Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2013. I. negyedéves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető....3
A PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ tevékenysége számokban....4
Szoftver sérülékenységek....4
Internetbiztonsági incidensek....6
Informatikai biztonság 2013....7
Lakossági eszközellátottság: internet- és PC-használat....7
Az IT-biztonság kihívásai a lakossági szektorban....22
Social engineering, mint alábecsült veszély....39
Összefoglaló 2013 első negyedévének IT biztonsági trendjeiről....45
Biztonság – felülnézetből....45
Kémek, katonák....47
Szüntelen szennyáradat....49
Kiemelkedő kártevők....52
Folt hátán folt....58
Elérhetőségeink....62

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2013. I. negyedéves jelentését, amely a negyedév legfontosabb IT- és hálózatbiztonsági momentumait gyűjti egybe és értékelést ad ezen technikai információk társadalmi és gazdasági hatásainak vonatkozásában az Információs Társadalomért Alapítvány közreműködésével, valamint bemutatja a negyedév 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 felhasználókat (home user) 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, értékek és kimutatások a PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ, mint Nemzeti Kapcsolati Pont hazai és nemzetközi kapcsolatai által szolgáltatott hiteles és aktuális információkon alapulnak.

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

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

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

Dr. Kőhalmi Zsolt
Puskás Tivadar Közalapítvány
a kuratórium elnöke

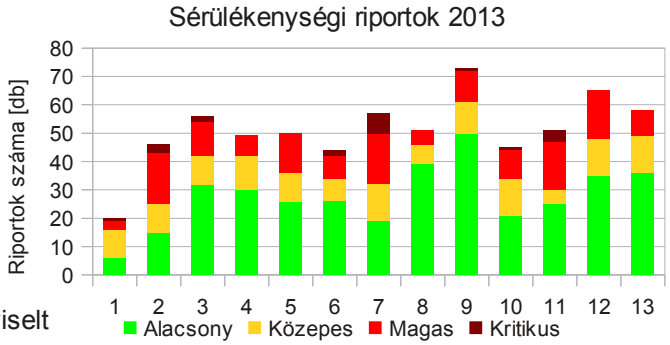
Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

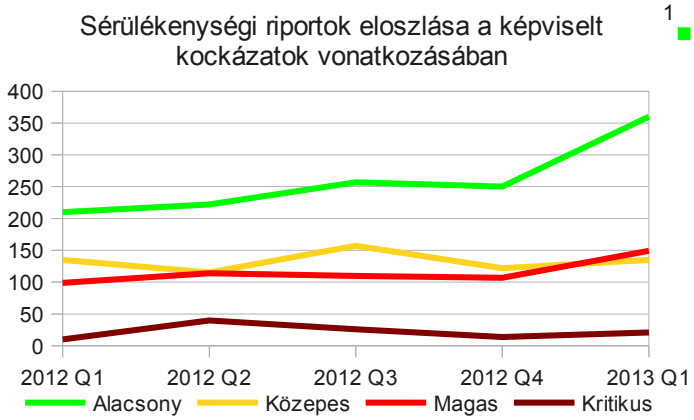
A PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ tevékenysége számokban

Szoftver sérülékenységek

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

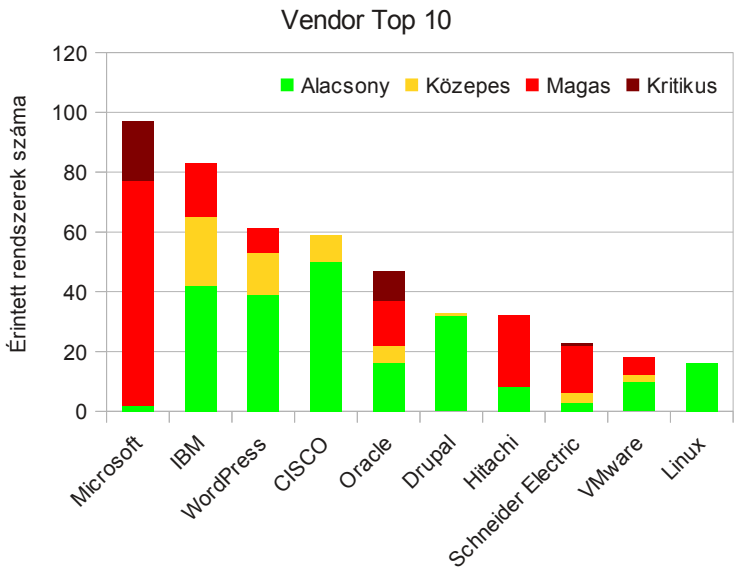
A **PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ (NHBK)** 2013 I. negyedéve során 665 **db szoftversérülékenységi információt** publikált, amelyekből 360 db alacsony, 135 db közepes, 149 db magas és 21 db kritikus kockázati besorolású.





Az elmúlt negyedév azonos időszakait vizsgálva elmondható, hogy az alacsony kockázati besorolással bíró szoftver sérülékenységek száma jelentősen nőtt. Ez magyarázható például azzal, hogy a gyártók sokkal nagyobb figyelmet fordítanak a kódok megírására, amit alátámasztanak az informatikával foglalkozó weboldalak és blogok cikkei, melyek szerint egyre több gyártó sandbox technikát használ a szoftvere fejlesztése során. A sandbox technika egy olyan biztonsági mechanizmus, amely a futó programokat és/vagy folyamatokat választja szét.

Gyakran használják nem tesztelt kódok futtatására, nem megbízható programok, alkalmazások futtatására is. A szoftverek fejlesztői által használt sandbox technika azt jelenti, hogy a program egyes részei ezen a sandbox-on belül maradnak, azaz magával az operációs rendszerrel nem lépnek közvetlenül kapcsolatba, így a kritikus folyamatok viszonylagos biztonságban vannak az egyes támadásoktól.

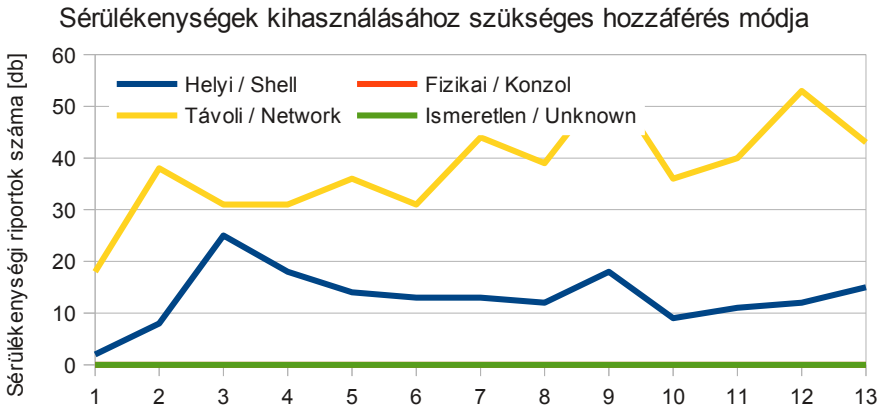


2013. I negyedévében is az érintett rendszerek száma szerint a Microsoft áll az első helyen. Ez azzal magyarázható, hogy a Microsoft világszerte a használt operációs rendszerek és szoftverek tekintetében kimagasló helyen áll. Ebben a negyedévben is folytatódni látszik a CMS (Content Management System), azaz tartalomkezelő rendszereket érintő szoftversérülékenységek számottevő jelenléte, mind core szinten, mind pedig a hozzájuk tartozó bővítmények szintjén.

Érdemes megemlíteni, hogy 2013. I negyedévében az érintett rendszerek száma szerint a TOP 10-be kerültek a Linux rendszerek sérülékenységei. Ez magyarázható például azzal, hogy nagyobb gyártók szoftverei egyre jobban integrálódnak a Linux rendszerekbe, így ezen szoftverek sérülékenységei ezeket a rendszereket is érinti.

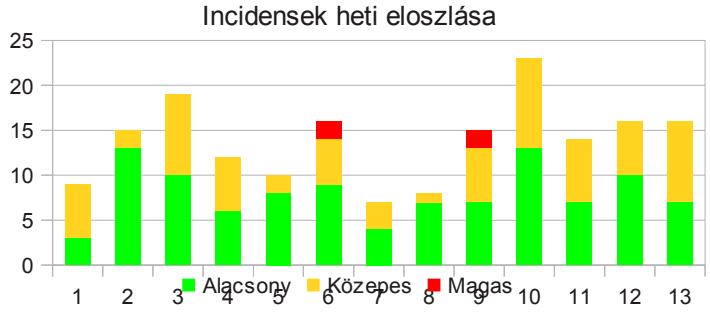
Nem mehetünk el ezen negyedévben amellett sem, hogy a SCADA (Supervisory Control And Data Acquisition) rendszereket is egyre nagyobb számban érintik a különböző szoftverek sérülékenységei. Ezek olyan számítógépes rendszerek, melyek segítségével monitorozhatóak és vezérelhetőek az infrastruktúrák és/vagy folyamatok.

A sérülékenységek sikeres kihasználásához szükséges hozzáférés tekintetében 2013. I. negyedéve sem mutat változást, azaz még mindig a távoli kapcsolaton keresztül kihasználható sérülékenységek száma a legmagasabb (közel 75%).



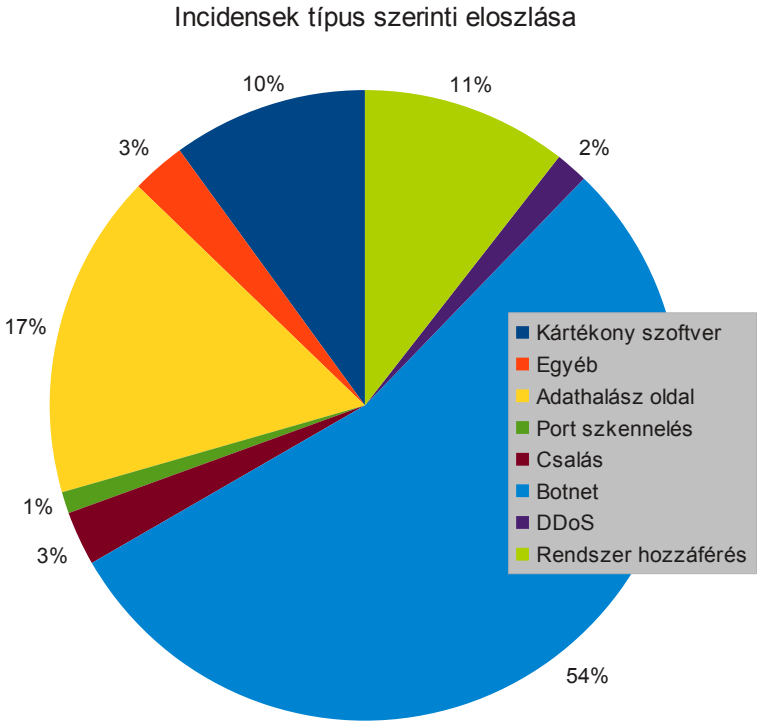
Internetbiztonsági incidensek

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 harmadik negyedévében **180 db incidens bejelentést** regisztrált és kezelt, ebből 104 db alacsony, 72 db közepes és 4 magas kockázati besorolású.

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



2013. I. negyedévében az incidensek típus szerinti eloszlásában az előző negyedévhez képest botnet hálózatok részét képező megfertőzött számítógépek kapcsán fogadott bejelentések száma 20%-kal tovább növekedett. Megjegyzendő, hogy ezek az adatok nem tartalmazzák Shadowserver Foundation-től be-érkező bejelentéseket. A botnet bejelentések közt, egyre növekszik a azon incidensek száma, mely sérülékeny tartalomkezelő rend-szerek által kompromittált web-oldalakat riportolnak, mint botnet végpont. Ezt azt jelenti, hogy a botnet-eket üzemeltető bűnözők már nem (csak) kéretlen levelek küldésére akarják felhasználni a kiépített botnet hálózataikat. Több botnet bejelentés köthető az elmúlt hónapokban a médiában is megjelent amerikai bankok ellen indított DDoS (elosztott szolgáltatás megtagadás) támadásokhoz.

2013. I negyedévében a botnet bejelentések mellett jelentős számban érkeztek a felhasználók megtévesztésén alapuló a banki és egyéb bejelentkezési adatok megszerzését célzó, adathalász tevékenységekről szóló incidens bejelentések, továbbá jelentős számban érkeztek rendszer hozzáféréssel kapcsolatos incidens riportok is. Az adathalászat és a rendszerhozzáférések a negyedév során kezelt bejelentések közel 28%-át teszik ki.

Kisebb derűre ad okot, hogy a negyedév során jelentősen csökkentek a kártékony kódot tartalmazó káros szoftver bejelentések.

Informatikai biztonság 2013.

Az első negyedév eseményei - Fókuszban a lakossági szektor

Az informatikai sérülékenységek, informatikai biztonsági kérdések meghatározó módon hatnak a nemzetgazdaság három fő csoportjára: a háztartásokra, a vállalati szektorra és a közszférára is. Azonban minden célcsoport mást és mást tapasztal ezekből a kockázatokból, incidensekből, más a felkészültségük, és ha fel akarjuk kelteni a figyelmüket és rá akarjuk bírni őket a szükséges intézkedésekre, minden egyes célcsoportot másképp kell megszólítani.

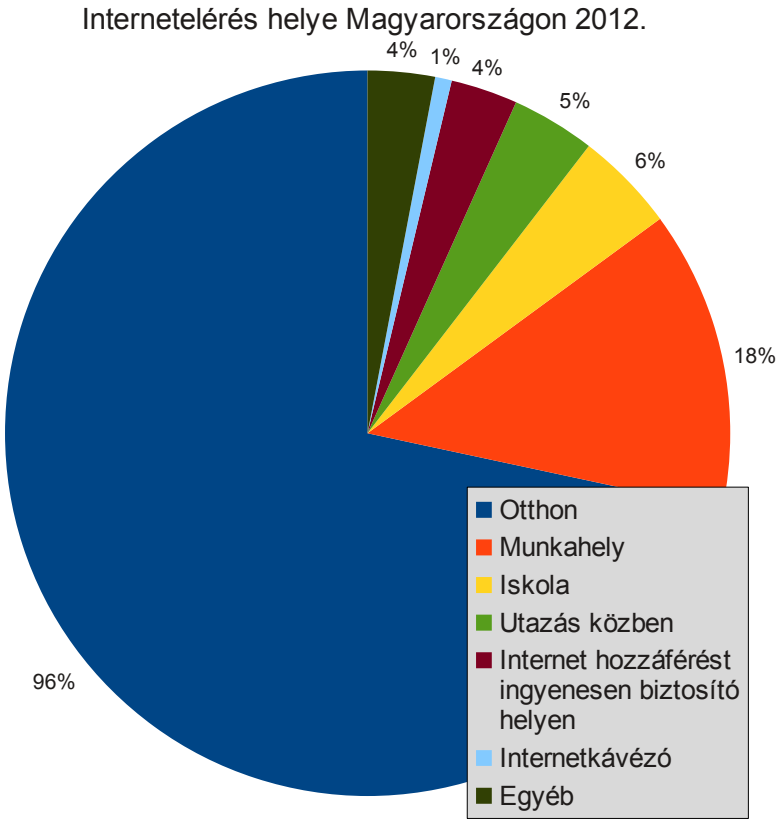
A 2013-as év első negyedévének fókuszcsoportja a háztartások, vagyis a home user tulajdonságait, lehetőségeit górcső alá véve, az őket érintő problémákat kiemelve, az ő jellegzetességeiket bemutatva áll össze a negyedév informatikai sérülékenységi összképe.

Lakossági eszközellátottság: internet- és PC-használat

A lakossági internetpiac

A 18 éves és idősebb lakosság közel kétharmada szokott internetezni 63% . Az internetezők szinte mindegyike internetezik otthon (96%), s majdnem minden ötödik közülük a munkahelyén is hozzáfér az internethez (18%). Az internet-hozzáférést ingyenesen biztosító helyeken az internetezők alig 4 %-a internetezik. Az internetkávézók részesedése csupán az ötöde (1%) a mobilinternetet használókhoz képest (utazás közben az internetezők 5 %-a internetezik).

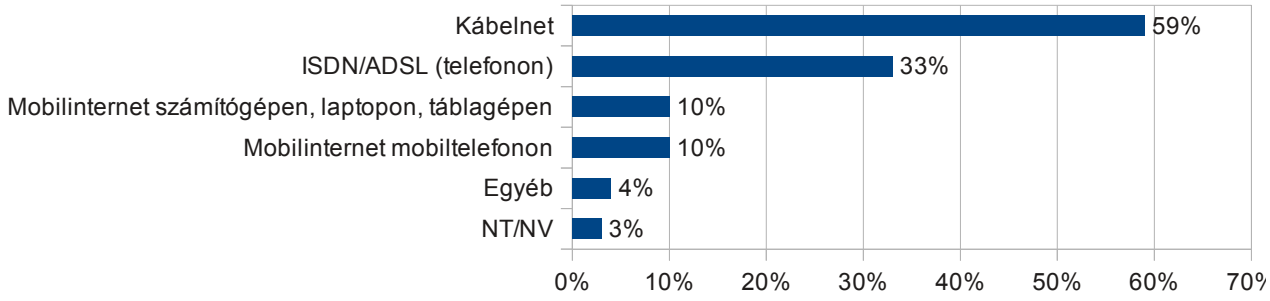
Forrás: Bellresearch[1]



1 Bellresearch: Magyar Infokommunikációs Jelentés 2012.

A legjellemzőbb otthoni internet a kábelnet, ami a 15 éves és idősebb online válaszadók által képviselt háztartások 59%-ában jelen van. Az ISDN/ADSL penetráció ennek alig több, mint fele (33%), míg a mobilinternet számítógépen és mobiltelefonon használva is a háztartások 10-10%-ában van jelen.

Lakossági internetelérés típusa Magyarországon 2012.



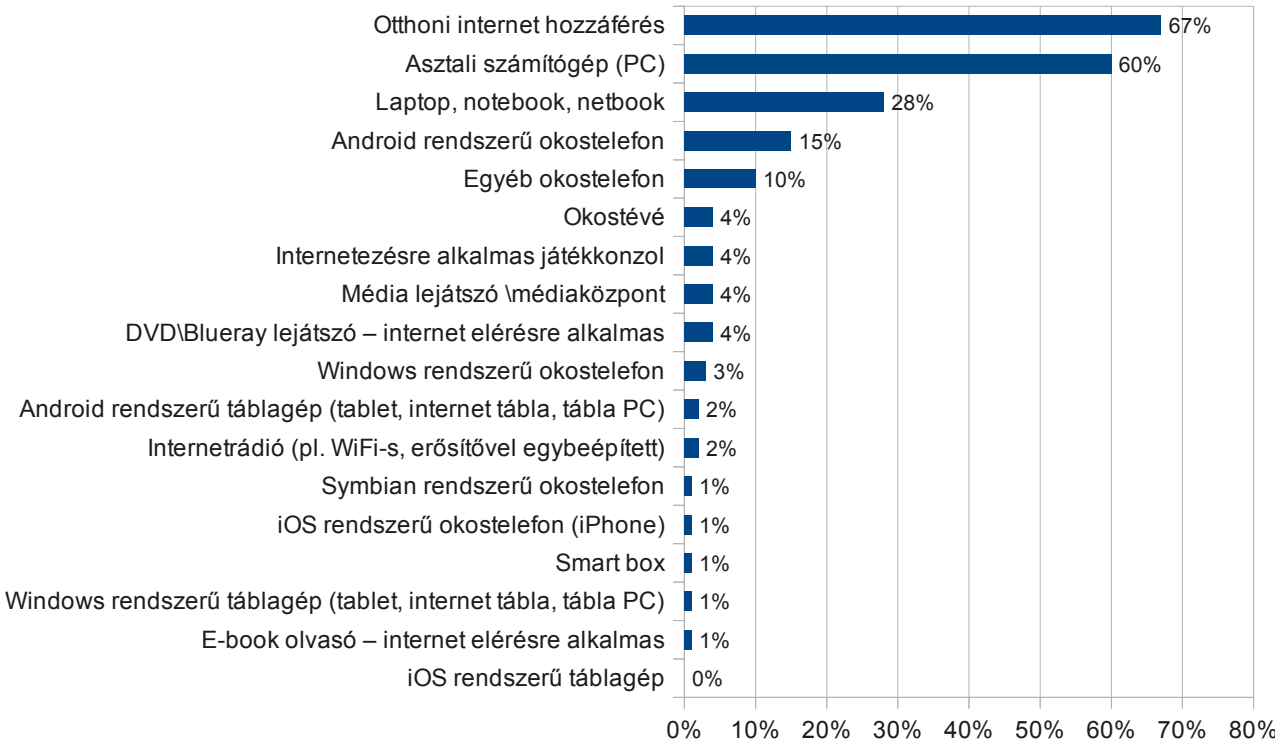
Forrás: NMHH[2]

Eszköz-ellátottság

A lakosság számára a legáltalánosabb telekommunikációs csatorna a televízió, ami gyakorlatilag minden magyar felnőtt otthonában jelen van. A 18 éven felüliek háromnegyede pedig otthoni internet hozzáféréssel is rendelkezik.

Okostelefon minden negyedik háztartásban van jelen, az okostelevíziók és táblagépek penetrációja 4-4%.

Lakossági eszköz ellátottság Magyarországon 2012.



Forrás: NMHH[2]

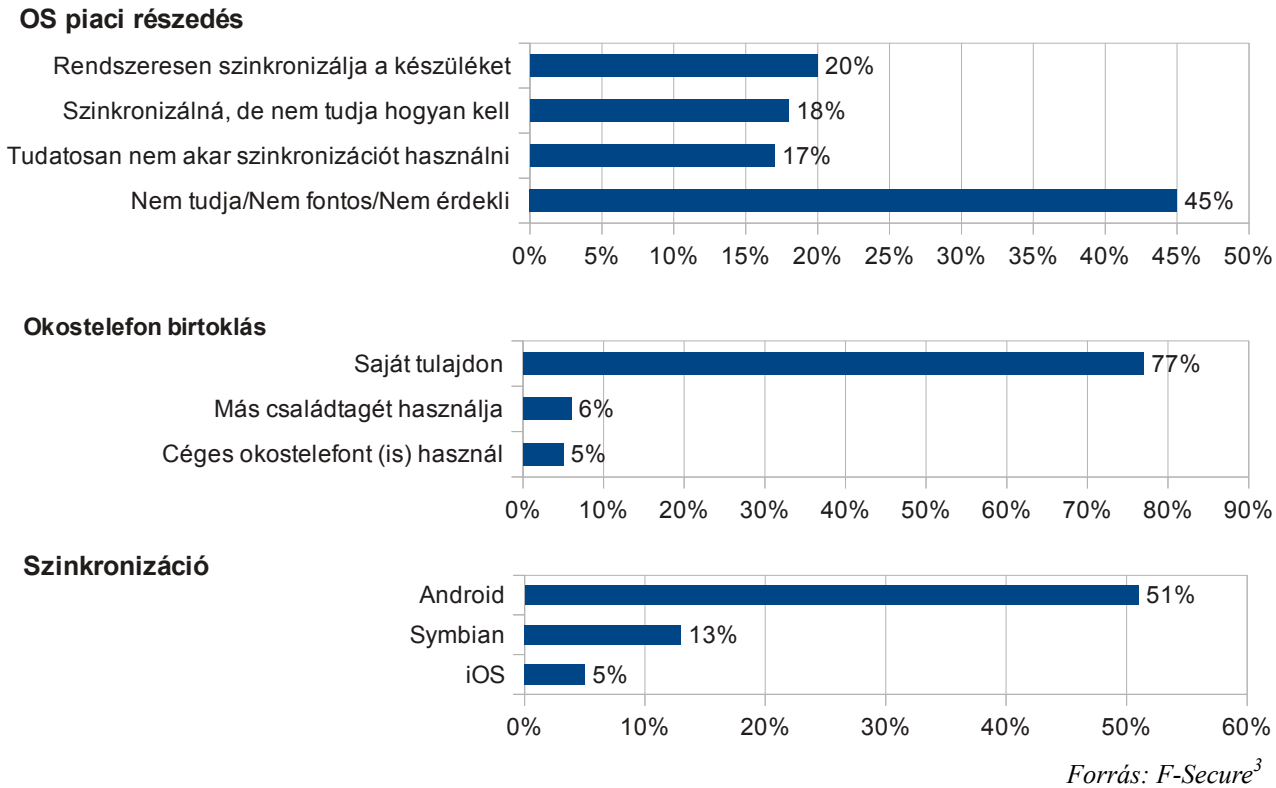
2 NMHH - Kutatópont: Infomédia monitoring 2012, NMHH 2013.03.01.

A 15 éves és az idősebb lakosság számára az internetelérés legnagyobb arányban asztali számítógépen történik, a laptopok 18%-os internetelérésben történő használata mellett az Android rendszerű okostelefonok használata nevezhető még jelentősebbnek (a lakosság 4%-a használja internetezéshez). A többi eszköz használata elenyésző.

Az internetezők között az internetelérésre történő PC használat (75%) majdnem másfélszerese a laptop használatnak (53%). Az okostelefonok internetelérésre történő használata tekinthető még jelentősnek, hiszen nagyjából minden negyedik internetező okostelefon segítségével használja az internetet. A többi vizsgált eszköz részesedése az internetelérésben várhatóan jelentősen megemelkedik majd a következő években az eszközök penetrációjának növekedésével párhuzamosan.

A válaszadók által használt okos mobilkészülékek 72%-ban saját tulajdonúak; 6% családban található okos eszközhöz fér hozzá, míg 5% saját és céges eszközzel is rendelkezik. A több okos készülékkel is rendelkező felhasználók 20%-a – amennyiben az operációs rendszer lehetővé teszi - szinkronizálja a készülékeket, 17%-a nem, 18%-a megtenné, de nem tudja, hogyan kell. Az okostelefonok terén a megkérdezettek 51%-a Android, 13%-a Symbian, 5%-a pedig iOS operációs rendszerű készüléket használ.

Okostelefonok és használati szokások Magyarországon 2013.

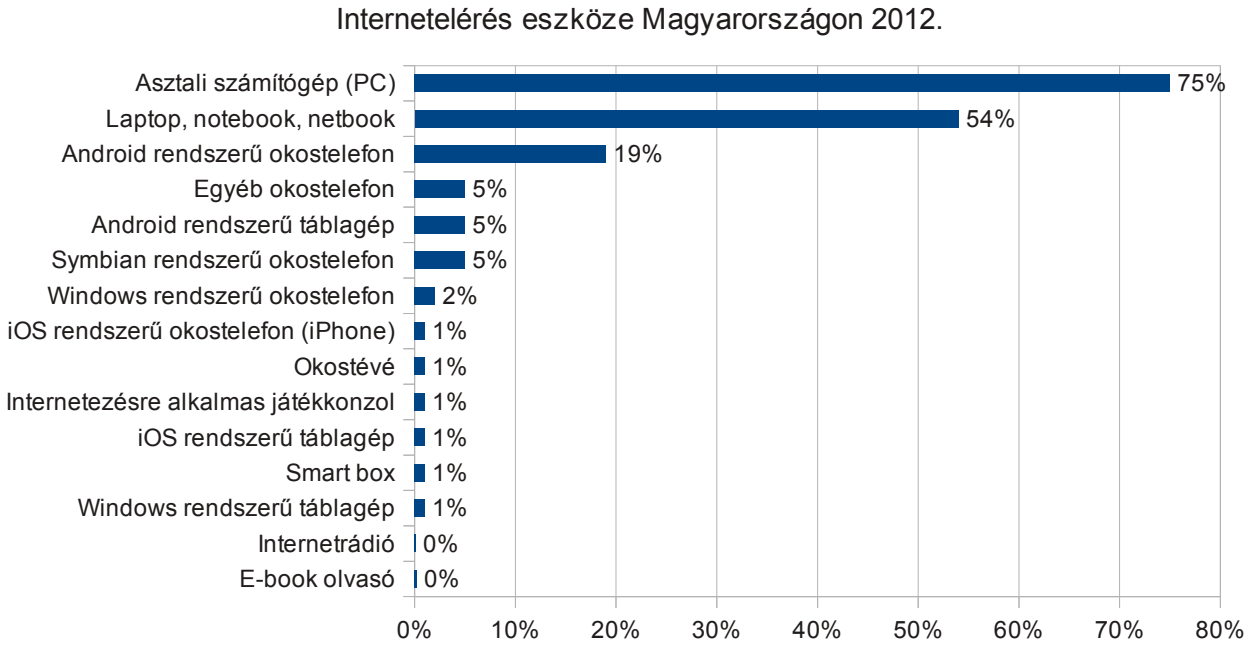


Forrás: F-Secure[3]

Lényegesen kevesebben, mindössze 15%-nyian birtokolnak táblagépet, ahol a Google operációs rendszerének dominanciája megkérdőjelezhetetlen: a készülékek 80%-a Androidos. Egy magyarra átlagosan 1,1 okos eszköz jut. Az Android rendszert használó márkák közül az okostelefonok között 44%-kal a Samsung vezet, 24% jut a Sony (Ericsson)-nak és 8% az LG-nek. Az Androidos tableteknél is a Samsung a piacvezető 39%-kal, a Huawei a második 32%-kal, a készülékek 13 %-a pedig ZTE.[4]

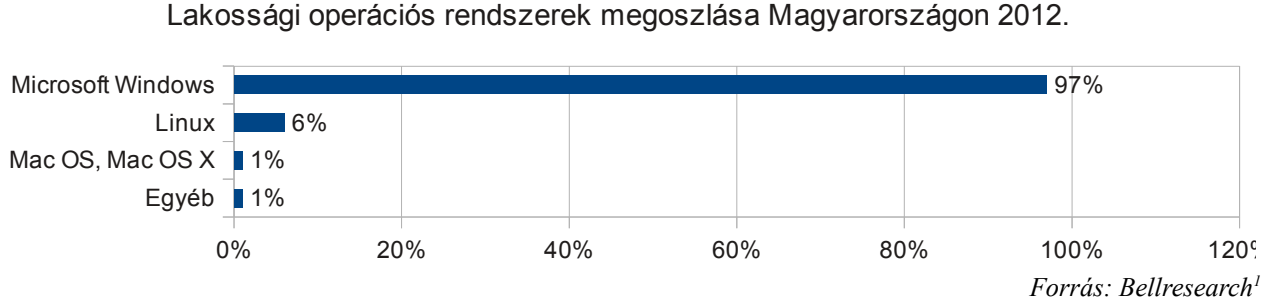
3 Félünk, de nem fizetünk a mobil vírusirtókért, Antivírusház Kft. – F-secure, 2013. január
4 F-secure: Mobile Threat report 2012Q4, 2013. január

A megkérdezettek átlagosan 16 applikációt használnak készülékükön: ötödük tíznél is kevesebb, 22%-uk viszont húsznál is több alkalmazást tart a mobilján. Fizetni viszont nem szeretnek a felhasználók: 44%-uk válaszolta azt, hogy csak ingyenes alkalmazást használ, ötödük pedig mindössze legfeljebb 600, 11% pedig maximum 1200 forintot adna egy-egy jó app-ért. A válaszadók 5%-a viszont akár 10 000 forintot is fizetne egy alkalmazásért – ha az maradéktalanul megfelel az elvárásainak. Letöltés előtt a felhasználók általában alaposan tájékozódnak: a válaszadók 69 %-a mindig megnézi az app-ra adott hozzászólásokat és azt is, hogy hány csillagot kapott, fele pedig hajlandó akár részletesen is utána olvasni egy-egy alkalmazásnak. Mindössze 12% válaszolta azt, hogy szeret maga meggyőződni egy alkalmazás minőségéről.[3]



Forrás: Bellresearch[1]

A Microsoft egyeduralkodónak mondható az online válaszadók által PC-ken és laptopokon használt operációs rendszerek tekintetében, egyedül a Linux tud még kismértékben megjelenni mellette a használati oldalon, de még a Linux-ot használók aránya is eltörpül a Windows használók mellett.



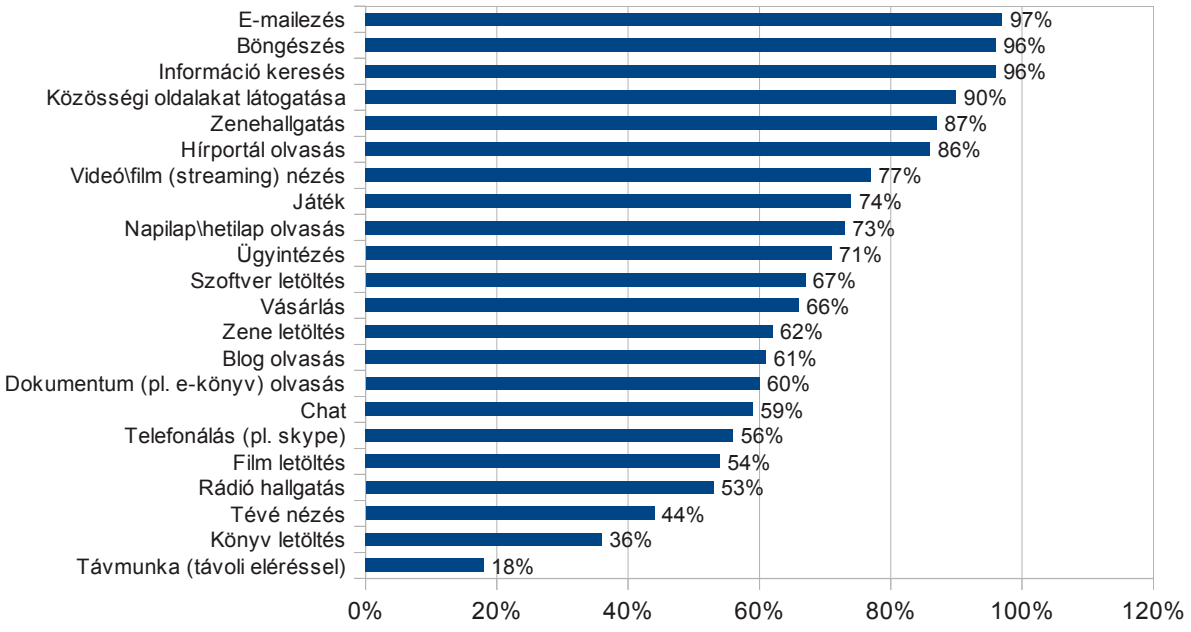
Forrás: Bellresearch[1]

Internet-használati szokások

Az internethasználat elsődlegesen böngészést, e-mailezést és keresést jelent a válaszadók számára (lényegében minden internetező válaszaiban megjelennek ezek a tevékenységek). Az internetező, 15. életévét betöltött lakosság túlnyomó része (90%) közösségi oldalakat is látogat internethasználat közben.

A médiatartalmak közül a hírportál olvasás (86%) és a zenehallgatás (87%) a legelterjedtebbek, de a válaszadók háromnegyede videókat/filmeket, 44%-a pedig tévét is szokott nézni.

A lakossági internethasználók tevékenysége Magyarországon 2012.

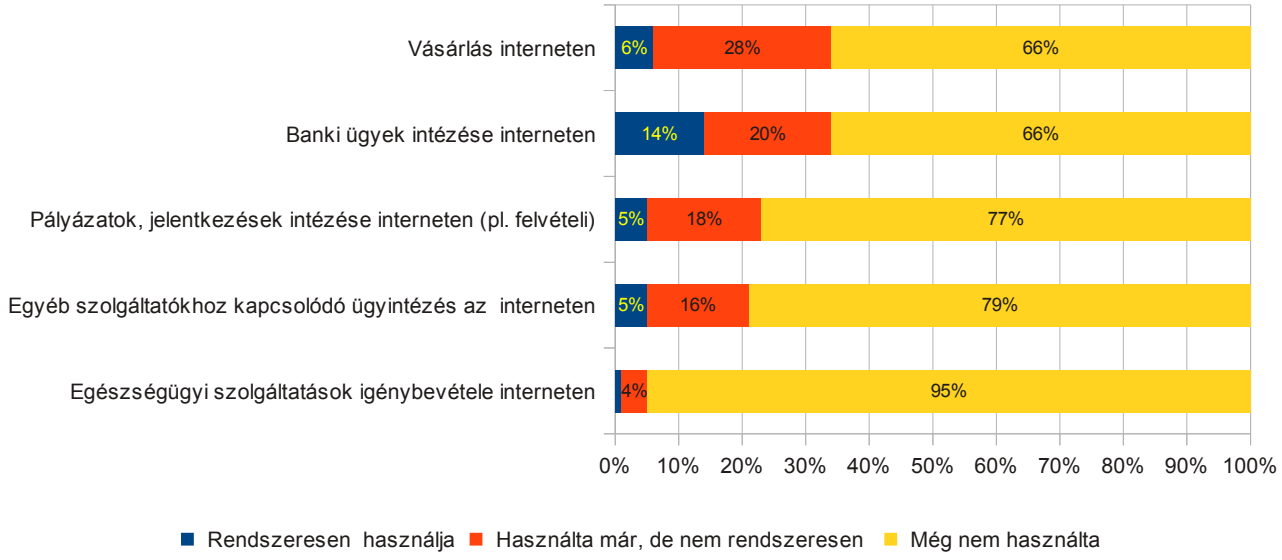


Forrás: NMHH[5]

A távmunka meglehetősen alacsony szinten van, hiszen az 15 éves és annál idősebb internetezők alig 18 %-a használja erre a tevékenységre az internetet.

A vásárlás (34%) és a banki ügyek intézése (34%) a legelterjedtebb elektronikus ügyintézési tevékenység a felsoroltak közül az internetező 18 éves és idősebb válaszadók között, melyek közül a banki ügyintézést a válaszadók 14%-a rendszeresen is használja. Legkevésbé az egészségügyi szolgáltatások igénybevétele elterjedt. Forrás: Bellresearch[1]

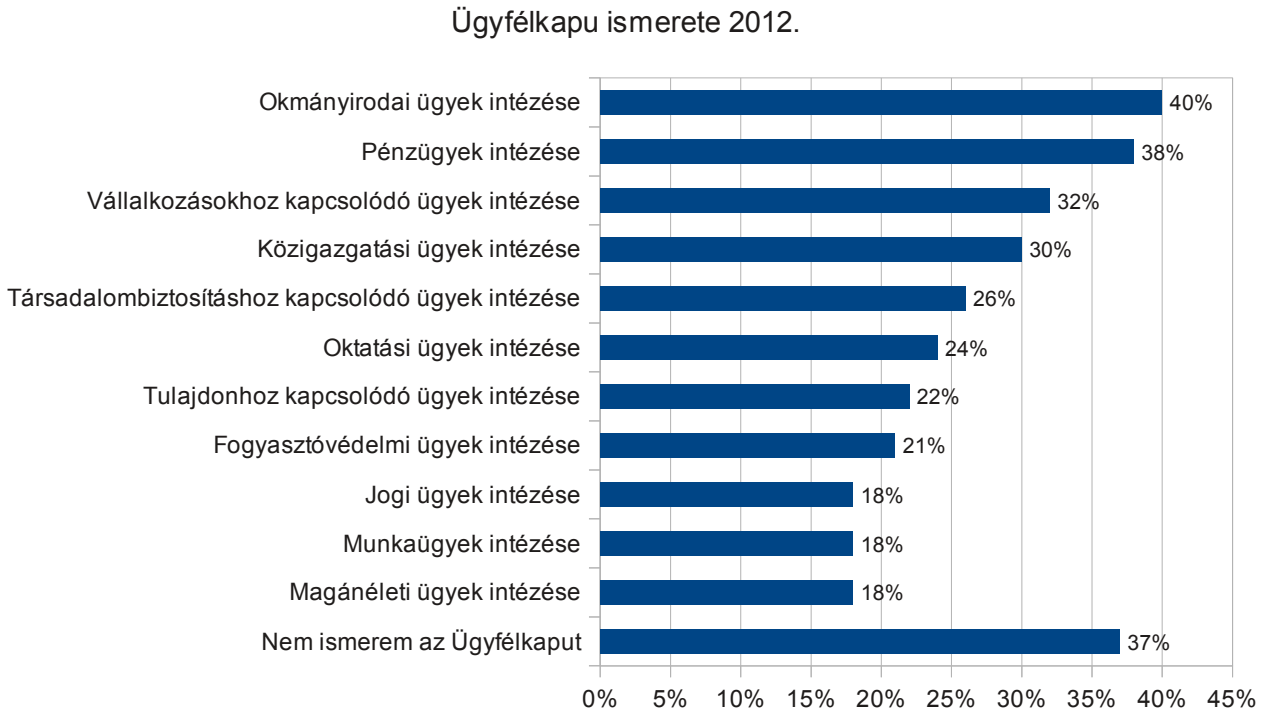
Elektronikus ügyintézés Magyarországon 2012.



Forrás: NMHH[5]

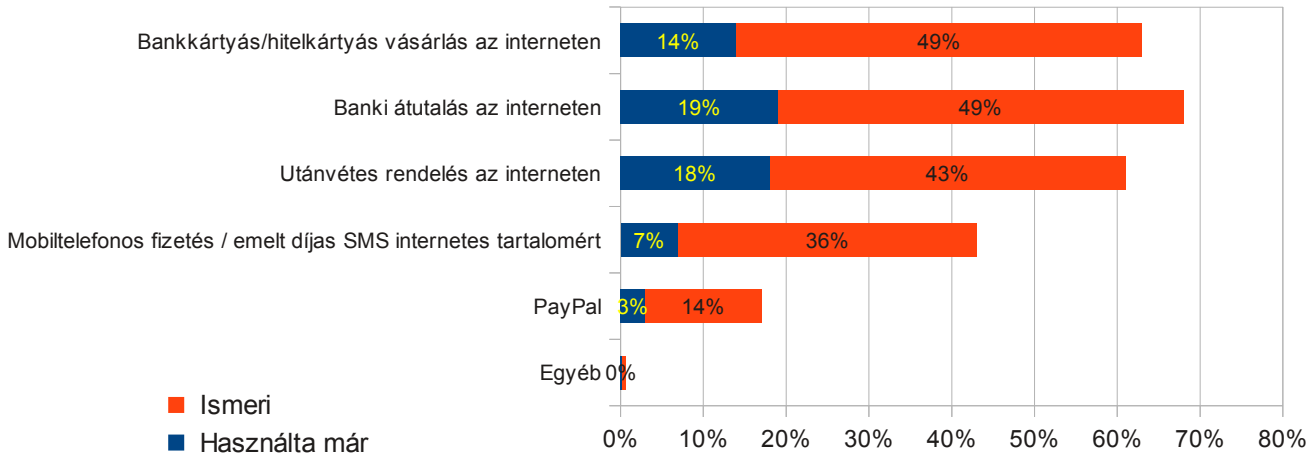
5 NMHH - Kutatópot: Infomédia monitoring 2012, NMHH 2013.03.01

Az Ügyfélkapu az internetező, 18. életévüket betöltött válaszadók több mint harmada számára ismeretlen (37%). Az Ügyfélkapuhoz elsősorban az okmányirodai ügyintézést (40%), és pénzügyek intézését kötik a válaszadók (38%). A jogi ügyek, munkaügyek és magánéleti ügyek intézésére nyújt legkevésbé lehetőséget az Ügyfélkapu a válaszadók szerint, hiszen csak 18-18%-uk tartja intézhetőnek a Magyar Kormány e-Ügyintézési oldalán.



Forrás: NMHH[5]

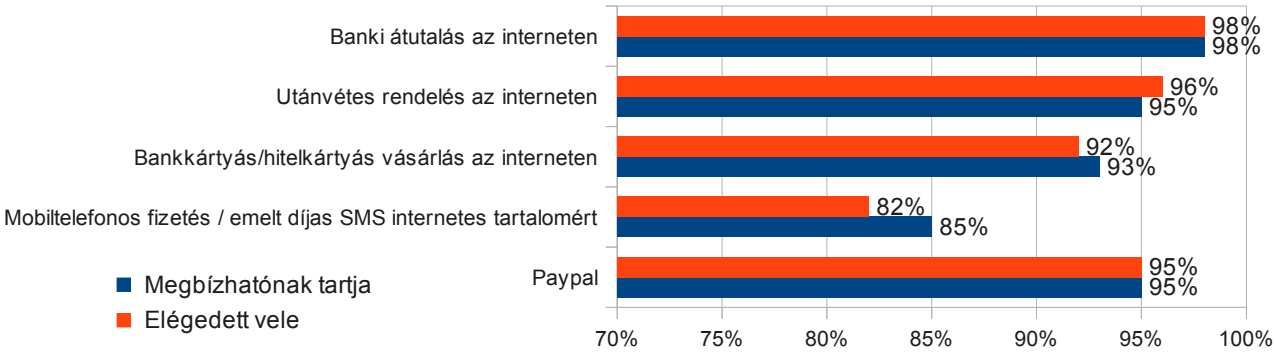
A legismertebb online fizetési módokat a lakosság közel fele ismeri, ezek a bankkártyás vásárlás (49%) és a banki átutalás az interneten (49%). Ugyanakkor a banki átutalás (19%) mögött legtöbben az utánvétes rendelést használták (18%).



Forrás: NMHH[5]

Akik a vizsgált fizetési módokat használták már, szinte kivétel nélkül megbízhatónak is találták azokat, és elégedettek is voltak velük. Leginkább a banki átutalás nyerte el az azt használók tetszését (a használók 98%-a találta megbízhatónak és ugyanennyien voltak elégedettek is vele), míg legkevésbé a mobiltelefonos fizetés internetes tartalomért (a használók 85%-a tartja megbízhatónak, és 82%-a elégedett vele).

Online fizetési módok megítélése Magyarországon 2012.

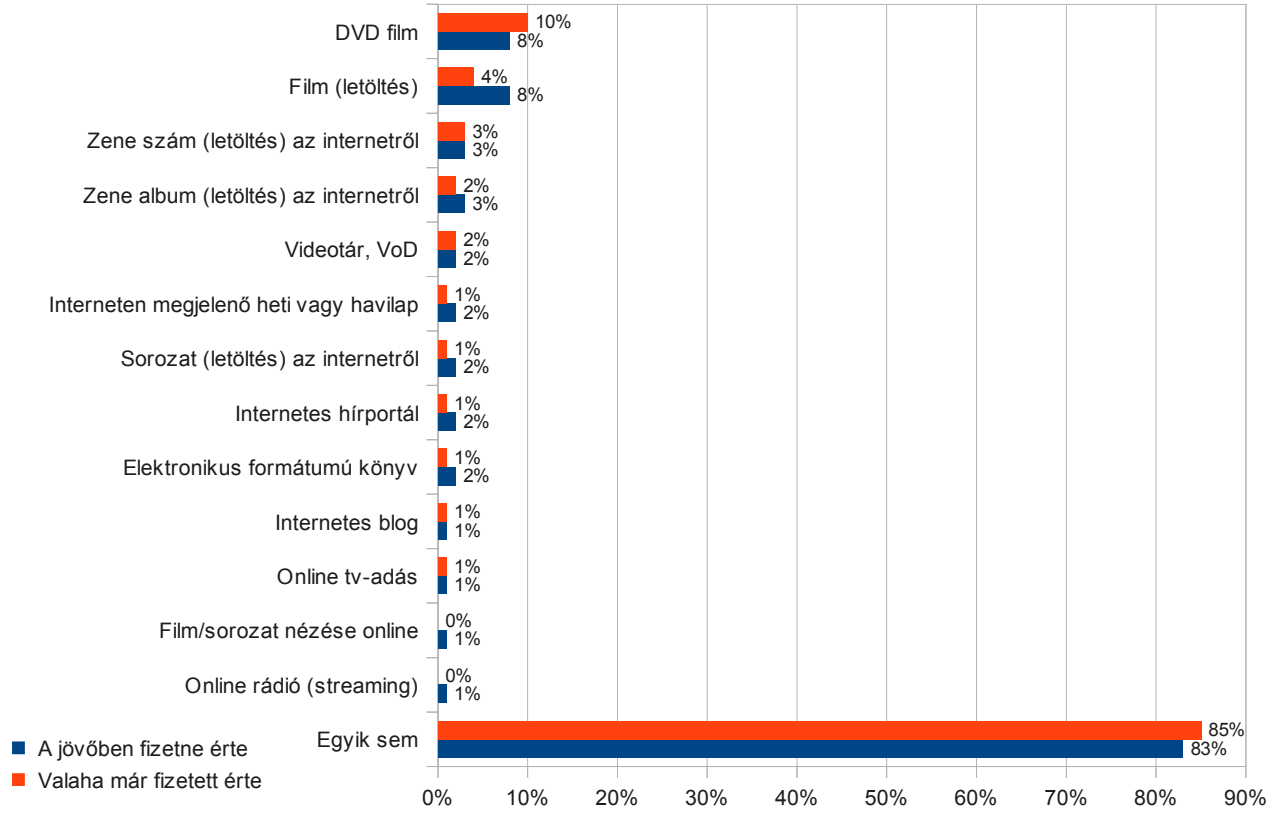


Forrás: NMHH[5]

Tartalom fogyasztás

Az egyes online médiatartalmakért nagyon kevesen fizettek eddig (internetező felnőttek 15 %-a), és a jövőbeni fizetési hajlandóság is igen korlátozott (17%). A filmletöltés lenne képes egyedül jelentősebb mértékben megnövelni a fizetési hajlandóságot, hiszen a jövőben a lakosság 4%-kal nagyobb arányban lenne hajlandó fizetni ilyen tartalomért. Ez természetesen fokozottan hat a biztonsági kockázatokra is, hiszen az ingyenes források gyakran fertőzött, kártékony kódokat futtató weboldalak közül kerülnek ki.

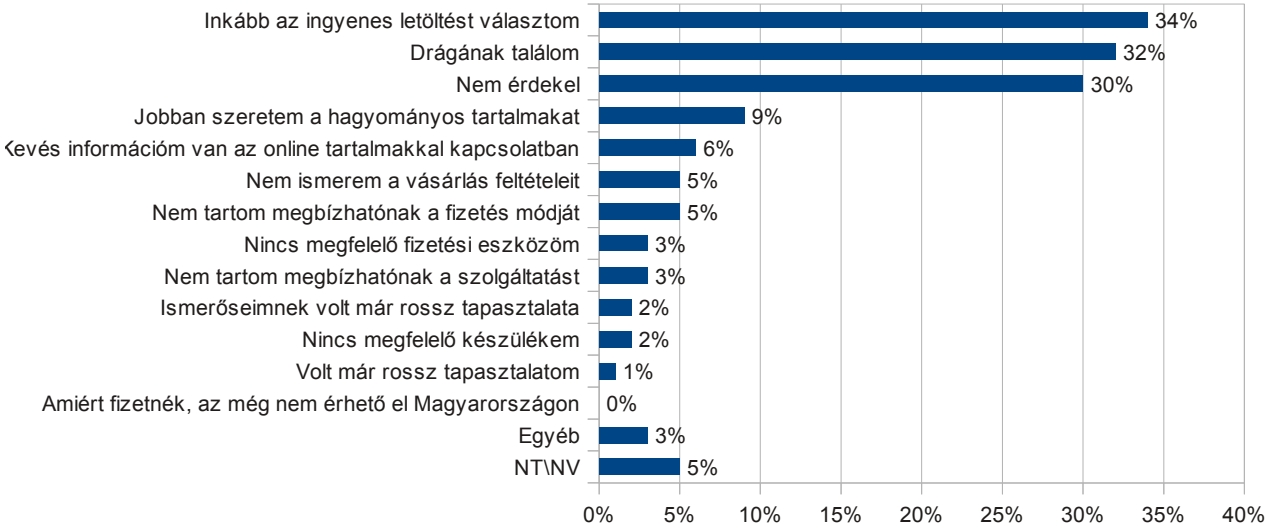
Fizetési hajlandóság internetes tartalomért Magyarországon 2012.



Forrás: NMHH[5]

Az online tartalmakért leginkább költséghatékonysági szempontból nem fizetnének az internetező válaszadók, 34%-uk inkább ingyen tölt le, 32%-uk pedig drágának találja az online médiatartalmakat. Jelentős még azon nem fizető internetező felnőttek aránya, akiket saját állításuk szerint nem érdekelnek az online médiatartalmak (30%).

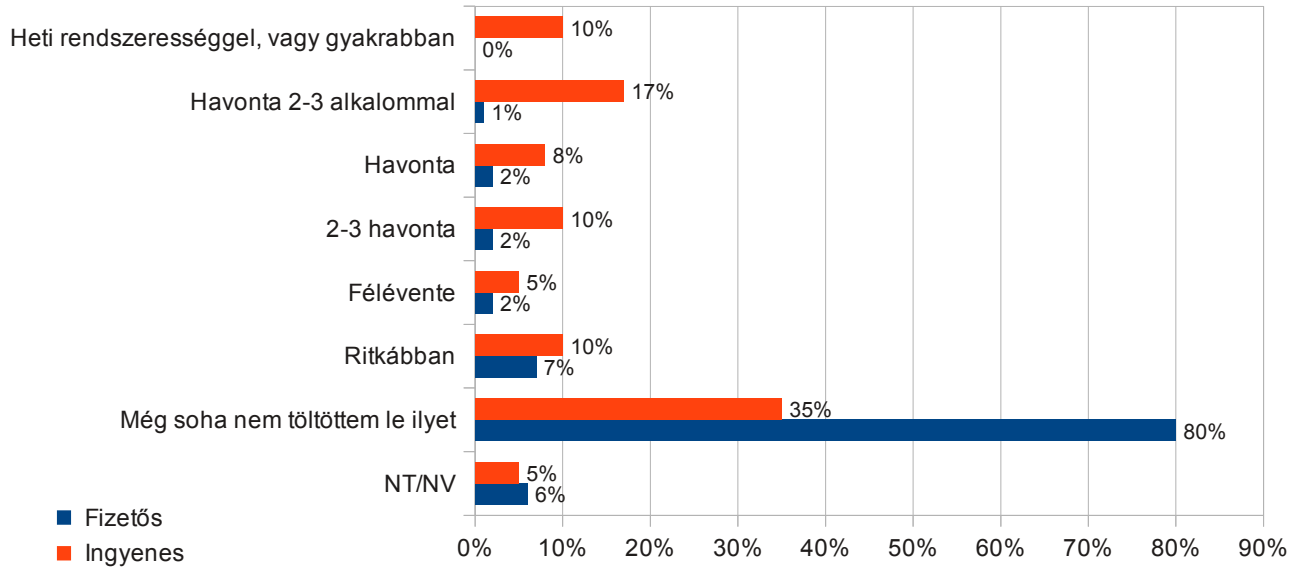
A nemfizetés okai Magyarországon 2012.



Forrás: NMHH[5]

A különféle internetképes készülékekkel rendelkezők szintén leginkább ingyenes alkalmazásokat töltenek le, sokszor itt is bizonytalan forrásokból. A válaszadók túlnyomó többsége (80%) még soha nem fizetett alkalmazásért. Ingyenes alkalmazást viszont a válaszadók 35 %-a havi rendszerességgel tölt le, igaz, ugyanekkora az aránya azoknak is, akik soha nem töltöttek még le ingyenes alkalmazást.

Appok letöltése okos mobileszközökre Magyarországon 2012.



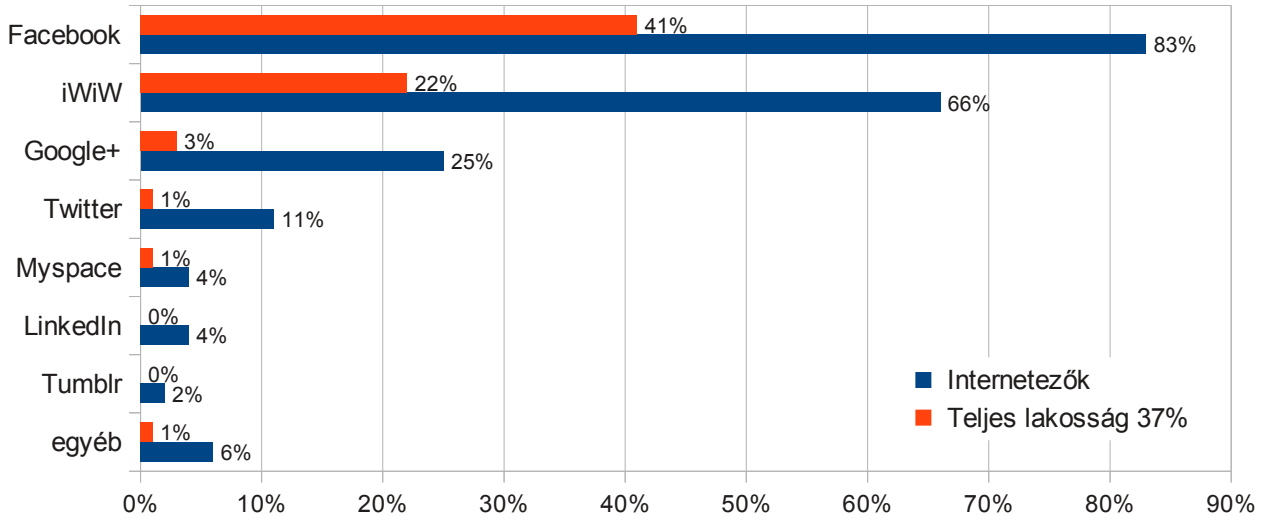
Forrás: F-secure[3]

Közösségi média használat

A 18 éves és idősebb lakosság 41%-a megtalálható a Facebook-on. Jelentős közösségi oldalnak számít még az iWiW, ahol a válaszadók ötöde regisztrálva van (22%). A többi közösségi oldal közül a Google+ tekinthető a legjelentékenyebbnek 3%-os penetrációjával.[6]

A 15 éves és idősebb internetezők között értelemszerűen magasabb arányú az egyes közösségi oldalak használata, de használat szerinti sorrendjükben és az egymáshoz viszonyított arányukban nincs különbség a teljes minta eloszlásaihoz képest.

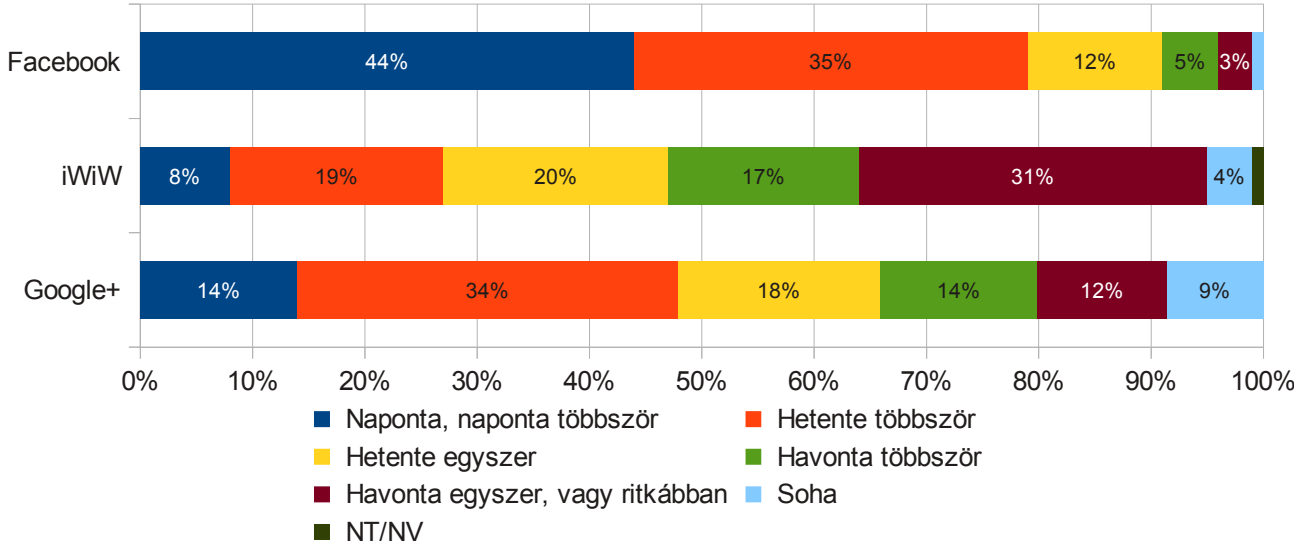
Jelenlét a közösségi oldalakon Magyarországon 2012.



Forrás: Bellresearch[1]

A közösségi oldalak közül a legintenzívebben a Facebook-ot használják a közösséghez tartozók, 44%-uk naponta legalább egyszer megtekinti azt. Az iWiW használati intenzitása a Google+-tól is elmarad, hetente egyszer a felhasználók 47%-a látogatja, míg a Google+-t a felhasználói 66%-a keresi fel legalább heti rendszerességgel.

Közösségi oldalak használati gyakorisága Magyarországon 2012.



Forrás: NMHH[5]

6 Cisco Systems: Gen Y: New Dawn for work, play, identity, Cisco Connected World Technology Report, 2012. augusztus

Az egyes közösségi oldalakon végzett tevékenységek szempontjából a Facebook és az iWiW egymáshoz hasonlónak mondható, a képek megosztásának aránya a legmagasabb, amit a mások által közölt magánjellegű információkhoz hozzászólás, és az érdekes hírek, események megosztása, azokhoz hozzászólás követ.

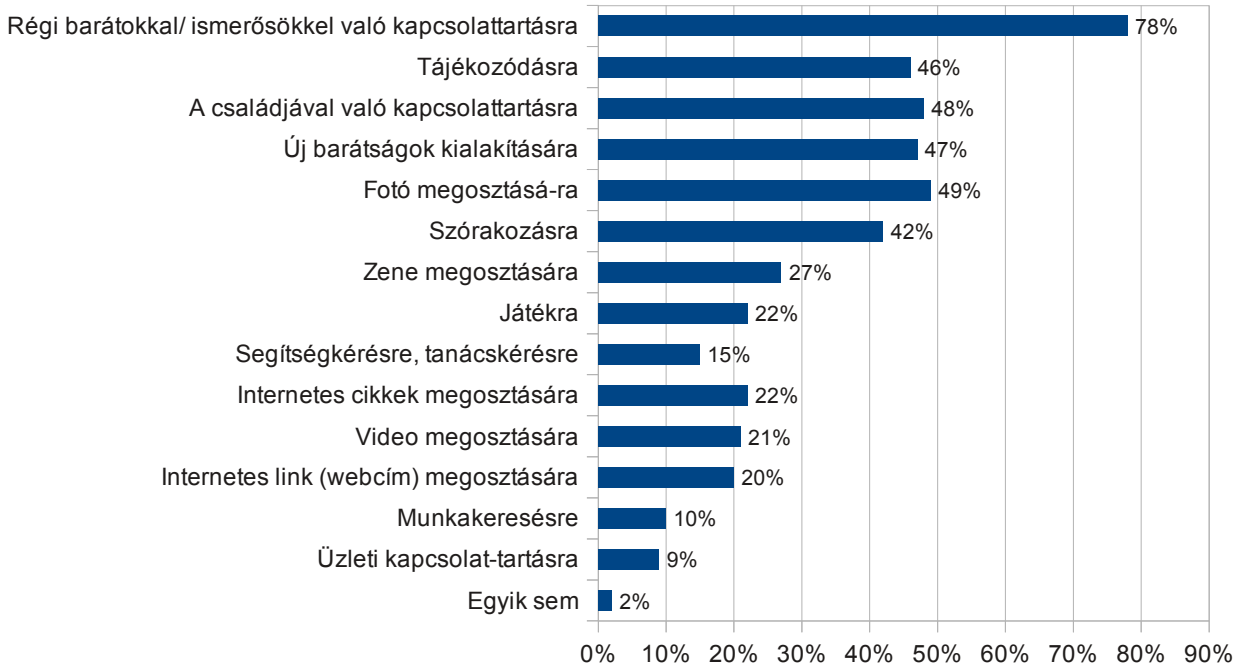
A másik két közösségi oldalhoz képest eltérő mintázatot mutat a Google+-on végzett tevékenységek egymáshoz viszonyított aránya, ahol leginkább érdekes híreket, eseményeket osztanak meg egymással a felhasználók, és ezekhez szólnak hozzá, a képfeltöltés itt kevésbé jelentős.

Milyen gyakran szokott…?
(Aktivitás a közösségi oldalakon, Magyarország, 2012.)

Forrás: NMHH[5]

A Facebook-ot és az iWiW-et a felhasználóik hasonló célokból használják, elsődlegesen az ismerősökkel és családdal való kapcsolattartásra, új barátságok kiépítésére, fotómegosztásra. A Google+ használatában jelentősebb szerepet kap a tájékozódás és a segítség-kérés.

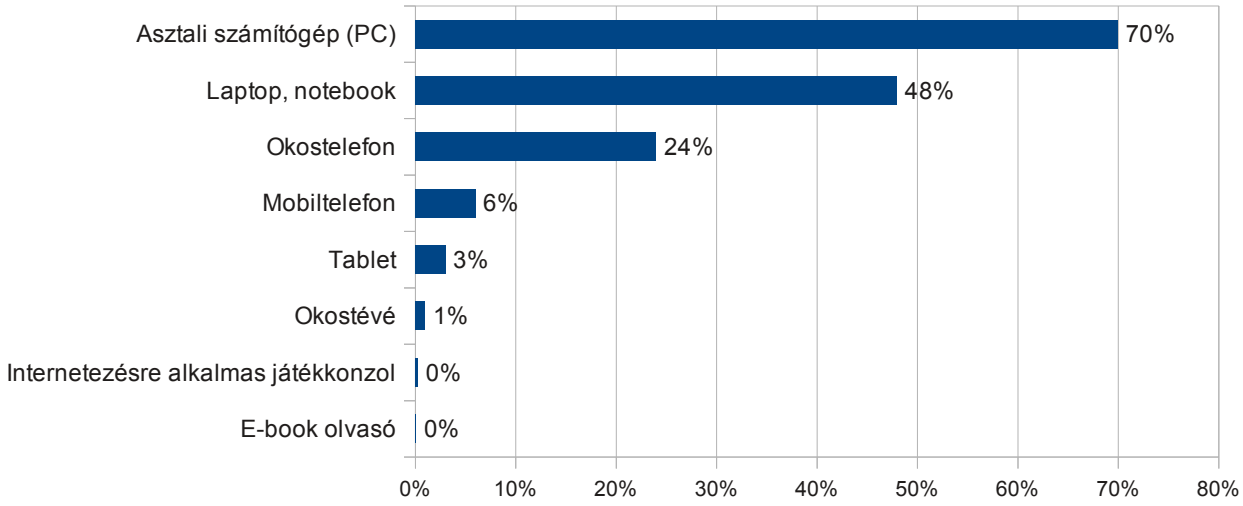
Közösségi oldalak használati célja Magyarországon 2012.



Forrás: NMHH[5]

A közösségi oldalak látogatása elsősorban az elterjedtebb internet elérésre alkalmas eszközökön történik (asztali számítógépen és laptopon), de igen jelentős a mobiltelefonok szerepe a közösségi kapcsolatépítésben, hiszen az online válaszadók közel negyede okostelefonról, további 6%-uk egyéb mobiltelefonról látogatja a közösségi oldalakat.

Eszközhasználat közösségi oldalak elérésére Magyarországon 2012.

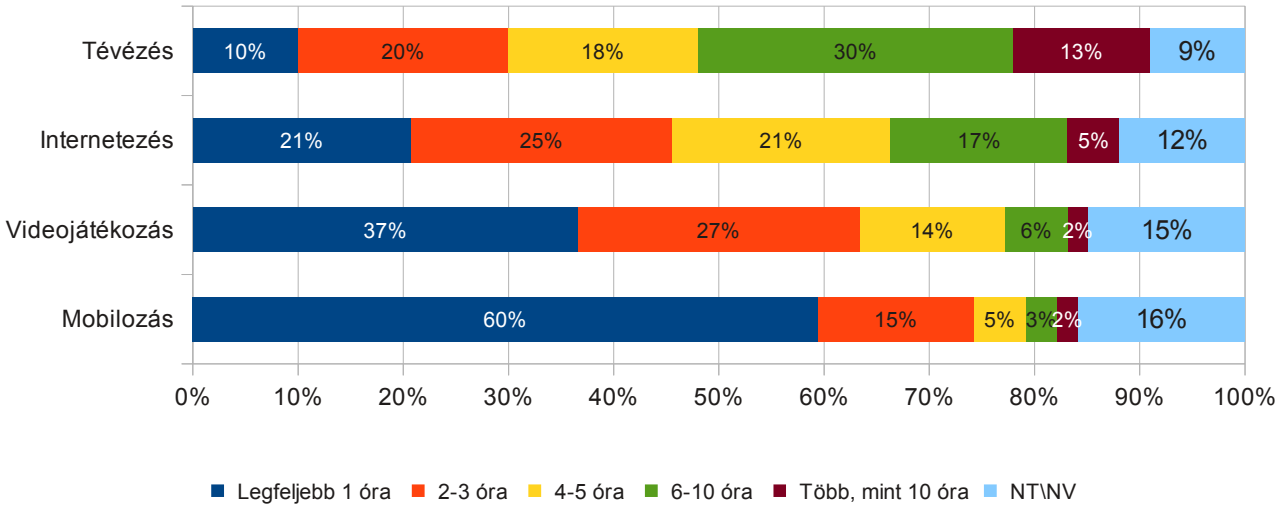


Forrás: Bellresearch[1]

A kiskorúak online jelenléte

A 18 éves és idősebb lakosság az általános iskolások televízió nézésével kapcsolatban a legelnézőbb (43%-uk heti 5 óránál többet engedélyezne), míg a mobiltelefonálási szokásaikat korlátoznák leginkább (a válaszadók 60%-a szerint heti 1 óránál több mobilhasználat nem engedhető meg a kiskorúak számára).

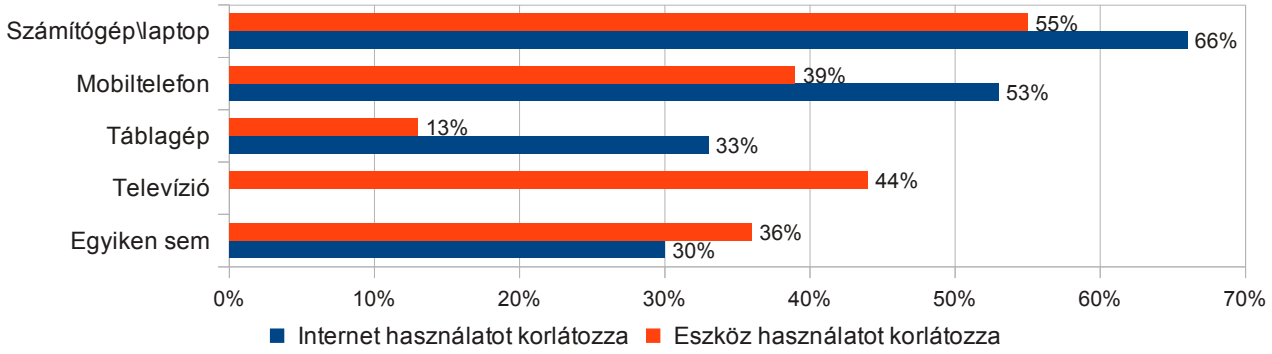
Kiskorúak internethasználata Magyarországon 2012.
(Hetente hány óra megengedhető az egyes tevékenységekre?)



Forrás: NMHH[5]

Általánosan jellemző a háztartásukban 14 éves, vagy annál fiatalabb gyermeket tudó válaszadók vélekedésére, hogy az egyes internetképes eszközök használatának korlátozásán túl annál nagyobb arányban korlátoznák az adott eszközön az internet használatot. Ez a vélekedés a kiskorúakra leselkedő internetes veszélyektől való félelemre utal.

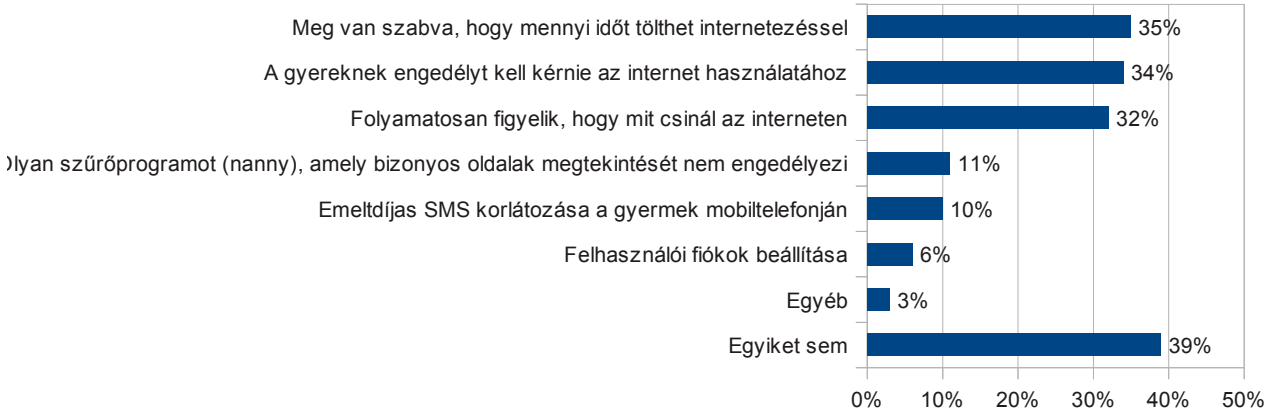
Kiskorúak elektronikus jelenlétének korlátozása Magyarországon 2012.



Forrás: NMHH[5]

A gyerekek internet használatát elsősorban nem technikai eszközökkel, hanem neveléssel, személyes ellenőrzéssel igyekeznek a válaszadók kontroll alatt tartani. Ez a hozzáállás a szűrőprogramokkal, eszközök beállítási lehetőségeivel kapcsolatos ismeretek esetleges hiányosságára, avagy az irányukban megnyilvánuló bizalom hiányára utal. A technikai eszközök alacsony használati aránya a szóba jöhető megoldások ismeretének hiányából, ill. azok használatának (bonyolult a használat) nem ismeretéből fakad - fontos tehát a megoldások ismertségének további növelése, egyszerű technikai eszközök biztosítása.

Kiskorúak internethasználatának ellenőrzésére Magyarországon 2012.



Forrás: NMHH[5]

Digitális írástudatlanság: igény, ismeret vagy infrastruktúra hiány?

Az információs társadalomban való részvétel nem szabadon választható opció, hanem kikerülhetetlen állapot. Előnyeit csak akkor tudjuk élvezni, ha mindenki számára olyan szolgáltatások állnak rendelkezésre, amelyek arra késztetik az embereket, hogy megszerezzék az igénybevételükhöz szükséges ismereteket. Az ismeretek megléte a digitális írástudás: egy összetett fogalom. Azokat a készséggé fejlesztett ismereteket tartalmazza, amelyek lehetővé teszik a felhasználó számára a számítógép és az internet adta lehetőségek kihasználását. Fokozatosan nő az e-közigazgatás szerepe is, és a hagyományos tanulás is egyre jobban az internetre tolódik.

Mivel a társadalom működése az abban részt vevő emberek mikrodöntésein alapul, a magasabb digitális jártasság jobb döntéseket, hatékonyabb időfelhasználást, ésszerűbb teljesítményt, tehát pozitív gazdasági hatást eredményez. Az üzleti életben például rendkívül fontos a bizalom. A bizalom felépítésében pedig nagyon fontos tényező, hogy a társadalom egymástól fizikailag elszigetelt csoportjai hogyan ismerik egymást. Minél több digitális jártassága van valakinek, annál több keresztkapcsolatot létesít másokkal, annál jobban megismer másokat. Az ismeretség bizalmat szül, a bizalom pedig a sikeres üzlet, illetve gazdaság alapja.

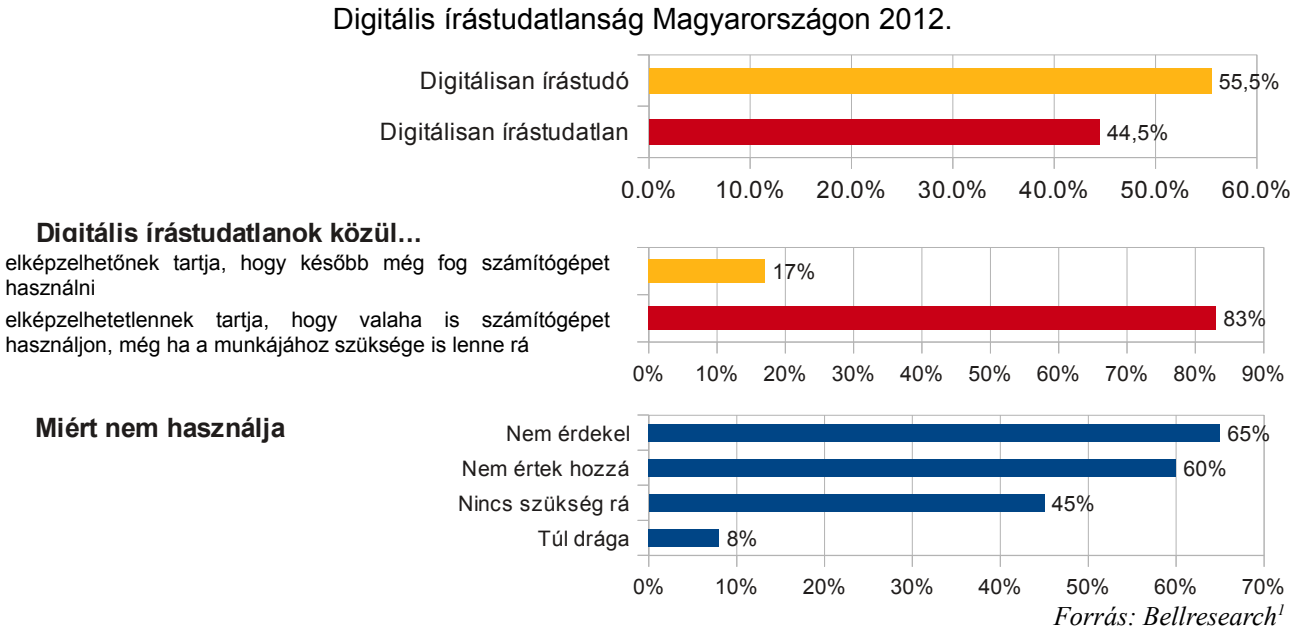
A digitális írástudás elsajátítása nemcsak a gazdasági versenyképesség, hanem az életminőség javulásával is jár. Hazánk lakosságának 4,5%-áról (450 ezer fő) biztosan el lehet mondani, hogy rendelkezik ezzel a tudással: a számítógépet nemcsak szórakozásra és kapcsolattartásra, hanem a napi munkában, illetve az elektronikus közigazgatási szolgáltatások igénybevételéhez is professzionálisan tudja használni. Ez ebben a kategóriában jelentős arány: Magyarország nemzetközi viszonylatban is az igen előkelő 7–8. helyen áll. Jelenleg általánosan elfogadott, hogy az ideális arány 6–8% . Digitális írástudás hiányában, munkaidő-kiesések következtében százmilliárdos nagyságrendű eredmény marad el évente, állítja több felmérés.[7]

Az igazi gond a mindennapokhoz szükséges, nélkülözhetetlen készségek ismeretének a hiánya. Eredményről e tekintetben viszont csak akkor beszélhetünk, ha összhangban a jelenlegi kormány eredeti elképzeléseivel, legalább 1-1,5 millió ember válik majd digitálisan írástudóvá, akik aztán továbbadhatják ismereteiket.

A digitális írástudásban két nagy törésvonal is fellelhető, s ezek háromfelé osztják a magyar társadalmat. Egyrészt a fő szakadék az eszközöket és az internetet használók és nem használók között húzódik, a másik pedig az eszközöket és az internetet értékteremtő módon használók, illetve az „öntudattalan" felhasználók között mélyül.

2012-ben a BellResearch Magyar Infokommunikációs Jelentése[1] szerint a magyarországi felnőtt lakosságon belül 44,5%-ra tehető a digitális írástudatlanok aránya. Ez a mintegy 3,5 millió ember egyáltalán nem vagy csak nagyon ritkán használ PC-t és internetet. A felnőtt lakosság közel fele főleg motivációs problémákkal küzd.

Jól mutatja a probléma súlyát, hogy 83% számára teljes mértékben elképzelhetetlen, hogy valaha is használjon számítógépet, még akkor sem, ha a munkájához lenne rá szükség. 43%-nak nincs rá szüksége, nem érzi hasznát, 65%-ot nem érdekel a PC, saját bevallása szerint nem ért hozzá 50–60% és csak 8% azok aránya, akik talán használnák, ha olcsóbb volna.



Forrás: Bellresearch[1]

7 Mártonffy Attila: Digitális írástudás: a jövő záloga, ITBusiness, 2012.02.20.

A szakadék már 45 év fölött kialakul, de 60 év fölött mélyül el igazán: ez utóbbi korosztály digitális írástudatlansága több mint 80%-os. Az írástudatlanság összefügg a képzettséggel is, a digitálisan analfabéták 88%-ának érettségije sincs.

A digitális írástudás szakmai definíciójába az eszközhasználatot is bele szokás venni, ugyanakkor a felhasználó nem mindig tudja, hogy például telefonja nyomogatása közben éppen a neten jár.

Ha viszont azt nézzük, hogy mi motiválja a még nem internetezőket a hálózat használatára, akkor jelentős tényező a barátoktól, ismerősöktől, reklámokból szerzett értesülés a neten való adásvétel előnyeiről. Az e-kereskedelem tehát így tudja előmozdítani a digitális írástudás terjedését. További jó példa e körön belül az internethasználat fokozására a bónuszus-kuponos vásárlás elterjedése. Az, hogy akár 50%-os kedvezménnyel meg lehet vásárolni termékeket, szolgáltatásokat, érezhető mértékben megdobja az e-kereskedelmi forgalmat, s ez végső soron élénkíti a gazdaságot.

Abból kiindulva, hogy valaki digitálisan írástudó, s emiatt például munkáját hatékonyabban, célszerűbben, gyorsabban tudja végezni, jelentős időt takaríthat meg. S mivel az idő pénz, a pénz pedig mérhető és összehasonlítható, a digitális írástudás terjedésének százalékban kifejezett növekedési üteme megfelelő arányban növeli a bruttó hazai terméket (GDP) is.

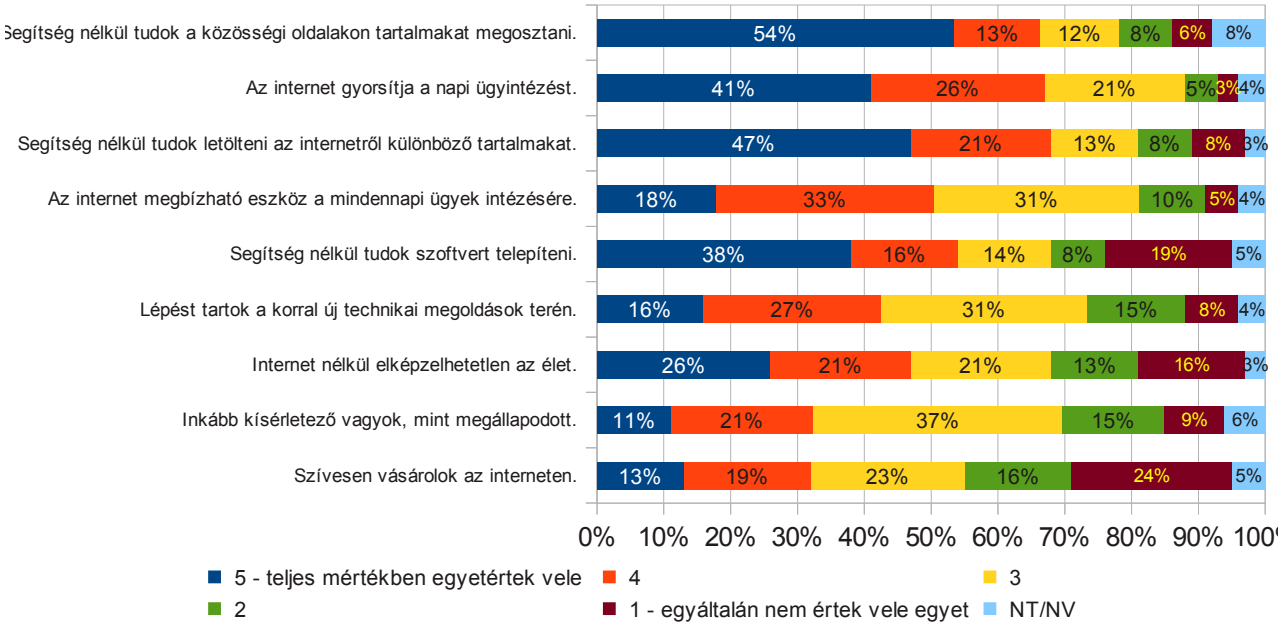
Az internethasználat tekintetében egyébként Magyarország nagyjából azonos szinten van a térség többi országával, az e-kereskedelemben azonban Csehország, sőt Szlovákia is megelőzi hazánkat.

Az internetezők közössége alapvetően eltérő tulajdonságokkal és jellegzetes attitűdökkel viseltetik a technológia mindennapi életre gyakorolt hatásait tekintve:

Az online válaszadók magukat tudatos vásárlónak tartják (technikai újdonság vásárlása előtt 75%-uk alaposan utána olvas), a közösségi oldalakon jártasnak tartják magukat (segítség nélkül tud tartalmakat megosztani 67%-uk), és abban is inkább egyetértenek, hogy az internet gyorsítja a napi ügyintézést.

Az online válaszadók a többi jellemvonáshoz képest kevésbé szívesen vásárolnak az interneten (40%-uk nyilatkozott így), és az újdonságok kipróbálása, megvásárlása sem a legjellemzőbb rájuk (41, illetve 76% nem értett ezekkel a kijelentésekkel egyet). Ezen jelenségek mögött szintén egyfajta tudatosság, körültekintés állhat.

Online viselkedési attitűdök Magyarországon 2012.



Forrás: NMHH[5]

Az IT-biztonság kihívásai a lakossági szektorban

2013 legfontosabb biztonsági kihívásai a végfelhasználói szektorban

Az idő előrehaladásával a IT-biztonság kulcsterületei is változnak, amelyek a legfontosabb kihívásokat hordozzák a végfelhasználók számára. Az alapszintű biztonsági szoftverek alkalmazása, a rendszeres frissítések fontossága, az alapvető bizalmatlanság az ismeretlen tartalommal szemben mára eléggé elterjedtek a végfelhasználók körében, még ha vannak is hiányosságok. A veszélyek viszont a felhasználói szokások változásával párhuzamosan folyamatosan átalakulnak.

- **Közösségi oldalak:** A közösségi oldalakon terjesztett harmadik féltől származó alkalmazások egyre nagyobb arányban tartalmaznak kártékony kódokat. E terület egyre növekvő népszerűsége 2013-ra az egyik legfontosabb kockázatforrássá emelte ezt a problémát. A közösségi oldalakon ráadásul összekeveredik a magánszféra és a munka világa is, hiszen barátaikon, ismerőseiken kívül a felhasználók egyre többször ügyfelekkel, munkatársakkal, partnerekkel való kapcsolattartásra is használják a Facebookot, a Twittert és a többi hasonló szolgáltatást. Ez a folyamat pedig minden korábbinál vonzóbbá teszi ezeket a csatornákat az „ismerősökön" keresztül indított social engineering típusú támadásokhoz.
- **SMS:** Bármilyen furcsa, az okostelefonok korának egyik új kihívása a GSM világ egyik legrégebbi és legnépszerűbb szolgáltatása. A mobilhasználó felnőtt lakosság 73%-a rendszeresen használja az SMS-szolgáltatást, egy átlag amerikai felhasználó pedig napi 41 SMS-t küld és fogad. A marketing célú SMS-ek körében egyre megszokottabb, hogy linkeket tartalmaznak, így az adathalász vagy a rosszindulatú kódokat tartalmazó weboldalakra mutató linkeket tartalmazó üzenetek egyre jobban beolvadnak a többi közé. És míg a számítógépek böngészői egyre fejlettebb adathalászat elleni szűrőkkel vannak felvértezve, az SMS kliensek és a mobil browser-ek ezen a téren vészesen le vannak maradva. A másik kockázat az SMS-ekkel kapcsolatban, hogy az internetképes telefonokkal a korábbi, kommunikációs csatornák szétválasztásán alapuló biztonsági megoldások (pl. az SMS onetime password) újra összecsúsznak, komoly kihívás elé állítva például a bankinformatikai szakértőket. A folyamat új azonosítási technológiák bevezetését fogja eredményezni a közeli jövőben.
- **App letöltés:** Mint ahogy az a fentiekben is látható volt, a felhasználók szeretnek appokat használni, fizetni viszont annál kevésbé szeretnek értük, így sokszor bizonytalan beszerzési forrásokhoz fordulnak, ez pedig lehetővé teszi a kártékony kódok egyre gyorsabb terjedését. Az okostelefon-alkalmazások többsége ráadásul komoly jogosultságokat kér és kap telepítéskor, legtöbbször anélkül, hogy a felhasználó valóban tudná és megértené mibe is egyezik bele az OK gombra kattintva. A mobil kártevők folyamatosan fejlődnek, kifinomultságuk és mennyiségük is exponenciálisan nő. 2013 végére a várakozások szerint már mintegy 1 millió veszélyes Android alkalmazás lesz, a 2012-es 350 ezerrel szemben.
- **E-mail:** az egyik legrégebben használt internetes kommunikációs forma is egyre újabb veszélyek hordozójává válik. Az adathalászat új fejlesztett módszertana, amelyet célzott adathalászatnak (vagy a halászati analógiához jobban illeszkedve „szigonyos halászatnak") neveznek, új kihívások elé állítja a felhasználói tudatosságot. Ezeknél az e-maileknél:
    1. a feladó látszólag valamilyen jól beazonosítható, ismert és megbízható forrás,
    2. az üzenet olyan bizalmas információkat tartalmaz, amelyek alátámasztják valódiságát,
    3. a benne foglalt kérés teljesen logikusnak, értelmesnek tűnik.

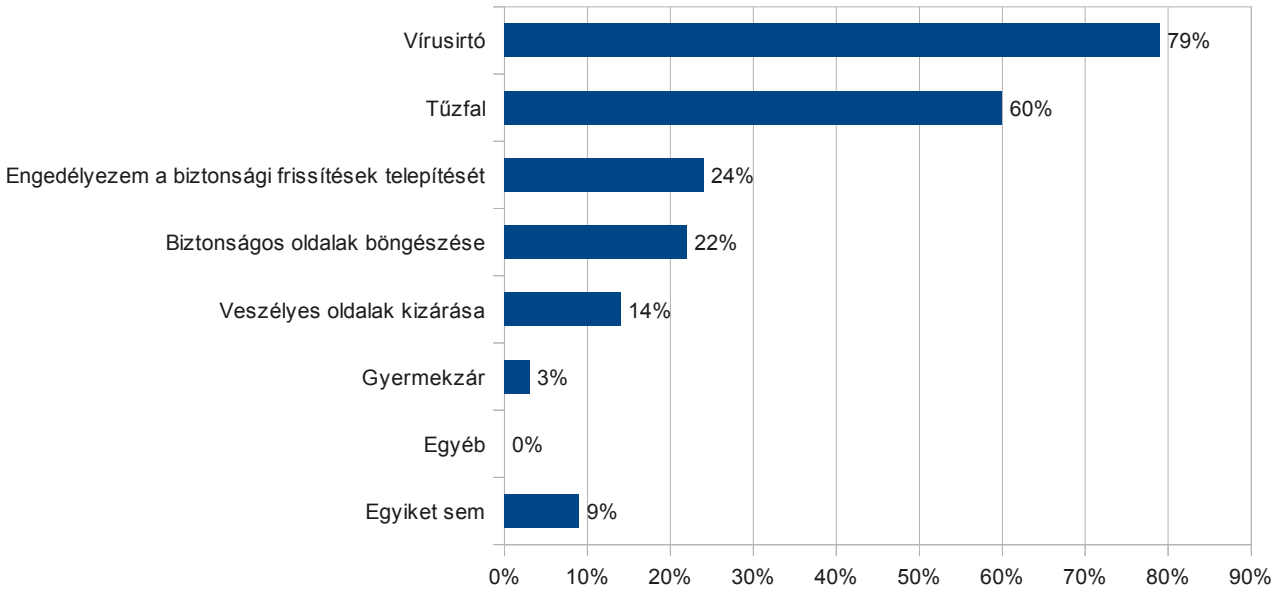
  Mindezekkel a módszerekkel jó esélyekkel rá lehet venni az áldozatot, hogy megnyisson egy rosszindulatú kódot tartalmazó csatolmányt, vagy linket.

- **Felhő szolgáltatások:** A felhasználó felhőszolgáltatások (Dropbox és más hasonló megoldások) rohamos terjedése, és könnyű használhatósága eltereli a figyelmet ezek biztonsági hiányosságairól. Az általános dokumentumok megosztására kiválóan használható alkalmazások példáján felbuzdulva, sok felhasználó a személyes, titkos, vállalati dokumentumai megosztására is ezeket kezdi használni, ezzel viszont komoly veszélynek (adatvesztés vagy kompromittálódás) teszi ki ezeket az információkat.
- **Jelszavak:** Az örökzöld téma 2013-ban is jelen van. A könnyű használhatóság és az elégséges biztonság közötti egyensúly megteremtése továbbra is komoly kihívás a felhasználóknak mind személyes, mind vállalati szinten. Továbbra is nagyon elterjedt a rövid, könnyen megfejthető jelszavak használata, amelyekkel a támadók hozzáférhetnek a rendszereinkhez, adatainkhoz. 2012-ben például a Yahoo beismerte, hogy egyetlen komoly támadás során, mintegy 450 ezer jelszót törtek fel ismeretlenek.
- **Elveszett eszközök:** Ahogyan egyre kisebb és egyre okosabb személyes kütyük tömegével szerelik fel magukat a felhasználók, amelyek mindennel szinkronizálnak, minden személyes és üzleti információt naprakész formában hordoznak, úgy egyre nagyobb kárt okozhat ezek elvesztése, ellopása, egyszóval illetéktelen kezekbe kerülése. 2012 során a Cisco kutatásában megkérdezett alkalmazottak 26%-a nyilatkozott úgy, hogy elvesztett valamilyen technológiai eszközt, amin fontos adatok voltak. Az ilyen esetek hatványozottan növelik az adatszivárgás veszélyét.

Biztonságos internetezés Magyarországon

Az internetező felnőtt korú lakosság az esetleges internetes támadások ellen leginkább a vírusirtókban bízik (79%, de jelentős még a tűzfalat használók aránya is (60%). A válaszadók alig tizede (9%) nyilatkozott úgy, hogy a felsoroltak közül semmilyen védelmet nem használ internetezés közben.

Alkalmazott biztonsági eszközök a magyar lakossági felhasználók körében 2012.

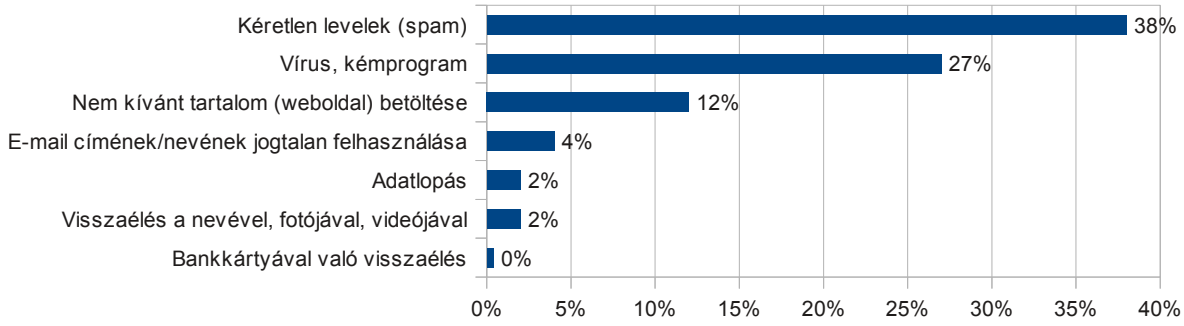


Forrás: Bellresearch[1]

Az internetező lakosság jelentős részét érték már kellemetlenségek internetezéssel kapcsolatban. 38%-uk kapott már kéretlen levelet, 27%-uk pedig már vírus vagy kémprogram áldozata is volt.

A személyes adatokkal való visszaélés a válaszadók állítása szerint nem volt jelentős: e-mail címükkel kapcsolatos visszaélésről 4%-uk számolt be, adatlopásról, fotóval visszaélésről 2-2%, bankkártyás károsult pedig alig akad közöttük. Ezen válaszok természetesen nem jelentik azt, hogy csak ilyen kevés visszaélés történt, csupán arról árulkodnak, hogy a válaszadóknak miről van tudomásuk.

Személyes érintettség internetes visszaéléssel kapcsolatban
a magyar lakossági felhasználók körében 2012.

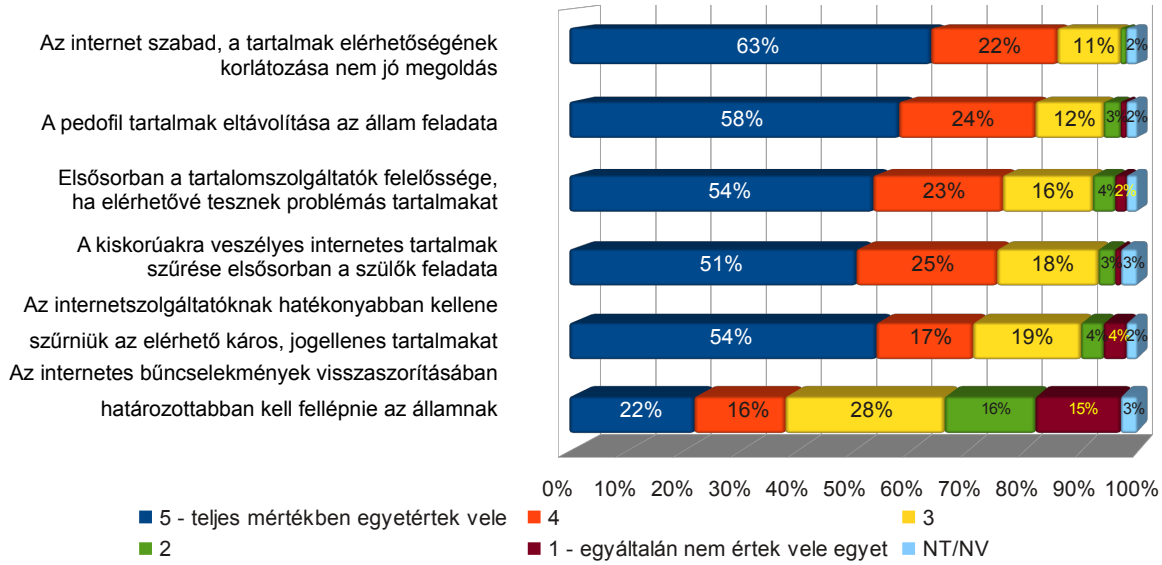


Forrás: Bellresearch[1]

Az internet biztonságát az internetezők szerint leginkább az államnak kellene szavatolnia, de a tartalomszolgáltatók felelősségét is felvetik a problémás tartalmak elérhetőségével kapcsolatban. A válaszadók szerint tehát az internet nem korlátozás, vagy jogmentes tér.

Habár a kiskorúakra veszélyes tartalmak szűrése részben a szülők feladata is (a válaszadók 77 %-a vélekedik így), a probléma ismertségének növelése és az eszközök biztosítása a szolgáltatók és a hatóság feladata.

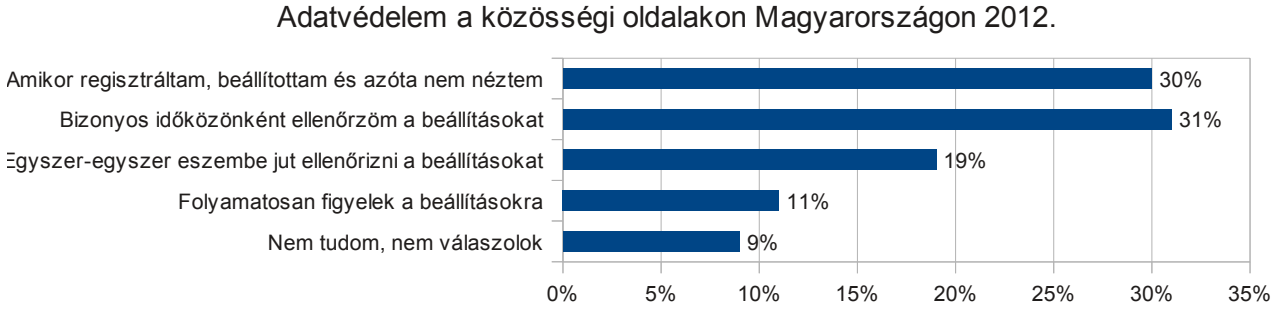
Vélemények az IT-biztonságról (lakossági felhasználók, Magyarország 2012)



Forrás: NMHH[5]

A 15 éves és idősebb közösségi oldalakat használók jelentős része (30%) csak regisztrációkor végzett adatvédelmi beállítást a profilján, azóta azt változatlanul hagyta, és mindössze 11%-uk az, aki folyamatosan figyelemmel követi beállításait. Összességében elmondható, hogy a közösségi oldalakat látogatók esetében az online válaszadók adatvédelmi szokásait az alkalmi odafigyelés jellemzi, hiszen 50%-uk bizonyos időközönként vagy egyszer-egyszer, alkalmanként ellenőrzi ezen beállításait.

Megjegyzendő ugyanakkor, hogy az általuk végzett adatvédelemmel kapcsolatos tevékenységet a válaszadók tökéletesen elégségesnek vélik, és magukról azt tartják, hogy nagyon odafigyelnek az adatvédelmi beállításokra, mint az a fókuszcsoportos kutatás tapasztalataiból kiderül.

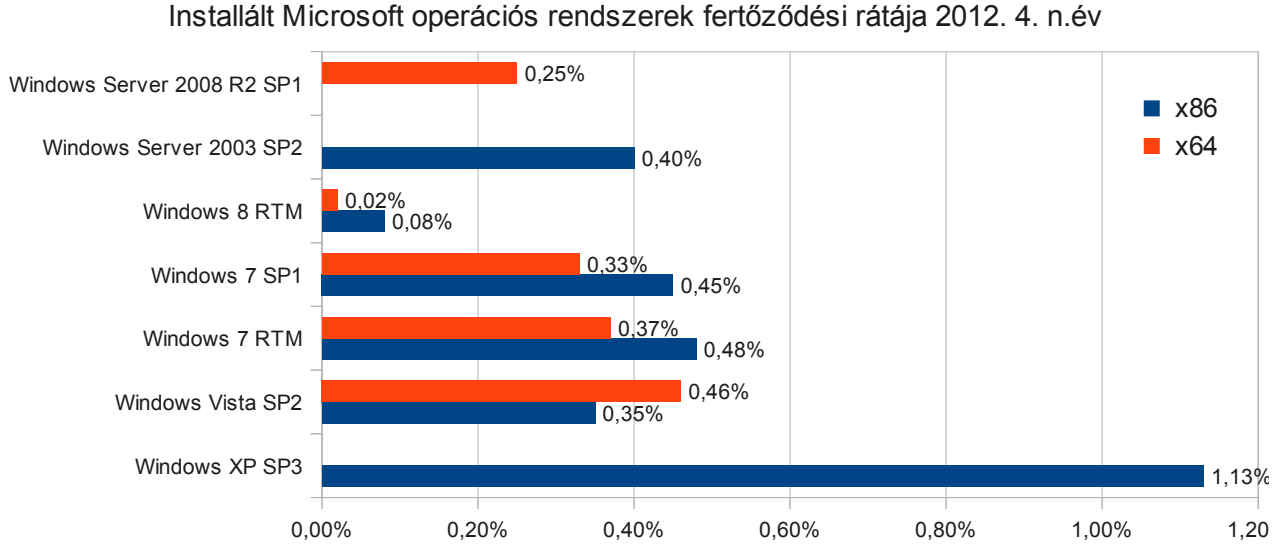


Forrás: NMHH[5]

Vírusvédelem

A Microsoft egyik legfrissebb tanulmánya külön kitért arra, hogy a számítógépek milyen szintű védelemmel vannak ellátva a különféle fenyegetettségekkel szemben. Kiderült, hogy a rendszerek 75%-án található víruskereső alkalmazás. Az ideális az lenne, ha ennél jóval több számítógépen lenne vírusvédelmi szoftver, de a Microsoft szerint a 75% is jobb arány, mint amire eredetileg számított.

A biztonsági kutatók egy érdekes megállapítást tettek, amivel a vírusvédelmi megoldások hasznát, szükségességét igyekeztek alátámasztani. Arra a következtetésre jutottak, hogy a naprakész víruskereső nélkül használt számítógépek átlagosan 5,5-szer nagyobb valószínűséggel fertőződnek meg, mint azok a rendszerek, amelyeket megfelelően frissített vírusvédelmi alkalmazás támogat.



Forrás: Microsoft[8]

"Az emberek tisztában vannak azzal, hogy a betörések ellen be kell zárniuk a házuk ajtaját. Mindez az informatikai biztonság terén sincs másként. Naprakész víruskereső nélküli webböngészés során nyitva hagyjuk az ajtót a kiberbűnözők előtt."

A Microsoft biztonsági megoldásai 2012 negyedik negyedévében összesen 3 millió számítógépen találtak és távolítottak el fertőzött e-mail csatolmányokat. Emellett 7 millió alkalommal ismertek fel olyan kulcsgeneráló (keygen) programokat, amelyek valamilyen vírust hordoztak.

8 Microsoft: Microsoft Security Intelligence Report, Vol. 14. 2013. január

Ezért a cég külön felhívta a figyelmet a nem legális forrásból származó szoftverek, filmek, játékok kapcsán felmerülő kockázatokra. Hasonlóan tette mindezt, ahogy például nemrégen az AVG is, amely szintén a nem hivatalos helyről beszerzett játékprogramok és kiegészítők veszélyeire világított rá. (Részletesen ld. a 2.3 alfejezetben.)

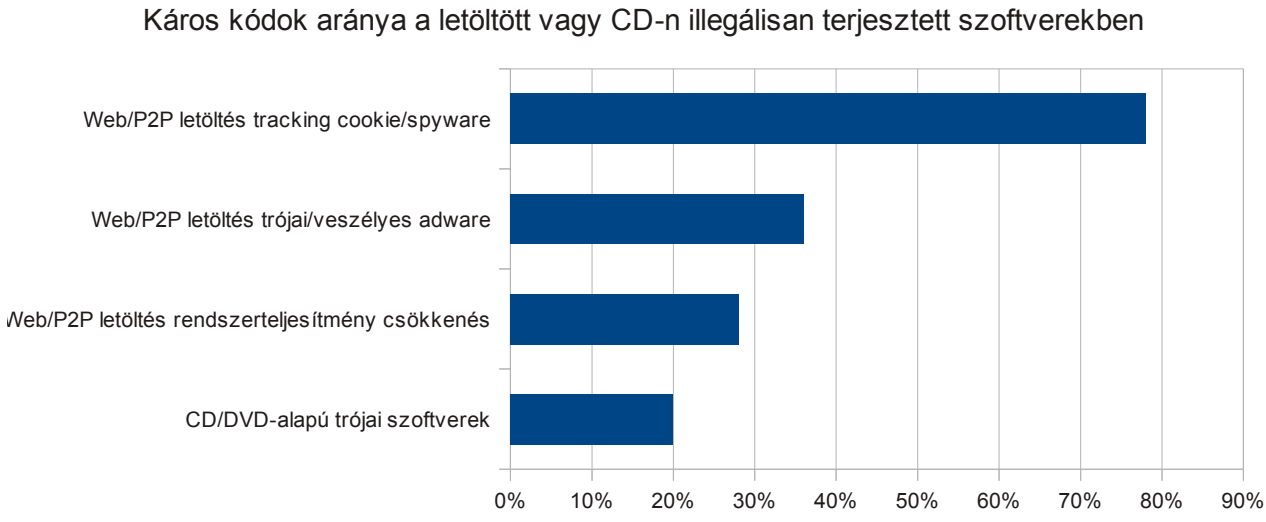
Illegális szoftverhasználat

A hazai felhasználók attitűdvizsgálatából is kitűnik, hogy az internetezők jelentős része próbál illegális úton szoftverekhez, tartalmakhoz jutni. Ennek veszélyeivel foglalkozik egy friss tanulmány, amelyet az IDC kutatóintézet készített a Microsofttal közösen. A probléma nem csak hazai szinten, de világméretekben is jelentős, és nem csak a szerzői jogok megsértése miatt, hanem a jelentős biztonsági aspektusok miatt is, amelyeket a kutatás feltárt.

Annak ellenére, hogy egyes felhasználók abban a reményben keresik az illegális szoftvereket, hogy pénzt takarítsanak meg, egy a háromhoz annak az esélye, hogy a magánfelhasználó számítógépe nemkívánatos, rosszindulatú kóddal fertőződik meg. A céges felhasználóknak még rosszabbak a kilátásaik: náluk ugyanez az arány egy a tízhez. (Most nem foglalkozunk a probléma azon aspektusával, amely többé-kevésbé egyértelmű: a szoftver szellemi termék, amelynek a tulajdonosa a szellemi termék előállítója, így ő határozza meg azt is, hogy ezt ingyenesen vagy pénzért bocsátja mások rendelkezésére.)

Az egész világra kiterjedő kutatás során 270 weboldalt és peer-to-peer (P2P) hálózatot, 108 letölthető szoftvert és 155 CD/DVD albumot vizsgált meg. Emellett kérdőíveztek is: 2077 fogyasztót és 258 IT-vezetőt vagy informatikai igazgatót kérdezett meg Brazíliában, Kínában, Németországban, Indiában, Mexikóban, Lengyelországban, Oroszországban, Thaiföldön, az Egyesült Királyságban és az Egyesült Államokban.

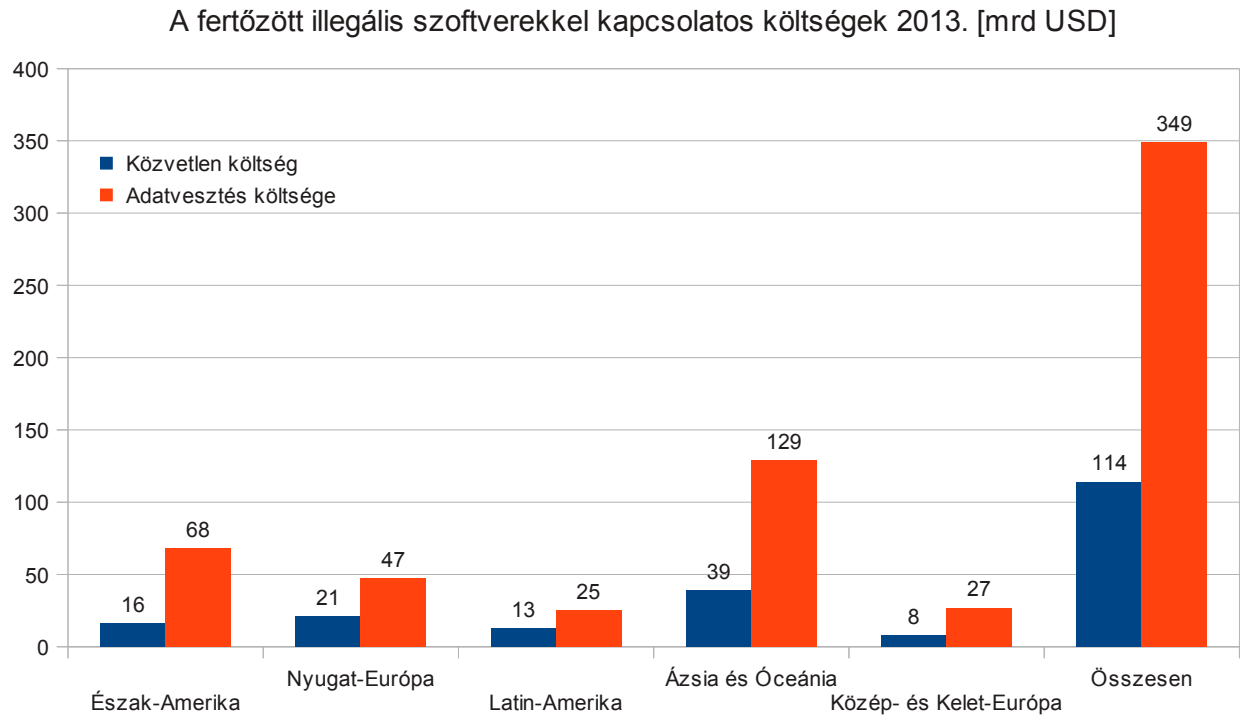
Az eredmények azt mutatják, hogy a nem számítógéppel vásárolt – azaz utólagosan feltelepített – illegális szoftverek 45%-a az internetről származik. Ezeknek a különféle weboldalakról és P2P hálózatokról letöltött szoftverek 78%-a tartalmazott valamilyen kémprogramot, 36%-a pedig trójait és reklámprogramot.



Forrás: IDC[9]

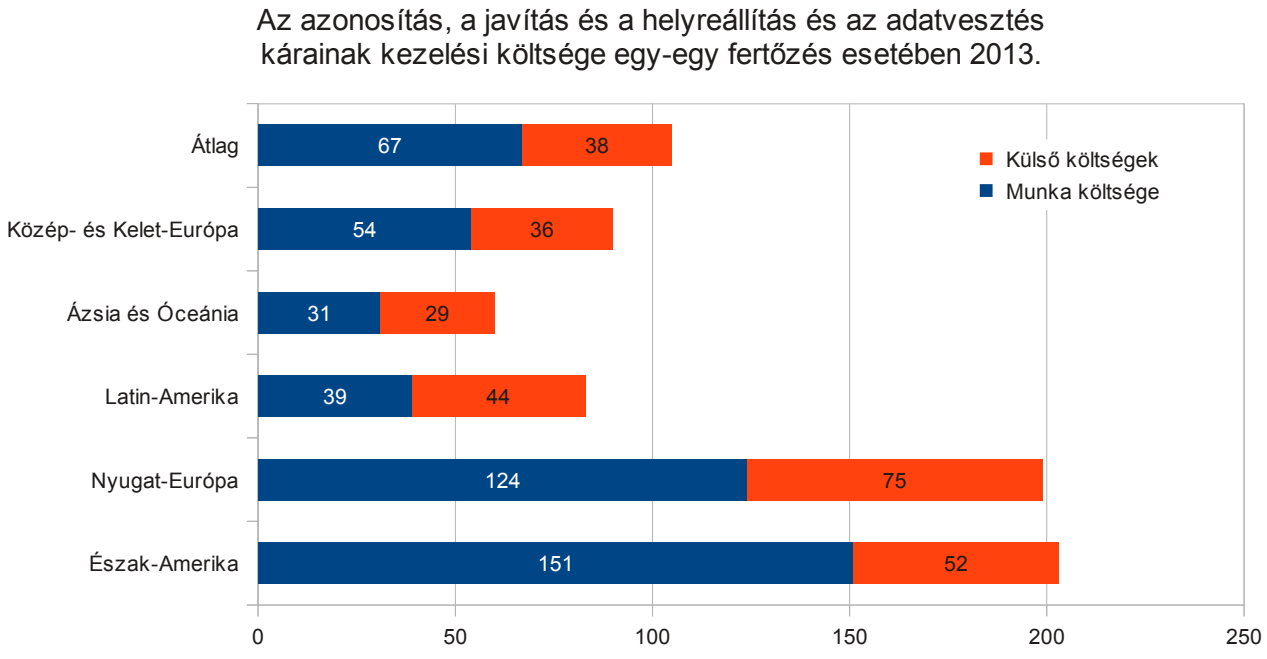
A kiberbűnözés úgy működik, hogy a programhamisítók a szoftver kódját módosítják, és hozzácsatolják a rosszindulatú alkalmazást. Az így telepített károkozók változatossága igen gazdag. Van köztük billentyűlenyomást naplózó keylogger, de olyan is, amelyikkel például a felhasználó gépén a mikrofont vagy a webkamerát lehet távolról aktiválni.

9 IDC: The Dangerous World of Counterfeit and Pirated Software, 2013. Március



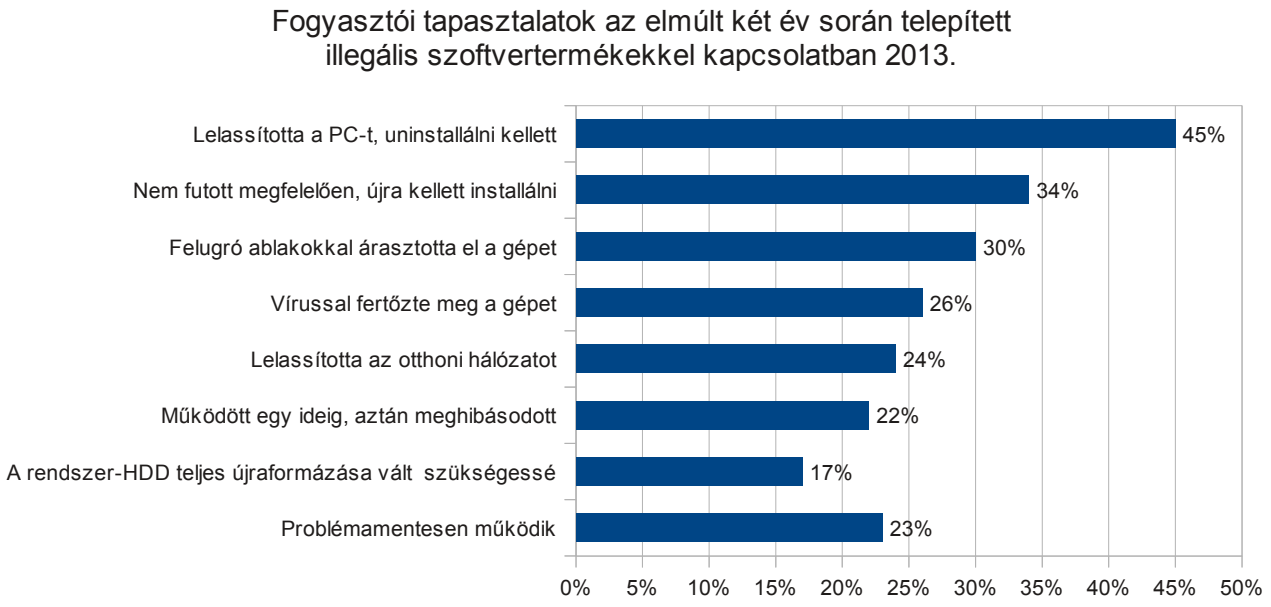
Forrás: IDC[9]

A fogyasztók világszinten 1,5 milliárd órát és 22 milliárd dollárt költenek a rosszindulatú alkalmazások megtalálására, ártalmatlanítására és az általuk okozott hatások megszüntetésére. A világméretű vállalatoknak pedig 114 milliárd dollárjába kerül a rosszindulatú szoftverek révén végrehajtott kibertámadások hatástalanítása (vélhetően évente, bár erről nem szól a kutatásról kiadott közlemény).



Forrás: IDC[9]

Azon válaszadóknak, akik tudatában voltak annak, hogy illegális forrásból beszerezett szoftver fut a gépükön, gyakran kellett szembenézniük biztonsági problémákkal. 64%-uk nyilatkozott úgy, hogy voltak már ilyen jellegű gondjai. Az esetek 45%-ában az illegális szoftver lelassította a számítógépet, és a szoftvert el kellett távolítani.



Forrás: AVG[10]

Persze azért alapvetően aggódunk: a válaszadók 48 %-a az esetleges adatvesztés miatt fél az illegális szoftverektől, 29%-uk egyébként leginkább a személyes adatok eltulajdonításától.

Az IDC tanulmány szerint a végfelhasználók előszeretettel telepítenek a vállalati számítógépeikre szoftvereket – valószínűleg engedély nélkül –, ami nagyon komoly biztonsági kockázatot jelent a vállalati rendszerre. Az IT vezetők 38%-a erősítette meg, hogy ez a jelenség létezik, sőt a dolgozók 57%-a maga is bevallotta, hogy telepített szoftver(eke)t a munkáltató tulajdonában lévő számítógépre. De azt sem titkolták, hogy ezeknek a szoftvereknek csak a 30%-a működött problémamentesen.

Érdekes adalék – sőt a cégek számára kicsit félelmetes is –, hogy mindössze az IT vezetők 65 %-a értett egyet azzal, hogy a felhasználók által telepített szoftverek fokozott biztonsági kockázatot jelentenek a szervezet számára.

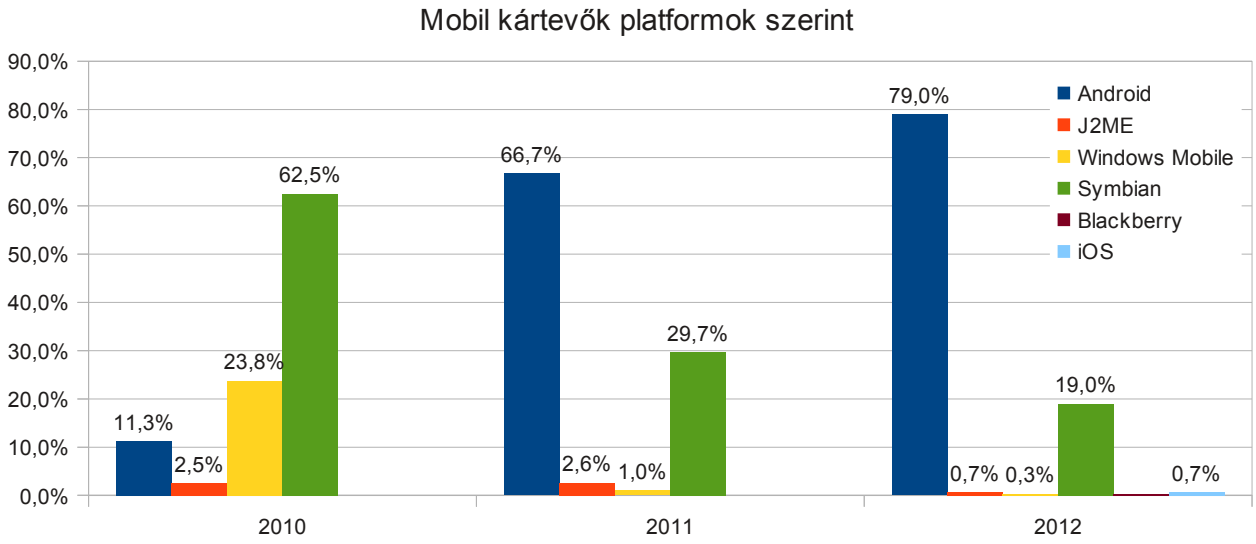
A felmérés fontos eredményeket jelenít meg, ám az ok-okozati összefüggésekre nem ad választ: A problémák gyökere valóban a programok illegalitásában keresendő, vagy inkább azzal függ össze, hogy aki a szoftverre nem költ, végképp nem foglalkozik a biztonsági kérdésekkel? Az igazság, mint általában itt is valahol középen keresendő, tehát a felelőtlen felhasználói attitűdnek legalább akkora szerepe van a veszélyes alkalmazások terjedésében, mint maguknak a fertőzött tartalmaknak.

Mobil biztonság

A válaszadók tizede talált már vírusfertőzést telefonján, harmada viszont semmilyen módon nem védi telefonját, 26 %-a nem is fizetne mobilos vírusvédelemért Az okostelefonok tulajdonosai átlagosan 16 alkalmazást használnak, viszont 44%-uk nem hajlandó fizetni az appokért.

Okostelefonokat, táblagépeket és a mobil biztonságot érintő felmérést végzett az Antivírusház Kft. Magyarországon, az F-Secure Hírek 50 000 olvasója megkérdezésével. A vizsgálat arra is kíváncsi volt, hogy a magyarok mire használják leginkább okos készüléküket, milyen applikációkat töltenek le, mennyit hajlandók fizetni ezekért, illetve mit tesznek meg online adataik védelméért. A megkérdezettek válaszaiból kiderül, hogy a magyarok háromnegyede rendelkezik okos eszközzel, közülük kétharmadnyian egy, egyharmadnyian pedig már két, vagy több okos készüléket mondhatnak magukénak.

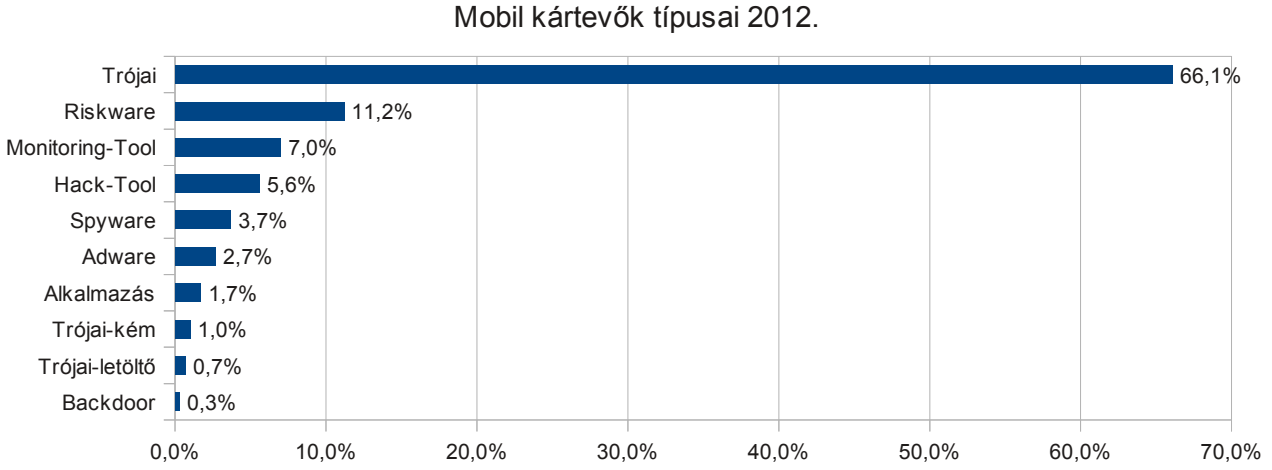
10 AVG: Insight April 2013. Issue 2.; The AVG Viruslab Research Group; 2013. április



Forrás: F-secure[4]

A mobilalkalmazások sérülékenységeinek egyik leggyakoribb oka, hogy a tapasztalatlan programozók nem fordítanak kellő figyelmet az adattárolás mikéntjére. Az SQLite-hoz hasonló adatbázis-kezelők megkönnyítik, hogy az adatokat helyben, a mobileszközökön tárolják. Ez az egyszerűség azonban visszaüthet, mert elkényelmesíti a fejlesztőt: hajlamos lesz nyílt szövegben vagy xml formátumban tárolni az adatokat.

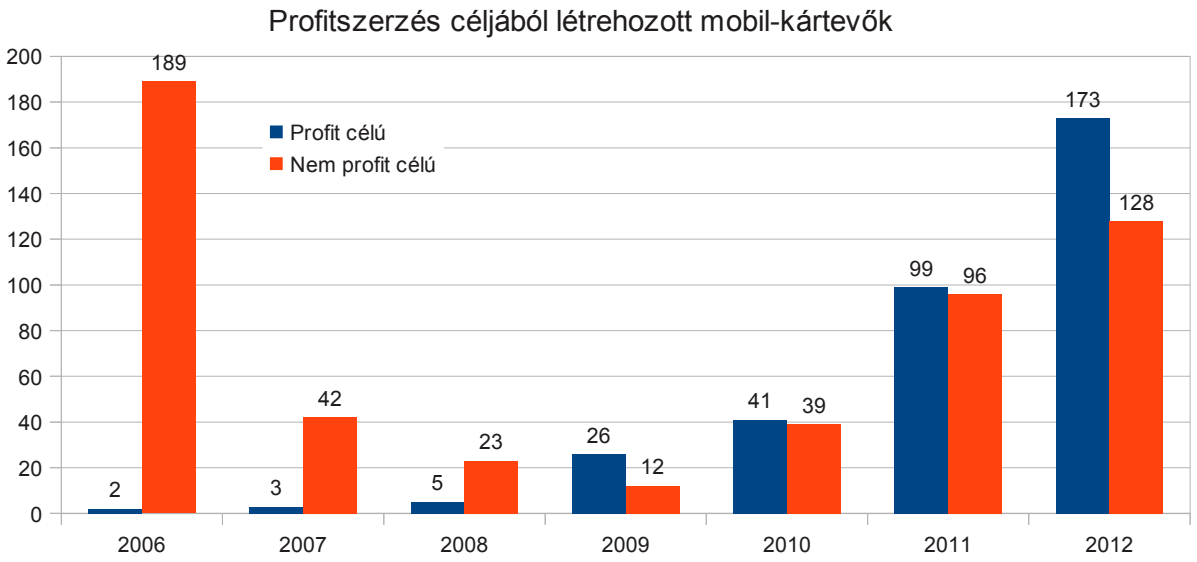
Az ilyen nyílt állományok viszont gyakorlatilag bárki számára elérhetővé teszik az alkalmazás adatait. Nem kell más, csak egy lezáratlan mobil és a rosszul megírt alkalmazás: könnyen ki lehet nyerni az alkalmazáshoz tartozó állományokat és azokban keresni. Ez igen veszélyes lehet, ha az adatbázis egy vállalati háttérrendszerhez kapcsolódik. Ezért aztán az érzékeny adatokat mindig titkosítsuk az eszköz szintjén, és a háttérrendszerekkel való kapcsolattartás során is csak titkosított kommunikációt alkalmazzunk.



Forrás: F-secure[4]

A felmérés során kiderült: a megkérdezettek 63 %-a dolgozik jelenleg, akiknek fele hozzáfér a céges levelezéshez és adatokhoz, ráadásul 45%-uk saját készülékről éri el a munkahelyi levelezést. A bizalmas adatok ugyanakkor könnyen hozzáférhetőek idegenek számára is: a felhasználók harmada semmilyen jelszavas védelmet nem használ okostelefonján, további 4% válaszolta azt, hogy nem is szeretne ilyen védelmet, mert fél, hogy elfelejti a kombinációt. A jelszót használók kétharmada számkódot, egyharmada pedig ábrát részesít előnyben a készülék zárjaként.

A munkaadók amiatt is aggódhatnak, hogy a válaszadók harmada amikor csak lehetősége van rá, felcsatlakozik az ingyenes wifi hálózatra és 53%-a pedig be is lép olyan oldalakra, amelyek felhasználónevet és jelszót kérnek. Az sem megnyugtató, hogy bár minden második megkérdezett fél attól, hogy ellopják telefonját, csak a válaszadók ötöde használ olyan applikációt, amely segítségével akár maga is megtalálhatná, 19%-a ismer, de nem használ, 43% pedig nem ismer és nem is használ ilyen alkalmazást.

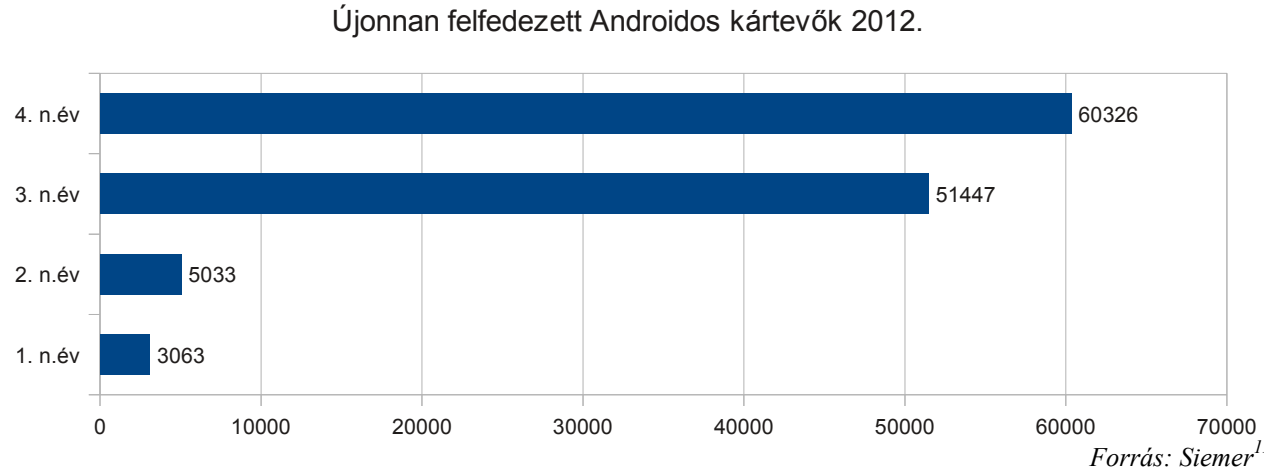


Forrás: F-secure[4]

Az Androidra írt mobilalkalmazásokat különösen veszélyeztetik a kártevők. Nem mintha a nyílt operációs rendszer sérülékenyebb lenne, hanem mert sokkal könnyebb a nem hivatalos forrásból (nem a Google vagy a készülékgyártók, szolgáltatók alkalmazásboltjaiból) származó alkalmazásokat telepíteni.

Használ ugyan megelőző védelmi mechanizmusokat a Google, de ezekkel sem lehet 100%-ig kiszűrni a kártevőket. Ezek írói ugyanis kisebb részekre bontják fel a kártevőt, hogy elkerüljék a detektálást, és általában népszerű alkalmazások nevével csábítják arra a felhasználókat, hogy letöltsék a fertőzött programot.

További kockázatokat jelentenek az Android esetleges frissítései és hibajavításai. Nem lehet arra számítani, hogy az Android majd időben frissíti magát, mert a Google Nexus eszközei kivételével a frissítések ütemezése a gyártók kezében van. Ez viszont megnehezíti, hogy mindig a legfrissebb (és remélhetően a leginkább védett) operációs rendszer legyen az eszközünkön.



Forrás: Siemer[11]

11 Siemer: Mobile Report Q1 2013., Siemer & Associates, LLC 2013. április

A modern telefonok és táblagépek egyre több funkciót kínálnak, a GPS-től az állandó internetkapcsolaton át a kameráig – ezek kiaknázása és összekapcsolása a telefonban tárolt információkkal egészen újszerű élményeket kínáló alkalmazások létrehozását teszik lehetővé. Nem mindegy azonban, hogy melyik alkalmazás és mikor fér hozzá ezekhez az erőforrásokhoz, és utána mit csinál azokkal.

A kártevők és mobilkockázatok elleni védekezés fontos összetevője, hogy a felhasználók tisztában legyenek azzal, miként állítják be telepítés után a mobilalkalmazások hozzáférési jogait. Az Android készülékeken minden esetben a felhasználónak kell jóváhagynia, ha egy alkalmazás hozzá akar férni más alkalmazásokhoz vagy adatokhoz, ezeknél viszont legalább olyan körültekintéssel kell eljárni, mint az ismeretlen feladóktól származó levelek csatolmányainak megnyitásakor. (A legtöbb ingyenes app „teljes internet-hozzáférést” igényel általában csak a reklámjai letöltése – rossz esetben pedig rosszindulatú működés – céljából.)

A veszély ráadásul nem csak Androidon áll fenn. A Path nevű alkalmazás például a barátokkal való kapcsolattartás egészen újszerű módjait kínálta, és általános elismerés övezte kiváló kezelőfelületét. Az azonban csak később, és szinte véletlenül derült ki, hogy a Path teljes kontaktlistákat töltött fel saját szervereire, az iOS-változat még csak engedélyt sem kért ehhez. A Path fejlesztőjének végül bocsánatot kellett kérnie az illetéktelen adatkezelésért.

A felhasználók többsége nincs tisztában azzal, mekkora értéket képvisel telefonjának címlistája, azzal pedig senki nem foglalkozik, hogy egy alkalmazás licencszerződése mit ír a személyes adatokhoz való hozzáférésről. A Path fejlesztőinek szándéka talán nemes volt – hiszen csak fokozni akarták a felhasználói élményt –, de egy kevésbé etikus fejlesztő ugyanezeket az adatokat kéretlen levelek küldésére, marketingre vagy éppen támadásokra is felhasználhatná.

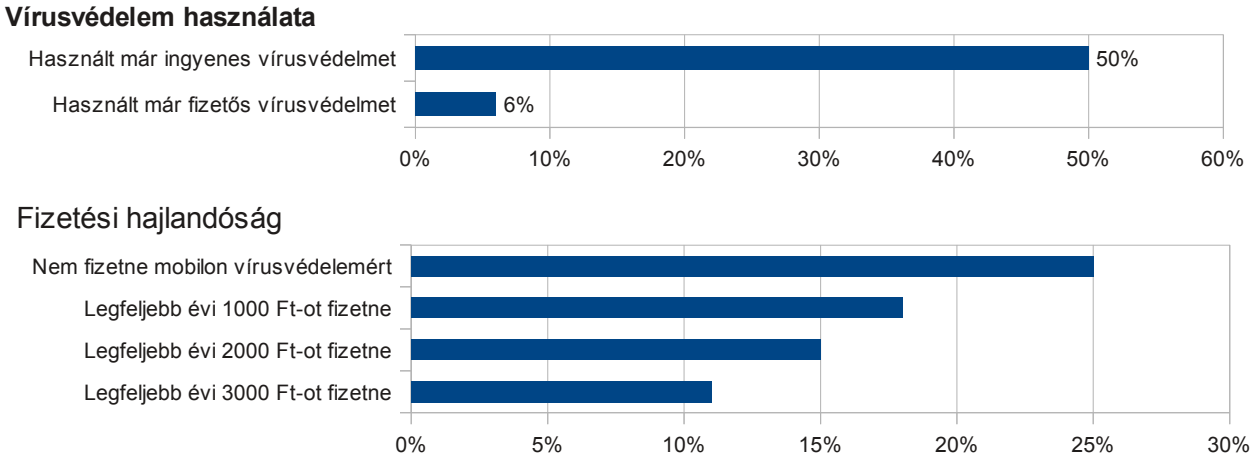
Veszélyesek lehetnek az adataikat a felhőben szinkronizáló alkalmazások is. A Dropbox-tól például kikerült jó néhány jelszó, ami számos felhasználói fiókot megnyitott egy hekker előtt. Szerencsére ebből az esetből nem lett nagyobb kár, mint néhány kéretlen levél, de ez csak a véletlenen múlt.

A Dropboxot más alkalmazások is használják az eszközök és egyéb szolgáltatások közötti szinkronizációra. Az alkalmazásfejlesztő vagy szolgáltató védelmi mechanizmusait a felhasználó nem tudja teljes mértékben ellenőrizni, csak abban bízhat, hogy a nyilvánosságra hozott biztonsági elveiket betartják és folyamatosan fejlesztik. Ám ha valami biztonsági probléma derül ki ezeknél a szolgáltatásoknál, az értesítés és a jelszó megváltoztatása általában email útján történik. Ha azonban a felhasználó ugyanazt a jelszót használta a felhőszolgáltatáshoz és az elektronikus levelezéshez is (például a Gmailhez), már ebben a módszerben sem bízhat – semmi nem garantálja, hogy leveleihez nem fértek hozzá.

Úgy lehet a leginkább kivédeni ezeket a veszélyeket, ha minden egyes alkalmazáshoz és szolgáltatáshoz más jelszót használunk (ami viszont jelentős nehézségeket okoz a könnyű használat szempontjából). A felhasználók azonban – úgy látszik – már tisztában vannak a megfelelően biztonságos jelszó jelentőségével: a válaszadók 35%-a mindig mindenhol más jelszót használ; 28%-a eltérő, de bejáratott jelszavakat alkalmaz, 16%-nyian alkalmazzák a jelszavakat kis módosításokkal és csak egyötödük válaszolta azt, hogy mindig, mindenhol ugyanazt a jelszót használja. Ráadásul a válaszadók 89%-a mindig használ kis- és nagybetűket, számokat és különleges karaktereket a jelszavak létrehozásakor.

A megkérdezettek ötöde még nem használt vírusirtót mobiltelefonján, de szeretne kipróbálni egyet, mivel tart a mobil vírusoktól. A válaszadók közel fele már használt ingyenes mobil vírusirtót, további 6% pedig már fizetett is érte. Aki használt már mobil antivírust, annak 14%-a pedig már többször is talált vírust telefonján.

Mobil vírusvédelem alkalmazása Magyarországon 2012.



Forrás: F-secure[3]

A mobilos vírusvédelemért a válaszadók negyede nem hajlandó fizetni, harmada pedig legfeljebb évi 2000 forintot, 11%-a pedig némileg többet, legfeljebb 3000 forintot adna egy mobil vírusirtóért.

Phishing

A phishing, vagyis a különböző kártékony kódokon és/vagy megtévesztéses támadásokon keresztüli adatlopás évek óta a felhasználók által egyik leginkább félt támadási forma.

Ahogyan a felhasználók egyre tudatosabbá és a védelmi megoldások egyre fejlettebbé válnak a támadóknak is fejlődniük kell, ha hasonló hatékonyságot akarnak elérni támadásaikkal, mint korábban.

Ennek a tendenciának egyik eredménye az új, magasan célzott, szinte teljes mértékben személyre szabott adathalász támadások megjelenése. A személyre szabás, az ismeretek ugyanis segítenek elaltatni az áldozat gyanakvását. Ezt az új módszert az angolszász terminológiában „spear phishing”-nek, vagyis szigonyos halászatnak nevezik. Az analógia jól látható, még a hagyományos adathalászat a nagy háló kivetését jelenti, amibe vagy beleakad valaki vagy nem, ezek a támadások pontos, személyre szabott formát öltenek.

Ennek alapesete, mikor az adathalász e-mail nem „Tisztelt ügyfelünk”, „Hölgyem/Uram” stb. megszólítással kezdődik, hanem névre szólóan érkezik (pontos adatok, rang, pozíció ismeretében) kifejezetten a címzett e-mail címére. Ehhez elsősorban a nem megfelelően védett a WEB 2.0-s alkalmazásokból, közösségi hálózatokról szedik össze a csalók az információkat. E célzott támadások 2012 során már mintegy 4 milliárd USD kárt okozta világszerte. Az elkövetési szám alacsonyabb, hiszen a célzottság elérése több munkával jár, viszont általában a kárérték is magasabb egy-egy sikeres támadás esetében.

A támadáshoz használt e-mail általában fertőzött mellékletet tartalmaz, vagy egy olyan linket, ami kártékony kódokat telepítő weboldalra mutat. A malware ezután eléri a vezérlő szervert és várja a támadó utasításait adatlopásra vagy éppen kéretlen levelek továbbítására.

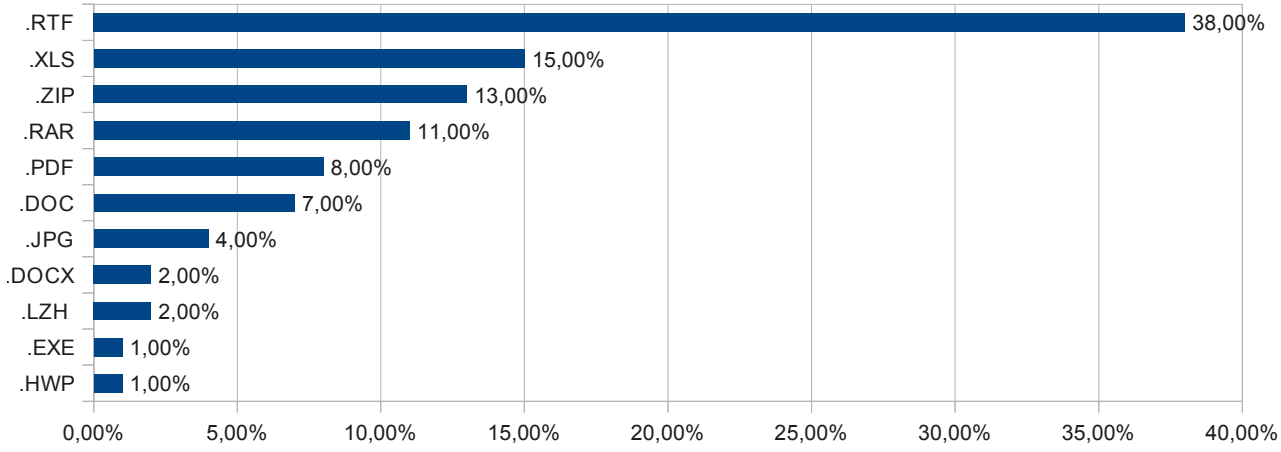
Célzott adathalász e-mailek csatolmánnyal vagy anélkül 2013.

Forrás: Trendmicro[12]

12 TrendLabs APT Research Team: Spear-Phishing Email: Most Favored APT Attack Bait, Trendmicro Research Paper,

A csatolmányok a leggyakoribb fájltípusok közül kerülnek ki, jellemzően olyan dokumentumok, amelyeket amúgy is használnak felhasználók (.doc, .xls), a futtatható fájlok (mint a .exe) nem különösebben népszerűek, mert ezeket a legtöbb védelmi megoldás szűri, ezért ezeknek inkább a betömörített formáját használják a támadók.

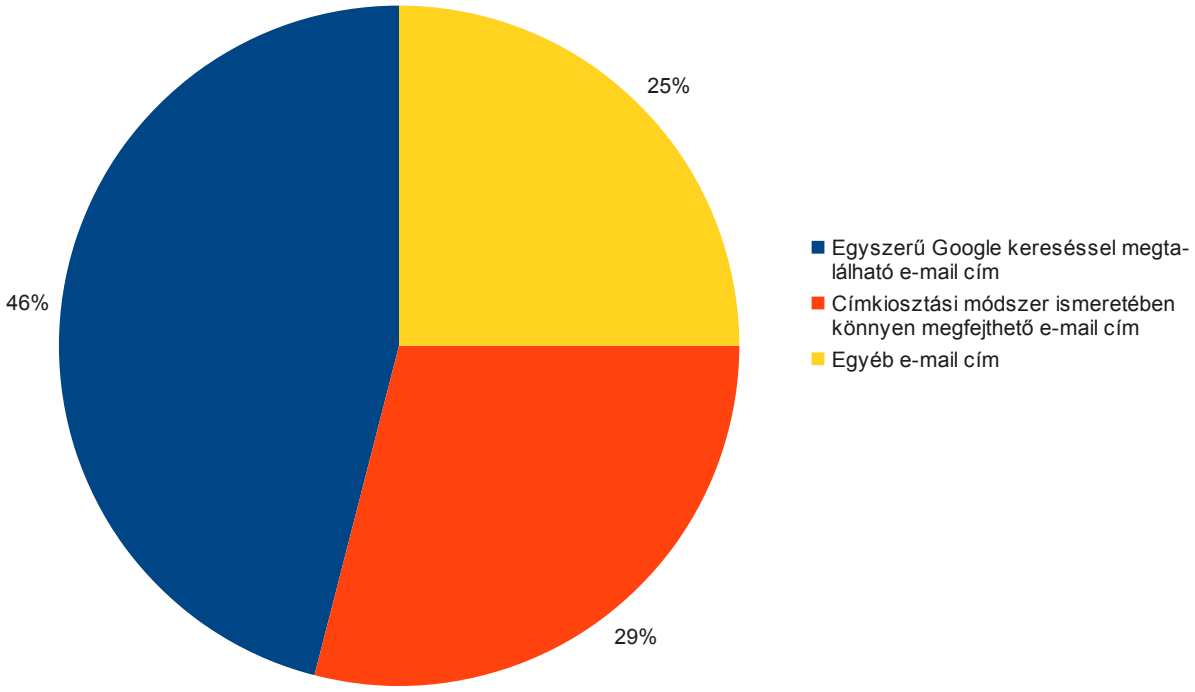
A célzott adathalászathoz használt leggyakoribb csatolmánytípusok 2013.



Forrás: Trendmicro[12]

A védekezés legjobb lehetősége, ha semmilyen formában nem tesszük nyilvánossá elérhetőségeinket. Megkérdezett áldozatok 46%-ának egyszerű Google-kereséssel megtalálható volt az e-mail címe valamilyen publikus felületen. Az első biztonsági lépcsőt megugró felhasználók 53%-ának e-mail címe egyszerű ráhibázásos módszerrel, az adott vállalat vagy e-mail szolgáltató szokványos címkiosztási módszerének (pl. vezetéknév.keresztnév@akarmi.hu) ismeretében könnyen kitalálható volt. Tehát az esetek ¾-ében a támadás egyszerűen kivédhető nem nyilvános és nem szokványos e-mail cím használatával.

A célzott adathalászatnak áldozatul esett felhasználók elérhetőségei 2013.

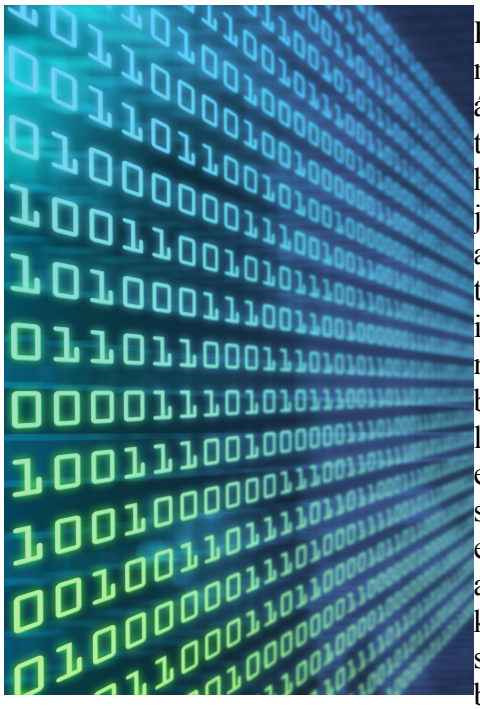


Forrás: Trendmicro[12]

[12] 2012. december

Social engineering, mint alábecsült veszély

Az elmúlt években egyre több szakember, cégvezető és egyéb kompetens személy nyilatkozott az informatikai biztonsággal kapcsolatban és talán meghökkentő, hogy milyen nagy hangsúlyt fektetnek az IT biztonság technikai szempontjaira az emberi hibából fakadó adatszivárgási problémákkal kapcsolatos megfontolások rovására.



Rendszerint számos aggály támad akörül, hogy hogyan kell megvédeni az IT rendszereket a szuper intelligens hackerek által kivitelezett, kifinomult támadásokkal szemben, miközben teljesen figyelmen kívül hagyják a szabályzatokat, a házirendeket és az eljárásokat be nem tartó személyzet által jelentett kockázatokat, illetve a személyzet megtévesztésére alapozó, ún. social engineering típusú, adatszerzésre irányuló támadásokat. Az adatvédelmi szabályok gyenge implementálása - például a nem megfelelő ellenőrzések és a meggondoltság hiánya - nagy veszélyt jelentenek az információ biztonságra. Különféle sérülékenységek is felszínre kerülhetnek legfőképp ott, ahol az emberek lusták, vagy nem értik az előírások be nem tartásának következményeit. Mindazonáltal számos módon lehet manipulálni az embereket social engineering eszközökkel, amely a támadásokat elősegítő adatszerzésre irányul, és ezt a kockázatot gyakran figyelmen kívül hagyják. Ebben a cikkben felvázoljuk, hogy mi is az a social engineering, és hogyan jelent kockázatot az információ biztonságra nézve.

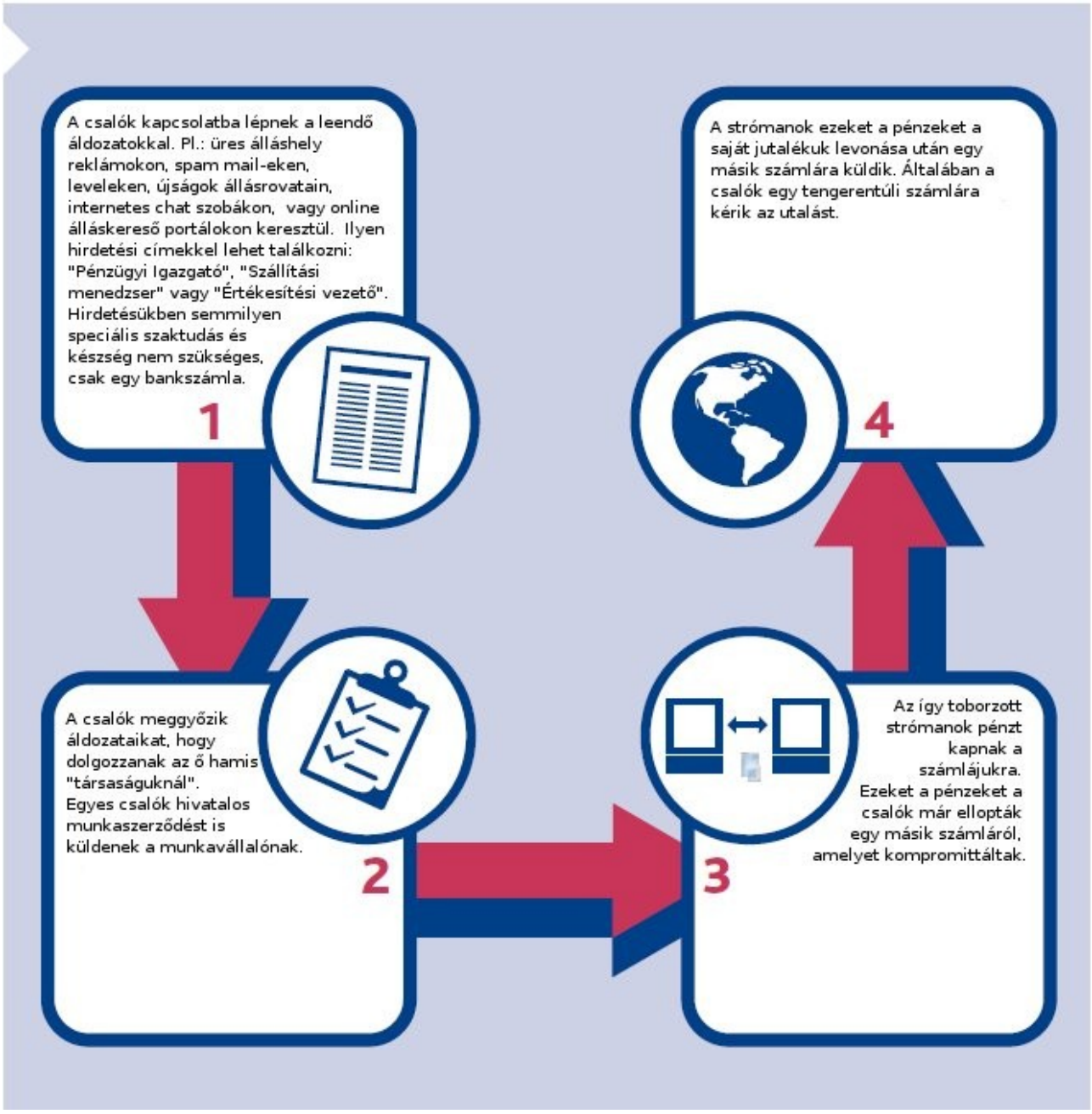
Mi is az a social engineering?

Social engineering-nek olyan tevékenységet nevezünk, amikor manipulálják az embereket, olyan dolgokra veszik rá őket, amelyek következtében kompromittálódhat a biztonság vagy bizalmas információk kerülhetnek nyilvánosságra. Kevin Mitnick szerint - aki egy jó útra tért számítógépes bűnöző - sokkal könnyebb rávenni valakit, hogy adja meg a jelszavát, mint feltörni a rendszerét.

A trükkök - hogyan csinálják?

A social engineering talán legismertebb eszköze az adathalászat - egy legitimnek látszó email vagy levél, egy intézmény vagy hatósági személy nevében azzal a céllal, hogy személyes vagy bizalmas információkhoz férjenek hozzá a támadók. Meglepő lenne, ha lenne olyan személy, aki nem kapott még olyan email-t például egy nigériai hercegtől vagy valaki hasonlótól, azzal a kecsegtető ajánlattal, hogy gyorsan, kisebb vagy nagyobb összeghez tudna jutni, amennyiben némi pénzt utalunk neki. Mindössze csak a nevünkre, címünkre és a banki adatainkra van szükség hozzá... Ezeket az adathalász támadásokat már könnyű észrevenni, de az ebben a témában kiküldött levél puszta mennyisége és az a tény, hogy ezek a levelek még mindig postafiókokban landolnak azt sugallja, hogy a küldők még mindig sikeresen vezetnek félre embereket. Továbbá bizonyos embercsoportokat különválasztják az ún. social engineer-ek, mivel egyes emberek fogékonyabbak az adathalászatra.

Vegyük például a piramisjátékokat, amelyekkel gyakran célozzák az idősebb embereket, akikről feltételezik, hogy van befektetni való pénzük, van idejük és talán magányosak, ezért örülnek a figyelemnek. Egy másik példa lehet a közelmúltban a diákokat, munkanélkülieket és külföldi állampolgárokat célzó pénzmosási átverés. Nem tudni, hogy a célszemélyeket a pénz keresés utáni kétségbeesés, a rossz gazdasági helyzetük, és/vagy az adott ország jogszabályainak és a banki normáknak hiányos ismerete hajtja-e a social engineer-ek karmai közé, de ezek az áldozatok könnyen rávehetők a „money transfer agent" vagy a „payment processing agent" szerep betöltésére. (lásd www.bbc.co.uk/news/business-21578985). A célszemélyek ekkor gyakorlatilag a saját bankszámlájukon keresztül mossák a bűnözők pénzét és egy százalékot kapnak a szolgálataikért. Ez természetesen illegális és végzetes következményekkel járhat az áldozatok számára, akik a végén a bűnügyi nyilvántartásban végzik és/vagy le is tiltják a bankszámlájukat.



Money Mule - a pénzmosás egy lehetséges változata

Bizonyított, hogy az adathalász támadások egyre kifinomultabbak. Egyre több az olyan legitimnek tűnő email, amely alig vagy csak nehezen megkülönböztethető az eredeti banki email-től. Ezen levelek megfogalmazása már nyelvtanilag is teljesen tökéletesnek mondható. Amerikában arra is van példa, hogy nagy cégeknél dolgozó személyeket célzottan keresnek meg hivatalosnak tűnő levelekkel, amelyekben tájékoztatják őket, hogy meg kell jelenniük a bíróságon. Ezek az e-mailek persze, rosszindulatú hivatkozásokat tartalmaznak. A célzott támadások jellege azt eredményezte, hogy elterjedt a spear phishing[13], és nem lenne meglepő, ha az ilyen támadások továbbfejlődnének a jövőben, mivel a célzott jellege növeli az esélyét annak, hogy az emberek eleget tesznek az email-beli kéréseknek.

Bár az adathalászat talán a leginkább közismert social engineering taktika, de semmi esetre sem az egyetlen. Számos más módja van annak, hogy a social engineer meggyőzze az embereket, hogy osszanak meg bizalmas információkat, vagy tegyék lehetővé számukra, hogy olyan rendszerekhez kapjanak hozzáférést, amelyhez nem lenne szabad hozzáférniük. Például:

- **Ismeretség kihasználása** - ez az egyik legjobb taktika, és egyik sarokköve social engineering támadásoknak. Dióhéjban, a támadó megpróbál arra törekedni, hogy mindenkinek úgy tűnjön, hogy amit csinál az teljesen normális.. Például úgy tesz, mintha egy munkavállaló lenne, hogy hozzáférést szerezzen valamihez – az azonosító kártyákat el lehet lopni vagy le lehet másolni, egyenruhát pedig vásárolni lehet. Ezt kombinálva a rossz hozzáférés-ellenőrzési eljárásokkal, könnyű zsákmányszerzési mód a social engineer-ek számára.

- **Pretexting** - a social engineer egy kitalált forgatókönyvet (másnével pretext) hoz létre és használ, azért hogy bevonja a célszemélyt oly módon, hogy növelje az információ nyilvánosságra hozásának vagy a tevékenység módosításának esélyét. Ez ismert még blagging-ként is.

- **Eltérítéses lopás** - a social engineer meggyőzi a szállításért felelős legitim személyt, hogy a szállítmányt máshol várják, és ellopja azt.

- **Csali (baiting)** - az igazi trójai. Ez az áldozat kíváncsiságra és a kapzsiságára alapoz, „túl jó, hogy igaz legyen” típusú befektetési lehetőségekkel.

- **Hatalmi pozícióban lévő személy megszemélyesítése** - ez egy általánosan használt taktika a social engineer-ek által. Az e-mailekben azt állítják, hogy ők méltóságok/hercegek, bűnüldözésben dolgozó személyek, vagy más hatósági személyek. A személyesség, a bizalmasság látszata és a meggyőző hazugság a social engineer számára hozzáférést eredményezhet bármilyen helyhez.

- **Követés**[14] - meglepően könnyű követni embereket védett helyekre. Az ajtók nyitva tartásának udvarias gyakorlata a social engineer-ek álma. Őszintén szólva, a legtöbb ember nem szeret konfrontálódni és nem valószínű, hogy feltartóztatja az ily módon jogosulatlanul besurranót.

- **Ellenségesség, rosszindulat** - ellentétben azzal, amit gondolnánk, a social engineer-ek alkalmanként, szeretik felhívni magukra a figyelmet azzal, hogy nagyon ellenségesek. Ez

13 Az adathalászat egy speciális fajtája. A támadási módszer lényege, hogy nem tömegeket érint, hanem csak egy jóval kisebb csoportot. A támadás egyik célja többek között az, hogy kártékony szoftvert juttassanak a célszemély számítógépére.

14 Tailgating

azért van, mert az emberek általában meg akarnak szabadulni az erőszakos emberektől, így sokkal valószínűbb, hogy teljesítik a kívánságait, és épp ezért működik jól ez a módszer, például ha megkéri az embereket, hogy nyissák ki az ajtót, vagy adjanak információt bizonyos dolgok helyéről. Egy példa a valós életből, hogy ha valaki elkezd vitázni valakivel egy ellenőrzési ponthoz érve, ami jelen esetben legyen a bejárat (pl. ha alkoholt próbál becsempészni egy fesztiválra), akkor a biztonsági személyzet nagy valószínűséggel átengedi ezeket az embereket és nem fogja őket átvizsgálni.

- **Valamit valamiért**[15] - ez az, ahol a social engineer felajánl valamit valamiért cserébe. Például az elégedetlen alkalmazottak megkörnyékezhetőek, hogy készpénzért cserébe adjanak bizonyos információkat.

Szemben azzal, amit sokan gondolnak, a social engineer alkalmanként, szeretné felhívni magára a figyelmet azzal, hogy ellenséges.

Sok technikát és megközelítést alkalmazhat a social engineer annak érdekében, hogy megkönnyítse a munkáját. Például:

- **Felügyelet** - célok azonosításában a rutin segít meghatározni a megközelítés legjobb módját. Azonban a megközelítésnek nem mindig kell közvetlennek lennie. Vegyünk például egy olyan forgatókönyvet, ahol a munkavállalói csoport rendszeresen ugyanabba a kocsmába megy péntek esténként. Néhány alkohol tartalmú ital elfogyasztása után könnyen olyan beszélgetés kerekedhet, amely bizalmas információk megosztásához vezethet.

- **A naivitás maximális kihasználása** - ezt a módszert a következő példa szemlélteti a legjobban. Tegyük fel, hogy épp egy vonaton ül csúcsidőben, amikor egyszer csak hallja, hogy a mögötte lévő egyik ember úgy dönt, hogy telefonon keresztül fizeti ki egyik számláját. Mire eljut a fizetési adatok megadásáig, elő tud venni egy tollat és egy jegyzettömböt, és képes lenne felírni minden hitelkártya információját, beleértve a 3 jegyű biztonsági kódot is a kártya hátulján. Képzelje el mi történhetne ha ezek az információk rossz kezekbe kerülnének...

- **A közösségi oldalak** - a LinkedIn, a Facebook, a Twitter és más közösségi oldalak rengeteg információt tartalmaznak. Meglepő, hogy mennyi személyes adatot lehet elérni valakiről a profilján keresztül. Ismerve az ilyen jellegű információkat, lehetővé válik egy idegen számára, hogy beszélgetésbe elegyedjen azt színlelve, mintha ismerné. Amennyiben nem elég óvatos, akkor további bizalmas információkat szerezhet, hogy a szándékához szükséges kulcsfontosságú információhoz hozzájusson. Néhány ember azt is megjeleníti, közzéteszi, hogy hol van az adott időpontban, és még azt is elárulja, mikor mennek nyaralni! Képzelje el, hogy Ön egy social engineer, és tudja, hogy István nyaralni megy - nem csak kifosztani tudja a házát, hanem felhasználhatja a róla szerzett személyes információkat és felhívhatja a munkahelyét, azt állítva, hogy együtt dolgozik vele valami fontos és sürgős munkán, és információt kér erről. Ez esetben csak az alkalmazott adatvédelmi szabályok minőségén múlik, hogy esetleg további bizalmas információkhoz jusson István egyik kollégájától.

- **Az új technológia** - ma már könnyebb személyazonosságot igazoló vagy belépő kártyákat hamisítani. Mindenféle apró kamerák és mikrofonok léteznek a piacon, amelyek segítik a social engineer-t az információgyűjtésben.

15 Quid pro quo

- **Szolgáltatások** - minden olyan szolgáltatás, amely magában foglalja a geotagging-et[16], könnyen árulkodhat a social engineer számára, hogy épp hol van. Nézzünk egy szituációt - ellop egy hitelkártyát egy idős hölgytől és szeretne vele drága termékeket vásárolni. Ennek megvalósításához meg kell változtatnia a hitelkártyához tartozó számlázási címet. A probléma az, hogy Ön nem egy idős hölgy és tettetni sem tudja ezt, így ha a bank Önt hívja, akkor lebukik. Amennyiben nincs egy ismerőse, aki az Ön nevében felhatalmazással járna el, akkor például vásárolhat egy ilyen szolgáltatást. Hiszi vagy sem, léteznek olyan cégek, akik 7-15 dollárért telefonálnak Ön helyett a bankba az Ön érdekeit képviselve, amennyiben elég információval látja el őket, a különféle biztonsági ellenőrzéseken történő átjutáshoz.

Kockázatos üzleti élet - veszélyben vagyok?

Igen! Mindenki kockázatnak van kitéve, hogy egy social engineer célpontjává válhat. Még ha egy social engineer úgy is gondolja, hogy közvetlen nem tud kapcsolatba lépni Önnel, úgy próbálkozhat a barátain, családján, kollégáin keresztül. Például, feltörhetik a barátja email fiókját, majd egy üzenetet küldenek amiben kérik, hogy egy linkre kattintson. Mivel megbízik a barátjában, Ön nagy eséllyel rá fog kattintani a linkre.

Tanácsok a kockázat csökkentésére

Személyes nézőpontból nézve, valószínűleg a legjobb tanács egy régi, de bevált mondás: „Ha valami túl szép, hogy igaz legyen, az valószínűleg átverés”. Valamint, ha egy email vagy levél hitelességében kételkedik, használjon független forrásokból származó elérhetőségeket (a levélben szereplők helyett), hogy ellenőrizhesse azt.

Egy vállalat alkalmazottjaként meg kell bizonyosodnia arról, hogy nem használják e ki üzleti titkok megszerzésére. Ilyen helyzetben, a social engineering alapos ismerete valamint egy kérdezősködő természet segíthet - például, ha valaki akit nem igazán ismer, valami bizalmas dologról érdeklődik, ne habozzon és kérdezzen vissza bátran.

Amennyiben kételyei támadnak, bizonyosodjon meg róla egy megbízható forrásból, hogy az az információ megosztható azzal a bizonyos személlyel, mielőtt kiadná. Valamint kövesse az adatvédelmi szabályzatokat - például ha azt az utasítást kapta, hogy a személyes emailjeit a munkahelyén ne olvassa, ne gondolja azt, hogy a munkáltatója túlzottan szigorú lenne, mivel valószínűleg nagyon jó oka van ennek.

Munkáltatóként vagy üzleti félként sose feledkezzen meg arról, hogy hasznos és bölcs dolog a technikai védelmi rendszerekre pénzt költeni, és ha alkalmazottjait nem készíti fel a social engineering támadások kivédésére, valamint a szabályzatokban foglalt adatvédelmi korlátozásokra, a rendszere még mindig sebezhető marad. Fontos elmagyarázni az alkalmazottak számára, hogy bizonyos, a szabályzatban foglalt pontok miért vannak életbe léptetve. Például, ha a személyes email fiókokhoz való hozzáférés tiltva van, ezzel csökkentve a kártékony programok letöltésének kockázatát, akkor tájékoztassa a személyzetet ennek okairól.

A „legkevesebb jogosultság”[17] alapelvének az alkalmazása szintén megfontolandó, melynek lényege, hogy a felhasználóknak csak bizonyos helyekhez van hozzáférése - alapvetően az „amennyit ismerni kell” lefordítható az „amennyihez hozzá kell férni” elvére. Összességében, amennyiben valaki nem fér hozzá egy rendszerhez, nem lesz képes visszaélni vele (akár szándékosan, akár véletlenül).

16 különböző médiák földrajzi adattal történő ellátása, például hol készült a fotó.
17 Least privilege

Szintén ajánlott a behatolás tesztelők alkalmazása, akik megfelelően tesztelni tudják a biztonsági eljárások hatékonyságát, többek között social engineering támadásokkal célozva a vállalatot. Az Ön által kért bármely biztonsági intézkedést képesek tesztelni, majd az eredmények tükrében ajánlásokat fogalmaznak meg, milyen intézkedésekkel javítható a biztonság. A behatolás tesztek lehetnek fizikai természetűek, például valaki megpróbálja kijátszani az épületben található őröket, vagy nem fizikai természetűek, például az informatikai rendszereken keresztül próbál meg valaki a rendszerbe behatolni, és információkat eltulajdonítani onnan. Egy apró tanács, ne szóljon az alkalmazottaknak, hogy egy behatolás tesztelés zajlik - mivel ez aláássa az egész akciót!

Kilátások

A social engineering támadások nem fognak abbamaradni. Valójában, minél fejlettebbek leszünk technológiailag, annál fontosabb lesz a social engineering támadások kivitelezése az informatikai rendszereken tárolt információk megszerzése érdekében. Nem valószínű, hogy a módszerek változnának - a social engineer támadók ugyanazokat az alapvető trükköket használják (például bizalommal való visszaélés) évek óta és semmi okuk ezek megváltoztatására. Az egyetlen különbség, hogy új technikákkal különböző módokon képesek elérni a céljaikat (például a támadásaik fejleszthetőek vagy automatizálhatóak). Továbbá a social engineering támadások valószínűleg egyre kifinomultabbá és célzottabbá válnak. Végül ne feledjük, hogy a közösségi média megszületése a social engineering támadásokat segíti, ezért legyen óvatos, hogy mit tesz közzé. Összefoglalva, ne feledje, hogy egy könnyű célpont könnyű információszerzést jelent és Ön is csak annyira erős, amennyire az információi leggyengébb láncszeme.

Forrás: (IN)SECURE Issue 37

Összefoglaló 2013 első negyedévének IT biztonsági trendjeiről

Végre itt a tavasz! Talán már biztonságban érezhetjük a gyümölcsfákat, a vetést. És vajon mi a helyzet számítógépeinkkel, okos mobil eszközeinkkel, hálózatainkkal? Jelen cikkünkben az idei év első három hónapjának informatikai biztonsági fejleményeit tekintjük át. Igyekszünk kitérni a legfontosabb eseményekre, kiemelni a trendvonalakat a hírek hatalmas szénakazlából.

A nagy világcégek adatai alapján felvázoljuk, leggyakrabban milyen fenyegetésekkel kellett szembenéznünk, s azok milyen forrásokból érkeztek. Megvizsgáljuk persze azt is, mit tettek a vezető szoftvergyártók a kockázatok kivédésére, hogyan orvosolták termékeik sérülékenységeit.

Biztonság – felülnézetből

Ha már nincs olyan napja az évnek, amikor rendszereink ne állnának fenyegetések keresztтüzében, legalább egy olyan nap legyen minden esztendőben, amelyet a fenyegetésmentes világháló eszméjének szentelünk! Nos, van ilyen nap. Február 5-e immár a világ száznál több országában – köztük az Európai Unió tagállamaiban, azaz hazánkban is – a Biztonságosabb Internet Napja (Safer Internet Day, SID).

Ez a nemzetközi program elsősorban a gyerekekre leselkedő netes veszélyekre hívja fel a fiatalok, a szülők és a tanárok figyelmét. A szakterület szokásos hazai tavaszi nyitórendezvénye, a március végi IDC IT Security Roadshow ezzel szemben azoknak szólt, akik nagyon is otthonosan mozognak a kártevők és egyéb kockázatok világában. *Thomas Vavra*, a piackutató cég regionális alelnöke kutatásaik alapján arról számolt be: bár a cégvezetők ma már első számú feladatuknak tekintik a biztonságos vállalati informatikai környezet megteremtését, mégis többnyire csak követik az eseményeket. Márpedig ha sikerrel akarják felvenni a kesztyűt a folyamatosan változó fenyegetésekkel szemben, akkor ezt a reaktív szemlélet proaktivitásra, előrejelzésre kell felcserélniük.

Az IDC a cégeknek ajánlott biztonsági stratégiát, az Európai Bizottság és az Unió külügyi és biztonságpolitikai főképviselője pedig a tagállamoknak. Február elején tették közzé a *Nyílt és biztonságos kibertér (An open, safe and secure cyberspace)* címet viselő dokumentumot, az informatikai üzemzavarok és támadások megelőzésére, kivédésére, elhárítására vonatkozó ajánlásaik gyűjteményét. A stratégia az alábbi öt fő prioritás mentén vázolja fel az uniós szakértők javaslatait:

- a támadásokkal és üzemzavarokkal szemben ellenálló informatikai környezet megteremtése;
- a számítógépes bűnözés erőteljes visszaszorítása;
- a közös biztonsági és védelmi politikának megfelelő kibervédelmi politika kidolgozása, illetve a megkívánt védelmi képességek kifejlesztése;
- az IT biztonsághoz szükséges ipari és technológiai erőforrások biztosítása;
- az uniós értékrendhez illeszkedő, egységes kibertér-politika érvényesítése.

A dokumentum megfogalmazza a felelősségtudatos hálózati magatartás alapszabályait, síkra száll a hatályos nemzetközi jogi normák kibertéri alkalmazása, a nemzetközi együttműködés fejlesztése mellett, ugyanakkor támogatást helyez kilátásba az EU-n kívüli országok kibervédelmi kapacitásának kiépítéséhez.

Kulcseleme a stratégiának egy irányelv-javaslat. A hálózat- és információbizonsági (Network and Information Security, NIS) direktíva tervezete azt tűzi ki célul, hogy a tagállamok internetes szolgáltatói és kritikus infrastruktúrát üzemeltető szervezetei – köztük a vezető e-kereskedelmi cégek, közösségi hálózatok, energetikai és közlekedési cégek, pénzintézetek, valamint egészségügyi szolgáltatók – EU-szerte biztonságos és megbízható digitális környezetet alakítsanak ki. Ha az irányelvet elfogadják, az három fontos intézkedés megvalósításával jár majd:

(1) Valamennyi tagállamnak ki kell dolgoznia hálózat- és információbiztonsági stratégiáját, s megfelelő pénzügyi és emberi erőforrásokkal rendelkező szervet kell megbíznia a területbe vágó kockázatok és incidensek megelőzésével, kezelésével, elhárításával.

(2) Együttműködési mechanizmust kell kialakítani a tagállamok, illetve az Európai Bizottság között, amelynek keretében időben figyelmeztethetik egymást a kockázatokra vagy incidensekre, s rendszeresen kölcsönös ellenőrzéseket szervezhetnek. Mindehhez biztonságos infrastruktúrát kell kialakítani.

(3) A már említett szektorokban működő, kritikus infrastruktúrát üzemeltető szervezeteknek, az információs társadalom számára alapszolgáltatásokat nyújtó cégeknek, valamint a területért felelős állami/közigazgatási szerveknek megfelelő kockázatkezelési gyakorlatot kell alkalmazniuk, s jelenteniük kell a jelentősebb incidenseket.

Hogy a Bizottság csakugyan komolyan veszi az IT biztonság ügyét, mi sem bizonyítja jobban, mint hogy alig egy hónappal a stratégia közzététele előtt nyitották meg az Európai Kiberbűnözési Központot (European Cybercrime Centre, EC3). Az intézmény Hágában, az Europol keretében működik. Feladatai közé tartozik:

- a területtel kapcsolatos adatok gyűjtése,
- a nyomozás és általában a bűnüldöző szervek munkájának támogatása,
- az elemzés, a trendek meghatározása, stratégia kidolgozása,
- a kutatás és szakemberképzés (szoros együttműködésben az Európai Rendőrakadémiával, a CEPOL-lal),
- együttműködés a tagállamok illetékes szerveivel, különösen a nemzeti hálózatbiztonsági központokkal (CERT-ekkel), valamint a területen működő nemzetközi szervezetekkel.

Az EC3 honlapja emlékeztet rá: egy tavalyi Eurobarometer felmérés szerint

- az EU polgárainak 12%-a esett már online csalás áldozatául,
- 74%-uk vélte úgy, hogy az elmúlt egy év alatt nőtt a kockázata annak, hogy áldozatokká váljanak,
- 61%-uk aggódott amiatt, hogy visszaélhetnek személyazonosságával,
- 45%-ukat aggasztotta, hogy egy esetleges kibertámadás miatt nem férnek hozzá valamilyen online szolgáltatáshoz.

A *Nyílt és biztonságos kibertér* stratégia közzétételét tudató sajtóközlemény további drámai számokkal támasztja alá a határozott lépések szükségességét:

- A Világgazdasági Fórum megítélése szerint a következő évtizedben 10 százalékos eséllyel számíthatunk valamilyen, a kritikus információs infrastruktúrát megroppantó súlyos incidensre, s ez 250 milliárd dolláros kárt okozhat.
- A Symantec úgy becsüli: a számítógépes bűncselekmények áldozatainak veszteségei évi közel 390 milliárd dollárra rúgnak.
- Egy McAfee tanulmány szerint a számítógépes bűnözők évente 1000 milliárd dollárt zsebelnek be.

Február végén azután újabb EU-megnyilatkozást hallhattunk. Ezúttal ezt szó szerint kell érteni: *Neelie Kroes-nek*, az Európai Bizottság Digitális menetrendért felelős alelnökének egy beszédére gondolunk.

A holland politikus Brüsszelben, az Európai Parlamentnek az internet szabályozásáról tartott kerekasztal-találkozóján fejtette ki álláspontját, *Vegyük elejét a digitális hidegháborúnak! (Stopping a digital cold war)* címmel.

„Időbe telt, mire a kormányok ráébredtek az internet jelentőségére. És, mint tudjuk, vannak kormányok, amelyeknek nem tetszik a nyíltság és az átláthatóság. Ők hagyományosabb szabályozási modellt szeretnének: hierarchikus, államközi megállapodásokon alapuló rendszert.

Mások viszont úgy vélik: a világháló jelenlegi szabályozásában igazságtalanul az Egyesült Államoké a főszerep, vagy hogy a modell többszereplős ugyan, de a szegények kirekesztésére irányul. Ezek a kormányok az ENSZ-től vagy más intézményektől azt várják, hogy több politikai beleszólást kapjanak [az internet ügyeibe].

Nem könnyű kérdések ezek. Mind nagyobb a bizalmatlanság, s ez aggaszt engem. Nem akarok egy új, digitális hidegháborút" – fogalmazott Neelie Kroes.

Kémek, katonák

Az uniós alelnök az internet szabályozása körüli feszültségek miatt húzta meg a vészharangot. Ám IT biztonsági cégek és szervezetek kongatják azt régóta, noha egészen más okból. Egyfelől már hagyományai vannak az informatikai eszközökkel folytatott kémkedésnek – vállalatok és kormányok is próbálnak így versenyelőnyhöz jutni. Másfelől pedig a Stuxnet 2010-es felfedezése óta bízvást mondhatjuk: kezdetét vette a nemzetállamok közötti kiberháborúk kora. Ki-ki eldöntheti, hogy ezeket a kiberfegyverekkel vívott ütközeteket hideg-, avagy inkább meleg háborúnak tekinti...

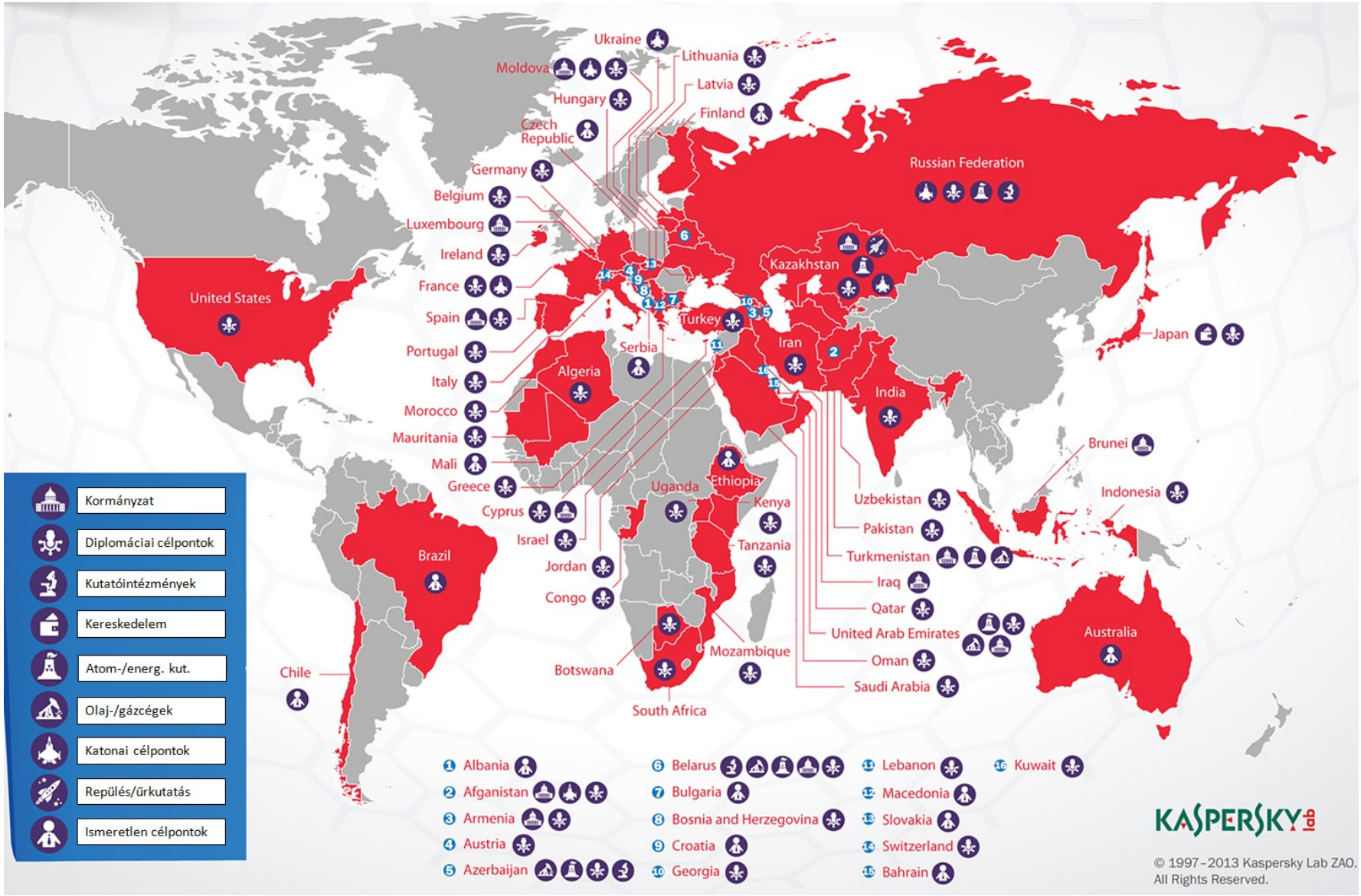
Január közepén a Kaspersky Lab újabb, elképesztő bizonyítékot szolgáltatott arra, micsoda kiterjedt gépi hírszerző tevékenység folyik a színfalak mögött. A cég nem kevesebbet állít, mint hogy ismeretlen tettesek egy kártevő segítségével immár öt éve a világ minden tájáról észrevétlenül szívták le diplomáciai testületek, kormányszervek, kutatóhelyek értékes adatait – mobil eszközökről, számítógépekről és hálózati eszközökről egyaránt. Ráadásul a kémhálózat jelenleg is működik, vezérlőszerverei aktívak.

A Kaspersky Lab kutatói hónapokon át elemezték az akció részleteit. Mint mondják, a hírszerző rendszer, melynek a Vörös október (Red October, röviden Rocra) nevet adták, a hírhedt Flame-éhez mérhető, komplex infrastruktúrára támaszkodik. A megfertőzött gépeket hatvannál több domain-ről, számos hosztról vezérlik. Ez utóbbiak többsége Német- és Oroszországban működik.

A kémkampány elsősorban kelet-európai, illetve a volt szovjet tagállamokban található szervezeteket vett célba, ám nem riadt vissza közép-ázsiai, nyugat-európai és észak-amerikai célpontoktól sem. A hálózat gazdái általában célzott adathalász támadással ragadták magukhoz áldozataik gépének vezérlését. Csaliként valamilyen fertőzött dokumentum szolgált.

Hogy hány országban milyen sokféle szervezet esett a Vörös októbert üzemeltető kémek hálójába, azt a Kaspersky Lab következő oldalon közölt térképén láthatjuk. Eszerint Magyarországon diplomáciai testületet ért támadás.

Ezek után nem is olyan meglepő a márciusi, Moszkvából érkezett hír, miszerint az IT biztonsági cég együttműködési megállapodást kötött az Interpol Globális Innovációs Központjával (Global Complex for Innovation, IGCI). Az IGCI jövőre kezdi meg működését: a 21. század eszközeit és ismereteit adja majd az Interpol tagállamok kiberrendőreinek kezébe. A Kaspersky Lab most vállalta, hogy a szervezet rendelkezésére bocsátja legkiválóbb szakértőit, adatokat szolgáltat a fenyegetésekről, s általában segíti az IGCI kapacitásának fejlesztését.


Ukraine
Moldova
Lithuania
Latvia
Hungary
Finland
Czech Republic
Germany
Belgium
Luxembourg
Ireland
France
Spain
Portugal
Italy
Morocco
Mauritania
Mali
Greece
Cyprus
Israel
Jordan
Congo
Botswana
South Africa
Mozambique
Tanzania
Kenya
Uganda
Ethiopia
Serbia
Algeria
Turkey
Russian Federation
Kazakhstan
Iran
Iraq
Qatar
United Arab Emirates
Oman
Saudi Arabia
Uzbekistan
Pakistan
Turkmenistan
India
Japan
Brunei
Indonesia
Australia
United States
Brazil
Chile
Kormányzat
Diplomáciai célpontok
Kutatóintézmények
Kereskedelem
Atom-/energ. kut.
Olaj-/gázcégek
Katonai célpontok
Repülés/űrkutatás
Ismeretlen célpontok
1 Albania
2 Afganistan
3 Armenia
4 Austria
5 Azerbaijan
6 Belarus
7 Bulgaria
8 Bosnia and Herzegovina
9 Croatia
10 Georgia
11 Lebanon
12 Macedonia
13 Slovakia
14 Switzerland
15 Bahrain
16 Kuwait
KASPERSKY lab
© 1997–2013 Kaspersky Lab ZAO.
All Rights Reserved.

Természetesen nem szűnik az a vita sem, amely Kína és a Nyugat között zajlik. Az Egyesült Államokban és Európában több nagy cég, illetve állami szerv elleni kibertámadásért kínai hacker-eket tesznek felelőssé.

Január végén a *New York Times* saját hasábjain számolt be arról, hogy hálózatát hosszan tartó, kifinomult támadás érte, amely a lap által megbízott szakértő nyomozása szerint Kínából indult ki, mégpedig „ugyanazokról a – kínai hadsereg által alkalmazott – egyetemi számítógépekről, amelyekről korábban amerikai katonai szállítókat támadtak", s a hacker-ek egy olyan kártevőfajt vetettek be, amelyet „Kínából indított számítógépes támadásokkal hoznak összefüggésbe".

Hogy miért került volna a lap az ázsiaiak célkeresztjébe? Nos – mondják a szerkesztők –, amiatt a leleplező cikk miatt, amelyet *Ven Csia-pao* miniszterelnök rokonainak vagyonáról jelentettek meg. A támadók nyilván az újságírók forrásait akarták beazonosítani. Kétszer is meggondolják majd a kínai polgárok: szóba álljanak-e külföldi újságírókkal, ha minden megígért titoktartás ellenére utoléri őket a hatóságok keze.

„A kínai törvények tiltanak minden olyan tevékenységet – így a rendszerek feltörését is –, amely veszélyezteti az internet biztonságát – válaszolta a *New York Times* kérdéseire a kínai nemzetvédelmi minisztérium. – Szilárd bizonyíték nélkül a kínai hadsereget kibertámadásokkal vádolni szakmaiatlan és megalapozatlan."

Ennek ellenére úgy tűnik, az Egyesült Államokban megalapozottnak gondolják a vádakat. *Obama* elnök televíziós nyilatkozatban erősítette meg: „kemény tárgyalásokat" folytatnak a kínai féllel az onnan induló, az állam által támogatott támadásokról. Az idei amerikai kormányzati kiadásokról szóló törvény, amely március végén lépett hatályba, ugyancsak Washington álláspontjának megkeményedéséről tanúskodik. A jogszabály megtiltja, hogy a kereskedelmi és az igazságügyi minisztérium, a NASA, valamint a Nemzeti Tudományos Alap (National Science Foundation) olyan technológiát vásároljon, amelyet Peking tulajdonában álló, vagy a kínai kormány által „üzemeltetett vagy finanszírozott szervezet állított elő, gyártott vagy szerelt össze". A törvény mindössze két kivételt enged meg: ha valamely technológia megszerzése nemzeti érdeknek minősül, vagy ha az FBI – a beszerzést indítani kívánó szervezet megkeresésére – azt állapítja meg, hogy a kérdéses rendszer beszerzése „nem jár kiberkémkedés vagy szabotázs kockázatával".

Bár április első hetében, vagyis az első negyedéven túl született a döntés, mégis ide kívánkozik még egy hír: az Egyesült Államok légiereje fegyvernek minősített át hat informatikai eszközt. Ily módon – magyarázta *John Hyten* altábornagy, a légierő űrparancsnokságának helyettes vezetője – a programok nagyobb eséllyel részesülhetnek a megkurtított katonai költségvetésből. A tábornok egyszersmind közölte: jelenlegi 6 ezer fős informatikai hadviselési állományukat 20%-kal, azaz 1200 új szakemberrel bővítik, hogy az ország jobban meg tudjon birkózni a világhálóról érkező támadásokkal. „Gyorsan kell cselekednünk. Nem várhatunk" – jelentette ki.

Szüntelen szennyáradat

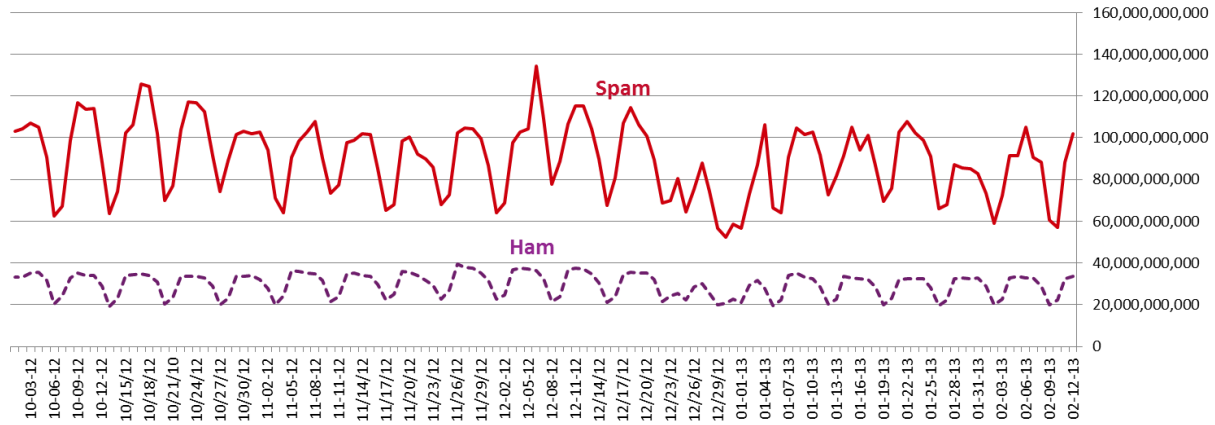
Mint már utaltunk rá, az előzőekben említett, nagy port kavart akciók egytől egyig úgynevezett spearphishing támadások voltak. Az elkövetők hozzájutottak a célba vett szervezet legalább egy munkatársának email címéhez, s olyan, ügyesen megszerkesztett dokumentumot küldtek neki, amelyet az gyanútlanul megnyitott. Ekkor pedig a csatolmányba rejtett kártevő segítségével magukhoz ragadták az uralmat az áldozat gépe felett, s onnan már könnyűszerrel haladhattak tovább a szervezeten belül – vagy azon kívül – más célpontok felé.

Nos, ezek a levelek kétségtelenül nevezhetők szemétnek, de nem minősülnek levélszemétnek, azaz spamnek, amely pedig szintén az IT biztonság egyik alapproblémája – például azért is, mert gyakran szintén kártevők terjesztésére használják.

Hogyan alakult a levélforgalom szennyezettsége a mögöttünk álló negyedévben? Erről a Commtouch adatai alapján próbálunk meg képet adni. A cég idei első – és eddig egyetlen – negyedéves trendelemzése *(Internet Threats Trend Report)* februárban látott napvilágot, s a 2012 október közepétől 2013 február közepéig terjedő időszakot öleli fel, ám így is jellemzőnek tekinthetjük.

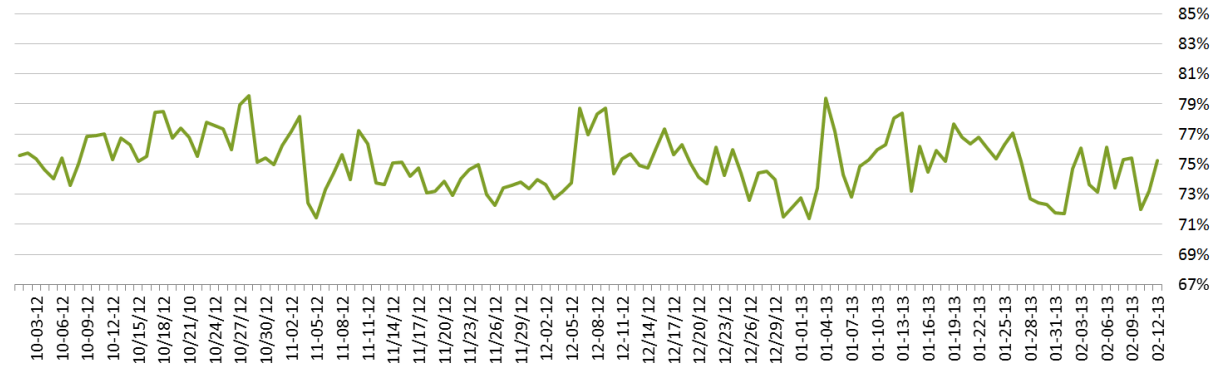
A vizsgált periódusban átlagosan napi 90 milliárd kéretlen levél közlekedett a neten – valamivel több, mint 2012 harmadik negyedévében. Más szóval – naptól függően – spam tette ki a világ teljes email-forgalmának 71-80%-át.

A spam és a hasznos üzenetek (ham) számának napi alakulása 2012 október közepe és 2013 február közepe között



Forrás: Commtouch

A spam részesedése a teljes globális email-forgalomból 2012 október közepe és 2013 február közepe között

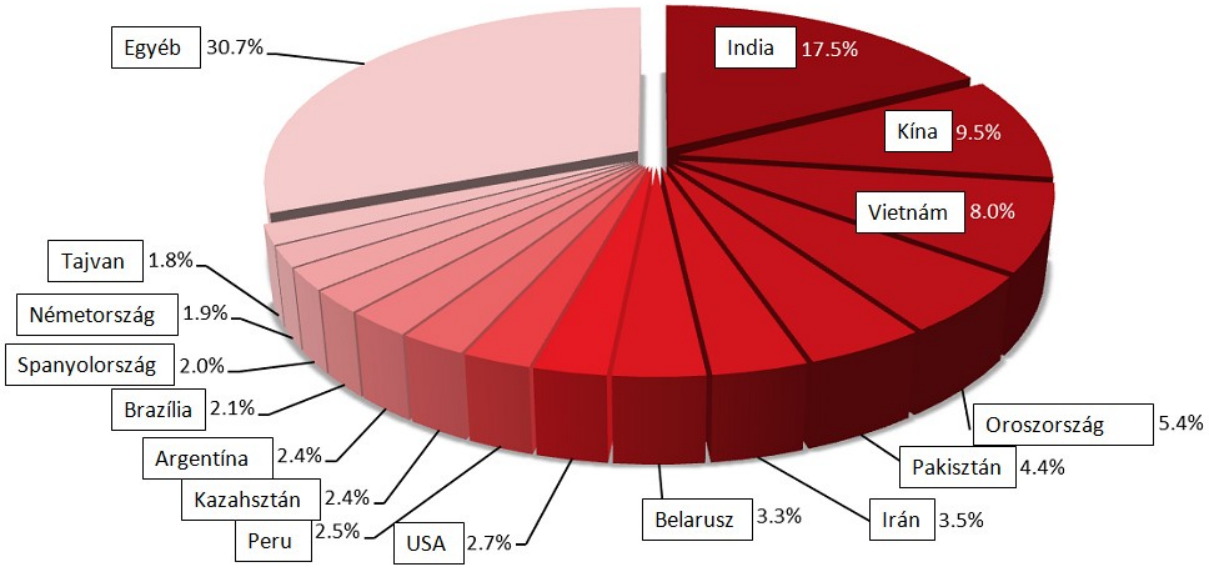


Forrás: Commtouch

Tudjuk: a spamszórásért legfőképpen a botnet-ek felelősek, amelyek világszerte gépek százezreit vagy éppenséggel millióit tarthatják zombisorban, s kényszeríthetik a vezérlőszerver utasításainak végrehajtására, anélkül, hogy gazdájuk tudna erről.

Jóllehet a Commtouch legutóbbi jelentésében ismét, sokadszor India kapta a világ legelzombisodottabb országa nem éppen megtisztelő címét, a kontinensnyi ország részesedése 20 százalék alá esett. Brazília, amely korábban dobogó második fokán állt, most a 12. helyre csúszott vissza.

Spamszóró zombik a világ országaiban 2012 október közepe és 2013 február közepe között



Forrás: Commtouch

A negyedév folyamán egyébként több fontos botnet-et is sikerült kiiktatniuk az IT biztonsági szakembereknek. Ezek az akciók egytől egyig példaértékűek, már csak azért is, mert általában több szervezet – nem egyszer több ország szervezeteinek – jól összehangolt együttműködését követelték meg.

Január vége felé például a lengyel és az orosz nemzeti hálózatbiztonsági központ (CERT) a Spamhaus nonprofit céggel közösen iktatta ki a Virut botnet-et, amely becslések szerint 300 ezer zombit tartott hatalmában.

Február elején a Microsoft és a Symantec az amerikai szövetségi bűnüldöző szervekkel együttműködve a Bamital botnet-et kapcsolta le sikerrel. Ez utóbbi elsősorban klikkeltérítő tevékenységéről híresült el, s hírek szerint 8 millió felhasználónak okozott bosszúságot vagy akár komoly kárt.

Megjegyezzük, hogy a bűnözők elleni fellépés nincs kockázat nélkül. Az imént említett Spamhaus március végén az internet történetének feltehetőleg legnagyobb – 300 Gbps-t lekötő – elosztott szolgáltatásmegtagadási (DDoS) támadását szenvedte el. Nagy fegyvertény, hogy a cég különösebb károsodás nélkül heverte ki az incidenst, s rendszereit és szolgáltatásait újra tudta indítani. Az elkövetők csapást mértek egyébként a CloudFlare-re is, arra a szolgáltatóra, amelyet a Spamhaus egy korábbi DDoS támadás kivédésére szerződtetett.

Jóllehet egy-egy nagyobb botnet kiiktatása általában világosan megmutatkozik a spamgrafikonokon, s a tettesek őrizetbe vételének nyilván valamelyest elrettentő hatása is van, egy nemrég napvilágot látott elemzés szerint ez kevés a spamszint leszorításához. A Fortinet tanulmánya arra a következtetésre jut, hogy a lekapcsolások, elkobzások, letartóztatások megnövelik ugyan kissé a bűnözők költségeit, ám a botnet-üzemeltetés így is viszonylag olcsó és igen jövedelmező vállalkozás. „Egy botnet felállítása és működtetése szinte ingyen van” – állítják a szerzők, hozzátéve, hogy aki segítséget akar kapni ehhez az üzletághoz, már 350-400 dollárért kaphat „szakértő tanácsadót”. Napi 5 órán át fenntartott DDoS támadásra hetente 535 dollárért lehet botnetet bérelni; 20 ezer spam üzenet kiküldése 40 dollárba, 30 spam comment fórumon való megjelentetése 2 dollárba kerül. Ugyanakkor ezer fertőzött hosztonként 100 dollár ütheti a botnet-üzemeltető markát. Van olyan hálózat – a Fortinet a ZeroAccess botnet-et, illetve az azt építő kártevőt említi –, melynek tulajdonosai ennek ötszörösét is kifizetik alvállalkozóiknak.

Kiemelkedő kártevők

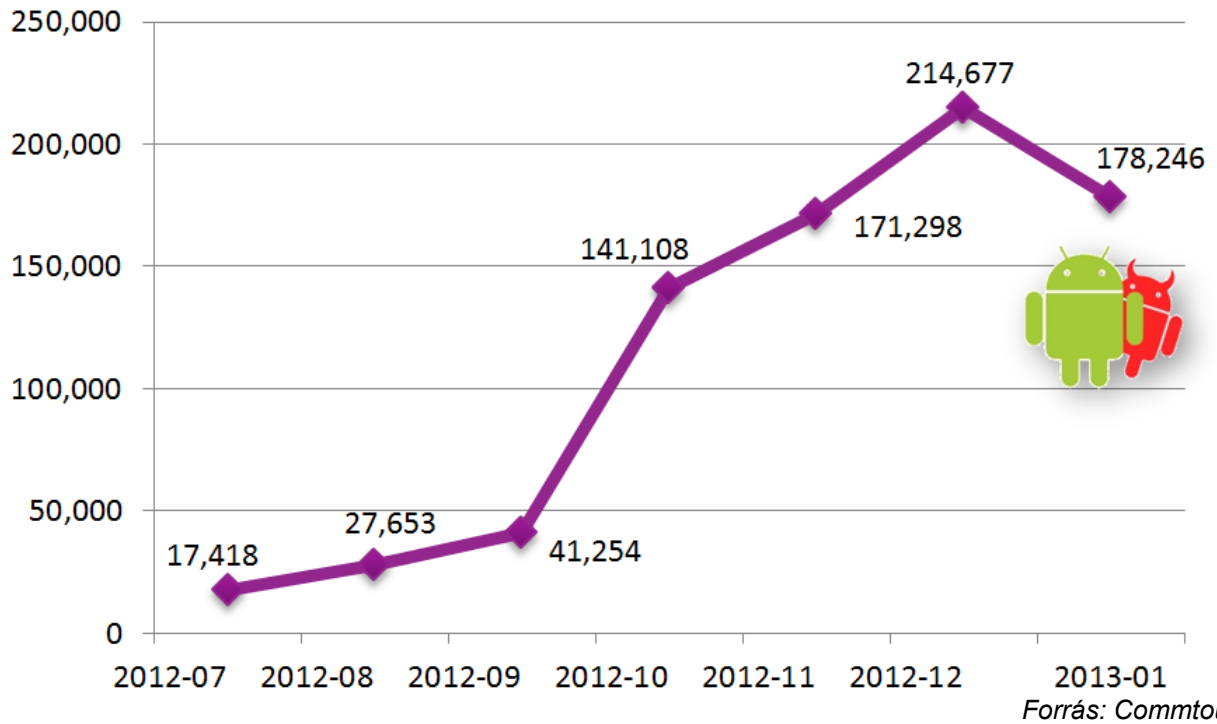
Mobil mérgek

Lássuk, melyek voltak az elmúlt időszak legjellegzetesebb kártevői, s hol – milyen informatikai, illetve földrajzi – környezetben bukkantak fel!

A számítógépeinket, különösen a windowsos rendszereket bombázó kórokozó-áradattal általában tisztában vagyunk. Még mindig kevesen gondolunk azonban arra, hogy napjaink okos mobil eszközei minden korábbinál vonzóbb platformot kínálnak a kártevőírók számára. Pedig a számok magukért beszélnek. A Gartner adatai szerint egyedül 2012 harmadik negyedévében 122 millió androidos eszközt – telefont, táblagépet – adtak el, több mint kétszer annyit, mint egy évvel korábban. Nem csoda hát, ha elemzők egybehangzóan az Androidra írt rosszindulatú programok rohamos szaporodásáról beszélnek.

Alább a Commtouch megdöbbentő adatait láthatjuk. Januárban a cég víruslaboratóriumában 178 ezernél több különböző androidos kártevőmintát dolgoztak fel. Riasztó szám. Igaz, 16 százalékkal kisebb a decemberi szintnél, de azt a csúcsot a Commtouch szakemberei anomáliának tartják.

Androidra írt kártevők – az egyedi minták számának havi alakulása 2012 júliusától 2013 januárjáig



Forrás: Commtouch

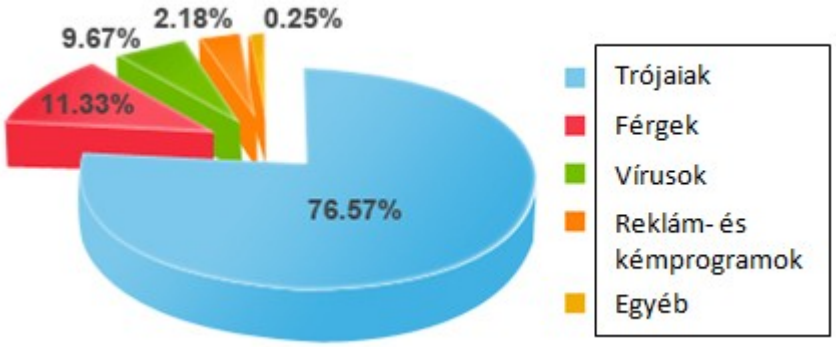
Februári jelentésében a PandaLabs egyebek között megemlíti, hogy bűnözők népszerű androidos játékokat – például az Angry Birdsöt vagy a Cut the Rope-ot – trójaival vegyítve csomagoltak újra, majd töltöttek fel a Google alkalmazásáruházába, a Play Store-ba. Ha a gyanútlan felhasználó letöltötte a játékot, csodálkozhatott, hogy miért küldözgetett a telefonja egy drága, fizetős számra SMS-eket. A fertőzött alkalmazások elszaporodását látva a Google elkezdte vizsgálni a feltöltött programokat, s csak azokat veszi fel katalógusába, amelyeknél nem tapasztal gyanús viselkedést. Ezzel a keresőóriás szerint 40 százalékkal sikerült csökkenteni a rosszindulatú letöltések számát.

Gépes gonoszok

Most pedig térjünk át a kártevők hagyományos célpontjára, a számítógépekre. Imént idézett jelentésében PandaLabs ugyan még csak a tavalyi számokat tudja összegezni, de azok jó jelzői az idei év elejének is. Mint a tanulmányban olvasható, a bűnözők 2012 minden egyes napján átlagosan 74 ezer új kártevőfajt dobtak a számítástechnika világarénájába. Ez éves szinten 27 millió új fajt jelentett. Ezzel a PandaLabs-nál kategorizált egyedi kártevőminták összes száma elérte 125 milliót.

A cég alábbi tortadiagramja a tavaly született új fenyegetések típus szerinti megoszlását mutatja. Mint látható, az összes 2012-ben írt rosszindulatú program több mint háromnegyede trójai volt.

2012-ben keletkezett új kártevőfajok típus szerinti megoszlása

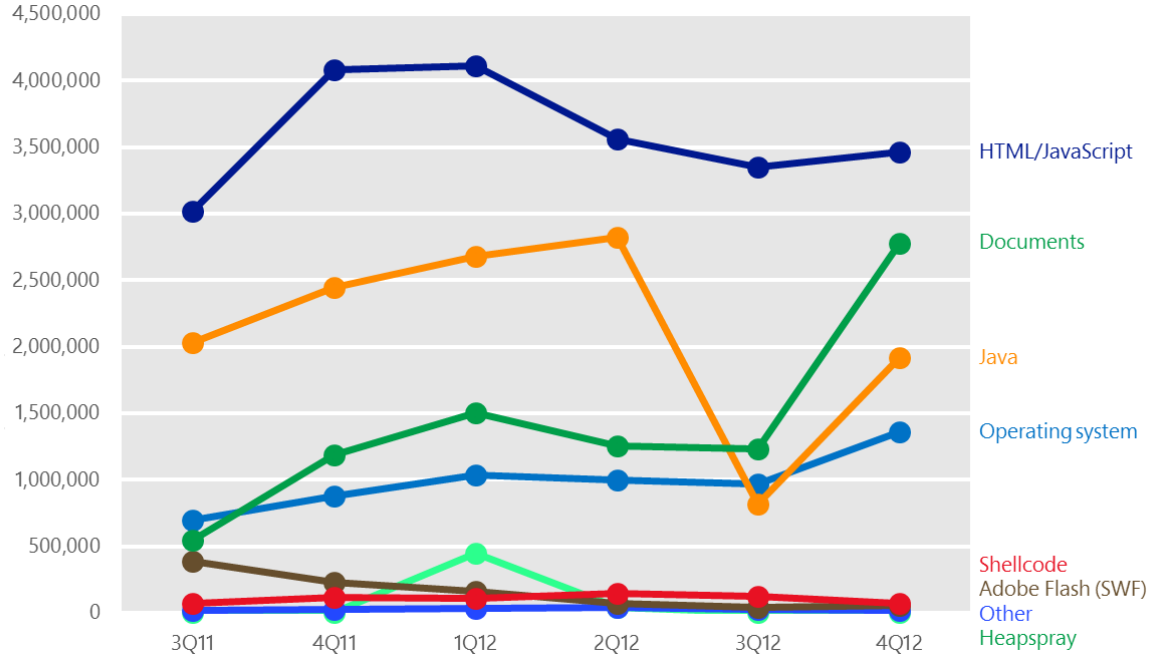


Forrás: PandaLabs

Milyen programok megtámadására specializálódtak legjellemzőbb módon a kórokozók? Erről például a Microsoft nemrég megjelent legújabb *Biztonsági Kutatási Jelentéséből* tájékozódhatunk. A tanulmány legfrissebb, 14. kiadása *(Security Intelligence Report, SIRv14)* 2012 második félévének adatait dolgozza fel.

Nos, a szoftveróriás megállapítja: a tavalyi év utolsó negyedévében különösen megugrott a dokumentumolvasók és -szerkesztők sérülékenységeit kiaknázó fertőzések száma. Ezért a növekedésért elsősorban a Microsoftnál Win32/Pdfjsc néven nyilvántartott – Adobe Readerre és Acrobatra specializálódott – kártevő volt a felelős. Ugyanakkor a Java-sérülékenységeken át bekövetkezett fertőzések száma 2012 harmadik negyedévében hatalmasat esett, de ennek a visszaesésnek a felét aztán sajnos az év végére ledolgozták a bűnözők. A HTML és JavaScript réseken át feltört gépek száma az év folyamán nem sokat változott, amit a Microsoft a Blacole kártevőcsalád folyamatos és nagyarányú elterjedtségével magyaráz. (Blacole gyűjtőnéven tartja nyilván a szoftveróriás azokat a rosszindulatú programokat, amelyeket a Blackhole elnevezésű támadókészlettel állítottak elő, illetve helyeztek el fertőző weblapokra.)

A kártevők által kiaknázott sérülékenységek szoftverkategóriák szerint. Az ábra a Microsoft vírusirtóinak észleléseit mutatja. A függőleges tengelyen a megfertőzött gépek száma látható



Forrás: Microsoft

Ugyanezeket a célba vett szoftverkategóriákat láthatjuk a Microsoft alábbi táblázatában is, amely negyedéves bontásban mutatja a fertőzések számának alakulását.

Kártevő/Rés	Platform / technológia	2012.I.né.	2012.II.né.	2012.III.né.	2012.IV.né.
Win32/Pdfjsc*	Dokumentumok	1.430.448	1.217.348	1.187.265	2.757.703
Blacole	HTML/JavaScript	3.154.826	2.793.451	2.464.172	2.381.275
CVE-2012-1723*	Java	—	—	110.529	1.430.501
Rosszindulatú IFrame	HTML/JavaScript	950.347	812.470	567.014	1.017.351
CVE-2010-2568 (MS10-046)	Operációs rendszer	726.797	783.013	791.520	1.001.053
CVE-2012-0507*	Java	205.613	1.494.074	270.894	220.780
CVE-2011-3402 (MS11-087)	Operációs rendszer	42	24	66	199.648
CVE-2011-3544*	Java	1.358.266	803.053	149.487	116.441
ShellCode*	Shell kód	105.479	145.352	120.862	73.615
JS/Phoex	Java	274.811	232.773	201.423	25.546

** Ezeket a sérülékenységeket a Blackhole támadókészlet is kiaknázza. Az itt megadott számok a Blackhole észleléseket nem tartalmazzák.*

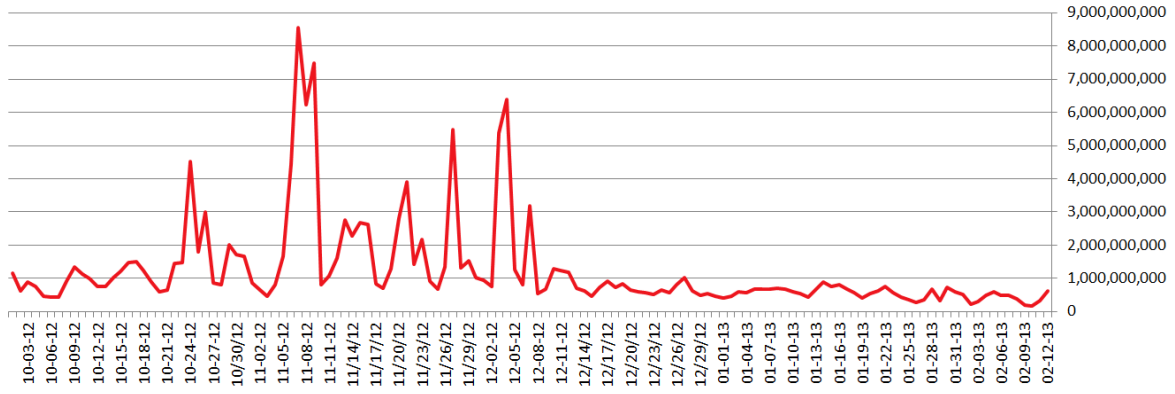
Természetesen az egyes kártevőcsaládok különböző operációs rendszerek alatt más és más gyakorisággal fordulnak elő. A Microsoft következő táblázata Windows-változatok szerinti bontásban jelzi, melyik platformon melyik család okozta a legtöbb fertőzést, a szoftveróriás antivírus megoldásainak észlelései alapján.

Helyezés (össz.)	Kártevőcsalád	Kártevő működésmódja	Helyezés: Win 8 RTM	Helyezés: Win 7 SP1	Helyezés: Win Vista SP2	Helyezés: Win XP SP3
1	Win32/Keygen	Kéretlen szoftver	1	1	10	5
2	Win32/DealPly	Reklámprogram	15	2	1	9
3	INF/Autorun	Kéretlen szoftver	3	3	14	3
4	JS/IframeRef	Trójai	2	7	8	2
5	Win32/Pdfjsc	Kártevő	20	4	3	7
6	Blacole	Kártevő	17	5	6	6
7	Win32/Onescan	Trójai	84	16	24	1
8	Win32/Obfuscator	Egyéb kéretlen szoftver	5	6	12	12
9	Win32/Dorkbot	Féreg	13	8	23	10
10	Win32/Sality	Vírus	11	12	41	4
14	Win32/Zw angi	Egyéb kéretlen szoftver	54	17	2	35

Honnan fertőződnek meg a felhasználók? A két fő forrást az email-csatolmányok, valamint a fertőzött weblapok jelentik.

A Commtouch már idézett trendjelentéséből az derül ki, hogy tavaly október és idén február között nagyjából egy szinten maradt a rosszindulatú csatolmányok száma, kivéve egy nagyjából egy hónapos kiugrást, melyért egy konkrét támadás felelős: egy zippelt csatolmány Xerox Workcenter-ről küldött beszkennelt anyagként tetszelgett akkor...

A rosszindulatú email-csatolmányok számának alakulása 2012 október közepe és 2013 február közepe között



Forrás: Commtouch

Jóllehet a fertőzések fő forrását továbbra is a levélcsatolmányok jelentik, mégis bizonyos szempontból a fertőzött weblapok jelentik a nagyobb veszélyt – figyelmeztet a Palo Alto Networks. A cég elemzése szerint ugyanis a webről érkező fertőzésekkel szemben a védelmi szoftverek nem egyszer hatástalanok. A Palo Alto Networks felmérése azt mutatta: az „ismeretlen kártevők” közel 90%-a böngészés közben került a felhasználók gépére. „Ismeretlen kártevőnek” azt minősítették a cég kutatói, amelyet hat vezető antivírus szoftver közül egy sem észlelt.

Ráadásul mind gyakrabban nem a hagyományosan veszélyesnek tartott pornósite-okon, hanem olyan weblapokon bukkannak fel kártevők, amelyeket a felhasználók tökéletesen megbízhatónak vélnek. A bűnözők nem egyszer úgy törik fel a site-ot, hogy az üzemeltető semmit nem vesz észre. A Cisco 2013. évi biztonsági összefoglalója szerint az online áruházak 21-szer, a keresőgépek pedig 27-szer gyakrabban vezetik a felhasználókat rosszindulatú tartalomra, mint a szoftverkalóz oldalak.

Hasonlóképpen: az online reklám 182-szer gyakrabban vezet rosszindulatú tartalomra, mint a pornó site-ok. A Cisco felmérése azt mutatja, hogy a webes kártevők túlnyomó többsége – 87 százaléka – valamilyen Java sérülékenységet aknázott ki. A második legnépszerűbb támadási célnak a PDF és Flash rések bizonyultak.

Akkor most milyen tartalmú site-okon ütközünk legnagyobb valószínűséggel fertőzésbe? A Commtouch trendjelentése 2012 negyedik negyedévéről tartalmaz erre vonatkozó adatokat:

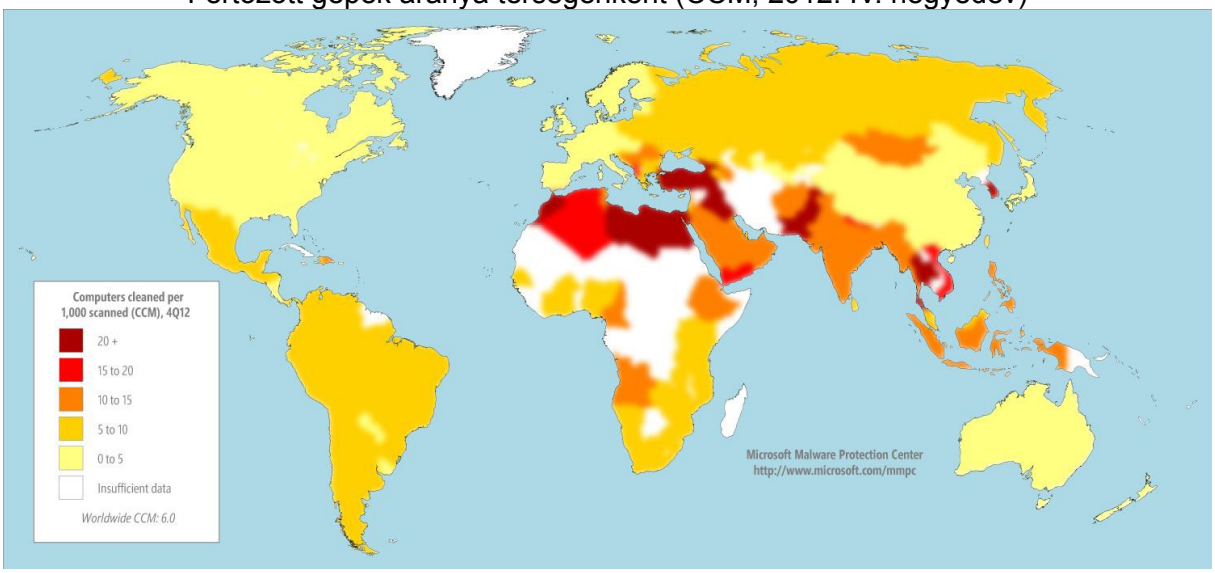
	A leggyakrabban kártevővel fertőzött tartalomkategóriák a weben (Commtouch, 2012. IV. né.)
1	Oktatás
2	Utazás
3	Sport
4	Céges
5	Szórakoztatás
6	Egészség
7	Éttermek, étkezés
8	Streaming média, letöltések
9	Szabadidő
10	Pornográfia, szex

Ugyanebben az időszakban adathalász támadásnak a következő tartalmú site-okon voltunk leginkább kitéve:

	A leggyakrabban adathalászattal szennyezett tartalomkategóriák a weben (Commtouch, 2012. IV. né.)
1	Portálok
2	Számítástechnika, technológia
3	Vásárlás
4	Oktatás
5	Divat, szépségápolás
6	Éttermek, étkezés
7	Céges
8	Streaming média, letöltések
9	Egészség
10	Utazás

Most pedig vizsgáljuk meg a fertőzések földrajzi eloszlását! A következő térkép a Microsoft *Biztonsági Kutatási Jelentésének* már idézett 14. kiadásából származik. Színei azt jelzik, hogy Földünk egyes régiói mennyire voltak fertőzöttek a tavalyi utolsó negyedévben. A szoftveróriás biztonsági szakemberei azokat az információkat értékelték ki, amelyeket a Windows Rosszindulatú Szoftvert Eltávolító Eszközétől (Malicious Software Removal Tool, MSRT), világszerte több mint 600 millió gépről kaptak. A fertőzöttségi arányt az MSRT ezer végrehajtására során valamilyen kártevőtől megtisztított gépek átlagos számával (computers cleaned per mille, CCM) fejezik ki.

Fertőzött gépek aránya térségenként (CCM, 2012. IV. negyedév)

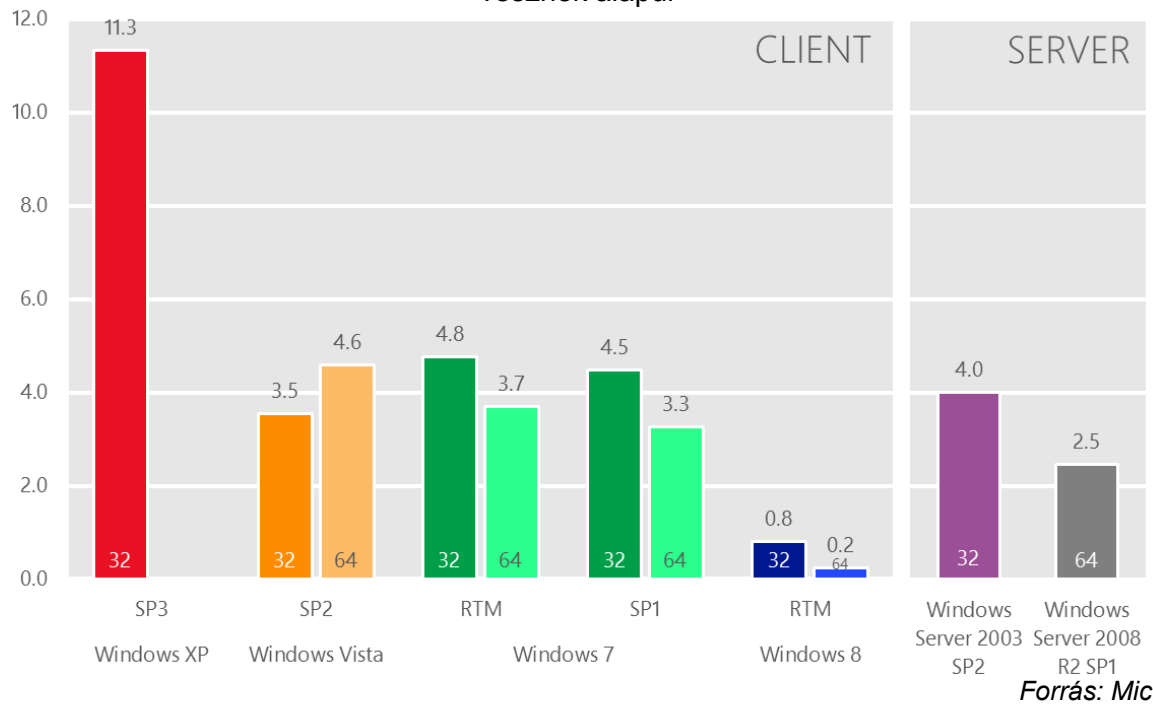


Forrás: Microsoft Malware Protection Center

Örvendetes és talán meglepő hír, hogy a fertőzések átlagos aránya globálisan valamelyest csökkent. A PandaLabs arról számol be, hogy míg 2011-ben világviszonylatban a számítógépek 38,49 százaléka hordozott valamilyen kártevőt, ez a szám 2012-ben „csak" 31,98% volt. Szemben a Microsoft negyedik negyedéves térképével, a PandaLabs 2012 egészére vonatkozó adatai szerint Kína volt a világ legfertőzöttebb országa, 54,89%-os fertőzöttségi aránnyal. A dobogó következő két fokát Dél-Korea és Tajvan foglalta el, 54,15, illetve 42,14%-kal. A skála másik végén európai országok álltak. A legkisebb fertőzöttségi arányt – 20,25%-ot – Svédországban mérte a PandaLabs. A legjobban teljesítők sora Svájccal és Norvégiával folytatódott (20,35, illetve 21,03%-kal). Magyarország sem állt rosszul a maga 27,37%-ával.

Végül ismét a Microsoft adataihoz fordulunk, hogy a fertőzések operációs rendszerek szerinti megoszlásáról is képet alkothassunk. Az ábra CCM-ben jelzi az egyes Windows kliens, illetve szerver környezetekben a tavalyi utolsó negyedévben mért fertőzöttségi rátát.

Fertőzött gépek aránya Windows verziónként (CCM, 2012. IV. negyedév; 32 = 32 bites, 64 = 64 bites változat). Az adatok normalizáltak, azaz mindegyik operációs rendszerre ugyanannyi gépet vesznek alapul



Forrás: Microsoft

Folt hátán folt

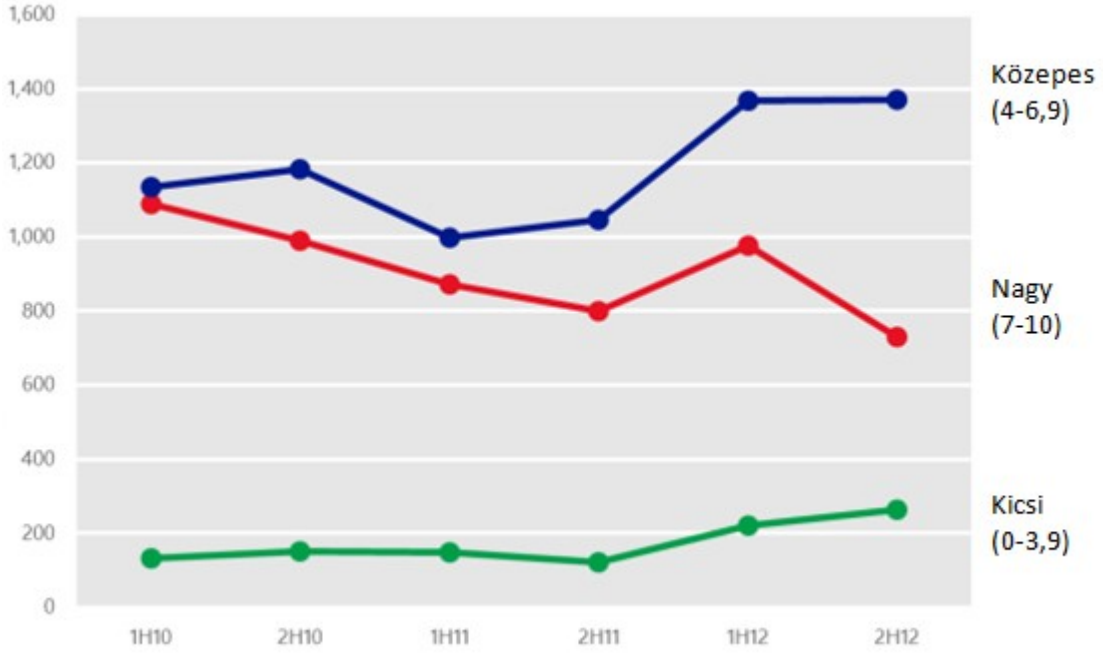
Természetesen a mögöttünk álló negyedévben sem volt hiány sérülékenységekben, azaz valamennyi gyártónak akadt – nem egyszer kritikus – foltoznivalója. Mielőtt azonban áttekintenénk az időszak legfontosabb biztonsági frissítéseit, vessünk egy pillantást a sérülékenységek számának alakulására!

A Microsoft *Biztonsági Kutatási Jelentése* megállapítja: a tavalyi második félévben összességében 7,8 százalékkal kevesebb sérülékenységet jelentettek be a gyártók, mint az első félévben, ami egyértelműen a legsúlyosabb („nagy" súlyosságú) rések megfogyatkozásának köszönhető. Ugyanakkor a 2011-es esztendő hasonló időszakához képest 20 százalékos növekedést látunk.

Az elmúlt három évben az alkalmazásokban átlagosan stagnált, az operációs rendszerekben csökkent, míg a böngészőkben folyamatosan növekedett a sérülékenységek száma.

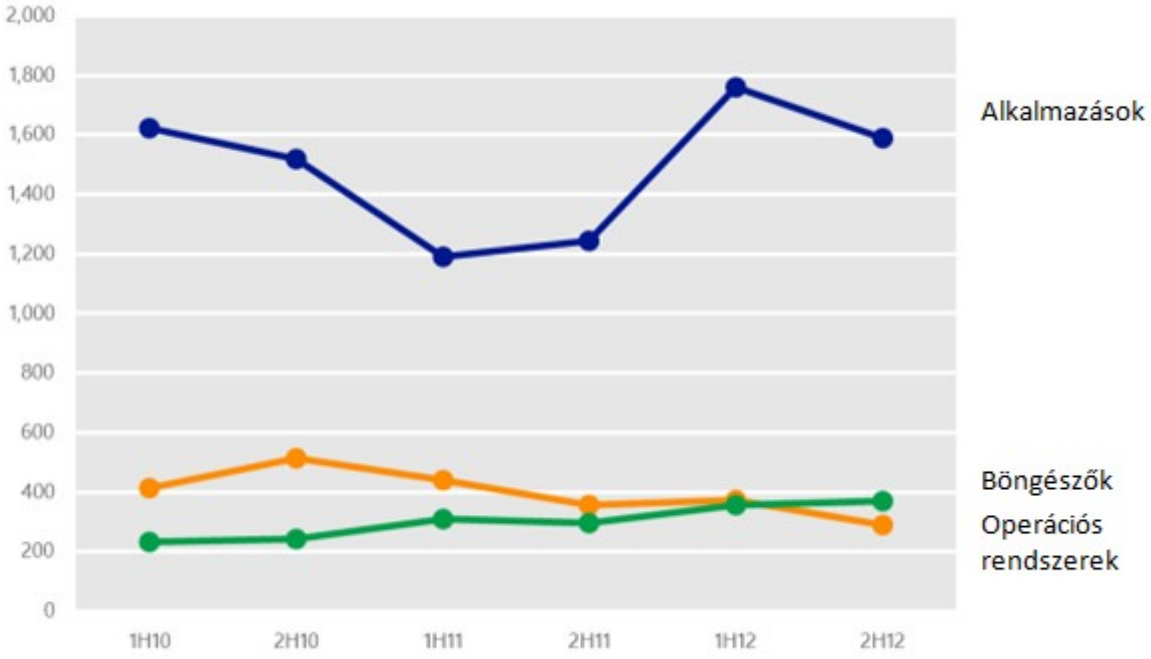
Ha pedig azt vizsgáljuk, hány sérülékenységet jelentett be a Microsoft, s hányat a többi gyártó együttvéve, azt tapasztaljuk, hogy az „Egyéb gyártók" grafikonja – nem meglepő módon – kísértetiesen követi az „Alkalmazások" görbéjét, a Microsoftnak pedig az utolsó két és fél esztendőben lassan fogyatkozó számú résről kellett beszámolnia.

A szoftvergyártók által újonnan bejelentett közepes *(kék),* nagy (*piros)* és kis *(zöld)* súlyosságú sérülékenységek számának alakulása 2010 első és 2012 második féléve között



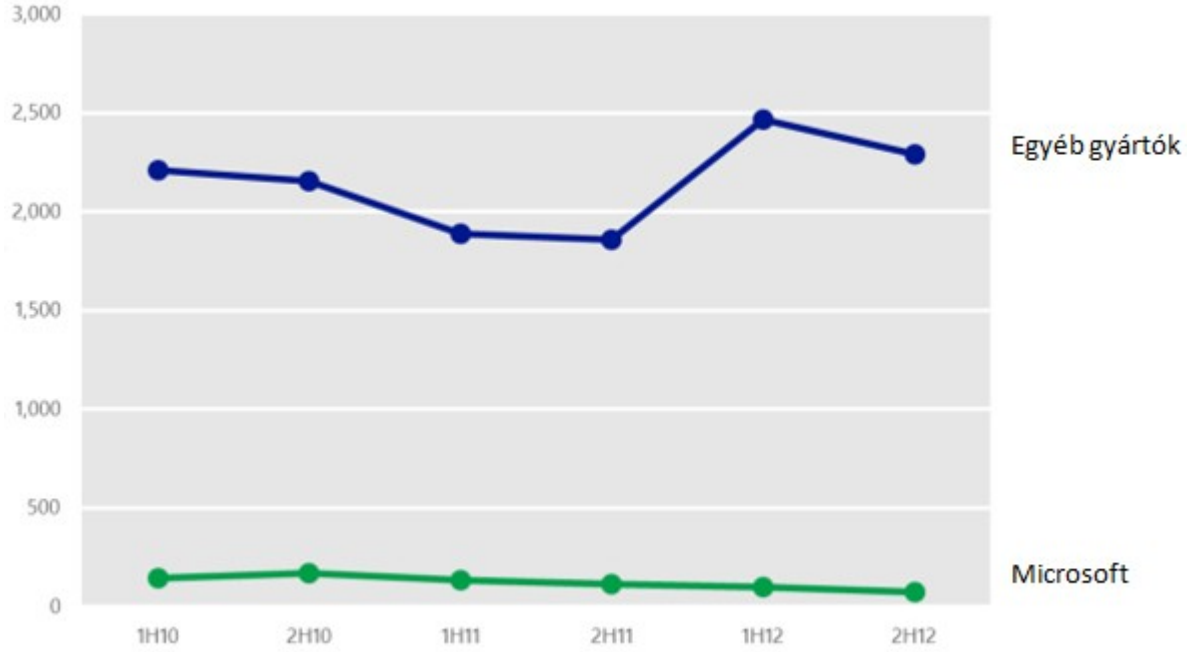
Forrás: Microsoft

Az alkalmazásokban (*kék),* böngészőkben *(zöld)* és az operációs rendszerekben *(narancs)* jelentett sérülékenységek számának alakulása 2010 első és 2012 második féléve között



Forrás: Microsoft

A Microsoft *(zöld)* és a többi szoftvergyártó *(kék)* által bejelentett sérülékenységek számának alakulása 2010 első és 2012 második féléve között



Forrás: Microsoft

Összefoglalónk végén az alábbiakban hónapról hónapra haladva áttekintést adunk a negyedév folyamán megjelent legfontosabb biztonsági frissítésekről.

Január

- Havi foltozó keddjén 7 javítócsomagot bocsátott ki a Microsoft. Közülük 2 kritikus, 5 pedig fontos besorolást kapott. A foltok összesen 12 rést fedtek be a következő termékekben: Windows, Office, Developer Tools és Windows Server.
- Alig egy héttel a foltozó kedd után soron kívül tömte be a Microsoft az Internet Explorer 6-8-as verzióinak rését, amelyet már támadni kezdtek a hacker-ek.
- A Microsoft foltozó keddjéhez igazítva menetrendszerű javítónapot tartott az Adobe is. Új verziót kapott a Flash Player, a Reader és az Acrobat. A PDF-programokban összesen 27, a Flash Playerben további 1 sérülékenységet orvosolt a cég.
- Ugyancsak menetrendszerű javító frissítés-csomaggal jelentkezett az Oracle. Az érintett termékek, illetve termékcsaládok: Database, Fusion Middleware, Enterprise Manager, E-Business Suite, Supply Chain, PeopleSoft, JD Edwards, Siebel, Sun Product Suite, MySQL Product Suite.
- Megjelent a Google Chrome böngészőjének 24-es kiadása, amellyel 11 kritikus hibát javítottak. Ezek felfedezőinek összesen 6 ezer dollárt fizetett ki a cég.
- 18.0-s kiadására váltott a Mozilla Firefox. Ezzel 12 kritikus sérülékenységet orvosoltak.
- Biztonsági frissítések érkeztek az Apple-től is. Az új termékverziók: Apple TV 5.2, iOS 6.1.

Február

- Rendszeres havi frissítési ciklusa keretében a Microsoft összesen 12 – 5 kritikus és 7 fontos besorolású – javítócsomaggal jelentkezett, melyek összesen 57 sérülékenységet orvosoltak. Az érintett termékek: Windows, Office, Internet Explorer, Exchange, .NET keretrendszer.
- Két, már támadott sérülékenységet orvosolt Flash Player-én az Adobe.
- Pár nappal később újabb biztonsági frissítést bocsátott ki a Flash Player-hez és a Shockwave Player-hez a cég. Ekkor összesen 19 rést foltoztak be. Ebből a Flash Player-be 17 jutott, s közülük 16-ot kritikusnak minősítettek.
- A hónap gazdag volt Apple foltokban. Mindjárt elsején frissült a Mac OS X-es Java, majd az OS X Server. Különösen fontos volt azonban az a folt, amelyet a hónap második felében kapott a Mac OS X alatt futó Java-gép. Ekkor sikerült betömni azt a rést, amelyen keresztül hacker-ek az Apple saját fejlesztői is megtámadták. Ugyanezt a sérülékenységet a Facebook megtámadására is kiaknázták a hacker-ek.
- Ismét feljebb lépett a Google Chrome változatszámlálója. A 25-ös verzió 8 kritikus rést tömött be, s a hibák bejelentői között 3500 dollár jutalmat osztottak szét.
- Négy kritikus sérülékenységet orvosolva megjelent a Mozilla Firefox 19.0-s kiadása.

Március

- A negyedév utolsó foltozó keddjén 7 biztonsági frissítés látott napvilágot a Microsoftnál. Közülük négyet kritikusnak, hármat fontosnak minősítettek. Az érintett termékek: Windows, Office, Internet Explorer, Server Tools, Silverlight.
- Ismét Java-frissítéssel jelentkezett, majd más termékeit is foltozta az Apple. Megjelent a Safari 6.0.3-as verziója, az Apple TV 5.2.1-es kiadása, valamint az iOS 6.1.3-as változata.
- Elkészült a Google Chrome biztonsági javításokat is tartalmazó 26-os változata, melyben 2 kritikus sérülékenységet orvosoltak. Ezek összesen ezer dollárt hoztak a bejelentők konyhájára.
- Egy kritikus hiba kijavítása miatt kiadták Mozilla Firefox 19.0.2-es változatát.

Elérhetőségeink

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

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937