Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2012. I. negyedéves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2012. 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 VirusBuster Kft. informatikai biztonsági trendjeiről szóló összefoglalóját. A jelentésben a főszerep ismét a hálózatbiztonságé.

A jelentés betekintést nyújt az informatikai biztonság berkeibe, az első negyedévben a lakossági szektort vesszük fókuszpontba IT-biztonsági szempontból, egy cikk erejéig kitérünk a cloud computing adatbiztonsági kérdéseinek jogi aspektusaira, valamint az okostelefonok és a mobil számítástechnika biztonságának fejlődési irányzatairól is szót ejtünk.

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

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

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

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

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

Dr. Kőhalmi Zsolt
Puskás Tivadar Közalapítvány
a kuratórium elnöke

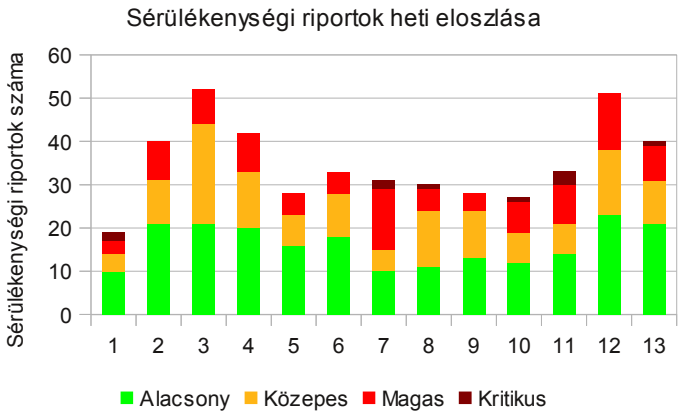
Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

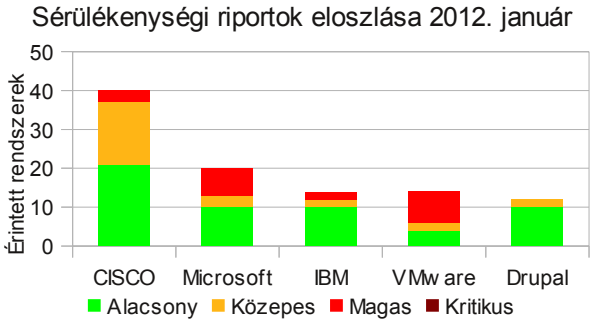
A PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ tevékenysége számokban

Szoftver sérülékenységek

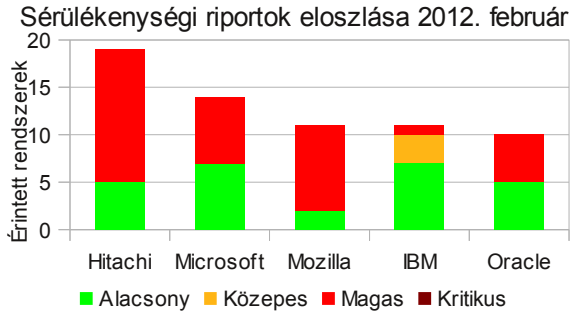
Szoftversérülékenység minden olyan szoftver gyengeség vagy hiba, amelyet kihasználva egy rosszindulatú támadó megsértheti az informatikai rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását.

A **PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ (NHBK)** 2012. I. negyedéve során **454 db szoftversérülékenységi információt** publikált, amelyekből 210 db alacsony, 135 db közepes, 99 db magas és 10 db kritikus kockázati besorolású.

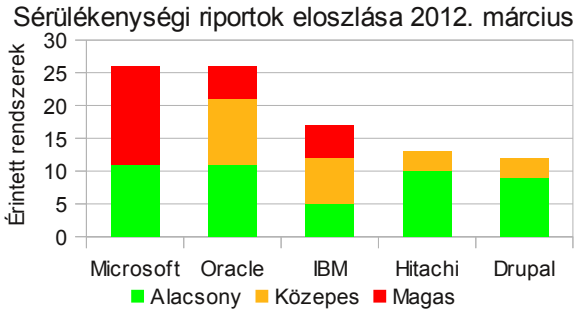




Érdemes figyelmet szentelni az I. negyedév sérülékenységeinek gyártók szerinti eloszlására, ugyanis január, február és március hónapokban, megfigyelhető, hogy a gyártók egyszerre nagy számban adták ki szoftvereiket érintő sérülékenységi riasztásaikat. Január hónapban a CISCO termékek érintettsége a legmagasabb, de nem elhanyagolható a Microsoft és az IBM termékek kitettsége sem.



Február hónapban a Hitachi termékeinek érintettsége a legnagyobb és csak ezt követik a Microsoft, Mozilla és az IBM termékek. Március hónapban kiemelkedően nagy számban érintették a szoftver sérülékenységek az Oracle és a Microsoft termékeit, amely a sebezhetőségek heti eloszlásban a 12. hét adat-oszlopán is jól látszik, de a Hitachi és az IBM termékeit érintő sérülékenységek számossága sem volt elhanyagolható a hónapban.

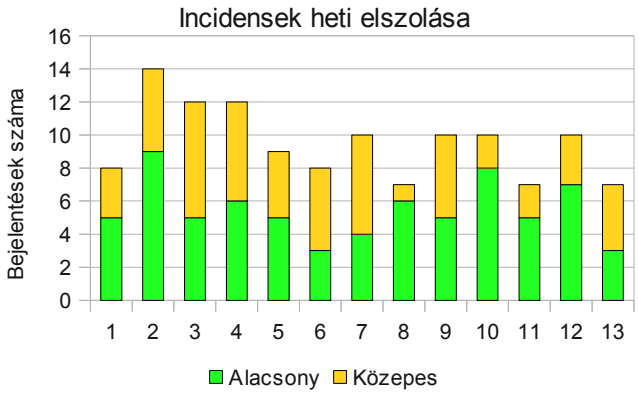


Összességében elmondható, hogy 2012. I. negyedévében a legtöbb terméket érintően még mindig a Microsoft vonatkozásában kerültek kiadásra szoftver sérülékenységek, de mostanra már felzárkózott az Oracle, az IBM és a Mozilla is a termékeiket érintő sebezhetőségek kapcsán felállított gyártói TOP5 kimutatásban.

Internetbiztonsági incidensek

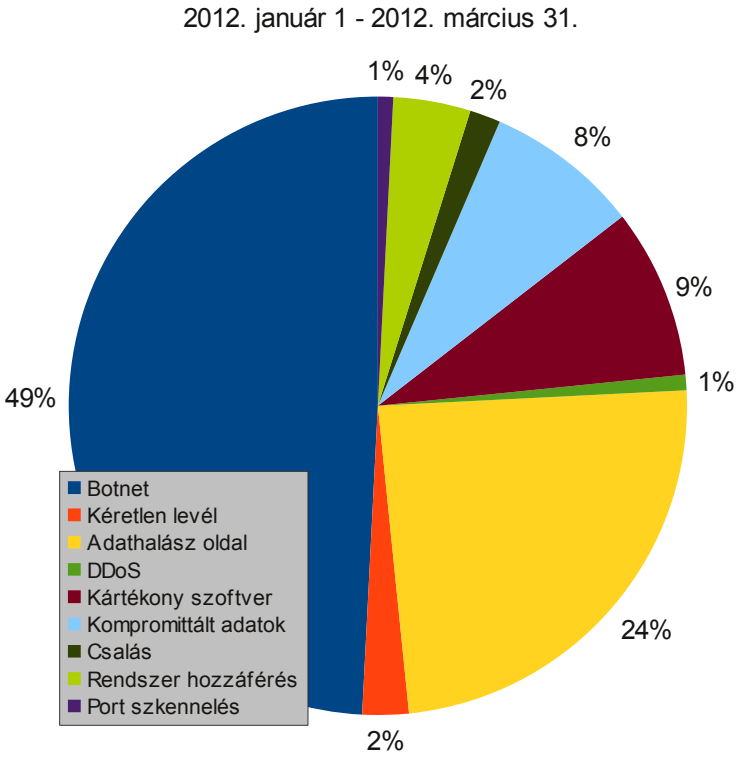
Internetbiztonsági incidens minden olyan biztonsági esemény, amelynek célja az információs infrastruktúrák bizalmasságának, sértetlenségének vagy rendelkezésre állásának megsértése az interneten, mint nyílt információs infrastruktúrán keresztül.

A PTA CERT-Hungary, **Nemzeti Hálózatbiztonsági Központ** a 2012-es év első negyedévében **124 db incidens bejelentést** regisztrált és kezelt, ebből 71 db alacsony és 53 db közepes kockázati besorolású.



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

A bejelentések többnyire külföldi partner szervezetektől érkeztek és több, mint 90%-ban hazai káros tevékenységgel vagy káros tartalommal voltak összefüggésben. Összesen 52 szolgáltató került bevonásra az egyes incidensek kezelése során és összesen 542 szálon folyt incidenskezelési koordináció.



A 2012-es év első negyedéves incidenskimutatását közel 50%-os arányban a botnet hálózatok által megfertőzött számítógépek kapcsán fogadott bejelentések vezetik, még úgy is, hogy ezek az adatok nem tartalmazzák Shadowserver Foundation-től beérkező bejelentéseket.

Továbbra is nagy számban érkeztek a felhasználók megtévesztésén alapuló a banki és egyéb bejelentkezési adatok megszerzését célzó, adathalász tevékenységekkel kapcsolatos bejelentések, melyek az incidensek 25%-át teszik ki. A relatív számosságukat tekintve ezek ugyan nem kiemelkedőek, de egy-egy incidens kapcsán több száz kompromittált felhasználó adatairól is beszélhetünk egyszerre. Az ilyen jellegű incidensek nem csak az adatszivárgás szempontjából érdekesek, hanem olyan szempontból is, hogy a megszerzett információk, hogy jutottak a támadók birtokába. Ezért az ilyen esetek kapcsán számba kell vegyük legalább egy esetleges sérülékeny szoftver vagy a felhasználó eszközeire települt káros szoftver jelentette kockázatokat is.

A fennmaradó 25% főként a kártékony szoftverek, az elosztott szolgáltatás-megtagadásos támadások valamint a kompromittált felhasználói adatok kapcsán érkezett incidens bejelentésekből tevődik össze. Ez utóbbi esetén érdemes megjegyezni, hogy bár ezek az incidensek a bejelentések mindössze 8%-át adják, a nagy számú érintett miatt ezen bejelentések kezelése az incidenskezelési koordináció közel 20%-át teszik ki.

Informatikai biztonság - 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.

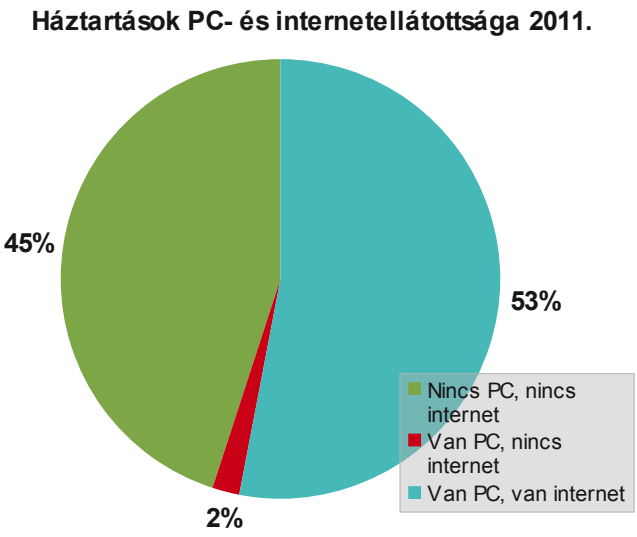
Az első negyedév fókuszcsoportja a háztartások, vagyis a home user tulajdonságait, lehetőségeit górcső alá véve, az őket érintő problémákat kiemelve, az ő jellegzetességeiket bemutatva áll össze a negyedév informatikai sérülékenységi összképe.

Eszközellátottság: internet- és PC-használat

A lakossági internetpiac

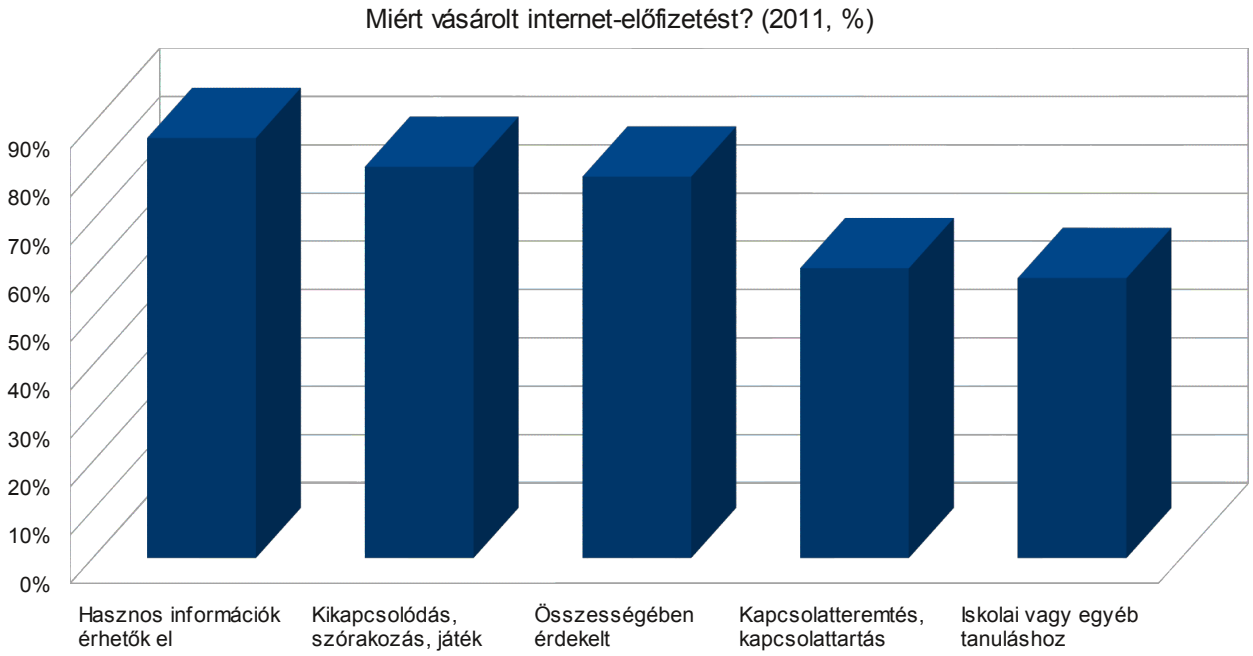
A lakossági internetpiacon a penetráció szolid, egyre kisebb mértékű bővülése mellett az előfizetések számának dinamikus emelkedése várható, elsősorban a mobilinternetnek köszönhetően.

A hazai háztartások több mint felében már ott az internet - derül ki a Magyar Infokommunikációs Jelentésből[1]. Az átfogó kutatássorozat legutóbbi, 2011. nyári adatfelvételének eredményei szerint az otthonok 53%-ában, mintegy 2,1 millió helyen férnek hozzá a háztartástagok a világhálóhoz, ami a penetrációs mutató egy évvel korábbi értékéhez képest mintegy 3,5%-os emelkedést jelent. A PC-ellátottság eközben szintén nőtt, de kisebb mértékben: a BellResearch több mint tíz évre visszamenő adatsorait egymás mellé illesztve látható, hogy az internet már csaknem utolérte a számítógépek elterjedtségének szintjét, noha öt évvel ezelőtt annak csupán a felét tette ki.

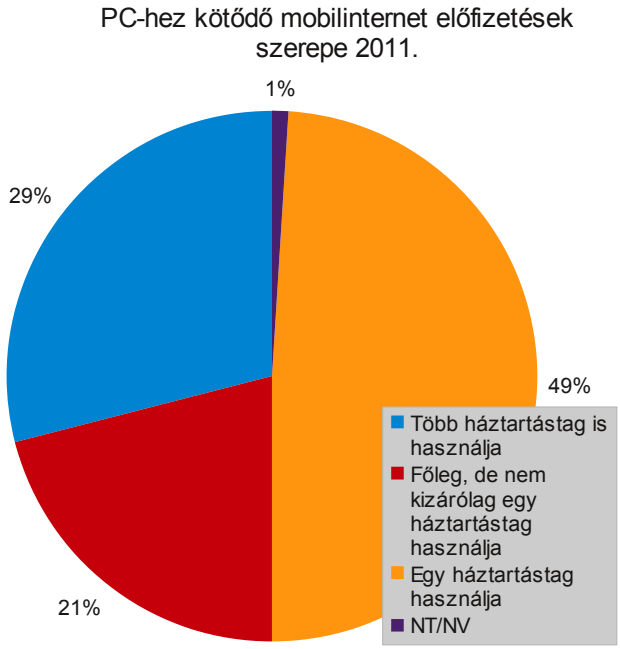


A két mutató közötti "olló" fokozatos záródása egyrészt örvendetes, ahol az eszközszintű infrastruktúra megvan, a világhálót sem nélkülözik már. A trendnek azonban árnyoldala is van, gyakorlatilag "elfogytak" azok a számítógéppel már rendelkező háztartások, amelyeknek az eszköz és az alapismeretek birtokában csak egyetlen, egyre kisebb, egyre könnyebb lépést kellett tenniük az internetig. Ma már a PC-használat egyik fő motivátora maga a világháló, az otthoni számítógép- és internetellátottság ezután gyakorlatilag együtt emelkedik tovább. A növekedés üteme azonban lassul, a trendgörbék egyre laposabbak: a leszakadóknál az eszköznélküliség, a teljes digitális írástudatlanság és az igény, motiváció hiánya ugyanis jelentős és nehezen áttörhető gátja a fejlődésnek.

1 Bellresearch: Magyar Infokommunikációs Jelentés 2011.



A Jelentés részletesen elemzi az egyes technológiák hozzáférési piacainak helyzetét és folyamatait is. A kutatás eredményeiből kiderül, hogy a "behálózott" háztartások túlnyomó többsége valamilyen vezetékes hozzáférést használ az internet elérésére, a legelterjedtebb ezen belül is a kábel (koax, optikai vagy hibrid), míg a DSL a második helyen áll, a mikrohullámú internet elterjedtsége viszont igen alacsony. A "large screen" mobilinternet (azaz a "nagy képernyős" eszközön igénybe vett, mobilnet-modemes, illetve -kártyás hozzáférés) a használó háztartások nagyobb részében jelenleg inkább a vezetékest helyettesítő megoldásnak tekinthető, és az érintettek jelentős hányada kizárólag otthon, illetve asztali gépen használja.



Át fog alakulni a mobil szélessáv szerepe. A jövőben egyre inkább a kiegészítés felé mozdul a súlypont, és tipikusabb lesz a vezetékes és a mobil hozzáférés együttes jelenléte, ami az előfizetések számának a penetrációnál dinamikusabb növekedését is eredményezi - prognosztizálják a BellResearch elemzői. A párhuzamos használatot több tényező indokolja, a helyhez kötött és a mobil technológiát más módon, eltérő körülmények között veszik igénybe a háztartástagok.

A fentieket alátámasztják a Telenor statisztikái is: 2011 végére a Telenor mobilinternet-előfizetőinek száma megduplázódott, 236 700-ról 478 100-ra növekedett 2010 decemberéhez képest. Jól látszik a mobilinternet gyors terjedése: 2011 decemberében összesen alig több mint 2 millió vezetékes, viszont majd 2,2 millió mobilinternet-előfizető volt hazánkban.

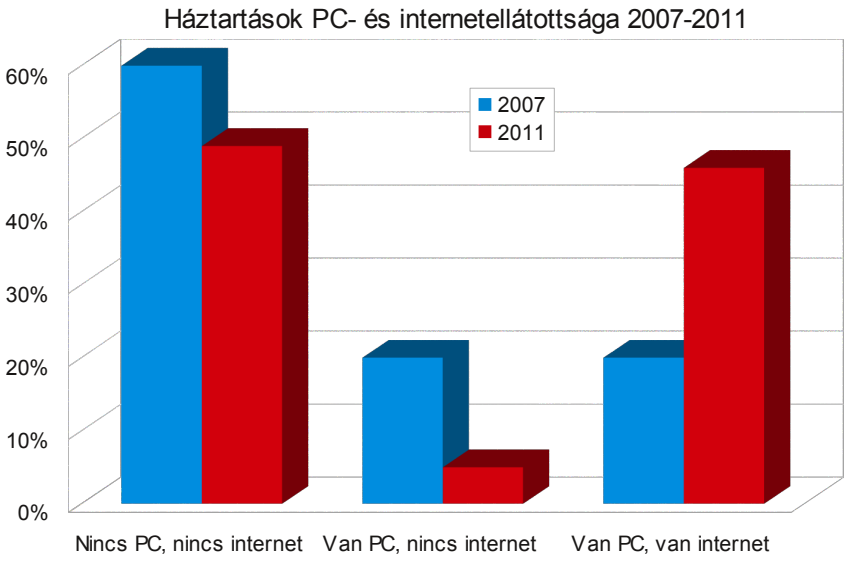
Okként a helyhez kötöttség minimalizálására vonatkozó felhasználói igény vezet, mely mobileszközök és szélessávú mobilinternet segítségével szinte bárhol, bármikor kielégíthető. Ezzel a lehetőséggel pedig élnek is a felhasználók, nálunk például egy év alatt az összesen forgalmazott adatmennyiség példátlan mértékben, 74%-kal, 713 500 gigabájtra nőtt. De nemcsak a mobilon való internethasználat intenzitása, hanem rendszeressége is növekvő tendenciát mutat. 2011. februárban még csak előfizetők 37%-a, novemberben pedig már 60%-a állította, hogy naponta többször kapcsolódik az internetre mobilján keresztül. Mindezek fényében kijelenthetjük, hogy 2012. a „mobilitás éve lesz".

PC-ellátottság

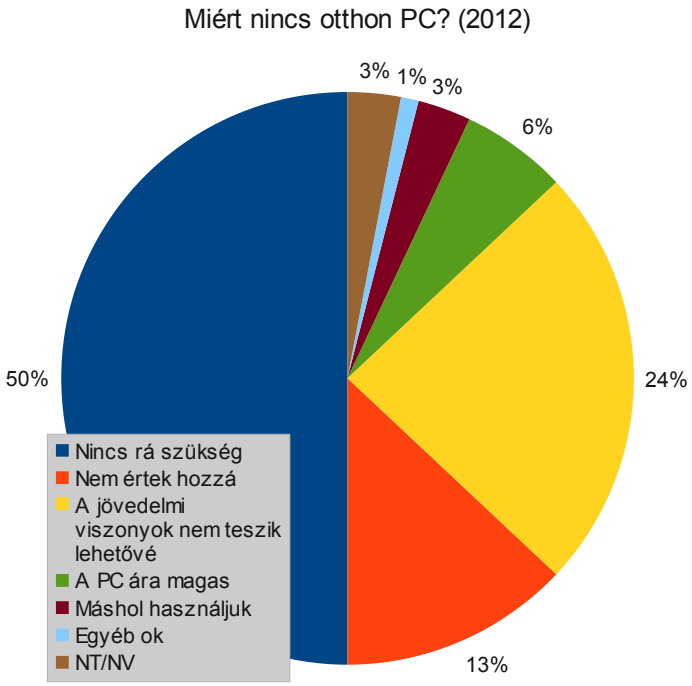
Lassan nő a hazai háztartások PC-penetrációja is, az otthoni számítógép és az internet elterjedtsége egyre jellemzőbb, a leszakadók felzárkóztatása pedig egyre nagyobb kihívást jelent. A bővülés dinamikája azonban lelassult - derül ki a Magyar Infokommunikációs Jelentés legutóbbi kiadásának eredményeiből.

A felmérés legutóbbi eredményei szerint legalább egy használatban levő személyi számítógépet 2,1 millió otthonban találunk, ami a magyarországi háztartások kicsivel több mint felét, 55%-át teszi ki. Az ellátottság azonban korántsem egyenletes, a kutatás számos jellemző mentén mutat rá különbségekre. Az adatokból kitűnik például, hogy a gyermek "igen jó hatással van" a PC-vásárlásra, ezen otthonok ellátottsága kétszerese azokénak, ahol nincs ilyen korú és státuszú háztartástag. A legfiatalabbak az iskolában mindenképp találkoznak a számítógéppel, ami erős motivációt jelent az otthoni eszközbeszerzésre és a családban úgymond megfertőzi az idősebbeket is. A településtípusokat tekintve a penetráció a fővárosban a legmagasabb, míg lemaradásban leginkább a községek vannak.

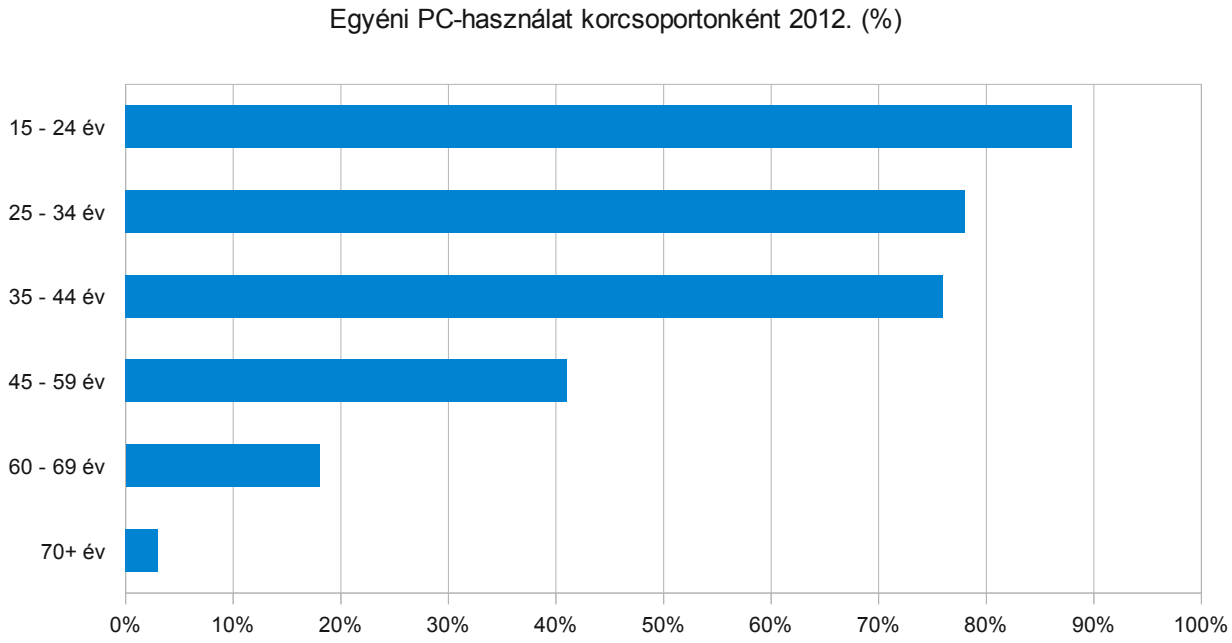
Az ellátottsági mutató az ellátatlanságot is jelzi. A háztartások 45%-a, közel 1,8 millió otthon máig nélkülözi a számítógépet, az információs írástudás alapvető eszközét. A digitális szakadék túloldalán, néhány ismérvet kiragadva, jellemzően az egy-két fős, idősebb, illetve az alacsonyabb iskolázottságú és jövedelmű háztartások állnak; az egyének szintjén a demográfiai profil hasonló.



A beszerzéstől visszatartó tényezők sorában az első helyen az érdektelenség, az igény hiánya áll. Minden második háztartásban, illetve a PC nélkül élők négyből három esetben nem érzik szükségét, nem látják hasznát egy számítógépnek, és sokan azért zárkóznak el, mert bevallásuk szerint nem értenének hozzá. Ez a többség. A jövedelem szűkössége, illetve a számítógép magasnak ítélt ára szintén számottevő hányadot tántorít el.



Érdekes és tanulságos összevetni a PC- és internetellátottság alakulását. Öt éve a behálózott háztartások aránya a számítógéppel rendelkezőkének csupán a fele volt. Ez az eltérés azonban mára alig 2%-ra kopott. Míg korábban a csak PC-t (internetet nem) használók széles utánpótlásbázist jelentettek az internetezés bővülésére, mostanra ez a tömeg elfogyott. Mivel az elzárkózás alapja az érdektelenség és az információhiány, a még mindig idegenkedők meggyőzése jóval nehezebb feladat, mint a korábbi, érdeklődő rétegek bekapcsolása. A gazdasági helyzet miatt az egyébként sem gazdag, digitálisan írástudatlan rétegek nem ruháznak be PC-vásárlásba és internet-előfizetésbe. Felzárkóztatásuk egyre nagyobb kihívást jelent.

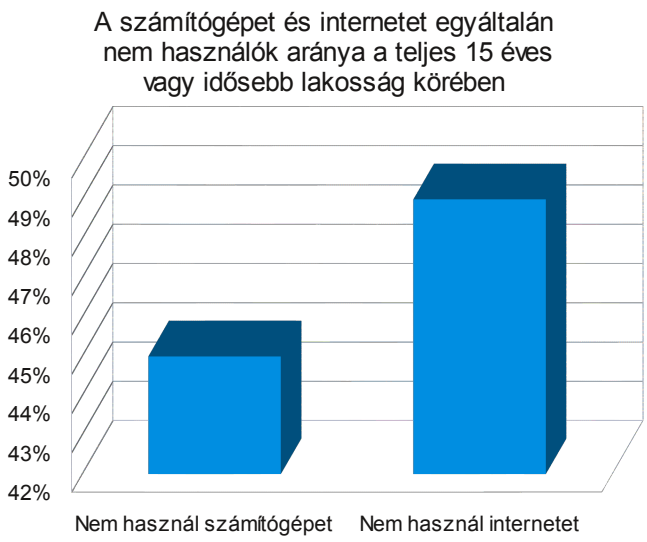


Digitális írástudatlanság: igény, ismeret vagy infrastruktúra hiány?

A fentiek alapján jól látható, hogy a jelenlegi számítógép- és internet-penetrációs szint mellett bőven van még tere a digitális érettség növekedésének – ehhez azonban láthatóan komoly erőfeszítések szükségesek.

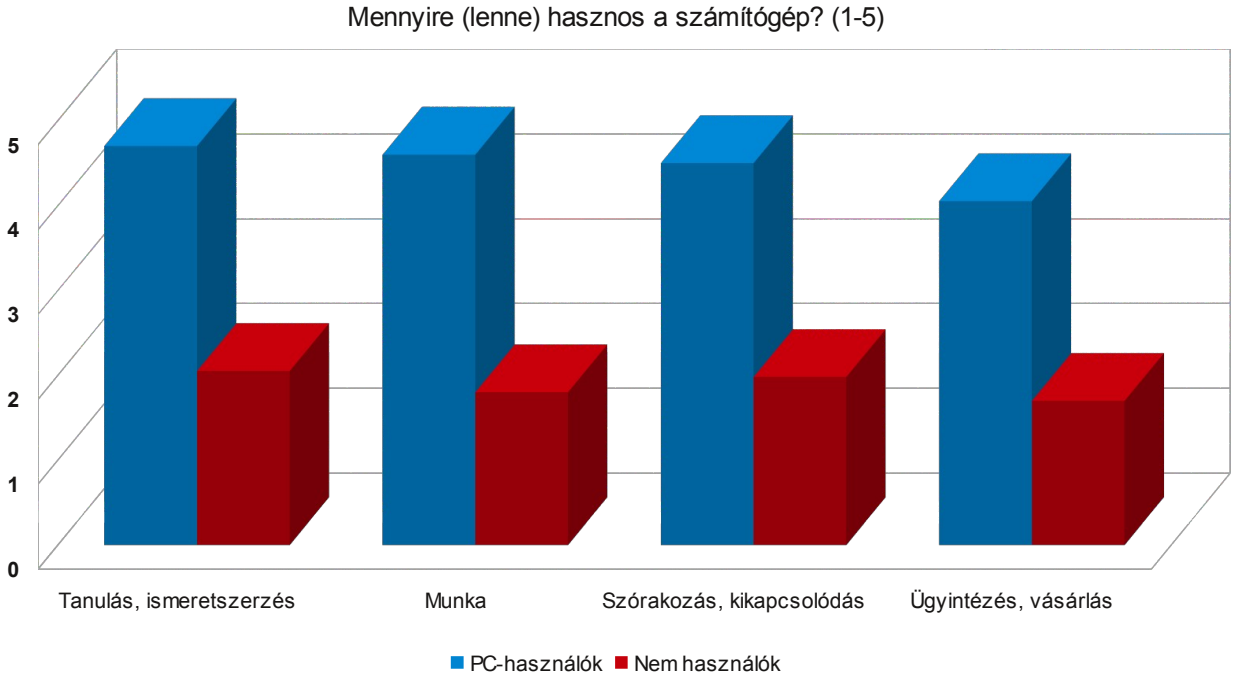
Az ICT-report 2011. év közepén készült lakossági felmérése szerint a 15 év felettiek 46%-a nem használ számítógépet, és minden második hazai lakos nem internetezik.

A kutatásból három fő tényező azonosítható, amelyek a számítógép- és internethasználat, illetve annak mellőzése szempontjából meghatározók.



Az első faktor a motiváció (igény), jobban mondva annak hiánya, ami az eredmények szerint a legfőbb akadály. A tartós PC- és nethasználat alapfeltétele, hogy e tevékenység a felhasználó számára értéket jelentsen, vagyis elég érdekes és hasznos legyen. Az információs társadalom teljes jogú tagja akkor lesz valaki, ha az internet a mindennapjai részévé, megszokott és új tevékenységeinek eszközévé válik, és ezekben hasznot, előnyt biztosít neki – akár felismeri ezt, akár csak hozzászokik.

A digitális szakadék két partja ily módon viszont mind messzebb kerül egymástól: a netezők mögött egyre inkább lemaradnak a világhálót nem használók, méghozzá nemcsak a PC- és internethasználati képességekben, hanem az élet számos területén, ahol a net valami pluszt, előnyt ad. A nem internetezőknél a világháló legnagyobb konkurense a televízió: szórakoztat és informál, méghozzá kényelmesen – és a többség azt gondolja, számára ez elég, a világ eddig tart. A PC-használók például a szórakozás és kikapcsolódás terén a számítógép hasznosságát 5-ös skálán 4,5 pontra, míg a nem használók csupán 2 pontra értékelték, de a különbségek egyéb vonatkozásokban is hasonlóak.

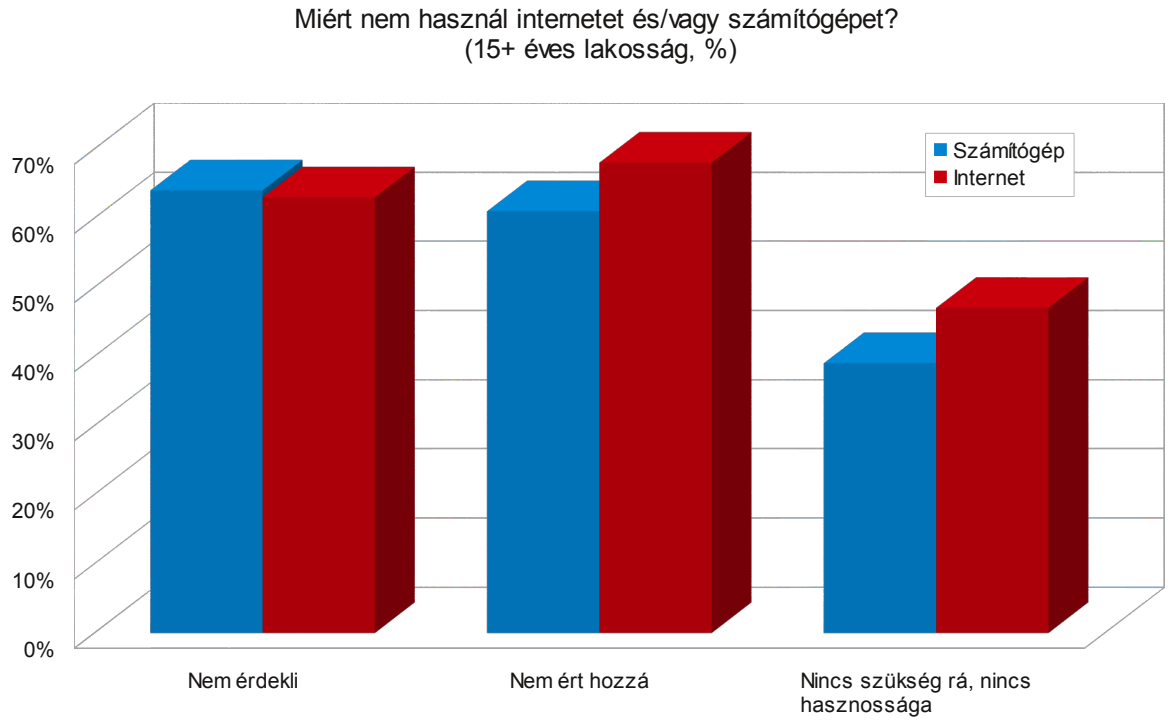


A következő meghatározó szempont a kompetencia (ismeret). A Jelentés eredményei szerint a hazai, 15+ évesek kevesebb mint fele (46%-a) vett részt bármilyen, számítógéphez vagy internethasználathoz kapcsolódó képzésen. Akiknek nem volt részük, lehetőségük fejleszteni ismereteiket, jellemzően az idősebb korosztályba tartoznak, illetve alacsonyabb végzettségűek.

A fiatalok – digitális „bennszülöttként” – már jó ideje az iskolában (is) kapják a tudást és a készségeket, amit szépen visszatükröznek a használati mutatók. Ebből az is nyilvánvaló, hogy a kevésbé szerencsések, s nem utolsósorban a nekik segíteni igyekvő, a digitális írástudás növelése iránt elkötelezettek számára nem kis kihívást jelent a helyzet feloldása, hiszen az érintettek többsége

már nemigen fog iskolai vagy egyéb oktatásban részesülni.

Végül pedig a hozzáférés: ugyan a visszatartó tényezők sorában jóval az igény és a tudás mögött áll, az elérési lehetőség hiánya a nemhasználók ötöd-hatodrészét tartja vissza az internetezéstől. Ezzel összefügg, hogy közel ugyanennyien anyagi okokra hivatkoznak, amelyek az esetleges jövőbeli használat feltételei között még jelentősebb súllyal szerepelnek. Az viszont, hogy milyen kiadást enged meg magának a háztartás, bizonyos mértékben a preferenciáktól, az észlelt fontosságtól is függ. Ezzel visszakanyarodtunk az igények és a motiváció, illetve az ismeretek kérdésére.



A fenti három tényező együttesen kiadja az információs társadalom egyszerűsített modelljét: infrastruktúra, ismeret, igény. Hol az egyik, hol a másik „i” válik meghatározó fontosságúvá. Mára az igény, a motiváció hiánya lett az információs társadalom kínálta előnyök kihasználhatóságának, a társadalmi esélyegyenlőség növelésének legfőbb gátja. Így aztán nem csoda, hogy a számítógép-használathoz szükséges ismeretek terjedése is jóval lassabb és kevesebb embert ér el, mint az kívánatos lenne.

Az igény felkeltésének számos módja van, a felhasználóbarát közigazgatási ügyintézés lehetőségétől az ismeretterjesztésen át a szórakoztatásig.

Az ismeretek terjesztésének tömegesítését Magyarországon többek között a Neumann János Számítógép-tudományi Társaság is a zászlajára tűzte, véleményük szerint 2-3 év alatt akár másfél millió embert érintő módon megoldható egy komplex ismeretterjesztő program kialakítása. A program, akár EU-s forrásból, a teljes projektet tekintve 10-15 milliárd forintból megvalósítható lenne, ráadásul számos munkalehetőséget teremtve az ország versenyképességét is javíthatná.

A jövőre vonatkozó várakozások a PC-t és internetet nem használók tervei, szándékai alapján igen visszafogottak. A motiváció, kompetencia, hozzáférés tényezőhármasból bármelyik faktor elégtelensége jelentősen visszafogja az új felhasználók belépési esélyeit. Ismeretek hiányában nem észlelhetőek és értékelhetőek a digitális írástudás előnyei.

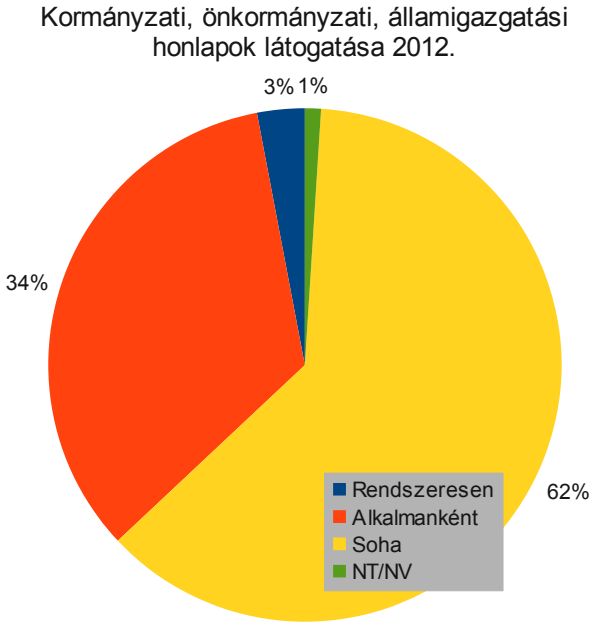
Igény és motiváció nélkül pedig a használattól most még tartózkodók nem lépnek be az információs társadalomba – és ott ragadnak a szélesedő digitális szakadék túloldalán.

Az e-ügyintézés, mint lehetséges motiváció

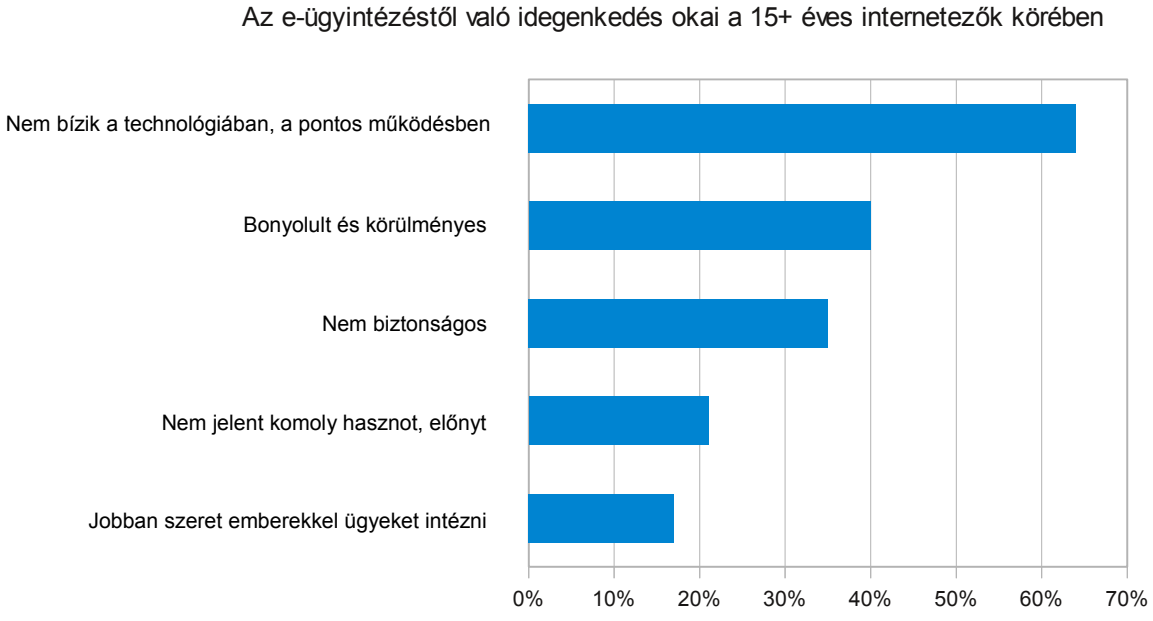
Jellemzően a tájékozódásra, információk beszerzésére terjed ki az e-ügyintézés. Nő az online csatorna jelentősége, de nem szorítja ki a személyes és telefonos kapcsolatot.

Közvetlen és járulékos előnyt is nyújt az online ügyintézés az ügyfelek és a intézmények, az üzleti szereplők számára is. Elterjedtsége az információs társadalom fejlettségének egyik fokmérője.

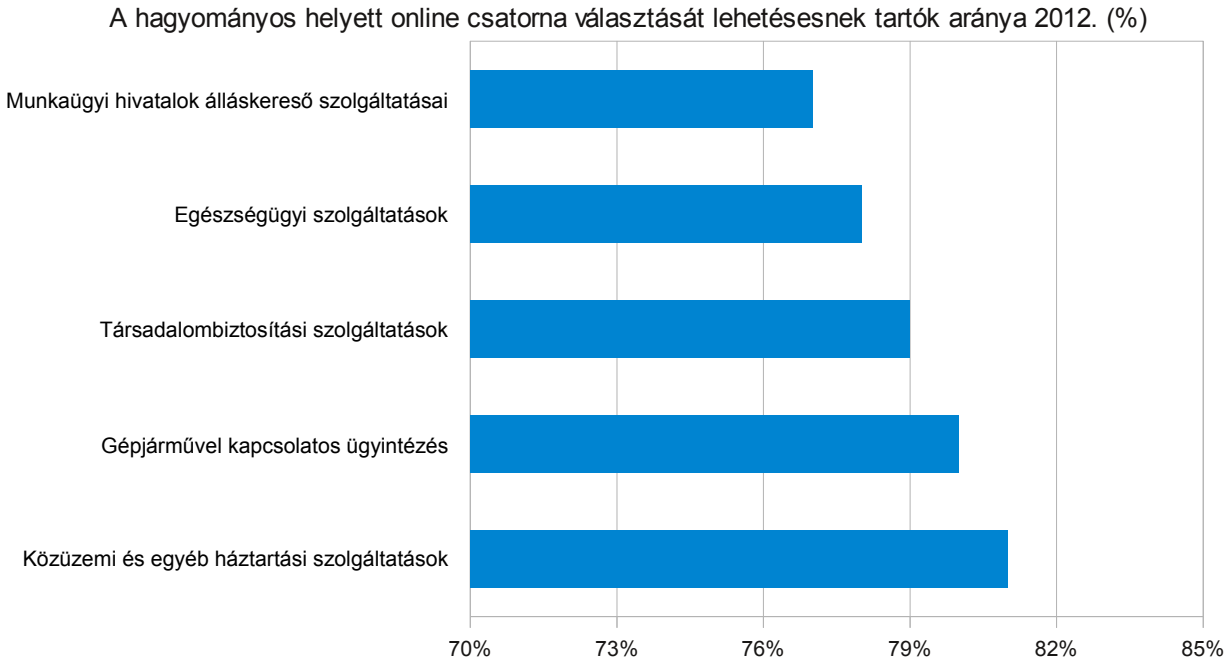
A használati célok között a kapcsolattartás, az információszerzés és tájékozódás, valamint a szórakozás, kikapcsolódás vezet. Ennél sokkal alacsonyabb azok aránya, akik az internetre az ügyintézés lehetséges platformjaként tekintenek. Ügyei intézésére a 15 éves és idősebb hazai internetezők szűk egyharmada használja a netet, az életkor szerint vizsgálva a 25 év felettiek körében magasabb az elterjedtségi arány. Ez a nagyjából 1,3–1,4 millió fő netpolgár a teljes, 15+ éves hazai lakosság 16%-át teszi ki. Az internetezők többsége tehát egyelőre sohasem, vagy csak ritkán kezdeményez ilyen tranzakciókat. Ugyanerre utal, hogy az internethasználók kicsivel több mint harmada, 37%-a keres fel legalább alkalmanként államigazgatási, kormányzati vagy önkormányzati honlapokat, a rendszeres használók aránya viszont csupán 3% körül alakul.



Az internetes ügyintézéstől való idegenkedés hátterében nem a bizalmatlanság vagy a hozzáértés hiánya áll, hanem az emberek személyes kontaktus és interakció iránti igénye. A megszokások csak lassan változnak, az ügyintézés fogalma a buktatókkal és a bürokráciával kapcsolódik össze, amelynek – sokszor már csak képzelt – útvesztőiben megnyugtatóbbnak tűnik, ha élő ügyintéző vezet végig a folyamaton, magyaráz, értelmez és segít. Mégis, a vizsgálatban megkérdezett internetezők kétharmada a világhálót hasznosnak tartja az ügyintézésben. A netezők közel fele a maga számára is vonzónak ítéli az online ügyintézést. Ez biztató alap a használói kör bővüléséhez.



Az űrlapok és iratminták letöltése, illetve az ügyintézés és adatszolgáltatás terén ítélték a leghasznosabbnak a válaszolók az online csatornát, de a közérdekű kérdésekhez való hozzászólás is a közepesnél magasabb pontszámot kapott. A konkrét használat tekintetében azonban a kutatás még alacsony arányokról számol be. Az internetezők körében három terület ért el 15%-os igénybevételt 2011-ben, a közérdekű információk elérése, az ügyindítás és időpontfoglalás, valamint az űrlapok és nyomtatványok letöltése. Teljes ügyet csak a netezők egytizede bonyolított az interneten, de erre amúgy csak az ügyek korlátozott körénél van mód.



Az egyes ügytípusok közül a személyi okmányokkal, a jövedelemadó-bevallással és az egészségügyi szolgáltatásokkal kapcsolatos ügyek relevánsak a többség számára. A kutatás rávilágít, hogy ezeken a területeken az érintettek nagy többsége elképzelhetőnek tartja a hagyományos ügyintézési mód helyett az internet használatát. A megítélés tehát pozitív, és az elvi fogadókészség is megvan – a „kínálati oldal" feladata, hogy tágítsa az elérhető szolgáltatások körét.

Az államnak komoly felelőssége lenne az elektronikus ügyintézés vonzóvá tételében. Nincs központi reklámkampány, meggyőző figyelemfelhívás. Talán azért, mert az elérhető szolgáltatások köre erősen korlátozott. Az időpont-foglalási és űrlapletöltési lehetőségek önmagukban nem vonzanak elég felhasználót. Az SZJA elektronikus bevallásának lehetősége nem a legmeggyőzőbb motivációs eszköz. Az is korlátozza az internetes ügyintézés terjedését, hogy sokszor még a digitális írástudók számára is kihívást jelent a legegyszerűbb ügyek végrehajtása is.

Pedig az online ügyintézés kiváló eszköz lehetne az államigazgatás kezében az életminőség érzékelhető javítására. De hiányzik a motiváció, sok esetben hiányzik a tudás, a vonzó, személyes megjelenést egyáltalán nem igénylő online szolgáltatások.

Senior felhasználók

Használják a közösségi site-okat, tudják, hogy a tévéműsort az interneten kell keresni. Az időskorú magyar internetezők egy része belül van a digitális szakadékon - derült ki az első nemzedékek közötti technológiai konferencián.

Az Óbudai Egyetemen 2012. április 14-én megrendezett Veletech 2012 kiállítás részben a megvásárolható csúcstechnológiáról szólt.

Ám az egyik teremben egy új, egyedi program zajlott: idősek beszélnek időseknek az internetről, amit teljesen a magukénak éreznek. Magyarország 6,5 millió internetezőjének nem mindegyike fiatalkorú. Nem vagyunk ugyan a világ élvonalában, az ötvenöt évnél idősebbeknek csupán 34%-a internetezik, ám nem is állunk a lista végén. Olaszországban például a senior internetezők csak 22%-a ül gép elé.

Van ráadásul olyan mutató is, amiben a magyarok a világ élvonalába tartoznak, rekordmennyiségű közösségioldal-használó van. Információs Társadalom- és Hálózatkutató Központ[2] [3] 2012 elején publikált tanulmánya szerint a hatvan évnél idősebbek felének (52%) van profilja valamelyik közösségi oldalon, az ötven évnél idősebbek esetében ez az arány még magasabb (61%).

A közösségi oldalakon való aktív jelenlét magyar sajátosság, sem a környékbeli, sem a digitális írástudás tekintetében jóval fejlettebb skandináv országokban nincs példa ilyesmire. Még Svédországban is csak az idősek negyede rendelkezik profillal valamelyik közösségi oldalon, de az USA-ban is csupán 43% ez az arány.

A rejtély megfejtése valószínűleg az iWiW, a magyar közösségi oldal a hazai internet egyik olyan szolgáltatása volt, ami miatt akár az internetet is hajlandóak voltak beköttetni az emberek. A régi ismerősök újbóli megtalálása, az emlékek felidézése magyar netes sporttá vált. Az iWiW egyeduralma az évek során megszűnt, az ITHAKA vizsgálata szerint az idős internetezők azóta a Facebook-ot is felfedezték maguknak.

A regisztrációval rendelkezők 64%-a naponta ellátogat kedvenc oldalára, fele pedig több mint száz ismerőssel áll kapcsolatban. Bár otthonosan mozognak ebben a közegben, keveset foglalkoznak az adatbiztonság kérdésével. Míg a fiatalok 40%-a nyilatkozott úgy, hogy közösségi médiás profilja nyitott, azaz mindenki számára látható, az idősebbek 69%-a nem használ semmilyen szűrőbeállítást, így például gyakran telefonszámuk, más elérhetőségük is publikus. 45%-uk soha nem is foglalkozott a biztonsági beállítások módosításával.

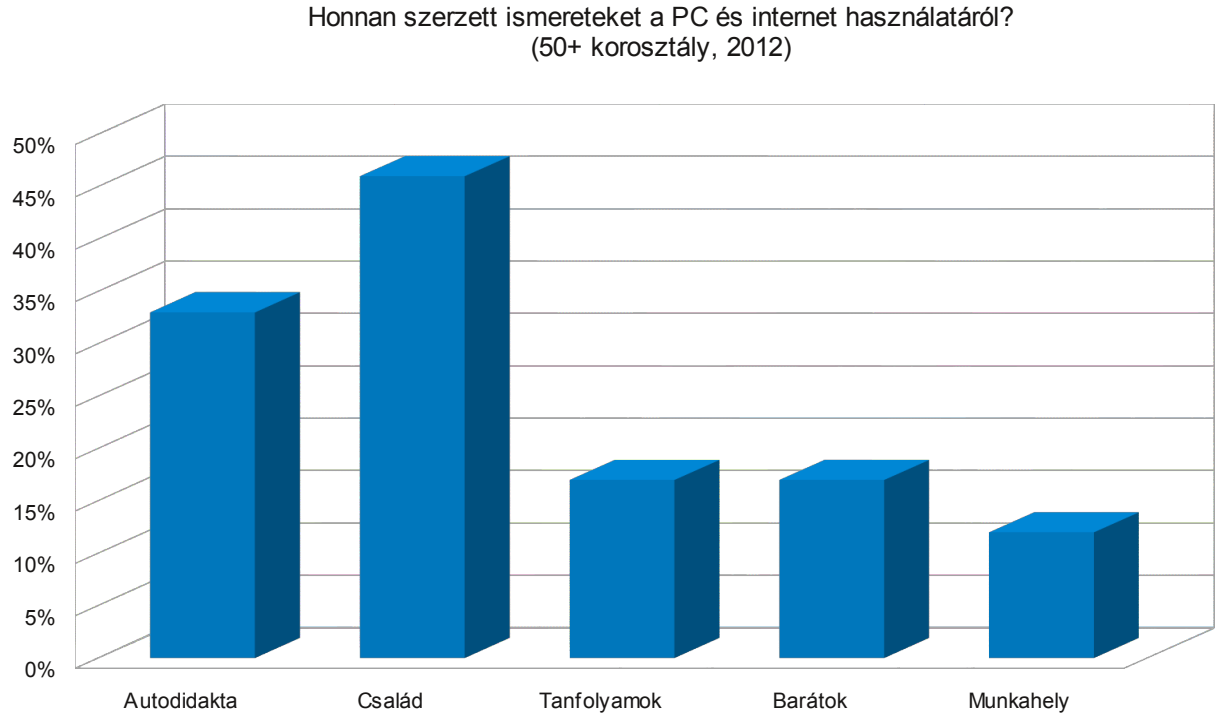
Azzal azért tisztában kell lenni, hogy az internetező és facebookozó idősek kisebb intenzitással használják az internetes szolgáltatásokat. Kevesebbet lájkolnak, ritkábban töltenek fel saját tartalmat, vagy osztják meg más műveit. Civil politikai aktivitásra, információszerzésre azonban ugyanolyan arányban (29%) használják a közösségi oldalakat, mint a 29 évnél fiatalabbak.

Az internetnek a kapcsolattartásban betöltött kiemelt szerepét jelzi az idősek körében az online kommunikációs lehetőségek aktív használata is. Az ötven év feletti válaszadók csaknem negyede használ rendszeresen internetes telefonszolgáltatást, ez 4%-kal nagyobb arány, mint a fiatalabbak esetében. Több mint egynegyedük (28%) pedig azonnali üzenetküldő segítségével chat-el. Körükben ugyanakkor az online csatornák és a mobiltelefon mellett továbbra is nélkülözhetetlen eszköz a hagyományos, vonalas telefon – a válaszadók több mint fele használja rendszeresen.

A technikának nem csak a bővebb információkínálat a jó hatása. A kutatás szerint például a mobiltelefonnal rendelkező idősek sokkal aktívabbak, kevésbé magányosak, mint a mobil nélküliek. A jövő több funkciót tömörítő eszközeinek pedig talán még erősebb lesz ez a hatásuk. Még az se lesz baj, ha a "minden egyben" kütyük elsőre bonyolultak lesznek. Az idősek arra számítanak, hogy ezek használatát is elsajátíthatják a fiatalabb generációtól.

2 Ithaka: Az 50 év feletti netezők újmédia- és internethasználati szokásai, 2011. december

3 Origo: Minden harmadik nagyi internetezik Összefoglaló a Veletech 2012. nemzedékek közötti technológiai konferenciáról, 2012.04.16.



Az ITHAKA felmérése arra is rámutat, hogy az idősek hajlandóak maguktól is megtanulni az új technikai eszközök használatát. Az ötven évnél idősebb internetezők egyharmadának senki sem tanította a számítógép és a világháló használatát, maguktól sajátították el. Ennél csak az a csoport a nagyobb (46%), akik a hagyományos úton, a fiatalabb családtagok segítségével barátkoztak meg a géppel.

Lényeges tudásforrásnak számítanak még 17-17%-os részesedéssel a szervezett tanfolyamok és a barátok is. A munkahelyen azonban csak 12% tanult internetezni. Úgy tűnik, hogy a munkáltatók hamarabb mondanak le a számítógépet nem ismerő idősekről, mint a barátaik.

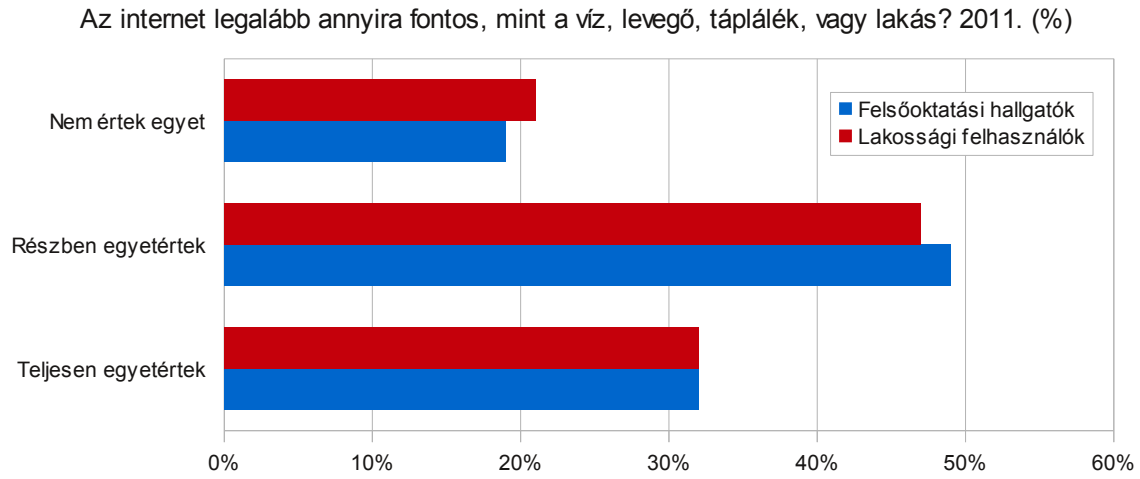
A 60+-os korosztály hír-centrikus, lelkes rádióhallgató, és hajlandó utánamenni az információknak. A vizsgálatban résztvevő idősek sok esetben megtanulták, hogy a tévét az interneten kell nézni. A monitor ugyan nem olyan kényelmes, mint a nagyobb képernyő, kevesebb ember fér elé, de ha az ember lemaradt egy programról, a tévék oldalán vagy a YouTube videomegosztón valószínűleg megtalálja.

A felmérésből kiderül, hogy a szeniorok nemcsak a netet, de a számítástechnikai és újmédiás eszközöket is egyre magabiztosabban használják. Az 50+ korosztály körében ugyan továbbra is az asztali számítógép a népszerűbb – 82%-uk rendelkezik PC-vel –, több mint egyharmaduk azonban notebookot, laptopot is használ. 70%-uknak van DVD-lejátszója – e tekintetben csak 2%-kal maradnak el az ötven év alattiaktól – és majdnem egynegyedüknek DVD-felvevője, amivel jócskán meg is előzik a fiatalabb korosztályt. Mindehhez tegyük hozzá azt is, hogy a műsorok rögzítéséhez a megkérdezettek csaknem fele még mindig hagyományos videómagnót használ. Amíg azonban a fiatalabbaknak csupán 4%-a ugorja át a reklámokat a visszanézésénél, az idősebbek 15%-a áttekeri őket.

Fiatal felhasználók

A legújabb digitális fogyasztással kapcsolatos Nielsen-tanulmány szerint Amerikában a 18-34 közötti korosztály „mindent visz”.

Megjelent a Nielsen és az NM Incite legújabb jelentése az amerikai felhasználókról. A State of the Media: U.S. Digital Consumer Report elnevezésű tanulmány középpontjában a Generation C-nek nevezett korosztály áll. A szinte folyamatos hálózati lét, online kapcsolódás (connected) után elnevezett generációhoz a 18-34 közöttieket sorolják a Nielsen kutatói.



Forrás: Cisco[4]

Ez az a korcsoport, amelynek tagjai az amerikai lakosság 23%-át alkotják, ám ennél jóval nagyobb hányadot alkotnak a készülékhasználatot, médiafogyasztást vizsgáló statisztikákban. Felülreprezentáltak a tablet-tulajdonosok körében (33%), az okostelefonosok (39%) között, és nagyobb arányban néznek online videókat (27%); valamint a közösségi oldalakon és blogokon is jelentősebb arányban (27%) vannak jelen. A fenti számok közül talán az a legelképesztőbb, hogy az összes amerikai okostelefon-tulajdonos közel 40%-át ezen korcsoport tagjai alkotják, de szinte mindegyik vizsgált kategóriában ez a korosztály a domináns. Egyetlen olyan kategória azért van, amelyben nem felülreprezentáltak, ez pedig a tv-nézés. A televíziózó amerikaiak között ugyanúgy 23% az arányuk, mint az összlakossághoz képest.

Minden (releváns) szempontból egyedi korosztályról van szó; amelynek célcsoportként való kezelése egyszerre jelent lehetőséget és komoly kihívást a marketingesek és a tartalomszolgáltatók számára.

A következő, a 35-49 év közöttiek alkotta csoport, a közösségi oldalak és a bloghasználat terén megelőzi (1%-kal) az egy kategóriával ifjabbakat, és szintén 28-27-re nyert a C-generáció ellen az online videófogyasztás tekintetében is.

Vizsgálták a nemek közötti megoszlást is az egyes kategóriákban. Az okostelefon-tulajdonosok fele férfi, fele nő, a tablet-birtoklás terén valamelyest a férfiak vannak többségben (53%), ám a többi tekintetben a hölgyek állnak jobban, mivel nagyobb az arányuk az online videófogyasztók, a közösségi site- és bloghasználók, valamint a tévézők között is.

4 Cisco: Connected World Technology Report 2011., 2011.12.14.
http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/CCWTR-Chapter1-Report.pdf
http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/2011_cisco_connected_worldtrechnology_report_chapter_2_report.pdf
http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/2011-CCWTR-Chapter-3-All-Finding.pdf

A tanulmány szerint napjainkban 274 millió amerikai fér hozzá – otthon, munkahelyén vagy más módon – az internethez. Ez több mint a duplája a 2000-ben mért 132 milliónak. A Szövetségi Kommunikációs Bizottság (FCC) szerint aggasztó, hogy 100 millió amerikai polgár otthonában nincs gyors internetkapcsolat, mondván nem szabad hagyni, hogy „digitális elit" alakuljon ki, az ország lakosságának harmada pedig kimaradjon a szélessávú gazdaság előnyeiből.

Az IT-biztonság kihívásai a lakossági szektorban

Az IT-biztonság társadalmi hatásai

A Trustworthy Internet Movement (TIM) nevű kezdeményezést 2012. március 1-jén[5] jelentették be az RSA San Franciscó-i konferenciáján. A TIM az elképzelések szerint olyan nonprofit, szállítóktól független projektként működik majd, amely egyesíti a technológiai ipar, az IT-biztonsági szakemberek és a tőkebefektetők erőforrásait az internet alapvető problémáinak orvoslására.

A szervezet első közleménye szerint ilyen probléma például a minősítő hatóságok elégtelen ellenőrzése, az SSL protokoll irányításának kérdései, vagy a malware és a botnetek terjedése, amelyek ellen beépített biztonsági megoldásokra lenne szükség már a publikus és privát felhők legalapvetőbb szintjén is. Bár a cloud technológiák a megfelelő köztes-rétegeken keresztül magukban hordozzák a magasabb szintű biztonsági kontroll lehetőségét, a TIM általában az internet megbízhatósági problémáinak megoldását tekinti legfontosabb kezdeti feladatának, ami bármilyen későbbi továbblépés feltétele lesz.

A kezdeményezés alapja, hogy többé nem technológiai, hanem társadalmi kérdésekről van szó, ahogy több mint kétmilliárd ember támaszkodik szakmai és magánéletében a világhálóra. A mindenütt jelenlévő rosszindulatú kódokon vagy éppen az e-mail spoofing (meghamisított feladóval küldött levelek) módszerein keresztül maga a böngésző vált az egyik legfőbb támadási vektorrá, míg az informatikai biztonsági megoldások jórészt reaktívan működnek.

A prevenció viszont a sebezhetőség nyilvános beismerését jelenti, ami a vállalatok, de még a magánemberek számára is nehézséget okoz. Ha a biztonsági technológiákat nem az alapoknál építik be valamibe, az a megoldás óhatatlanul ki lesz téve a nulladik napi támadásoknak.

A Trustworthy Internet Movement kezdeményezéséhez elvben bárki csatlakozhat, akár Magyarországon is. A szervezet oldala szerint ugyanúgy várják a fejlesztők, szakértők, cégek, befektetők vagy tudományos intézmények jelentkezését akár a szakmai munkában való részvételre, akár egy speciális probléma megoldásának finanszírozására, sőt adott esetben a TIM is anyagi segítséget nyújtana más nonprofit projektek megvalósulásához. Kezdetben azonban mégis a háttérben működnének, így a csatlakozó partnerek listáját sem lobogtatják.

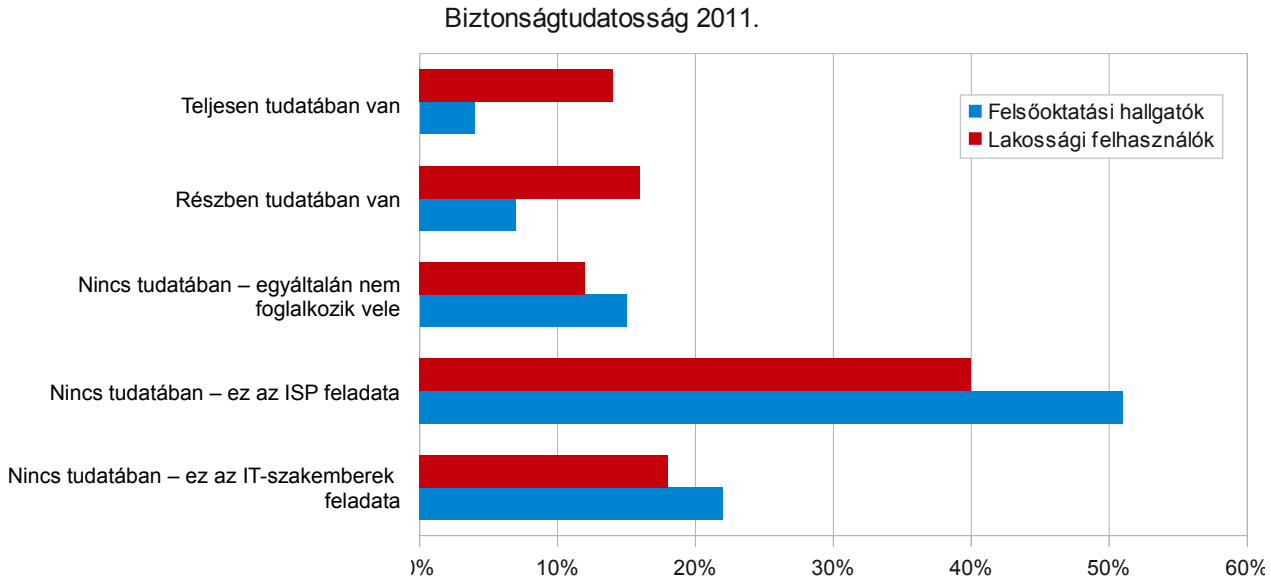
Ennek oka, hogy első lépésben megoldást akarnak találni valamilyen közismert biztonsági problémára, hogy később jobb eséllyel álljanak a kockázati tőkebefektetők elé. A megoldás csak a nagyvállalatok, felhőszolgáltatók vagy szakmai szervezetek tehetséges szakembereinek összekapcsolásával lehetséges, és az internetszolgáltatókra is csak szervezetten lehet bármiféle nyomást gyakorolni.

5 Tököli Gábor: Ma már társadalmi probléma az online biztonság, 2012.03.02.

Felkészültség és tudatosság

A napjaikban zajló digitális forradalom kapcsán az egyik legnagyobb fenyegetést a számítógépes bűnözés jelenti a gazdasági visszaélések között. A kiberbűnözés mára világszerte bekerült a négy legfőbb gazdasági bűnözési típus közé.

Jó páran estek már áldozatul számítógépes bűnözésnek, és sokan mondják, hogy felkészültek, de a váratlan támadást még nehezen tudják kivédeni. Ugyanakkor a kiberbűnözésnek nincs egységes, nemzetközileg is elfogadott definíciója. Az elkövetési móddal kapcsolatos ismeretek hiányában megvan annak az esélye, hogy a szervezetek nem tudják, milyen veszélyekkel kell szembenézniük, azok honnan érkezhetnek, és milyen módon érinthetik az üzletmenetet, így azokat nagyon nehéz beazonosítani és küzdeni ellenük.



Forrás: Cisco[4]

A PwC globális gazdasági bűnözésről készített felmérése[6] szerint, míg globális szinten a válaszadók 26%-a, Közép- és Kelet-Európában pedig a 22%-a gondolja azt, hogy valószínűleg számítógépes bűncselekmény áldozatául fog esni a következő 12 hónapban, addig Magyarországon ez a szám mindössze 8%. Aggodalomra ad okot, hogy a megkérdezett cégek csaknem fele nem kapott semmilyen számítógépes biztonsággal összefüggő képzést az elmúlt 12 hónapban, ráadásul több mint felük nem rendelkezik az elhárításhoz szükséges erőforrásokkal.

Internetes bűnözés Magyarországon

Magyarországon 2011-ben körülbelül 21 milliárd forintnyi veszteséget okoztak az online bűnelkövetők. A legnagyobb visszaéléseket bankkártyákkal hajtják végre - derül ki a Symantec és a BRFK közös felméréséből.[7]

2011 során 21%-kal nőtt a BRFK-nál bejelentett online visszaélések aránya 2010-hez képest, 2009-hez viszonyítva viszont már 63%-os emelkedésről lehet beszélni. 2011-ben közel 900 ezer felnőtt magyar volt célpontja internetes bűncselekménynek, melyek összesen 21 milliárd forint kárt okoztak az érintetteknek. A rendőrség, a Btk. alapján, a következő eseteket különbözteti még meg: rendszer elleni támadások, internetes csalások, adathalászat, szerzői joggal kapcsolatos bűncselekmények, egyéb feltörések, zaklatások és pedofília. Az online visszaélések visszaszorítása érdekében a BRFK együttműködik a Puskás Tivadar Közalapítvány által működtetett Biztonságosinternet Hotline-al.

6 PriceWaterhouse Coopers: Globális Gazdasági Bűnözés Felmérés 2011. – Magyarországi jelentés
7 Sági Gyöngyi: Tavaly 900 ezer hazai célpontja volt az online bűncselekményeknek, 2012.02.21.

A lakossági bejelentések kétharmada káros internetes tartalmakra vonatkozik, amely nem mindig számít bűncselekménynek, de már sértheti az egyének vallási, etnikai hovatartozását, illetve személyiségi jogait. Ilyen esetekben, mint például a közösségi médiában feltett sértő képek/videók eltávolításában együttműködik jogi, illetve civil és állami szervezetekkel, hogy mielőbb kapcsolatba léphessünk a gyakran külföldi tulajdonban lévő üzemeltetőkkel.

A Symantec által évente kiadott világméretű kiberbűnözési elemzés[8] adatai is alátámasztják az online bűnözés folyamatos térnyerését. A 2011-es riport szerint több mint 286 millió egyedi rosszindulatú program létezik világszerte, ez 19%-os növekedést jelent a 2009-es adatokhoz képest, akkor a károkozók száma 240 millió volt. Magyarországon is a vírusok és kártevők állnak az élen, részarányuk eléri a 60%ot.

A vírusok között a leggyakrabban azok a ma már hétköznapinak számító kémprogramok bukkannak fel, amelyek legtöbbször a felhasználók tudta nélkül futnak számítógépeiken és folyamatosan gyűjtik a bizalmas információkat. A kémprogramok esetében általában hasonló forgatókönyvhöz szoktak folyamodni a bűnözők: vagy egy ingyenesen letölthető program mellé fűzik károkozóikat, illetve felugró ablakokon hívják fel a figyelmet egy nagyon kedvező vagy ingyenes ajánlatra, ezekhez általában egy igen, illetve nem opció is tartozik, amelyre ha a felhasználó rákattint, elindítja a vírus letöltését.

Az elmúlt két évben a károkozók legjobb táptalajává a közösségi média, illetve az új típusú mobil eszközök váltak. A mobiltámadásokat illetően a Norton jelentése több mint 42%-os növekedésről számolt be 2009-hez képest. Az új mobil operációs rendszerek sebezhetőségének száma ugyanis 115-ről 163-ra nőtt 2010-ben.

A mobilfenyegetések mellett a közösségi hálózatok és a megfelelő védelem hiánya okozza a számítógépes bűnözés növekedését. A magyar felnőtt internetezők több mint egyharmada semmilyen óvintézkedést nem tesz a telefonos internetezés biztonságáért. A legutóbbi nagyobb mobil támadási hullámról az elmúlt hetekben számolt be a Symantec, amikor hamisított Android Market-et azonosított, ezen különböző alkalmazásoknak álcázott vírust tölthettek le a gyanútlan felhasználók.

Az okostelefonokra veszélyt jelenthetnek az ingyenes Wi-Fi hotspotok is, amelyeknél gyakran előfordul, hogy a kiberbűnözők adatcsomag-monitoring szolgáltatást vásárolva sikeresen lehallgathatják a felhasználók hívásait, illetve ellophatják a titkosítatlan jelszavakat.

8 Symantec: Norton Cybercrime Report 2011, 2012.01.13.

Adatbiztonsági kihívások a számítási felhő szolgáltatások kapcsán

Kétségtelen tény, és már-már közhely a gyorsan terjedő felhő szolgáltatások előnyeiről és gazdaságosságáról beszélni. Ugyanakkor az egyéni felhasználók, és a felhő szolgáltatásokat igénybe vevő cégek sok esetben elfelejtik az egyszerűség és gazdaságosság miatt igénybe vett szolgáltatásoknál az így kötött kompromisszumokat is értékelni. Ahogy mind nagyobb tömegben veszünk igénybe ilyen kihelyezett szolgáltatásokat, célszerű elsősorban meghatározni az igénybe vett szolgáltatás típusát, majd pedig azokat az adatvédelmi kockázatokat, ami a cégünket érheti.

A számítási felhő (cloud computing) elnevezés az informatikában alkalmazott rajzjelekből származik, amelyben felhő jelölte azokat a hálózatokat, amelyeknek a belső felépítése lényegtelen, kizárólag az input és output rendelkezik jelentőséggel, és ily módon a felhő szolgáltatások lényegében kiszervezett informatikai szolgáltatások.

Egy outsourcing szerződés legfontosabb eleme a szolgáltatási szint megállapodás (Service Level Agreement, SLA), amelyben kikötésre kerül minden lényeges körülmény: rendelkezésre állási mutató, hibajavítási idő, válaszidő, kötbér, stb, melyek a felhő alapú szolgáltatások megrendelésénél is jelentős szerepet játszanak. [9]

A szolgáltatások típusai

A felhőszolgáltatások több csoportra bonthatóak a nyújtott szolgáltatás jellege alapján, amelyek mindegyikét XaaS, mint szolgáltatás (something as a service) néven illetjük. Így beszélhetünk: infrastruktúra szolgáltatásról (IaaS- infrastructure as a service), platform szolgáltatásról (PaaS - platform as a service) és szoftver szolgáltatásról (SaaS - software as a service). Ezen fő kategóriák mellett egyéb elemek is előfordulnak, például a Salesforce által használt fejlesztés, mint szolgáltatás (DaaS - development as a service).

A lehetséges biztonsági problémák értékelésénél a jelen cikkben bemutatott szempontok mérlegelésén és vizsgálatán túl célszerű a felhőbiztonság kérdéseit vizsgáló szervezet, a Cloud Security Alliance ajánlásait is tanulmányozni.

Minden esetben, mikor egy felhő alapú szolgáltatást veszünk igénybe, elsőként vizsgálni kell, hogy az adataink fizikailag hol kerülnek tárolásra. Az említett ajánlások a biztonság minden területére kiterjednek, így az adatok elhelyezésére is, ugyanis sem jogilag, sem gyakorlati, sem technikai szempontból nem mindegy, hogy az adatok fizikailag hol, melyik országban, melyik földrészen helyezkednek el. [10]

Általánosságban elmondható, hogy egy országban, ahol van törvény az adatvédelemről, az adatvédelmi törvények megkülönböztetnek adatkezelőt és adatfeldolgozót, és a felhőszolgáltatás jellege határozza meg azt, hogy a szolgáltatóra melyik minősítés vonatkozik.

Az adatvédelem, az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire vonatkozik.

9 http://doktori-iskola.law.pte.hu/files/tiny_mce/File/Vedes/szadeczky/ertekezes_szadeczky_nyilv.pdf

10 http://www.bitport.hu/biztonsag/meg-mindig-sok-a-kerdes-a-cloud-szolgaltatasok-biztonsaga-koeruel

Az adatvédelemről Magyarországon az információs önrendelkezési jogról és az információszabadságról szóló **2011. évi CXII. törvény** rendelkezik. Törvényünk az alábbi definíciók mentén határozza meg az adatkezelő, adatkezelés, adatfeldolgozó és adatfeldolgozás fogalmát:

- ***adatkezelő:*** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;
- ***adatkezelés:*** az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;
- ***adatfeldolgozó:*** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi;
- ***adatfeldolgozás:*** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik;

Angolszász nyelvterületen az adatvédelemre a privacy kifejezést használják. A privacy jelentésébe beletartozik, hogy az adatalany meghatározhatja, hogy mely adataik juthatnak mások tudomására, meghatározhatja, hogy személyiségének mely jellemzőihez ki férhet hozzá és egyben egy állapotot is jelöl, amelyben az adatalany személyes adataihoz, gondolataihoz való hozzáférés korlátozott.[11] Az adatbiztonság szűkebb értelmezésében technikai adatvédelem, tehát a jogi úton történő magánszféra-védelem műszaki-technikai megvalósítása. A törvény és az irányelvek értelmében az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.

11 http://www.bitport.hu/vezinfo/mire-kell-figyelni-egy-cloud-szerzodesben

Mi alapján határozható meg az alkalmazandó jog?

Az egyik fő kérdés a felhő szolgáltatással kapcsolatban a felek közti szerződéses viszonyra alkalmazandó jog kérdése. Ha a szolgáltató és a felhasználó azonos országból származik, ez a probléma általában nem áll fenn, más esetben a szolgáltatók gyakran élnek a jogválasztás lehetőségével, és a szerződésben kikötik, mely ország jogát kívánják alkalmazni. Tekintettel arra, hogy a felhő szolgáltatások megrendelésére kötött szolgáltatási szerződés is egy kötelmi jogviszony, a szolgáltatónak jogában áll ezt meghatározni.

Jogválasztás hiánya esetén azonban a szolgáltatás jellegétől függően, a tárolt adatok fajtájából - például személyes adat, szellemi tulajdon - adódóan is más-más jog alkalmazása merülhet fel. Az ebből felmerülő jogviták rendezése még kérdéses, egyelőre elméleti síkon lehet csak megoldani.[12]

Fontos vizsgálni továbbá a felhő szolgáltatókkal kötött szerződések esetén a kárfelelősség kérdését[13]. A szétszórt infrastruktúra, a többtényezős műszaki összetétel miatt a szolgáltatók az esetek többségében minimális felelősséget vállalnak a szolgáltatás zavartalan és hibátlan működéséért, az esetleges károkért pedig legtöbbször kizárják felelősségüket, vagy pedig minimális kötbér, illetve a havidíjból adott engedmény útján rendezik a kérdést.

A személyes adatok átadása, védelme, a hozzáférés kérdése

Az Európai Uniós irányelvek közül a személyes adatok védelmére személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló a **95/46/EK**[14] irányelv és az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló **2002/58/EK**[15] irányelv vonatkozik.

Az Uniós irányelvek értelmében kizárólag abban az esetben adhatók át az Európai Unió területén keletkezett, átadott és feldolgozott adatok másik szolgáltatónak tárolásra, kezelésre, ha a nem Európai Unión belül letelepült cég elfogadja, és biztosítja az Uniós irányelvben megfogalmazott követelményeket. Ennek okai keresendőek egyrészt az Európai Unióban jellemző differenciált és szigorú jogi szabályozásban, valamint az gazdasági szereplők adatainak védelméhez és átláthatóságához fűződő komoly gazdasági érdekekben.

Példának okáért, a Magyarországon hatályos számviteli szabályozás szerint, a számvitelben, így a társaságok gazdasági nyilvántartásaiban, könyveiben foglalt adatoknak a valóságban megtalálhatónak, bizonyíthatónak kell lennie. A hazai szabályozásból csak levezethető, más, nyugat-európai országokban a jogi szabályozás egyértelműen kimondja, hogy az informatikai rendszerekben tárolt adatok biztonsága nélkül ez nem teljesülhet.

A számviteli információk informatikai biztonságára a hazai elfogadott gyakorlatok között megtalálható, hogy a könyvvizsgálói ellenőrzésnek a részét képezi az informatikai biztonsági ellenőrzés is.

A könyvvizsgáló szempontjából az informatikai rendszerek feletti ellenőrzések akkor hatékonyak, ha azok megőrzik a rendszerek által feldolgozott információk sértetlenségét és az adatok biztonságát.

Az általános informatikai ellenőrzések az alábbiak ellenőrzését foglalják magukban:

- adatközpont és hálózati működés;
- rendszerszoftverek beszerzése, módosítása és karbantartása;
- hozzáférés-biztonság;
- alkalmazásrendszerek beszerzése, fejlesztése és karbantartása.

12 http://www.dataprivacy.hu/archives/891
13 http://www.bitport.hu/vezinfo/mire-kell-figyelni-egy-cloud-szerzodesben
14 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:hu:HTML
15 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:hu:HTML

Az Amerikai Egyesült Államokban a legszigorúbb az informatikai biztonsági kontroll, melyet elsősorban a Sarbanes-Oxley Act (SOX) követel meg a befektetők védelmében. Ez kimondja, hogy az amerikai tőzsdén jegyzett cégek adatainak nyilvánosnak kell lenniük. Ide tartozik továbbá, hogy az amerikai Safe Harbor Act úgy rendelkezik, hogy az adatkezelést mint szolgáltatást végző, az amerikai tőzsdén jegyzett cégeknek biztosítaniuk kell az EU Adatvédelmi irányelve szerinti adatbiztonsági előírásokat, ha a felhasználók között adott esetben Európai Uniós állampolgárok is lehetnek.

Az adatvédelmi kérdések kapcsán szükséges beszélnünk a személyes adatok megismerhetőségéről, és az egyes országokban hatályos különös szabályokról, így az Egyesült Államokban hatályos jogról. Az Egyesült Államokban a 2001-es terrortámadások megismétlődésének elkerülése érdekében fogadták el a Patriot Act-et, amely többek között lehetővé teszi az adatok kiadását, amennyiben azok tárolása amerikai közreműködéssel történik. Tehát akkor is lehetővé válik az erőszakos kiszolgáltatás, ha ugyan az adatok nem az USA területén vannak, de a szolgáltatásban amerikai cég is részt vesz.

A törvény kiterjesztését, és az adatok feletti rendelkezést célozza a jelenleg tárgyalás alatt lévő CISPA (Cyber Intelligence Sharing and Protection Act) törvény is. A CISPA célja az, hogy a cégek megosszák egymással és az amerikai kormánnyal a kiberfenyegetéssel kapcsolatos információikat. Ez adott esetben lehetővé tenné a cégek számára, hogy mindenféle következmény nélkül felhasználói adatokat cseréljenek a kormánnyal és egymással.

Biztonsági kockázatok

A biztonsági kihívások között első helyen szerepel a felhőszolgáltatások tekintetében a szolgáltatóhoz való kötődés. Ez azt jelenti, hogy a felhőben jelenleg alkalmazott rendszerek és szolgáltatások nem szabványosak, nem teszik lehetővé az átjárhatóságot. Amíg a belépéskori adatbevitel egyszerű és a szolgáltató által támogatott, addig a szolgáltatás lemondása után az adatok exportálása rendkívül nehézkes.

Ez a probléma nemcsak szolgáltató önkéntes váltásakor léphet fel, hanem a szolgáltató csődje esetén is, valamint akkor, ha jogsértés miatt leállítják a szervereket. Nemrégiben nagy port kavart, mikor a MegaUpload fájl feltöltő és megosztó oldalt a hatóságok lekapcsolták, és tulajdonosát letartóztatták. Azonban azokkal a következményekkel és kérdésekkel senki nem számolt, hogy ilyen esetben mi lesz a sorsa annak a közel 60 millió embernek, akiknek az adatait, tartalmait tárolták a lekapcsolt közel 1100 szerveren. Ilyen esetekben könnyen számolhatunk a teljes adatbázisunk elvesztésével, és hiába tisztázott a kárfelelősség kérdése, ha a szolgáltató a fent írt okok miatt nincs abban a helyzetben, hogy a kárunkat megtérítse.

További kockázati elem a nem-megfelelőségből. A rendszerek megfelelőségét a különböző jogszabályi és szabványi megfelelőségek érdekében tanúsítani szükséges, amelyre a felhő nem biztosít lehetőséget. A szolgáltató számára jelenleg túlzott költséget jelentene az audit és a keresleti piacon nincsen rákényszerítve a nagyobb fokú együttműködésre az ügyféllel, jogilag nincs kötelezve az ilyen ellenőrzés lefolytatására.

Az adatok védelme

Amikor felhőről beszélünk, megváltozik a fizikai biztonság értelme, ugyanis a felhő nem működik virtualizáció nélkül. A virtualizáció adja a rendszer stabilitását, könnyű konfigurálhatóságát, mindazt, ami a felhő szolgáltatásokat vonzóvá teszik. A felhőben, legyen az privát vagy publikus, meg kell oldani az adatokhoz való hozzáférés kontrollálását. A meghibásodás ellen, a folyamatos rendelkezésre állás és az SLA szerinti szolgáltatási színvonal biztosítása érdekében megoldásként a rendszereket legtöbb esetben megtöbbszörözik. Ez a feladat a felhő rendszerek használata esetén

magától értetődő, sőt a szolgáltatói szerződés tartalmazhatja is a tartalék rendszerek számát, az adatok esetleg többszörözését, a szolgáltatási szerződésben foglalt kötelezettségek teljesítése érdekében. A tartalék rendszerek csak akkor működhetnek megfelelően, ha az adatok folyamatosan replikálódnak, és a frissítési gyakoriságnak megfelelően mindig egyformák. Az így elhelyezett adatok helyének meg kell felelnie az érvényes adatvédelmi szabályozásnak. A replikált adatok tehát csak azokon a földrészeken helyezhetők el, amelyeket az adatvédelmi törvény nem tilt. Ez gyakorlatilag használhatatlanná teszi a legnagyobb biztonságot adó, különböző földrészekre szétválasztott replikációt.

Mi történik, ha lemondom?

További érdekes kérdés, hogy mi történik a szolgáltatás lemondásakor. A felhő szolgáltatást nyújtó, vagy a technológiát felhasználó szolgáltatást nyújtók az adat törlés kérésekor logikai törlést alkalmaznak, ami a felhasználóban azt a tévképzetet kelti, hogy az adatai törlődtek a szolgáltatást nyújtó cég rendszeréből. Ugyanakkor a valóságban mindaddig megtalálható az átadott személyes adatunk, míg azt felül nem írják a világ valamely pontján elhelyezett szerveren. A felhasználó nem tudja ellenőrizni, hogy adatai valóban törlésre kerültek-e, el kell fogadnia, hogy az adatai felett nem rendelkezik teljes ellenőrzési és rendelkezési joggal, nem tudja ellenőrizni a szolgáltató szerződésben foglalt kötelezettségeinek teljesítését.

RSA Konferencia 2012 – San Francisco[16]

2012. márciusában rendezték meg az RSA konferenciát. Ebben az évben a konferencián a biztonsági szakemberektől hallott információk talán az elmúlt tíz évhez képest most még fontosabbak és még használhatóbbak voltak - vélekedett a magazin szerkesztője. A konferencián elhangzottakból két cikket emeltünk ki, amelyek jó perspektívát adnak arról, hogy milyen irányba vagy irányokba indulhat el az informatika, a felvetett témák vonatkozásában.

Alkalmazás biztonság

Nem kérdéses, hogy napjaink egyik legnagyobb problémája az alkalmazásbiztonságban a képzett alkalmazásbiztonsági szakemberek hiánya. Rengeteg a területet érintő álláshirdetés. Egy friss LinkedIn közvéleménykutatás is újabb bizonyítékkal szolgál, hogy a munkaerő bérlés a legnagyobb kérdés.

A probléma oka, hogy lényegében egy sikeres alkalmazásbiztonsági program számos szempontból megkövetel némi „speciális szakértelmet”. Ez magában foglalja a sebezhetőségi értékeléseket, behatolási teszteket, forráskód elemzéseket, webalkalmazás-tűzfalak ismeretét, fenyegetés-modellezési, szoftverfejlesztési és egyéb minőségbiztosítási ismereteket is.

Képzett alkalmazásbiztonsági emberekre van szükség, függetlenül attól, milyen technológiájú terméket vásárol egy szervezet, vagy milyen folyamatokat fogadnak el.

Nincs fegyver a szoftver biztonságot fenyegető fenevad megölésére és nagy valószínűséggel nem is lesz. A technológia részéről csak annyi várható el, hogy az emberek munkáját hatékonyabbá és a folyamatokat következetessé formálja. Tehát meg kell tanítani az embereket az alkalmazásbiztonsági termékek használatára és az ezekbe beépített folyamatok kezelésére, irányítására.

A munkaerő hiányból fakadó problémával akkor szembesülünk leginkább, amikor megpróbáljuk megbecsülni az alkalmazásbiztonsági ipar jövőbeni emberszükségletét. Az OWASP[17] egy hasznos módja annak, hogy megszervezze a három, fő alkalmazásbiztonsági munkaköri feladatokat.

Építők (Builders): azok, akik biztonsági kódot fejlesztenek.

Megszakítók (Breakers): azok, akik sérülékenységeket keresnek a megírt kódban.

Védelmezők (Defenders): azok, akik elhárítják az aktív weboldalak ellen irányuló támadásokat.

Építők (Builders):

Gary McGraw (CTO, Cigital) szerint durván az összes programozó 1%-a lehet biztonsági specialista, vagy „Építő” a mi esetünkben. Gary az 1%-os eredményhez a nagyvállalatok tucatnyi biztonsági programjainak, valamint azok képességeinek mérésével jutott el.

A világon jelenleg körülbelül 17 millió programozó van, ez azt jelenti, hogy az 1% az 170 ezer embert jelent. A becslések szerint ebből a 170 ezer emberből ma csak 1-3% tevékenykedik aktívan.

Megszakítók (Breakers)

Az 550 millió működő weboldalból minimálisan 1,2 millió olyan „fontos” weboldal létezik (SSL támogatással), amelyeket a sérülékenységek szempontjából folyamatosan és átfogóan kell értékelni.

16 RSA Konferencia - San Francisco

17 Open Web Application Security Project – https://www.owasp.org/index.php/Main_Page

A „megszakítók” esetében 100 internetes oldal/1 fő arányt alkalmazzuk. Ez az arány a WhiteHat Security saját mérésén alapszik, amely az elmúlt 8 év alatt több mint 5000 weboldalt magába foglaló értékeléséből került kiszámításra.

Ezen értékelések minősége egyenértékű vagy jobb, mint bármely más nagy tanácsadó cégé. Ezeket figyelembe véve matematikailag 12000 fő „megszakítóra” van szükség, amelyekből jelenleg talán 2000 fő áll rendelkezésre. A „megszakítók” létszáma könnyedén növelhető lenne, ha valamilyen módon megbecsülhetnénk az általuk vizsgálandó környezetek számát.

Védelmezők (Defenders)

A védelmezők számának megbecsülése meglehetősen nehéz feladat, de számuk legalább tízezerre tehető. A védendő weboldalak eszközeinek hatalmas számát figyelembe véve, valakinek meg kell bizonyosodnia az 1 milliárd online felhasználó megfelelő magatartásáról, valamint az általuk generált nagy mennyiségű adatforgalmat valakinek figyelemmel kell követnie.

Lehetséges, hogy mindenki monitoroz egy IDS / IPS képernyőt, de rendkívül nehéz egy olyan számot találni, amelyből ezt le lehetne vezetni, vagy amiből ezt konvertálni lehetne.

Összességében a három területre, durván 200 ezer képzett alkalmazásbiztonsági szakember szükségességét jelenti. Ez egy „csillagászati” szám, amely a valóban rendelkezésre álló szakemberek számának többszöröse.

Az elmúlt néhány évben a nagy szoftvergyártók, mint például a Google, a Microsoft, az Adobe, a Salesforce, már a rendelkezésre álló alkalmazásbiztonsági szakemberek nagy részét beolvasztották saját szervezeteikbe. A munkanélküliségi ráta gyakorlatilag nulla azok számára, akik a fent említett három kategóriába sorolhatóak és rendelkeznek a megfelelő szakképzettséggel.

A szakértői tudás hiányából kifolyólag a szervezetek rengeteget költenek alkalmazásbiztonsági technológia vásárlására, de programjaik továbbra is hibásak, valamint weboldalaik továbbra is feltörhetőek maradnak. A rengeteg elköltött pénz így hiábavaló és csak hamis biztonságérzet kelt.

Az online üzleteket bonyolító cégek, különösen azok, melyek érzékelik az alkalmazásbiztonsági labor hiányát ahhoz, hogy kulcsfontosságú döntést hozzanak, vagy:

- Folytatják a versenyt a szakképzett munkaerő után, akiket folyamatosan kell alkalmazni, továbbképezni, valamint megpróbálni átképezni a saját alkalmazás biztonsággal foglalkozó csapataikat, vagy
- Kiszervezik azokat a nehéz emberfüggő és szakképzettséget kívánó folyamatokat, amelyekkel rendelkeznek, legfőképpen biztonsággal foglalkozó cégek részére. Így a szervezetek üzleti döntéseket hozhatnak a személyzet skálázható problémájának másra hárításáról.

A szervezetek többségének, melyek nem rendelkeznek elegendő tőkével vagy olyan presztízzsel mint például a Google, a Microsoft és az Adobe, azok számára a „B.” lehetőség marad az egyetlen elérhető megoldás.

A biztonsággal foglalkozó cégek alapvető üzleti tevékenységéből kifolyólag, technikailag jobb helyzetben vannak a tehetséges alkalmazásbiztonsági szakemberek alkalmazása, oktatása és megtartása tekintetében, mint egy átlagos, nem alapvetően a biztonsággal foglalkozó cég. Azért mondjuk, hogy „technikailag”, mert így a biztonsági cégek lehetnének azok, akik megoldhatnák a szakképzett munkaerő hiányának problémáját, de ezt kevesen vállalják fel.

A lényeg az, hogy ha egy szervezet legnagyobb problémája a képzett alkalmazásbiztonsági szakemberek hiánya, akkor létfontosságú, hogy figyelembe vegye az iparág dinamikáját és fel kell mérje, hogy adott alkalmazások és/vagy rendszerek megfelelően biztonságos fejlesztéséhez/üzemeltetéséhez mennyi szakképzett munkaerőre van szüksége, illetve hogy azt milyen forrásból tudja biztosítani.

Az okostelefonok és mobil számítástechnika biztonságának fejlődési irányzatai

Meglehetősen érdekes időket élünk, ami az okostelefonok és a mobil számítástechnika területét illeti. Ezek eggyé válnak és egy „tökéletes vihart" alkotnak a mobil eszközöket használók, a bűnözők, valamint maga a technológia egymásra gyakorolt hatása által.

A technológia, az ár, a képességek és az okostelefonok népszerűsége együttesen gerjesztenek egy gyorsan növekvő piacot. Ugyanakkor ezek a sokrétű, sok funkcióval rendelkező népszerű eszközök a bűnözők figyelmét is magukra vonták, mivel nagyon értékes adatokat szerezhetnek ezen eszközök támadásával.

A jelenlegi irányzatok

Az okostelefonok nagyméretű, drága és nem túl vonzó megjelenésű eszközként kezdték a pályafutásukat. Aztán méretük csökkent, egyre stílusosabb és szebb megjelenésűek lettek, hordozhatóbbá váltak, mint nagyméretű elődeik. Ez teszi őket egyre elfogadottabbá és közkedveltebbé a felhasználók számára. Ugyanakkor ezen tulajdonságaik által válnak sebezhetővé mind biztonsági szempontból, mind fizikailag, ide értve az eszközök fizikai amortizálódását vagy azok véletlen elvesztését, illetve eltulajdonítását.

A legfontosabb tényező az okostelefonok elterjedésében az ár. A meglévő technológia egyre olcsóbb lett, egészen addig, amíg a nagyon olcsó okostelefonok versenyképesek lettek a legtöbb hagyományos mobiltelefonnal.

Láttuk, ahogy egyre gyorsabb kétmagos processzorok és egyre több és több memória kerül a telefonokba és az idén tanúi lehetünk annak is, hogy az újabb felső kategóriás eszközökben megjelennek a négymagos processzorok.

A mobiltelefonok képességeinek fejlődése túlmutat a puszta számítási kapacitás növelésén, újabb képességeket kapnak. Hamarosan láthatunk Near-Field Communications (NFC)[18] képességű telefonokat, amelyek a „tap and go"[19] fizetési rendszer szerint működnek, ezzel kiváltva egyes bank- és hitelkártya tranzakciókat.

Az okostelefonok zseb-szuperszámítógépekké válnak.

Egy másik fontos tényezője az okostelefonok és a táblagépek egyre nagyobb körben történő elterjedésének a világában, a jelenleg is több ezernyi olcsó - akár ingyenes - alkalmazás, melyek száma rohamosan nő. Vegyük csak például a játékokat, mint pl. az Angry Birds és a Words with Friends, melyek nagyon népszerűek és elterjedtek, ezzel is segítve az okostelefonok terjedését a fiatalok és az idősebbek körében egyaránt.

Nem csak a vásárlói piacon van kereslet ezen eszközökre. Az elmúlt néhány évben gyorsan terjed az üzleti életben is a BYOD, más néven Bring Your Own Device[20] használatával.

Részben az okostelefonok nagy számítási kapacitásai miatt, részben mivel a telefonok a gyártók által telepített nem kívánt alkalmazásokat tartalmaznak és részben azért, mert a közösségben nagy számban vannak jelen a megszállott buherátorok, megjelentek az alulról szerveződő projektek az okostelefonok szoftveres módosítására.

18 kis hatósugáron belül működő vezeték nélküli adatátviteli technológia
19 érintésmentes fizetést lehetővé tévő bankkártyás szolgáltatás
20 A legújabb trend szerint az alkalmazottak beviszik saját mobil eszközeiket a munkahelyekre, amelyekkel aztán különféle vállalat erőforrásokhoz csatlakoznak, mint például e-mail, fájl szerverek, és az adatbázisok. - http://antivirus.blog.hu/2012/04/12/a_byod_egyaltalan_nem_lol

A felhasználók jailbreak-elni[21] tudják az eszközeiket, vagy visszavonni adott alkalmazások korlátozásait az olyan eszközökön, amelyek iOS-t futtatnak. A folyamtok root-olásával a felhasználók képesek rendszer szintű jogosultságot szerezni a mobil eszközökön, táblagépeken, számítógépeken, más szavakkal modding-olni vagyis módosítani az operációs rendszert, custom modified firmware (mod roms) létrehozásával. A jailbreaking és a rooting szavak furán hathatnak, de teljesen legális eljárásnak számítanak.

A sötét oldal irányzatai

A kártékony kódot tartalmazó programok írói is felfigyeltek a mobil eszközök népszerűségének növekedésére. Kártékony kódot tartalmazó program majdnem minden platformon és operációs rendszeren létezik, de korábban csak limitált hatásuk volt.

Kártékony kódot tartalmazó programok képesek ellopni a telefonon tárolt személyes információkat (pl. a banki adatokat), vagy emelt díjas SMS-ek küldésével okozhatnak kárt. Egyes esetekben a bűnözők fognak egy népszerű játékot vagy alkalmazást, trójai programot csempésznek bele, majd újracsomagolják és ingyenesen vagy alacsony áron kínálják letöltésre a piactereken. A tendencia az mutatja, hogy az ilyen esetek száma egyre nő.

A bűnözők tevékenysége nem merül ki a kártékony kódot tartalmazó programok írásában. Az eszközöket el lehet lopni, de egyéb más módon is hozzájuk lehet férni. A mobil eszközökhöz gyakran a szabványos micro USB porton keresztül férnek hozzá, hogy ellopják a személyes adatokat, vagy egyéb káros kódot fecskendezzenek be.

Az egyik legérdekesebb támadási forma a QR (Quick Response) kódokon keresztül történik. Ezek a kódok 2 dimenziós vonalkódok, amelyek Európában és Ázsiában terjedtek el leginkább, gyakran szerepelnek újságok vagy TV műsorok hirdetéseiben.

Történtek már biztonsági incidensek káros tartalmú QR kódokon keresztül, amelyek hirdetésekben szerepeltek, amelyeket a valódi QR kódok helyett használtak. Ezeket az eseteket nagyon nehéz felismerni. Volt már precedens arra is, hogy SMS/MMS vagy email üzenet formájában érkezett a hamis QR kód az áldozat telefonjára.

A védekezés

Szerencsére komoly erőfeszítések zajlanak ezen fenyegetettségek csökkentésre. A szoftvergyártó cégek a biztonsági megoldások széles skáláját alkalmazzák termékeikben. Kutatások zajlanak virtualizált, izolált felhasználói fiókokkal, hogy megvédjék az alkalmazottak telefonján tárolt vállalati adatokat. Egyes nagyvállalati szoftver gyártók végponti ellenőrző rendszereket használnak arra, hogy távolról lehessen menedzselni a telefonokat, ezzel biztosítva az eszköz integritását.

Az alkalmazások piacterei egyre több óvintézkedést tesznek, hogy a megvásárolható vagy ingyen letölthető alkalmazások közé ne kerülhessenek be veszélyes, illetve káros programok. A Google a „Bouncer” nevű szkennerével elkezdte megvizsgálni a többezernyi alkalmazást, amit a piacterén elérhetővé tett, az Apple pedig óvatos és korlátozó politikát folytat a letölthető programokkal kapcsolatban.

21 tiltott funkciókat elérhetővé tenni, vagy egyes előre beépített funkciókat működésképtelenné tenni

Következtetések

Többet kell tenni, hogy megvédjük az okostelefonok felhasználóit saját maguktól. Tudatosítani kell bennük, hogy ezek nem csak egyszerű telefonok, hanem nagy teljesítményű számítógépek. Tudniuk kell megvédeni magukat a jelenlegi eszközök felhasználásával. Meg kell érteniük a kockázatokat és ismerniük kell az eszközökön található adatok értékét.

A felhasználóknak tudniuk kell, hogy kerüljék el a veszélyhelyzeteket, valamint fel kell hívni figyelmüket arra, hogy óvintézkedéseket kell tenniük. Van amit oktatással, van amit alkalmazásokkal el lehet érni, továbbá van amit pusztán fizikai elővigyázatosságból magának a felhasználónak kell megtennie.

Talán első és legfontosabb, hogy ne töltsenek le alkalmazásokat nem megbízható forrásból! Egy ingyenes játék csábító lehet a gyereknek, de egy nem várt kellemetlen meglepetés lehet a szülőnek. De még a megbízható piactérből származó alkalmazásokkal is óvatosan kell eljárni.

Az anti-vírus szoftverek ajánlottak, de nem árt felkészülni a legrosszabbakra is, és telepíteni olyan alkalmazásokat, melyek által az eszköz távolról is elérhető és akár nyomon követhető. Több eset is ismertté vált, amikor az elveszett, ellopott okostelefonok helyzetét a tulajdonos távolról meghatározta és nyomon követte a GPS programok segítségével.

QR kód szkennelése közben a vonalkód olvasó mindig megkérdezi a felhasználót, hogy mit tegyen az adattal a felhasználás előtt. Soha ne olvassunk le veszélyesnek látszó vagy láthatóan módosított kódot!

A biztonsági mentések nagyon fontosak, hogy elkerüljük az adatvesztést. Akkor lehet rá szükség, ha a telefon elveszik, ellopták, és szükséges hogy mindent töröljenek róla.

Érdekes módon azok, akik jailbreak-elik, root-olják vagy modding-olják a telefonjukat, kevésbé vannak kitéve a támadás kockázatának. A szabadon elérhető eszközök segítségével módosított telefonok nem kevésbé sérülékenyek, de azoknak, akiknek root jogosultságuk van a telefonhoz, jobb biztonsági eszközöket tudnak telepíteni eszközeikre. Ezenkívül nincs olyan támadó, aki speciálisan ezeket a felhasználókat venné célba. Azonban ez (jailbreak, root vagy modding) nem ajánlott egy átlagos felhasználónak, akinek nincs meg a szükséges technológiai tudása, hogy használja ezen programokat.

A vállalatoknak is fel kell készülniük arra, hogy biztonsági alkalmazásokat és eszközöket telepítsenek az alkalmazottak telefonjaira függetlenül attól, hogy az saját vagy céges eszköz, mivel az adatok a vállalat tulajdonában vannak. Fel kell ismerni, hogy az okostelefonok biztonsága nem elválasztható a felhasználótól. A különböző embereknek különböző szintű igényeik, képességeik és eszközeik vannak.

Az eszközök növekvő kapacitása és képességei, sokoldalúsága egyre népszerűbbé teszi őket a fogyasztók számára. Ezzel együtt jár a megnövekedett kockázat is, illetve az igény, a felhasználók védelmének növelésére.

Forrás: http://www.net-security.org/dl/insecure/INSECURE-Mag-RSA2012.pdf

A VirusBuster Kft. összefoglalója 2012 első negyedévének IT biztonsági trendjeiről

Mi történt az idei év első három hónapjában az informatikai biztonság területén? Beszámolónkban a trend értékű híreket, adatokat igyekszünk sorra venni, s a VirusBuster Kft. víruslaboratóriumának észlelései alapján áttekintést nyújtunk a 2012. január-március időszak leggyakoribb számítógépes károkozóiról, illetve azok legjelentősebb webes forrásairól is.

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

Való világveszedelem

Idén érkezett hetedik kiadásához a davosi tanácskozásairól ismert Világgazdasági Fórum évente megjelenő kiadványa, a *Globális veszélyek jelentés (Global Risks Report)*. Miért említjük ezt? Nos, azért, mert a világ mértékadó üzleti-politikai köreinek véleményét feltérképező tanulmány az előttünk álló évtized legsúlyosabb fenyegetései közé sorolja az online biztonsági kockázatokat.

A szerkesztők évről évre ötvenes, majd ezen belül ötös toplistát állítanak össze az emberiség, pontosabban a világgazdaság közeljövőjét leginkább veszélyeztető tényezőkből. A kiberbiztonság ügye – a jelentés történetében idén először – bekerült a vezető szakembereket legjobban aggasztó öt kockázat közé.

Pontosítsunk: a felmérés két tengely mentén rangsorolja a veszélyforrásokat. Az egyiken azt mérik, milyen hatással járna – mekkora kárt okozna –, ha beteljesülne egy adott fenyegetés. A másikon azt: mennyire valószínű, hogy a baj bekövetkezik. Ez utóbbi skálán került a negyedik helyre az IT biztonság témája. A tanulmány szerint a következő tíz évben a következő problémáktól kell leginkább tartania az emberiségnek:

- súlyos jövedelemkülönbségek,
- krónikus pénzügyi egyensúlyzavarok,
- az üvegházhatású gázok kibocsátásának növekedése,
- kibertámadások,
- válságos vízhiány.

„Mindennapi életfeltételeinket biztosító kritikus infrastruktúránk mindinkább sokszorosan összeköttetésben álló online rendszerekre támaszkodik – állapítják meg a szerkesztők. – Korábban súlyos geopolitikai vagy üzleti kárt csak jelentős erőforrások megmozgatásával lehetett okozni. Ma viszont megfelelően képzett tettesek számítógép-hálózatokon keresztül névtelenül, a távolból is elérhetik ezt. Mind több hatalom kerül át a kézzelfoghatóból a virtuális szférába. A digitális világ egészsége, működőképessége ilyen körülmények között csak új szemlélettel, új módszerekkel őrizhető meg.”

A tanulmány hangsúlyozza: az online biztonság az egész társadalom javát szolgálja; ám miközben az előnyöket mindannyian élvezzük, a költségek az egyes emberekre vagy cégekre hárulnak. Ha biztonsági szoftvert veszünk, a saját érdekünkben tesszük – nem gondolunk arra, hogy ezzel mások spam- és támadásvédelméhez is hozzájárulunk. Az ország vagy a világ kritikus infrastruktúrájának védelme pedig végképp nem szokott szempont lenni a vásárlási döntésben.

Új mechanizmusokat kell kidolgozni, amelyek a magánszektort is érdekeltté teszik a sérülékenységek feltárásában, kiaknázásuk megelőzésében. Egy stabilan ellenálló, szilárd rendszer kiépítése olyan beruházás-igényes feladat, amely csak újszerű módon, valamennyi szereplő együttműködésével oldható meg. A jelentés afféle Murphy-törvényként leszögezi: mielőtt harcba szállnánk a sötét oldallal, tudomásul kell vennünk két axiómát.

1. Nincs az a szoftver-vezérelt eszköz, amelyet ne lehetne olyasmire kényszeríteni, ami az alkotóknak soha nem állt szándékában.
2. Ha egy eszköz hálózatra kapcsolódik, akármilyen legyen is a hálózat vagy a kapcsolat, biztos, hogy az eszközt valaki a távolból fel tudja törni. Sok ilyen behatolásra a mai napig nem derült fény.

Az IT biztonságnak szentelt fejezet végén a Világgazdasági Fórum szakemberei négy, ugyancsak elgondolkodtató kérdéssel fordulnak az üzleti és politikai döntéshozókhoz:

- Milyen lépésekkel javítható az információcsere, milyen óvintézkedésekkel mérsékelhetjük a kiberfenyegetést az előttünk álló évtizedben?
- Hogyan ösztönözhetjük az üzleti és a közszférát a kritikus IT infrastruktúra ellenállóbbá, stabilabbá tételét szolgáló beruházásokra?
- Hogyan élhetünk a nyílt forráskódú szoftverben rejlő innovációs előnyökkel úgy, hogy közben tudjuk: lesznek, akik rosszindulatú céllal nyúlnak bele a kódba?
- Vajon valóban szükséges, szerves része-e behálózott világunknak a névtelenség, az anonimitás?

A válaszok nem várathatnak sokáig magukra. A kibertámadások évről évre világszerte több százmilliárd dollárnyi kárt okoznak a szervezeteknek és magánszemélyeknek. A brit NCC csoport február elején közzétett kutatási eredményei szerint tavaly a legtöbb hackerakciót – az összes támadás 40%-át – az Egyesült Államokból és Kínából indították, s ezek összesen több mint 44 milliárd dollár kárt okoztak a világgazdaságban. Hollandia, Franciaország, Dánia és Németország követi a két éllovast a sorban. Ezekből az országokból összesen csaknem 200 millió támadás indult ki – a számított kárérték 16 milliárd dollár. Mint februárban megtudhattuk, hazánkban is 900 ezer körül jár azoknak a száma, akik elszenvedtek már valamilyen számítógépes bűncselekményt. A közvetlen anyagi kár 7 milliárd forint, s 14 milliárd forintra becsülik a kiesett idő értékét. És persze a világon mindenhol vannak, lehetnek pénzben ki nem fejezhető károk is...

Nem csoda hát, hogy 2002-es megalakulása óta most márciusban már ötvenedik szakmai fórumáig jutott a szakma egyik fontos hazai szervezete, a Hétpecsét Információbiztonsági Egyesület, s hogy 2008-ban a Budapesti Rendőr-főkapitányság számítógépes bűnözéssel foglalkozó alosztály létrehozására kényszerült. A negyedév végén pedig Brüsszelből érkezett a hír: az Europol keretében várhatóan jövő januárra megszervezik az Európai Kiberbűnügyi Központot (European Cybercrime Centre).

Bitbomba-riadó

A számítógépes bűnözők a magánszemélyeket, cégeket, állami és egyéb szervezeteket ostromolják anyagi haszonszerzés céljából vagy – mint jelentésünk következő fejezetében olvashatják – különféle ideológiák jegyében. Egy szinttel magasabban azonban folyik egy másik, rejtettebb támadássorozat is. Nemzetállamok indítanak kiberakciókat más államok vagy más országok cégei ellen. Ha elszigetelt incidensekből áll is, a kiberháború voltaképpen elkezdődött. Az ellenfelek próbálgatják egymást, felmérik egymás erejét.

Március végén az amerikai Szenátus illetékes szakmai bizottságának meghallgatásán *James Peery,* a Sandia National Laboratories információsrendszer-elemző központjának igazgatója így nyilatkozott: „Nem hinném, hogy a kémeket határainkon kívül tarthatjuk.

Mostani kiberháborús modellünkben olyan rendszerben gondolkodunk, amelyet nem érhet támadás... Rossz megközelítés. ... Szerintem a modellnek abból a feltételezésből kell kiindulnia, hogy az ellenség bent van a hálózatunkban. Ott van a gépeinken, és nekünk ilyen körülmények között is dolgoznunk kell." Az amerikai védelmi minisztérium 15 ezer hálózaton mintegy hétmillió számítástechnikai eszközt működtet. Egy ilyen komplex rendszert tökéletesen megvédeni gyakorlatilag lehetetlen – magyarázta hallgatóságának a szakember.

Ha állami szintű kibertámadásról kerül szó, szinte már közhelyszerűen Kína az első számú gyanúsított. Válaszul a vádakra az ázsiai nagyhatalom gyakran hangoztatta, hogy inkább maga is áldozata, mintsem szervezője az akcióknak. Az amerikai Nemzetbiztonsági Hivatal (National Security Agency) igazgatója mégis Kínára mutatott, amikor a negyedév végén az egy esztendővel korábban az RSA ellen elkövetett, nagy port kavart kiberbetörésről beszélt. (Mint emlékezetes, az RSA-tól elemelt biztonsági kóddal nem sokkal később a Lockheed Martin katonai óriás ellen kíséreltek meg támadást.) Január közepén pedig arról érkeztek hírek, hogy kínai hackerek egy trójai segítségével olyan chipkártyákat törtek fel, amelyeket számos amerikai kormányzati épület beléptető rendszerében alkalmaznak.

Ugyancsak Kínából indult ki a jelek szerint az a jól szervezett, márciusi akció, amelynek tettesei hamis Facebook oldalt nyitottak *James Stavridis* tengernagynak, a NATO európai főparancsnokának nevében. A főtisztről közismert, hogy aktívan kommunikál a közösségi hálózaton. A támadók nyilván abban bíztak, hogy az ál-oldallal lépre csalt látogatók révén további, kémkedésre felhasználható bizalmas információkhoz juthatnak.

Kiberháborút a szó tágabb értelmében persze nemcsak maguk az államok, hanem hazafiúságtól fűtött polgáraik is vívhatnak. Az arab-izraeli konfliktusnak láthattuk például az év elején effajta vetületét. Állítólagos szaúdi hackerek azzal kérkedtek, hogy izraeli site-okról mintegy 400 ezer izraeli polgár személyi adatait, köztük bankkártya-információit emelték el. Az illegális adatgyűjtés ténye beigazolódott, ám az áldozatok valós száma izraeli források szerint „csupán" 14 ezer volt. Utóbb az is felmerült, hogy esetleg nem is szaúdi csoport, hanem az Egyesült Arab Emirátusok egy Mexikóban élő ifjú állampolgára fejezte ki ily módon Izrael-ellenes érzelmeit.

Mindenesetre a zsidó állam külügyminiszter-helyettese, *Danny Ayalon* terrorcselekménynek minősítette az arab akciót, s megtorlással fenyegette az elkövetőket. Ám az első válaszcsapást ő maga szenvedte el: személyes site-ját feltörték és rövid időre egy iszlám lapra irányították át. Nem kellett sokat várni az izraeli hackertársadalom bosszújára: egy Hannibal fedőnevű kiberlovag azt állította, hogy 100 ezer arab Facebook belépőjét tette közzé.

Ahogy azt már évek óta tapasztalhattuk, az incidensek sora nyilván most is vég nélkül folytatódik majd.

Arctalan alakulat

Persze hackerkedésre nemcsak nemzeti érzület, hanem bármilyen más ideológia is indíthatja azt, aki erre hajlamos. Márciusban jelent meg a Verizon felmérése a 2011-ben elkövetett adatbetörésekről *(Data Breach Investigations Report),* melynek összeállításában az amerikai titkosszolgálat, valamint a brit, a holland és az ausztrál rendőrség is közreműködött. Az ötödik évfolyamába lépett kiadványból az derül ki, hogy a kibertámadások motivációja gyökeresen megváltozott az utóbbi esztendőben. Míg korábban az akciók többségét bűnözők követték el, anyagi haszonszerzés reményében, addig a tavalyi behatolások 58%-áért hacktivisták voltak a felelősek – vagyis olyan személyek vagy csoportok, akik politikai vagy társadalmi célokat tűztek zászlajukra. Ezzel párhuzamosan egy év alatt több mint másfélszeresére – 36-ra – bővült azoknak az országoknak a köre, ahonnan a támadások indultak. Szomorúan, bár nagyobb meglepetés nélkül vehetjük tudomásul, hogy a hackerek az esetek csaknem 70%-ában Kelet-Európából vetették ki hálójukat.

Rövid kitérőként megjegyezzük: a Verizon értékelése szerint a feldolgozott 855 betörésnek csak a 4%-a követelt nagyobb erőfeszítést az elkövetőktől. Az esetek 79%-ában, mondhatni, ölükbe hullt a zsákmány. A betörések során eltulajdonított összesen 174 millió adatrekord 97%-a könnyen, komoly anyagi ráfordítások nélkül megvédhető lett volna...

Visszatérve kiindulópontunkhoz, a Verizon-hoz hasonló eredményekre jutott a hackertevékenység indítékait kutatva az Arbor Networks is. Az utóbbi cég egy szűkebb akciófajta, az elosztott szolgáltatásmegtagadási (DDoS) támadások elkövetőit vizsgálta. Februárban közzétett tanulmányukban azt írják: 2011 előtt a DdoS támadásokat általában egyszerűen „üzleti" okból szabadították rá az áldozatra. Vagy versenytársat akartak ily módon büntetni, vagy zsarolással próbáltak pénzhez jutni. Tavaly azonban ez megváltozott. Az ideológiai motiváció került előtérbe. „Bármilyen, online jelenléttel rendelkező szervezet célkeresztbe kerülhet, profiljától és méretétől gyakorlatilag függetlenül, akár azért, amivel foglalkozik, akár azért, hogy kivel-mivel ápol – valódi vagy csak feltételezett – partneri viszonyt. Ráadásul robbanásszerűen elterjedtek, könnyen és olcsón hozzáférhetővé váltak a támadó eszközkészletek, amelyekkel szinte bárki végrehajthat egy DDoS akciót" – vélekedett *Roland Dobbins,* az Arbor Networks szakembere.

A hacktivista mozgalmak nem feltétlenül legelső, de mindenképpen legismertebb képviselője a „névtelenek" csoportja, vagyis az Anonymous, melynek sejtjei ma már az egész világot behálózzák. Természetesen az idei év sem indulhatott úgy, hogy a társaság neve ne forgott volna rendszeresen a szaksajtó lapjain.

Január mindjárt azzal kezdődött, hogy több mint két hétre elsötétült a világszerte nagyra tartott politikai elemző cég, a Stratfor webhelye. Az ok: az Anonymous még decemberben betört, 200 gigabájtnyi adatot szippantott le – állítólag többek között az ügyfelek listáját, több mint négyezer bankkártya információit és e-mailek tömegét. Az ügy különösen kényes, hiszen a Stratfor szolgáltatásait nagy bankok és vállalatok mellett az amerikai hadsereg és rendőrség is igénybe vette. A Stratfor elnézést kért az incidensért – biztonsági szakemberek szerint okkal. A vizsgálat ugyanis elemi hibákra világított rá: a cég például nem titkosította a jelszó-adatbázisát.

Február elején az Anonymous közzétett egy MP3 állományt – egy konferenciabeszélgetés felvételét, melynek során a Scotland Yard és az FBI ügynökei épp az Anonymous, illetve a hozzá tartozó LulzSec hackercsoport ügyeit vitatták meg. Nyilvánosságra hozták azt az e-mailt is, melyről azt állítják: annak a 40 – amerikai, brit, francia, holland, ír és svéd – rendőrtisztnek az adatait tartalmazza, akik részt vettek az értekezleten. Hogy a lehallgatást hogyan oldották meg, nem tudni. Miután azonban az említett üzenetben a telefonszám és a belépési kód is szerepel, még az sem kizárt, hogy egyszerűen betárcsáztak.

Pár nappal később egy jogi céghez törtek be, ahonnan – mint állították – 2,6 gigabájtnyi e-mailt emeltek el. Ebből egy adagot bizonyítékként meg is jelentettek – olyan leveleket, amelyek egy 24 iraki polgári halálos áldozatot követelő 2005-ös amerikai katonai akcióval kapcsolatosak.

Ezután nem kisebb célpontra lőttek, mint a Symantec. Egy, az Anonymous-szal kapcsolatban álló indiai csoport, a Lords of Dharmaraja állítólag megszerezte a pcAnywhere forráskódját, és 50 ezer dollárt remélt a Symantec-től annak fejében, hogy nem teszi közzé a zsákmányt. A cég azonban értesítette a rendőrséget, és a hackerek tárgyalópartnere valójában ügynök volt. A „tárgyalások" valamilyen okból kudarcba fulladtak, mire válaszul a csoport nyilvánosságra hozott egy 1,27 gigabájtos torrentet, amely szerintük nem más, mint a forráskód.

Február végén aztán lecsapott az Interpol, ha nem is Indiában. A „Leleplező hadművelet" (Operation Unmask) fedőnevű akció keretében huszonöt – 17 és 40 év közötti – feltételezett Anonymous-tagot tartóztattak le Európában és Latin-Amerikában. Tizenöt városban, negyven helyszínen összesen 250 számítástechnikai eszközt, valamint mobil telefonokat, bankkártyákat és készpénzt foglaltak le.

A bosszú nem késett soká, s az IT biztonsági szakmát, konkrétan a Panda Security céget sújtotta, amely a hacktivisták szerint segítséget nyújtott az FBI-nak. Március 6-án belerondítottak a vállalat

néhány weblapjába. A Panda nyilatkozatban sietett közölni: az érintett webszerver nem volt rajta a cég belső hálózatán, ahhoz a támadók egyáltalán nem fértek hozzá. Így sem forráskód, sem vírusadatbázis-frissítési vagy ügyféladatok nem került illetéktelen kezekbe.

Egy nap se telt el és az Anonymous már Olaszországban lépett akcióba. A Vatikán weblapjait irányították át több órán keresztül más site-ra, mint üzenetükben mondták, a katolikus egyház pedofília botrányai és a Szentszék történelmi cselekedetei miatt.

És ha valaki azt hitte, hogy Magyarország kimaradhat egy ilyen világméretű mozgalomból, hát súlyosan tévedett. Március első hétvégéjén az Anonymous az Alkotmánybíróság site-ján nemes egyszerűséggel átírta az Alaptörvény szövegét.

Arcok (és harcok) könyve

Kevés csillag emelkedett oly hirtelen oly magasra, mint a Facebook-é. Hogy milyen fontos lett felhasználói számára a világ legnépszerűbb közösségi hálózata, azt mi sem mutatja jobban, mint hogy egy februári felmérés szerint a britek nagyobb becsben tartják Facebook-jelszavukat céges számítógép-jelszavuknál. A kétezer válaszadó 34%-a adta már át másnak vállalati IT-belépőjét, ám 80%-uk úgy nyilatkozott: Facebook-azonosítóját nem mondaná meg senkinek.

Azt pedig már régóta tudjuk, hogy ha egy szolgáltatás ennyi embert vonz, akkor vonzó célponttá válik a bűnözők számára is. Alig köszöntött be az új esztendő, már szólt a riadó. Egy eredetileg bankszámla-feltörő féreg, a Ramnit indult terjedésnek a Facebook-on. Amikor a Seculert biztonsági cég megtalálta a vezérlőszervert, 45 ezer, a közösségi hálózaton használt e-mail címre és hozzá tartozó jelszóra bukkant. A jórészt brit és francia áldozatok adatait átadták a Facebook-nak.

Ekkoriban jelentek meg a hírek a Carberp nevű trójairól is, amely szintén a facebookozókat vette célba. Egy manipulált PDF vagy Excel dokumentum megnyitásakor fertőzött, hozzáférhetetlenné tette a felhasználó számára a gépet, majd „váltságdíjat” követelt annak felszabadításáért.

Január a bűnesetek felderítése szempontjából is fontos hónap volt a Facebook életében. Ekkor határozta el ugyanis a cég biztonsági vezetése, hogy nyilvánosságra hozzák, kik álltak a rengeteg kárt okozó Koobface fertőzés mögött.

Mint emlékezetes, a vállalatnak még a nevét is kifigurázó, a gépeket botnetbe szervező vírus 2008-tól két és fél éven át garázdálkodott a hálózaton – egészen addig, míg 2011 márciusában ki nem iktatták a vezérlőszerverét. Szakértők szerint fénykorában, 2010-ben a botnetben 400-800 ezer PC működött és a szemétszoftver eladásából, illetve a hirdetésbevételekből több millió dollárt hozott a vírusírók konyhájára.

Az, hogy a Facebook megjelentette a Koobface-banda tagjainak névsorát, fordulópontot jelent a számítógépes bűnözők elleni küzdelem történetében. Eddig ugyanis nem szoktak vírusírókat megnevezni. Az adott esetben egyes szakértők attól is tartottak - mivel a nyomozás még hivatalosan nem zárult le - hogy a Szentpéterváron kényelmesen éldegélő banda az utolsó pillanatban nyomokat tüntethet el. Efféle baleset azonban nem történt, és bár a hálózat már régóta Koobface-mentes, a Facebook-nál kijelentették: „addig nem hirdetünk győzelmet a vírus felett, míg szerzőit nem állítjuk bíróság elé”.

Mark Zuckerberg cége, mely részvénykibocsátásra készül, más szempontból is történelmet csinált. A Facebook az első vállalat, amely az amerikai tőzsdefelügyelet (Securities and Exchange Commission, SEC) elé terjesztett iratokban felhívja leendő részvényesei figyelmét a spam és a hackertámadások kockázatára. A SEC tavaly októberben szólította fel a tőzsdén jegyzett cégeket: adjanak számot az IT biztonsági kockázatokról, s jelentsék, ha kiberbetörés éri őket, hiszen ez kihathat pénzügyi teljesítményükre is.

Most a Facebook, mely 5 milliárd dollárt remél a börzére való bevezetéstől, kendőzetlenül a befektetők elé tárta fenyegetettségét. „Ágazatunkban minden korábbinál gyakoribbá váltak a számítógépes kártevők, vírusok, az adatbetörések és adathalász támadások. Ezekre a múltban is volt példa rendszereinkben, s a jövőben is bekövetkezhetnek. ... Mivel az élvonalban vagyunk, úgy gondoljuk, különösen vonzó célpontjai vagyunk az ilyen támadásoknak. ... Nem garantálhatjuk, hogy a spam-hullámok ellen bevetett technológiáink és munkatársaink képesek lesznek megakadályozni, hogy platformunkról spam-et küldjenek. Elképzelhető, hogy a spam-tevékenység miatt felhasználóink kevésbé használják a Facebook-ot vagy végképp elpártolnak termékeinktől” – olvasható a SEC-hez benyújtott anyagban.

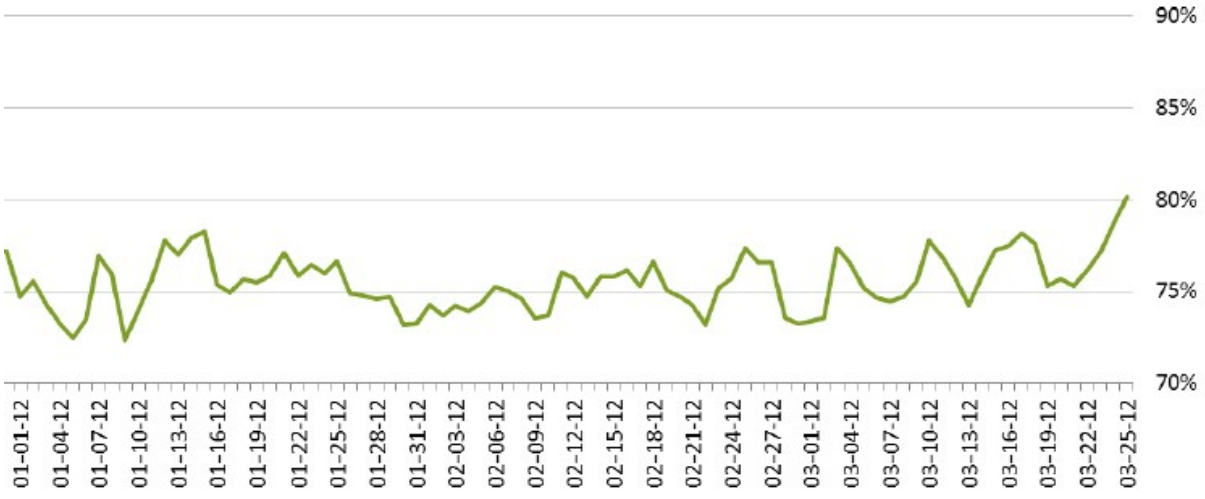
Spam és botnetek

De hogy is állt a világ spam dolgában az idei első negyedévben? Erről a Commtouch-nak az időszakot elemző *Internetes fenyegetés-trendjelentéséből (Internet Threats Trend Report)* kaphatunk képet.

Nos, ez a kép meglehetősen pozitív. A cégek – különösen a Microsoft – és a kormányok, illetve a bűnüldöző szervek erőfeszítései a botnetek felszámolására, üzemeletetőik bíróság elé állítására, s ezzel a spam-áradat visszaszorítására nem maradtak eredménytelenek. A tavalyi első negyedévhez viszonyítva az idei január-március időszakban közel 40%-kal kevesebb spam-et mértek. A kéretlen és adathalász levelek napi átlagos száma 94 milliárdra esett vissza. Az első negyedévben a globális teljes e-mailforgalomnak „mindössze” 75%-a volt a spam. Azt azonban a Commtouch sem meri megjósolni, hogy az éveken át tartó emelkedés után ez az alacsonyabb szint tartósan meg tud-e maradni.

Magyarországról csak a teljes 2011-es esztendőre vonatkozó adat áll rendelkezésünkre, s az a Cisco *Éves biztonsági jelentéséből (Annual Security Report)* származik. Eszerint tavaly 91%-kal alacsonyabb volt a spam-szint hazánkban, mint egy évvel korábban.

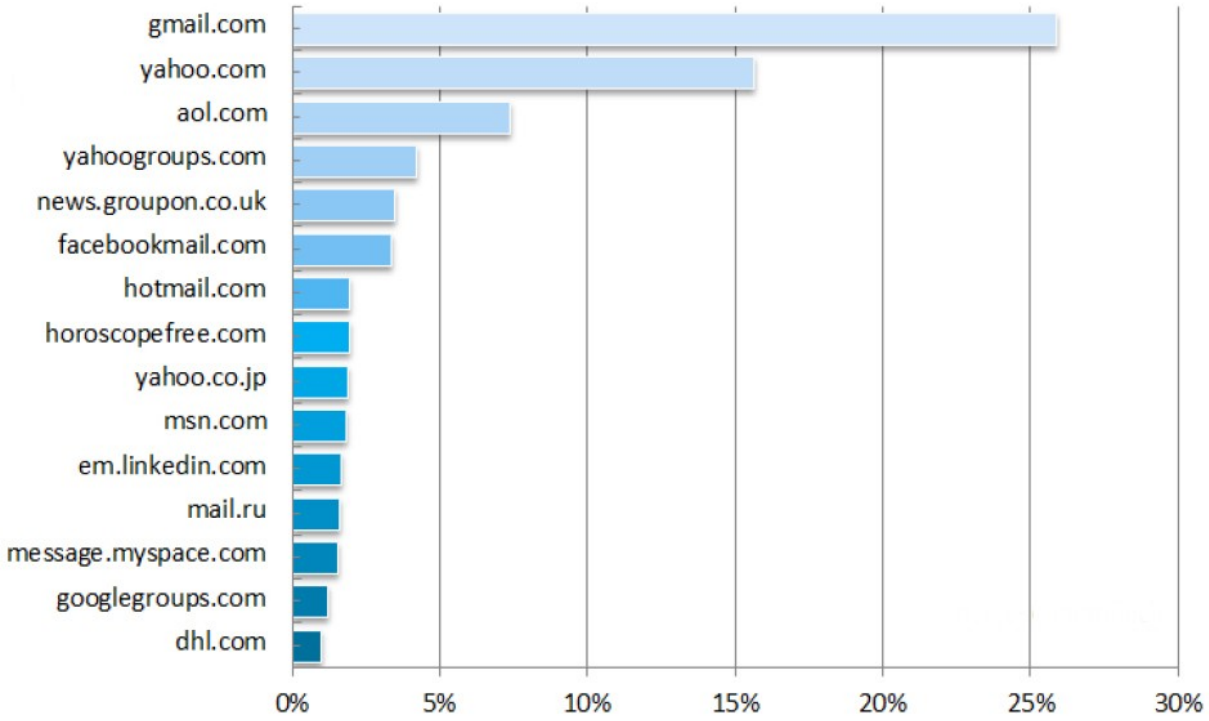
A spam aránya a globális teljes e-mailforgalomban 2012 első negyedévében



(Forrás: Commtouch)

Visszatérve a globális porondra, miről szólnak a kéretlen levelek? Leggyakrabban (majdnem 40%-ban – 8%-kal nagyobb arányban, mint a megelőző negyedévben) gyógyszert reklámoznak. És vajon honnan érkeznek? A Commtouch felmérése szerint a Feladó sorban legtöbbször az alábbi domain-ekkel találkozhattunk. Tegyük hozzá: a spammerek a küldő címet általában hamisítják.

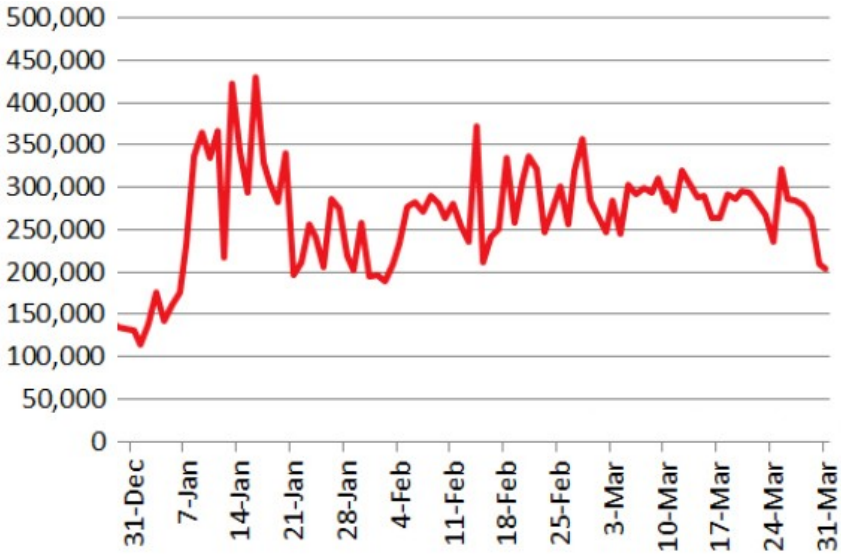
A kéretlen levelek Feladó sorban leggyakrabban szereplő (általában hamisított) domainek 2012 első negyedévében



(Forrás: Commtouch)

A spamszint nagymértékben attól függ, hány és mekkora botnet tevékenykedik, hány zombigép működik szerte a világban. Az első negyedévben átlagosan napról napra 270 ezer új zombi állt hadrendbe, kezdett spamet szórni – derül ki a Commtouch tanulmányából. A tavalyi utolsó negyedévben ez a szám még „csupán” 209 ezer volt.

Újonnan belépő zombigépek száma 2012 első negyedévében



(Forrás: Commtouch)

Előző negyedévekhez hasonlóan most is Indiában állították be a legtöbb új zombit. Ezzel együtt India részesedése a 2011. október-december időszakban mért közel 24%-ról 20% alá csökkent. Ezúttal a dobogó második fokára Brazília került, a bronzérmet pedig Oroszország „érdemelte ki”.

A botnetek elleni harcban továbbra is vezető szerepet játszik a Microsoft. A szoftveróriás január végén az Egyesült Államokban feljelentést tett a szentpétervári Andrej Szabelnyikov ellen, akit azzal vádol: ő írta a fénykorában több mint 40 ezer gépet mozgató, napi 3,8 milliárd kéretlen levelet szétszóró Kelihos botnet programját, s tartotta fenn a hálózatot. Szabelnyikov, aki korábban az orosz Agnitum IT biztonsági cégnél dolgozott, a BBC-nek úgy nyilatkozott: egyáltalán nem bűnös, és be fogja bizonyítani ártatlanságát.

Miközben a fejleményekre vártunk, március végén már a Kelihos utódjának kiiktatásáról érkezett hír. A bűnözők ezúttal az eredeti kártevőt felhasználva a réginél csaknem háromszor nagyobb botnetet építettek ki.

Újabb sikert könyvelhetett el a Microsoft a negyedév végén, amikor két amerikai városban, összehangolt hadművelettel lekapcsolta a hírhedt ZeuS és SpyEye banki trójaiakat terjesztő botnetek vezérlőszervereit. A szoftveróriás világszerte 13 millió gépen észlelt ZeuS vagy SpyEye fertőzést; közülük 3 millió az Egyesült Államokban működött. Most a szerverek kiiktatásával egyidejűleg a Microsoft 39 – meg nem nevezett – alperes ellen is eljárást indított.

Kiemelkedő kártevők

Ha már a ZeuS trójait említettük, amely igazán a „kiemelkedő" kártevők közé tartozik, el kell mondanunk, hogy a bűnözők immár nemcsak készen és olcsón beszerezhető kártevőgyártó eszközkészletek segítségével teszik hatékonyabbá munkájukat. A Seculert IT biztonsági cég nemrég arról számolt be, hogy az alvilágban hódítani kezdett a nyílt forráskódú fejlesztés modellje. Erre éppen az szolgáltatta az egyik első példát, hogy tavaly közzétették a ZeuS forráskódját, s ennek alapján új lendületet vett a banki trójaiak fejlesztése.

Az ellenkező végletet képviseli *Németh Attilának,* hazánk 26 éves polgárának esete a Marriott szállodalánccal. Hazánkfia éppenséggel nem nyílt, hanem nagyon is rejtett kóddal operált. Még 2010 végén trójaival fertőzött levelet küldött a hotelvállalat dolgozóinak. A megfertőzött PC-kről azután behatolt a cég szervereibe, amelyekről bizalmas információt emelt el. Ezután állást követelt a Marriott-nál, mondván: ha nem kap munkát, közzéteszi a megszerzett adatokat. A cég az amerikai titkosszolgálathoz fordult, s egy szállodai HR-esnek álcázott ügynök fiktív állásajánlattal Washingtonba csábította Némethet. Az ügy természetesen honfitársunk elítélésével végződött. Februárban egy amerikai bíróság 30 hónap szabadságvesztést szabott ki rá.

A szállodának szánt trójai csak magyar vonatkozása miatt érdemelte ki a „kiemelkedő" minősítést. Lássuk azonban, melyek voltak azok a kórokozók, amelyek valóban kiemelkedően sok bajt okoztak – ha nem is a nagyvilágban, hanem a hazai felhasználók körében. Híven hűséges kutyájáról szóló jelmondatához – *„Buster mindig éberen figyel"* – a VirusBuster folyamatosan nyilvántartást vezet a magyar neten észlelt számítógépes károkozókról. A cég szakemberei kiértékelik házon belüli, illetve különböző helyeken működtetett levelezésvédő rendszereik fogását, s az adatokból hónapról hónapra toplistát készítenek, melyet a vállalat site-ján is megjelentetnek, a www.virusbuster.hu/labor/virus-toplista címen.

Idén az év első három hónapjában az alábbi kártevők tűntek fel leggyakrabban:

	Kártevő	Részesedés
1	Exploit.MS04-028	22,15%
2	Win32.Sality.AP.Gen	20,26%
3	Trojan.PWS.Qbot!wBBAJ1poFzc	11,71%
4	Win32.Sality.BL	8,90%
5	I-Worm.Brontok!aFqxT3myUcc	8,55%
6	Trojan.Patched!7PoD6otsVGk	6,77%
7	Trojan.Qbot!wl8JBlHH+Rs	6,04%
8	Trojan.Conficker.Gen!Pac	5,84%
9	Trojan.Ceeinject.Gen	5,73%
10	Trojan.Kryptik!yvKWdTs6/wk	4,05%
		100,00%

Napjaink elterjedtebb kártevőit alkotóik weboldalakon keresztül (is) folyamatos frissítik. A kártevők felismerésének biztosítása érdekében más vírus-laborokhoz hasonlóan a VirusBuster is folyamatosan nyomon követi ezeket a webhelyeket. A gyakori frissítések miatt természetesen a cég csak generikus felismerési módszerekkel kezeli őket, az utánkövető feldolgozás nem szolgálná a felhasználók érdekeit.

Alábbi táblázatunk 2012. január-március legaktívabb kártevőszóró domain-jeit foglalja össze, megadva azt is, hogy a gyakoribb kártevőfajtákból hány file-t mutattak ki egy-egy domain-en. Láthatóan a bűnözők továbbra is aktívan használják a fájlmegosztó oldalakat, mint amilyen például a dropbox.com.

Domain	File-ok száma	Vírus	Féreg	Back-door	Adware	T. kém-program	Letöltő	Jelszó-lopó	Dropper	Trójai	Packer
origin-ics.fivemillionfriends.com	800				9		1			1	
zunegateway.com	594				49					1	
soft.foxtab.com	578										
dl.dropbox.com	474	4	22	17		33	80	26	38	105	34
www.toptenreport.com	421				47				1	1	
screenblaze.com	404						213				
origin-ics.clickpotato.tv	372				72						
origin-ics.ravenbleu.com	262										
78.111.51.123	255				1					32	
74.82.207.242	174					3				4	

Jó tudnunk azt is, hogy a weben barangolva hol kell leginkább fertőzéstől vagy adathalászattól tartanunk. Erre vonatkozóan a Commtouch már idézett Internetes fenyegetés-trendjelentése ad eligazítást. A cég statisztikái szerint az első negyedévben (gyakorisági sorrendben) a következő site-kategóriákon bújtattak meg a bűnözők valamilyen kártevőt:

Leggyakrabban fertőző site-kategóriák	
1	Pornó/szex
2	Parkolt domain
3	Divat és szépségápolás
4	Portál
5	Szórakoztatás
6	Oktatás
7	Egészségügy
8	IT, technológia
9	Céges site
10	Pihenés és szabadidő

Hangsúlyoznunk kell, hogy szinte mindig „ártatlan” site-okról van szó, azaz a bűnözők a site tulajdonosának, üzemeltetőjének állítják a szervereket sötét cél szolgálatába. Jellemző, hogy a Commtouch felmérése szerint az üzemeltetők 90%-a nem vett észre semmilyen rendellenességet, pedig site-ját feltörték és javában szórta a spam-et. A webmesterek kétharmada nem tudta, hogyan hatolhattak be a hackerek.

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

Leggyakrabban adathalászó site-kategóriák	
1	Portál
2	Vásárlás
3	Divat és szépségápolás
4	Oktatás
5	Céges site
6	Sport
7	Pihenés és szabadidő
8	Egészségügy
9	Ingatlan
10	Személyes site

Az iparág nagyjai egyébként nemcsak a spam és a botnetek, hanem az adathalászat ellen is igyekeznek minél erőteljesebben és hatékonyabban fellépni. Ennek legújabb eszköze egy *de facto* szabvány, melyet többek között a Facebook, a Google, a Microsoft, a PayPal és a Yahoo is támogat. A DMARC (Domain-based Message Authentication, Reporting & Conformance, domain-alapú üzenet autentikáció, visszajelzés és megfelelés-vizsgálat) specifikáció a „tiszta" levelek feladói és címzettjei közötti együttműködésre épít. A szabványos e-mailben a feladó házirendeket állíthat be, s ezek alapján a fogadó levelezőszerver könnyen szét tudja válogatni a valódi, „tiszta" leveleket azoktól, amelyekben hamisították a feladó domaint.

A szabvány nyilvánvalóan nem fogja teljesen megszüntetni az adathalászatot, de mindenképpen nagy előrelépést jelent. Elterjedésére nem is kell sokáig várnunk, mivel bevezetése már másfél évvel a mostani nyilvános bejelentés előtt csöndben megkezdődött. A Gmailre érkező levelek 15%-a például már megfelel a DMARC-nak.

Folt hátán folt

Komolyan veszélyezteti az internetezőket, hogy rohamosan nő a szoftver-sérülékenységek száma – figyelmeztetett február közepén kiadott, 2011-re vonatkozó *Éves jelentésében (Yearly Report)* a Secunia. A növekedésért elsősorban nem a Microsoft programok, hanem szinte kizárólag a más cégek által fejlesztett alkalmazások a felelősek. Míg egy tipikus gépen a nem-Microsoft sérülékenységek aránya 2006-ban 45% volt, 2011-re elérte a 78%-ot. Tavaly a fennmaradó 22%-ból 10-zel a Microsoft alkalmazások, 12%-kal az operációs rendszerek részesedtek. A sérülékenységek száma pár év alatt megháromszorozódott, s 2011-ben meghaladta a 800-at. Tovább rontja a képet, hogy a rések több mint felét „nagyon kritikusnak" vagy „rendkívül kritikusnak" minősítette a Secunia. A sérülékenységek nyilvánosságra kerülésének napján 72%-ukra már készen állt a folt, vagyis a védekezés megszervezése a felhasználó szervezetek feladata – állapítja meg a cég.

A foltozatlan rések viszont értéket képviselnek a piacon. Persze a fekete, a szürke és a fehér piacon más és más ez az érték. Márciusban a neves amerikai üzleti magazin, a *Forbes* annak járt utána, mennyit lehet kapni egy sérülékenység bejelentéséért – nem bűnözőktől, nem is a fejlesztő cégtől, hanem egy homályba burkolódzó, ám teljesen legális csatornán keresztül. A lapnak egy Grugq fedőnevű hacker-üzletközvetítő beszélt arról, hogy amerikai kormányzati beszállító cégek, kormányszervek hat számjegyű dollárösszeget is fizetnek egy-egy újonnan felfedezett résért. Legértékesebbnek az Apple iOS lyukai számítanak ezen a piacon. Egy ilyen például Grugq gyakorlatában negyedmillió dollárért cserélt gazdát. A Chrome és az Internet Explorer sérülékenységei 200, a Firefox és a Safari rései 150 ezer dollárt érhetnek. Ezekhez az összegekhez képest potom pénz az, amit a fejlesztő cégek ajánlanak. A Google jutalomprogramja például legfeljebb 3.133,70 dollárt ad egy kritikus Chrome sérülékenységért...

Mindenesetre azt leszögezhetjük, hogy a szoftvercégeknek az idei első három hónapban is bőven volt foltoznivalójuk. A következőkben röviden, időrendben a legfontosabb biztonsági frissítéseket tekintjük át.

Január

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

Február

- Kilenc javítócsomag – köztük négy kritikus és öt fontos – volt a februári foltozó kedd mérlege. A szoftveróriás összesen 21 sérülékenységet orvosolt, egyebek mellett az Internet Explorerben és a C futásidejű könyvtárban. A cég megragadta az alkalmat, hogy megemlékezzék arról: 10 évvel azelőtt jelent meg *Bill Gatesnek* az a feljegyzése, amely a biztonságot állította a Microsoft fejlesztés és támogatás középpontjába.
- Hét lyukat tömött be a Flash Player frissítésével az Adobe. Kilenc kritikus sérülékenységet szüntetett meg a cég a Shockwave Playerben is.
- Összesen 20 biztonsági problémát oldott meg a Google a Chrome 17-es verziójának kibocsátásával. Az új böngésző letöltés előtt egybeveti a kijelölt file-t egy feketelistával, így hathatósan véd rosszindulatú állományok, például hamis antivírus termékek letöltése ellen.
- A Mozilla egy kritikus hiba javítása kedvéért a Firefox és a Thunderbird verziószámát 10.0.1-re, a SeaMonkeyét 2.7.1-re emelte.

Március

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

A VirusBuster Kft.-ről

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

Elérhetőségeink

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

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937