Puskás Tivadar Közalapítvány

PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ

2011. I. negyedéves jelentés

PTA CERT HUNGARY

NEMZETI HÁLÓZATBIZTONSÁGI KÖZPONT

Tartalom

Bevezető

A Puskás Tivadar Közalapítvány által működtetett Nemzeti Hálózatbiztonsági Központ elkészítette 2011. első 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 a magyar otthoni felhasználók számítógép és internetellátottságáról, valamint felhasználói szokásaikról. Többek között szó esik a vírusirtók- és közösségi oldalak használatáról, valamint hasznos tanácsokkal látjuk el a szülőket gyermekeik internet használatával kapcsolatban.

Egy cikk erejéig kitérünk a napviharok vezérlő-rendszerekre és kritikus infrastruktúra ellenőrző rendszerekre gyakorolt káros hatásainak ismertetésére.

A Nemzeti Hálózatbiztonsági Központ továbbra is eredményesen működteti szakmai közönségének és partnereinek szóló IT biztonsági oldalát a Tech.cert-hungary.hu-t.

Az oldalon a látogató megtalálhatja a legfrissebb szoftversérülékenységi és riasztási információkat, valamint a TechBlog hírfolyam naponta frissülő nemzetközi hírekkel és érdekességekkel látja el a hazai olvasótábort, magyar nyelven.

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

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

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

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

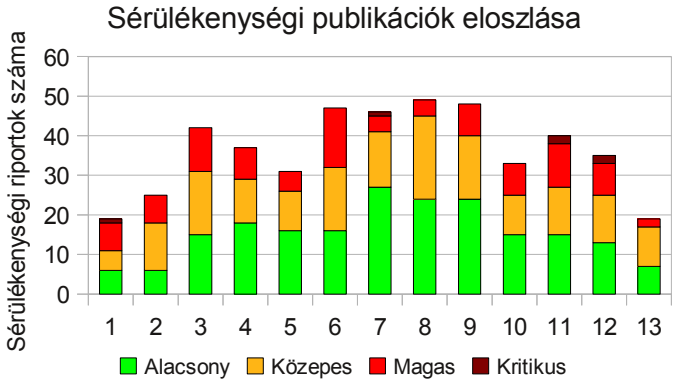
Dr. Suba Ferenc
Puskás Tivadar Közalapítvány
Nemzeti Hálózatbiztonsági Központ
nemzetközi képviselő

Dr. Kőhalmi Zsolt
Puskás Tivadar Közalapítvány
a kuratórium elnöke

Bódi Gábor
Puskás Tivadar Közalapítvány
ügyvezető igazgató

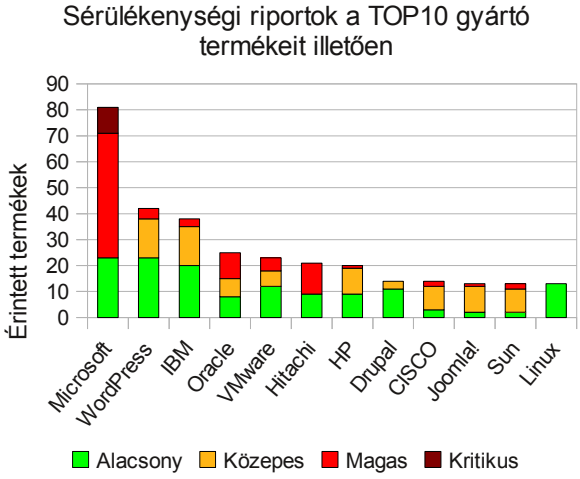
Szoftver sérülékenységek

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



A **PTA CERT-Hungary, Nemzeti Hálózatbiztonsági Központ (NHBK)** 2011. első negyedéve során **471 db szoftver-sérülékenységi információt** publikált, amelyekből 202 db alacsony, 165 db közepes, 98 db magas és 6 db kritikus kockázati besorolású.

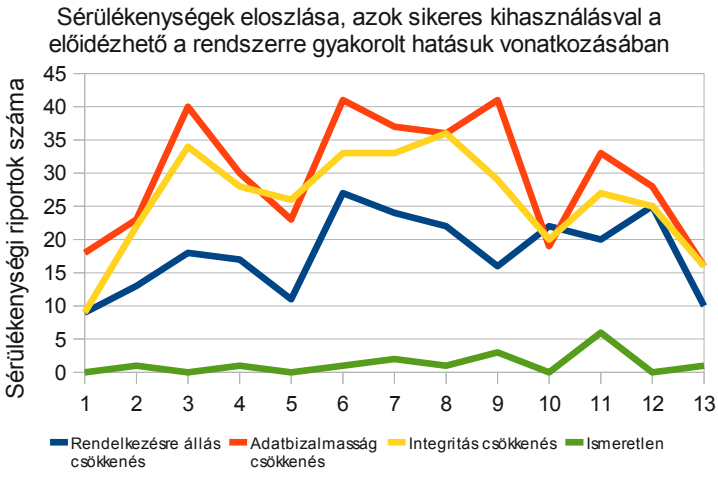
Az előző negyedévhez képest 7%-kal nőtt a kiadott sérülékenységi információk száma. Legnagyobb számban februárban kerültek kiadásra sérülékenységi információk, melyek közel 40%-át teszi ki az összes publikációnak.



A 2011. év eleje sem hozott nagy újdonságot az egyes sérülékenységek által érintett szoftverek kimutatásában, de jól látszik, hogy az egyes sebezhetőségek által érintett termékek száma és azok elterjedtsége között szignifikáns összefüggés mutatható ki. A negyedév adatai lapján is még mindig a Microsoft termékek vezetik a kimutatást, közel kétszeres túlsúllyal a soron következő WordPress és IBM termékek előtt.

A helyzetet csak tovább rontja, hogy a Microsoft termékek 60%-a magas és további 12%-a kritikus kockázatú sérülékenységek kapcsán kerültek regisztrálásra.

A sebezhetőségek értékelésénél fontos az, hogy a biztonságon belül melyik biztonsági követelményt fenyegeti. Mindezek figyelembevételével lehet a következő negyedéves informatikai biztonsági kontroll-fókuszokat kidolgozni az egynél több sebezhetőséget jelentő adott gyártók termékeit vagy termékeket használó szervezetek körében.

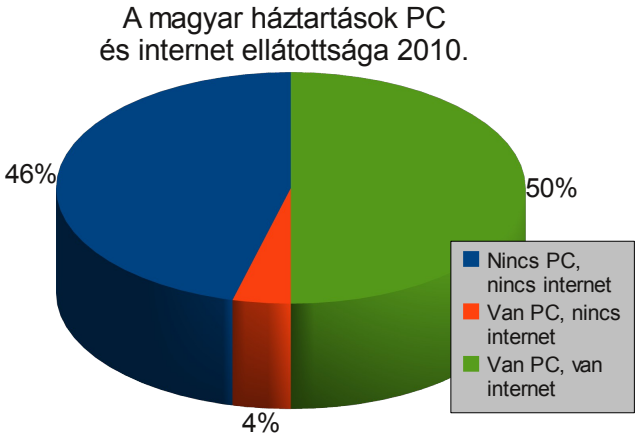


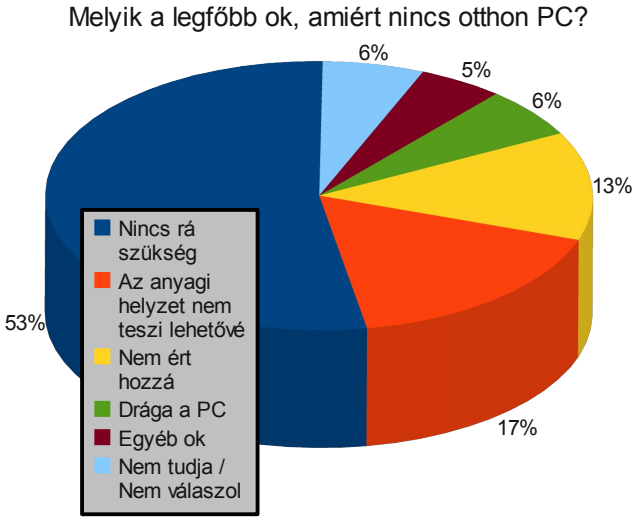
Legnagyobb számban adatbizalmasság és integritás csökkenés előidézésére alkalmas sérülékenységek láttak napvilágot az elmúlt negyedévben. Az előző periódushoz képest 8%-kal, illetve 11%-kal több azon sérülékenységek száma melyek sikeres kihasználása adatbizalmasság, illetve integritás csökkenését eredményezheti. Ezért ezen támadhatóságok irányába javasolt az ellenőrzéseket fókuszálni az elkövetkezendő időszakban, továbbá az életbe léptetett kontrollok hatékonyságát és megelőző képességét javasolt mindenhol megvizsgálni.

Számítógépek és internet otthon – a felhasználói környezet

Otthoni PC és internet ellátottság

A hazai otthonok közel felében még hiányzik a családi készülékparkból a személyi számítógép - mutat rá a Magyar Infokommunikációs Jelentés kutatássorozatának legfrissebb elemzése. A tíz éve futó kutatássorozat számai azt mutatják, hogy a háztartások számítógép- és internet-ellátottsága közötti olló lassan bezárul. Míg öt évvel ezelőtt a 37%-os PC-penetráció jó kétszerese volt az internet elterjedtségének, mára a különbség alig négy százalékpontra apadt. Nagyon megfogyatkozott tehát az a tömeg, akikhez „már csak az internetet kell odavinni”, mert az eszközszintű alap-infrastruktúrájuk és az alapvető számítógép ismeretük megvan a világháló használatához.





A BellResearch kutatási eredményeiből legfőbb visszatartó tényezőként **az igény és a motiváció hiánya, az érdektelenség rajzolódik ki**: a PC-vel nem rendelkezők háromnegyede szerint a háztartásában senkinek sincs rá szüksége, és a legtöbbek számára ez egyúttal a legfőbb ok is. Kedvezőtlen jövedelmi viszonyokra jóval kevesebben hivatkoznak - a válaszadók kevesebb, mint kéttizede számára jelent ez elsődleges korlátot - csakúgy, mint a hozzáértés hiányára.

A meginterjúvolt háztartások döntéshozóinak tervei nem kecsegtetnek túl sok jóval: a PC-vel nem rendelkezők mintegy négyötöde biztosan nem készül a következő egy esztendőben asztali vagy hordozható személyi számítógépet vásárolni, és csupán két százalékuk biztos a vételi szándékában. Az otthoni PC beszerzését elképzelhetőnek tartó háztartásoknak viszont több mint fele internet-előfizetést is vásárolna a géphez, míg relatíve sokan - a válaszadók egyharmada - bizonytalanok e tekintetben.

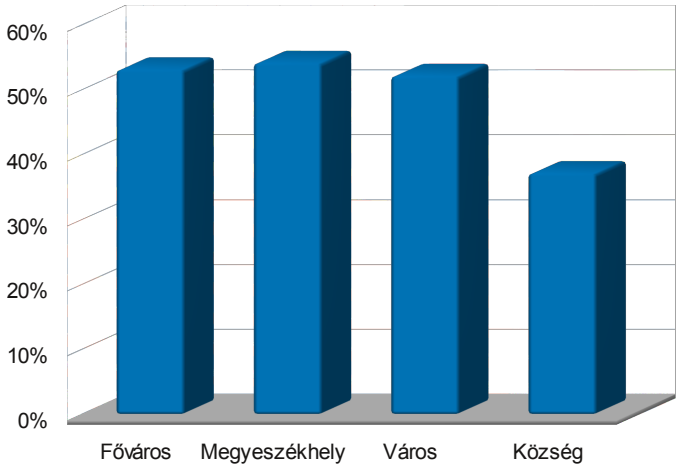
Noha az otthoni sávszélesség nagyságát nem mindenki (tízből csak hét válaszadó) ismeri pontosan, a legtöbben a 2-5 MBit/s sebességet jelölték meg. Figyelemreméltó, hogy a felhasználók több mint 16 százaléka már 15 MBit/s-nél nagyobb sávszélességű hozzáféréssel rendelkezik.

A helyzet azért is elgondolkodtató, mert a kimaradók között még sok a gazdaságilag aktív ember, aki rendszeresen intéz ügyeket, fizet be csekkeket, vall be adót. Érdektelenségük miatt ők azt sem tudják, hogy az ICT mennyire megkönnyíthetné az életüket.

A legfontosabb feladat ezért az igények felkeltése lenne. A kutatók szerint az egyik lehetséges kitörési pont a digitális televízió lehetne: a közös technológiai alapok révén az internetet is be lehetne csempészni számtalan háztartásba, és a megfelelő, könnyen elérhető tartalom már kellő motivációt jelentene a használatára.

A PC-beszerzési tervekhez hasonló a helyzet a számítógéppel ellátott otthonok internet-bevezetési szándékai terén is: a PC-vel már rendelkező hazai háztartások bő négyötöde azt nyilatkozta, hogy nem tervezi a következő egy évben előfizetés vásárlását.

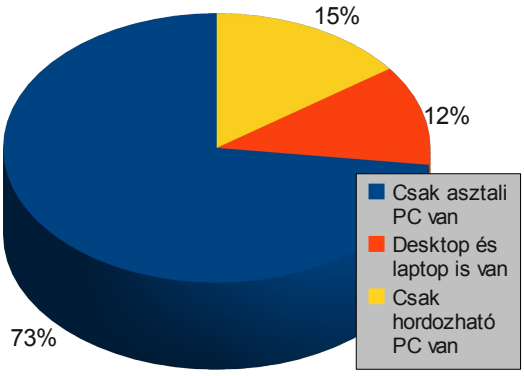
A magyar háztartások internet ellátottsága 2011.



A lakossági eszközpark

A BellResearch adatai alapján a tipikus otthoni PC ma asztali számítógép, legalább hároméves, hagyományos crt-monitor kapcsolódik hozzá és Windows XP fut rajta; egyre több azonban a hordozható PC, s nemcsak második, hanem kizárólagos eszközként is megjelent.

Destopok és laptopok aránya
a magyar háztartásokban 2011.

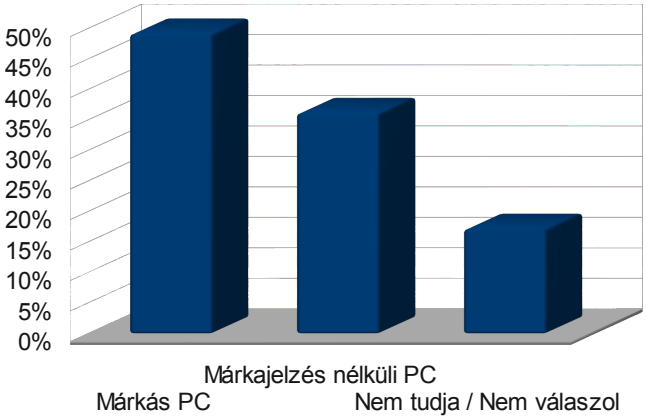


A négymillió magyar háztartás 53 százaléka, azaz több mint 2,1 millió otthon rendelkezik legalább egy személyi számítógéppel, ami az egy évvel ezelőtti penetrációs szinthez képest csupán kismértékű emelkedést jelent.

A háztartások egyre növekvő hányadában ülhetnek gép elé egyszerre többen is, jelenleg közel minden ötödik otthonban van legalább két eszköz. A többség (73%) ugyan csak desktop konfigurációval rendelkezik, azonban évről-évre egyre nagyobb hányadban jelennek meg a hordozható PC-k második, illetve kizárólagos eszközként.

A háztartásokban megtalálható számítógépek nagyobbik része – eredetileg – valamely gyártó márkás, készre szerelt terméke. Ebben nagy szerepe van az új beszerzéseket tekintve egyre népszerűbb notebookoknak is, amely termékkategóriában nem beszélhetünk márka nélküli, a felhasználó által összeállított eszközökről.

Márkás és noname PC-k jelenléte
a magyar háztartásokban 2011.



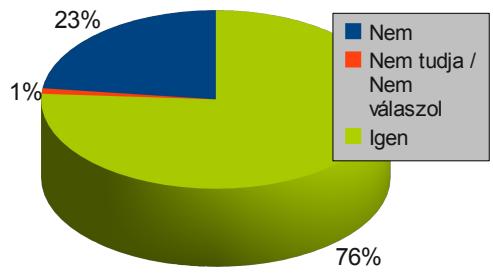
Az egyedi összeállítás két típusát különböztethetjük meg, az átlagfelhasználó számára a szakkereskedések egyedi konfigurációi pénztárcához szabott megoldást kínálnak, az egyedi komponensek gondos, saját igények szerinti összeválogatása pedig a viszonylag csekély létszámú, informatikailag magasabban képzett lakossági felhasználói kör esetében jellemző.

Továbbra is vezetnek az otthon használt operációs rendszerek körében a Windows különböző verziói, ezen belül pedig még mindig a közel tízéves XP a legelterjedtebb (a háztartások 75%-ában megtalálható); a Vistát az alig egy éve elérhető Windows 7 is megelőzi.

A legelterjedtebb alkalmazások között első helyen a játékprogramok állnak (85%), ami egyenes következménye annak, hogy minden második háztartásban legalább hetente játszik a gépen valaki, tehát az egyik legfőbb felhasználói tevékenységnek tekinthető. A zene-, dvd-, multimédia-lejátszó szoftverek, illetve a képnézegetők szintén az elsők között szerepelnek a rangsorban, az ilyesfajta kikapcsolódás a játékhoz hasonlóan népszerű.

Biztonsági szempontból kimutatható, hogy az otthoni gépeknek már háromnegyedén fut vírusvédelmi szoftver, és nagyjából a felén valamilyen tűzfalmegoldás. Széles körben elterjedtek a szövegszerkesztők és a táblázatkezelők is, ezek túlnyomórészt Microsoft Office programok.

Irodai programok használata
a magyar PC-használók körében 2011.



Az otthoni PC-használati célok között az internetezés első helye megkérdőjelezhetetlen: a háztartások több mint kétharmadában ez napi rutinnak számít. Az otthoni munkavégzés viszont jóval kevésbé jellemző, erre csak minden negyedik háztartás használja a PC-jét rendszeresen, azaz legalább hetente.

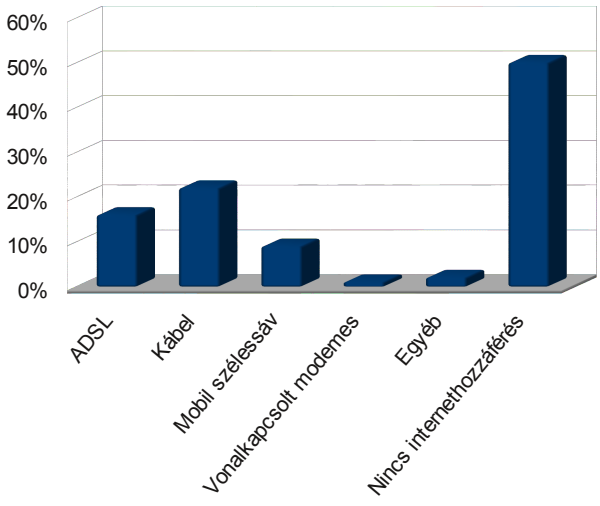
Mobilizálódó felhasználók

Bár ma még az internetezés domináns eszköze az asztali számítógép, a helyhez kötöttségtől mentes használat előnyeit egyre többen és egyre inkább kihasználják. Ez nemcsak az eszközök „mobilizálódásának”, de a szélessávú mobilinternet térhódításának is köszönhető.

A fentiekben bemutatott eltűnő olló az IT-eszköz és az internethasználat között előrevetíti, hogy a mobilkommunikációs eszközök esetében hasonló folyamatok várhatók. A webképes mobiltelefonok svga-felbontással, a világhálóra csatlakozó televíziók, a YouTube-kompatibilis médialejátszók, az „intelligens” háztartási eszközök olyan előnyökkel kecsegtetnek, amelyek egy évtizede jobbára még csak a jövőkutatók elképzeléseiben éltek.

Mind a hozzáférés eszközét, mind a használat módját tekintve a legmarkánsabb változást a szélessávú mobilinternet térhódítása jelenti. A háztartások közel 10 százalékában található meg ilyen típusú kapcsolat, ami az online háztartások közel ötödét, 18 százalékát jelenti; sok helyütt a vezetékes internetet teljesen kiszorítva kizárólag a SIM-kártyával üzemelő eszközök jelentik a kapcsolatot a világhálóval.

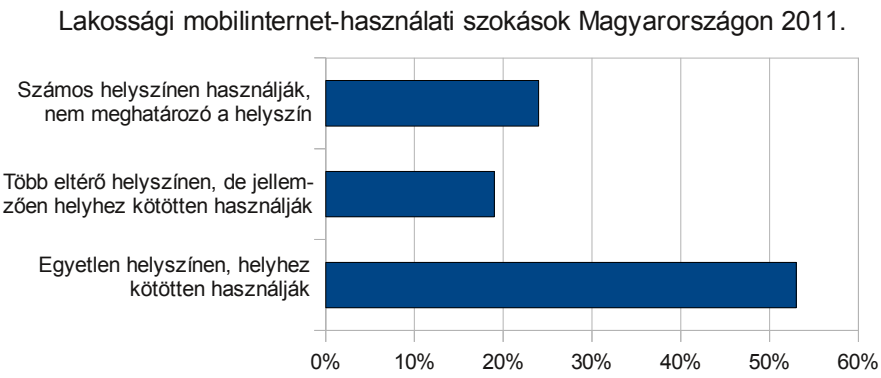
A lakossági internet hozzáférések technológiai
eloszlása Magyarországon 2011.



A Magyarországon szélesebb kör számára alig három éve elérhető, mai fogalmaink szerinti szélessávú mobilinternet nem pusztán alternatív technológiaként jelenik meg az ADSL vagy a kábeltévés hozzáférések konkurenseként, de a használat jellegét is átalakítja. Bár a többség ma még egyetlen helyszínen, az otthonában használja internetkapcsolatát, a helyhez kötöttségektől mentes felhasználási mintázatok gyorsan teret nyertek. **A mobilinterneten keresztül csatlakozók között többségben vannak a notebookok az asztali gépekhez képest, négyből egy mobilinternet-előfizető (háztartás) számára pedig a hozzáférési helyszín másodlagos, ők az „always-online” userek**.

A hazai 18-49 éves lakosság 18%-a rendelkezik okostelefonnal, amely szám az elkövetkező években hatalmas növekedés előtt áll. A vizsgált alapsokaságban, - mint az várható -, a 18-29 évesek között találhatók legnagyobb arányban (25%) okostelefont használó személyek, míg a 39-49 éves korcsoportban ez az arány csak 10%. Amennyiben bázisként a már okostelefonnal rendelkezőket tekintjük, akkor láthatjuk, hogy Magyarországon egyelőre még a Symbian (30%) rendszerrel rendelkező készülékek vezetik az oprendszerek listáját, de nyomukban már ott található az Android (25%), a Microsoft (14%) és az Apple (6%). Az adatokból az is kiderül, hogy bár az iPhone-nak nagyon kicsi még hazánkban a penetrációja, azonban ez az a márka, amelynél a legnagyobb a különbség a használt és vágyott telefonmárka között.

Az okostelefonok internetelérésben betöltött szerepéről meg kell jegyeznünk, hogy mindössze a felhasználók 9%-a tekinti készülékét a hagyományos internetelérés alternatívájának, és használja rendszeresen böngészési célzattal, míg az okostelefon használók 55%-a egyáltalán nem tekinti a PC alternatívájának telefonját.



A kutatási eredmények szerint a mobilinternetet használók többsége szerint igényeiknek, szokásaiknak tökéletesen megfelel a kábelektől mentes hozzáférés - annak ellenére, hogy jellemzően legfeljebb havi 3-5 GB adatforgalomra szólnak a szerződések. Mindez érdekes kérdéseket vet fel a sávszélességben egymásra licitáló vezetékes internetszolgáltatásokra nézve. Igaz ugyan, hogy vannak előfizetők, akik igénylik az akár 100 megabites csomagokat, de ennél is nagyobb hatást gyakorol a felhasználás milyenségére a nem helyhez kötött hozzáférés megvalósulása.

Digitális írástudás, digitális középosztály

Az IKT használat adatai egy más szemszögből, azt vizsgálják, hogy bizonyos felhasználói csoportok hogyan viszonyulnak e technológiai körhöz, milyen kategorizálás mutatja meg legjobban az egyes otthoni felhasználói csoportok markáns különbségeit. Az Információs Társadalom és Hálózatkutató Központ (Ithaka) munkatársai ezekre a kérdésekre keresték a választ [2]:

- A digitális írástudás olyan mértékben vált kiemelt elvárássá a munkaerőpiacon, hogy hiánya vagy hiányosságai korlátozott foglalkoztathatóságot eredményeznek, ami alapvetően visszaveti az egész ország versenyképességét.
- Az IKT felhasználói ismeretek szintjének elmaradása az adott munkakör által igényelt ismeretszinttől kimutathatóan pénz- és időveszteséggel jár a gazdaság és a közszféra számára is.
- Az alacsony digitális írástudásra vezethető vissza, hogy az online kormányzati, közigazgatási és egészségügyi szolgáltatások is csak lassan terjednek, ami elodázza a költséghatékony, a milliárdokban mérhető megtakarítást eredményező online szolgáltatások alkalmazását.
- Az alacsony digitális írástudás szintje megakadályozza az online oktatási, képzési formák tömeges elterjedését, ezáltal meggátolja a tömeges részvételt a felnőttképzési programokban, ami szintén visszahat az alacsony munkaerő-piaci versenyképességre, az alacsony foglalkoztathatóságra.
- A fogyatékkal élők és más hátrányos helyzetű csoportok kimaradnak az IKT nyújtotta előnyökből, ezáltal tovább mélyül a szakadék a társadalom egyes rétegei között.

- A digitálisan írástudók körében is alacsony az online tranzakciók aránya.
- A hiányzó digitális írástudás miatt alacsony az igény az online szolgáltatásokra, ezért a húzóiparágba tartozó online szolgáltatások piaca nem tud fejlődni.
- 16 év feletti lakosság csaknem fele még mindig nem digitálisan írástudó. Különösen nagy a lemaradás az idősek, hátrányos helyzetűek, kistelepülésen élők és alacsony végzettségűek körében.
- Az elmúlt három év eredményét nézve azt láthatjuk, hogy jelentős mértékben (14 %-kal) nőtt a digitálisan írástudók aránya, azaz az offline PC használatot követően a világhálót elkezdték használni. Ugyanakkor a teljesen digitálisan írástudatlan réteg csak 5 %-kal csökkent.
- Külön probléma, hogy „zárul az olló”, azaz az internet- és számítógép-használók számában fennálló különbség minimálisra csökkent, azaz (a korábbiaktól eltérően) elmondhatjuk, hogy aki számítógépet használ, az internetet is. Felmérések alapján nem várható, hogy a PC–vel rendelkező felhasználók aránya jelentős mértékben növekedne a jövőben. Ez ahhoz vezethet, hogy a digitálisan írástudók és írástudatlanok közti szakadék állandósul.
- A KKV-kat és különösen a mikrovállalkozásokat vezetők körében alacsony a digitális készségek szintje.
- A képzésbe még nem épült be a digitális eszközök és tartalmak készségszintű használata.
- A digitális átállásra az érintett 8-900 ezer háztartást még fel kell készíteni.

Ahogyan az az 1.1. fejezetben is látható volt, probléma legfőbb oka a motiváció és a készségek hiánya: az internet-előfizetések elmaradásának okát vizsgáló piackutatások szerint a megkérdezettek több mint fele azt válaszolja, hogy nincs szüksége az internetre. A „digitális esély” alakulásában egyre lényegesebb szerepe van az eddig is meghatározó első kézből való tapasztalatnak. Az elemzések szerint semmi nem növeli jobban annak az esélyét, hogy valaki internethasználó legyen, mint az igazán közeli, akár saját háztartásban szerzett tapasztalat egy adott eszközzel kapcsolatban, illetve az internetet már használó családtagok, barátok segítsége, vagy akár csak jelenléte. Az alulról szerveződő, civil kezdeményezések képesek leginkább megszólítani és érdekeltté tenni a leszakadókat.

Az alap- és középfokú oktatás IKT képzési szintje alacsony, nem alkalmazás-orientált, nem biztosítja készségszinten az IKT eszközök mindennapi életben és a vállalkozásokban történő használatát. A piacképes tudással rendelkező IKT szakemberhiány folyamatosan nő.

Ezzel együtt elkezdett kialakulni egy, az IKT-t napi szinten biztonsággal használó, online elit is az országban, akik a „digitális középosztály”-nak nevezett réteget erősítik. Összességében az internethasználók több mint háromnegyede egyetért azzal, hogy az új technológiák jobbá teszik az életünket, kétharmaduk örömmel veszi, hogy ezeken keresztül sok információ zúdul rá és ez a bőség nem ejti őket zavarba. Az új kommunikációs csatornák intenzív használata következtében a szórakozás, informálódás, kapcsolattartás és a közösségi lét új paradigmája van kialakulóban, immár a hétköznapokban is.

Az internetezők közel fele tartozik abba a két csoportba, akiket szokásaik alapján online virtuózoknak, illetve digitális középosztálynak neveznek a kutatók. Ők a teljes magyar lakosságnak körülbelül a negyedét teszik ki. Ők azok, akiket életük szinte minden területén folyamatosan digitális eszközök veszik körül, és ezeket aktívan használják is. A különbség a két csoport között, hogy, míg az online virtuózok jellemzően a diákéveiket töltik és ezáltal több idővel rendelkeznek a szórakozás, kommunikáció, WEB 2.0 típusú tevékenységekben, a digitális középosztály inkább a fiatal dolgozó felnőttekből épül fel ennek a szerepnek megfelelő, munkához, mindennapi élethez, ügyintézéshez szorosabban kapcsolódó IKT fogyasztással.

Az internet és a pénzügyek

A megtakarítással rendelkező magyar lakosság 24 százaléka intézi pénzügyeit az interneten. A legnagyobb arányban a 40 - 49 évesek használják a netes banki szolgáltatásokat rendszeresen.

A személyes ügyintézés után az internetes a második legnépszerűbb banki ügyintézési mód a megtakarítással rendelkező magyarok körében. A kétharmada a személyes, 24 százaléka az interneten keresztüli, míg 10 százaléka a telefonos ügyintézését részesíti előnyben. Meglepő módon azok, akik inkább a személyes lebonyolítást szeretik, szinte kizárólag így is intézik ügyeiket, ezzel szemben az internetes ügyintézést kedvelők banki ügyleteiknek csupán 69 százalékát intézik elektronikusan, a fennmaradó egyharmadot ők is személyesen szeretik letudni. A telefonos ügyintézést inkább kiegészítéseként alkalmazzák.

Lakhelyüket tekintve az internetes ügyintézők közt erősen felülreprezentáltak a fővárosiak, valamint a 2000 főnél kisebb településeken élők, míg a személyes bonyolítás elsősorban a kisebb városokban népszerű.

Az internet szerepe a pénzügyi tájékozódásban is megkérdőjelezhetetlen. A Pécsi Tudományegyetem egy friss kutatása [3] szerint a lakossági banki ügyfelek 35 százaléka ugyanis elsősorban a világhálóról szerzi be a pénzügyi lehetőségekkel kapcsolatos információkat. Az online információszerzés népszerűségét csak a bankok tudták megközelíteni, a válaszadók 30 százaléka fordul ugyanis elsőként közvetlenül a pénzintézetekhez az anyagiakkal kapcsolatban.

Az internet, mint fő döntéstámogató terep jelentőségét az is mutatja, hogy a kutatás szerint a válaszadók közel fele egyedül határoz a pénzügyekről: 45 százalékuk ugyanis általában nem kér személyes tanácsot ilyen ügyekben - számukra kiemelten fontos lehet az interneten fellelhető információk sokrétűsége és áttekinthetősége. Azok, akik inkább bevonnak valakit a döntésbe, egyenlő arányban választják a családi, baráti körüket és a pénzintézeteket, szakembereket (31-31%).

Informatikai biztonság lakossági szemmel

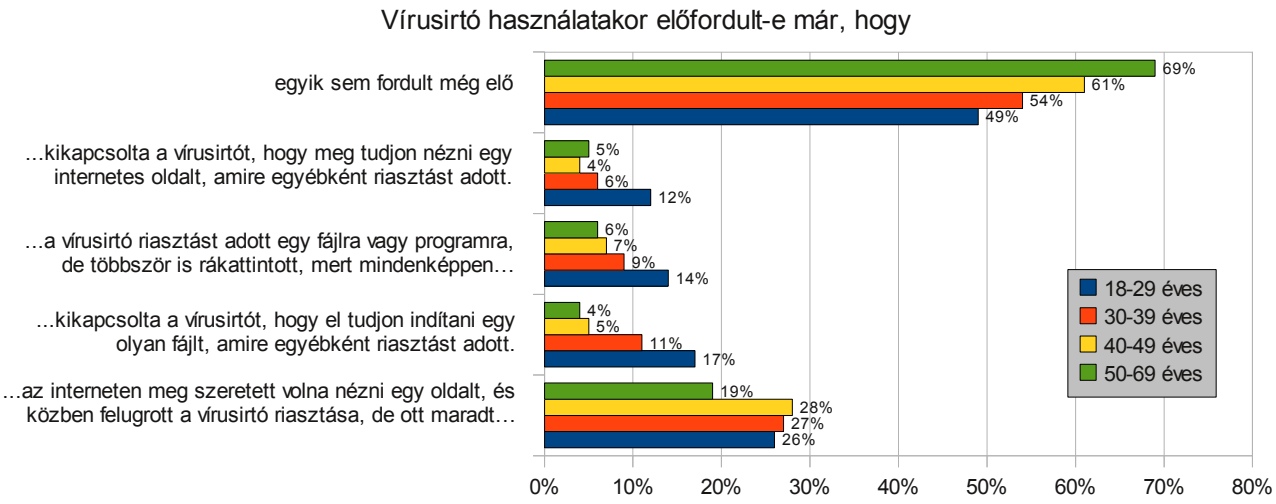
A vírusirtók hatékonysága

Az 1.2. fejezet statisztikái alapján örvendetes, hogy a lakossági felhasználók szinte teljes köre el van látva legalább az alapszintű vírusvédelmi megoldásokkal, 50%-uk pedig valamiféle tűzfallal (ezek hatékonysága igen változó, beletartoznak ebbe a körbe az operációs rendszerek beépített eszközei, a hálózati eszközök, útvonal-választók megoldásai, valamint a külön telepített célmegoldások) is rendelkezik.

Egy, az ESET megbízásából 2011. februárjában végzett piackutatás [4] a magyar internetezők viselkedését vizsgálta online kérdőíves felmérés segítségével, ahol a minta reprezentatív a 18-69 év közötti, legalább heti rendszerességgel internetezőkre nem, korcsoport, végzettség és lakóhelytípus szerint. A kutatás eredményeiből kiolvasható, hogy a magyar internetezők egynegyede a vírusirtó szoftverének riasztása ellenére is végignéz egy fertőzött weboldalt, ha annak tartalma érdekli.

A férfiak 15%-a ezenkívül ki is kapcsolja vírusirtóját, hogy el tudjon indítani egy fájlt, amit a biztonsági szoftver fertőzöttnek jelzett, míg a nőknek 6%-a tesz így. Különösen veszélyeztetettek a fiatalok. A 18-29 évesek 17%-a szokta kikapcsolni a vírusirtóját azért, hogy fertőzött fájlokat tudjon elindítani, 12%-uk pedig azért, hogy fertőzött weboldalakat látogathasson.

A vírusok készítői kihasználják az emberi kíváncsiságot és a monitor előtt ülő felhasználók téves biztonságérzetét. A felmérésünkből az is kiderült, hogy a legnagyobb veszélynek pont a tapasztaltabb internetezők vannak kitéve.



Ők azok, akik tévesen azt gondolják, hogy könnyedén tudják kezelni a veszélyeket, és azt is megengedhetik maguknak, hogy fertőzött weboldalakat látogassanak, vagy kikapcsolják a vírusirtót annak érdekében, hogy meg tudjanak nyitni egy fertőzött fájlt, a megfelelő számítógépes védelem alkalmazása mellett a felhasználóknak a felelősségteljes internet használatra is törekednie kellene.

A vírusirtó program jelzéseinek figyelmen kívül hagyása, vagy a biztonsági szoftver kikapcsolása jellemzőbb a férfiakra és a fiatalabb korosztályra (18-29 évesek), míg a legóvatosabb a legidősebb korcsoport (50-69 évesek). Egyetlen biztonsági szoftver sem védheti meg a felhasználókat, ha nem foglalkoznak annak riasztásaival.

Személyes adatok védelme és jelszóhasználat

Az ESET Software megbízásából az NRC által januárban elvégzett kutatás [5] bizonyította azt a vélekedést, hogy a magyar felhasználók jelentős része könnyen feltörhető jelszavakat használ. A legegyszerűbb jelszavakat a nők alkalmazzák. 27%-uk szimpla számsort vagy betűsort - mint a „levelezes” vagy az „123456” - használ jelszóként, míg férfiak esetében ez az arány 19%. Ugyanakkor a férfiak 36%-a már betűket és számokat (például „sanyi1982”, „baba12”) is alkalmaz jelszavában, míg a nőknek csak 31%-a teszi ezt meg. Kis- és nagybetűket a nők 18%-a, a férfiaknak pedig 24%-a használ.

Még a legkiválóbb vírusirtó használata mellett sincsenek biztonságban a felhasználók adatai és személyes dokumentumai, ha azokat egyszerű, könnyen feltörhető jelszavakkal próbálják védeni. A jelszavak feltörésére alkalmazott technológia fejlődése miatt az ideális jelszó ma már 10-12 karakter felett van, és egyaránt tartalmaz számokat, illetve kis- és nagybetűket, valamint egyéb írásjeleket (pl. a „Tomitom321-G” vagy a „PapusCant33;” már a jobb jelszavak közé tartozik. A szakértők szerint ugyanakkor nehezen feltörhető jelszavakat jelentenek a kifejezések is, az „ingyombingyomtáliber” vagy a „jajdejóahabossütemény” hosszúságánál fogva szintén az erős jelszavak közé tartozik. A kutatók eredménye szerint ilyen kifejezéseket a férfiak 3%-a, míg a nők 6%-a használ adatainak védelmére. A hölgyek emellett emlékezőképességüket tekintve is megelőzik az urakat, mivel míg mindössze 2%-uk nyilatkozott úgy, hogy nem tudja a jelszavát, mert azt a gép tárolja, a férfiaknak 4%-a állította ugyanezt.

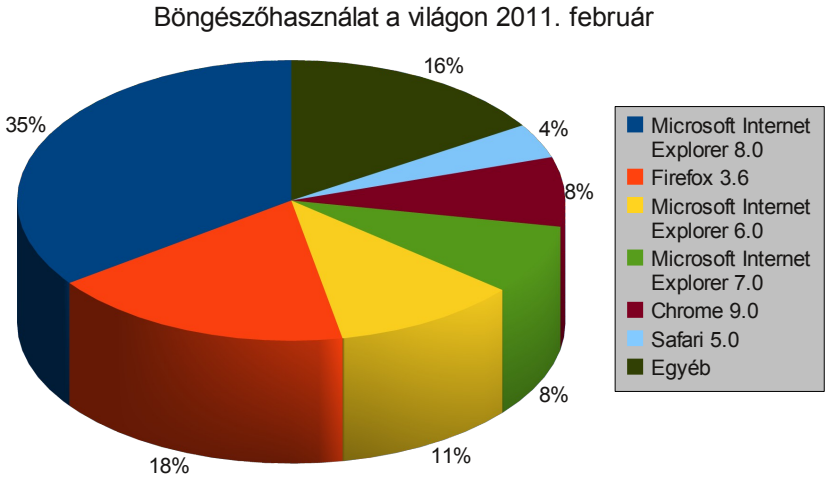
Eltérő a jelszóhasználat életkor szerint is. A többi korcsoporthoz képest a 18-29 évesek nagyobb arányban használnak kitalált szavakat („avager”, „taminor”), kifejezéseket adataik védelmére, míg az 50-69 közötti korosztály inkább tart elegendőnek egy egyszerű szót vagy számsort.

A budapesti lakosokra és a felsőfokú végzettségűekre jellemzőbb a kis és nagybetűk kombinált használata, míg a fővárosiakhoz képest a községekben lakók közül kétszer annyian választanak nehezebben feltörhető kifejezéseket adataik védelmére.

Az NRC által végzett piackutatás a magyar internetezők véleményét vizsgálta online kérdőíves felmérés segítségével, többszörösen rétegzett, véletlen mintavétellel. A minta reprezentatív a 18-69 év közötti, legalább heti rendszerességgel internetezőkre nem, korcsoport, végzettség és lakóhely-típus szerint.

Elavult böngészők

Tekintettel gyorsan változó világunkra, tíz év még egy autónál is sok, nemhogy egy számítógépes programnál. Ezek után talán nem is csoda, hogy a Microsoft azzal „ünnepelte" az Internet Explorer 6 (IE6) tizedik születésnapját, hogy világméretű kampányt kezdeményezett a régi böngésző lecseréléséért, s a nemes cél érdekében egy külön webhelyet is létrehozott. Az „IE6 visszaszámláló" oldalon láthatjuk a tízéves szoftver pillanatnyi világpiaci részesedését – februárban 12 százalékon állt –, sőt azt is, hogy egyes fontosabb országokban a netezők mekkora hányada ragadt le az IE6-nál. Jóllehet, már évek óta a 8-as verzió is ingyenesen letölthető, s nemrégiben már a 9-es kiadás is megérkezett, sokan még ma is az elavult 6-ossal vannak jelen a világhálón. [6]



Ilyen öreg járművel szörfözni pedig kimondottan felelőtlenség. Közel félezer ki nem javított biztonsági hiba van az IE6-ban, majdnem négyszer annyi, mint az összes többi böngészőben együttvéve.

Márpedig egy ilyen kiöregedett szoftver esetében az mindenképpen meglepő, hogy például Kínában a netezők 34,5 százaléka IE6-ot használ, de a koreai netezők mintegy negyede is az elavult böngészőt részesíti előnyben. Tíz százalék felett van ezt a verziót használók részesedése Indiában, Japánban és Vietnámban is – de ezen már nincs mit csodálkozni, ha hozzátesszük, hogy még a britek 3,5 vagy az amerikaiak 2,9 százaléka is az IE6-tal járja a világhálót. Az IE6 elterjedtsége szorosan összefügg a kalóz operációs rendszerek (Windows XP) használatával is, főleg a fejlődő világban, mivel a kalóz verzióhoz nem járnak az ingyenes frissítések, így az újabb böngészők sem jelennek meg a felhasználók gépein, sőt az IE6 korábban felismert hibáinak javításaival is sok esetben ugyanez a helyzet.

Magyarországról nem közöl adatot a Microsoft-site, de ezek után valószínű, hogy mi sem jeleskedünk az új verziókra való áttérésben. Ez pedig nem kis kockázatot jelent. A szakértők erősen javasolják, hogy aki még mindig IE6-tal navigál, váltson mielőbb!

Átalakuló SPAM

A Magyarországról februárban kiküldött emailek 85,5 százaléka számított levélszemétnek, ezzel az aránnyal negyedik az ország a világranglistában - derül ki a Symantec legfrissebb felméréséből [7].

A kéretlen reklámlevelek terén Kína vezeti a listát, az ország levélforgalmának 88,1 százaléka spam. Az Egyesült Államokban és Kanadában a levelek 81,4 százaléka számít kéretlen üzenetnek, míg Angliában ez az arány 81,1 százalék.

A jelentés szerint a világon minden 290. e-mail vírussal fertőzött, ez főként a károkozók egyidejű támadásának, ezen belül is a Zeus, a Bredolab és a SpyEye vírusoknak köszönhető. Az eddig

inaktívnak tekintett Bredolab vírus ismét életre kelt, és újra népszerű a károkozó programok körében. A múlt hónapban a MessageLabs szűrői a Bredolab trójai vírus 40 különböző variánsát azonosították, amelyek a felderített spamek 10,3 százalékát alkották.

Február első két hetében a MessageLabs Intelligence négy különböző alkalmazást is felfedezett, amelyek fő feladata a Zeus, Bredolab és a SpyEye vírusok struktúrájának átalakítása és különböző variánsok létrehozása volt.

Az elmúlt évben feltűnően elszaporodtak a PDF formátumba rejtett kártékony programok. Ez a formátum tűnik a legalkalmasabb vírushordozónak, 2009-ben a vírusok 52,6 százaléka használta ezt a módszert, míg 2010-re az arány 65 százalékra növekedett. Ha ez a tendencia továbbra sem változik, 2011-re a célzott támadások 76 százalékát alkotják majd a PDF-alapú vírusok.

Az internet történetében először, 2010-ben világszinten csökkent a levélszemét mennyisége (108 ezer milliárdról 100 ezer milliárdra). Ezen belül azonban a különböző régiók eltérő tendenciákat mutatnak: egyes fejlett országokban, ahol egyre nagyobb teret nyer a szélessávú internet, növekedett a spam mennyisége. Ugyanakkor néhány fejlődő országban jelentősen csökkent ez a szám annak köszönhetően, hogy több nagy és hírhedt botnetet sikerült leállítani, és az internetszolgáltatók is korlátozzák a szélessávú hálózatokból küldött rosszindulatú e-mailek forgalmát. A PC-platformok és alkalmazások gyártói számos biztonsági elemet építettek termékeikbe, és nagy figyelmet fordítottak a sérülékenységek kijavítására, így a csalók kénytelenek voltak más pénzszerzési lehetőségek után nézni.

A fejlett országokban a csökkenő tendencia 2008-ban kezdődött több rosszindulatú szerverhoszting és tárhelyszolgáltató, valamint néhány nagyobb zombihálózat lekapcsolásával. Bár ezek helyét gyorsan betöltötték a riválisok, a 2008-as csúcsértékeket már sosem érte el a mennyiség. Magyarországon is fordulópont volt a 2008-as év, de hazánkban ekkor éppen növekedni kezdett a hazai forrású kéretlen reklámok száma. Megváltozott a spamtörvény, már csak a magánfelhasználókat védte, a cégek info@ kezdetű fiókjaiba ettől kezdve legálisan lehetett reklámokat küldeni. A fellendülő címlistaüzlet és a tömegből kitűnni vágyó kis cégek nagy száma egyaránt hozzájárult ahhoz, hogy egyre több kéretlen levelet kelljen kezelniük a levelezőrendszereknek. Az alacsony - esetenként maximum 500 ezer forintos - büntetések ráadásul arra bátorították a drágább termékeket hirdetőket, hogy a várható büntetést a marketingköltségek részeként tartsák számon.

A legtöbb usernek fogalma sincs hány kéretlen levelet kap, a nagy levélkezelő hálózatok szűrői ugyanis észrevétlenül és nagy hatékonysággal dolgoznak. A teljes levélforgalom hetven és kilencven százaléka közé esik a spamek aránya iparági becslések szerint. Az arány volt már jóval nagyobb is, kilencvenöt százalék feletti. Ezeknek az üzeneteknek a nagy része el sem jut a spamszűrőig, már korábban elkapja őket a levelezési szolgáltató. Az első védelmi vonalon túljutó leveleknek még mindig majdnem a fele kéretlen reklám. A következő szűrő ennek tíz százalékát blokkolja, a fennmaradó 30 százalék pedig a felhasználó spam mappájában landol - oda is a szűrő küldi, de azzal az engedménnyel, hogy ennek spam-mivoltáról még dönthet a címzett.

A levélszemét özöne már csak a kisebb saját levelezőszervert üzemeltető cégek dolgozóit terheli. A beérkező üzenetek 60-65 százaléka levélszemét egy átlagos magyar kisvállalkozásnál. A havi körülbelül hatvanezer levél túlnyomó többsége szemét, amelynek nyolcvan százaléka az angolszász világból érkezik. A szemétnek csupán tíz százalékát küldik magyar címről, a fennmaradó tíz százalék pedig a világ többi országából érkezik. A rendszergazda dolgát a tiltólisták könnyítik meg, amelyek a spamek felét rögtön kiszűrik, csak a fennmaradó húsz százalékkal kell a helyi levélszemétszűrőnek dolgoznia.

Mindegy, hogy melyik nagy e-mail szolgáltatónál regisztrálnak címet a felhasználók, biztonságban lesznek a SPAM-től. A Gmail, a Hotmail és a Yahoo Mail egyaránt megvédi a levelezőket. Egy-két spam ugyan képes átcsúszni a szűrőkön, de a rendszer minden egyes hibájára több ezer megfogott reklámüzenet jut. Csupán a Hotmaillel kapcsolatban merültek fel felhasználó panaszok, miszerint a

védelmi rendszere túlzottan agresszív. A kéretlen üzenetek mellett hajlamos a tömeges hírlevélküldésre használt, ám legális üzenetek kiszűrésére is. Az ismerősöktől kapott, valódi tartalommal rendelkező leveleket pedig egyik szolgáltatónál sem fenyegeti veszély.

E tendenciák miatt az internetes csalók, akik korábban SPAM küldésben „utaztak", kezdenek átköltözni a közösségi hálózatokra. A közösségi hálózatok belső üzenetküldő rendszerei szolgáltatásaikban egymást túllicitálva, rohamléptekben fejlődnek, viszont az üzenetek tartalmi szűrésére - az egész üzleti-kommunikációs modelljük alapelveiből kifolyólag – egyszerűen nincsenek felkészülve, nincsenek megfelelő biztonsági protokollok. Másrészt a hagyományos e-mail alapú csalás is nagyobb eséllyel csúszik át a szűrőkön, sőt a felhasználó józan ítélőképességén is, ha megfelelő környezettanulmány után, kellően személyes hangvételt sikerül megütni. Ehhez pedig a közösségi oldalakon található profilinformációk szolgáltatják az elsődleges inputot. Az ismerősi hálózat letapogatása a BotNet hálózatokat kialakító rosszindulatú adathalász szoftverek feladata, amelyek, ha sikerrel járnak, már el is árasztják ismerőseinket a látszólag tőlünk érkező üzenetekkel. 2011 elején a Cisco kutatói szerint a közösségi üzenetek mintegy 24%-a volt SPAM.

Közösségi oldalak

Már a fentiekből is látszik, hogy a közösségi oldalak válnak az informatikai biztonsági küzdelem egyik legfőbb színterévé, főként ha a privát felhasználókról van szó. (Amely természetesen nem különíthető el élesen a munkahelyi, iskolai, stb. felhasználástól, mivel alanyai megegyeznek.) A közösségi oldalak kockázataira számos forrás világít rá egyre erőteljesebben, ezek közül az egyik legátfogóbb a Cisco éves biztonsági jelentése [8].

A technika egyszerű, ha a felhasználót valamilyen érdekes képpel, hírrel, tartalommal sikerül rávenni arra, hogy lájkoljon egy rosszindulatú oldalt, az oldal gazdája innentől kezdve üzenetet küldhet a felhasználónak újabb hírekről, eseményekről, amelyek többsége már adathalász, vagy más rosszindulatú kódokat fog tartalmazni. Az ügyfelek nagy része ellenáll az ilyen kísértéseknek, a felhasználó kör 3%-a viszont rendszeresen és meggondolatlanul kattint és lájkol mindent, ezzel pedig, bár a 3% nem tűnik kiugróan magas számnak, fontos lyukakat üt a vállalata, az otthona vagy a ismerősi köre biztonsági falain. Így nemzetgazdasági szempontból ez a csoport jelentős kockázati tényezőnek tekinthető. Épp ezért egyre fontosabbá válik a közösségi oldalak mind szabályozottabb használata és a belső biztonsági intézkedések – minden bizonnyal felhasználói szabadságot csorbító – szigorítása.

A hamis profilok, a bizalomba férkőzés, a „social engineering" típusú csalások terjedése szintén felhívja a figyelmet a közösségi oldalak felelőtlen használatának veszélyeire. Az ilyen csalók a meggondolatlan visszajelölések révén valós „baráti körre" tesznek szert az oldalakon, amely mintegy legitimálja, hitelesíti alteregójukat, amit természetesen céljaiknak megfelelően alakítanak ki. Azután megkezdik munkájukat az ismerősi körön belül, ahol már senki nem emlékszik rá, hogy az említett szimpatikus felhasználó hogyan került az ismerősi körébe, de ha az összes ismerőse, ismeri, nagy baj biztosan nem lehet. Az így érkező üzleti ajánlatok, segítségkérés felé mindenki nyitottabb.

Mobilizálódó kockázatok

A Cisco jelentés [8] több más kutatóval egyetértésben szintén kiemeli, hogy fordulóponthoz érkezett az internetes bűnözés. Míg korábban a cyberbűnözők a Windows alapú PC-ket támadták nagy vehemenciával, addig ma a támadások kereszttüzébe egyre jobban más operációs rendszerek és a különféle mobilplatformok kerülnek. A trend megfordulásának okát abban kell keresni, hogy a PC-s operációs rendszereket az elmúlt évtizedben ért támadások kivédésére a PC-platformok és alkalmazások gyártói számos biztonsági elemet építettek termékeikbe, és nagy figyelmet fordítottak a sérülékenységek kijavítására, így a csalók más pénzszerzési lehetőségek után néznek. E tendencia

másik lényeges oka a mobileszközök és -alkalmazások széles körű elterjedése. Különösen a külső fejlesztőktől származó mobil alkalmazások jelentenek komoly kockázatot. Az ITU adatai szerint 2011 elején mintegy 5 milliárd mobil előfizetés volt aktív a világon, ebből 3,8 milliárd a fejlett országokban, ahol a lefedettség, szinte 100%-os, de a fejlődő világban is elérte a 68%-ot.

A MacOS, az iOS és az Android eddig túl kis falat volt a csalók számára, ám a trendek rohamosan változnak.

Az Android alapvetően szabad fejlesztésű nyílt rendszere sok kockázatnak teszi ki a felhasználót, főleg hogy az okostelefonok egyre inkább személyes adataink első számú tárházává lépnek elő. A rendszer robbanásszerűen terjed és fejlődik, nagy szabadsága viszont sok ellenőrizhetetlen vadhajtást is szül. Az elsőszámú kockázatot az adathalászati funkciókat tartalmazó, látszólag hasznos, vagy érdekes alkalmazások, amelyek segítségével a bűnözők hozzáférhetnek a telefonban, vagy tableten tárolt információkhoz, kontaktokhoz, sőt egyes esetekben a GPS ellenőrizetlen aktiválása révén a felhasználó mozgása is követhető általuk.

Az iOS zárt rendszere ebből a szempontból biztonságosabb lenne, de a felhasználók ezt a korlátozást tudatosan megkerülik az operációs rendszer feltörésével (jail break), hogy külső fejlesztésű alkalmazásokat is telepíthessenek eszközeikre, illetve, hogy tetszőleges hálózatokon használhassák azt, ehhez azonban ki kell iktatni az operációs rendszer számos védelmi modulját, ami így fontos támadási felületet eredményez.

Az IT biztonsági iparág lassan reagál az új fenyegetésre, a PC-kéhez hasonlóan szofisztikált, ám az okostelefonok erőforrásaihoz szabott biztonsági megoldások, szoftverek, még nem terjedtek el tömegesen, nincs is akkora választék a piacon, mint a hagyományos gépek esetében. A telefonok egyre gyakrabban csatlakoznak az otthoni és nyilvános hálózatok mellett a munkahelyi hálózatokra is, így a kockázatok egyértelműen eszkalálódnak a vállalti és kormányzati szektor irányába, még fontosabbá téve a védekezést.

Gyerekek a hálózaton

A digitális technológiák fejlődésével és terjedésével párhuzamosan egyre fontosabbá válik annak a vizsgálata, hogy megértsük a gyermekekre és a családokra leselkedő veszélyek és kockázatok komplex természetét. Egyre több kutatás veszi górcső alá a gyerekek, mint a legfogékonyabb és a neten legtöbb időt eltöltő korosztály sajátos problémáit, kockázatait. Ennek érdekében 2009 - 2011 között az EU Kids Online II projekt [9, 10] keretében átfogó európai vizsgálat zajlik a 9 és 16 év közötti fiatalok, illetve szüleik részvételével. A projekt célja, hogy nemzetközi viszonylatban is összehasonlítható adatok álljanak rendelkezésünkre az európai gyermekek internethasználati szokásaival kapcsolatban. E kutatás néhány eredményét láthatjuk az alábbiakban kombinálva a Norton Online Family kutatás [11] legfrissebb eredményeivel.

Internet és közösségi oldalak

A magyar 9 és 16 év közötti internethasználó gyermekek európai uniós összehasonlításban átlagosnak tekinthetők a használat gyakorisága szempontjából. A magyar gyermekek közel háromötöde (58%) naponta, egyharmaduk (35%) heti egyszer-kétszer, 7 százalékuk ennél is ritkábban használja az internetet. A magyar gyermekek - ugyancsak az EU-átlagnak megfelelően - átlagosan 9 éves korukban kezdik el használni a világhálót.

A 25 európai ország 9-16 éves nethasználó fiataljai közül a magyaroknak van a legtöbb ismerőse valamelyik közösségi oldalon (pl. Iwiw, Facebook). A magyarok 45 százaléka 100-nál is több visszaigazolt kapcsolattal rendelkezik - ezt csak Nagy-Britannia (43%) közelíti meg, míg az uniós átlag mindössze 29 százalék. A bejelölt kapcsolatok számától függetlenül is átlagon felüli közösségi aktivitást mutatnak a magyar netező gyerekek: kétharmaduknak van saját profilja valamelyik közösségi oldalon.

Az internetező magyar 11-16 éves gyermekek ugyanakkor az uniós átlagnál valamivel gyengébb készségekkel rendelkeznek a digitális írástudásra és a biztonságos internet-használatra vonatkozóan: a magyar 2,7-es érték ugyan látszólag nem sokkal marad el a 25 ország 3.1-es átlagától, azonban Magyarország ezzel az eredménnyel - Olaszország (2,6), Románia (2,6) és Törökország (1,9) után - mégis hátulról a negyedik csupán a sorban.

A magyar netező 11-16 éves fiatalok európai összehasonlításban kevéssé tapasztalják a túlzott internet-használat jeleit: ritkábban érzik úgy, hogy az internetezés a családi és baráti együttlétek, az evés vagy az alvás rovására menne, emellett kevésbé tapasztalják a net hiányára visszavezethető zaklatottságot. A túlzott internethasználatnak a kutatásban vizsgált megnyilvánulásai közül legalább egyet a magyar válaszadók ötöde (20%) tapasztalt magán gyakran - ez a 25 ország átlagának (30%) csupán csak a kétharmada. Ennek alapján a túlzott netezés a magyar gyerekeknél csak az olaszokra (14%) jellemző kevésbé Európában.

Az interneten keresztül megvalósuló zaklatásban (bullying) a 9-16 éves magyar internetező gyermekeknek és fiataloknak az uniós átlagnak megfelelő mértékben volt részük az elmúlt egy év során: 100 megkérdezettből 6 tapasztalt ilyet. A szülők száz esetből azonban mindössze négyben (4%) tudnak a gyermeküket ért online zaklatásról - ebben viszont Magyarország sereghajtónak bizonyult az Unióban. Ez az arány a kontinens 25 országában átlagosan ugyanis majdnem egyharmad (30%).

Hasonló a helyzet a weben látható szexuális tartalmakkal: a mintába került magyar gyermekek az EU-átlagnak (13%) megfelelően találkoztak ilyesmivel (11%) az elmúlt egy évben, szüleik közül azonban fele annyian tudnak minderről (10%), mint Európa többi részén (22%).

Összességében a kutatás adatai alapján megállapítható, hogy Magyarországon a vizsgált korosztály az internethasználat alapmutatóiban nem tér el jelentősen az uniós átlagértékektől. Ugyanakkor a digitális írástudás minőségi mutatóiban a magyar gyermekek inkább átlag alatti értékekkel jellemezhetők, továbbá fontos, hogy a szülői kontroll és támogatás hazánkban jóval átlag alatti.

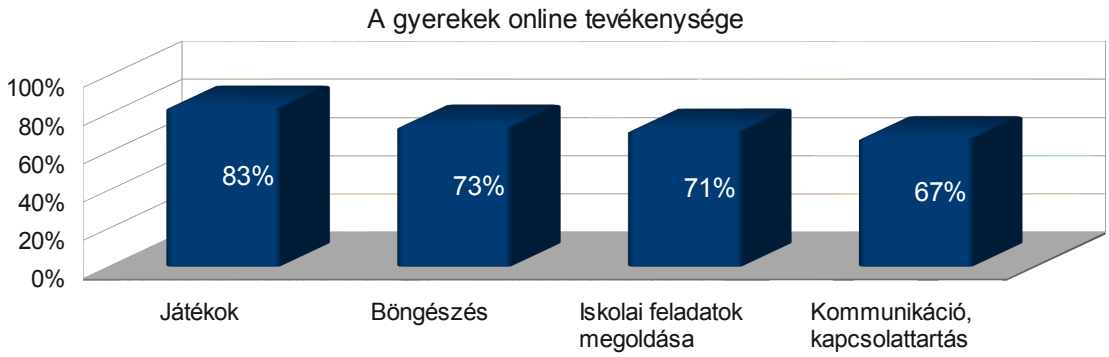
Szabályok és biztonság

Örvendetes, hogy a kitettség, a kockázatok kezdenek megfelelően tudatosodni, mind a szülőkben, mind a gyerekekben és a legtöbb család fontos szabályokat, lépéseket tesz a biztonságos internethasználat irányába.

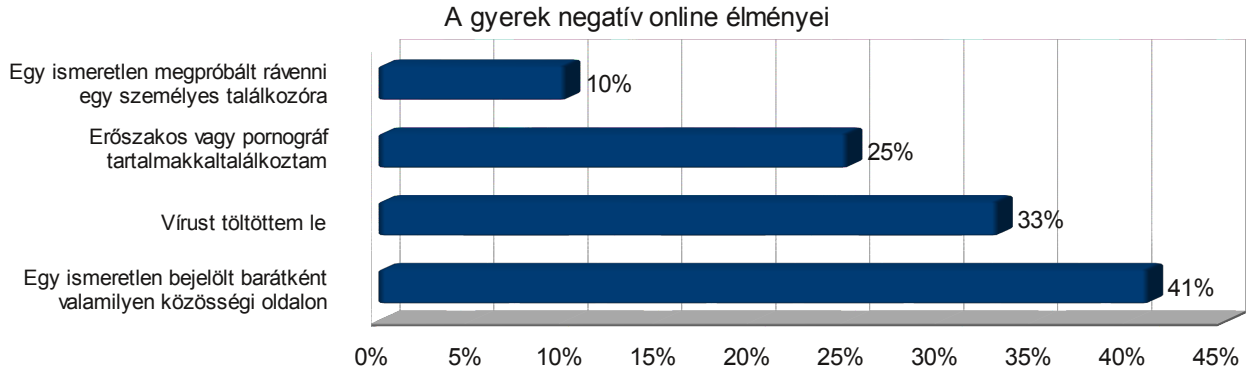
Természetesen a szülői kontroll a gyerekek online tevékenysége fölött nagyban függ az adott ország kultúrájától, valamint a szülők digitális képzettségi szintjétől, hiszen csak akkor tudnak ellenőrzést gyakorolni, ha maguk is értik, mit csinálnak a fiatalok az online környezetben. Ebből a szempontból hazánk nincs túl jó helyzetben, ahogyan a digitális középosztályról szóló fejezetben látható, főként a tinik és a fiatal felnőttek vannak az IKT képzettségnek olyan szintű birtokában, amely lehetővé teszi ezt az ellenőrzést, ez a korosztály viszont jórészt még gyermektelen. Ez azt is előrevetíti, hogy a folyamatos generációváltás ebben az ellenőrzésben is jelentős fejlődést fog hozni, és a Magyarországon is érvényesek lesznek a fejlettebb, a digitális úton előbbre járó országokban már megtapasztalt tendenciák.

A legnagyobb probléma a szülői kontrollal, hogy míg a gyermekek 2/3-a számolt be valamilyen negatív élményről, ami az interneten érte őket, ezzel mindössze a szülők 45%-a van tisztában, tehát egy erős 20%-os ollóról beszélhetünk, ahol a gyerekek segítség nélkül kell, hogy kezeljék a problémákat.

Az átlag gyerek napi 1,6 órát tölt online, ami az előző év hasonló adataihoz képest 10%-os emelkedést jelent. Meglepő módon, maguk a gyerekek is soknak tartják ezt, 48%-uk vélekedett így. A szülők 52%-a nincs minden esetben tisztában azzal, hogy a gyermekük, mit csinál az interneten. 5%-uknak pedig saját bevallásuk szerint közelítő fogalma sincs erről, a gyerekek szerint viszont a szülők 20%-a tartozik ebbe a csoportba.



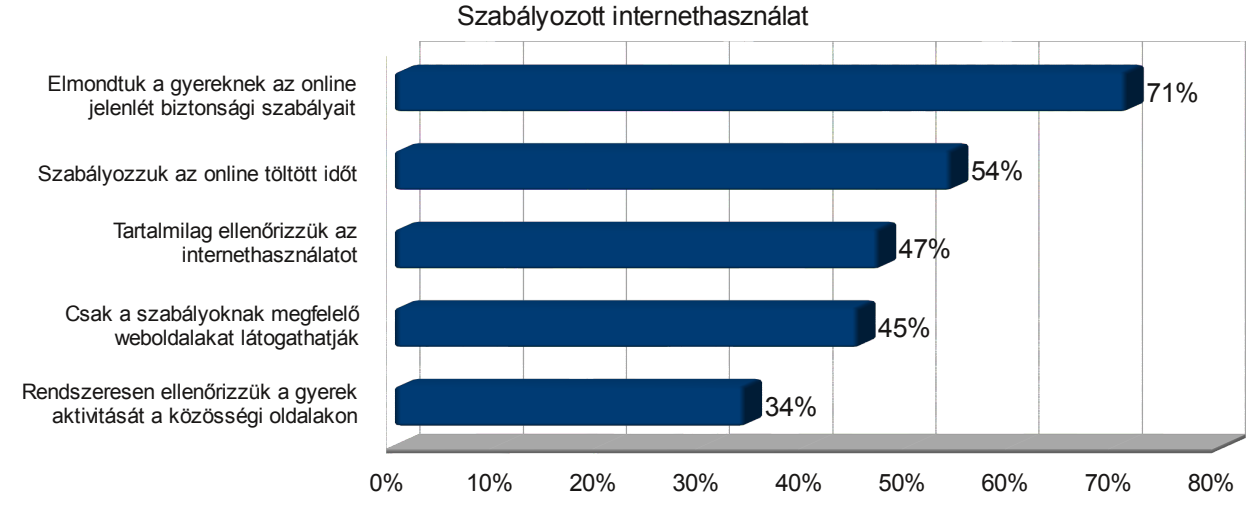
A gyerekek 62%-a találkozott már egyébként valamiféle negatív élménnyel internethasználat közben, amelyek palettája a hagyományos elektronikus kártevők letöltésétől az idegenek által való megkörnyékezésig széles skálán mozog. Lényeges, hogy a szülői tudatosság kb. 20%-os ollója itt is jelen van, hiszen a szülőkkel mindössze a gyerekek 45%-a osztotta meg negatív élményeit.



Ezek az élmények érzelmileg is megviselik a fiatal felhasználókat, igen sokan hibáztatják magukat, dühösek vagy szégyenkeznek a negatív események bekövetkezése miatt. Sokszor akkor is, ha valójában nem az ő hibájuk, ami történt.

Szerencsére a gyerekek többsége bízik a környezetében, több, mint 80%-uk jelzi, ha valamiféle atrocitás éri őket a neten, 70%-uk pedig a szerintük nem helyénvaló, gyanús dolgokra is felhívja a szülők figyelmét. Jellemző erre a digitálisan már „bennszülött” generációra, hogy 48%-uk úgy érzi: óvatosabbak és tudatosabbak az online világban, mint a szüleik. 51%-uk szülői felügyelet nélkül tölthet le tartalmakat (főként játékokat, zenét) az internetről, ebből is látható hogy a biztonság tudatosítását nem lehet elég korán megkezdeni a felhasználók legifjabb generációjánál.

Persze ehhez az is kell, hogy a szülők is meg akarják védeni a gyerekeiket, és ez a legtöbb esetben így is van, az esetek 90%-ában családi szabályok vonatkoznak az internet használatra, és a gyerekek 90%-a saját bevallása szerint be is tartja ezeket.



A kockázatok és a mélyebb megértés következtében a gyerekek örvendetes módon belső szabályokat is kialakítanak maguknak, amelyekhez konzekvensen tartják magukat online jelenlétük során. E szabályok főként a személyes adatokhoz és a magánélet védelméhez tartoznak, ebből is látható, hogy az új felhasználói generáció tudattalanul is ezeket tartja a legfőbb problémának. A legfontosabb szabály a többiek online zaklatását tiltja (68%) és támogatja, hogy áldozattá válás esetén minél gyorsabban felnőtt segítségét kell kérni (67%), a gyerekek 60%-a tartja fontosnak, hogy senkiről ne tegyen fel megalázó tartalmat, fényképet a hálózatra, 55%-uk pedig már a SPAM-ek elleni védekezés fontosságával is tisztában van.

A biztonságtudatosság más területeken is megjelenik: a gyerekek 70%-a tisztában van a jelszavaik védelmének fontosságával, 40%-uk pedig kifejezetten bonyolult jelszavakat használ és rendszeresen cserélik is. 60%-uk tisztában van az ismeretlen e-mailek megnyitásának veszélyeivel, 33%-uk pedig a felugró ablakok és a bannerek veszélyeit is ismeri. A „túl szép ahhoz, hogy igaz legyen” típusú ajánlatokat is 30-40%-uk kapásból gyanakodva kezeli.

A közösségi oldalakon némileg azonban lazábban kezelik a gyerekek még saját biztonsági elveiket is. A közösségépítő weboldalakat használó gyermekek egynegyede úgy nyilatkozott, hogy a profilja nyilvános. A nyilvános profillal rendelkező gyerekek egyötöde azt a választ adta, hogy a profilon látható a címe és/vagy a telefonszáma. A 25 országból 15-ben a 9–12 évesek körében jobban elterjedt a nyilvános profil, mint a 13–16 évesek körében.

A 11–12 évesek mindössze 56 százaléka nyilatkozott úgy, hogy tudja, hogyan kell módosítani profilja adatvédelmi beállításait. A náluk idősebb fiatalok már nagyobb hozzáértéssel rendelkeznek: a 15–16 évesek 78 százaléka mondja azt, hogy tisztában van az adatvédelmi beállítások módosításának mikéntjével.

Tanácsok szülők számára

A szülő felelőssége, hogy

- meggyőződjön arról, van biztonsági szoftver telepítve a gépre és az megfelelően aktív és frissül,
- megtanítsa a gyereknek a biztonsági szoftver használatát, üzeneteinek értelmezését,
- megfelelő tartalomszűrő alkalmazások telepítésével védje a gyereket a káros tartalmaktól.

A szülő könnyen ellenőrizheti a gyerek online tevékenységét

- a böngésző történetből,
- illetve speciális monitoring alkalmazásokon keresztül (ezek általában részét képezik a gyerekek védelmét szolgáló tartalomszűrő csomagoknak).

A beszélgetés és a gyerek felhatalmazása bizonyos döntésekre sokkal hatékonyabb, mint a kategorikus tiltás

- ha a gyerek megérti, hogy egyes cselekedetei milyen hatással lehetnek rá, illetve a családra, könnyebben elfogadja a szabályokat,
- sokat kell beszélgetni és létrehozni a családi szabályzatot, amihez mindenki tartja magát.

A közösségi oldalakon

- csak olyanokat jelöljön be a gyerek, akiket tényleg ismer,
- a szülő adassa magát ismerősként a gyereke profiljához, hogy láthassa a belső tartalmakat is,
- ha az online ismerősök közül valaki személyes találkozót kér, azt a gyerek azonnal jelezze,
- mindig kísérjük el a gyereket egy ilyen találkozóra.

Nagyon fontos, hogy a gyerek megbízzon a szülőben, ezért hallgassuk meg és vegyük komolyan, ha problémát, negatív tapasztalatot akar megosztani.

Fontos a szabályok kijelölése, de a teljes tiltás nem célravezető, a gyerekek, sok esetben nagyobb tapasztalatuknak köszönhetően meg fogják keresni a kiskapukat, vagy nem otthonról csatlakoznak a hálózatra, így a bizalom elvesztése mellett a kontroll is csökken.

Források

[1] Bellresearch: Magyar Infokommunikációs Jelentés 2010.

[2] Információs Társadalom és Hálózatkutató Központ (Ithaka): Digitális Média Riport 2010. http://www.upc.hu/pdf/ITHAKA_UPC_kutatas.pdf

[3] Mártonffy Attila: Így bankolunk mi, 2011.03.08. http://www.itbusiness.hu/hirek/legfrissebb/igy_bankolunk_mi.html

[4] Csizmazia István: Hát, ha csak úgy nem, 2011.04.06. http://antivirus.blog.hu/2011/04/06/hat_ha_csak_ugy_nem

[5] IT Cafe: A nők egyszerűbb jelszavakat használnak, 2011.02.17. http://itcafe.hu/hir/magyar_internetezok_jelszavakat_felmeres_eset_nrc.html

[6] Miski Gábor: Nem csak ciki az öreg böngésző 2011.03.12. http://www.itbusiness.hu/hirek/legfrissebb/Veszelyes_az_oreg_bongeszo.html

[7] Symantec: The State of SPAM and Phishing Report 2011.03 http://www.symantec.com/.../b-state_of_spam_and_phishing_report_03-2011.en-us.pdf

[8] Cisco 2010 Annual Security Report http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf

[9] EU-London School of Economics and Political Science (LSE): Risks and safety on the internet: The perspective of European children - Full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries Risks and safety on the internet, 2011.01.13. ISSN 2045-256X http://www2.lse.ac.uk/.../EUKidsOnlineIIReports/D4FullFindings.pdf

[10] EU-LSE: EU Kids Report II. magyar nyelvű vezetői összefoglaló http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsII%20(2009-11)/EUKidsExecSummary/HungaryExecSum.pdf

[11] Norton Online Family Report: Global insights into family life online 2010., http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/nofr/Norton_Family-Report-UK_June9.pdf

A bűnelkövetés és áldozattá válás együtthatói informatikai környezetben

Szükségesnek találtuk, hogy mostantól fogva ne csak az IT biztonsági és kockázati kérdésekről nyújtsunk tájékoztatást, hanem mindazon jogi háttérről és szükséges ismeretekről, amelyek az informatika világában való mindennapi létezéshez, túléléshez fontossá váltak.

Új rovatunk első témájaként azt járjuk körül, hogy a büntető eljárásjog és anyagi jog milyen módon függ össze az online világ mindennapos eseményeivel, hogy mit lehet tenni az online világban minket érő támadásokkal szemben, vagy olyan esetben, mikor virtuális szemtanúi leszünk olyan eseményeknek, melyek veszélyesek lehetnek ránk, vagy a társadalom bármely tagjára.

Internetes önvédelem, tudatosság növelés

Szakértelemtől, informatikában való jártasságtól függetlenül az Internet egy olyan világot nyújt számunkra, ami semmiben sem különbözik egy zsúfolt belvárosi éjszakától. Vannak egyértelműen széles, kivilágított utcák, ahol tudjuk, semmi bántódásunk sem eshet, és ott vannak mellette azok a kis utcák, sikátorok, ahol, ha nem vigyázunk, bármi megtörténhet. Szükséges tehát, hogy megtanuljuk magunkat megvédeni.

Az EMC biztonsági divíziójának, az RSA-nak 2011. áprilisban megjelent kutatásából kiderül, ebben az évben nemhogy csökkenne a számítógépes bűncselekmények száma, hanem új fenyegetésekkel is szembe kell néznünk. Nem elég, hogy évről évre döbbenetes mértékben növekszik az informatikai környezetben elkövetett bűncselekmények száma, de sokkal okosabb elkövetési módszerekkel kell megküzdenünk.[1] Az RSA-hoz beérkezett jelentések szerint ebben az évben mintegy 181 országban 321 millió online támadást vertek vissza. Ki kell jelentenünk azonban, hogy ezek csak a felfedezett és sikeresen visszavert támadások, ennek sokszorosa lehet azon támadások száma, melyek sikeresek voltak és még csak fel sem ismerték őket.

A jelentés kitér rá, hogy 2011-ben új típusú malware programok[2], és ezek révén a számítógépes bűncselekmények új hullámát az okostelefon tulajdonosok lesznek kénytelenek elszenvedni. Az okostelefonok, Android, Windows Phone 7 és iOs mobiltelefon platformokat már nem lehet élesen elválasztani az asztali számítógépek által használt operációs rendszerektől, továbbá az új telefonok által használt processzorok és chipkészletek sok esetben megegyeznek az elmúlt években a netbookokban használtakkal. Az okostelefonokra 2010-ben letöltött programok számából kiindulva 2011-re a jelentés közel a dupláját prognosztizálja, megközelítőleg 25 milliárd letöltést. 2011 elején már visszavontak több mint 50 programot az Android Marketből[3], miután bebizonyosodott róluk, hogy kártékony kódot tartalmaznak.

A használt eszközöktől független viszont, hogy milyen informatikai bűncselekményeknek lehetünk áldozatai. Miután online üzemmódba váltottunk, és beléptünk a kibertérbe (legyen szó bármilyen eszközről), számolnunk kell az esetleges veszélyekkel és felkészülnünk arra, hogy erre milyen választ adhatunk.

Jogi szempontból fontos meghatároznunk, hogy az adott bűntett kapcsán az informatika milyen szerepet játszik. Az informatikai szakzsargonban használt, tipikusan informatikai bűncselekményeknél sok esetben maga az elkövetési magatartás és az elkövetés tárgya egy már régóta létező bűncselekmény típus, viszont az internet és a számítástechnika megjelenésével új megvalósulási módot talált magának.

---

1 „RSA 2011 cybercrime trends report The Current State of Cybercrime and What to Expect in 2011”, www.rsa.com

2 Az angol malware kifejezés a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszer működését láthatatlanul ellenőrző rootkitek.

3 Forrás: http://nonstopmobil.hu/karelharitasba-kezdett-a-google-20110306.html

Akkor beszélhetünk kifejezetten informatikai bűncselekményekről, mikor az adott bűncselekmény kizárólag informatikai környezetben tud megvalósulni, anélkül nem értelmezhető.

Hatályos jogi szabályozásunk az interneten naponta megvalósuló, a felhasználók által sérelmesnek érzett élethelyzetekre nem tud mindig adekvát választ adni, mivel sok esetben az adott cselekmény jogilag nehezen kategorizálható illetve olyan új elkövetési magatartást valósít meg és olyan jogtárgy sérül, amivel korábban a jogalkotó még nem találkozott.

Az alábbi táblázatban olvashatóak az egyes informatikai környezetben megvalósuló bűncselekmény típusok és egyéb visszaélések magyar jogban való megfeleltetéseik, néhány példával bemutatva:

Pedofil oldalak	Btk. 204.§. Tiltott pornográf felvétellel való visszaélés
Internetes Zaklatás, chates zaklatás	Btk. 176/A.§ Zaklatás
Uszító, rasszista oldalak	Btk.269.§ Közösség elleni izgatás Btk.269/B.§ Önkényuralmi jelképek használata, Btk.269/C.§ A nemzeti szocialista és kommunista rendszerek bűneinek nyilvános tagadása
Drogfogyasztásra csábítás	Btk.282/A. § Visszaélés kábítószerrel
Hack, Crack	Btk. 300/C.§ Számítástechnikai rendszer és adatok elleni bűncselekmény, Btk. 300/D.§ - Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása
Számítógépes vírusok terjesztése, készítése	Btk. 300/C.§ Számítástechnikai rendszer és adatok elleni bűncselekmény, Btk. 300/D.§ - Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása
Phising, adathalászat, klikkes csalás,	Btk. 318.§ Csalás
Adattal, képmással való visszaélés	Ptk.80.§ (1), Személyhez fűződő jogok megsértése

Ahogy a felsorolásból is látható, sok esetben ami tipikusan számítógépes bűncselekménynek látszik, azok valójában teljesen “átlagos” bűncselekmények, csupán lehetővé vált internetes elkövetésük is. Különbséget egyedül a Számítástechnikai rendszer és adatok elleni bűncselekmények jelentenek, ahol valóban olyan az elkövetési tárgy és magatartás ami szorosan kötődik a számítástechnika világához, annak létezése nélkül elkövetése lehetetlen volna, az informatika létezése teremtette meg ezt a bűnelkövetési formát.

Vírusirtóktól és megbízható rendszerektől függetlenül a legfontosabb az a tudatosítás és önképzés, amit az internet biztonságos használata megkövetel a felhasználótól. Autodidakta képzésre szorítja rá az azt használókat és megteremti a közös, egymástól tanulás lehetőségét.

Ennek segítésére rengeteg idegen és magyar nyelvű oldal található a világhálón, ezek közé tartozik pl. a www.biztonsagosinternet.hu is, ahol lehetősége van minden ez iránt érdeklődőnek olyan információhoz jutnia, ami képessé teszi az egyes, fentebb említett veszélyek felismerésére.

A következő lépés…

A számítógépes bűncselekmények áldozatává váláshoz nem szükséges tudnunk azt, hogy minek estünk áldozatul, elég az az egészséges jogérzet, hogy valaminek sértettjei lettünk. Sok esetben nem is az elkövetéskor döbbenünk rá arra, hogy történt valami, hanem akár hetekkel, hónapokkal később (pl. számítógépes vírusok, adatlopás, hacker betörés).

Arra viszont fontos felkészülnünk, hogy hova fordulhatunk, mit tehetünk ilyen esetekben. Az új bűnözési trendekkel párhuzamosan a rendőrségnek is szembesülnie kellett azzal, hogy egyre többen fordulnak hozzájuk olyan bűncselekményi és részben bűncselekményi kategóriába eső bejelentésekkel, amire a hatályos jog nem minden esetben tud adekvát választ adni, és napi szinten kell találkozniuk jogértelmezési kérdésekkel.

Nem csak az volt kérdéses, hogy a fentebb említett, egyes újdonságként megjelenő cselekmények milyen Btk. szerinti kategóriába esnek bele, hanem hogyan értelmezendőek az informatika robbanásával előállt új eljárásjogi helyzetek.

Példának okáért, amíg korábban személyesen vagy postai úton volt lehetséges feljelentést tenni, addig ez most már e-mail útján is lehetővé vált. Kérdésként merült fel, hogy a névtelen feljelentések tételének ez az új módja nem vonja-e magával annak a lehetőségét, hogy névtelen feljelentések tucatjai lepik-e majd el a rendőrséget, megbízhatatlanabbak-e az ilyen módon kapott információk mint a hagyományos feljelentéseknél, feljelentés kiegészítésének szükségessége esetén lenyomozhatja a rendőrség az e-mail cím tulajdonosát, ha az névtelenül tette a feljelentést, valamint fontos megvizsgálni azt a hálózatbiztonsági kérdést is, hogy a rendőrség rendszerébe beérkező és ott megnyitott elektronikus üzenet akár tartalmazhat olyan rejtett malware programot is, ami a Stuxnethez hasonlóan támadást készít elő.

Alapesetben, mikor valaki feljelentést tesz, megadja a nevét és elérhetőségét abból a célból, hogy ha esetleg később a rendőrségnek még információra lenne szüksége, tudja hogy kit kereshet meg. Az e-mailen tett feljelentések nem feltétlenül köthetőek a bejelentőhöz, így a Büntetőeljárásról szóló törvény (továbbiakban Be.) 172/A §. szerinti feljelentés kiegészítése sem rendelhető el. Az e-mailen tett, névtelen feljelentések eljárásjogi sorsa legtöbb esetben az, hogy azt rendőrség, mint saját hatáskörben észlelt bűncselekményként értékeli és ennek megfelelően is jár el. Ilyen esetekben nem köti őket a feljelentés eljárást kiváltó hatása, és csak abban az esetben kezdeményeznek eljárást, ha a gyanút megalapozottnak találják. A hivatalosan tett feljelentéstől ez különbözteti meg, egyéb esetben a rendőrség köteles lenne eljárást indítani.

Mit tehet a jó szándékú állampolgár?

Bűncselekmények gyanúja esetén a nyomozó hatáskörrel felruházott szervezet Magyarországon a rendőrség. A hatályos szabályozás szerint még a titkosszolgálatoknak sincs nyomozási hatáskörük, kizárólag a rendőrség van ezzel a jogosítvánnyal felruházva.

A számítástechnikai rendszerek útján megvalósuló bűncselekményekkel kapcsolatban alapvetően az elkövetés helye szerint illetékes rendőrkapitányság járhat el, viszont a Nemzeti Nyomozó Iroda, Csúcstechnológiai Bűnözés Elleni Osztálya országos hatáskörrel rendelkezik az ilyen ügyekkel kapcsolatosan. Alapesetben azonban a helyi rendőrkapitányságon kell a feljelentést megtenni, és az adott üggyel kapcsolatos hatáskör és illetékességi kérdéseket az adott rendőri szerv hivatalból megvizsgálni köteles, és ezt követően továbbítja majd a feljelentést az arra hatáskörrel, illetékességgel rendelkező szerv felé.

Miért foglalják le a bejelentő, feljelentő adathordozóit, ha informatikai környezetben megvalósult bűncselekménnyel kapcsolatban tesz feljelentést?

A hatályos jogi szabályozás értelmében, egyes bűncselekmények esetében nehéz meghatározni, hogy az azt bejelentőnek milyen kapcsolata van a bejelentésben foglaltakkal, így a jogi szabályozás szigorúan vett értelmezése szerint a rendőrségnek nincs más lehetősége, mint a jóhiszemű bejelentőnél is lefoglalást végezni, ha a bűncselekményre vonatkozó adat valószínűsíthetően a nála megtalálható adathordozón rögzült, és azon fellelhető. Ez nem a jogi szabályozás hibája, vagy a rendőrség eljárásának hibája, hanem egy olyan szükségszerű technikai körülmény, amit a jog eszközeivel nem lehet oly módon szabályozni, hogy egy magasabb jogi érdek, társadalmi érdek ne sérülne.

Alapvetően kijelenthetjük, hogy minden olyan esetben, mikor informatikai környezetben valósul meg egy bűncselekmény, és annak mi szemtanúivá válunk (pl.egy botnet hálózat zombie gépe a mi számítógépünk is, vagy megnyitottunk egy phising oldalt, pedofil oldalt), valójában az az eszköz tölti be a szemtanú szerepét amin keresztült ezt tapasztaltuk, és mivel annak technikai működéséből adódóan az azon átfolyó adatok rögzítésre kerülnek, így a használt eszköz bizonyítékot tartalmaz a kérdéses bűncselekménnyel kapcsolatban. Függetlenül attól, hogy az az adat a cache tárolóban került letárolásra vagy tartósan történt a rögzítése, rendőrségi nézőpontból erre mindaddig nem derül fény, míg a számítógépünkben, informatikai eszközünkben tárolt adathordozót át nem vizsgálták. Ebből következik, hogy a rendőrség a nyomozati szempontból, bizonyítékként releváns adat nálunk való fellelhetőségét vélelmezi, és csak a merevlemez szakértői vizsgálatát követően derül fény arra, hogy mennyire tartalmaz a nyomozás szempontjából releváns információt a kérdéses adathordozó.

Civil megoldások

Tekintettel a rendőrségi út bürokratikus és hivatali hátterére, sok esetben túlontúl lassú ez az eljárás és a bűncselekményt észlelők nem kívánják kitenni magukat a rendőrségi eljárás miatt rájuk nehezedő figyelemnek és plusz kötelezettségeknek. Az állam és az állampolgárok között fennálló szakadék áthidalására jöttek létre azok a nemzeti civil és nemzetközi szervezetek, melyek célkitűzése az ilyen eljárások felvállalása és az egyes bejelentők anonimitásának biztosítása. A káros, illegális és jogsértő tartalmak bejelentésére hozták létre az INHOPE (International Association of Internet Hotlines) szervezetet, mely a nemzeti online forródrótokat tömörítő, információ elosztó és eljárást kezdeményező nemzetközi szervezet. Elsődleges célja, a kiskorúak sérelmére, online elkövetett visszaélések és szexuális jellegű bűncselekmények megfékezése, az Internet biztonságosabbá tétele, és egy ilyen cselekmények, tartalmak bejelentésére szolgáló nemzetközi forródrót rendszer működtetése.

Magyarországon a www.biztonsagosinternet.hu weboldalon érhető el az ilyen káros, illegális és jogsértő tartalmak bejelentésére szolgáló oldal, online forródrót, amely az INHOPE hálózat magyarországi tagszervezete. A magyarországi oldalnak is az a célja, hogy az azt üzemeltető szakemberek a bejelentések vizsgálatát követően az erre kialakított rendőrségi és civil mechanizmusokon keresztül a sértő tartalmat a lehető legrövidebb időn belül eltávolíthassák az internetről és az azt hozzáférhetővé tevők büntetőjogi felelősségre vonása megtörténjen.

Felelősök-e a tárhely szolgáltatók (közvetítő szolgáltatók) a náluk hosztolt tartalomért?

Az egyes tárhely szolgáltatók, közvetítő szolgáltatók[4] alapvetően felelősek az általuk közvetített tartalomért, egyébiránt a tartalomért való felelősségüktől az Elektronikus kereskedelemről szóló, 2001. évi CVIII. Törvény, 8.-11.§ terjedő része foglalkozik részletesen. A tárhely szolgáltató (közvetítő szolgáltató) saját felelősségének kizárása érdekében blokkolhatja vagy eltávolíthatja azt a tartalmat, amelynek jogellenességéről értesül.

Gyakorlati oldalról első lépésként szükséges a szolgáltató nevének és elérhetőségének meghatározása, lokalizálása (erre több weboldal is található, pl. a http://www.domain.hu/domain/domainsearch/), majd ezt követően e-mailes vagy postai úton értesítése.

Az értesítésben meg kell jelölnie a bejelentőnek a szerinte jogellenes oldal elérhetőségét, a sértő tartalmat, hogy miért tartja azt jogellenesnek, valamint az ő, mint bejelentő elérhetőségét.

A tárhely szolgáltató ilyen esetben mérlegelhet, hogy valóban jogellenes-e az a tartalom vagy se, és eldönti, hogy eltávolítja-e azt.

Ha a tárhely szolgáltató ezt nem teszi meg, akkor büntetőjogi esetben a rendőrséghez kell fordulnia a sértettnek és feljelentést tennie, polgári jogi esetben pedig a bírósághoz keresetet benyújtania és kérnie az oldal blokkolását.

Amennyiben szerzői joggal kapcsolatos jogsértést történt az adott weboldalon, a tárhely szolgáltatónak az erről való értesülést követően kötelessége eltávolítania vagy a hozzáférést blokkolnia a jogsértő tartalomhoz. Szerzői vagy szomszédos jogok sérelme esetén nincs mérlegelési jogköre, törvényi kötelessége a jogsértő tartalom eltávolítása vagy a hozzáférés blokkolása. Ezt az eljárást nevezik a Notice & Take Down eljárásnak.

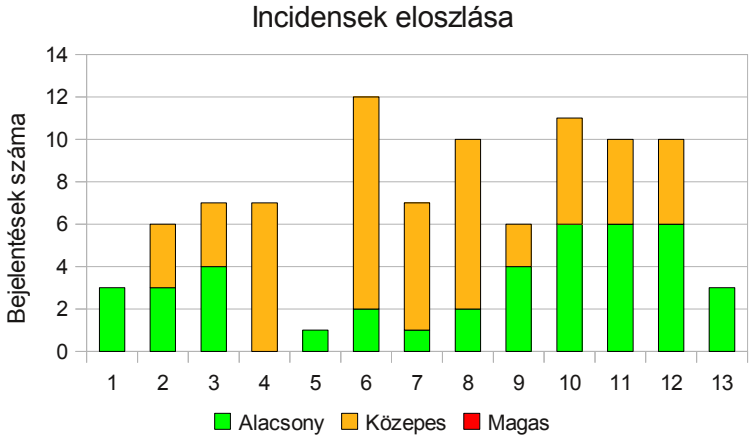
4 2001. évi CVIII. Törvény: "Közvetítő szolgáltató: az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltató, amely
la) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, vagy a távközlő hálózathoz hozzáférést biztosít (egyszerű adatátvitel és hozzáférés-biztosítás);
lb) az igénybe vevő által biztosított információt távközlő hálózaton továbbítja, és az alapvetően a más igénybe vevők kezdeményezésére történő információtovábbítás hatékonyabbá tételét szolgálja (gyorsítótárolás);
lc) az igénybe vevő által biztosított információt tárolja (tárhelyszolgáltatás);
ld) információk megtalálását elősegítő segédeszközöket biztosít az igénybe vevő számára (keresőszolgáltatás);"

Internetbiztonsági incidensek

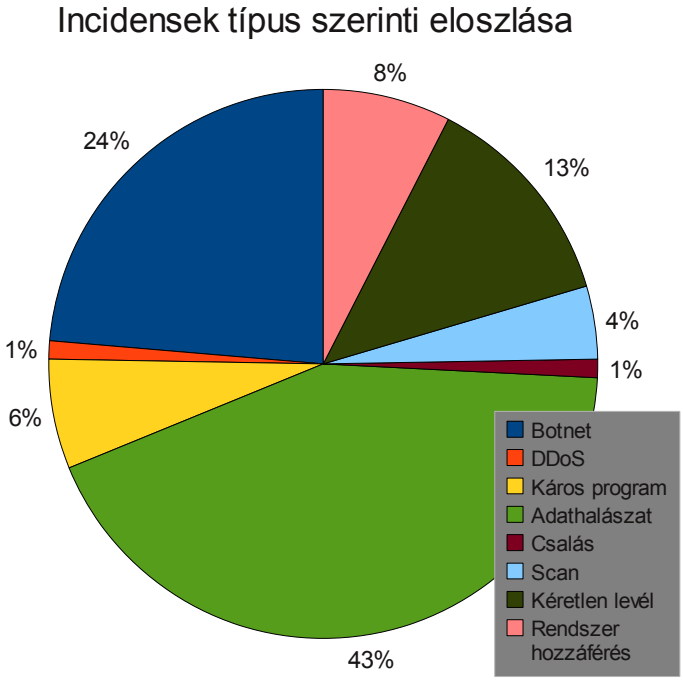
Internetbiztonsági incidens minden olyan biztonsági esemény, amelynek célja az információs infrastruktúrák bizalmasságának, sértetlenségének vagy rendelkezésre állásának megsértése az interneten, mint nyílt információs infrastruktúrán keresztül.

A PTA CERT-Hungary, **Nemzeti Hálózatbiztonsági Központ** a 2011. első negyedéve során összesen **93 db incidens bejelentést** regisztrált és kezelt, ebből 41 db alacsony és 52 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.



2011. I. negyedévében az incidens bejelentések túlnyomó többsége adathalász tevékenység és botnet hálózatok részét képező fertőzött gépek kapcsán érkezett, leszámítva a Shadowserver Foundation-től beérkező botnet hálózatokról szóló bejelentéseket.



Az említett két kategóriába tartozó incidensek mintegy kétharmadát tették ki az összes belejelentésnek. Számottevőek voltak még a rendszer hozzáférési kísérletek és spam tevékenység kapcsán beérkezett bejelentések, melyek együttesen 21%-át teszik ki az összes bejelentésnek.

A bejelentések többsége külföldi partner-szervezetektől érkeztek és több mint 90%-ban haza káros tevékenységgel vagy káros tartalommal voltak összefüggésben. Az egyes incidensek elhárítása kapcsán összesen 91 szolgáltató került bevonásra és összesen közel 900 szálon folyt incidenskezelési koordináció.

Az adathalász oldalak (phishing oldalak) meglehetősen nagyszámú jelenléte azt mutatja, hogy a felhasználói szokások még mindig teret engednek az ilyen jellegű social engineering támadások megvalósításának. Ez a tendencia várhatóan nem is fog megváltozni, amíg a felhasználók fel nem ismerik az elektronikus azonosítóik és személyes adataik védelmének fontosságát.

Biztonság a közösségi hálózatokon

Az Internet használatában járatosabbak feltehetően hallottak már a közösségi hálózatokról. Akik nem, azok előbb vagy utóbb találkoznak azokkal az interaktív Internetes alkalmazásokkal, amelyek lehetőséget teremtenek a felhasználóknak személyes profiljaik létrehozására, információk megosztására és kapcsolataik ápolására. Ilyen oldal többek között az IWIW, Facebook, Twitter vagy a LinkedIn. Ezeknek az oldalaknak a népszerűsége az elmúlt években robbanásszerűen nőtt, gyakorlatilag a mindennapi kommunikációnak egy fontos csatornájává nőtték ki magukat. Ezek a hasznos és szórakoztató szolgáltatásokat nyújtó közösségi portálok számos biztonsági és adatvédelmi kockázatokat is hordoznak magukban.

A cikk célja, hogy egyrészt áttekintést adjon a közösségi hálózatok használatával járó kockázatokról, másrészt bemutassa a három legelterjedtebb támadási módszert, valamint azok védekezési lehetőségeit.

Biztonsági kockázatok a közösségi hálózatokon

Az egyre népszerűbb és felkapottabb közösségi oldalak nem hagyják hidegen a támadókat sem. A portálok adta lehetőségek gyakorlatilag megkönnyítik a dolgukat céljaik elérésében.

Négy fő ok, ami vonzóvá teszi a közösségi oldalakat a támadók számára:

- Nagy számú felhasználó bázis
- Személyes információk elérhetősége
- Kölcsönös bizalom a felhasználók között
- Relatív gyenge biztonság

A közösségi hálózatok természetéből fakadóan a támadók éppúgy kreálhatnak profilokat, ahogyan a jóindulatú, rendeltetésszerűen használó felhasználók, így lehetetlen megkülönböztetni őket. Ez minimum két kockázatot eredményez:

- Közösségi oldalak használatával fertőzés áldozatává válhatunk, amely a számítógép feletti teljes kontroll elvesztését eredményezheti.
- A támadók betekintést nyerhetnek személyes adatainkba, kapcsolatainkba, amelyek visszaélés tárgyát képezhetik.

Kevés statisztika áll rendelkezésre a sikeresen végrehajtott támadásokkal kapcsolatban, ami elérhető az is felszínes, eseti alapú információ.

Hogyan működnek a támadások?

A támadások elemzésével nagyobb lehetőség nyílik azok korai felismerésére és elkerülésére. A közösségi hálózatokon használt támadási módszerek részben megegyeznek a megszokott, felhasználót célzó támadási módokkal pl.: phishing, malware terjesztés. A támadók igyekeznek kihasználni a közösségi környezet nyújtotta előnyöket, így ennek megfelelő támadási módokat fejlesztenek pl.: rosszindulatú alkalmazásokat.

Adathalászat (Phishing)

A közösségi hálózatok használatát többcélúság jellemzi. Egyik legfontosabb funkciója maga a hálózati funkció, amely segítségével új és meglévő kapcsolatok alakíthatóak ki ill. ápolhatóak. A felhasználó személyes információk megosztásával elősegítheti a közösségi (hálózati) kommunikációt.

A támadók felhasználhatják ezeket az információkat célzott, általános üzenetnek vagy személyes üzenetnek látszó adathalász üzenetek küldésére. Az üzenetek célja, hogy elhitessék a címzettel, hogy a levél feladója egy közösségi oldal vagy például egy pénzügyi szolgáltatásokat nyújtó szervezet. Ahogy a levélmegnyitási és válaszolási tendenciák mutatják, könnyen áldozatul eshetnek a felhasználók.

Ezek a hamis üzenetek a közösségi hálózat egy másik felhasználójaként adják ki magukat és a baráti körhöz, hálózathoz való csatlakozást szorgalmazzák. Az üzenetek rendszerint tartalmaznak egy „visszaigazoló" vagy „elutasító" gombot, amely a közösségi oldal bejelentkezési oldalát jeleníti meg. A támadónak ekkor nyílik lehetősége a bejelentkezési adatok megszerzésére.

http://tech.cert-hungary.hu/tech-blog/110411/a-facebookon-terjedo-bully-video-valojaban-egy-xss-exploit

Malware terjesztés

A malware, más néven kártékony szoftver pl.: vírus, trójai, féreg stb. fontos láncszeme az illegális tevékenységeknek, folyamatoknak. Kártékony szoftverrel fertőzött gép felhasználható más támadásokhoz vagy személyes információk szerzéséhez.

A közösségi hálózatokat felhasználó támadások során a kártékony link az e-mailben kerül elhelyezésre. Ez a következőképpen fordulhat elő:

1. A támadók üzenetet küldhetnek egy kompromittált felhasználói profilból.
2. A támadók kreálhatnak egy általános profilt linkjeik terjesztéséhez.

Az első eset kínálja a legnagyobb lehetőséget a támadónak, mivel itt visszaélhet a kölcsönös bizalommal és az ismert kapcsolat végett kevesebb figyelmet fordít a potenciális veszélyekre a címzett.

A támadók különféle Internetes szokásokat felhasználva is terjesztik malware szoftvereiket. Ilyen például a rövidített URL-ek használata. Az így álcázott linkek lehetővé teszik a támadók számára, hogy elrejtsék a rosszindulatú hivatkozásokat, valamint a célpontok gyanútlanak maradjanak.

http://tech.cert-hungary.hu/tech-blog/110407/a-hackerek-uj-kedvencei-a-kozossegi-oldalak-es-a-rovid-linkek

Káros alkalmazások

A közösségi portálokon használt alkalmazások száma folyamatosan nő. A támadók természetesen ezeket a fejlesztéseket is ki akarják használni és saját céljaikra fordítani azokat. A kísérleteik nem eredménytelenek, mivel tudják hogyan szolgálják ki a közösségi igényeket. Erre kiváló példa a *Profile Creeper* nevű Facebook alkalmazás, amely elméletileg megmutatja, hogy ki látogatta meg a profilunkat, de a gyakorlatban csak egy felmérésre, szavazásra épülő csalás. A *Profile Creeper* a következőképpen kerülhet a felhasználók látóterébe:

"I just saw who STALKS me on Facebook! You can see who creeps around your profile too! [LINK]"

A fenti üzenetre történő kattintással ugyanez az üzenet jelenik meg a felhasználó ismerőseinél, kapcsolatainál és ez így terjed tovább. Hatványozottan nő a potenciális áldozatok száma, miközben ez csak a támadás első lépése. Az alkalmazás engedélyezésekor egy kérdőívet kell kitölteni, amelyek jellemzően melegágyai a rosszindulatú tevékenységeknek és visszaéléseknek.

http://tech.cert-hungary.hu/tech-blog/101007/facebook-linkek-tizede-spam-vagy-malware

Egyéb kockázatok

Az egyéb, másodlagos kockázatok elsősorban a megosztott személyes adatokhoz kapcsolódnak. Az alapértelmezett adatvédelmi beállítások a közösségi portálokon jellemzően a „publikus" beállításon állnak. Ez azt jelenti, hogy bárki (publikusan) hozzáférhet a személyes adatokhoz mindaddig, amíg a személyes adatvédelmi beállításai ezt engedik. A profilban tárolt információk nem feltétlenül publikusak.

http://tech.cert-hungary.hu/tech-blog/100901/kozossegi-halozatok-es-az-anonimitas-illuzioja

Létezik egy közvetett kockázat is az információmegosztáskor, ez pedig a munkáltatóval kapcsolatos. Konfliktus alakulhat ki az alkalmazott és a munkáltató között, amennyiben a munkavállaló információkat oszt meg munkáltatójáról vagy munkájával kapcsolatban. Több eset is napvilágot látott a médiában, ahol a munkavállaló közösségi hálózati aktivitása kihatással volt karrierjére.

http://tech.cert-hungary.hu/tech-blog/100920/az-interpol-vezetojenek-profiljat-hamisitottak

A közösségi hálózatok általános feltételei leírják a személyes adatok kezelésének módját. Ezek tartalmazzák, hogy mely adatokat használhatják fel, valamint melyekre formálhatnak jogot. Ez a poszt tartalmára nézve kockázatot jelent, vagyis melyik szellemi szerzői jog kerüljön érvényre.

Biztonságos használatot segítő intézkedések

A közösségi oldalak használata mindig valamilyen kockázatot hordoz magában. A következő tanácsok segíthetnek minimalizálni a lehetséges veszélyeket:

- Tájékozódjon az általános szerződési feltételekről

  Ahogy korábban szó volt róla, az általános szerződési feltételek alapos átolvasása elengedhetetlen előfeltétele a megfontolt döntésnek a személyes adatokat illetően. A rendszeresen frissülő és változó általános szerződési feltételek folyamatos után követést igényelnek.

  http://tech.cert-hungary.hu/tech-blog/101007/facebook-biztonsagi-es-adatkezelesi-utmutato

- Korlátozza a profilhoz való hozzáférést barátaira, ismerőseire

  Tiltsa le az idegeneknek a személyes profilhoz történő hozzáférést, korlátozza csak az ismerőseire

- Kizárólag ismerősöket, barátokat igazoljon vissza

  A meglévő ismerősök és üzleti partnerek bejelölése mellett, új kapcsolatok építése is szórakoztató lehet. Sokan sportot űznek a kapcsolatok minél nagyobb számú építéséből. Ez természetesen lehetővé teheti idegenek számára a profilunkhoz való hozzáférést. A profil megfelelő korlátozása sem feltétlen kockázatmentes, mivel az ismerősi kapcsolatokon keresztül is történhet visszaélés az adatokkal. Amennyiben kétségei támadnak egy visszaigazolás alkalmával, a legjobb módja a kételyek eloszlatásának a telefonos vagy e-mailes megkeresés. A lényeg, hogy a közösségi hálózatokban bárki személyes adatával történhet visszaélés.

  http://tech.cert-hungary.hu/tech-blog/110412/hivatalos-profil-ellenorzo-alkalmazas-facebook-csalas

- Fontolja meg mit publikál

  Ami egyszer kikerül azt Internetre azt nagyon nehéz onnan eltávolítani vagy éppenséggel lehetetlen. A publikus információk a keresőmotorok cache tárolójában végezhetik pl.: Google, amelyek aztán más oldalakra „ragadhatnak”.

  http://tech.cert-hungary.hu/tech-blog/101104/lanya-hozta-kellemetlen-helyzetbe-a-brit-titkosszolgalatok-fonoket

- Kövesse a munkáltató közösségi hálózat használatával kapcsolatos irányelveit

  Egyre több munkáltató készíti el és vezeti be a közösségi hálózatok használatára vonatkozó irányelveit. Bizonyosodjon meg afelől, hogy betartja ezen irányelveket, hogy elkerülje az ebből származó konfliktusokat.

- Használjon erős jelszavakat

  A profilok ill. fiókok illetéktelen hozzáférésének minimalizálása érdekében használjon erős jelszavakat. Az egyszerű jelszavak nem jelentenek kihívást a támadóknak, továbbá kerülje a jelszavak többszöri felhasználását.

- Bizonyosodjon meg afelől, hogy naprakész a vírusirtója

  Az antivírus szoftverek képesek detektálni és jelezni a kártékony szoftvereket. Az esetleges támadások hatásai jó eséllyel csökkenthetőek.

- Telepítsen friss szoftvereket, telepítse a böngésző frissítéseit

  A sérülékenységek kihasználásának elkerülése érdekében mihamarabb telepítse a gyártói javításokat, frissítéseket.

http://tech.cert-hungary.hu/tech-blog/100816/5-tipp-arra-hogyan-vedd-magad-a-facebookon

A felsorolt intézkedések elsősorban a kockázatok minimalizálására összpontosítanak de nem szüntetik meg azokat teljesen. Ebből kifolyólag nagyon fontos, hogy megismerjük azokat a technikákat, módszereket, amelyek csökkenthetik egy sikeres támadás hatásait. Amennyiben mégis egy rosszindulatú hivatkozásra kattintunk, a legjobb amit tehetünk, hogy eltávolítjuk a további kattintás (pl.: ismerősök) megakadályozása érdekében. Hasonló módon csökkenthetjük egy esetleges illetéktelen fiókhozzáférés következményeit, ha értesítjük ismerőseinket, kapcsolatainkat, akár a közösségi hálózat üzemeltetőinek bevonásával.

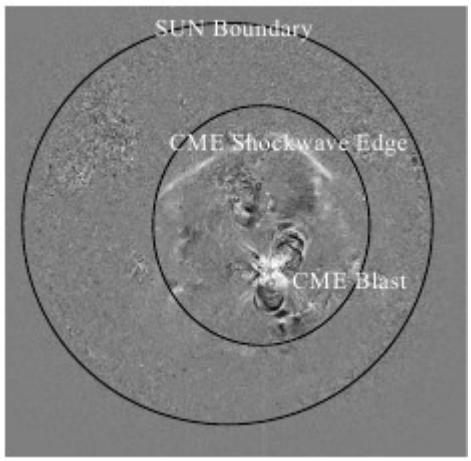
http://tech.cert-hungary.hu/tech-blog/101110/online-szolgaltatasok-biztonsagi-ertekelese

Forrás:

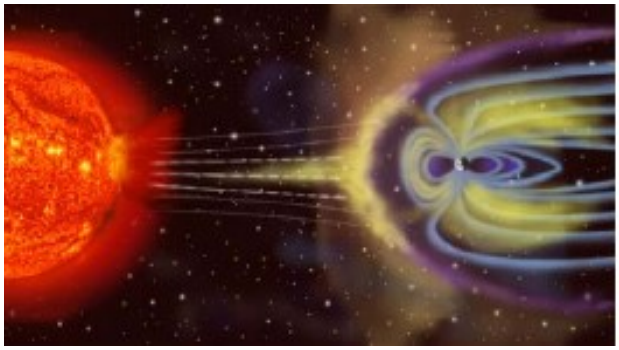
GovCert.NL (Version 1.1 – 2011. április 21.), Secure on Social Networks - Factsheet FS 2011-01
http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/factsheet-secure-on-social-networks.html

A nap mágneses viharainak hatása a vezérlő rendszerekre

A Nap kitöréseket és korona kidobódásokat (coronal mass ejection - CME) generál, amelyeknél megközelítőleg 11 éves ciklus figyelhető meg. Ezek az események olyan plazma felhőket generálnak, amelyek geomágneses viharokat válthatnak ki, amelyek aztán zavarokat okoznak a földi kommunikációban és más elektronikai rendszerekben. Így joggal vetődnek fel a kritikus infrastruktúrára jelentett kockázatok is. A Föld körül keringő műholdak az utóbbi négy év napkitörései és CME-k[5] által okozott legerősebb mágneses viharát derítették fel. Az első ábra érzékelteti a CME lökéshullámok kiterjedésének méretét a Nap méretéhez képest a kitörés pillanatában.



Február 15. 0156 UT időpontban (Universal Time a Föld forgásához viszonyított idő), az 11158. aktív régió X2 osztályú kitörése volt megfigyelhető[6]. Az X-flare típusú kitörések a legnagyobb X-ray típusú kitörések, és az első ilyen kitörés az új 24. Nap Ciklusban. A robbanás, amit ez a kitörés keltett, tekinthető úgy, mintha a Nap cunami hullámokat küldött volna a saját atmoszféráján keresztül, majd a CME-t a Föld felé „lökte". A CME tevékenység tovább folytatódik Nap ciklus folyamatának részeként.



1. ábra. Az X2 típusú napkitörés és korona kidobódás a kitörés pillanatában. Mire a CME eléri a Földet, addigra a lökéshullámok határ vonala körülbelül 40 millió mérföldre terjed ki.

Jelen cikk azért készült, hogy tájékoztassa az ipari vezérlő rendszerek (industrial control systems – ICS) közösségét a Nap mágneses viharainak a kritikus infrastruktúrát vezérlő rendszerekre gyakorolt hatásairól.

Előrejelzések

A Nemzeti Óceán- és Légköri Szervezet (National Oceanic and Atmospheric Administration - NOAA) napi időjárás előrejelzést biztosít a Nap tevékenységről, űr időjárás riasztásokat készít, és a napkitörésekkel és CME eseményekkel kapcsolatos tanácsokat ad, ugyanis ezek hatással lehetnek a navigációra, a rádiózásra, a villamos energiára és a műhold tevékenységekre[7].

5 National Oceanic and Atmospheric Administration (NOAA), Space Weather Prediction Center, http://www.swpc.noaa.gov/sxi/index.html, last accessed March 1, 2011.
6 James A. Marusek, "Solar Storm Threat Analysis," http://www.breadandbutterscience.com/SSTA.pdf, last accessed February 16, 2011.
7 National Oceanic and Atmospheric Administration (NOAA), Space Weather Prediction Center, http://www.swpc.noaa.gov/SWN/index.html, last accessed March 1, 2011.

A nap viharok háttere

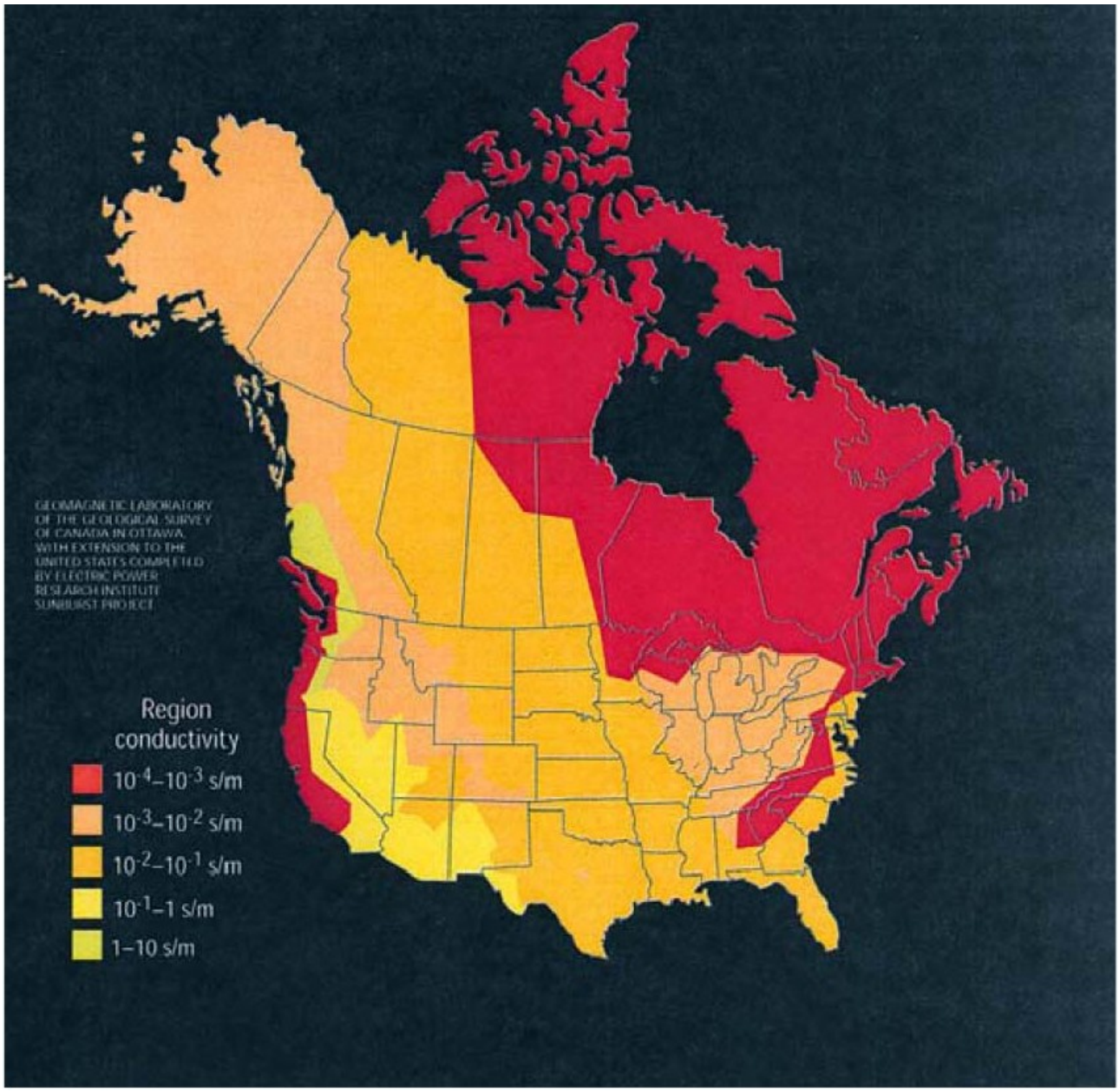
1. A napkitörések következményei az erős sugárzás-kitörések (burst of radiation) (röntgen sugár, erős UV sugárzás, gamma sugárzás és rádió frekvencia hullámok), valamint a felső atmoszféra felmelegedése és ionizációja. A napkitörések zavarják a műholdas kommunikációt, a radarokat és a rövid hullámú rádiózást. A sugárkitörések fénysebességgel terjednek, így a kitöréstől számítva 8 perc alatt érik el a Földet. A napkitöréseket egymáshoz viszonyított méretük szerint osztályozzák: a B-típusú kitörések mérete megközelítőleg 10%-a a C-típusú kitörésekének; a C-típusú kitörések megközelítőleg 10%-os méretűek az X-típusú kitörésekhez képest. Az X osztályon belül a kitöréseket egy lineáris skálán ábrázolják (pl.: X-1, X2). Az eddig mért legnagyobb napkitörés 2003. november 4-én történt, és X-45[2] [8] erősségűnek értékelték.
2. A kitöréseket nap proton (solar proton event – SPE) események követik. Terjedési sebességük kisebb, mint a fénysebesség, a kitörés után körülbelül egy órával érik el a Földet. Az SPE nagy energiájú kozmikus sugárzást (protonok és ionok) eredményez, ami képes eltéríteni a műholdakat, károsíthatja az űrhajók elektronikáját, zavarhatja a földi rövid hullámú rádiózást a sarki területeken és károsítja az ózon réteget.
3. A CME-ek mágneses mezőt tartalmazó, plazmával töltött hatalmas felhőket hoznak magukkal, amelyek 40 millió mérföldet tesznek meg mire elérik a Földet. A CME lökéshullámok terjedési sebessége eltérő, megközelítőleg 5 millió mérföld óránként, így ezek körülbelül 18 (esetleg több) óra alatt érik el a Földet.

Az ionoszféra (az atmoszféra felső rétege, 85-600 km-es föld feletti magasságban) kritikus a rádió jelek terjedése szempontjából. A napsugárzás az ionoszférát az atmoszféra felső rétegének ionizálásával hozza létre. Rádióadás továbbításakor az ionoszféra visszaveri a jeleket, hogy azok elérjék a kívánt célt[9].

Amikor a CME-hez kapcsolódó mágneses mező a Föld mágneses mezőjére hat, akkor mágneses vihar keletkezik, amely hatásai egy-két, esetleg több napon át tarthatnak. A CME elektromágneses energiája megtöri az ionoszféra visszaverődési képességét, kedvezőtlenül befolyásolva a rádió jelek továbbítását. Ez hatással lehet az általános helymeghatározó rendszerek (global positioning system - GPS) műholdas jeleire is, zavarva a navigációs rendszereknél és egyéb ellenőrző rendszereknél használt GPS idő hivatkozásokat. A geomágneses viharnak a Föld mágneses mezőjére gyakorolt hatása miatt felületi feszültségek keletkeznek a Föld változó ellenálló képessége miatt (lásd 2. ábra[10]. A CME-től megváltozott elektromágneses mező az erőművekben az elosztáskor és a földi továbbító rendszerekben feszültség ingadozást okozhat, geomágnesesség okozta áramot termelhet (geomagnetic-induced currents - GIC), ami károsíthatja az erőművek és állomások által használt csatlakozó (három fázisú – wye-connected) transzformátorokat. Például a GIC akár 1000A is lehet, bár a legtöbb nagy transzformátort még nem tesztelték ilyen tartományban[11].

2 James A. Marusek, “Solar Storm Threat Analysis,” http://www.breadandbutterscience.com/SSTA.pdf, last accessed February 16, 2011.
8 N. R. Thomson, C. J. Rodger, and M. A. Clilverd, Large solar flares and their ionospheric D region enhancements, American Geophysical Union: Journal of Geophysical Research, Vol. 110, A06306, http://www.agu.org/pubs/crossref/2005/2005JA011008.shtml, 2005, last accessed March 21, 2011.
9 Carolyn Jo Shields, “The Effects of Radio Frequency (RF) Propagation within the Work Place,” Oakridge National Laboratory, August 2008.
10 T. S. Molinski, W. E. Ferro, and B. L. Damsky, “Shielding grids from solar storms,” IEEE Spectrum, November 2000, pp. 5560.
11 A. Pulkkinen, R. Pirjola, and A. Viljanen, Statistics of extreme geomagnetically induced current events, Space Weather, 6, S07001, July 2008, pg. 9.

A Föld alap ellenálló képessége



2. ábra. A föld alap ellenálló képessége az alatta lévő sziklarétegektől függ. A vezetőképesség mérését a kanadai (Ottawa) Geológiai Földmérő Geomagnetikai Laboratóriuma végezte, kiegészülve az Egyesült Államok Elektromos Energia Kutató Intézet Napfény projektjével. (Geomagnetic Laboratory of the Geological Survey of Canada in Ottawa, United States Completed by Electric Power Research Institute Sunburst Project.) Mértékegység: Siemens per méter (a vörössel jelölt területeknek gyakorlatilag nincs vezetőképességük[6]).

6 T. S. Molinski, W. E. Ferro, and B. L. Damsky, "Shielding grids from solar storms," IEEE Spectrum, November 2000, pp. 5560.

A kritikus infrastruktúra ellenőrző rendszerekre gyakorolt hatások

Rádió vételi zavarok

A geomágneses viharok közvetlen zavarokat okozhatnak a GPS és rádió kommunikációban az ionoszféra megzavarása miatt. Ezek a zavarok a generált zajoktól a teljes jelvesztéséig terjedhetnek. A geomágneses viharok közvetett hatást gyakorolnak sok más rendszerre is; ide tartoznak azok az ellenőrző rendszerek, amelyek GPS vagy rádió technológián alapulnak[12].

Azok az ellenőrző rendszerek, amelyek az alábbi technológiákat alkalmazzák, a tapasztalatok szerint részleges vagy a teljes szolgáltatási üzemzavart szenvedhetnek el - különböző időtartamút a vihar erejétől (és más tényezőktől) függően.

Közvetlenül érintett rendszerekben

- Elosztott vezérlő rendszerek, amelyek GPS Position Navigation and Timing (PNT) jel alapú szekvenciákat és ellenőrzési folyamatokat használnak.
    - Ilyet használnak az olaj, a gáz és a villamosenergia-iparban, a tengeri és légi közlekedésben, víz és szennyvíz iparban, valamint a vonatok esetében.
- A rövid hullámú vezeték nélküli kommunikációban.
- A vészhelyzet esetén hívható szolgáltatások kézi vezeték nélküli kommunikációjában.

Közvetetten érintett rendszerek

- Azok a vezérlő rendszerek, amelyek támogatják a vezeték nélküli technológiát (pl.: Wi-Fi, mobil hálózatok) és GPS idő meghatározó jeleket használnak
    - Távoli terminál egységek (remote terminal units - RTUs), programozható logikai vezérlők (programmable logic controllers - PLCs), és intelligens elektronikus eszközök (intelligent electronic devices – IEDs) és egyéb vezérlők.
    - Hordozható műszerek és teszt felszerelések.

Az elektromos hálózat zavarai

Folytatódik az a trend, hogy minél több elektromos energiát továbbítsanak, minél hosszabb vezetékeken, amely már közelíti a teljesítmény határokat, ami egyenesen arányos a geomágneses viharok erőssége és az elektromos hálózati hatások között fennálló kapcsolatokkal. Egy geomágneses vihar számos problémát okozhat az elektromos erőművek rendszereinek működési csúcs időpontjában. Ez különösen igaz egyes régiókra, például az Egyesült Államok északi részén és a tengerparti területeken, ahol a vulkáni eredetű sziklák geológiailag csökkentik a Föld vezetőképességét (lásd A napvihar tevékenység hatásai időrendi sorrendben c. fejezet)[13].

A napviharok alatt a CME plazma felhő és annak mágneses mezője összeütközik a Föld mágneses mezőjével, ami átmenetileg óriási mágneses zavarokat idéz elő. Ezek a zavarok vagy geomágneses viharok megzavarhatják a Föld mágneses mezőjét, akár két napnál hosszabb időre is.

12 Ron Behren, P. E., “Trouble in the Sky! Solar Activity May Cause Problems for Utilities,” The Hartford Steam Boiler Inspection and Insurance Company, http://www.hsb.com/thelocomotive/story/FullStory/ST-FS-SOLAR.html, last accessed February 16, 2011.

13 P. R. Barnes, D. T. Rizy, B. W. McConnel, F. M. Tesche, E. R. Taylor, Jr., *Electric Utility Industry Experience with Geomagnetic Disturbances*, ORNL-6665, Oakridge National Laboratory, November 25,1991.

A geomágneses viharok a Föld felszínén különböző feszültségeket kelthetnek, így olyan feszültség különbségek jönnek létre a terep pontok között, amelyek GIC-eket (Geomagnetically induced currents - geomágnesesség gerjesztette áram) keltenek, majd ezeken keresztül áramlanak a transzformátorokon, az erőművek továbbító vezetékein és a terep pontok között. A GIC-eknek számos hatása lehet a három fázisú transzformátorokra és az automata transzformátorokra a szigetelések túlmelegedése és a létrejött összegződések miatt (lásd: A napviharok hatása a transzformátorokra – technikai analízis c. fejezet).

Az alacsony vezetőképességű területek, mint a vulkáni eredetű sziklás geológiai területek, érzékenyebbek a geomágneses viharok hatásaira. Ezeken a területeken a beépített erőmű továbbító rendszerekben a geomágneses zavarokból eredő lényegesen nagyobb GIC-eket tapasztaltak. Észak Amerika területét a Föld vezetőképessége szempontjából öt nagyságrenddel jellemezték (lásd 2. ábra). A GIC-ek nagyságrendje fordítottan arányos a továbbító rendszerek ellenálló képességével. A továbbító vezetékek hatékonyan zárják rövidre a transzformátorok elosztó rendszerei és a transzformátorok földelése között átáramló GIC-eket. Egy napvihar egyszerre sok ponton gyakorolhat hatást az elektromos hálózatra, ami több ponton fellépő meghibásodásokat eredményezhet. Azok a transzformátorok, amelyek támogatják a továbbító vezetékeket (transmission lines), költségesek és sokáig, akár két évig is eltarthat a leszállításuk és üzembe helyezésük (lásd B melléklet). A NOAA Űr Időjárás Előrejelző Központ számos mérési módszert biztosít a geomágneses viharok és nap-sugár kitörések, valamint a rádiózási üzemzavarok mérésére. Az alábbi két hivatkozáson a NOAA Űr Időjárás Előrejelző Központ elektromos közműveket érintő időjárási helyzet tudatosítási programja található:

- Elektromos Erőművek Elektromos Közművek Információs Oldala (Riasztások és tanácsok) http://www.swpc.noaa.gov/ElecPower/
- NOAA Űr Időjárási Mérések (NOAA Űr Időjárás Geomágneses Viharok jegyzéke) http://www.swpc.noaa.gov/NOAAscales/index.html#RadioBlackouts.

A NOAA mérései a mágneses mező három óránkénti változásait tükrözik, a GIC-ek a mágneses mezőben bekövetkezett változások mértékétől függenek. Ez annak a megfelelője, hogy a vihar nem azért okoz károkat, mert alacsony a légköri nyomás, hanem a légnyomás változás keltette szél miatt. A mágneses mező változási értékeiről az információ jelenleg nem egyszerűen érhető el, bár a NASA dolgozik egy új index létrehozásán, ami kifejezi a változás mértékét.

Olaj, gáz és egyéb csővezetékekben bekövetkezett zavarok

A napviharok hatással lehetnek a vezeték és a talaj közötti feszültségre, az áram vezetésével megzavarhatják az áramlásmérő jeleket, így az a vezeték hamis áramlási adatokat mutathat. A gerjesztett áram növelheti a vezeték korrózióját is. A külső szigetelés célja, hogy megszakítsa az áram útját, és ezen a ponton az elektromos feszültséget a talajba vezesse, ami megnöveli a korrózió jelentette kockázatot[2].

A napviharok hatása a transzformátorokra – technikai analízis

Az Amerikai Haditengerészet fizikusa, James A. Marusek, "A napviharok veszélyeinek elemzése" (Solar Storm Threat Analysis) című cikkében az alábbi elemzést adta:

"A geomágnesesség keltette áram (Geomagnetic Induced Currents - GIC) azt okozhatják, hogy a transzformátorok csak fél ciklusos telítettséggel vezetnek, ahol a transzformátor magja mágnesesen telített a váltó ciklusban. Csak néhány amper szükséges a transzformátor műveletek megszakítására. Egy GIC szinten keltett feszültség 1-2 Volt/kilométer és 5 amper elegendő a semleges magas

2 James A. Marusek, "Solar Storm Threat Analysis," http://www.breadandbutterscience.com/SSTA.pdf, last accessed February 16, 2011.

feszültségű tekercselésekben, hogy a földelt három fázisú csatlakoztatott elosztó transzformátor telítetté váljon akár egy másodpercre[9] is. Geomágneses viharok alatt, az Amerikai Egyesült Államokban egy transzformátor semleges lábnál mértek már 184 amperes GIC áramot is[6]. A legnagyobb, eddig mért GIC áram 270 amper volt, Svédország déli részén, 2000. április 6-án egy geomágneses vihar alatt."

"Ha a transzformátor fél ciklusos telítettsége folytatódik, akkor a kóbor áram belép a transzformátor szerkezeti tartály részeibe és a szigetelésekbe. A transzformátor-tartályok elszigetelt pontjain a hőmérséklet néhány percen belül több száz fokkal megemelkedik[11]. A mért hőmérsékleti csúcs 750°F (~271°C) volt. A transzformátor kapcsolók másodpercenként 60-szor váltakoznak telített és nem telített állapot között, az átlagos transzformátor zaja érdes, szakadozott. Párhuzamba állítva egy ökölnyi mágnes összeütközését egy fém tányéréval és rezgésével, akkor egy 100 tonnás transzformátor egy kisebb háznak felel meg. Ez a hatás a geomágneses vihar néhány órája alatt következik be. A GIC keltette telítettség a transzformátorokban túlzott gázkibocsátást eredményezhet. Az azonnali hibákon kívül, a veszélyre figyelmeztet a transzformátor-olaj gáz tartalmának megemelkedése, különösen azoké a gázoké, amelyeket a cellulóz lebomlása okoz, a transzformátor tartályának és magjának rezgése, a transzformátor zajszintjének megemelkedése (a mért megemelkedett zajszint 80dB is volt már)[9]. A GIC transzformátor károsító hatása fokozódó természetű. A kialakult túlmelegedésből eredő kár eredményeképpen megrövidül a transzformátor tekercselés szigetelésének élettartama, ami végül idő előtti tönkremenetelhez vezet.

"Végezetül, a transzformátor fél ciklusos telítettség okozta problémái, vonzzák a nagy gerjesztett áramot, aminek van egy alap frekvenciájú komponense, ami 90 fokkal késlelteti a feszültség szolgáltatást, így a transzformátor egy kiszámíthatatlan töltést ad a rendszernek. Ennek eredménye a harmonikus torzítások és hozzáadott terhelések, a meddő teljesítmény vagy VAR (Volt-Ampere Reactive - a reaktív villamos erő mérésére használt egység) következtében.

Az elektromos rendszernek csökken a feszültsége és túlterheli a hozzákötött szállító vezetékeket. Végül, a harmonizáció miatt a védelem nem megfelelően működik, és a kondenzátor mellékáramkörök túlterhelődnek. Ezek a feltételek előidézik a súlyos erőmű hibákat."[9]

A hatások csökkentése

Elektromos hálózat

Az elektromos erőművek rendszereiben a kockázatok csökkentésének még a napvihar bekövetkezése előtt kell megtörténnie. A kockázatok csökkentése a műszaki tervezésnél alkalmazott hibavédelemmel és a szimulációknál, valamint a továbbító vezetékek felmenő transzformátor táp vezetékeinek védelmével kezdődik. Megfelelő műszaki vizsgálatok nélkül nem lehet kiküszöbölni vagy csökkenteni az eredeti erőmű védelmi rendszerének tervezési hibáit, változtatni kell az elosztó rendszereken, hogy védekezni lehessen a napviharok hatásai ellen. A kockázatok elleni megfelelő védekezés feltétele egy teljes körű rendszer tervezési szemléletmód, hogy elkerülhetőek legyenek a nem kívánt kölcsönhatások. Az ellenáram és feszültség hatásait elemezni és értelmezni kell, hogy már a rendszer tervezésekor biztosítani lehessen az átfogó hibavédelmet. Továbbá az eszközök

9 P. R. Barnes, D. T. Rizy, B. W. McConnel, F. M. Tesche, E. R. Taylor, Jr., *Electric Utility Industry Experience with Geomagnetic Disturbances*, ORNL-6665, Oakridge National Laboratory, November 25,1991.

6 T. S. Molinski, W. E. Ferro, and B. L. Damsky, "Shielding grids from solar storms," IEEE Spectrum, November 2000, pp. 5560.

11 S. Odenwald, "The 23rd Cycle: Learning to live with a stormy star," Columbia University Press, New York, 2000.

9 P. R. Barnes, D. T. Rizy, B. W. McConnel, F. M. Tesche, E. R. Taylor, Jr., *Electric Utility Industry Experience with Geomagnetic Disturbances*, ORNL-6665, Oakridge National Laboratory, November 25,1991.

9 P. R. Barnes, D. T. Rizy, B. W. McConnel, F. M. Tesche, E. R. Taylor, Jr., *Electric Utility Industry Experience with Geomagnetic Disturbances*, ORNL-6665, Oakridge National Laboratory, November 25,1991.

tulajdonosainak és az ellenőrző rendszer forgalmazóknak meg kell teremteniük a lehetőséget a hibák elleni védekezésre, műszerekkel való ellátással, valamint ennek a médiában való kommunikálására. Amennyiben egy eszköz tulajdonosa úgy látja a műszaki hiba számítások (engineering fault calculations) alapján, hogy a CME által keltett várható energia meghaladja a rendszer védelmi képességeit, akkor a legjobb mérséklési lehetőség a vihar idejére, egy ellenőrzött üzemleállás lehet.

Egyéb ajánlott kockázat csökkentési eljárások egyike, hogy az elosztó transzformátor föld lábára kondenzátort vagy ellenállást kötnek (vagy ezek kombinációját), hogy csökkentsék a GIC maximumát. Az ilyen rendszerekhez szükség van egy GIC érzékelőre, amely előidézi az átkapcsolást, majd a vihar elmúlása után feloldja a földláb rövidre zárását. Az ilyen rendszerek kifejlesztése és üzembe állítása a magas költségek miatt a közeljövőben nem valószínű. Továbbá, a rövidre záró kapcsoló akadályozza a földláb biztonságos működését, amíg aktív. A NERC-nek jelenleg van egy geomágneses zavarok munkacsoportja, amitől ennek a területnek aktívabb kutatását várják el.

Egyéb vezérlő rendszerek

A napviharok alatt az üzemeltető személyzetnek a felügyelő rendszerek kommunikációs adatait figyelemmel kellene kísérnie, mivel a kommunikáció is érintett lehet, így felderítheti a normál értékektől való eltérést és üzemzavarokat. A kommunikációs rendszerek átmeneti vagy hosszan tartó üzemzavara tapasztalható. A védett fizikai réteget használó média kommunikációban nem tapasztalhatóak üzemzavarok. A tulajdonosoknak folyamatosan figyelniük és monitorozni kell a túl-feszültség-védelmet és alkalmazniuk kell szünetmentes tápegység (uninterruptible power supply – UPS) rendszereket ezen időszakban. A PLC, RTU, IED és más vezérlők, ha hatékony feszültség- és áramvédelemmel vannak telepítve, akkor nem lesznek érintve a mobilhálózat vagy vezeték nélküli szolgáltatás megszakadások által.

A fémburkolattal ellátott elektronikai eszközök valószínűleg jobban védettek a közvetlen elektromágneses hatásoktól. Viszont az eszközöknek maguknak is ellenőrizniük kell a hálózati feszültséget védő készülékeket, hogy fenntarthassák megfelelő működésüket. Az üzemeltetőknek gondoskodniuk kell az elektronikai eszközök további védelméről, nem elég a fémburkolat általi védelem. Amennyiben a működtetésre nincs feltétlenül szükség, akkor érdemes a felszerelés áramellátását lekapcsolni, az áramforrásokról lecsatlakoztatni a vihar jelzett időszaka alatt[14].

A vezérlő rendszerek kommunikációs rendszereit nem érintik közvetlenül a GIC-ek, de használják az elektromos hálózati erőforrásokat. Közülük számos rendszer épít a GPS-ek időzítő jeleire. Az ilyen rendszerek esetén a műszaki személyzetnek kell beavatkoznia az elektromos hálózat vagy a GPS üzemzavarai esetén a rendszer rugalmasságának megítélése alapján.

A műszaki hiba kalkulációkat alapul véve, a műszaki személyzetnek meg kell határoznia a feszültség által keltett energiát, ha ez meghaladja a rendszer tervezett védelmi kapacitását, akkor dönteniük kell egy szabályozott üzemszünetről a hatások mérsékelésére.

A nap viharok hatással lehetnek a vasúti közlekedést felügyelő rendszerekre, az adatszolgáltató rendszerek (SCADA) küldési műveleteire és a vezeték nélküli technológiákat alkalmazó kommunikációs hálózatokra, különösen azokra, amelyek függenek a GPS időzítő jelektől. A mérnököknek és a háttér karbantartó személyzetnek együtt kell működniük a CME események során, különösen ha úgy döntenek, hogy a rendszer kézi üzemmódban fusson.

A hosszútávú elképzelések szerint, azoknak a tulajdonosoknak és ipari vezérlő rendszer üzemeltetőknek, akik GPS időzítő jeleket használnak (pl.: mobil hálózatok RTU-k, IED-ek), gondoskodniuk kell integrált időzített mentéseket végző rendszerről, hogy egy vételi zavar vagy hiba esetén helyre lehessen állítani az ideiglenesen elveszett GPS-t. A GPS navigáció és

14 Government of Canada, "Geomagnetic Storms Reducing the Threat to Critical Infrastructure in Canada," http://www.solarstorms.org/CanadaPipelines.html, last accessed March 17, 2011.

helymeghatározó információk vételi zavara hatással lehet az olaj- és gázipar tengeri flottájának kritikus infrastruktúrájára, ahol a feltárási tevékenységekhez gyakran pontos helymegtartási műveletekre van szükség. A hajók el vannak látva hajófenék-rögzítő képességgel, ami felesleges funkciónak tűnik, habár, ha a hajó ellenőrzőrendszere nem tartalmazza a fenék rögzítő képességet, akkor a napvihar elmúltáig a hatáscsökkentő műveleteket fel kell függeszteni.

Koronakidobódás

Forrás: http://hu.wikipedia.org/wiki/Koronakidobódás

Koronakidobódás a SOHO űrobszervatórium LASCO koronagráfjának felvételsorozatán.

A **koronakidobódás** a naptevékenység egyik megnyilvánulása: a napkorona egy darabjának kilökődése a bolygóközi térbe.

Az angol szakirodalomban a koronakidobódások neve: „coronal mass ejection” vagy elterjedt rövidítéssel **CME**. (Magyar szövegekben gyakran találkozhatunk a „koronakitörés” vagy „koronakilövellés” elnevezésekkel is, ezek azonban mind az angol eredetit, mind a jelenség lényegét kevésbé hűen adják vissza. A Skylab-program idején – az 1970-es években – még „koronatranziens” néven is említették.)

A koronakidobódás oka a Nap mágneses terének instabilitása. A mágneses erők hatására a kidobódó plazmafelhő (melynek helyét természetesen azonnal kitölti a környező gáz) egyre gyorsuló emelkedésbe kezd, s a Napot elhagyva **bolygóközi mágneses felhő**vé válik. Az emelkedés sebessége végül többé-kevésbé állandóvá válik, bár ha a környező napszél (4-500 km/s-os) sebességétől jelentősen eltér, a közegellenállás miatt még további fokozatos lassulásnak vagy gyorsulásnak van kitéve. Egyes koronakidobódások sebessége akár a 2-3000 km/s-ot is elérheti.

A kidobott plazmafelhő tömege 10^{11} és 10^{14} kg között van, átlagosan 10^{12} kg. A kidobódás kezdetén mérete legfeljebb 100 Mm, hőmérséklete 1-2 millió K, benne a mágneses tér erőssége néhány gauss. A felszállás során a környező nyomás csökkenése miatt a plazmacsomó tágul és hűl.

A nagyobb sebességű koronakidobódások a környező koronában szuperszonikusan mozogva maguk előtt (és oldalt) lökésfrontok keltenek. Az ilyen nagy kidobódások ezért óriási, táguló buborék vagy csepp formájában jelennek meg a koronagráfos felvételeken. A lökésfront okozta plazmaoszcilláció rádiókitörést is okoz. Ilyen ún. II. típusú rádiókitörések a koronakidobódások mintegy 2/3-át kísérik.

Földi hatások

A naptevékenységi jelenségek közül a koronakidobódásoknak van a legerősebb földi hatása. A közvetlen hatások a következők:

- A kidobódásokat kísérő rádiókitörések megzavarhatják a rádiós kommunikációt és a radarok működését.
- A lökésfrontban felgyorsított nagy energiájú (akár 100 MeV feletti) protonok és más részecskék károsíthatják az űreszközöket, az űrhajósok, és a repülőgépek személyzetének egészségét.
- Ha a Föld a kidobott anyag útjába esik, a földi magnetoszférának ütközve mágnese vihart okozhat. A vihar megzavarhatja a navigációt, megbolondítva az iránytűket. Emellett a mágneses tér gyors ingadozása erős kóboráramokat indukálhat az elektromos berendezésekben, ami túlterhelést okoz, ez pedig olykor - elsősorban magas földrajzi szélességeken, például Kanada, Skandinávia - nagy területeket érintő áramkimaradásokhoz vezet.

- A magnetoszférában - a van Allen-övekben állandóan jelenlevő töltött részecskék a mágneses vihar következtében a sarkvidékeknél bejuthatnak a Föld felső légkörébe, ott a sarki fény néven ismert fényjelenséget okozva.
- A magnetoszférában a töltött részecskék mennyisége jelentősen megnőhet, ha a Földet eltaláló (koronakidobódásból eredő) bolygóközi mágneses felhő mágneses polaritása a magnetoszféráéval ellentétes. Ekkor ugyanis a felhő és a magnetoszféra között mágneses átkötődés történhet, s ennek révén a felhő plazmája bejuthat bolygónk magnetoszférájába.

A napvihar tevékenység hatásai időrendi sorrendben

1972. augusztus 2. - A napviharból származó GIC-ek a vízi- és elektromos áram erőműben 230 kV-os transzformátor robbanást okoztak[11].

1980. december 19. - Egy 735 kV-os transzformátor 8 nappal az Óriás Vörös Sarki fény (Great Red Aurora) után meghibásodott. A tartalék 735 kV-os transzformátor szintén tönkre ment a következő évben egy másik geomágneses vihar után[2].

1989. március 13. - Napviharból származó GIC-ek túlterhelték az észak-amerikai erőmű rendszert, ami számos állomáson a teljesítmény-kiegyenlítők deaktiválását okozta. Egy - ½ percen belül az erőmű rendszerben teljes áramszünet lett, és ez működési hiba több mint 15 különálló védelmi rendszerre volt hatással[2] [12].

Továbbá, a napviharokból származó GIC-ek egy 12 millió dolláros feszültségfokozó (step-up) transzformátort tettek tönkre egy másik erőmű rendszerben. A transzformátor kritikus eleme volt az elektromos erőmű elosztó rendszerének. A 288.8/24 kV-os egyfázisú, shell-form transzformátor egy földelt három fázisú (Delta csatlakozás) összeállításhoz volt csatlakoztatva. A transzformátorban okozott kár tartalmazza az alacsony feszültségű tekercselést, mindhárom fázis hőszigetelésének tönkremenését, és a vezető megolvadását[9]. Amennyiben elrendelik egy eszköz pótlását, akkor ennek magas a prioritása, de közel két évbe telik teljesíteni[6]. Attól számítva, hogy hozzájutnak az ideiglenes pótalkatrészhez, hat hét kell az üzembe helyezéshez az online működésig.

2003. október 30. - A svéd elektromos hálózatban 20-50 perces áramszünetet tapasztaltak egy erős napvihar miatt. Ugyanez a vihar okozott kárt 15 dél-afrikai transzformátorban, ahol néhány teljesen tönkre is ment[2].

---

11 S. Odenwald, “The 23rd Cycle: Learning to live with a stormy star,” Columbia University Press, New York, 2000.

2 James A. Marusek, “Solar Storm Threat Analysis,” http://www.breadandbutterscience.com/SSTA.pdf, last accessed February 16, 2011.

2 James A. Marusek, “Solar Storm Threat Analysis,” http://www.breadandbutterscience.com/SSTA.pdf, last accessed February 16, 2011.

12 J.G. Kappenman, L.J. Zanetti, and W.A. Radasky (1997) Geomagnetic storms can threaten electric power grid, American Geophysical Union: Earth in Space, Vol. 9, No. 7, March 1997, pp. 9−11.

9 P. R. Barnes, D. T. Rizy, B. W. McConnel, F. M. Tesche, E. R. Taylor, Jr., *Electric Utility Industry Experience with Geomagnetic Disturbances*, ORNL-6665, Oakridge National Laboratory, November 25,1991.

6 T. S. Molinski, W. E. Ferro, and B. L. Damsky, “Shielding grids from solar storms,” IEEE Spectrum, November 2000, pp. 5560.

2 James A. Marusek, “Solar Storm Threat Analysis,” http://www.breadandbutterscience.com/SSTA.pdf, last accessed February 16, 2011.

A VirusBuster Kft. összefoglalója 2011 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, majd a VirusBuster Kft. víruslaboratóriumának észlelései alapján áttekintést nyújtunk a 2011. január-március időszak leggyakoribb számítógépes károkozóiról, illetve azok legjelentősebb webes forrásairól.

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.

Kiemelkedő esetek

Van ok aggódni. Van a biztonsági szakembereknek miért dolgozniuk. És van a felhasználóknak jó okuk a védekezésre, korszerű, naprakész védelmi megoldás alkalmazására.

Dőlnek a vírusok, férgek, az őket terjesztő spam. Az idei első negyedévben könyvelte el az ötvenmilliomodik mintát kártevő-nyilvántartásában a nemzetközileg ismert IT-biztonsági laboratórium, az AV-Test. A nevezetes szám egy PDF file-nak jutott, amely az Adobe Reader egy sérülékenységét kiaknázva próbálja megfertőzni a Windows gépeket. A kártevő nyilvántartásba vétele újabb jele annak, hogy a számítógépes bűnözők fő célpontját már nem az operációs rendszerek vagy a böngészők, hanem a különböző cégektől származó alkalmazások jelentik. Az Adobe Reader mellett leggyakrabban a Flash plugineket és a Javát támadják.

Miközben szaporodnak és terjednek a mind kifinomultabb kártevők, a számítógépes bűnözők nemcsak a technológiát fejlesztik, hanem újabb és újabb trükkökkel állnak elő. Kreativitásukat sarkallja, hogy egy-egy ötletből – de akár csak egy botnet üzemeltetéséből – rengeteg pénzt zsebelhetnek be.

Egy amerikai férfi például közel 8 millió dollárra tett szert számítógépes csalásból. A 37 éves *Asu Pala* és társai olyan szoftverrel fertőzték meg áldozataik gépét, amely észrevétlenül többletdíjas telefonszámokat tárcsázott. A szoftverfejlesztőket Pala alkalmazta, majd a tesztelt programot kiosztotta bandája tagjainak. A beprogramozott telefonszámokat természetesen a csoport bérelte – érdekes módon németországi szolgáltatóktól. Valahányszor valamelyik számra hívás érkezett, a bandának pénz ütötte a markát. Pala ily módon 2003 és 2007 között összesen 7,94 millió dollárt zsebelt be. Az ügyészség szerint Németországban – és elképzelhető, hogy más európai országokban – legalább 250-en estek a bűnözők áldozatául, s fizették ki a többletszámlákat.

Pala „csak” pénztárcákat veszélyeztetett, ám más számítógépes bűnözők akár emberéletekre is törhetnek. Intő jel, hogy egy brit bíróság márciusban négy, terrorizmussal kapcsolatos vádpontban is bűnösnek találta a British Airways (BA) egyik volt rendszergazdáját.

A 31 éves *Radzsib Karim* a manchesteri egyetemen frissen szerzett elektronikai diplomával a zsebében posztgraduális gyakornokként, 2007-ben lépett be a légitársasághoz. Munkakörét azonban terrorista anyagok gyűjtésére és terjesztésére használta, s online kapcsolatot tartott egy radikális muszlim pappal. Mint a nyomozók kiderítették, Karim a BA londoni és newcastle-i hálózatáról rendszeresen bizalmas információkat küldött a Dzsammat-ul Mudzsahedin Banglades (JMB) elnevezésű terrorista csoportnak. Állítólag egy támadás részeként a légitársaság kritikus számítógép-rendszereinek lekapcsolására is készült.

„Radzsib Karim mindent megtett, hogy leplezze tevékenységét. A rendőrség terrorizmuselhárító parancsnokságán (Metropolitan Police Service Counter Terrorism Command) dolgozó szakértőknek azonban kilenc havi munkával sikerült megfejteniük 300, a vádlott gépének merevlemezén tárolt titkosított üzenetet" – nyilatkozott *Stuart Osborne* parancsnokhelyettes a BBC-nek. Hozzátette: ez volt csapatuk eddigi legbonyolultabb titkosítás-feltörési feladata.

Kiemelkedő áldozatok

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

Nos, az idei év első hónapjai többszörösen felhívták a figyelmet arra: senki nincs biztonságban. Hackertámadás áldozata lett például a francia elnök. Facebook lapján a betörők azt írták: nem indul jövőre az újraválasztásért.

A helyesírási hibákkal tűzdelt üzenet nem kevesebbet állított, mint hogy *Nicolas Sárközy* az „ország előtt álló rendkívüli körülmények miatt" úgy döntött: nem áll rajthoz az elnökségért 2012-ben esedékes versenyben. A szövegben egy másik Facebook lapra mutató link is volt, mely utóbbi oldal a *„Búcsú Nicolas Sárközytől"* címet viselte.

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

A közleményt egy bizonyos #hackercup2011 jegyezte, s mire a rendszergazdák a lapot visszaállították, már több mint 1800-an nyomták meg rá a Tetszik gombot.

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

Nem kis költségvetésű szervezetek is voltak a negyedév áldozatai között. Úgy tűnik, mindinkább hozzá kell szoknunk nemzetállamok, politikai egységek elleni online támadásokhoz. A gazdasági és politikai konfliktusok a kibertérbe is eszkalálódnak.

Márciusban kapott szárnyra a hír: a francia pénzügyminisztérium másfélszáznál több gépébe törtek be kiberbűnözők, s állítólag más minisztériumokat is támadás ért. A behatolások tavaly decemberben kezdődtek. A hackerek a nyomozás eredményei szerint a februári – Franciaország által elnökölt – G20 csúcsra vonatkozó állományokra vadásztak.

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

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

Egyes elemzők Kínát gyanítják a mostani akció hátterében, bár erre utaló konkrét bizonyítékot eddig nem találtak. Hogy ennek ellenére felmerült a gondolat, annak az az oka, hogy a

csúcstalálkozó központi témája a kereskedelem kiegyensúlyozatlansága volt – márpedig ebben az ügyben az ázsiai ország ugyancsak érdekelt.

Röviddel később ugyancsak súlyos informatikai támadás érte – mégpedig a brüsszeli csúcstalálkozó előestéjén – az Európai Bizottságot és az EU külügyi szolgálatát, hogy behatoltak a Bizottság Microsoft Exchange levelezőszerverébe. „Gyakran vesznek célba bennünket, de most nagyszabású támadás történt" – közölte a BBC-vel egy nevét elhallgató illetékes. Az uniós szakemberek azonnal reagáltak. A veszély felmérése után az Európai Bizottság – „annak érdekében, hogy ne kerüljön információ illetéktelen kezekbe" – letiltotta az e-mail és az intranet külső elérését, és a munkatársakat felszólították: változtassák meg jelszavaikat.

Ám a sorozatnak még nincs vége. Újabb pár nap elteltével az Európai Parlament lett kibertámadás áldozata, mire a strasbourgi biztonsági szakemberek többek között egy időre letiltották a webmail-hozzáférést.

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

Kiemelkedő kártevők

Ahogy telik az idő, hajlamosak vagyunk megfeledkezni minden idők „legeredményesebb" kártevőjéről, a Confickerről. Pedig a csönd nem jelenti azt, hogy elmúlt a veszély – mutatott rá a féreggel foglalkozó munkacsoport (Conficker Working Group, CWG) januárban közzétett tanulmánya, amelyet eredetileg a Rendon Group készített, az amerikai belbiztonsági minisztérium forrásai alapján. Hiszen meglehet: csak annak köszönhető, hogy nem okozott komolyabb kárt a féreg, mert alkotói visszariadtak az ellenük felvonultatott óriás erőtől.

A Conficker-nek keresztelt botnet-fertőzést 2008 novemberében fedezték fel, s 2009-ben végigsöpört az egész világon. Biztonsági szakemberek már 2008-ban összefogtak a féreg ellen – ez az együttműködés vezetett végül magának a CWG-nek a megalakításához. A Conficker elleni küzdelem hatalmas erőforrásokat mozgatott meg, s különböző szervezetek olyan szinten fogtak össze a probléma megoldása érdekében, amire korábban nem volt példa. Mindebből – hangoztatják a tanulmány szerzői – fontos tanulságokat lehet levonni arra nézve: hogyan célszerű felvenni a harcot az ilyen, egész világot érintő fenyegetésekkel szemben.

Mint megállapítják: annak ellenére, hogy a CWG-nek sikerült elvágnia a férget a bűnözőktől – azaz lehetetlenné tette a Conficker irányítását --, az anyag összeállítása idején még mindig 5 és 13 millió között becsülték a fertőzött windowsos PC-k számát.

Milyen ajánlásokat tesz az anyag a jövőre nézve? Nos, a szerzők egyebek mellett globális stratégia kidolgozását javasolják, hiszen hosszú harcra kell felkészülnünk. Fontosnak tartják a kormányok, valamint különböző szervezetek, például az ICANN bevonását.

Miután megemlékeztünk a kártevők koronázatlan királyáról, szóljunk pár szót az utóbbi hónapok „kisstílűbb", de attól még szintén veszélyes főkolomposairól!

Híven hűséges kutyájáról szóló jelmondatához – *„Buster mindig éberen figyel"* – a VirusBuster folyamatosan nyilvántartást vezet a hazai neten észlelt számítógépes károkozókról. A cég szakemberei kiértékelik házon belüli, illetve különböző helyeken működtetett levelezésvédő rendszereik fogását, s az adatokból hónapról hónapra toplistát készítenek, melyet a vállalat site-ján is megjelentetnek, a www.virusbuster.hu/labor/virus-toplista címen.

„Januárban folytatódott a szokásos, botnetekről terjesztett trójaiak áradata. Érdekesség, hogy az év első toplistájának elejére befutott egy fájlfertőző vírus is, a (táblázatainkban pirossal kiemelt) Win32.Sality, amely egyébként szintén köthető botnetekhez. Ez utóbbi azután később is megőrizte előkelő helyét. Emellett az egész negyedévben folyamatosan bombáztak minket a hamis antivírus

szoftvert telepítő trójaiak" – szólt észleléseikről *Szappanos Gábor,* a VirusBuster víruslaboratóriumának vezetője.

A három első hónap alább látható toplistájában a visszaköszönő családokat azonos színnel jelöltük.

Január

	Kártevő	Részesedés
1.	Trojan.Buzus	31.53%
2.	Win32.Sality.BK	5.92%
3.	Worm.SdBot.GAP	3.66%
4.	Trojan.Refroso.CYV	3.48%
5.	IRC.Flood.AQ	3.48%
6.	Trojan.DR.Agent	3.48%
7.	BAT.Noshare.AD	3.48%
8.	Worm.Rbot.BBRV	3.48%
9.	Backdoor.Rbot.BBVR	2.79%
10.	I-Worm.Netsky.Q	2.61%
	Egyéb:	36.06%

Február

	Kártevő	Részesedés
1.	Trojan.Buzus	30.00%
2.	TrojanSpy.SpyEyes	15.75%
3.	Win32.Sality.X	8.50%
4.	Trojan.DR.Agent	3.75%
5.	IRC.Flood.AQ	3.25%
6.	I-Worm.Netsky.Q	3.25%
7.	Trojan.Sasfis	2.75%
8.	BAT.Noshare.AD	2.75%
9.	Trojan.Buzus.BZNH	2.25%
10.	Trojan.Buzus.CADC	2.00%
	Egyéb:	25.75%

Március

	Kártevő	Részesedés
1.	Trojan.DL.Stohil	34.13%
2.	Trojan.Buzus	23.93%
3.	Trojan.DL.Chepvil	18.26%
4.	Win32.Sality.X	6.55%
5.	Trojan.PWS.Banker	3.15%
6.	I-Worm.Netsky.Q	1.64%
7.	I-Worm.NetSky.AB	1.01%
8.	IRC.Flood.AQ	1.01%
9.	BAT.Noshare.AD	0.88%
10.	Trojan.Buzus.CADC	0.63%
	Egyéb:	8.82%

Az sem érdektelen, hogy a weben barangolva hol kell leginkább fertőzéstől vagy adathalászattól tartanunk. Erre vonatkozóan a Commtouch elemzése 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	Parkolt domainek
2	Spam site-ok
3	Portálok
4	Pornográf, ill. szexuális tartalom
5	Oktatás
6	Szórakoztatás
7	Céges, üzleti site-ok
8	Vásárlás
9	Divat és szépségápolás
10	Számítástechnika, technológia

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

Leggyakrabban adathalászó site-kategóriák	
1	Játék
2	Egészségügy
3	Portálok
4	Számítástechnika, technológia
5	Divat és szépségápolás
6	Szabadidő, üdülés
7	Vásárlás
8	Sport
9	Oktatás
10	Streaming média, letöltések

Atomerőművek ellen?

Külön fejezetet érdemelnek a kiemelkedő kártevők közül, amelyek ipari folyamatirányító rendszerek ellen vethetők be. Tavaly világszerte nagy visszhangot keltett az első ilyen féreg, a Stuxnet terjedése. Lehet, hogy nem elég a földrengés, most már amiatt is aggódhatunk, hogy hackerek támadnak a reaktorokat irányító számítógépekre?

A kérdés nem alaptalan, elvégre a Stuxnetet szakértők szerint az iráni atomprogram tönkretétele vagy legalábbis hátráltatása céljával fejlesztettek ki.

A féreg 2009 júniusában kezdett terjedni. A közelmúltban azután *Meir Dagan,* a Moszad visszavonuló vezetője és *Hillary Clinton* amerikai külügyminiszter egymástól függetlenül annak a véleményének adott hangot, hogy az iráni nukleáris fejlesztés több évvel visszaesett. Tavaly novemberben *Mahmud Ahmadinedzsád* iráni elnök elismerte: kibertámadások „néhány centrifugában kisebb problémákat okoztak".

A *New York Times* nyomozása szerint az iráni Natanz urándúsító telepen használt Siemens centrifugavezérlő rendszerek sérülékenységeit az Egyesült Államok energetikai minisztériumához – az amerikai atomfegyverekért felelős kormányszervhez – tartozó Idahoi Nemzeti Laboratóriumban térképezték fel, még 2008 elején. Állítólag *George Bush* elnök titkos programot hagyott jóvá a Natanz körüli elektromos és számítástechnikai rendszerek megrongálására. A programot aztán kormányzati források szerint *Barack Obama* felgyorsíttatta, s állítólag hasonlóan léptek az izraeliek

is. A *New York Times* azt írta: a Stuxnet hatékonyságát egy, a Negev sivatagban működő titkos izraeli komplexumban tesztelték, ahol ebből a célból a natanzihoz megszólalásig hasonló centrifugasort állítottak üzembe.

Mindez új fejezetet nyitott nemcsak a kártevők, hanem a kiberhadviselés történetében is. Ámde szerepelhetnek-e hétköznapi hackerek egy olyan fejezetben, amelyet nagyhatalmi szóval írtak?

Nos, ugyancsak a negyedév híre, hogy egy orosz cég veszedelmes programkészletet dobott piacra, A Gleg nevű vállalkozás ipari folyamatirányító szoftverek sérülékenységeiből, illetve az ellenük bevethető kódból gyúrt össze támadókészletet, majd website-ján árulni kezdte a csomagot. Az Agora SCADA+ Pack 23 modulból áll, s állítólag a vevő a célba vehető szoftverek gyenge pontjairól szóló magyarázatot is talál az összeállításban. Aki megveszi a szettet, az különösebb programozói tudás nélkül is könnyen felépíthet egy ipari folyamatirányító rendszerek elleni szoftveres támadást – riogatott a sajtó.

Szappanos Gábor, a VirusBuster víruslaboratóriumának vezetője szerint figyelemre, elővigyázatosságra szükség van, aggodalomra azonban nincs ok. „Szerencsére egy ipari folyamatirányító géphez nem olyan könnyű hozzáférni. Meg aztán, bár az orosz szett összeállítói ügyesen igyekeznek meglovagolni a Stuxnet keltette érdeklődést, nem hiszem, hogy csomagjuk kasszasikert arat. – magyarázza a szakember. – Aki egy folyamatirányító rendszert akar megtámadni, az bizonyára óvatosabb annál, semhogy fegyverét az interneten vásárolja meg. Az sem valószínű, hogy egy hacker többféle rendszert venne célba, vagyis a potenciális vásárlóknak legfeljebb a csomag egy kis részére lenne szükségük. Mindenesetre az orosz cég lépése újra ráirányítja a figyelmet arra, amivel eddig nem sokat foglalkoztunk: a kritikus infrastruktúra felügyeletét ellátó számítógépes rendszerek sem sebezhetetlenek. Ugyanúgy hardver- és szoftverkomponensekből állnak, mint irodai társaik, vagyis óhatatlanul tartalmaznak kisebb-nagyobb sérülékenységeket. Mivel pedig ezek a rendszerek a kritikus infrastruktúra részei, kiemelt célpontnak számíthatnak, s ezért kiemelt figyelmet érdemelnek.”

Spam és botnetek

Rengeteg erőforrást leköt világszerte a kéretlen levelek, s legfőbb forrásuk, a botnetek elleni küzdelem. Mint a Commtouch világhálós fenyegetések alakulását elemző tanulmánysorozatának 2011 első negyedévéről szóló kiadásából kiderül, az idei év első három hónapjában átlagosan naponta 149 milliárd darab spam vagy adathalász üzenet röppent ki a világhálóra.

Ugyanakkor az átlag nem kis változást takar. Míg március elején még napi 168 milliárd kártékony üzenetet regisztráltak, a negyedév utolsó két hetében már „csak” 119 milliárdot. A drasztikus csökkenés oka egy olyan hír, amely nemcsak szaklapokban került előkelő helyre: a hírhedt Rustock botnet lekapcsolása. Egy cégcsoport, élén a Microsofttal sikeresen kiiktatta a hálózat vezérlőszervereit (amelyek egyébként csaknem mind az Egyesült Államokban működtek), s letiltotta a botnet által használt domain-eket. Ennek hatására a spamszint – tartósan – közel 30 százalékkal csökkent. Elemzők hozzáteszik: az óriási robothálózatban mintegy egymillió fertőzött PC ontotta a spamet. Volt idő, amikor a Rustock botnet szórta ki a világ spamtermelésének több mint felét.

És milyen témákról szóltak leggyakrabban a kéretlen levelek? Nos, továbbra is a gyógyszer vitte a prímet, noha részesedése a 2010 utolsó negyedévi 42-ről 28 százalékra esett. Eközben nőtt az előlegkérő, férfiaknak szánt és társkereső témájú üzenetek száma.

Akármilyen fontos eredmény egy nagy botnet kiiktatása, sajnos a robothálózatok tovább terjeszkednek. Az első negyedévben átlagosan naponta 258 ezer új zombit állítottak hadrendjükbe a kártevő- és levélszemét-szóró kiberbűnözők. Szerencsére azonban a botnet-fertőzöttség növekedése lassuló tendenciát mutat: 2010 harmadik negyedévében még 339 ezer, az év utolsó három hónapjában pedig 288 ezer gép került a rosszindulatú hálózatokba.

Továbbra is India a földkerekség „legelzombisodottabb” országa. Tizenhét százalékos részesedéssel vezet a – 12 százalékkal – második helyezett Brazília előtt. A dél-amerikai óriás negyedévvel korábban még a harmadik helyen állt, 8 százalékkal.

Nagyjából megfelelnek a fenti adatoknak az ICSA Labs mérési eredményei. A neves gyártófüggetlen amerikai tesztlaboratórium egy februári hét összesen közel 2,5 millió szemétbe való üzenetét feldolgozva a következő toplistát állította fel a küldő országokról:

	Ország	Üzenetszám	Részesedés
1	Brazília	292,046	12.1%
2	Oroszország	217,773	9.0%
3	India	195,295	8.1%
4	Indonézia	151,172	6.2%
5	USA	145,192	6.0%
6	Vietnam	137,568	5.7%
7	Ukrajna	100,052	4.1%
8	Kolumbia	60,807	2.5%
9	Dél- Korea	54,630	2.3%
10	Belorusszia	47,688	2.0%

Folt hátán folt

Bőven volt okuk az elmúlt hónapokban is a szoftvergyártóknak arra, hogy termékeikhez biztonsági frissítéseket bocsássanak ki.
A következőkben röviden, időrendben a legfontosabb foltokat tekintjük át.

Január

- Két biztonsági frissítést bocsátott ki menetrendszerű foltozó napján a Microsoft. A foltok összesen három sérülékenységet orvosoltak. A javítócsomagok közül az egyik „kritikus”, a másik „fontos” minősítést kapott. Mindkét folt a Windowshoz készült.
- A Google 8.0.552.237-as számú Chrome verziójával összesen 16 sérülékenységet orvosolt.
- Összesen 66 sérülékenységet orvosolt az Oracle. Kritikus folto(ka)t kapott például az adatbázis-szerver, az Application Server, a WebLogic Server, a Solaris, a Fusion Middleware, az Audit Vault, a PeopleSoft Enterprise és az Open Office.

Február

- Februári foltozó keddjén 12 biztonsági frissítéssel jelentkezett a Microsoft. A foltok összesen 22 sérülékenységet orvosoltak. A javítócsomagok közül három „kritikus”, a többi kilenc „fontos” minősítést kapott. A foltok által javított szoftverek: Windows, Office, Internet Explorer and IIS (Internet Information Services).
- Kritikus sérülékenységeket orvosolt népszerű PDF-szoftvereiben az Adobe. A hibák következtében az alkalmazás összeomolhatott, illetve a réseket kiaknázó esetleges támadók irányításuk alá vonhatták az áldozat gépét. Az érintett programváltozatok: Reader és Acrobat X Windows és Macintosh környezetben, valamint a Reader 9.4.1-es és régebbi kiadásai Windows, Macintosh, illetve UNIX alatt.
- Biztonsági frissítést bocsátott ki Java futásidejű környezetéhez az Oracle. Az új változat összesen 21 sérülékenységet orvosolt, melyek közül 19 kiaknázása akár rosszindulatú szoftver távolból való telepítését is lehetővé tette egy esetleges támadó számára.

- A Microsoft védelmi motorjának (Malware Protection Engine) frissítése egy sérülékenységet is javított. A probléma által érintett szoftverek: Windows Live OneCare, Microsoft Security Essentials, Windows Defender, Forefront Client Security, Forefront Endpoint Protection 2010, valamint a Rosszindulatú Szoftvert Eltávolító Eszköz (MSRT).

Március

- Böngészőjének új változatával összesen 19 sérülékenységet is orvosolt a Google. Három híján valamennyi Chrome-résnek komoly kockázatot tulajdonított a keresőkirály.
- Három biztonsági frissítést bocsátott ki e havi menetrendszerű foltozó napján a Microsoft. A foltok összesen négy rést fedtek be. A javítócsomagok közül egy „kritikus", a másik kettő „fontos" minősítést kapott. A foltok a Windowshoz és az Office-hoz készültek.
- Kirukkolt a Google a Chrome 10-es változatával. A 10-es verzió biztonsági szempontból is több új elemet tartalmazott: homokdoboz- (sandbox-) védelmet kapott Windows platformon az Adobe Flash Player plug-in, s a fejlesztők 25 sérülékenységet – köztük számos „nagy kockázatot jelentőnek" minősítettet – is javítottak.
- Felfrissítette böngészőjét az Apple. A Safari 5.0.4 kibocsátásával az almás cég nem kevesebb, mint 62 sérülékenységet orvosolt. Biztonsági frissítés jelent meg az Apple TV-hez és az iOS-hez is.
- Megjelent a MacOS 10.6.7 jelű változata, amely az almás operációs rendszer 10.5.8-as, valamint 10.6-10.6.6-os verzióját váltotta fel. Része volt a frissítésnek a 2011-001-es számú biztonsági folt, mely a hírek szerint összesen 56 sérülékenységet orvosolt.
- Hat rést tömött be a Google böngészőjének új változata, a Chrome 10.0.648.204.

Hiába jelennek meg azonban a foltok, a frissítések, ha a felhasználók nem telepítik őket.

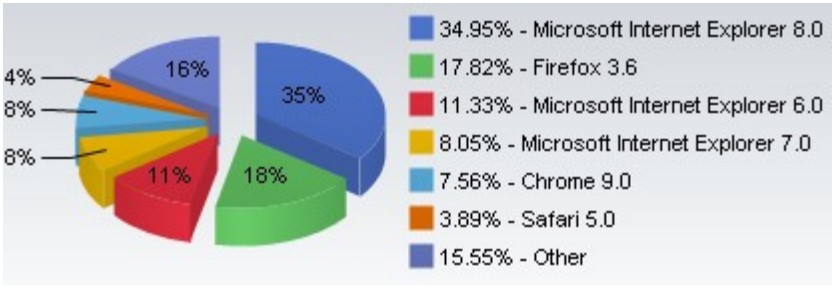
Elkeserítő számokkal jelentkezett ebben a tekintetben az év elején a Qualys. A cég tavaly tette elérhetővé BrowserCheck elnevezésű ingyenes szolgáltatását, amely Windows, Mac és Linux alapú gépeken kutatja fel a kockázatot jelentő réseket. A megoldás a böngésző mellett összesen 18 gyakran használt plugin-t is átvilágít, köztük az Adobe Flasht és a Windows Media Player-t. A szolgáltatás valamennyi elterjedt böngészőre – Internet Explorerre, Firefoxra, Safarira, Chrome-ra és Operára – egyaránt alkalmazható.

Nos, az idén januári adatok szerint az összes átvizsgált gép 80 százalékában nyitva állt legalább egy – a gyártó által már javított – böngésző-rés. Mindez különösen aggasztó, ha figyelembe vesszük, hogy aki a BrowserCheck-kel átnézeti a gépét, az nyilván biztonságtudatosabb az internetezők többségénél.

Úgy tűnik, a plugin-ek közül legkevésbé az Oracle Javát frissítik a felhasználók – ez az esetek 40 százalékában bizonyult sérülékenynek. Persze más plugin-ek foltjainak telepítésében is bőven van elmaradás: az Adobe Reader 32, a QuickTime 25, a Flash 24, a Shockwave 22, a Windows Media Player pedig 10 százalékos sebezhetőségi arányt mutatott.

És ha már a böngészők frissítéséről szólunk, negyedéves áttekintésünk végén nem hagyhatjuk említés nélkül azt a kampányt, amelyet a Microsoft indított az Internet Explorer immár több mint tízéves 6-os verziójának a világhálóról való eltüntetése, az új változatokra való áttérés érdekében.

Gyorsan változó korunkban tíz év még egy autónak is sok, nemhogy egy számítógép-programnak. Nem csoda, hogy a Microsoft azzal „ünnepelte" az Internet Explorer 6 tizedik születésnapját, hogy külön webhelyet állított fel a felhasználók felvilágosítására. Az „IE6 visszaszámláló" site-on (www.theie6countdown.com) láthatjuk a tízéves szoftver pillanatnyi világpiaci részesedését – ami februárban 12 százalékon állt –, sőt azt is, hogy egyes fontosabb országokban a szörfösök mekkora hányada ragadt le az IE6 mellett.



Forrás: NetApplications.com

Egy ilyen régi – és különösen egy ingyenes – szoftver esetében meglepőnek tűnhet, de tény: Kínában ez az arány 34,5, Koreában pedig 24,8 százalék. Tíz százalék felett van a verziót használók részesedése Indiában, Japánban és Vietnámban is – de ezen már nincs mit csodálkozni, ha hozzátesszük, hogy még a britek 3,5 vagy az amerikaiak 2,9 százaléka is az IE6-tal járja a világhálót. Magyarországról nem közöl adatot a Microsoft-site, de ezek után valószínű, hogy mi sem jeleskedünk az új verziókra való áttérésben. Ez pedig nem kis kockázatot jelent.

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

A VirusBuster Kft.-ről

A több mint 15 éves szakmai tapasztalattal rendelkező, kizárólag magyar tulajdonú VirusBuster Kft. (www.virusbuster.hu) 1997 óta nyújt teljes körű vírusvédelmi és biztonságtechnikai megoldásokat szinte minden platformon a magyar és a külföldi piac számára. A kft. termékei számos magyar és nemzetközi független teszten kaptak kitűnő minősítést. A cég fő terméke, a VirusBuster Professional több alkalommal szerezte meg a „Virus Bulletin 100%" díjat, a „Checkmark Anti-Virus Level One" és „CheckVir" elismerést, valamint az ICSA Labs nagy nemzetközi presztízsű „Desktop/Server Anti-Virus Detection" minősítését, majd 2007-ben és 2008-ban elnyerte az ICSA Labs „Desktop/Server Anti-Virus Cleaning" tanúsítványát. 2008-ban a cég megszerezte az OESISOK tanúsítványt, mely azt igazolja, hogy egy alkalmazás tökéletesen együttműködik a vezető piaci fejlesztők –- a Cisco, a Juniper, a NORTEL, a 3Com, az F5 –- hálózati eszközeivel, illetve a hálózatok védelmét szolgáló, a csatlakozó végpontok „egészségét" ellenőrző NAP, NAC és TNC rendszerekkel.

A VirusBuster világszerte elismert szakemberei rendszeres előadói hazai és nemzetközi konferenciáknak. Bozsó Julianna, a cég ügyvezető igazgatója az Informatikai Vállalkozások Szövetségétől (az IVSZ-től) 2008-ban elnyerte az „Év Informatikai Cégvezetője" díjat.

A kft. 2003-ban „Év innovatív üzleti megoldása", 2004-ben pedig „IT Reménység" díjban részesült. Két ízben is megkapta a cég az IVSZ-től a „Minősített Szoftver Exportőr" címet és 2005-ben megszerezte az MSZ EN ISO 9001:2001 szabvány szerinti minőségirányítási tanúsítványt. A VirusBuster webáruháza 2009-ben kiérdemelte a „Fair Business" minősítést, s ugyanebben az évben a cég Üzleti Etikai Díjat kapott.

Elérhetőségeink

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

1063 Budapest, Munkácsy M. u. 16.

Levélcím: 1398 Budapest, Pf.: 570.

Tel: (1) 301-20-30

Fax: (1) 353-19-37

Web: www.cert-hungary.hu

A 0/24 órás Nemzeti Hálózatbiztonsági Központ ügyelet adatai:

E-mail:cert@cert-hungary.hu

Tel.: +36-1-301-2079

Fax: +36-1-353-1937