összeállított alábbi ábra 2012 első három negyedévében mutatja a spam és ham üzenetek számának alakulását. A vizsgált kilenc hónapban a levélszemét tömege átlagosan nagyjából állandó maradt. Napi szinten nagyjából 60 és 120 milliárd között ingadozott a kéretlen levelek száma.

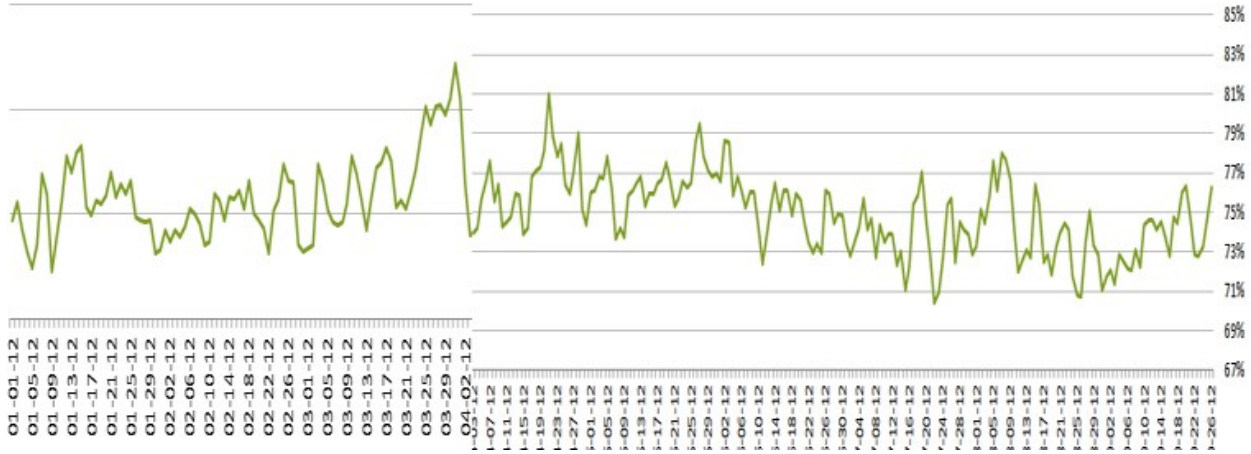
A spam és ham üzenetek száma a globális teljes email forgalomban 2012 első három negyedévében (milliárd darab)



(Forrás: Commtouch)

A következő, ugyancsak két Commtouch grafikonból összeillesztett ábra szerint a levélszemét részesedése a teljes email forgalomban az év közepe felé csúcsot ért el, ám az év elején és a harmadik negyedévben valamelyest csökkent. Az első három negyedévben a spam a levélvolumen 70-83%-át tette ki.

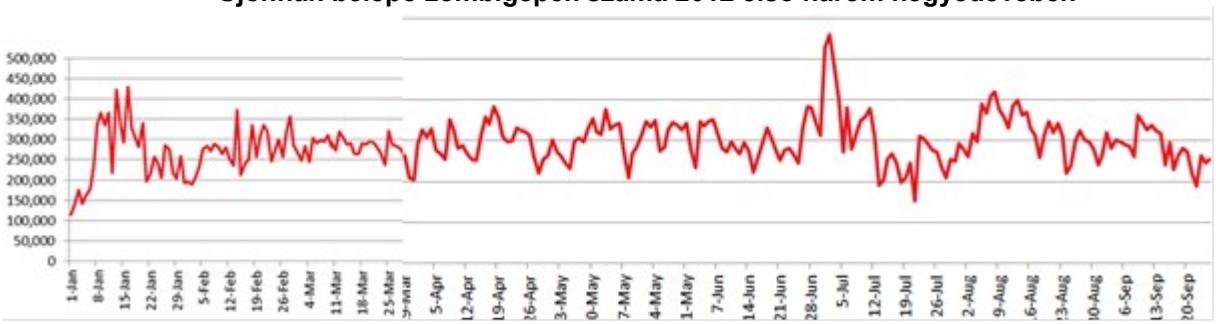
A spam százalékaránya a globális teljes email forgalomban 2012 első három negyedévében



(Forrás: Commtouch)

A spamszint nagymértékben attól függ: hány és mekkora botnet tevékenykedik, hány zombigép működik szerte a világban. Az első negyedévben átlagosan napról napra 270 ezer új zombi állt hadrendbe, kezdett spamet szórni – derül ki a Commtouch tanulmányából. Ez a szám sajnos a második-harmadik negyedévre némileg megemelkedett, 300 ezer fölé csúszott.

Újonnan belépő zombigépek száma 2012 első három negyedévében



(Forrás: Commtouch)

Feltétlenül ki kell emelnünk, milyen fontos szerepet játszott tavaly is a botnet-ek elleni harcban a Microsoft. Az első negyedév végén például két amerikai városban, összehangolt hadművelettel lekapcsolta a hírhedt ZeuS és SpyEye banki trójaiakat terjesztő botnet-ek vezérlőszervereit. A szoftveróriás világszerte 13 millió gépen észlelt ZeuS vagy SpyEye fertőzést; közülük 3 millió az Egyesült Államokban működött.

Alább táblázatosan adunk áttekintést a 2011-es utolsó, illetve a 2012-es első három negyedév főbb, spam-mel kapcsolatos statisztikai adatairól, ismét a Commtouch *Internetes fenyegetés-trendjelentései* alapján. Láthatólag a vizsgált időszakban senkinek nem sikerült elhódítania Indiától a legelzombisodottabb ország címét. Hasonlóan szilárdan tartja magát a gyógyszer, mint leggyakoribb spamtéma, s a Gmail, mint a spammer-ek által leggyakrabban feltüntetett (többnyire hamis) feladó domain.

Zombik és spam a Commtouch szerint			
2011. IV. né	2012. I. né	2012. II. né	2012. III. né
Aktivált zombi naponta (ezer)			
209	270	303	304

Legtöbb zombit adó országok			
India	India	India	India
Vietnam	Brazília	Brazília	Brazília
Pakisztán	Oroszország	Vietnam	Kína

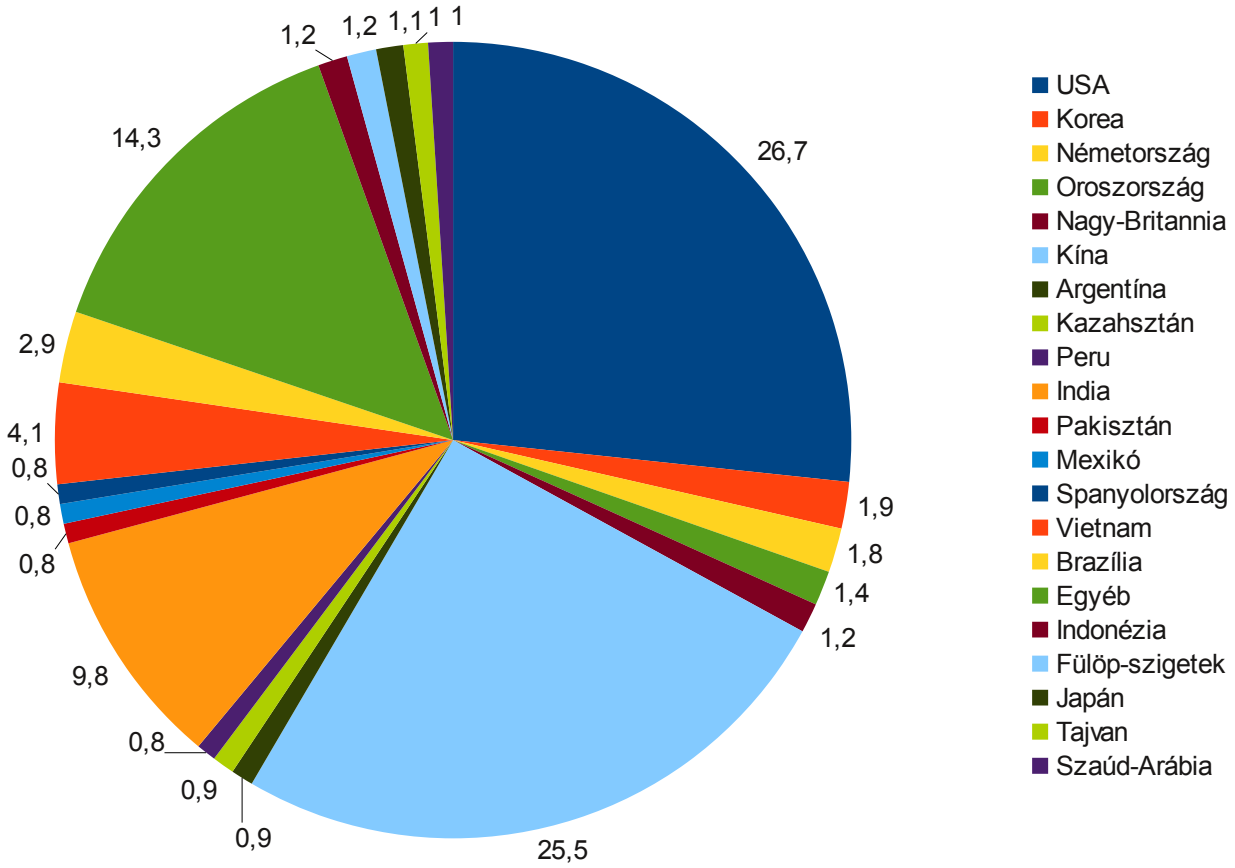
Spam ill. adathalász üzenetek átlagos száma naponta (milliárd)			
101	94	91	87

Leggyakrabban spam küldésre használt domainek			
gmail.com	gmail.com	gmail.com	gmail.com
yahoogroups.com	yahoo.com	yahoo.com	yahoo.com
yahoo.com	yahoogroups.com	yahoogroups.com	yahoo.co.jp
googlegroups.com	news.groupon.co.uk	att.net	facebookmail.com
yahoo.com.ph	facebookmail.com	googlegroups.com	fmt.com.tw

Zombik és spam a Commtouch szerint				
	2011. IV. né	2012. I. né	2012. II. né	2012. III. né
Legnépszerűbb spam témák				
Gyógyszer	31,2%	38,5%	41,2%	31,5%
Termékutánzatok	14,2%	18,9%	11,8%	6,4%
Szex segédeszköz	13,9%	10,5%	16,3%	25,8%
Társkereső	11,7%	8,3%	5,3%	8,3%
Pénzkérő	7,1%	4,1%	4,5%	4,7%
Adathalász	6,2%	4,2%	3,9%	3,8%
Fogyókúra	4,0%	2,1%	7,8%	7,9%
Pornó	3,5%	2,0%	3,0%	3,3%
Diploma	2,0%	0,8%	0,4%	2,4%
Szoftver	1,8%	5,2%	1,2%	1,2%
Egyéb	4,5%	4,5%	4,6%	4,7%

S hogy földrajzilag honnan küldték a legtöbb levélszemetet? Erről a Kaspersky Lab harmadik negyedévről készült kördiagramját adjuk közre.

Spamforrás országok a küldött üzenetek száma szerint, 2012 harmadik negyedévében



(Forrás: Kaspersky Lab)

Kiemelkedő kártevők

Korábban már szóltunk a tavalyi esztendő legfontosabb, trendjelzőnek mondható rosszindulatú programjairól. Természetesen azonban nem az ott említett kórokozók bosszantották leggyakrabban a hétköznapi felhasználókat. Alábbi toplistáinkból az derül ki: mely kártevőket mutatta ki leggyakrabban a világhálón a Commtouch antivírus laboratóriuma.

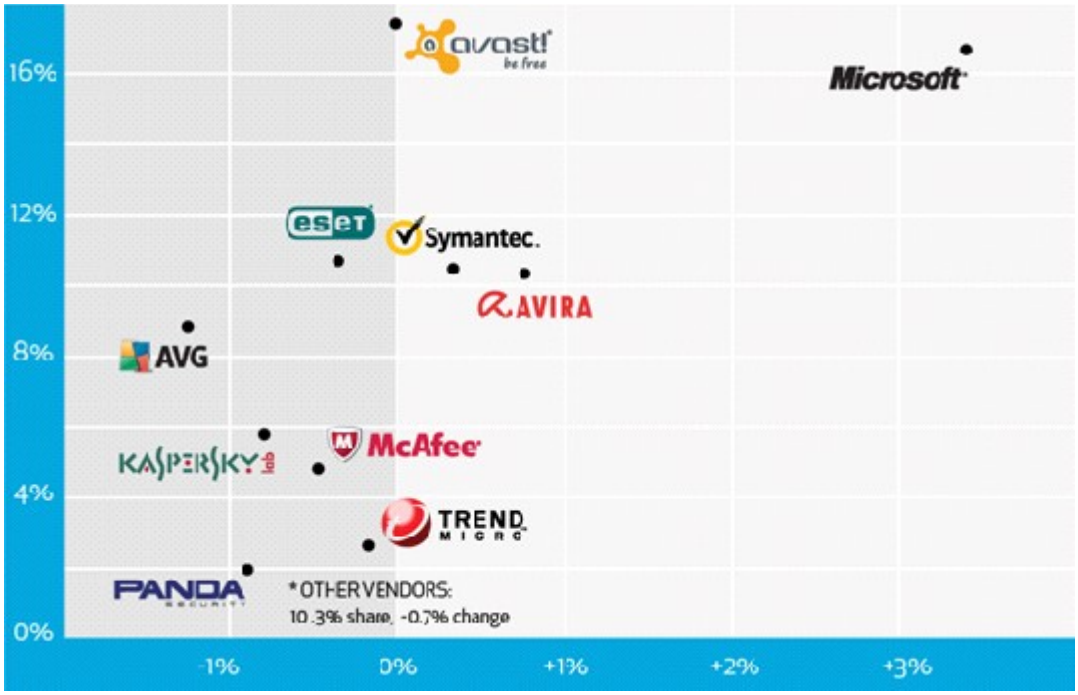
2012 I. negyedév		*2012 II. negyedév*
1. W32/InstallCore.A2.gen!Eldorado	1.	1. W32/RLPacked.A.gen!Eldorado
2. W32/RLPacked.A.gen!Eldorado	2.	2. W32/InstallCore.A2.gen!Eldorado
3. W32/Sality.C.gen!Eldorado	3.	3. W32/Sality.C.gen!Eldorado
4. W32/Heuristic-210!Eldorado	4.	4. W32/HotBar.L.gen!Eldorado
5. W32/RAHack.A.gen!Eldorado	5.	5. W32/Heuristic-210!Eldorado
6. W32/Sality.gen2	6.	6. W32/Sality.gen2
7. W32/HotBar.L.gen!Eldorado	7.	7. W32/RAHack.A.gen!Eldorado
8. W32/Vobfus.AD.gen!Eldorado	8.	8. W32/OnlineGames.FL.gen!Eldorado
9. JS/Pdfka.CI.gen	9.	9. W32/Vobfus.AD.gen!Eldorado
10. W32/Korgo.V	10.	10. JS/Pdfka.EV.gen

	2012 III. negyedév
1.	1. SWF-malform-1
2.	2. W32/Ramnit.Q
3.	3. W32/Conficker!Generic
4.	4. W32/Mabezat.A-2
5.	5. W32/Agent.PJ.gen!Eldorado
6.	6. CVE-2010-3333
7.	7. W32/MyWeb.D@adw
8.	8. W32/Injector.A.gen!Eldorado
9.	9. W32/Mabezat.A-1
10.	10. W32/Tenga.3666

Miközben a kártevőírók lankadatlanul ontották rosszindulatú alkotásaikat, hogyan alakult a különféle vírusirtók piaci részesedése a nemzetközi porondon? Erről az OPSWAT negyedéves statisztikáinak legutóbbi, decemberi kiadásából tájékozódhatunk. Az adatok a cég AppRemover elnevezésű, ingyenesen letölthető eszközétől származnak, s az idézett jelentés több mint 150 ezer gép beküldött információi alapján készült.

A következő ábrán az OPSWAT a teljes világpiaci részesedés (függőleges tengely) és az utolsó félévben a részesedésben bekövetkezett változás (vízszintes tengely) koordinátarendszerében helyezte el a szállítókat. Láthatóan a félév nagy nyertese a Microsoft, s nem panaszkodhat az Avira sem.

Antivírus termékek gyártóinak világpiaci részesedése (függőleges tengely) és e részesedés változása 2012 második félévében



(Forrás: OPSWAT)

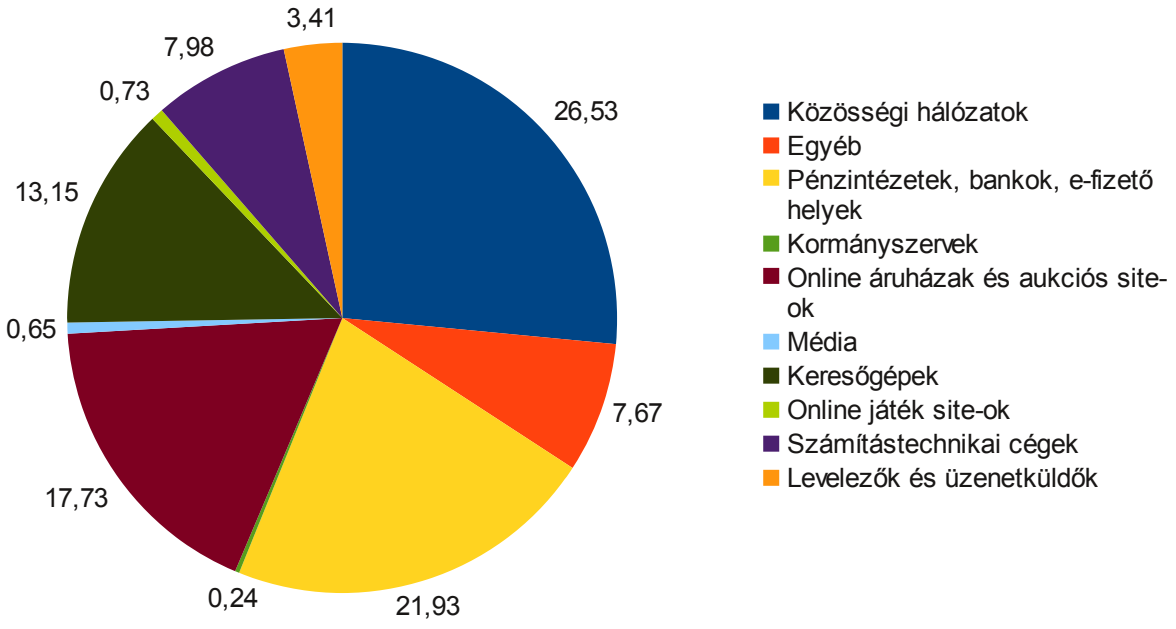
Jó tudnunk, hogy a weben barangolva hol kell leginkább fertőzéstől vagy adathalászattól tartanunk. Erre vonatkozóan a Commtouch már idézett *Internetes fenyegetés-trendjelentése* ad eligazítást. Következő táblázatainkat a cég a 2011-es utolsó, illetve a 2012-es első három negyedévet feldolgozó statisztikáiból állítottuk össze. Eszerint (gyakorisági sorrendben) a következő site-kategóriákon bújtattak meg a bűnözők valamilyen kártevőt vagy adathalász csapdát. Hangsúlyoznunk kell, hogy szinte mindig „ártatlan” site-okról van szó, azaz a bűnözők a site tulajdonosának, üzemeltetőjének tudta nélkül állítják a szervereket sötét céljaik szolgálatába.

	A kártevőket leggyakrabban terjesztő site-kategóriák a Commtouch szerint			
	2011. IV. né	2012. I. né	2012. II. né	2012. III. né
1.	parkolt domainek	pornó/szex	oktatás	oktatás
2.	portálok	parkolt domainek	utazás	áruház
3.	pornó/szex	divat/szépség	céges	sport
4.	oktatás	portálok	szórakoztatás	céges
5.	céges	szórakoztatás	éttermek, étkezés	szórakoztatás
6.	szórakoztatás	oktatás	sport	éttermek, étkezés
7.	áruház	egészségügy	szabadidő	utazás
8.	egészségügy	IT/technológia	egészségügy	egészségügy
9.	utazás	céges	divat/szépség	streaming m., letöltés
10.	IT/technológia	szabadidő	streaming m. letöltés	szabadidő

	Adathalászattal leggyakrabban fenyegető site-kategóriák a Commtouch szerint			
	2011. IV. né	2012. I. né	2012. II. né	2012. III. né
1.	játék	portálok	portálok	játék
2.	portálok	áruház	divat/szépség	portálok
3.	áruház	divat/szépség	sport	áruház
4.	oktatás	oktatás	áruház	oktatás
5.	divat/szépség	céges	oktatás	divat/szépség
6.	sport	sport	céges	sport
7.	céges	szabadidő	művészet	céges
8.	szabadidő	egészségügy	streaming m. letöltés	szabadidő
9.	szórakoztatás	ingatlan	IT/technológia	szórakoztatás
10.	ingatlan	személyes site-ok	utazás	ingatlan

Nem érdektelen az sem, milyen vállalatok, vállalkozások, szervezetek virtuális háza táján halásznak leggyakrabban adatokra az orvhalászok. Logikusan ott kutakodnak, ahonnan belépési azonosítókat, személyi adatokat, közvetlenül vagy közvetve pénzt remélhetnek.

Adathalászok célkeresztjében leggyakrabban megjelenő cégek, szervezetek 2012 harmadik negyedévében



(Forrás: Kaspersky Lab)

Megjegyezzük, hogy tavaly decemberben a hazai bankok ügyfeleire is kivetették hálójukat a bűnözők. Az OTPdirekt belépő oldalán például a következő üzenet fogadhatta a látogatót:

„A számítógépes hacker-ek Európában és most már hazánkban is egy új módszerrel próbálják meg a banki ügyfelek számláit jogtalanul megterhelni. A bűnözők a nem megfelelő védelemmel rendelkező ügyfelek számítógépe, okostelefonja felett egy kémprogram segítségével átveszik a teljes irányítást. Miután az ügyfél bejelentkezik az internetbankba, egy adategyeztetésre felhívó és az ügyfél türelmét kérő üzenetet jelenítenek meg, miközben a háttérben jogosulatlan pénzátutalásokat kezdeményeznek..."

Védekezésül az OTP Bank 2013. január 1-jével minden, a legkisebb értékű tranzakcióra is kötelezővé tette a mobil aláírást.

Folt hátán folt

A szoftvercégeknek a 2012-es esztendőben is bőven volt foltoznivalójuk. Persze nem lehet eléggé hangsúlyozni, hogy minden folt hiábavaló, ha a felhasználók nem telepítik. A Kaspersky Lab november elején arról számolt be, hogy minden sérülékeny gépen átlagosan nyolc különböző sebezhetőséget találtak. Leggyakrabban a Javán tátongott rés. A tízes toplistába még öt Adobe és két Apple termék (a QuickTime és az iTunes), valamint a Nullsoft Winamp médialejátszó került be. Fontos fejlemény ugyanakkor, hogy – a Windows automatikus frissítési mechanizmusának köszönhetően – már egyetlen Microsoft termék sem szerepelt a tíz leggyakrabban sebezhető termék között.

Tanulmányunk végén a következőkben röviden, időrendben az év legfontosabb biztonsági frissítéseit tekintjük át.

Január

- Havi foltozó keddjén nyolc rés betömésére összesen hét javítócsomagot bocsátott ki a Microsoft. Közülük 1 kritikus, a fennmaradó 6 fontos minősítést kapott. A kritikus javítás a Windows Media Playerhez készült.
- Elkészült az Adobe Acrobat és Reader 10.1.2 és 9.5 jelű változata. A frissítés a 10.1.1 és 9.4.7 verziók kritikus hibáit is javította.
- Januári kritikus foltozó napján (Critical Patch Update, CPU) nem kevesebb, mint 78 biztonsági frissítéssel jelentkezett az Oracle. Tizenhat sérülékenység a távolból, autentikáció nélkül is kiaknázható volt. A foltok számos Oracle terméket érintettek, köztük a 10g és a 11g jelű adatbáziskezelőt, a Fusion Middleware 11g-t, a 10g jelű alkalmazásszervert vagy a MySQL Servert.
- Feljebb tekerte a Chrome verziószámlálóját a Google. A 16.0.912.77-es kiadás négy súlyos sérülékenységet is orvosolt.
- Új változattal rukkolt ki a Mozilla is. Frissült a Firefox, a Thunderbird és a SeaMonkey csomag is. A Firefox 10.0 összesen nyolc rést tömött be a böngészőn, melyek közül ötöt kritikusnak minősítettek.

Február

- Kilenc javítócsomag – köztük 4 kritikus és 5 fontos – volt a februári foltozó kedd mérlege. A szoftveróriás összesen 21 sérülékenységet orvosolt, egyebek mellett az Internet Explorerben és a C futásidejű könyvtárban. A cég megragadta az alkalmat, hogy megemlékezzék arról: 10 évvel azelőtt jelent meg *Bill Gatesnek* az a feljegyzése, amely a biztonságot állította a Microsoft fejlesztés és támogatás középpontjába.

- Hét lyukat tömött be a Flash Player frissítésével az Adobe. Kilenc kritikus sérülékenységet szüntetett meg a cég a Shockwave Playerben is.
- Összesen 20 biztonsági problémát oldott meg a Google a Chrome 17-es verziójának kibocsátásával. Az új böngésző letöltés előtt egybeveti a kijelölt file-t egy feketelistával, így hathatósan véd rosszindulatú állományok, például hamis antivírus termékek letöltése ellen.
- A Mozilla egy kritikus hiba javítása kedvéért a Firefox és a Thunderbird verziószámát 10.0.1-re, a SeaMonkeyét 2.7.1-re emelte.

Március

- Összesen hat – 1 kritikus, 4 fontos és 1 mérsékelten fontos – javítócsomagot bocsátott ki menetrendszerű frissítési napján a Microsoft. Ezek a Windows, a Visual Studio és az Expression Design együttesen hét sérülékenységét orvosolták.
- Biztonsági javítást kapott az Adobe Flash Player. Emellett a cég bevezette a Flash csomagok automatikus frissítését.
- Márciusban, egyetlen hónap leforgása alatt háromszor bocsátott ki új Chrome változatot a Google. Először a 17.0.963.65-ös tizenhét, majd a 17.0.963.83-as verzió kilenc rést tömött be. Ezt követte a 18-as sorozat első tagja, a 18.0.1025.142, amely kilenc (köztük hat súlyos) sérülékenységet orvosolt.
- Előrébb lépett a Mozilla Firefox, Thunderbird és SeaMonkey verziószáma is. Az előbbi kettőből a 11-es, az utóbbiból a 2.8-as került a felhasználókhoz, természetesen biztonsági javításokkal.
- Windows és Mac OS X platformon is frissítette a Safarit az Apple. Az új, 5.1.4-es változat több mint 80 rést szüntetett meg a böngészőn.

Április

- Havi foltozó keddjén hat 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: 2014 áprilisában megszűnik a Windows XP és az Office 2003 támogatása.
- Google Chrome-ba integrált Flash Player-ének 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 az rá irányuló támadások.

Május

- Rendszeres havi frissítési ciklusa keretében a Microsoft összesen hét – 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

- Júniusi foltozó keddjén hét 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.

Július

- Havi foltozó keddjén kilenc javítócsomagot bocsátott ki a Microsoft. Közülük 3 kritikus, 6 pedig fontos besorolást kapott. A foltok összesen 16 rést fednek be a következő termékekben: Windows, Internet Explorer, Visual Basic for Applications, Office.
- Menetrendszerű javító frissítés-csomagjával jelentkezett az Oracle. Az érintett termékek, illetve termékcsaládok: Database, Fusion Middleware, Enterprise Manager, E-Business Suite, Supply Chain, PeopleSoft, Siebel, Health Sciences, Oracle Sun Product Suite, MySQL Server.
- Megjelent a Google Chrome böngészőjének 21-es kiadása, amely több biztonsági problémát is orvosolt.
- Biztonsági frissítések érkeztek az Apple-től. Az új termékverziók: Xcode 4.4, Safari 6.0.

Augusztus

- Rendszeres havi frissítési ciklusa keretében a Microsoft összesen kilenc – 5 kritikus és 4 fontos besorolású – javítócsomaggal jelentkezett, melyek összesen 26 sérülékenységet orvosolnak. Az érintett termékek: Windows, Internet Explorer, Exchange Server, SQL Server, szerverszoftver, Developer Tools, Office.
- Megérkezett a foltozó keddhez igazított menetrendszerű frissítés az Adobe-tól. Az új verziók: Reader X (10.1.4), Reader 9.5.2, Shockwave Player 11.6.6.636, Flash Player 11.3.300.271 (Windows, Macintosh) és 11.2.202.238 (Linux). A hónap folyamán később még egy frissítést kapott a Flash Player és folt került a Photoshop CS6-ra is.

- Soron kívül javított egy sérülékenységet adatbázis-szerverében az Oracle. A rést az előző havi Las Vegas-i Black Hat konferencián demonstrálták.
- Háromszor is feljebb lépett augusztusban a Google Chrome verziószámlálója. Mindannyiszor biztonsági problémákat is javítottak. A hónap végén a böngésző legfrissebb stabil kiadása Windows, Macintosh és Linux platformon egyaránt a 21.0.1180.89 számot viselte.
- Biztonsági frissítést kapott az Apple Remote Desktop. Az új verzió: 3.6.1.

Szeptember

- A hónap foltozó keddjén két biztonsági frissítés látott napvilágot a Microsoftnál, mindkettő fontos besorolással. Az érintett termékek: Visual Studio Team Foundation Server, System Center Configuration Manager.
- Szeptember vége felé soron kívüli foltot tett a Microsoft az Internet Explorer 9-es és korábbi verzióinak sérülékenységére, amelyet már támadni kezdtek a hacker-ek.
- Megjelent a Google Chrome biztonsági javításokat is tartalmazó 22-es változata. A keresőóriás ismét emelte a hibák bejelentőinek kifizethető jutalmat. A 22-es verzióban kijavított sérülékenységek közül egy 10 ezer, kettő pedig 5-5 ezer dollárt ért.
- Egy sor Apple szoftver kapott biztonsági frissítést. Az új verziók: Apple TV 5.1, OS X Server v2.1.1, Safari 6.0.1, OS X Mountain Lion v10.8.2, OS X Lion v10.7.5, iOS 6, Apple Remote Desktop 3.5.3, iTunes 10.7.

Október

- Októberi foltozó keddjén hét – 1 kritikus és 6 fontos minősítésű – biztonsági frissítést bocsátott ki a Microsoft. Az összesen 20 folt a Windows, az SQL Server és az Office réseit fedte le.
- Biztonsági frissítést kapott a hónap elején minden platformon az Adobe Flash Player, a hónap vége felé pedig a Shockwave Playerre került folt.
- Egy sérülékenység kijavítása miatt 16-ról 16.0.1-re léptette a Mozilla a Firefox változatszámlálóját.
- Kétszer is kapott biztonsági problémákat is orvosló változatfrissítést a Google Chrome. A keresőóriás az októberi, Kuala Lumpurban rendezett HITBSecConf2012 konferencia alkalmából Pwnium 2 néven egynapos bajnokságot írt ki a Windows 7 alatt futó Chrome feltörésére. A 60 ezer dolláros díjat egy kritikus sérülékenységért, illetve kiaknázásáért a *Pinkie Pie* fedőnéven indult versenyző nyerte.
- A Mac OS X környezetben foltozta a Javát az Apple.
- Októberi kritikus foltozó napján összesen 109 rést tömött be különböző termékein az Oracle. Egyebek mellett az adatbázis, a Fusion Middleware, a Peoplesoft Enterprise család, a Sun Product Suite, a MySQL Server és az E-Business Suite kapott javítást.

November

- A havi foltozó kedd termése hat biztonsági frissítés. Közülük 4 kritikus, 1 fontos, 1 pedig mérsékelten fontos minősítést kapott. Az összesen 19 folt a Windows Shell, a Windows Kernel, az Internet Explorer, az Internet Information Services (IIS), a .NET keretrendszer és az Excel sérülékenységeit javította.

- Újabb biztonsági frissítésen esett át az Adobe Flash Player, minden platformon.
- Megjelent a Firefox böngésző 17-es kiadása, amellyel számos biztonsági problémát is orvosolt a Mozilla.
- A hónap elején új verzióval rukkolt ki a Google Chrome csapat is. A 23-as kiadás szintén betömött réseket is. A sérülékenységek bejelentőinek összesen 9 ezer dollár jutalom ütötte a markát. November végén azután kétszer egymás után ismét frissült a böngésző. A két alkalommal közel 10 ezer dollárt osztottak ki a résvadászoknak, köztük az októberben említett *Pinkie Pie*-nak.
- Az iOS 6.0.1-e s kibocsátásával indította a novembert az Apple.

December

- Hét biztonsági frissítéssel a Windows, az Internet Explorer, a Word és a Windows Server összesen 12 rését tömte be menetrendszerű foltozó napján a Microsoft. A javítócsomagok közül 5 kritikus, a fennmaradó 2 fontos besorolást kapott. December 29-ei bejelentés szerint azután – kis számban ugyan – célzott támadások indultak az Internet Explorer 6-os, 7-es és 8-as változata ellen. A kritikus hibát az év utolsó napján orvosolta a szoftveróriás.
- Sérülékenységeket javított a ColdFusion-ön és a Flash Player-en az Adobe.
- Minden platformon előrébb léptette a Chrome verziószámlálóját a Google. A 23.0.1271.97 jelű verzió kibocsátásával javított sérülékenységek bejelentői 4500 dollár jutalmat kaptak.

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:

Email:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937