Hírek a digitális világból

(Hírtallózó)

Tartalom: **2008/október** | Archívum | Eddigi hírek

2008.10.31. ← Az netezés fejleszti az agyunkat?
2008.10.30. ← A gazdaság gyengül: reagálnak a bűnözők is
2008.10.29. ← Értékes gépeket loptak a PTE Biofizikai Intézetéből
2008.10.28. ← Svédországban életre keltik az elemi gonoszságot
2008.10.27. ← Követhetetlen botnetek
2008.10.26. ← Könnyű kijátszani a netcenzúrát
2008.10.25. ← A netezés jót tesz a nagyinak
2008.10.24. ← Alig található szabványos weboldal az interneten
2008.10.23. ← Kötelező internetszűrést vezet be az ausztrálok
2008.10.22. ← Bezárták az online „bűnözőboltot"
2008.10.21. ← Horogra akadt az egyházromboló fiú
2008.10.20. ← A privacy vége: azonosítót kapnak a kínai netezők
2008.10.19. ← Telefonálj az összes berlini rendőrnek!
2008.10.18. ← Mától mindenkiből lehet digitális bliccelő
2008.10.17. ← Vásárolni lehet a YouTube-videókból
2008.10.16. ← E-vásárlás: most éri utol az uniós jog hazánkat
2008.10.15. ← Banki adatokra halásznak a pénzügyi válságban
2008.10.14. ← Több ezren blogolnak a szegénység ellen szerdán
2008.10.13. ← Üzenet az UFOknak
2008.10.12. ← Saját térképet rajzolhat a Google Mapsre
2008.10.11. ← Levélszemét: 236 millió dollár büntetés
2008.10.10. ← Félnek a bankok a hackerbiztos számítógépektől
2008.10.09. ← Fotóalbumot lehet készíteni az iWiW-en
2008.10.08. ← Új internetes szervezet a gyermekek védelmére
2008.10.07. ← Adható-vehető hazánkban az e-mailes címlista
2008.10.06. ← Terroristák a kamera memóriájában
2008.10.05. ← Hiba miatt volt letölthető 40 ezer film
2008.10.04. ← Súlyos sebezhetőség a böngészőkben
2008.10.03. ← Korlátozott netelérés – bírói engedéllyel
2008.10.02. ← Kutass prímeket 150 ezer dollárért!
2008.10.01. ← Alattomosan támad a Limbo trójai

↑ Az internetezés fejleszti az agyunkat, serkenti az agyműködést (2008. október 31.)

Egy tanulmány szerint az agyi aktivitásunk jelentősen megnő, amikor a hálón böngészünk, s egy szimpla keresés lefuttatása is jobban serkenti a szürkeállományunkat, mint egy könyv olvasása.

A Daily Telegraph brit napilap értesülései szerint egy kutatás kimutatta, hogy az efféle tevékenység közben jelentősen megnő a homlok- és a temporális lebeny aktivitása, amelyek az emberi szervezet vizuális központját, a döntéshozó mechanizmusokat és a memóriát is működtetik.

Az absztrakt gondolkodásért és az empátiáért felelős agyterületek ezzel szemben csaknem teljesen sötétek maradtak. A tanulmányt készítő kutatók szerint vizsgálatuk rámutat arra, hogy agyunk miként fejlődhet a technológia hosszú távú használatának köszönhetően.

Ennek ellenére figyelmeztettek rá, hogy aki túlzásba viszi az internetezést, az a szociális életét, illetve emberi interakciós képességeit károsíthatja. Korábbi vizsgálatok szerint az intenzív számítógép-használat fokozhatja a figyelemhiány-hiperaktivitás (Attention Deficit Hyperactivity Disorder – ADHD) szindrómát.

„A mai fiatalokat szinte megfullasztja a rájuk zúduló információtömeg, ráadásul az ő agyuk még jóval inkább formálható, mint az idősebbeké" – magyarázta a Telegraph riporterének Dr. Gary Small, a University of California, Los Angeles öregedési központjának igazgatója. „Darwin szerint a következő generációk már alkalmazkodnak a környezetükhöz. Azok, akiknek jó érzékük van a technológia használatához, előnyösebb helyzetben lesznek, jobb anyagi helyzetet teremthetnek maguknak, s utódaiknak egyaránt."

A vizsgálat során 24, 55-76 év közötti önkéntes agyát vizsgálták. A mágneses szkennerrel végzett kísérletek közben az alanyoknak internetes kereséseket kellett végeznie, illetve könyveket olvasnia. Az eredmények azt mutatták, hogy az első csoport tagjainak agya jóval aktívabb volt.

„Az eredmények biztatóak, ugyanis azt a következtetést vonhattuk le belőlük, hogy a számítógépes technológiáknak pszichológiai hatása is lehetnek, s jótékonyan befolyásolhatják a középkorú, de akár az idősebb felnőtteket is" – tette hozzá a szakember. „Az internetes kereséshez összetett agyi aktivitásra van szükség, amely serkentheti az agyfunkciókat."

A felfedezést az amerikai időskori pszichiátriával foglalkozo American Journal of Geriatric Psychiatry című folyóiratban publikálták.

Nem mindenki ért egyet azonban a kutatókkal, Igor Aleksander az Imperial College London neurális rendszerekkel foglalkozó mérnöke úgy fogalmazott: „lehetséges, hogy az internetezéssel különböző agyterületeket stimulálhatunk, azonban nem látom, hogy ugyanezt miért ne lehetne más helyzetben, más módszerrel is elérni."

(Forrás: Hvg.hu)

↑ A gazdaság gyengülésére is reagálnak az online bűnözők

(2008. október 30.)

A kiberbűnözőket is érzékenyen érinti a gazdasági válság: a bankcsődökkel és a tőzsde ingadozásával együtt alakul a feketegazdaság is.

A PandaLabs újonnan nyilvánosságra hozott kutatásai szerint a kiberbűnözők és az általuk működtetett „online feketegazdaság" is rendkívül érzékeny a gazdasági élet változásaira. A bankcsődökre reagálva például az online „kampányok" az elmúlt hónapokban megváltoztak: a statisztikák azt mutatják, hogy az adathalász (phishing) támadások visszaszorulóban vannak, helyette új, jóval közvetlenebb módszerekkel próbálkoznak a bűnözők.

„Nem olyan régen hívtuk fel a figyelmet arra, hogy hamis antivírus-termékek megvételére próbálják meg rávenni a felhasználókat a csalók" – magyarázta Sándor Zsolt, a Panda Security magyarországi igazgatója. „Az adathalász támadások áttételesek, hiszen banki jelszavakra és hozzáférésekre irányulnak; a hamis vírusirtós próbálkozásokkal a csalók már közvetlenül a pénzre utaznak. Számításaink szerint mindezzel nagyjából havonta 10 milliós profitot termelnek az online feketegazdaságnak."

A szakemberek szerint a csalások egyre kifinomultabbak, és egyre szervezettebbek lesznek: az összehangolt támadások eredményeképpen a profit is növekszik.

„Természetes a fordított arányosság a gazdaság és az online feketegazdaság között – fűzte hozzá Sándor Zsolt. – A gazdasági vészhelyzetben az emberek nagyobb figyelmet fordítanak a pénzügyekre, esetleg nem is intéznek pénzügyeket, hanem kivárnak. Ilyen esetekben a bűnözőknek sokkal nagyobb támadást kell indítaniuk, hogy azonos eredményt érjenek el."

(Forrás: Hvg.hu)

↑ Értékes számítógépeket loptak a PTE Biofizikai Intézetéből

(2008. október 29.)

Értékes, speciális kártyákkal felszerelt, öt év kutatási adatait tároló számítógépeket loptak el a napokban a Pécsi Tudományegyetem (PTE) Biofizikai Intézetéből, a kár tízmillió forint – közölte a intézet adjunktusa.

Grama László beszámolt arról, hogy az ismeretlen elkövetők a mikroszkópos laborba törtek be, onnan vittek el berendezéseket az azokhoz tartozó, mikroszkópokat vezérlő kártyákkal, továbbá a merevlemezeken rögzített, sejtek és sejtekből izolált fehérjék vizsgálatával kapcsolatos alapkutatási adatokkal együtt.

Hozzátette, a kutatási eredmények kilencven százalékáról készült biztonsági másolat, így azok nagy része nem veszett el, a kártyák pótlása ugyanakkor milliókba kerül, azokat pályázati források elnyerése nélkül az intézet nem tudja beszerezni.

Mártonfalvi Zsolt egyetemi gyakornok arról szólt, hogy a speciális kártyák és az emberi test sejtműködésének jobb megértését célzó kutatási adatok önmagukban eladhatatlanok, de hiányuk miatt hónapokig nem tud dolgozni az ezzel foglalkozó szakembergárda.

Megjegyezte, bíznak abban, hogy a rendőrség elfogja az áruk eszmei értékéről mit sem tudó tolvajokat, vagy a számítógépek és a kártyák megtalálója értesíti az intézetet, s visszaadja az ellopott berendezéseket.

(Forrás: Hvg.hu)

↑ Svédországban életre keltik az elemi gonoszságot

(2008. október 28.)

Négy évnyi kutatás után új mérföldkövéhez érkezett az emberi gonoszság kutatása. Selmer Bringsjord, a Rensselaer Politechnikum kognitív tudományok tanszékének vezetője egy olyan virtuális személyiséget alkotott meg, amely szeret másoknak ártani és már lehet is vele beszélgetni. Igaz, megalkotója nem merné elhelyezni a Second Life-ban sem.

Ahhoz, hogy valaki igazán gonosz legyen, olyan morálisan rossz tettet kell elterveznie, amellyel reményei szerint másoknak jelentős kárt tud okozni, emellett pedig kvázi lényegtelen is az, hogy ezt végre tudja-e hajtani – mondja Bringsjord. Ehhez még hozzájárul az is, hogy ha ezen gonosz személyiség indokait akarjuk elemezni, az általa felhozott érvek vagy inkoherensek lennének, vagy pedig tudatában lenne annak, hogy mások által morálisan rossznak tartott cselekedetre készül, de ezt ő jónak tekintené.

Bringsjord és társai először 2005-ben hozták létre azt az „E" névre keresztelt szoftverszemélyiséget, amely a fenti definíció alapján működött. Eredetileg E csak egy program volt, a kutatók azonban egy, a képen is látható fizikai külsőt is kölcsönöztek neki. Bringsjord szerint E gonoszabb verziója az 1989-es Holt Költők Társasága c. filmben szereplő Mr. Perry-nek, bár szerinte még ez a külső sem tükrözi pontosan a gondolati hátteret, így vélhetően E „arcot fog váltani" a jövőben.

A virtuális személyiséggel legutoljára egy esettanulmányt reprodukáltak, amely a kísérletet ihlető M. Scott Peck pszichiáter könyvén alapul: a példában egy fiú szerepel, akinek a szülei azt a fegyvert adják a kezébe, amellyel a bátyja követett el korábban öngyilkosságot. E jelenleg az érvelés és a morális döntések azon szintjén áll, amelyen azt képes állítani: ő adta oda a pisztolyt a bátyjának, mert annak éppen szüksége volt egyre.

2008 végére a gonosz negyedik generációját hozzák létre, amely a belekötött mesterséges intelligencia révén már tud angolul beszélgetni azokkal, akik megszólítják, a szlenget viszont még nem fogja érteni. Bringsjord maga is bevallja, hogy projektje még egy szoftver esetében is etikai kérdéseket vet fel. Azt mondja, ezt a karaktert semmiféleképpen nem rakná be a Second Life-ba, de még egy egyszerű virtuális környezetbe sem előre kialakított biztonsági rendszerek nélkül – ezek olyan etikai szabályok lennének, amelyeket Asimov fogalmazott meg a robotika három alaptörvényeként: a robot nem árthat az embernek és nem nézheti tétlenül azt, hogy az embert veszély fenyegeti, köteles engedelmeskedni az emberek parancsainak, ha ezzel nem veszélyeztet embert, illetve köteles magát megvédenie addig, amíg ez nem ütközik az előző szabályokba.

(Forrás: Hvg.hu)

↑ Követhetetlen botnetek

(2008. október 27.)

A botnetek világa folyamatos változáson esik át. A kártékony hálózatok hol eltűnnek, hol újra életre kelnek.

Az elmúlt időszakban több biztonsági cég is jelezte, hogy a Storm trójai révén kiépült, fertőzött számítógépekből álló botnet hálózat jelentősen meggyengült. Többek között a Marshal valamint az Arbor Networks is arról adott hírt, hogy ennek következtében a Storm botnet által generált spamek mennyisége jelentősen csökkent.

A Storm trójai 2007 elején bukkant fel, és azóta jelentős károkat okozott. Az általa felépített botnet 2007 közepén volt a legnagyobb, amikor a világszerte terjedő levélszemét 20 százalékát generálta. Tavaly szeptemberben azonban a Microsoft úgy határozott, hogy a kártékony programokat eltávolító eszközét felkészíti a Storm irtására. A cég döntése és megoldása sikeresnek bizonyult, ugyanis nem sokkal később a Storm botnet mérete 250 ezer számítógéppel csökkent. Jose Nazario, az Arbor Networks biztonsági kutatója azonban arra egyelőre nem tudott magyarázatot adni, hogy az elmúlt hetekben mi is történhetett a Storm botnettel.

A Storm gyengülése azonban nem azt jelenti, hogy a védekezésben van egy kis szusszanásnyi idő, ugyanis a napokban – a változatosság kedvéért – a Warezov botnet aktivitása növekedett meg jelentős mértékben. A SecureWorks szerint a Warezov féle kártékony hálózat elsősorban a Hotmail rendszerét szemelte ki magának, és ennek felhasználásával igyekszik minél több spamet a postafiókokba eljuttatni. A Warezov meglehetősen sikeresen képes áthatolni a Hotmail CAPTCHA rendszerén. A szakemberek egyelőre még nem tudják, hogy pontosan miként kerüli meg ezt a védelmi vonalat, de feltételezhető, hogy az optikai karakterfelismerés mellett emberi tényező is szerephez jut.

A SecureWorks szerint a támadók most már óvatosabbak, és megfontoltabbak. Ennek oka, hogy a feltört vagy az automatikus eszközök révén létrehozott Hotmail postafiókokból naponta csak néhány spamet küldözgetnek ki, és ezzel hatástalanná válnak a Hotmail mennyiségi korlátozásai.

A spammerek számára fontos, hogy jól ismert, webes levelezőszolgáltatásokhoz tudjanak automatizált módszerek révén hozzáférni, ugyanis ezzel meg tudják kerülni az egyre nagyobb szerephez jutó, reputációs eljárásokat is felvonultató spamszűrőket. Ha például a Hotmail rendszeréből küldik ki a leveleiket, akkor a „hírnév alapú" védelem nem fogja kiszűrni a levelet, és így azokat nagyobb valószínűséggel képesek eljuttatni a felhasználók postafiókjába.

(Forrás: Biztonsagportal.hu)

↑ Könnyű kijátszani a netcenzúrát

(2008. október 26.)

Könnyen kijátszhatóak a szólásszabadságot korlátozó rendszerek, a hatalom pedig néha több kárt okoz magának a korlátozásokkal, mint amennyi a haszna ezen – magyarázta számos példát felhozó előadásában Ethan Zuckerman, a világ legkülönbözőbb pontjain élő civil újságírók által működtetett Global Voices híroldal képviselője az Internet Hungary konferencián, Tihanyban. A kilencvenes évek Malajziájának egyik, a hivatalos médiából külföldön működtetett honlapokra szorult ellenzéki vezetőjét később államfővé választották, a helyi parlament egyik tagja pedig bloggerként szerzett – később mandátumra váltott – országos ismertséget, Bahreinben a kormány azért gátolta meg egy internetes térképprogram elérését, mert azzal könnyűszerrel kideríthető volt: a kevés megművelhető föld nagyján palotakertek, nem pedig ültetvények vannak – sorolta, „Demokratizáltuk mára az internetet: nem a tudósoké már, hanem mindenkié, akinek van közölnivalója" – jegyezte meg, azt vizionálva, hogy a nemsokára már nem a mobiltelefonokon, hanem online tárolt saját felvételekkel „mindannyian kiadókká válunk".

A kormányzat számára nem kívánatos tartalmakat kiszűrő „Kínai Nagy Tűzfal" példáját említve arról beszélt: mivel a világ legnépesebbállamában nem gátolják a privát témák netes kitárgyalását, így sok ottani fiataltól azt hallani, Kínában zabadabb a világháló-használat, mint például az Egyesült Államokban. Előadása végén Ethan Zuckerman megjegyezte: „a szólásszabadság nem garancia arra, hogy meg is hallgatnak bennünket".

(Forrás: Origo.hu)

↑ A netezés jót tesz a nagyinak

(2008. október 25.)

Amerikai kutatók szerint középkorú és idős emberek számára kifejezetten hasznos lehet az internetezés, ezzel ugyanúgy karbantartható az agyműködés, mint mondjuk keresztrejtvényekkel – írja a BBC.

A Kaliforniai Egyetem Los Angeles-i kutatócsoportjának kísérletei szerint a weben való barangolás, keresgélés az agy azon területeit stimulálja, amelyek döntéshozatalkor vagy bonyolult érvelés során aktívak. Az internetezéssel akár még azok az öregedéssel járó fiziológiai változások is visszafordíthatók, amelyek a gondolkodás lassulását okkozzák – számoltak be a kutatók kísérleteik eredményeiről az American Journal of Geriatric Psychatry szaklapban.

A BBC beszámolója szerint az már régóta ismert, hogy a keresztrejtvények fejtésével vagy más hasonló, az agy működését aktívan igénylő foglalatosságokkal minimalizálható az öregedés hatása, a friss kutatás szerint ezekhez a tevékenységekhez a weben való szörfözést is hozzá lehet venni a jövőben. Gary Small, a egyetem kutatását vezető professzor szerint eredményeik bíztatók, például kiderítették, hogy az internetes keresések végrehajtása is egy olyan komplikált művelet, amely segít tréningezni az agyműködést, ami segíthet elejét venni az öreg kori elbutulásnak...

A kísérletet huszonnégy 55 és 76 év közötti korú önkéntesekkel hajtották végre, a csoport felét gyakorlott internetező volt, s a feladatok végrehajtása közben monitorozták agyműködésüket. Ebből kiderült, hogy a webes keresés és egy könyv olvasása egyaránt komoly aktivitásra sarkallta az agynak azon részeit, amelyek a nyelvek megértésével, az olvasással, a memóriával vagy a látással kapcsolatosan. Ugyanakkor az internetet már gyakorlottan használók esetében azt is felfedezték, hogy az agy döntéshozatalokért és érvelésért felelős régiói is aktivizálódtak az internetezés során, a világhálóval frissen ismerkedők esetében viszont nem.

(Forrás: Origo.hu)

↑ Alig található szabványos weboldal az interneten

(2008. október 24.)

A böngészőiről ismert norvég Opera Software nyilvánosságra hozta egy folyamatban lévő kutatásának részeredményeit, betekintést engedve a jelenleg működő weboldalak szerkezetébe.

A cég a kutatáshoz létrehozott egy eszközt (MAMA – Metadata Analysis and Mining Application), mely átrágta magát 3,5 millió weboldalon, indexelve azok felépítését, programozási megoldásait és egyéb statisztikai adatait. Az összegyűjtött adatok elemzésével az Opera mérnökei a webfejlesztésben felmerülő trendekkel kapcsolatban jutottak meglepő eredményekre, emellett megvizsgálhatták azt is, hogyan használják a szabványos technológiákat szerte a világhálón.

Az előzetesen publikált adatok alapján jónéhány érdekesség derült ki a HTML-elemek használatával kapcsolatban. Az még nem meglepő, hogy a MAMA által elemzett oldalak legnépszerűbb HTML-címkéi a head, title, html, body, a, meta, img és a table voltak, míg a legritkábban használtak a var, del és a bdo, hiszen ezt kutatás nélkül is megmondta volna bárki. Az sem borzolja fel a kedélyeket, hogy CSS-t főként színezésre és betűformázásra használnak a weboldalkészítők.

Az viszont már figyelemfelkeltőbb, hogy az összes weboldal 35 százaléka használ Adobe Flash-t, sőt, Kínában az oldalak kétharmadán találhatóak ilyen tartalmak. Az AJAX technológiákat viszont csak az oldalak 3,2 százalékán találtak a robotok, ebben éppen az Opera hazája, Norvégia volt kiugró a maga egytizedes arányával. Abszolút elterjedtnek számít viszont a CSS, ami a vizsgált oldalak 80 százalékában volt fellelhető, JavaScript-kódokat pedig a lapok háromnegyede futtat.

Az Opera az alaptechnológiák mellett a MAMA-t egy W3C-jóváhagyó eszközzel is felvértezte, hogy ne csak az derüljön ki, hogy mit használnak a készítők, hanem az is, hogy mennyire sikerül betartaniuk a szabványokat. Az eredmények igazán kínosak, a meglátogatott weblapoknak csak 4,13 százaléka volt a szabványoknak megfelelő. Ennél csak az elképesztőbb, hogy az oldalak több mint fele viselt valamilyen tanúsítványt arról, hogy teljesen megfelel az előírásoknak és szabványoknak. A kutatók nem feltételezik a rosszindulatot, inkább arról lehet szó, hogy az eredeti tartalom valóban szabványos volt, de a később végrehajtott változtatások, hozzáadott részek már nem.

Kíváncsiságból az Opera elemezte azt is, hogy ezek az oldalak mely webszerkesztővel készültek, és van-e összefüggés a hibák előfordulása és a használt szoftverek között. Meglepetésre az Apple iWeb hozta a legmagasabb arányban az érvényes oldalakat 81 százalékkal, míg a népszerű Adobe Dreameweaver mindössze 3,4 százalékot produkált. A kutatás következő lépéseként egy keresőmotort építenek az indexelt adatbázisra, így a web- és böngészőfejlesztők, illetve a szabványokkal foglalkozó szakemberek könnyen juthatnának valós adatokhoz az élő weboldalakkal kapcsolatban.

A MAMA-projekt során többek közt a webszerverek megoszlásáról, a dokumentumok átlagos méretéről, felépítéséről is gyűjtöttej adatokat. Aki kíváncsi a részletes számokra, az böngészheti az eredményeket az Opera fejlesztői oldalán.

(Forrás: HWSW)

↑ Kötelező internetszűrést vezet be az ausztrál kormány

(2008. október 23.)

Egy ausztrál kezdeményezés blokkolná az illegális tartalmak hozzáférését. Az eredetileg önkéntesnek szánt rendszer, úgy tűnik, kötelező érvényű lesz a kontinensen.

Az Ars Technica értesülései szerint a ausztrál internetbiztonsági kezdeményezés (Cyber-Safety Plan) az illegális tartalmak mellett a gyerekek számára tiltott pornográf oldalak hozzáférését is blokkolná. A rendszert most tesztelik, és a fejlesztésben érintett mérnökök szerint nem lehet majd kibújni az állami szintű szűrés alól.

Az ausztrál kormány a tavalyi év során jelentette be a kezdeményezést, amelyre összesen 189 millió ausztrál dollárt (több mint 25 milliárd forintot) fordítottak. Ebből a pénzből állítják üzembe azokat a szűrőrendszereket, amelyeket az internetszolgáltatóknak kötelező jelleggel kell működtetniük. A szolgáltatók az ausztrál kommunikációs és médiahatóság (ACMA) hivatalos feketelistájáról tájékozódhatnak a tiltott tartalmakról.

A bejelentést óriási felháborodás követte, ennek ellenére a kormány februárban megkezdte a rendszer első tesztjét Tasmániában. Akkor az ACMA közleményben jelezte, hogy a szűrők alapértelmezetten be lesznek kapcsolva, de a felhasználóknak lehetőségük nyílik rá, hogy egy kérvény segítségével kiléphessenek a tartalom-védelmi programból.

Úgy tűnik, ez csak részben volt igaz. Mark Newton, az Internode nevű cég hálózati mérnöke a Computerworldnek nyilatkozva azt mondta: a felhasználók kiléphetnek ugyan a gyerekekre vonatkozó szűrési feltételek alól, ám a fő feketelista – amely az ausztrál kormány által meghatározott illegális tartalmakat sorolja fel – rájuk is érvényes marad.

„Amit a kormány illegális tartalomnak könyvel el, az úgy is marad" – magyarázta a szakember. „Ha pedig megvan a szükséges infrastruktúra, hogy ezeket a tartalmakat szűrjék, akkor az alól nem lehet majd kibújni."

Az ausztrál kommunikációs miniszter szóvivője megerősítette, hogy a szűrés kötelező jellegű lesz minden ausztrál állampolgár számára.

A kérdés nagy vihart kavart, s a felhasználók azóta találgatják, milyen tartalmak kerülnek majd fel a feketelistára. A szűrést annak ellenére vezetik be, hogy az ausztrál kormány felkérésére készített 2006-os tanulmány kimutatta: az internetszolgáltatók szűrése költséges, ám nem elég hatékony.

(Forrás: Hvg.hu)

↑ Bezárták az online „bűnözőboltot"

(2008. október 22.)

Üzemen kívül helyeztek egy weboldalt, amelyen hitelkártya-adatokkal kereskedtek internetes bűnözők.

A The Independent értesüléseri szerint a Darkmarket nevű fórum valamivel kevesebb mint 3 éve üzemelt, s azzal kapcsolatos információkat értékesítettek, hogy hogyan lehet hozzájutni lopott identitásokhoz és hitelkártya-adatokhoz.

A BBC értesülései szerint az oldal bezárása óta eddig 60 embert tartóztattak le az esettel kapcsolatban Nagy-Britanniában, Európában és az USÁ-ban. A weboldalt kizárólag meghívó leveleken keresztül lehetett elérni, s olyan információk is szerepeltek rajta, mint például a hitelkártyák mágnescsíkjaiba kódolt adatok. Ezekkel aztán jelentős pénzösszegekhez lehetett hozzáférni.

„A Darkmarket igazi ezermester-áruház volt a csalók számára" – nyilatkozta a BBC-nek Sharon Lemon, a brit szervezett bűnözés elleni osztály (SOCA) igazgatóhelyettese. „A fórumon szinte szabadon lehetett szervezni a bűntényeket és szinte bármilyen eszközt vagy felszerelést el lehetett adni, vagy meg lehetett vásárolni. Ezek nem csínytevő kisdiákok, hanem komoly, szervezett bűnözők."

(Forrás: Hvg.hu)

↑ Horogra akadt az egyházromboló fiú

(2008. október 21.)

Egy 18 éves New Jersey-beli fiút, Dimitrij Guznert ítélt el pénteken a bíróság a Szcientológiai Egyház számítógéphálózata ellen indított támadás ügyében. Guzner a hírhedt Anonymous hackercsoport tagja – írja a Wired.

Guznert a januári denial-of-service, azaz hálózatlebénítási támadás ügyében ítélték el, amikor is nemcsak a szcientológusok számítógéphálózatát terhelték le, hanem telefon- és faxvonalaikat is, illetve emellett több nagyvárosban is hangos tüntetést szerveztek. Emiatt sok alkalmi szimpatizáns vélte tévesen azt a hackercsapatról, hogy kizárólag ez az egy téma mozgatja őket.

Az Anonymous a neten terjengő elemzések és vélemények tükrében inkább tekinthető mindenellenes, mint antiszcientológus csoportnak, igaz, az egyház azután szállt rá, hogy elkezdte terjeszteni a videómegosztókon és egyéb weboldalakon Tom Cruise megszellőztetett videóanyagát.

A csapat már korábban is nagyobb felhördülést okozott, például akkor, amikor epilepsziás betegek internetes fórumában helyezett el villogó képeket, legutóbb pedig akkor hallott róla a média, amikor David Kernell 20 éves tennessee-i diák betört Sarah Palin republikánus alelnökjelölt e-mail-fiókjába, és annak jelszavát, valamint egyes leveleit kitette az Anonymous egyik üzenőfalára.

Guzner valószínűleg 12 és 18 hónap közti letöltendő börtönbüntetést kap, továbbáz 37.500 dollár pénzbüntetést is kell fizetnie.

(Forrás: Hvg.hu)

↑ A privacy vége: egyedi azonosítót kapnak a kínai internetezők

(2008. október 20.)

A legutolsó kormányrendelet szerint december közepétől az összes pekingi internetkávézót fel kell szerelni kamerákkal és személyikártya-leolvasókkal. Az internetezők egyéni számokat kapnak, amikkel felmehetnek a világhálóra, böngészési szokásaikat pedig megfigyelik és eltárolják – adta hírül a kínai Xinhua hírügynökség. (Kínában jelenleg 250 millió internetező van – tízszer annyi, mint 2000-ben volt –, az internetkávézókba azonban csak azok léphetnek be, akik legalább 18 évesek.)

A rendelet értelmében a fő- és külvárosi kerületekben lévő 1500 internetkávézó mindegyikét fel kell szerelni kamerákkal és szkennerekkel. A kamerák folyamatos megfigyelés alatt tartják majd az internetezőket, a világhálóra pedig csak úgy lehet felmenni, hogy személyi igazolványuk bemutatása (és beszkennelése) után egyedi azonosítót kapnak. Az azonosító révén a pekingi rendfenntartó ügynökség képes nyomon követni, hogy az egyes állampolgárok milyen tartalmak iránt érdeklődnek.

Az egyik internetkávézó üzemeltetője elmondta a Xinhua hírügynökségnek, hogy amikor beüzemelte az új felszereléseket, látogatóinak 80 százaléka azonnal otthagyta a kávézót, de egy hónap után kénytelen-kelletlen visszatértek, mert nem tudtak másutt, kevésbé szigorú megfigyelés mellett internetezni.

A The Times munkatársai hiába próbáltak online kínai véleményeket találni a bejelentéssel kapcsolatban. Mindez véleményük szerint azért van, mert a kritikus kommentárokat a kormány azonnal törli az érintett oldalakról. A People"s Daily online közvéleménykutatása azonban azt mutatja, hogy a válaszadók 72 százaléka jogsértőnek tartja a rendeletet, 26 százalékuk szerint pedig csak azért elfogadható, mert „a gyermekeket védi".

(Forrás: Hvg.hu)

↑ Nyilvánosságra került az összes berlini rendőr telefonszáma

(2008. október 19.)

Nem sokáig örülhettek a berlini rendőrök a frissen kapott szolgálati mobiltelefonoknak, mert a telefonszámok egyik napról a másikra „a riválisok tábor", azaz a bűnözők kezébe kerültek.

Keddi értesülések szerint a kereken 14 ezer mobiltelefonszám napokon keresztül hozzáférhető volt az interneten, gyilkosok, betörők, tolvajok és kábítószeresek pedig a feketepiacon kereskedtek velük. A rendőrség egyelőre sötétben tapogatódzik, hogyan történhetett meg mindez. A német rendőrök szakszervezete szeptember végén a belügyminisztérium hathatós támogatásával intézte el, hogy a főváros rendjére ügyelő 14 ezer egyenruhás alkalmazott megkapja élete első szolgálati mobiltelefonját, mégpedig azzal a céllal, hogy ez is segítse az egymással való kapcsolattartást, amit a rendőrök – mint annyi más állami hivatal alkalmazottai – nem szívesen tettek a magántelefonnal.

A rendőrök arra hivatkoztak, hogy a fizetés amúgy sem magas, s felesleges azt még a priváttelefon számlájával is csökkenteni. A szolgálatinak viszont annál jobban örültek, hisz a költségek fedezését a berlini rendőrség ígérte, s mindenki arra számított: mostantól – hála a hivatali mobiltelefonnak – jóval sikeresebb lesz a bűnüldözés.

Csakhogy a telefonszámok szinte másnap rákerültek az internetre, s a lista – amely a készülék számát és a tulajdonos nevét tartalmazta – szabad préda lett. Azt ugyanis valaki egyszerűen letöltötte a szakszervezet különlegesen titkos jelszóval védett honlapjáról. A szakszervezet rádöbbent: a telefon mostantól immár aligha az eredeti tulajdonosokat, hanem inkább a bűnözőket segíti, akik megtréfálhatják, félrevezethetik, molesztálhatják az eddigi ellenséget.

Nem csoda, hogy a rendőröknek elment a kedve a szolgálati telefontól. A szakszervezet kedden bocsánatot kért a kínos ügy miatt, s felajánlotta, hogy minden rendőr azonnal telefonszámot cserélhet, de a berlini biztonságiak már nem bíznak az új számban sem, s attól tartanak: ami ma megtörtént, az megtörténhet holnap is. És azzal érvelnek, hogy a bűnözőkkel való „forró drót" lehetőségét a hátuk közepére sem kívánták. Sokan közülük azt fontolják, hogy visszaadják a szolgálati mobilt, és inkább telefonálnak – legfeljebb kevesebbet – drágábban, a sajátjukkal. De legalább őket sem hívhatja akárki.

(Forrás: Origo.hu)

↑ Mától mindenkiből lehet digitális bliccelő

(2008. október 18.)

Mindenki számára elérhetővé tették a digitális jegyek feltörésének módját holland kutatók. A leendő bliccelőknek száz dollárnyi felszerelésre van szükségük – adta hírül a BBC.

A Bart Jacobs vezette csoport az Esorics 2008 konferencia alkalmából publikálta az elterjedt digitális kártyák által használt titkos algoritmusokat. A Mifare Classic rendszerek megtöréséhez mindösszesen egy száz dollárba kerülő kártyaolvasóra és némi szoftverre van szüksége a bliccelni vágyóknak.

A napvilágra került adatok birtokában bárki elcsípheti az utastársak kártyájának lemásolásához szükséges információkat. Ha pedig egy üres kártyája is van kéznél, egyszerűen készíthet magának másolatot a hacker, hogy ne saját zsebből fizesse utazásait.

A kutatásban részt vevő Karsten Nohl szerint az RFID azonosítórendszerek iránt érdeklődő és sokat tömegközlekedő hobbi hackerek fogják először kipróbálni a nyilvánosságra hozott információk használhatóságát. Igaz, őket még nem a pénzszerzés fogja motiválni hanem a szórakozási lehetőség.

A Mifare Classic rendszerű jegyeket több közlekedési cég használja, köztük a 2000 kilométernyi vonalat üzemeltető bostoni MBTA és a teljes londoni tömegközlekedés is. A sebezhető kártyák olyan metropoliszokban is szolgálatban állnak, mint Bangkok és Delhi.

3ric Johanson, a CNet által megkérdezett biztonsági tanácsadó szerint nagyjából 3,5 milliárd Mifare Classic kártya lehet forgalomban. A szakértő hatvanra tette azoknak a városi szintű RFID-s rendszereknek a számát, ahol a sebezhető eszközt használják.

A kutatás eredményét először 2008 márciusában próbálta nyilvánosságra hozni a Bart Jacobs professzor vezette csapat. Erre a kártyákat gyártó NXP csoport perrel való fenyegetőzése miatt nem került sor. A holland bíróság júliusban hozott ítéletet arról, hogy a cég nem tiltathatja be a kutatási anyag publikálását. A kártyákat gyártó NXP szóvivője a BBC-nek azt nyilatkozta, hogy csupán a biztonsági rés nyilvánosságra hozásának idejét akarták eltolni a perrel, nem volt céljuk az anyag teljes betiltatása.

Az amerikai Defcon biztonsági konferenciáról is próbáltak perrel kitiltani egy a kártyák feltöréséről szóló előadást. A korlátozást abban az esetben is feloldotta a bíróság, így az MIT-s diákok beszélhettek arról, miért nem biztonságos titkos elven működő biztonsági eszközökben bízni.

(Forrás: Origo.hu)

↑ Vásárolni lehet a YouTube-videókból

(2008. október 17.)

Egy kattintással meg lehet venni a YouTube-videókban látott, vagy azokhoz kapcsolódó termékeket két nagy amerikai webáruház kínálatából. A szolgáltatást a Google minél több parnterrel bővítené a közeljövőben.

A világ legnépszerűbb videomegosztóját birtokló Google új szolgáltatást vezet be az Egyesült Államokban: a YouTube-klipekben látott termékeket egy kattintással meg is lehet majd vásárolni. Az internetes vállalat a iTunes zeneáruházzal és az Amazon.com internetes áruházzal fogott össze a szolgáltatás elindításához, amelynek fő profilja a könyv, a CD és a DVD és a videojáték, de ezen kívül szinte mindent árulnak már.

A nézők a YouTube-lejátszó ablak alján találnak majd egy gombot, amellyel egy kattintással letölthetik vagy megrendelhetik a klipben látott terméket a két online áruház kínálatából. A cég olyan árukat is felkínál majd megvételre, amelyekről csak említés esik, vagy valahogy kapcsolódnak a látottakhoz.

A Google a közeljövőben szeretne további forgalmazókat is bevonni a kezdeményezésbe, elsősorban a filmipar, a televíziós produkciók, a zenekiadás illetve a könyvkiadás területéről – mivel ezek azok a termékek, amelyeket gyakran megjelennek a webes klipekben és könnyű őket az interneten keresztül értékesíteni.

A YouTube mindeddig nem generált jelentős bevételeket a Google-nak, amely nem egészen két évvel ezelőtt 1,65 milliárd dollárért vásárolta fel azt alapítóitól. Hirdetések ugyan jelennek meg az oldalon, de a legtöbb klipet beágyazott formában tekintik meg az internetezők, ahol ezek nem látszanak, a vásárlásra ösztönző gombok azonban a lejátszó ablak részeként jelennek majd meg.

(Forrás: Origo.hu)

↑ E-vásárlás: most éri utol az uniós jog hazánkat

(2008. október 16.)

Az egész Európai Unióra kiterjedő egységes fogyasztóvédelmi szabályozást terveznek bevezetni az elektronikus vásárlások kapcsán. Az uniós tervezettel már ma nagyjából azonosak a hazai jogszabályok, ezért nálunk nagy változás nem várható.

A Meglena Kuneva uniós fogyasztóvédelmi biztos által beharangozott új direktíva-tervezet olyan kérdéseket szabályoz, amire nálunk már van törvény. Például az, hogy a netes vásárlás előtt a fogyasztók egyértelmű tájékoztatást kapjanak az árakról és a további költségekről és díjakról, nálunk már meglehetősen alapvetőnek mondható. A felvilágosítás a termék főbb jellemzőiről, a kereskedő nevének és címének a feltüntetése – melyek az uniós tervezetben szerepelnek – nálunk már közel tíz éve jogszabályba foglalt kötelezettségek az e-boltok tulajdonosai számára.

Azt az ötletet, hogy hogy a neten megrendelt terméket 30 napon belül házhoz kell szállítani, egyelőre csak a direktíva-tervezet tartalmazza, nálunk nincs ilyen szabály. Ám mint Klíma Katinka, a Nemzeti Fogyasztóvédelmi Hatóság (NFH) szóvivője érdeklődésünkre elmondta: a piaci viszonyok kényszerítik rá a hazai kereskedőket, hogy mihamarabb kiszállítsák a megrendelt termékeket: ez a legtöbb esetben nem 30 napot jelent, hanem egy-két munkanapot.

Két tekintetben lenne jobb az uniós szabály, mint a hazai: ha valaki meggondolja magát és mégsem kéri a terméket (ezt manapság már csak a távértékesítéssel, tehát például az interneten rendelt holmiknál lehet megtenni), jelenleg 30 napon belül kell, hogy visszakapja a vételárat. Az unió ezt a határidőt leszállítaná hét napra, tehát hamarabb jutna a pénzéhez a netes fogyasztó. A másik könnyítés, hogy most 8 napon belül gondolhatja meg magát a vásárló, az unió azonban 14 napot adna az áru próbálgatására, s ezen belül lehetne elállni a vásárlástól.

Egy furcsa nehezítéssel is találkozni az uniós ötlettárben: ott kötelező elállási formanyomtatványt vezetnének be, melyen a vásárló jelezheti, hogy eláll a vásárlástól. Ennél jelenleg egyszerűbb hazánkban a helyzet: elegendő például egy e-mailben írnia a vásárlónak, és már küldheti is vissza az árut.

Bár a hazai jogszabályok hasonlók az uniós tervezethez – ráadásul nem is mai rendeletről van szó, nálunk már 1999-ben előírtak számos, a vásárlókat védő rendelkezést, igaz, akkoriban még inkább a virágzó csomagküldő szolgálatokra gondoltak, a hasonló rendszerben működő internetes boltok csak később terjedtek el –, a gyakorlatban még a mai napig gondok vannak a net magyar szegletének webáruházaival.

Egy, az NFH által tavaly elvégzett, fél évig tartó, próbavásárlásokkal tarkított ellenőrzés során meglehetősen siralmas kép alakult ki a netes boltokról. A vizsgált több mint 200 hazai webáruház közel felénél hiányzott valamelyik alapadat (cég neve, címe, elérhetősége adószáma stb). Valamivel jobb volt a helyzet az árfeltüntetéssel (a honlapok 13 százalékáról hiányzott), de például a szállítási költségeket és feltételeket az e-boltok fele hallgatta el.

Az uniós tervezet feketelistát is létrehozna, nálunk már ilyen is van – igaz, azt nem egy hatóság, hanem maguk az internetezők tartják karban. A fogyasztóvédelmi hatóság a vizsgált 215 hazai internetes áruház üzemeltetői közül 150-re rótt bírságot 2007-ben a fenti hiányosságok miatt – összesen közel 13 millió forint értékben. A tapasztalatok alapján kijelenthető: az uniós jog még csak most éri utol a hazai szabályozást, de a magyar e-boltoknak még van mit behozniuk, hogy európai versenytársaikhat utolérjék.

(Forrás: Origo.hu)

↑ Banki adatokra halásznak a pénzügyi válság örvényében

(2008. október 15.)

A bankszámlaadatok megszerzésére irányuló internetes bűncselekmények szaporodásával járhat a nemzetközi pénzügyi válság – figyelmeztetnek amerikai és brit állami és bankszakmai testületek, illetve biztonságtechnikai szakértők.

Az amerikai Szövetségi Kereskedelmi Bizottság (FTC) és egy brit parlamenti bizottság egyaránt arra hívja fel a figyelmet, hogy a pénzügyi válság hatására az online adathalászat (phising) területén elmozdulás várható az identitástolvajlástól a banki ügyféladatok megszerzésére irányuló kísérletek felé. Az FTC szerint a zavarosban halászó csalóknak kiváló lehetőséget biztosít a bankszférában végbemenő viharos változás, amelynek során számos pénzintézetnek hirtelen megváltozott a tulajdonosi szerkezete. A bűnözők a megroggyant bankházak élére kinevezett állami válságmenedzserek vagy az új tulajdonos nevében léphetnek fel, és adategyeztetésre kérhetik a gyanútlan ügyfeleket – áll a bizottsági közleményben.

A testület azt javasolja az internetező bankszámla-tulajdonosoknak, hogy ne reagáljanak az olyan emailekre vagy felugró ablakokon elhelyezett üzenetekre, amelyek számlaadatok megadására szólítanak fel, még akkor sem, ha ezek látszólag a banktól érkeznek. Az identitástolvajlással (ID Theft) kapcsolatos ügyekkel foglalkozó brit parlamenti bizottság éves beszámolója szerint a krízis miatt szigorodó hitelfeltételek hatására gyakoribbá válhatnak a számlatulajdonosok elleni támadások. „Hitelt szerezni lopott identitással is egyre nehezebb, a bűnözők ezért aktívabban törekedhetnek a már létező számlák megcsapolására" – áll a bizottság második éves beszámolójában.

A Secure Computing IT-biztonságtechnikai cég legfrissebb jelentése szerint az adathalászok legkedveltebb célpontjai a válságban megtépázódott amerikai pénzintézetek, és a Wachovia, a J. P. Morgan Chase és a Bank of America mellett a közeljövőben – az 500 milliárd fontos állami bankmentő program befejeztével – a brit bankok is igen népszerűek lesznek a bűnözők körében.

Mindeközben a brit bankrenszer fizetési iparágát összefogó szervezet, a Fizetési Klíring Szolgáltatók Szövetsége (APACS) arról számolt be, hogy az adathalász-támadások száma már a világ pénzügyi rendszerét megrázó válság kirobbanása előtt is meredeken emelkedett. A szövetség idén január és június között összesen 20.682 ilyen esetet regisztrált, ami 186 százalékkal több, mint 2007 első hat hónapjában – áll a BBC hírportálján megjelent összefoglalóban.

(Forrás: Origo.hu)

↑ Több ezren blogolnak a szegénység ellen szerdán

(2008. október 14.)

A másodszorra megrendezett Blog Action Day során a különböző műfajú webes naplók szerzői egyetlen témáról publikálva igyekeznek felhívni a figyelmet égető társadalmi problémákra. Idén a középpontban a szegénység áll.

Az október 15-én rendezett Blog Action Day online, non-profit esemény, amelynek lényege, hogy egyesítse a bloggereket, a videonaplók és podcastok készítőit, hogy tevékenységükkel ráirányítsák a figyelmet az olyan kérdésekre, mint például a szegénység.

A szervezők hitvallása szerint egy ilyen összetett kérdésre nincsen egyszerű, tömör válasz. Ám több ezer, különböző hátterű ember véleménye és nézőpontja a szegénység sarkalatos témáiról szóló különleges társadalmi vitát generál. A kiírás szerint minden blogger saját naplójának témájához illeszkedve ír majd a szegénységről. Ez hatalmas lefedettséget biztosít a szervezőknek, hiszen minden blog más stílusban, más olvasóközönséget szólít meg.

A tavalyi Blog Action Day témája a környezet védelme volt, s a kezdeményezés nem várt sikerrel zárult. A bloggerek közül sokan kísérleteket végeztek, újító ötleteket publikáltak különböző fenntartható technológiákról és olvasóközönségük figyelmét a különböző zöld szervezetekre és a környezetbarát technológiákkal foglalkozó vállalatokra irányították.

A Blog Action Day mottója: „a legkisebb webes naplóktól az olvasott online magazinokon és az EU miniszterein át a profi és amatőr bloggerekig. A Blog Action Day lényege a tömeges részvétel. Bárki csatlakozhat, s nincs határa a bejegyzések számának és a témával kapcsolatos gondolatoknak".

A kezdeményezés weboldala szerint eddig 7892 oldal jelezte részvételét, ami közel tízmillió – 9 655 320 – potenciális olvasót jelent.

(Forrás: Hvg.hu)

↑ Az ufóknak küldött üzenetet a brit közösségi oldal

(2008. október 13.)

Az űrlényeknek üzennek egy brit közösségi oldal vállalkozó tagjai. Az ukrajnai rádióteleszkóppal elküldött csomag 501 képet, rajzot és rövid szöveget tartalmazott.

Greenwichi középidő szerint reggel hatkor indították útjára az ukrajnai Jevpatoriában található RT-70-es rádóteleszkópjáról azt az üzenetet, amelyet a Bebo közösségi oldal tagjainak üzeneteiből állítottak össze. Az adatcsomag 1.7 másodperc alatt elérte a holdat, négy perc elmúltával pedig a Marsot hagyta maga után. Oli Madgett, az üzenetért felelős technikai igazgató szerint a közösségi oldal használóinak üzenete nagyjából holnap reggeli időben hagyja maga mögött a Naprendszert. Az üzenet célja az a Gliese 581C bolygó, amelyről már lapunk is írt a Naprendszeren kívüli legérdekesebb bolygókat felsoroló cikkében.

A Bebo tizenkétmillió felhasználója egy erre létrehozott aloldalon küldhette be a pályázatát, amiből aztán a közösség válogatta ki a legjobbakat. Az elküldött üzenetet a legjobb indulattal sem lehet azonnalinak nevezni, leghamarabb negyven év múlva érkezhet meg rá a válasz. Bár az esélytelen, hogy pörgős chat alakuljon így ki, a mostani sikeres nyerteseknek van esélyük megérni az esetleg létező idegenek válaszát.

Mindenképp felmerül a kérdés, hogy megfelelő üzenet-e a kapcsolatteremtésre a közösségi oldal felhasználói által összehordott 501 kép és szövegdarab. Seth Shostak, a BBC által megkérdezett SETI csillagász szerint az üzenetnek mindösszesen a létezésünkre hívja fel a figyelmet. Így a Bebo által történelmi lépésnek beharangozott küldemény valójában csak egy hatalmas „Figyeljetek, van rádiónk!" kiáltás az űrbe.

Bár a rádióhullámot nem is lehet látványosan követni, kitartóan halad a fény sebességével a Gliese 518C-felé, a projekt oldalát mégis érdemes megnézni. A megtett kilométerekről tudósító számláló alatt megtekinthetőek például az elküldött képek, illetve a Bebo üzenetét Ukrajnába elszállító fiatalok úti videója is.

(Forrás: Origo.hu)

↑ Saját térképet rajzolhat a Google Mapsre

(2008. október 12.)

Ha el szeretnénk magyarázni, hogy valami hol van, vagy hogyan lehet odatalálni, a legegyszerűbb, ha rárajzoljuk a Google Mapsre a Quikmaps segítségével.

A Quikmaps.com webcímen található kis eszközzel a Google Maps webes térképeit szabhatjuk személyre igényeink szerint úgy, hogy szabadon rajzolgathatunk rájuk. A végeredményt az oldalon regisztrálva el lehet menteni, el lehet küldeni ismerőseinknek, hogy megmutassuk, vagy készíthetünk belőle a weboldalunkra beágyazható kódot is.

Az oldalon térképet rajzolni akár regisztráció nélkül is lehet. A rajzeszközök a Google Maps térképablak fölött találhatók: húzhatunk egyenes vonalat (draw lines), vagy rajzolgathatunk szabad kézzel (scribble), így akár írhatunk, firkálhatunk is a térképre. A rajzoláshoz a vonal színét (pick) és pixelben mért vastagságát is megadhatjuk (width).

A térképablak mellett rengeteg ikont találunk, amelyeket szintén rádobhatunk a rajzra. A Google Mapsen megszokott, földrajzi helyeket jelölő placemark-ikonok mellett zászlócskát is leszúrhatunk egy pontra, vagy figyelmeztető táblát helyezhetünk el, illetve megfeliratozhatjuk a térképet.

Lehet szemléltető eszköz isA navigálást segítő jelek mellett rengeteg más ikonkészletet is elérhetővé tettek a fejlesztők (például smiley-k, irodai eszközök, és így tovább), amelyekre a Markers felirat melletti legördíthető listából válthatunk át. Ezeknek már kevésbé van közük a térképezéshez, de fel lehet dobni velük az ábrát.

A szerkesztőprogramba a Google Earth-höz készült KML vagy GPS-készülékeken használható GPX-fájlokat is be lehet tölteni, illetve létre lehet hozni a megszerkesztett térképekből, így azokat a weben kívül is használni lehet. Az alkalmazásban minden Google által szolgáltatott térképre rajzolgatni lehet, így a csillagos égbolt, a Hold vagy a Mars térképeire is rajzolgathatunk.

A Quikmaps használata igen egyszerű, a készítők nem bonyolították túl a benne használható eszközöket: a szájtot arra szánták, hogy gyors skicceket dobhasson vele össze az ember. A szájt egyetlen hátránya, hogy eléggé leterheli a böngészőt a webes térképen futtatott grafikus alkalmazás. A weboldallal az útbaigazítás mellett könnyedén rajzolhatunk egyszerű szemléltető alkalmazásokat, saját térképeket, amelyek sokféle célra fel lehet használni.

(Forrás: Origo.hu)

↑ Egy amerikai házaspárt 236 millió dollárra büntettek levélszemétért

(2008. október 11.)

Levelenként 10 dollár kártérítésre ítéltek egy amerikai házaspárt, amiért kéretlen elektronikus levelek millióival bombázták egy internetszolgáltató rendszerét.

Henry Perez és Suzanne Bartok összesen 236 millió dollárt (43 milliárd forint) köteles fizetni egy Arizona állambeli szövetségi bíróság döntése szerint a CIS internetszolgáltatónak, amiért 2003-ban négy hónapon keresztül levélszemét-áradatot zúdítottak a cégre.

A támadás miatt az alig ötezer ügyfelet kiszolgáló CIS jelentős összeget felemésztő rendszerfejlesztésre kényszerült, három új szervert kellett üzembe állítani a spamek kezelésére. A hatalmas levélforgalom ráadásul foglalta a sávszélességet, ezért lelassult a szolgáltatás és sorra hagyták ott az előfizetők a céget. 2004 végére csupán 1200-an maradtak.

Nemcsak Perez és Bartok bombázta a CIS rendszerét. Az amerikai internetszolgáltatói piacon alig észrevehető vállalat ellen valóságos spamháború indult 2003-ban; naponta 500 millió kéretlen e-mail érkezett. Robert Kramer, a cég tulajdonosa szerint ennek az lehetett az oka, hogy a cis.net domain név zavarba ejtően hasonlít a cis.com domainra, amelyet az egyik legnagyobb szolgáltató, a CompuServe használt.

Időközben számos spamküldőt beazonosítottak és Kramer kártérítési pert indított ellenük. A bíróság tíz eljárásban az CIS javára döntött, a kiszabott összegeket azonban nehéz behajtani, mert a károkozók külföldre menekítik a pénzüket vagy eltűnnek – mondta a cégvezető az ITWorld.com informatikai hírportál tudósítása szerint.

(Forrás: Hvg.hu)

↑ Félnek a bankok a hackerbiztos számítógépektől

(2008. október 10.)

A világ első megtörhetetlen számítógéphálózatát mutatták be Ausztriában. A Bécsben és St. Pöltenben elhelyezett hat számítógépet 200 kilométernyi fényszálas kábel kötötte össze, védelmüket pedig egy olyan gyökeresen új rendszer, a kvantumtitkosítás adta. A megkérdezett bankok mindegyike azt állítja, szívesebben veszítenének pénzt a törhetetlenség helyett.

A kritikus adatokat és kommunikációt védő megoldások olyan matematikai megoldásokon alapulnak, amelyeket a megfelelő idő és processzoridő birtokában nemcsak elméletben, hanem gyakorlatban is megtöhetnek a hozzáértők. Az újdonságnak számító kvantumrendszerek azonban azon a kvantumelméleten alapszanak, amelyek biztosítják az elméleti és gyakorlati lehallgathatatlanságot is.

A kvantumtitkosítás alapötletét 25 éve dolgozta ki Charles Bennett és Gilles Brassard. Brassard a bécsi bemutatón elmondta, minden kvantumtitkosítás Heisenberg bizonytalansági elvén alapul, amelynek lényege az, hogy a kvantuminformációt nem tudjuk anélkül megvizsgálni, hogy megzavarnánk. A demonstrációban ennek megfelelően jól látszódott, hogy amikor egy harmadik fél megpróbált belehallgatni egy két ember között felhúzott kvantumrendszerbe, az adatokat, illetve a titkosító kulcsot tartalmazó fotonok összekeveredtek, a hibaszázalék emelkedése támadást jelzett, ennek következtében a rendszer pedig automatikusan lezárta magát anélkül, hogy bármilyen információ egy harmadik félhez kerülhetett volna.

A demonstráció során az is kiderült, hogy a kvantumtitkosítással felszerelt rendszer igen masszív, hiszen ha egy kvantumlinket lezárnak lehallgatásveszély miatt, a telefonhívások átirányításához hasonlóan a hálózati kommunikációt más, hasonló módon működő szerverek közé is át lehet irányítani, így a hálózaton lévő két rendszer folyamatos kontaktban maradhat.

Dr. Hannes Hübel, a bécsi egyetem kutatója azonban azt mondja, ez önmagában nem garantál egy biztos rendszert. A megkérdezett bankok biztonsági szakemberei ugyanis egyöntetűen úgy nyilatkoztak, inkább vesztenének 10 millió eurót, minthogy rendszerük két órán keresztül működésképtelenné váljon. Így olyan rendszert kell alkotniuk, amely akár több hétre előre is képes kvantumkulcsokat generálni és úgy tudjon lehallgathatatlan maradni, hogy közben működőképes is.

(Forrás: Hvg.hu)

↑ Fotóalbumot lehet készíteni az iWiW-en

(2008. október 9.)

A felhasználók az eddiginél jóval több képet feltölthetnek az iWiW-re, és albumokba is rendezhetik azokat, amelyeket el is rejthetnek mások szeme elől.

Az eddigi két megabájtos felső határ megszűnt, és havonta száz megabájtnyi fotót tölthetnek fel a felhasználók az adatlapjukhoz – adták hírül az üzemeltetők. Így elvileg bármennyi képet fel lehet tölteni, csak ki kell várni az egy hónapot egy-egy százmegás adag között.

A feltöltött képeket albumokba is lehet rendezni, és szabályozni lehet, hogy ki láthatja azokat. A hozzáférést mindenki, csak az ismerősök, vagy bizonyos csoportok számára lehet engedélyezni.

Az adatlapokhoz eddig tartozó képek egy Profilképek nevű albumba kerültek, ezek továbbra is mindenki számára publikusak lesznek. Az albumokban ugyanúgy megadható egy alapértelmezett kép, mint a profilképeknél.

További újdonság, hogy egyidejűleg több kép is feltölthető párhuzamosan, az albumokban a képek sorrendje szabályozható, a képeket át lehet mozgatni az albumok között. A képeknek külön címet és leírást lehet adni, illetve elláthatók cimkékkel is. Hamarosan újabb, a képekkel kapcsolatos funkciók is bevezetésre kerülnek – adták hírül az üzemeltetők.

(Forrás: Origo.hu)

↑ Új internetes szervezet a gyermekek védelmére

(2008. október 8.)

Egy újonnan létrehozott szervezet fog gondoskodni Nagy-Britanniában a gyermekek internetes védelméről, megóvva őket a pornográf, az erőszakos és az öngyilkosság témájával foglalkozó honlapoktól – jelentette be a brit belügyminiszter hétfőn.

Jacqui Smith hangsúlyozta: ez az eddigi legátfogóbb, a köz- és a civilszférába tartozó szervezetek közti együttműködés, amely a gyermekek internetes védelmét szolgálja. A Gyermekek Internetes Védelmének Tanácsa (UK Council for Child Internet Safety) célba veszi a káros tartalmú illegális oldalakat, felhívja a fiatalok figyelmét a rájuk leselkedő virtuális veszélyekre, és létrehoz egy viselkedési kódexet a videók és üzenetek megosztására alkalmas honlapok számára. A szervezet az erőszakos játékok ellen is küzdeni fog, valamint támogatja majd a felelősségteljes online reklámokat.

„Eltökéltük: mindent megteszünk annak érdekében, hogy az internet ne jelentsen többé veszélyt gyermekeinkre" – mondta a belügyminiszter a London belvárosában hétfőn bemutatkozó szervezettel kapcsolatban. A 100 tagot számláló szervezet, amelyhez többek között a Facebook, a Google, a Microsoft és a Vodafone is csatlakozott, közvetlenül Gordon Brown miniszterelnök felügyelete alá tartozik.

Az utóbbi időben többen is kritikával illették a brit kormányt, amiért nem lép fel elég határozottan az erőszakos játékok és internetes oldalak ellen. Tanya Byron pszichológus témába vágó márciusi beszámolójában azt javasolta az illetékes miniszteriumnak, hogy hozzanak létre egy gyermekvédelmi tanácsot. A brit kultuszminiszter, Andy Burnham véleménye szerint a szervezet arról fog gondoskodni, hogy „ami nem elfogadott az interneten kívül, az ne legyen elfogadható az interneten belül sem."

Magyarországon a több civil szervezet által létrehozott Barátságos Internet Fórum foglalkozik leginkább a gyerekek internetes védelmével, de van biztonságos kereső is, és találni gyerekek szempontjai szerint minősített oldalak jegyzékét is.

(Forrás: Origo.hu)

↑ Adható-vehető hazánkban az e-mailes címlista

(2008. október 7.)

Egy évvel ezelőtt sokak kaptak olyan leveleket, amelyekben magyar internetezők komplett e-mailes címlistáját ajánlgatta egy ismeretlen. Már a rendőrségi eljáráson is túl kimondható: büntetlenül.

Hiába szerepel a büntető törvénykönyvben a személyes adatokkal való visszaélés, hiába a Nemzeti Hírközlési Hatóság feljelentése és a rendőrségi nyomozás, a jogszabályok nem teszik lehetővé, hogy elkapják azokat a spammereket, akik egy ideje boldog-boldogtalannak kínálgatják a hazai internetezők e-mail címeiből összeállított jegyzéket. A szintén spamként – azaz kéretlenül – érkező ajánlatok száz- és ötszázezer magyarországi e-mail címet kínálnak megvételre, különválogatva a magánszemélyek és vállalkozások címeit.

Vállalkozásoknak ma már lehet küldeni kereskedelmi üzeneteket, de a magánszemélyek adatait (így e-mail címeit) az ő beleegyezésük nélkül gyűjteni, tárolni, kezelni és főként marketingcélra felhasználni nem szabad. Ennek ellenére néhány, az adatbázist felkínáló kiberbűnözővel váltott levél alapján kiderült: a címeket a netről gyűjtötték, az érintettek jóváhagyása nélkül. A címlistákat 50 ezer forintért vesztegették, legalábbis az egyik blogger által folytatott levelezésből ez derül ki, mert összeg magukban az ajánlatokban nem szerepelt.

Több bejelentés is érkezett az ügyben a Nemzeti Hírközlési Hatósághoz. Sylvester Nóra, az NHH informatikai szabályozási igazgatóságának vezetője korábban lapunknak elmondta: bejelentést tettek az ügyben a rendőrségnél, mivel a hatóságnak a kéretlen levelek küldőivel szembeni eljáráshoz van joguk, a címlisták értékesítői már bűncselekményt követnek el. Az NHH nem tud nyomozni, nem tudja kideríteni, hogy ki áll a nyilvánvalóan hamis névvel küldött ajánlatok mögött. A rendőrség azonban idén januárban arról értesítette a hatóságot, hogy megszüntették a nyomozást személyes adattal való visszaélés hiánya miatt.

Sylvester elmondta: értesülésük szerint a címlistát kínálgató jóember nyilvános helyeken beszél meg találkozót, ahova azonban nem ő megy el, hanem küld maga helyett valakit, egy „futárt", aki valószínűleg az ismeretségi köréből kerül ki. Így bár a lista elektronikus formátumban vehető át, de az nem az interneten érkezik, hanem valamilyen adathordozón, ráadásul a terjesztő fel sem bukkan a történetben – legalábbis személyesen nem.

Az NHH a kéretlen levelek kapcsán a Nemzeti Fogyasztóvédelmi Hatóságot is megkereste. Az NFH ugyan nem vizsgálja a spameket (ez az NHH feladata), de reklámfelügyeleti eljárást indíthat a hirdetett termékkel, azaz a címlistákkal kapcsolatban. Mint Kathi Attila, az NFH társadalmi kapcsolatok főosztályának vezetője elmondta: akkoriban egy próbavásárlással akartak meggyőződni arról, hogy a címlisták valóban megvehetők-e, ám a megadott e-mail címre küldött levelükre nem érkezett válasz. Egyébiránt Kathi szerint az NFH-nak legfeljebb marginális szerepe lehet hasonló ügyekben, hiszen ők inkább a termékspecifikus tilalmak megszegői ellen lépnek fel: gyerekekre káros termékeket, dohányárut hirdetők állnak a célkeresztben.

Az NHH feljelentését követően az ügy a Nemzeti Nyomozó Iroda high-tech zsaruihoz került. Gazdag Tibor, az NNI csúcstechnológiai bűnözés elleni osztályának vezetője elmondta: a büntető törvénykönyvben nevesített tétel a személyes adattal való visszaélés vétségnek számít és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel súlytható az elkövető. Ahhoz, hogy a visszaélést megállapítsák, két dolognak kell teljesülnie: egyrészt meg kell történnie a személyes adatok jogosulatlan, vagy a céltól eltérő kezelésének, másrészt más vagy mások érdekeit jelentősen sértenie kell az elkövetőnek.

Ha a két feltétel közül csak az egyik teljesül, akkor a törvény szerinti vétség nem áll fenn. Hiába kapnák el a spammert, ha senki nem jelzi, hogy az ő e-mail címével való kereskedés érdeksérelmet okozott, akkor a rendőrség sem tud továbblépni. Gazdag szerint jelentős érdeksérelem lehet például, ha valakinek meg kell változtatnia az e-mail címét, mert a kéretlen levelek már olyan mértékben özönlik el postafiókját, hogy kezelhetetlenné vált a levelezés. Amíg ilyen – bizonyítható, és a bíróság előtt is megálló – bejelentés nem érkezik a rendőrséghez, nem tudnak hozzányúlni a spammerhez.

Ha valaki mégis bejelentést tenne a rendőrségen, akkor is igazolódnia kell annak, hogy az illető e-mail címe (amit le kellett cserélnie), szerepel azon a címlistán, amit értékesíteni akart a kiberbűnöző. Mivel a fenti feltételrendszer aligha fog teljesülni, ezért valószínű, hogy hazánkban soha nem fognak el egyetlen e-mail cím gyűjtőt sem, a listákkal való kereskedés pedig a jelenlegi jogszabályok közepette ha nem is legális, de következmények nélküli, jól jövedelmező tevékenység marad.

(Forrás: Origo.hu)

↑ Terroristák fotói az interneten vásárolt kamera memóriájában

(2008. október 6.)

Nyomozást indított a brit rendőrség egy internetes árverésen vásárolt digitális kamera ügyében, amelyen a londoni The Sun értesülése szerint a gyanútlan új tulajdonos al-Kaida-terroristák fotóit és ujjlenyomatait, rakétavetők és rakéták képeit fedezte fel.

A fényképezőgép feltehetően az MI6 brit titkosszolgálat egyik ügynökének tulajdonában volt korábban, a vevő alig 17 fontért (5200 forint) vásárolta a világhálón, majd magával vitte fényképezésre a vakációra. A gép előéletére akkor derült fény, amikor saját fotóit elkezdte letölteni a számítógépére – és a képernyőn megjelentek az al-Kaida terroristák és a rakéták is.

A hertfordshire-i rendőrség hivatalosan megerősítette kedden, hogy vizsgálatot indított, miután egy magánszemély jelezte számára a kamera tartalmát. A nyomozásban részt vesz a titkosszolgálat is. Az ügyről nyilatkozva a külügyminisztérium illetékese nem bocsátkozott részletekbe, így azt a sajtóértesülést sem erősítette meg, amely szerint a fényképezőgépet esetleg az MI6 egyik ügynöke adta el.

Az incidens csak a legfrissebb a hasonlóan zavarba ejtő esetek sorában. Az ügyészség bejelentette, hogy a titoktartási szabályozás megsértése miatt vádat emel egy hivatalos személy ellen, aki szigorúan titkos, az al-Kaida terrorszervezetről és az iraki biztonsági erőkről szóló adatokat felejtett egy londoni helyiérdekű vasúti kocsiban.

Tavaly egy köztisztviselő olyan számítógépes lemezeket vesztett el, amelyen 25 millió személy nevét, címét és banki adatait tárolták, januárban pedig a védelmi minisztérium közölte, hogy nyoma veszett egy hordozható számítógépnek, rajta 600 ezer sorozott katona adataival. A belügyminisztérium augusztusban jelentette be, hogy egy alvállalkozója elvesztette minden angliai és wales-i rab személyes adatait.

(Forrás: Origo.hu)

↑ A flashszerver hibája miatt ingyen volt letölthető 40 ezer film az Amazonról

(2008. október 5.)

A világ legnagyobb webáruháza, az Amazon.com online videotékájának teljes kínálata letölthető volt ingyen a flashszerverek hibája miatt.

Valójában ez nem is programhiba, egyszerűen rosszul lett megtervezve az egész rendszer – mondta a Reutersnek Bruce Schneier, a British Telecom biztonsági szakértője.

Az Amazon Video on Demand szolgáltatása a YouTube-hoz hasonló streaming technológián alapul, vagyis valós időben tölti a videofájlt a felhasználó gépére, aki már akkor elkezdheti nézni a videót, amikor annak a vége még nincs is ott a gépén. A lejátszás gyorsítása miatt a flashszervere, ami a letöltést intézi, nem titkosítja az adatokat, csak a felhasználó parancsait (a lejátszás elindítása, megállítása és hasonlók). Ez lehetővé teszi olyan, videocatchernek, vagyis videóelkapónak nevezett programok működését, amik a titkosítatlan adatfolyamot egyszerűen lementik a gépre, mielőtt még a lejátszóig eljutna.

Az Amazon 40 ezer tévéműsort és mozifilmet tartalmazó online videotékájában minden egyes videó első két percét megnézheti bárki ingyen, kedvcsinálóként, aztán a 24 órás kölcsönzés 4 dollárba kerül, egy film megvásárlása után pedig 15 dollárt hagyunk a kasszánál. A rendszer a képperces előzetesnél is elkezdi az egész filmet letölteni a gépünkre (és két percnél küld egy pause parancsot a lejátszónak), így a videocatcherrel gond nélkül lementhető a teljes film.

Az Amazon vetélytársai, az egyre népszerűbb Hulu online tévé, vagy az NBC és CBS tévécsatornák portáljai sem jártak jól. Itt ingyenesek a videók, és a bevételt a filmeket megszakító reklámok hozzák. A videocatcher programok viszont automatikusan kivágják a lementett anyagból a reklámblokkokat.

A megoldás a flash alapú videók titkosítása lenne, ami persze lelassítja a letöltéseket, és megemeli a hardverigényt, hiszen az adatfolyamot dekódolni kell a lejátszás előtt. Az Adobe hivatalosan egyelőre nem tervez ilyesmit (külső cégek viszont már ajánlanak ilyen megoldást flashszerverekhez). Piaci elemzők szerint egyébként sincs az egész videocatcher-kalózkodásnak olyan nagy hatása, mert a programok használata túl bonyolult ahhoz, hogy az átlagfelhasználók tömegesen szokjanak rá. Igaz, annak idején hasonlókat mondtak a fájlcserélőkről is.

Kedd reggelre a hibát elhárították, és végetért az ingyen letöltögetés. Mint kiderült, a hiba nem a flashszerverben volt, hanem az Amazon szerverein, ahol egy régi típusú titkosítást alkalmaztak, azt is rosszul beállítva.

(Forrás: Index.hu)

↑ Súlyos sebezhetőség a böngészőkben

(2008. október 4.)

Súlyos biztonsági rést fedeztek fel biztonsági szakemberek, akik már fel is vették a kapcsolatot a fontosabb böngészőkészítőkkel. A hiba ellen száz százalékos védelem jelenleg nincs.

A sebezhetőségek egy új típusát fedezték fel nemrég biztonsági szakemberek, írta meg az IT.café. A „clickjacking" néven emlegetett támadásról egyelőre nem sokat tudni, csupán azt, hogy a népszerű böngészők mindegyikén működik. A módszert egy múlt heti szakkonferencián, az OWASP NYC AppSec 2008-on tervezte bemutatni két szakértő, Robert „RSnake" Hansen és Jeremiah Grossman, de az egyik érintett cég, az Adobe kérésére végül lemondtak a részletek közzétételéről mindaddig, amíg el nem készül a hibát javító patch.

Amint Hansen a Computerworld-nek elmondta: a clickjacking hasonló az ún. CSRF (cross-site request forgery) támadáshoz – amely a weboldal felhasználó iránti bizalmára épül és hamis HTTP-kéréseket használ –, de mégis különbözik attól annyira, hogy a jelenlegi CSRF-ellenes védelmi megoldások nem működnek ellene.

„Gondoljunk azokra a gombokra, amelyek egy weboldalon megjelenhetnek. Ilyeneket használunk a banki átutalásoknál, de ilyenek a Digg gombjai vagy a reklámbannerek is. A lista gyakorlatilag végtelen, és ezek relatíve ártalmatlan példák. Utána gondoljunk egy olyan támadásra, amely ezeket a gombokat láthatatlanul képes a felhasználó egérmutatója alá tenni, hogy amikor az rákattintana arra, amit lát, valójában arra kattintson, amit a támadó helyezett el az oldalon" – próbálta megvilágítani az attak működését a másik előadó, Jeremiah Grossman. Ráadásul a támadás kivitelezéséhez nem is kell feltörni a kérdéses szájtokat.

A sebezhetőséget csak a böngészők patchelésével lehet megszüntetni – állítja a páros. A Microsofttal, a Mozillával és az Apple-lel már fel is vették a kapcsolatot, de azt egyelőre nem tudni, hogy a cégek mennyire veszik komolyan a hibát, és mennyire sietnek annak befoltozásával. Jelen pillanatban a legjobb védelmet a clickjacking ellen a NoScript kiegészítővel ellátott Firefox jelenti – Hansen szerint ez a támadások 99,99 százaléka ellen megvéd –, ez viszont csak profibb felhasználóknak ajánlott.

Hansen és Grossman példakódokkal együtt közzé fogja tenni a részleteket, amint az Adobe elkészül a saját patchével. Azt sem a sebezhetőséget felfedező szakértők, sem a szoftvercég nem árulta el, hogy melyik Adobe-terméket érinti a hiba, de jó eséllyel gyanítható, hogy az internetes oldalakon széles körben használt Flashről van szó.

(Forrás: Index.hu)

↑ Csak bírói engedéllyel korlátozható az internetelérés az EU döntése szerint

(2008. október 3.)

Kizárólag bírósági eljárás során lehet arra kényszeríteni a szolgáltatókat, hogy felhasználóikat bármilyen formában korlátozzák, szankcionálják illegális letöltések miatt – mondja ki az új közösségi telekommunikációs szabályozás 138-as, nagy többséggel elfogadott módosítása. Franciaországot azonban nem érdekli az Európai Parlament döntése, ők lehetnek az elsők, akik kötelező tartalomkontrollt írnak elő az internetszolgáltatóknak.

Az Európai Parlament szerdán szavazott a „Telekom csomag" nevű törvényről, mely a teljes európai telekommunikációs piacot szabályozná. A törvény ellen az internetszolgáltatók már azelőtt ágáltak, hogy a parlament elé került volna hiszen a lelkes Viviane Reding ezúttal a roaming díjaknak üzent hadat. A bevételeiket féltő szolgáltatóknak ez nyilván nem tetszett, de végleg a szerzői jogok védelme érdekében beillesztett passzusok bőszítették fel őket. Ezek arra köteleznék a szolgáltatót, hogy önmaga oldja meg a tartalmak szűrését, vizsgálatát és a jogosulatlan letöltéseket bonyolító felhasználókat korlátozza le, büntesse meg – az elgondolás szerint a harmadik figyelmeztetés után a szolgáltatóknak joguk lett szerződést bontani a notórius visszaesőkkel.

A képviselők százával adtak be módosító javaslatokat a telekomcsomaghoz, nehezen követhetővé téve az amúgy is bonyolult törvényalkotási folyamatot. A sok közül két javaslat vált híressé, mégpedig a 133-as illetve a 138-as számú. A 133-as, "Filtering" című módosítás megakadályozta volna a tagországokat, hogy rákényszerítsék a helyi szolgáltatókat, hogy maguk szűrjék a tartalmat, hiszen a módosítás kizárta volna bármilyen megfigyelésre alkalmas technológia használatát az internetelőfizetőkkel szemben. Ezzel a javaslattal nem szimpatizált a parlament, így leszavazták.

A 138-as módosítójavaslat esetében a kulcsfigura Guy Bono, francia szocialista képviselő volt, akinek az inditványa szerint csak és kizárólag bírói határozat alapján lehet a szolgáltatókat arra kényszeríteni, hogy szankcionálják az illegális fájlcserében érintett felhasználókat. Ezzel Bono gyakorlatilag meghagyná az elméleti lehetőséget az illegális letöltők lekapcsolására, de a gyakorlatban olyannyira lelassítaná a folyamatot, hogy értelmetlenné válna az alkalmazása. Ez a kifacsart megoldás jobban tetszett az európai honatyáknak, mint a technológiai tiltásra építő javaslat, így nagy többséggel elfogadták.

Még több országnak is el kell fogadnia az EU központi jogi útvesztőjén átment törvényt, a gond viszont majd csak a ratifikálás után kezdődik. Az Európai Bizottság jövő év elejére ígéri, hogy részletesebb útmutatásokkal rukkol elő az elfogadott szöveg alapján. Az EU-ban viszont a legtöbb közösségi törvény csak kötelezően ajánlott, el lehet tőle térni adott esetben. Így nem meglepő, hogy a francia kulturális miniszter, Christine Albanel azonnal jelezte, őket nem érdekli a 138-as módosítás, Franciaországban várhatóan életbe léptetik a szolgáltatók felelősségéről szóló szabályozásokat.

Viviane Reding, a telekommunikációs reformok vezetője a francia elutasításnál is meglepőbb ötlettel állt elő, mégpedig az elfogadott módosítás erőszakos visszavonásáról kezdett ábrándozni. Az 574 képviselő által támogatott és mindössze 74 által elutasított 138-as módosítással kapcsolatban Reding azt szerette volna elérni, hogy vonják vissza a szavazás eredményének ellenére. Eközben követői saját országaikon belül igyekeznek támogatást szerezni a kontroll bevezetéséhez. A politikusnő és társainak viselkedése többek szerint demokrácia-ellenes, a 138-as módosítást benyújtó Guy Bono is dühösen reagált kollégája nyilatkozataira.

A háttérben a szerzői jogokat védő szervezetek is drukkolnak, a lemezkiadók jogaiért küzdő nemzetközi IFPI és az amerikai RIAA is figyelemmel kíséri a folyamatot. Nyilvánvalóan komoly eredményként értékelnék, ha Európában megszorongathatnák a zenék és filmek „alternatív" terjesztését és végre valós büntetéssel fenyegethetnék az átlagos felhasználókat is. Eközben Bono felháborodottan azt nyilatkozta Reding ötletéről, hogy nem lehet szembe menni a parlament ilyen többségű döntésével, gyakorlatilag az európai polgárok akaratával, bármilyen témáról is legyen szó.

(Forrás: HWSW)

↑ Kutass prímeket 150 ezer dollárért!

(2008. október 2.)

Két héten belül kétszer is megdőlt a 2006-ban felállított prímszámrekord. Az új csúcstartó 12.978.189 jegyből áll.

A kisebbik óriásprím 11.185.272 jegyből áll, és szeptember 6-án találta meg Hans Michael Elvenich. A kölni hobbimatematikus elektromérnök megkaphatta volna az Electronic Frontier Foundation (EFF) 100 ezer dolláros (kb. 17 millió forint) díját, mert tízmilliónál több jegyű prímszámot számolt ki, ám közben kiderült, hogy Edson Smith, a Los Angeles-i Egyetem matematikusa már két héttel korábban rálelt egy tízmilliónál több jegyű prímre. A felfedezések érdekessége, hogy mindkettő a Nagy Internetes Mersenne-Prímszám Kutatás (GIMPS) elnevezésű nemzetközi projekt keretében született. A most kiszámolt törzsszámok a 45. és a 46. Mersenne-prímszámok, amelyek a 2 az n-edik hatványon) mínusz 1 alapján jönnek ki).

Az 1996-ban indult GIMPS projekthez világszerte több mint 100 ezer önkéntes csatlakozott, akik egy olyan, ingyenesen letölthető kliens szoftvert telepítettek a számítógépükre, amely a gép szabad számítási kapacitását használta fel újabb Mersenne-prímek kiszámolására. Az így létrejött, az elosztott számítások módszerével dolgozó hálózat, a PrimeNet olyan számítási teljesítményre képes, mint egy szuperszámítógép, másodpercenként 29 billió művelet végrehajtására képes. (Néhány éve hasonló módzserrel dolgozott a hazánkban is népszerű SETI projekt.) A két újjal együtt a GIMPS mostanáig 12 Mersenne-prímmel gazdagította az emberiséget.

„Az internet hatalmas erővel képes támogatni a kooperáción alapuló kutatómunkát. Ennek az erőnek a kihasználására alkalmas megoldások kidolgozására ír ki az EFF pályázatokat" – Scott Kurowski, a PrimeNet fejlesztője.

A következő pályázat díja 150 ezer dollár. Az kapja meg, aki százmilliónál több jegyből álló Mersenne-prímszámot talál.

(Forrás: Computerworld.hu)

↑ Alattomosan támad a Limbo trójai

(2008. október 1.)

A Limbo trójai ugyan nem új kártevő, de egyre több problémát okoz a nagyon trükkös adatgyűjtési módszerével.

A Limbo trójai néhány évvel ezelőtt bukkant fel először. Azóta az online alvilág mind kedveltebb eszközévé nőtte ki magát. Uri Rivner, az RSA egyik vezetője is arra világított rá, hogy a Limbo egyre több problémát okoz. A trójai szinte láthatatlanul van jelen a fertőzött számítógépeken, és a háttérben nagyon alattomos módon próbál bizalmas adatokat gyűjtögetni. A kártékony program a webböngészőkbe épül be, és az úgynevezett HTML injection módszert alkalmazza a tevékenysége során. Ezáltal, ha a felhasználó például egy banki weboldalt látogat meg, akkor a trójai az eredeti weblapba különböző adatbekérő mezőket szúr be. A felhasználó mindebből legfeljebb csak annyit vesz észre, hogy valamilyen oknál fogva a bankja több adat megadását várja el tőle, mint eddig. A valóságban azonban csak a trójai kíváncsiskodik, és a gyanútlan felhasználó által gondosan kitöltött űrlapok révén szerez bizalmas adatokat. A Limbo gyakran bankkártyaszámok és PIN kódok iránt „érdeklődik".

A Limbo a számítógépekre számos módon kerülhet rá. Gyakran weboldalakról töltődik le, de az is előfordulhat, hogy különféle adathalász támadások szerves részeként környékezi meg a PC-ket. Amint megfertőz egy számítógépet, attól kezdve a böngészőn keresztül folyamatosan figyeli a felhasználó internetezési szokásait, és egy alkalmas weblap letöltésekor beszúrja az oldalba a saját kódját.

Uri Rivner szerint a Limboval kapcsolatos másik probléma, hogy egyre könnyebben szerezhető be az Interneten keresztül. Két évvel ezelőtt még 5000 dollárért lehetett hozzájutni az online bűnözők körében, míg tavaly már 1000 dollárért „osztogatták". Rivner szerint napjainkban pedig akár 350 dollárért is meg lehet vásárolni. Természetesen mindez jelentősen elősegíti a Limbo egyre szélesebb körű elterjedését, így érdemes gondosan szemügyre venni a megbízhatónak látszó webes űrlapokat is.

(Forrás: Computerworld.hu)