ENERGIADILEMMA

Egy felmérés szerint 2008-ban a világ energiafogyasztásának 4 százaléka IT-vonatkozású volt, és ez az arány 2030-ra 40 százalékra nőhet. » 14. oldal

AZ IKT ÉS A CSR

Társadalmi felelősségvállalás, röviden CSR. Kérdés, hogy a vállalatok mennyire átgondoltan, milyen arányban járulnak hozzá a fenntartható fejlődéshez. » 22. oldal

445 forint

SZÁMÍTÁSTECHNIKA

ICT-STRATÉGIA DÖNTÉSHOZÓKNAK • WWW.COMPUTERWORLD.HU
ALAPÍTVA 1969 • 2010. AUGUSZTUS 3. • XLI. ÉVFOLYAM 31–32. SZÁM

IDG HUNGARY

COMPUTERWORLD

Az informatika detektívjei

A jó- és a rosszfiúk véget nem érő küzdelméről szóló könyvek, filmek, hírek nagy érdeklődésre tartanak számot. Ha pedig a nyomozások, a bizonyítékok felkutatása és a különféle vizsgálatok az informatika korszerű technológiáival vegyülnek, akkor egy még izgalmasabb terület tárul elénk, amely nem más, mint a computer forensic.

Összeállításunk a 9–11. oldalon

9 770587 151006 10032

Megjelent a PC World!

Augusztus 5-étől keresse az újságárusoknál!

Ajándék szoftver

- Ashampoo Anti-Malware (teljes verzió)

Fókuszban

- Intel vs. AMD körkép
- A nagy platformteszt
- Az internet új ruhája
- E-book forradalom
- Little Susie Linux

Szolgáltatások:

DVD Authoring

CD, DVD sokszorosítás

Egyedi CD, DVD írás

Csomagolás és logisztika

Elérhetőségek:

8000 Székesfehérvár, Aszalvölgyi u. 7. tel.: 22/533-571 fax.: 22/533-599 e-mail: vtcd@vtcd.hu www.vtcd.hu

authoring studió: 1021 Budapest, Hüvösvölgyi út 54. tel.:+36 1 3921-217 fax:+36 1 3921-238 e-mail:authoring@vtcd.hu

Minőség, tapasztalat, megbizhatóság...

VTCD VIDEOTON

Kompaktlemez-gyártó Kft.

AKTUÁLIS

FÓKUSZ

ÜZLET

TECHNOLÓGIA

HORIZONT

ÁLLANDÓ ROVATAINK

Pénzt köpködött a meghekkelt bankautomata

A Black Hat hekkerkonferencián egy biztonsági kutató bemutatta, miként lehet feltörni a banki automatákat.

» computerworld.hu/cikk/atm-hekkeles

Őszre megérkezik a 3D kamera

Úgy tűnik, előbb forgathatunk mi magunk 3D házimozit, mint hogy számottevő 3D Blu-ray mozifilm lenne elérhető.

» computerworld.hu/cikk/3dkamera

Itt az új Amazon Kindle

A harmadik generációs e-olvasó könnyebb és a képernyője is jobb, emellett árban is a piac előtt jár. A wifis változat ára 139 dollár, míg a 3G-seké 189 USD.

» computerworld.hu/cikk/kindle3

Összefogott a Google és a Yahoo! Japan

Ismét a Google technológiáját használja a japán Yahoo! leányvállalat. Erről a megállapodásról a napokban tett bejelentést a két cég.

» computerworld.hu/cikk/google-japanban

WWW.COMPUTERWORLD.HU

IMPRESSZUM COMPUTERWORLD-Számítástechnika
ICT-stratégia döntéshozóknak • alapítva 1969 • 2010. augusztus 3. • XLI. évfolyam 31–32. szám

Kiadja	IDG Hungary Kft. 1075 Budapest Madách Imre út 13–14. A ép.
HU ISSN 0237-7837	Postacím: 1374 Budapest 5, Pf. 578 Internet: www.idg.hu
Bankszámlaszám	10300002-20328016-70073285
Felelős kiadó	Bíró István ügyvezető – ibiro@idg.hu
Műszaki vezető	Babinecz Mónika – mbabinecz@idg.hu
Nyomás és kötészet	D-Plus Kft. 1037 Budapest, Csillaghegyi út 19–21.
Ügyvezető igazgató	Németh László

SZERKESZTŐSÉG

Főszerkesztő	Dervenkár István – idervenkar@idg.hu
Főszerkesztő-helyettes	Szalay Dániel – dszalay@idg.hu
Olvasószerkesztő, korrektor	Sz. Erdős Judit – jerdos@idg.hu
Munkatársak	Dávid Imre – idavid@idg.hu Egri Imre – iegri@idg.hu Horváth Ádám – ahorvath@idg.hu Kis Endre – ekis@idg.hu Kodolányi Balázs – bkodolanyi@idg.hu Makk Attila – amakk@idg.hu Mallász Judit – jmallasz@idg.hu Vass Enikő – evass@idg.hu
Szerkesztőségi ügyelet	Bödör Eszter – ebodor@idg.hu Telefon: 577-4343, fax: 266-4343 Internet: www.computerworld.hu e-mail: levelek@idg.hu

Újságíróink szakmai képzésének hátterét a NetAcademia Oktatóközpont biztosítja. www.netacademia.net

TIPOGRÁFIA

Berényi István – iberenyi@idg.hu
Berényi Teréz – tberenyi@idg.hu

HIRDETÉSFELVÉTEL

Hirdetési igazgató	Melovics Csaba – csmelovics@idg.hu Telefon: 577-4310, fax: 266-4274
Lapreferens	Rodriguez Nelsonné – irodriguez@idg.hu Telefon: 577-4311
Kereskedelmi asszisztens	Bohn Andrea – abohn@idg.hu Telefon: 577-4316, fax: 266-4274 e-mail: keriroda@idg.hu

TERJESZTÉS ÉS ÜGYFÉLSZOLGÁLAT

Terjesztési igazgató	Babinecz Mónika – mbabinecz@idg.hu Telefon: 577-4301, fax: 266-4343 MediaShop: mediashop.idg.hu e-mail cím: terjesztes@idg.hu

MARKETING

PR-munkatárs	Kovács Judit – jkovacs@idg.hu

KONFERENCIA

Rendezvényszervezés	Bödör Eszter – ebodor@idg.hu Odrovics Szonja – szodrovics@idg.hu

JOGI KÖZLEMÉNYEK

Szerkesztőségünk a kéziratokat lehetőségei szerint gondozza, de nem vállalja azok visszaküldését, megőrzését.
A COMPUTERWORLD-ben megjelenő valamennyi cikket (eredetiben vagy fordításban), minden megjelent képet, táblázatot stb. szerzői jog védi. Bármilyen másodlagos terjesztésük, nyilvános vagy üzleti felhasználásuk kizárólag a kiadó előzetes engedélyével történhet.
A hirdetéseket a kiadó a legnagyobb körültekintéssel kezeli, ám azok tartalmáért felelősséget nem vállal.

TERJESZTÉSI, ELŐFIZETÉSI, ÜGYFÉLSZOLGÁLATI INFORMÁCIÓK

A lapot a Lapker Rt., alternatív terjesztők és egyes számítástechnikai szaküzletek terjesztik. Előfizethető a kiadó terjesztési osztályán, az InterTicketnél (266-0000 9-20 óra között), a postai kézbesítóknél (06/80-444-4444; hirlapelofizetes@posta.hu, fax: 303-3440)
Előfizetési díj egy évre 16 440 forint, fél évre 8220 forint, negyed évre 4110 forint.

Lapunkat a MATESZ auditálja

Olvasóink szokásait a Nemzeti Médiaanalízis méri fel.

A Computerworld az IVSZ hivatalos médiapartnere.

print-audit GfK Ipsos

A szerkesztőségi anyagok vírusellenőrzését a **NOD32 Antivirus** programmal végezzük, amelyet a szoftver magyarországi forgalmazója, a **Sicontact Kft.** biztosítja számunkra.

Küzdelem az IT-biztonsággal:
a törvény szava a valóság ereje ellen?

Keleti Arthur
az ITBN
főszervezője

Arról, hogy mennyit ér egy törvény, sokan sokféleképpen vélekednek. Függ ez attól, hogy miről szól egy törvény, vagy mit akar elérni, és persze attól is, hogy ki gondolkodik róla. Martin Luther King azt mondja: „Igaz lehet, hogy egy törvény nem oldja meg, hogy valaki szeressen engem, de visszatarthatja attól, hogy meglincseljen, és ez azt hiszem, elég fontos dolog." Eközben Mark Twain pedig éppen amellett érvel, hogy a törvény olyan, mint a homok, ami megkerülhető, de egy beérett szokás, mint a szikla, biztos büntetést hoz a bűnösre.

Azt gondolom, hogy mindkettő egyszerre igaz. Törvények nélkül nincsenek viszonyítási pontok, szokások nélkül pedig nincsen gyakorlat. A baj csak az, hogy szervezeti és társadalmi szinten ma Magyarországon elég rosszul áll a biztonság ügye a törvények és a szokások tekintetében egyaránt. Az előbbiért évek óta küzd a piac és szakmai szervezetei – közepes eredménnyel –, mivel még nem sikerült elfogadni általánosan érvényes és teljes informatikai biztonsági törvényt. Több verzió is készült az elmúlt években, de nem lehetetlen, hogy a jelenlegi kormányzat újra fogja gombolni a kabátot, és talán nemcsak az informatika biztonságát kezeli majd, hanem az információ biztonságát is, amely egyértelműen tágabb kör, és jó reményekkel kecsegtető szakmai nyitás lenne.

Másik oldalról az adatvédelmi törvény – amely annak ellenére, hogy az egyik legszigorúbb az EU-n belül – sok szempontból nyitva hagyja a kockázatok kezelését érintő kérdéseket. Az adatvédelmi biztos persze érvényt szerez a törvény szavának, de lehetőségei ma még nem minden esetben biztosítanak neki elég mozgásteret. Arról is olvashattunk már a hírekben, hogy a Facebook és más aktívan nagy mennyiségű elektronikus adatot kezelő szolgáltatások robbanásszerű népszerűsége európai szinten az Európai Unió 1995-ben kiadott adatvédelmi direktívájának újragondolására készteti a brüsszeli döntéshozókat. Nem kizárt az sem, hogy európai szintű globális megoldással rukkolnak majd elő.

Akárhogy is áll az adatvédelmi törvény szénája, az adatok és információk aktív védelmének és megfelelően biztonságos kezelésének az igazán jó hagyománya nem alakult ki Magyarországon. Legelőrébb talán a pénzintézeti szektor tart, ahol a Pénzügyi Szervezetek Állami Felügyeletének a tevékenysége ad egy kis erőt a területre érvényes és a többi szférához képest tartalmasabb biztonsági előírásoknak. Más területen (különösen az államigazgatásban) nem túl szívderítő a helyzet. Persze a fejlődés reményét hordozza magában az a tény, hogy egyre több üzemeltető és jogász ismeri föl a téma fontosságát, és annak ellenére igyekszik tenni a biztonság ügyéért, hogy nem egyértelműek a törvényi környezet támasztotta követelmények.

> Az adatok, információk aktív védelmének és megfelelően biztonságos kezelésének az igazán jó hagyománya még nem alakult ki Magyarországon.

Dacára az ilyen erőfeszítéseknek a szokások területén – talán a gazdasági válságnak köszönhetően is –, nagyobb súlya lett a gazdasági igazgató értelmezésének az anyagi helyzetről, mint a biztonsági szakértő aggodalmas szavainak az adatvesztések kockázatáról. Törvények híján a biztonság talpköveit a piaci szolgáltatók, tanácsadó cégek próbálják lefektetni de facto szintre avanzsált saját módszertanokkal. Ezek házi ajánlások, hatásuk nem tekinthető globálisnak. A szabványoknak való megfelelés (pl. ISO, SOX) valamelyest derít a képen, de ezek inkább a szervezet biztonsági szándékainak indikátorai, és kevésbé a biztonság napi gyakorlatáé (tisztelet a kivételnek). A biztonság ügyét elméletben minden döntéshozó fontosnak tartja, hiszen ki ne szeretne biztonságban lenni? Csak az ára és az oda vezető út erőforrás-szükséglete fékezi a lendületet.

Miben segíthetnek itt a törvények? Egyrészt feloldják a vezetők áldilemmáit, mert megfelelő szankciók kilátásba helyezésével más utat mutatnak arrafelé, ahol eddig a költséges biztonsági beruházások édes alternatívája, a tétlenség lakozott. Másrészt meghúzzák az alapvonalat, a kötelező minimális szintet például abban, hogy az állampolgárok személyes adatait hogyan kezelje az államigazgatás összetett informatikai rendszereiben és az intézmények közötti kommunikációban, vagy miképpen járjanak el a szereplők egy biztonsági incidens nyilvánosságra hozatalában. Segíthetnek abban is, hogy hogyan értelmezzük a biztonság eltérő fogalmait, a veszélyeket, a kockázatokat és kezelésük módját. Szerintem ezek egységes szemléletének és a szankcionálásnak a hiánya ma komoly gátja olyan alapvető feladatoknak, mint a kritikus infrastruktúrák és a nemzeti vagyon informatikai védelme, valamint az állampolgárok saját biztonságának megteremtése és propagálása (például az identitás- és az adatlopás elleni védelem).

A szükséges törvények meghozatalához és a végrehajtáshoz akarat és erőforrás kell. Még nem jelenik meg markánsan, de az előbbihez talán került az új kormányzat raktárába némi elszántság, és hosszabb távon nemcsak információvédelmi törvényben, hanem hivatalos szervben is reménykedhetünk. Az erőforrások tekintetében viszont szkeptikus vagyok, mert a biztonság drága, és nem túl látványos. Több szférában eddig sem az akarat, hanem a biztonság mellé rendelt anyagi és emberi erőforrás fullasztotta meg a védelmi elképzeléseket. Ugyanakkor a biztonság jó, mert gazdasági stabilitást teremt, ami egy éppen talpra álló, növekvő gazdaság legfontosabb alapköve... kellene, hogy legyen.

Legális az iPhone feltörése

Egri Imre ▪ *Steve Jobs* kereshet újabb módszert, hogy az iPhone-tulajdonosokat az App Store-hoz kösse. Az amerikai szövetségi jogértelmezés szerint ugyanis a telefon felszabadítása ártalmatlan, sőt akár még hasznos is lehet. Az Apple ezentúl nem tudja jogi úton meggátolni, hogy független forrásból töltsünk fel tartalmat, szoftvert készülékeire.

A napokban jelentette be az amerikai szerzői jogi iroda, a U.S. Copyright Office, valamint a Kongresszusi Könyvtár (Library of Congress), hogy elbukott az Apple kezdeményezése, miszerint bűncselekménynyé nyilvánítaná az úgynevezett „jailbreaking”-et, vagyis azt a törést, amelynek révén az iPhone-ra feltölthetővé válnak a nem Apple-től származó tartalmak is. A szövetségi döntés az eszközök gyártói kötöttségek alól való felszabadítását azok közé a praktikák közé sorolta, amelyek nem sértik a Digital Millenium Copyright Act (DMCA) elveit.

„Amennyiben valaki annak érdekében tör fel egy okostelefont, hogy a rajta futó operációs rendszer együttműködhessen a függetlenül fejlesztett alkalmazásokkal, amelyeket a telefon, illetve operációs rendszerének gyártója nem hagyott jóvá, a tisztán az együttműködés céljából végrehajtott módosítások tisztességesnek minősülnek” – olvasható a rendelkezésben.

Egyúttal elutasították az Apple 2009-es beadványát, amelyben kérte az iPhone feltörésének törvénytelenné nyilvánítását arra hivatkozva, hogy ehhez az iOS és a bootloader (indítómodul) kalózváltozatára van szükség. A szerzői iroda úgy ítélte meg, hogy a hardver- és operációsrendszer-gyártónak semmilyen kára nem származik abból, hogy a feltörést követően független, nem jóváhagyott alkalmazások futtathatók a készüléken.

Még 2008-ban kérte az Electronic Frontier Foundation (EFF), hogy a mobiltelefon feltörését illetően adjon ki a jogvédő hivatal mentességi nyilatkozatot, amire az Apple hivatalos megjegyzésekben reagált. Az EFF és az azt támogató cégek – mint például a Firefox böngészőt fejlesztő Mozilla – kezdettől azt szerette volna elérni, hogy a szerzői jogi hivatal adja áldását arra, hogy a felhasználók minden büntetéstől való félelem nélkül telepíthessenek olyan alkalmazásokat, amelyek nem az Apple App Store-ból származnak. Most ez hivatalosan is törvényessé vált, az EFF pedig nagy örömmel üdvözölte a hatóság döntését.

Az EFF közbenjárása nyomán nemcsak a telefonfelszabadítók (jailbreak) lélegezhetnek fel, hanem azok is, akik hálózatfüggetlenítik mobiljukat, azaz feltöréssel lehetővé teszik, hogy bármely szolgáltató SIM-kártyáját használni lehessen bennük. A hivatalos álláspont most már lehetővé teszi, hogy valaki a használt mobilkészülékét – nem az újonnan vásároltat! – „kilokkolja” – vagyis eltávolítsa a SIM-lockot – és más szolgáltató hálózatán használja tovább. Annál is inkább támogatja a Copyright Office a használt mobilok hálózatfüggetlenítését, mert az megkönnyíti újrafelhasználásukat életciklusuk kiterjesztésével, ezzel csökkentve a környezet terhelését.

Sőt, annak sem kell félnie, aki jogkövető módon megvásárolt DVD-inek másolásvédelmét feltörve rövid részleteket emel ki kedvenc filmjeiből, hogy ezekből zenei klipeket mixeljen, és azokat megossza olyan videós oldalakon, mint például a YouTube. A DVD-rip tehát ártatlan céllal – legalábbis Amerikában – már nem számít jogsértőnek.

A Mozillát – a norvég Opera Software-rel egyetemben – olyannyira irritálta az Apple zárt, a felhasználót kizárólagosan uraló rendszere, hogy emiatt nem is indultak el a Mozilla- és Opera-böngészők iPhone projektjei. Mára az Opera Mini ugyan mégis megjelent iPhone-ra is, de a Mozilla továbbra sem adja be a derekát, több mobil Firefox kiadáson is dolgozik jelenleg, de ezek között nincs ott az iPhone változat.

A hatósági döntés által nemcsak a felhasználók élvezhetnek nagyobb szabadságot, de zöld lámpát kaptak azok a kutatók is, akik eddig azért nem tudtak biztonsági rések után kutatni a PC-s és konzolos játékokban, mert a törvény tiltotta a kódot védő rendszer kijátszását, feltörését.

„A közösség számára haszonnal kecsegtető célú számítógépes biztonsági vizsgálódás és a kutatás eredményének publikálása nincs kihatással a munka kreatív oldalára, és nem valószínű, hogy kedvezőtlen hatással lenne a piacra vagy a jogvédett termék értékére” – áll a hivatalos döntésben. Sőt, a Kongresszusi Könyvtár jóváhagyását élvezi a javaslat, miszerint egyes videojátékok feltörése és visszafejtése is jogszerűen művelhető lesz, amennyiben tesztelés, elemzés és a biztonsági hibák felderítése céljából történik.

Ismét vásárol a Magyar Telekom

A Magyar Telekom Nyrt. megállapodást írt alá a Daten Kontor Csoport 100 százalékának megvásárlásáról – jelentette be a távközlési óriás. A Magyar Telekom július 20-án írta alá az adásvételi megállapodást a Daten Kontor Kft., a DK Telecom Zrt. és a DK Consulting Zrt. (DK-csoport) 100 százalékának megvásárlásáról. Az adásvételi szerződésben megállapított vételár maximum 1,4 milliárd forint, amely függ a következő két üzleti év pénzügyi eredményeitől, és korrigálják a zárás időpontjában fennálló nettó adósságállománnyal. A DK-csoport informatikai alkalmazások fejlesztésével, telepítésével és üzemeltetésével foglalkozik. A cégcsoport konszolidált árbevétele 2009-ben 2,2 milliárd forint, EBITDA-ja 357 millió forint volt. A Magyar Telekom az akvizícióval tovább kívánja erősíteni pozícióját az informatikai szolgáltatások piacán. A közlemény hangsúlyozza: a tranzakció lezárásához a Gazdasági Versenyhivatal jóváhagyása is szükséges lesz.

SZEMÉLYI HÍREK

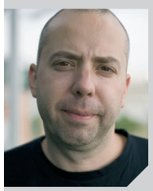
Winkler János

A Magyar Telekom volt vezérigazgató-helyettese a Malév igazgatóságának tagja lett. *Winkler János* 1992-től a Westel Rádiótelefon Kft.-nél, majd 1996-tól a T-Mobile Magyarország Rt.-nél (korábban Westel Mobil Rt.) marketing és értékesítési vezérigazgató-helyettesként, 2006-tól pedig vezérigazgatóként dolgozott. Kiemelkedő szerepe volt a 2004. évi Westel/T-Mobile név- és márkaváltásban. 2006-tól a Magyar Telekom Nyrt. vezérigazgató-helyettese, a Mobil Szolgáltatások Üzletág vezetője, 2008-tól a Lakossági Szolgáltatások Üzletág vezetője volt. Idén áprilisban közös megegyezéssel távozott a holdingcégtől.

Rozgonyi Krisztina

A Nemzeti Hírközlési Hatóság volt elnöke a PRK Partners regionális ügyvédi iroda magyarországi képviseleténél, a technológiai, illetve médiaszabályozási terület vezetőjeként dolgozik júliustól. *Rozgonyi Krisztina* június 15-én jelentette be lemondását az NHH éléről. A szakember néhány hónapig irányította a hatóságot, amelynek élére *Pataki Dániel* tavaly decemberi lemondását követően nevezték ki. Az NHH élére *Orbán Viktor* nem nevezett ki elnököt, mert a hatóságot összevonják az ORTT-vel.

Nádori Péter



Nádori Péter lett az Origo főszerkesztője. *Weyer Balázs*, az eddigi főszerkesztő a társoldalak és szolgáltatások vezetőjeként dolgozik tovább. Ezzel egy már régebb óta működő feladatmegosztást tett hivatalossá a Magyar Telekom médiavállalata. Az indoklás szerint az Origo Zrt. portfóliójának bővítése egyre több munkát igényel, ezért választották külön a hírportált és a társoldalakat, a mobiltartalmakat és a most induló blogszolgáltatást is magában foglaló cégcsoport főszerkesztői feladatait. Nádori 1998 és 2001 között egyszer már volt az Origo vezetője, mielőtt a HVG Online főszerkesztője lett.

HÍRMOZAIK

SAS Risk Management

A SAS Risk Management for Banking az operatív és stratégiai szintű döntéshozatalt egyaránt támogatja. A megújult alkalmazás olyan átfogó eszköz a bankszektor számára, amelynek fejlett adatkezelési, analitikai és jelentéskészítési képességei vannak. A szervezetek ezáltal meg tudják állapítani a kockázatokat és kitettségeket minden kockázattípusra. Nem csupán hitelkockázatról van tehát szó, hanem a bank minden szintjén előforduló különböző kockázati területekről.

SQL Anywhere 12

Megjelent a Sybase SQL Anywhere adatbázis-kezelő új verziója, amely erős térinformatikai és iPhone-támogatást, továbbfejlesztett mobil szinkronizációs technológiát és a most debütáló scale-out technológia révén vállalati „adatbázisfelhők" létrehozását biztosítja. Az alkalmazást vállalati adatközpontokon kívül futó, üzletileg kritikus adatbázis-rendszerek működtetésére optimalizálták. Fut nagyvállalati szerverként és mobileszközökön; alkalmas vállalati „adatbázisfelhők" létrehozására.

Gyorsuló folyamatok

Az elfoglalt, változatos dokumentum-kezelési megoldásokat igénylő irodák számára kínál megoldást a Xerox új, fekete-fehér multifunkciós nyomtatója, a WorkCentre 3550. A készülék akár 33 lap/perc sebességgel nyomtat, továbbá másol, szkennel és faxol A/4-es méretben. A berendezés alkalmas az automatikus kétoldalas nyomtatásra és – a CentreWare Internet Sevices eszközkezelő és -felügyelő szoftver segítségével – a munkafolyamatok felgyorsítására.

REGISZTRÁLJON

Ha szeretné hétről hétre a legfontosabb szakmai résztvevőkhöz eljuttatni az Ön cégével kapcsolatos információkat, regisztráljon Céginfó szolgáltatásunkra oldalunkon.

ceginfo.computerworld.hu

Adattovábbítás fénnyel

Egri Imre ▪ Az Intel bejelentette, hogy kifejlesztette a fény továbbítása útján kommunikáló belső összeköttetés prototípusát. Az új technológiával a számítógépen belüli kommunikáció sávszélessége nagyban megnő, másodpercenként 50 gigabitet képes forgalmazni az optikai technológia. Kutatói szerint az optikai jelátvitel véglegesen kiválthatja a számítógépekben eddig alkalmazott réz mikrohuzalozást, amelyeken a viszonylag lassan mozgó elektronok szállították az információkat. A fény annyival gyorsabb, hogy egy komplett nagy felbontású mozit továbbíthatunk ezen az optikai kapcsolaton egyetlen másodperc alatt. A technológia másik előnye, hogy nagyobb távolságra vihetők át a jelek.

Justin Rattner, az Intel technológiai főnöke áttörésként értékelte az optikai átvitel prototípusát, hiszen a rézalapú elektromos jelátvitel már elérte a technológia határait. Rengeteg adatot kell továbbítani a modern rendszerekben, és a rézalapú átvitel már másodpercenként 10 gigabit továbbításánál kihívásokkal küzd. Még ha sikerül is megvalósítani ilyen masszív átvitelt rézalapokon, az akkor is mindenképpen visszaüt, lerövidül az átviteli távolság.

Rattner szerint „a fotonika adja meg a lehetőséget, hogy gazdaságos módszerrel ilyen tömeges adatmennyiséget keresztüljuttassunk egy szobán". Eddig is használtak lézert olyan elektronikai berendezésekben, mint például a DVD-olvasó, és használták nagyobb távolság áthidalására alkalmas adattovábbító rendszerekben is. A lézertechnológia azonban meglehetősen drága is lehet, és az Intel szeretné olyan költségszintre hozni, hogy az beépíthető legyen mindennapi eszközeinkbe. Rattner szerint a cég szeretné továbbfejleszteni az optikai átvitel technológiáját a csatornák számának növelésével, hogy elérje az 1 Tbps (másodpercenként 1 terabit) adatátviteli teljesítményt.

A jelenlegi bemutatón egyelőre annyi bizonyosodott be, hogy az Intel egy kísérleti rendszerben már tudja működtetni az „optical interconnect" rendszert. A következő lépésben egy lapkán belül fogják alkalmazni a technológiát, majd tömeggyártásba viszik, hogy az évtized közepére elérhesse a fogyasztókat is, és meghonosodjon a PC-k, kiszolgálók és mobileszközök világában.

Mario Paniccia az Intel nevében elmondta, hogy ugyan nem láthatjuk viszont a lapkák belsejében az optikai összeköttetés technológiáját, de már előbb megjelenhet az alaplapokon, kiváltva mondjuk a CPU-t és a memóriát eddig összekötő nyomtatott áramköri vezetékeket. Ezzel csökkenne a késleltetés, gyorsulna a feldolgozás.

Rattner szerint elsőként az adatközpontokban érezhetné magát otthon az optikai kapcsolat, de hasznát vehetnék fogyasztói vonalon, mondjuk akkor, amikor egy mozifilmet kell áttölteni mobileszközre.

A kutatási prototípus több előzőleg létrehozott Intel-fejlesztést foglal magában, ezek a fény kibocsátásában, manipulálásában, kombinálásában, szétválasztásában és észlelésében játszanak szerepet. Az optical interconnect rendszer egy PC-alaplapon magában foglal egy átviteli lapkát, amely négy optikai csatornát nyit üvegszálakon, emellett egy vevő lapkára is szükség van, amely fogadja a beérkező fényt, elosztja a jelet és a fényimpulzusokat elektronikus jellé alakítja.

Az Intel már eddig is dolgozott egy olyan optikai összeköttetésen, amely tárolóeszközöket, mobilkészülékeket és megjelenítőket, monitorokat köthet össze a PC-vel, akár 100 méteres távolságot áthidalva. A Light Peak interfész 10 Gbps sávszélességig vehető igénybe, és az Intel az USB potenciális utódját látja benne.

Fejlesztőcéget vesz az Adobe

Szalay Dániel ▪ Az Adobe Systems megállapodott a szoftverfejlesztéssel foglalkozó Day Software Holding megvásárlásáról – jelentette be a leendő tulajdonos. Az Adobe 240 millió dollárt fizet az akvizícióért.

A svájci (bázeli) központú Day Software webes tartalomkezelő, digitális vagyongazdálkodási menedzsment, valamint csoportmunka szoftvermegoldásokat fejleszt. Ezeket az Adobe szeretné beépíteni a vállalatoknak kínált termékportfóliójába. „A Day megvásárlásával tovább tudjuk bővíteni kínálatunkat" – olvasható az amerikai szoftvercég közleményében.

A Day az Adobe Digital Enterprise Solutions üzletágába tagozódik be – mondta el a felvásárolt vállalat ügyvezetője, *Erik Hansen*, aki a megállapodás értelmében csatlakozik az Adobe csapatához. A megállapodást még a hatóságoknak is jóvá kell hagyniuk. Az akvizíció az Adobe tervei szerint a 2010-es pénzügyi év negyedik negyedévére zárulhat le. Az Adobe egyébként nyilvános vételi ajánlatot tesz a Day nyilvánosan jegyzett részvényeire.

Külföldre megy a Kulcs-Soft

A társaság 2010. éves üzleti tervének megfelelően a Kulcs-Soft megkezdte a terjeszkedést a nemzetközi piacon – jelentette be a Budapesti Értéktőzsde B szekciójában jelen lévő informatikai vállalkozás. A tájékoztatóban úgy fogalmaznak, hogy a június 10-i spanyol piacra lépést követően mára már Szlovákia, Románia, Csehország, Oroszország, Anglia, az Egyesült Arab Emirátus és a Dél-afrikai Köztársaság területén is értékesítik az adott ország nyelvén, lokalizált formában szoftvereiket. A részvénytársaság ezt nagy előrelépésnek tartja. A szoftvereket minden országban a helyi törvényeknek megfelelően lokalizálták, amihez a Kulcs-Soft minden esetben helyi szakemberek segítségét vette igénybe. A vállalat közölte: a kezdeti eredmények nagyon kecsegtetők, mert július folyamán a lokalizált verziók hatására a külföldi piacokból származó bevétel július hónapban 200 százalékkal nőtt az előző hónapok bevételéhez képest.

Uniós vizsgálatok az IBM ellen

Szalay Dániel ▪ Trösztellenes vizsgálatot indított az Európai Bizottság a Kék Óriás ellen, amiért az – legalábbis a gyanú szerint – megsértette az EU monopolellenes rendelkezéseit a nagy teljesítményű, úgynevezett mainframe számítógépes rendszerek piacán. Az IBM közölte: kész együttműködni a hatósággal.

A lapunkat is kiadó IDG nemzetközi hírügynöksége, az IDG News Service brüsszeli beszámolója szerint az Európai Bizottság (EB), az EU fő antitröszt hatósága azt közölte, hogy két különálló ügyben is vizsgálódnak az IBM ellen. Mindkét ügy az IBM mainframe piaci magatartásával függ össze.

Az első vizsgálat az emulátorszoftver-gyártó T3 Technologies és Turbo Hercules panasza nyomán indult. Ők azt állították keresetükben, hogy az IBM a saját maga által gyártott hardverek beszerzéséhez köti operációs rendszerének felhasználhatóságát, és ezzel kizárja a kisebb fejlesztőket a versenyből. „Az IBM gyakorlata megakadályozza a TurboHerculest abban, hogy olyan felhasználók számára is elérhetővé tegye mainframe megoldásait, akik a nyílt forráskódú rendszereket választanák" – jelentette ki még korábban *Roger Bowler*, a francia cég elnöke. Az IBM egyébként – még a vizsgálat megindulása előtt – meglehetősen lekezelően nyilatkozott az őt most bepanaszoló cégről. A TurboHerculest olyan vetélytársnak nevezte, „amely a nagygépeink működését imitáló rendszerek forgalmazása révén szeretne hasznot húzni az IBM nagyarányú befektetéseiből". Más helyütt meg olyan zugcégekhez hasonlította a TurboHerculest, amelyek az ismert ruházati gyártók termékeinek rossz minőségű, olcsó „koppintásával" kereskednek.

A másik ügyben az Európai Bizottság azt vizsgálja, hogy az IBM valóban diszkriminatív módon viszonyul-e a mainframe gépeket karbantartó szolgáltatókhoz. Az eljárás pikantériája, hogy az unió épp nemrégiben hozott létre közös cloud computing konzorciumot az IBM-mel.

Az IBM, amely mind a mai napig a világ egyik legnagyobb mainframe számítógépgyártója, a vizsgálat bejelentése után közölte, teljes mértékben kész együttműködni az EU-val. Ugyanakkor jelezte, hogy a Turbo Hercules, illetve a T3 beadványának hátterében riválisát, a Microsoftot véli felfedezni. A Microsoft részéről egyelőre nem kommentálták az IBM vádjait.

ESET NOD32 ANTIVIRUS A NAV N GO-NÁL

Egyenes út a sikerhez

A Nav N Go sikertörténete 2005-ben kezdődött. A hazai szoftverfejlesztő cég iGO névre keresztelt navigációs szoftverével vált ismertté a magyar és a külföldi közönség számára, mára pedig a legdinamikusabban fejlődő hazai IT-vállalkozások között tartják számon. A közel 300 alkalmazottat foglalkoztató Nav N Go számítógépeit 2007 októbere óta az ESET NOD32 Antivirus védi.

„Gépeink 80 százalékán szoftverfejlesztés folyik, a maradék 20 százalékon pedig pénzügyi programok és a hagyományos Office alkalmazások futnak, így nem mindegy, hogy a vírusirtó mennyire terheli le a rendszert. Elsősorban kollégáink korábbi pozitív tapasztalatai miatt döntöttünk az ESET NOD32 mellett. Azt hiszem, az nyomott a legtöbbet a latban, hogy használtuk már, ismertük, jó volt és jól működött" – foglalta össze a kezdeti tapasztalatokat *Lipcsák Róbert*, a Nav N Go Kft. IT-vezetője.

Mivel a Nav N Go számítógépein mind a telepítés, mind pedig a frissítés központilag zajlik, a bevezetés előtt a megfelelő szerver-kliens beállításokat is tesztelni kellett. „A fejlesztések miatt jó néhány tesztkörnyezettel rendelkezünk, így nem okozott gondot a beállítások tesztelése. Megnéztük, hogyan működik a központi adatbázis-frissítés, illetve hogy a kliensgépek rendesen frissülnek-e, nincs-e valamilyen fennakadás" – magyarázta a Nav N Go szakembere. A cég végül pár hónapos tesztelés után vásárolta meg a licenceket, a telepítés pedig központilag, szegmensenként történt úgy, hogy a felhasználók nagy része nem is vette észre a változást. „Mivel alapvetően már sok kliensgépen amúgy is a NOD futott, a kollégák nem nagyon észlelték a váltást. Nagyon kevés visszajelzést kaptunk, de azt hiszem, hogy ez csak jót jelenthet, hiszen a munkatársak általában akkor jeleznek, ha probléma van. Ilyen pedig nem volt. Természetesen sok utólagos beállításbeli finomítást követelt, hogy a vírusirtó tényleg ne akadályozzon semmilyen egyéb szoftvert, de ezek minden esetben megoldódtak" – összegezte Lipcsák Róbert. A telepítéshez és a frissítésekhez a cég szakemberei az ESET Remote Administrator központi menedzsmenteszközt használják, mely lehetővé teszi a teljes hálózat egyetlen számítógépről történő felügyeletét.

> A telepítéshez és a frissítésekhez a cég szakemberei az ESET Remote Administratort használják...

A kliensgépeken futó NOD32 egy komplett biztonsági rendszer része, amelybe hardveres tűzfal, önálló spamszűrő és az e-mail forgalmat szűrő külső szerver is beletartozik. „Nagyon ritka, hogy ezeken átjut valamilyen károkozó" – mondta a szoftverfejlesztő cég szakembere.

A cég nemrég tért át a NOD32 Antivirus legújabb, 4-es verziójára. Ehhez a hazai forgalmazó szupport csapatától kértek segítséget. „Arra voltunk kíváncsiak, hogyan álljunk át a 4-es verzióra. Teljesen tökéletes támogatást kaptunk, abszolút korrekt és elegendő mennyiségű információval. Az átállás így problémamentesen zajlott, és azóta sem tapasztaltunk semmilyen fennakadást" – összegezte a szupporttal kapcsolatos tapasztalatait Lipcsák Róbert. ■

A Nav N Go Kft.-ről

A 2005-ben alakult Nav N Go Kft. műholdas navigációs szoftvereiről vált ismertté Magyarországon és világszerte egyaránt. Az iGO szoftver nemzetközi sikerének köszönhetően, a vállalat rövid idő alatt jelentős növekedést ért el, és a kezdetben 7 fővel induló cég mára már közel 300 alkalmazottat foglalkoztat. A Nav N Go jelenleg mintegy 70 OEM-partnerrel rendelkezik világszerte és 20 országban tart fenn disztribúciós központot, így szoftverei szinte az egész világon elérhetők. Az általuk fejlesztett 3D-s navigációs programokat ma már olyan márkák használják, mint a HP, a Sony PSP vagy a Clarion.
A Nav N Go időközben az ország egyik legdinamikusabban fejlődő IT-vállalkozásává nőtte ki magát, 2009 októberében elnyerte a Deloitte *„Rising stars"* díját. Legújabb szoftverüket, a prémium kategóriás *iGO primo* sorozatot a 2010-es CeBIT-en mutatták be.

Kérdéses a WiMax jövője?

Egri Imre ▪ Bezárt a tajvani Intel WiMax iroda, emiatt a szigetországban kitört a médiavihar és megkérdőjeleződött a WiMax jövője.

Nagyon úgy tűnik, hogy Tajvan vezetése és a WiMax mobilhálózat érdekeltségi köre szerint azt jelenti a helyi Intel WiMax iroda bezárása, hogy mindenestül dobja a technológiát. Nem kis frusztrációt váltott ki a hír, hiszen ha az Intel kihátrálna az ügy mögül, akkor az egész helyi érdekeltségi kör helyzete tarthatatlanná válna.

A szigetország nagyjai a WiMax mellett állnak, így nagy nyugtalanság tört ki még a helyi tőzsdén is. Tajvan gazdasági minisztere kellett, hogy megnyugtassa a közvéleményt: az ország akkor is a WiMax mellett lesz, ha maga az Intel dobja a technológiát: „Tajvan WiMax melletti elkötelezettsége gondos tervezés eredménye, amelyben részt vett az ipar, a kormány és az akadémiai szakértők is, így rakva le a helyi WiMax-fejlesztés terveit. A tajvani ipar és kormányzat erősen bízik abban, hogy folytatódik a technológia fejlesztése, és egy vállalat belső döntése nem változtat a kormány vezérelvein."

A nagy kavarodás ellenére az Intel ragaszkodik hozzá, hogy egyáltalán nem hátrál ki a WiMax mögül. Pusztán azért döntött az iroda bezárása mellett, mert az elvégezte feladatát, és megfelelőképpen előmozdította a WiMax ügyét az országban. Valahogy ez az információ nem jutott el a tajvaniakhoz. Az Intel elismerte, hogy hibát követett el, amikor nem értesítette előzetesen a kormányt az iroda bezárásáról. Ezután pedig már hiába adott ki a processzoróriás nyilatkozatot a WiMax mellett, az nem törte meg a rémhírek erejét. A miniszter beszéde és a sajtókonferencia ellenére az újságcímek még mindig az Intel megerősítő válaszára váró állapotot tükrözik. A kavarodást akaratlanul fokozta, hogy az Intelt senki nem hívta meg a sajtókonferenciára, ahol még idejekorán tisztázhatta volna a helyzetet. Így *Nick Jacobs*, az Intel szóvivője csak e-mailben reagálhatott a fejleményekre: „Minden, amit tehetünk az, hogy ismételten megerősítjük a tényt, miszerint semmi sem változott, az Intel továbbra is elkötelezett a WiMax mellett" – írta.

FTC–Intel: peren kívüli egyezség

Az Egyesült Államok Kereskedelmi Bizottsága (Federal Trade Commission, FTC) két héttel kitolta az Intellel a cég trösztgyanús viselkedésével kapcsolatban indított vizsgálata keretében folytatott tárgyalások határidejét. Az FTC eredetileg június 21-én függesztette fel ideiglenesen a vállalat elleni jogi lépéseket; az új megegyezés értelmében a felek augusztus 6-áig tárgyalnak az esetleges megegyezéssel kapcsolatos szerződésről.

Az FTC decemberben nyújtott be keresetet az Intel ellen. Az ügynökség vádjai szerint a gyártó domináns piaci helyzetével visszaélve, több mint egy évtizede akadályozza a szabad verseny kialakulását a nemzetközi chippiacon. A bizottság szerint az Intel „szisztematikus kampányt" folytatott annak érdekében, hogy akadályozza konkurensei megerősödését; korlátozta a vásárlók szabad termékválasztáshoz való jogát és az innovációs törekvéseket is letörte.

Böngészőalapú szoftveres mérési rendszer

Computerworld.hu ▪ Az NRC és az Adverticum a közismert VMR-kutatás közel 50 ezer főt számláló paneljére, valamint az Adverticum AdServer NG adataira építve VMR-AdProfile néven egy új, böngészőalapú szoftveres mérési rendszert indított el azért, hogy a hirdetők, a médiatulajdonosok és az ügynökségek médiatervezői pár kattintással, az eddig megszokott adatok mellé a kampány által elért célcsoport demográfiai összetételéről is fontos adatokat kaphassanak, segítve ezzel a hirdetőket céljaik elérésében.

Az online hirdetések egyik legnagyobb előnye a többi médiummal szemben, hogy a reklámozó pontosan láthatja, hányan találkoztak online hirdetésével. A kattintásokról, az egyedi látogatókról, a kampány hatására vásárlókról (post-view, post-click) pontos számot kaphat, és ennek köszönhetően értékelheti kampánya hatékonyságát. Azt, hogy kiket szólított meg reklámja, kiket ért el valójában, eddig csak külön kutatás megrendelésével tudta meg a hirdető.

A hamarosan 10 éves VMR, amely a honlapok demográfiai profiljának mérésével segítette a hazai online hirdetési piac fejlődését, az elmúlt év fejlesztésének köszönhetően egy jelenleg 50 000 fős VMR-panel segítségével a hirdetőknek, médiatulajdonosoknak és ügynökségeknek már nemcsak a médiatervezésben, de a kampány által elért célcsoport demográfiai profiljának megismerésében is segítséget nyújt. Az AdProfile mérésben az NRC független kutatócégként a VMR-panel felépítésével, üzemeltetésével és a mérési sztenderdek elkészítésével, illetve a mérés auditálásával vesz részt, míg az Adverticum az AdServerNG-ben lévő adatokhoz csatolja a VMR-panelben lévő demográfiai és egyéb VMR-kutatásból származó adatokat. Ezeket a médiatulajdonosok, illetve a kampányt menedzselő ügynökségek a kampányriportokban kérhetik le.

A kampányjelentésekből a hirdetők, ügynökségek a nem, kor, iskolai végzettség, illetve lakóhely típusa alapján ismerhetik meg az elért célcsoport összetételét. Igény esetén, kampánymérettől függően további részletes adatokhoz is juthatnak az Adverticum AdServer NG-t használó vállalatok, úgymint foglalkozás típusa, családi állapot, háztartásban élő személyek száma és összetétele, ESOMAR státusz, internethasználati szokások, online vásárlási szokások stb.

A VMR-panelen alapuló mérés a kampányprofil megismerése mellett lehetőséget teremt arra is, hogy úgynevezett reklámutóteszt segítségével megtudjuk a kampány célcsoportra gyakorolt hatását is: kik emlékeznek a reklámra, milyen üzenet jutott át, mi változott a márkafogyasztó kapcsolatában stb. „Az AdServerNG megtervezésekor nagy figyelmet fordítottunk arra, hogy a jelenlegi és a közeljövőben megjelenő online trendek követésére alkalmas, robusztus, ugyanakkor a változó igényekhez is gyorsan igazítható, rugalmas rendszert hozzunk létre, s ennek köszönhető ez a most elindított közös szolgáltatás is" – mondta *Szutor Ferenc*, az Adverticum kereskedelmi és kommunikációs igazgatója.

Új tulajdonos az Adverticumban

A B&P Braun & Partners 26 százalékos minősített kisebbségi részesedést szerzett az online hirdetéskiszolgálás piacán ismert Adverticum Zrt.-ben. Az eladó a korábbi vezetőkből és szakmai befektetőkből álló magánbefektetői csoport. Az Adverticum honlapján olvasható közlemény szerint: „Az Adverticum piaci pozíciója, tervezett fejlesztései, működési területei számos szinergiát rejtenek a B&P Braun & Partners csoporttal, és a tulajdonosi kapcsolaton túli stratégiai partnerség mindkét cég számára előnyöket kínál." A B&P Braun & Partners az elmúlt időszakban növelte piaci részesedését Romániában, ahol branding cégben szerzett tulajdont, valamint néhány hónappal ezelőtt – a tanácsadó cégek között elsőként – social media officert nevezett ki.

FÓKUSZ

Az informatika detektívjei

A jó és a rosszfiúk véget nem érő küzdelméről szóló könyvek, filmek, hírek nagy érdeklődésre tartanak számot. Elég, ha csak a címlapokon szereplő rendőrségi közleményekre, vagy éppen a helyszínelők munkáját bemutató, világszerte nagy népszerűségre szert tett sorozatokra gondolunk. Ha pedig a nyomozások, a bizonyítékok felkutatása és a különféle vizsgálatok az informatika korszerű technológiáival vegyülnek, akkor még izgalmasabb terület tárul elénk, amely nem más, mint a computer forensic. Írta: Kristóf Csaba

Szinte mindennap hallani arról, hogy a hatóságok a házkutatások során számítógépeket, adattárolókat foglalnak le, illetve, hogy egyes szervezetek, intézmények különféle incidensek miatt tesznek feljelentéseket. Mégis kevesek fejében fordul meg az a gondolat, hogy ezekben az ügyekben vajon kik és hogyan segítenek a hatóságoknak, milyen elemzéseknek vetik alá a lefoglalt eszközöket, illetve a támadásoknak áldozatul esett rendszereket. Így aztán nem meglepő, hogy **a computer forensic, amit az USA-ban és több fejlett országban is a bűnügyi tudományok egy elismert ágaként tartanak számon, hazánkban még nem igazán került be a köztudatba,** sőt megkockáztatható, hogy sok esetben még informatikai körökben is csak csekély mértékben vált ismertté. Pedig egy érdekes, rendkívül széles körű szakismereteket felölelő informatikai területről van szó, amely a számítógépes bűncselekmények burjánzása miatt egyre inkább meghatározója lesz mindennapjainknak.

A COMPUTER FORENSIC CÉLJA

A számítógépes bűnözés minden lehetőséget megragad arra, hogy a korszerű technológiák saját céljaira történő felhasználásával károkat okozzon és/vagy anyagi haszonra tegyen szert. A rosszfiúk – akik egyébként roppant módon képesek tartani a lépést az IT fejlődésével – természetesen igyekeznek mindent elkövetni annak érdekében, hogy cselekedeteik nyomait elrejtsék. A fertőzött számítógépekből felépülő botnetek, az országok határain átívelő bűnözői csoportosulások, a rootkitek stb. többek között azt a célt szolgálják, hogy a bizonyítékokra, a bűncselekményekre, illetve az azok mögött álló elkövetők kilétére ne derülhessen fény. Itt lép színre a *computer forensic*, amelynek legfontosabb célja a számítógépekkel, informatikai eszközökkel, illetve mobiltechnológiák felhasználásával elkövetett bűncselekmények felderítése, modellezése, rekonstruálása, az egyes tevékenységek időbeliségének megállapítása, valamint a bizonyítékok felkutatása, összegyűjtése.

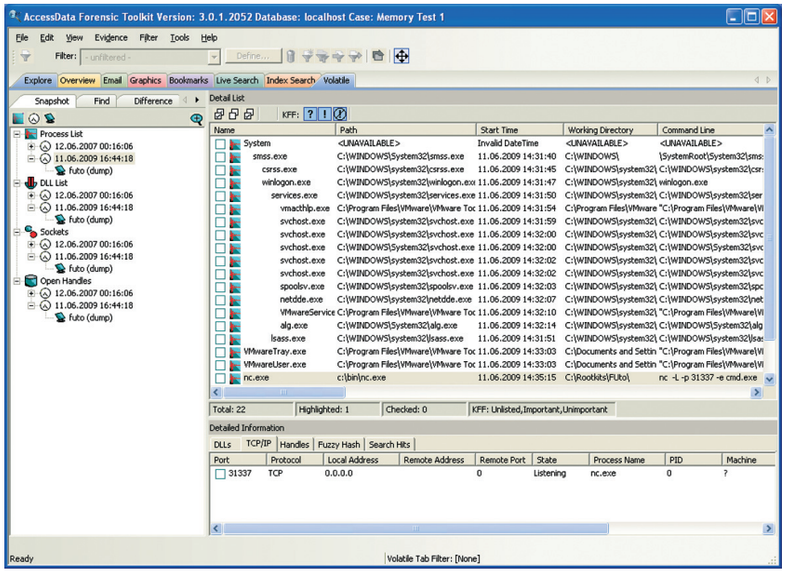
> A computer forensic célja az informatikai eszközökkel elkövetett bűncselekmények felderítése, modellezése, rekonstruálása...

FORENSIC-VIZSGÁLAT

Egy computer forensic vizsgálat többlépcsős folyamat, amely nyilvánvalóan az egyes ügyek, feladatok esetében eltérő lehet. Azonban általánosságban elmondható, hogy minden vizsgálat egy felkéréssel vagy kirendeléssel kezdődik. **A computer forensic az informatika számos területére beteszi a lábát egy-egy eset kapcsán, ugyanakkor a szakértők sem érthetnek mindenhez. (Például egy hálózatbiztonságban vagy forráskódelemzésben jártas szakembertől nem várható el, hogy egy speciális mobilkészülékből kiforrasztott chipről bizonyítékokat nyerjen ki.)** Az viszont elvárható, sőt követelmény, hogy a szakértő csak olyan ügyet vállaljon el, amelyhez megvan a kompetenciája és a megfelelő eszközparkja.

A forensic-vizsgálat következő lépése az adatok begyűjtése, ez elvégezhető akár helyszíni szemle vagy házkutatás során is. Az adattárolók lementése, image-elése online vagy offline módon valósulhat meg attól függően, hogy a vizsgált rendszert lehet-e vagy kell-e áramtalanítani. Legkésőbb ekkor kell eldönteni azt is, hogy egy adott informatikai eszközt szükséges-e lefoglalni vagy sem.

Az adatbegyűjtést követően a forensic-szakértő rendelkezésére állnak a vizsgálatban érintett rendszerekről, adathordozókról készült pillanatképek (image-ek) és azok az információk, amelyek révén elvégezhetők az elemzések. Fontos megemlíteni,



Az AccessData Forensic Toolkit grafikus felülete

hogy az úgynevezett master vagy elsődleges pillanatképről minden esetben egy további másolatot kell készíteni, amely az elemzőmunka során használható. Erre azért van szükség, mert az eredeti, többnyire bizonyítékként szolgáló master pillanatkép sértetlenségéről a teljes forensic folyamat alatt gondoskodni kell, azaz alapvető fontosságú a bizonyítékok nagy körültekintéssel való kezelése.

Barta Csaba
vezető IT-biztonsági tanácsadó
Deloitte

A forensic-vizsgálat utolsó fázisa a jelentés, szakvélemény elkészítése, amelynek során tényszerűen, objektíven és teljes körűen kell ismertetni a ténymegállapításokat, a vizsgálatok részleteit, és a lehetőségekhez mérten mindenki számára érthetően megfogalmazott véleménnyel kell előállni.

FORENSIC-ESZKÖZÖK

Egy megalapozott, az elvárásoknak megfelelő forensic-vizsgálat elvégzéséhez speciális eszközökre van szükség, amelyek között hardvereket, perifériákat és szoftvereket is fellelhetünk. **A hardveres eszközök gyakran a hitelességet és a sértetlenséget szolgálják. Adathordozók vizsgálata során alapvető fontosságú az írásvédettség megteremtése, ennek legbiztosabb módja a hardveres írásvédő. Ezek különböző (IDE, SATA, SCSI, USB, FireWire, stb.) interfészekkel ellátott változatokban érhetők el.** Amennyiben a forensic-szakértő ilyen módon csatlakoztatja a számítógépéhez az adattárolót, biztos lehet benne, hogy azon egy bit sem változik meg. Ugyancsak hasznos eszköznek számítanak az úgynevezett duplikátorok, amelyek többnyire merevlemezek tükörmentésére, pillanatképek készítésére és hash-ek kalkulálására alkalmasak. Ezek az eszközök írásvédettséget is biztosítanak a forráslemezt illetően. A forensic hardverek között találhatunk még jelszó-visszafejtést felgyorsító megoldásokat, és számos olyan eszközt, amelyek lehetővé teszik a mobiltelefonok vizsgálatát. A magyar szakértők körében leggyakrabban Tableau márkájú készülékek bukkannak fel. (A Tableau-t májusban felvásárolta a Guidance Software vállalat.)

A számítógépek, adattárolók vizsgálatához természetesen szoftverekre is szükség van. A forensic-szakértők számára kereskedelmi forgalomban elérhető és nyílt forráskódú megoldások is a rendelkezésre állnak. Hazánkban az egyik legnépszerűbb szoftver az AccessData Forensic Toolkit (FTK), amely többek között az adathordozókról való pillanatkép-készítésben és azok mélyrehatóbb elemzésében, a memória dumpok analizálásában, a titkosítások visszafejtésében, valamint a dokumentumokban és elektronikus levelezésben történő bizonyítékkeresésben is komoly segítséget nyújt. Nem utolsósorban pedig a jelentések összeállítását is felgyorsítja.

A kereskedelmi forgalomban kapható alkalmazások mellett természetesen a forensic területéről sem hiányoznak a nyílt forráskódú szoftverek, amelyek egyes esetekben a hardveres megoldásokat is képesek kiváltani. Az úgynevezett forensic live CD-k vagy DVD-k (Helix, DEFT, Raptor stb.) Linux-alapon igyekeznek megkönnyíteni a vizsgálatokat, a pillanatképek készítését, valamint azok elemzését. Ezek a rendszerek tartalmazzák azokat a nyílt forráskódú, igencsak hasznos szoftvereket is, amelyek szintén analizálási célokat szolgálnak. Noha Windowszal kompatibilis, ingyenes forensic-eszközökből kevesebb érhető el, mint a Linuxhoz, azért e téren is akad néhány hasznos példány. A leggyakrabban alkalmazott program az FTK Imager, amely elsősorban a pillanatkép-készítést és megnyitást támogatja.

Itt kell megemlíteni, hogy a **hardveres és szoftveres eszközök mellett egy forensic-szakértő számára rendkívül fontos a lehető legmélyebb szintű szakirodalom és a különféle dokumentációk ismerete, ugyanis e nélkül megalapozott megállapítások az esetek zömében nem tehetők.**

TITKOSÍTÁSI ÉS FELHŐALAPÚ PROBLÉMÁK

Számos olyan informatikai megoldás létezik, amely a számítógépes bűncselekmények felgöngyölítését, illetve a bizonyítékok gyűjtését nehezíti vagy adott esetben lehetetlenné teszi. Ezek közül a legérdekesebb a titkosítás, amely a mindennapi életben a biztonság megteremtésében nélkülözhetetlen szerepet játszik, azonban a forensic-vizsgálatokat hátrál-

tathatja. Természetesen tudják ezt a bűnözök is, így egyre gyakrabban vértezik fel számítógépeiket teljes lemeztitkosítással, vagy egyéb kódolási módszereket alkalmaznak annak érdekében, hogy a tevékenységükből származó fájlokat, nyomokat elérhetetlenné tegyék a hatóságok, illetve az igazságszolgáltatás számára. Ez a probléma világszerte jelentkezik, és ennek megfelelően a hatósági, illetve a bírói gyakorlat is eltérő. Vannak országok, ahol a titkosítások feloldásához szükséges jelszavakat „rámenősebben” igyekeznek beszerezni az illetékes szervek, míg máshol inkább a jogi alkuk stb. a jellemzők, legalábbis abban az esetben, ha a szakértőknek nem sikerül (vagy túlságosan hosszú ideig tartana) a titkosítások visszafejtése.

Forensic szempontból érdekes problémát vet fel az egyre többet emlegetett cloud computing is. Hiszen amíg a hagyományos rendszerek esetében a rendőrség lefoglal egy számítógépet, és azt szakértőkkel elemezteti, addig a felhőalapú számítástechnika sajátossága miatt sok esetben azt sem lehet tudni, hogy az adatokat a világ melyik részén tárolták el. **Amíg viszont nincsenek meg az adatok, addig nincs is mit vizsgálni. Ezért a jövőben nagyon fontos lesz a hatóságok, az igazságszolgáltatás és a felhőalapú szolgáltatásokkal foglalkozó vállalatok közötti fokozottabb együttműködés kiépítése.** Ez biztos nem lesz zökkenőmentes, hiszen nemzetközi szintű problémáról beszélünk. Mindenesetre kedvező jelek már mutatkoznak arra, hogy megfelelő szabályozás esetén van esély a cloud computing megzabolázására is.

TANULJUNK COMPUTER FORENSICET!

Idén immár hazánkban is elindult az első computer forensic-képzés, amely márciusban zajlott le a Deloitte és a NetAcademia együttműködésében. Az EC-Council Computer Hacking Forensic Investigator (CHFI) tanfolyam keretében a hallgatók a számítógépek felhasználásával vagy a számítógépes rendszerek ellen elkövetett bűncselekmények felderítésébe nyerhettek betekintést. Ide tartoznak például az adatszivárgással kapcsolatos esetek, az internetes betörések, a hekkertámadások, a zsaroló üzenetek vagy az illegális CD-, DVD-másolatok készítésének vizsgálata.

A computer forensic hazai helyzetéről *Barta Csabát*, a Deloitte Infor-

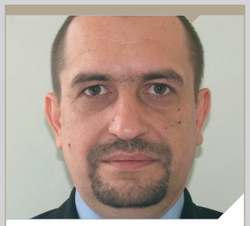
Mi a feladata?

„Az igazságügyi szakértő feladata, hogy a bíróság, az ügyészség, a rendőrség és a jogszabályban meghatározott más hatóság (továbbiakban együtt: hatóság) kirendelése, vagy megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel segítse a tényállás megállapítását, a szakkérdés eldöntését.” [Forrás: 2005. évi XLVII. törvény az igazságügyi szakértői tevékenységről 1.§ (1)]

Forensickel a hatékony adatfeldolgozásért

Komáromi László, az INFOLABOR Infokommunikációs Szakértői Iroda igazságügyi informatikai biztonsági szakértője a *Computerworld* számára adott interjújában a computer forensicről beszélt.

Computerworld: Milyen kihívásokkal, nehézségekkel kell szembenéznie egy computer forensic-szakértőnek Magyarországon?
Komáromi László: Technikai szempontból az adatmennyiség – háttértároló-kapacitás – növekedésének kezelését tartom általánosan megoldandó problémának. Ez a tendencia a vizsgálati eljárások erőforrásigényét jelentősen növelő tényező. A megnövekedett adatmennyiség az olcsón elérhető, nagy tárolókapacitású háttértárak általános elterjedése kapcsán jelent kezelendő feladatot a hiteles másolatkészítésnél, a tárolt élő és törölt adattartalom feldolgozásánál, elemzésénél, a releváns információk kiszűrésénél és prezentálásánál. Ma már elképzelhetetlen forensic-céleszközök nélkül a minőségi és hatékony adatfeldolgozás. Speciális másolóberendezések szükségesek a bizonyítékként szolgáló háttértárak adatainak gyors és hiteles klónozásához. Visszaírást megakadályozó ún. írásvédő eszközökkel biztosítjuk az eredeti bizonyítékok sértetlenségét. Adatbázisokra épülő elemző alkalmazások segítségével nyerjük ki az adathalmazból azokat az információkat, amelyek a későbbi felhasználás során bizonyítékként szolgálnak egy hatósági eljárásban. Ezek a vizsgálatot támogató eszközök nemzetközi szinten teljesen elfogadottak, hatékonyságuk és hitelességük bizonyított. Alkalmazásuk – főként tőlünk nyugatabbra – mind a hatósági, mind a szakértői érában mindennapos. Nálunk azonban a kiszolgáló technológia beszerzése, szinten tartása és fejlesztése mind technikai, mind monetáris alapon is elég nagy kihívást jelent.



Komáromi László
igazságügyi informatikai biztonsági szakértő, INFOLABOR

CW: A munkája során mi volt a legérdekesebb esete?
K.L.: A legizgalmasabbak általában az adattartalom-rekonstrukciók. A törölt adattartalomban való „elmerülés” sokszor a gyöngyhalászathoz hasonlítható. Az adatok helyreállítására épülő információszerzés kétes kimenetelű. Azonban ha eredménnyel jár, az kárpótlást jelent a befektetett energiáért. Számomra a legtanulságosabb egy többször is újratelepített számítógép „életútjának” rekonstruálása volt. A törölt adattartalom elemzése során kinyerhetők voltak a korábbi operációs rendszerben kialakított felhasználói fiókok, az azokhoz tartozó dokumentumok, levelezés, chatelés. Megállapítható volt, hogy mettől meddig „porosodott” a gép használaton kívül, és a gazdája mikor telepítette újra – próbálván elfedni korábbi tevékenységének nyomait.

CW: Mekkora veszélyt rejt a magyar számítógépes bűnözés, és milyen fokú az ilyen bűncselekmények elkövetőinek felkészültsége?
K.L.: Tapasztalatom alapján ma még a szakértői munka jelentős részét nem a „számítógépes bűnözők” produktuma szolgáltatja. Inkább jellemző az infokommunikációs eszközökkel és lehetőségekkel támogatott tradicionális bűncselekmények eszközhasználatának vizsgálata. A leggyakoribb feladat a bűncselekmények elkövetését alátámasztó kommunikációban rejlő információk kinyerése.

CW: A magyar jogszabályok mennyire képesek lépést tartani az informatika, illetve a computer forensic fejlődésével? Milyen változtatásokat látna szívesen a jogi szabályozás terén?
K.L.: A magyar jogszabályok a nemzetközi egyezmények (pl. Cybercrime), a jogharmonizáció, illetve az ebből fakadó büntetőjogi változások hatására általánosságban megállják helyüket az infokommunikációhoz kapcsolódó területeken. Áttörő változást jelentene azonban a nyomozati munkában a hatóságok számára, ha lehetőségük adódna a bizonyítékok közvetlen rögzítésére, előzetes adattartalom analízisére. Tehát, hogy egy háttértároló klón elkészítése, egy mobilkészülék adattartalmának letöltése a hatóság kiképzett technikusa és hitelesített eszközök segítségével önállóan – szakértők bevonása nélkül – akár a bűntett helyszínén legyen megvalósítható. Szerintem ez – hasonlóan az ujjnyomat rögzítéséhez vagy fénymásolat készítéséhez – alapvetően technikai jellegű feladat. A legtöbb esetben ilyenkor nincs eldöntendő vagy megválaszolandó kérdés a szakértő részére. A lehetőség mind a bűnügyi, mind az eljárás alá vont érdekeit is szolgálná, hiszen csak a hiteles másolat elkészítéséig lenne szükség az eredeti eszközre, így a tulajdonosi érdekek sérülése minimalizálhatóvá válna.

matikai Biztonság és Adatvédelem üzletágának vezető IT-biztonsági tanácsadóját, a NetAcademia CHFI-oktatóját kérdeztük. A szakember elmondta: a legnagyobb nehézséget az jelenti, hogy a vállalatok, amelyek valamilyen incidens kapcsán forensic-szakértőt bíznak meg, már azelőtt tesznek bizonyos lépéseket a probléma felgöngyölítése érdekében, mielőtt a szakértő a helyszínre érkezik. Ezek a lépések legtöbbször nem a kívánt hatást érik el, hanem adott esetben akár a bizonyítékok hitelességét is veszélyeztethetik. Ez általában abból fakad, hogy mielőtt külső szakértőt fogadnának, megpróbálják az incidenst „házon belüli” erőforrások segítségével megoldani. A szakma másik jelentős problémája a megfelelő oktatás hiánya. Nagyon kevés a színvonalas tanfolyam vagy vizsga, amit egy leendő szakértő elvégezhet. **Sajnos sok esetben elavult ismereteket oktatnak, amelyeket nem vagy csak részben tudnak alkalmazni. Természetesen mindenkinek lehetősége van az internet segítségével tudásának bővítésére,** azonban a jól rendszerezett ismeretanyag és annak megfelelő átadása jóval hatékonyabb lehet.

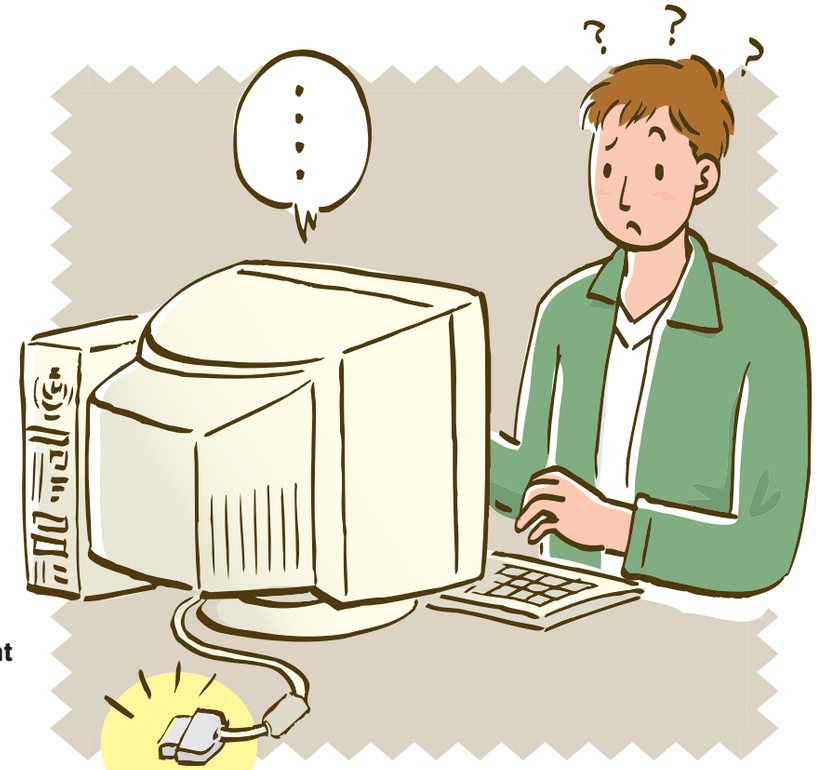
– Magyarországon alacsonynak mondható a magas felkészültséggel rendelkező számítógépes bűnözők száma. A komolynak nevezhető bűncselekményeket általában nem is az ország határain belül élők követik el. Ennek oka igen egyszerű: így egy fokkal megnehezíthető a nyomozók dolga, hiszen a határokon átnyúló bűncselekmények felderítése nemzetközi törvények figyelembevételével, illetve az érintett országok nyomozószerveinek együttműködésével lehetséges csak. Ez az együttműködés nem minden esetben megy zökkenőmentesen, illetve a törvények, jogszabályok is eltérhetnek egymástól, ami esetenként megnehezíti a nyomozást – vélekedett a szakember.

Barta Csaba néhány tanáccsal is szolgált a bűncselekmények megelőzése, illetve azok minél hatékonyabb felderíthetősége érdekében. Szerinte a megelőzés sok esetben nemcsak a kiépített informatikai rendszer védelmét kell, hogy jelentse, hanem az alkalmazottak megfelelő felkészültségét is. A számítógépes bűncselekmények nem magát a rendszert veszik célba, hanem a felhasználót. Lehet az információt védő rendszer bármilyen modern, illetve erős, ha az azt üzemeltető vagy használó ember nem felkészült egy őt érő esetleges támadással szemben. Természetesen a megfelelő naplózás is elengedhetetlen, hiszen az ésszerűen beállított naplózó rendszer által gyűjtött, megfelelően tárolt naplóinformációk akár perdöntő bizonyítékként is szolgálhatnak. A naplóbejegyzéseket célszerű központi helyen (naplógyűjtőn) tárolni, és ha lehetséges, digitális aláírással ellátni. Ez biztosítja, hogy az igazságszolgáltatás számára bizonyítékként elfogadhatók legyenek.

– A bűncselekmények felgöngyölítésével kapcsolatban legfontosabb talán, hogy egy minimális képzés keretében az alkalmazottak megismerjék az alapvető incidensreagálási lépéseket, illetve a bizonyítékkezeléssel kapcsolatos szabályokat. Ezeket egy külön erre a célra készített incidensreagálási politika tartalmazza; azonban a reagálásban részt vevő személyek nem mindig vannak tisztában ennek tartalmával, illetve betartásának jelentőségével – tette hozzá Barta Csaba.

***

Egy computer forensic-szakértő sokszor teljesen más szemszögből vizsgálja a számítógépeket, a szoftvereket, a dokumentumokat, az adatbázisokat, mint ahogy azt egy informatikus, fejlesztő vagy egy adatbázis-adminisztrátor teszi. Ez a szemléletbeli különbség teszi igazán érdekessé a szakértői tevékenységet, melynek során felelősségteljes, rendkívül körültekintő és szakszerű munkavégzésre van szükség.



Képzetlenül a PC előtt

Miközben a hazai vállalatok informatikai osztályain dolgozók felkészültsége többnyire megfelel a nemzetközi normáknak, a nem kifejezetten IT-területen dolgozók számítógépes hozzáértése sok vállalatnál a mai napig komoly hiányosságokat mutat. Számukra ugyan számtalan tanfolyami képzési lehetőséget kínál a piac, a tanfolyamok mégis nehezen eladhatók. Írta: Szalay Dániel

Alapvetően rendben lévőnek találja az IT-osztályok, a programozók, rendszergazdák felkészültségét *Fóti Marcell*, a NetAcademia Oktatóközpont ügyvezetője, akinek vezető oktatóként igen közeli rálátása van a területre. Szerinte alapvetően a „kis cég, kis odafigyelés – nagy cég, nagy odafigyelés" elve érvényesül, vagyis minél nagyobb egy vállalat, annál több erőforrást fordítanak az IT-guruk továbbképzésére. – Ami azonban a nem informatikus felhasználókat illeti – teszi hozzá – közel sem ilyen pozitív az összkép: a vállalatok többségénél a felhasználók képzése még mindig megmarad a jó öreg Word-Excel-PowerPoint tengelyen. Illetve rosszabb esetben még e téren is hiányosságok mutatkoznak.

– A legnagyobb probléma az – mondja Fóti –, hogy **a számítógépüket nap mint nap használó, sokszor akár kritikus üzleti információkkal dolgozó munkatársak biztonsági értelemben teljesen érintetlennek számítanak.** Csak egyetlen példa a száz közül: egy átlagos dolgozónak fogalma sincs arról, mi a különbség a belső és a külső hálózat között, így bátran beállítja céges jelszavát publikus weboldalakon is. Ugyanazt a jelszót küldi ki nyílt, olvasható formában az internetre, amit a belső, vállalati hálózaton a rendszergazdák gondosan titkosítva kezelnek. – De ilyen felhasználás mellett minek egyáltalán titkosítani? – teszi fel a kérdést a szakember. Fóti szerint az előbbieket támasztja alá az is, hogy bár az IT-biztonsági képzéseikre jelentős kereslet mutatkozik, a felhasználók biztonsági képzése „egyelőre eladhatatlan". Az oktatóközpont vezetője szerint ez abból is fakad, hogy más büdzséből kerül ki és más döntéshozók hatáskörébe tartozik az informatikusok és a felhasználók képzése. Előbbiről elsősorban az informatikai vezető, a CIO dönt, míg utóbbiról például a HR-igazgató vagy az ügyvezető. Fóti ezzel kapcsolatban megjegyzi: „Ez utóbbi körben nem ártana valakinek komoly felvilágosító tevékenységet végeznie."

Fóti Marcell

ügyvezető
NetAcademia Oktatóközpont

Egyébként Fóti Marcell tapasztalataival nagyon hasonló eredményeket hozott a Business Solutions Report, a BellResearch idén elkészült elemzése is, amelynek adatfelvételét 2009 őszén végezték el 760, tíz vagy annál több főt alkalmazó hazai vállalatnál. E szerint **a legalább 10 főt foglalkoztató hazai vállalatok kétharmada, 22-23 ezer cég tart képzéseket munkavállalói számára**, és a nagyvállalatok ebből a szempontból aktívabbak: körükben 88 százalékos a munkahelyi képzést szervezők aránya, míg ugyanez az arány körülbelül 10 százalékponttal alacsonyabb a középvállalatok körében, a kisvállalatok esetében pedig 63 százalék. A szervezett képzést folytató vállalatoknak összességében bő egyharmada (35 százalék) oktatja dolgozóit szoftverek használatával kapcsolatban, ami nagyjából megegyezik az általános iparági ismeretekre, illet-

GKIeNet munkaerő-piaci kutatás

A vállalati dolgozók felkészültségét vizsgáló legutóbbi, 2008-as GKIeNet munkaerő-piaci kutatás szerint a 10 vagy annál több embert foglalkoztató cégek alig negyedénél beszélhetünk magas vagy kiemelkedő informatikai intenzitásról, ami azt jelenti, hogy az ilyen cégek száma nem éri el a 8 ezret. A GKIeNet felmérése megállapította, hogy a vállalatok 2007-ben átlagosan 300 ezer forintot fordítottak alkalmazottaik továbbképzésére, ami országos szinten 10,2 milliárd forintot tett ki. A kutatás elkészítésekor a vállalatok kevesebb mint negyede (23 százalék) foglalkoztatott informatikust. Kiderült, hogy a 10 fő feletti cégeknél a számítógépet használó dolgozók 70 százalékának semmilyen informatikai jellegű képesítése nincs. Még sötétebb a kép, ha figyelembe vesszük, hogy a képesítettek több mint fele „csak" ECDL-vizsgával vagy egyéb képesítéssel rendelkezik. Ez összefügghet azzal is, hogy a számítógéppel dolgozó beosztott pozícióknál a vállalatok négyötöde nem támasztott elvárást a jelöltekkel szemben. 4 százalékuk vár el ECDL-vizsgát, 10 százalékuk OKJ-s képesítést, 9 százalékuk pedig informatikai szakközépiskolai végzettséget, míg a fejlesztői állásoknál már az egyetemi végzettség dominál az elvárások között. A vállalatok általános véleménye, hogy a különböző típusú informatikai képzésben részt vevők nem kapnak megfelelő minőségű képzést, valamint nem minden esetben a szoftverek aktuális változatának használatát tanulják. A cégek egyértelműen a főiskolai, egyetemi képzéssel vannak leginkább megelégedve, ugyanakkor még messze nem tartják megfelelőnek a felsőfokú informatikai képzések minőségét. Egyébként a legjobb egyetemnek a BME-t nevezték meg.

ve a cég termékeire-szolgáltatásaira vonatkozó oktatás elterjedtségével. Amíg azonban az utóbbi területeken az egyes vállalati szegmensek gyakorlata hasonló, az informatikai oktatás területén jelentősek a különbségek: a nagyvállalatoknál 61 százalékos az arány, a középvállalatok fele, a kisvállalatoknak pedig alig 30 százaléka képzi munkavállalóit az informatikai alkalmazások használatára.

HOZZÁ NEM ÉRTÉSBŐL ADÓDÓ KÁROK

Mekkora károkat okozhat egy-egy hozzá nem értő user által elvégzett számítógépes művelet? Fóti szerint a kár mértéke nem a tudáshiány mértékétől függ: „Ha valaki tudatlansága folytán beenged egy crackert, onnantól a károkozás mértéke csakis a támadó hozzáállásán múlik." Szerinte azért is lenne fontos odafigyelni a megfelelő képzettségre, mert „nincs kisember és nagyember", vagyis ugyanolyan „nehéz" a portás számítógépéről és felhasználói szintjéről domain adminisztrátorrá válni egy crackernek, mint amilyen „nehézséget" egy vezérigazgatói hozzáférés megszerzése jelentene. „Ha egy támadónak bármilyen szintű hozzáférése van, az emelt szintű jogosultság megszerzése rutinfeladat, ezért félmegoldásokra, féloktatásokra semmi értelme pénzt kidobni" – figyelmeztet Fóti Marcell, aki szerint ideje kimondani: logikátlan, hogy csak a kiemelt „nagyvadak" (vezetői szintek) részesüljenek biztonsági oktatásban, mert ettől még a gyenge láncszemek megmaradnak a hálózatban. „Igaz, megtakarítottuk pár száz dolgozó oktatását, de kidobtunk egy csomó pénzt feleslegesen egy szűk kör oktatására"– mondja. Az oktató szerint súlyos gond, hogy mégis ez a bevett gyakorlat.

AZ OKTATÁSRA FORDÍTOTT ERŐFORRÁS

Egyébként a minimális képzési elvárás a biztonsági ismeretek karbantartása lenne, méghozzá valamennyi dolgozó számára – vélekedik Fóti Marcell. Ez szerinte 2-3 munkanap alatt teljes körűen elvégezhető. Ezenfelül szükség lesz az új szoftvermegoldások használatának elsajátítására, ami további 2-3 napot vehet igénybe, de már csak azoknak a dolgozóknak, akiket ez a munkája miatt érint. Az IT-részleg képzése pedig ennél is több időt vesz igénybe, hiszen számukra mérnöki szintű magas fokú tudást kell átadni, amelynek időigénye 5 nap. Ugyanakkor az időráfordítás és a költségek ellenére azt mondhatjuk, hogy a dolgozók képzése még mindig kevesebbe kerül, mint a tudatlanság miatt előidézett károk, adatkiszivárgások. Ideális esetben dolgozónként az éves képzés néhány tízezer forintba kerül, és csak az informatikusok oktatása „húzósabb" – ez dolgozónként néhány százezer forintos tételt jelent. **A továbbképzéseket egyébként akár a szakképzési hozzájárulás terhére is igénybe lehet venni, és az informatikusok oktatásának finanszírozásába sokszor a nagy gyártók is beszállnak**, ahogy például a Microsoft is teszi oktatási kuponok, úgynevezett SA voucherek formájában.

ROSSZ KIFOGÁS A LÉTSZÁMHIÁNY

A cégek részéről – ahonnan ritkábban vagy akár soha nem küldik továbbképzésre a dolgozókat – gyakran hangoztatott érv a tanfolyamok ellen, hogy azok sok időt vesznek igénybe, és ezalatt nélkülözniük kell az érintettek munkáját. A válság persze ennek az indoknak a hangoztatásához még alapot is adott, hiszen a vállalatok nemcsak a tanfolyamokra költhető összegeken próbálnak takarékoskodni, de a dolgozói létszámon is. Vagyis ott, ahol a létszámleépítések miatt két ember látja el három munkáját, nemigen akad szabad munkanap oktatási célra. **Ugyanakkor ma már az oktatóközpontok is rugalmasabbak: készek akár a cég székházában vagy akár interneten keresztül, távoktatással képezni a „hallgatókat".** Ilyen esetben a dolgozóknak nem kell sehová eljárniuk, s ha időnként ki is esnek a képzés ritmusából, a teljes tanfolyam rendelkezésükre áll videón, vagyis mindent pótolni tudnak. Ezeket a tanfolyamokat akár munkaidő utánra is megszervezik. Fóti Marcell ezzel kapcsolatban azt mondja: az online tanfolyamok esetében általában ki is derül, hogy valójában megvannak az oktatásra szánható összegek, csak éppen hagyományos, nappali tantermi oktatásra egyre nehezebb elkérni ezeket.

e-Learning

Az e-learning az üzleti döntéshozók jelentős része számára ma már egyre kevésbé tűnik „titokzatos" dolognak – ezt a Bell Research adatai is alátámasztják. A minimum 10 fős vállalati körben négyből három vezető legalább fogalmi szinten tisztában van a fogalom jelentésével. A tisztánlátáshoz persze az is hozzátartozik, hogy az e-learning pontos mibenléte – a részletek – ennél azért kisebb hányaduknak, mindössze 46 százalékuknak világos. A nagyobb cégeknél – vélhetően az eredendően magasabb szintű kompetenciák miatt – a többség számára ismert e terület.
Az előbbiek tükrében a gyakorlat mindenképpen jelentős kontrasztot mutat: a BellResearch adatai szerint a legalább 10 fős hazai cégek mindössze 7 százaléka alkalmazza ténylegesen az e-learninget. A nagyvállalatok láthatóan előrébb járnak ezen a téren, körükben több mint kétszeres az arány. Jelenleg mintegy 2500 hazai 10+ fős cég él az e-learning adta előnyökkel. A hazai gyakorlat nem nyúlik vissza hosszú időre, a cégek többsége még csak néhány éve alkalmazza. Az e-learning témáit tekintve a szoftverek használatához kapcsolódó IT-oktatás népszerűnek számít, az érintett vállalatok fele ezen a területen is alkalmazza ezt a módszert. A BellResearch kutatási eredményei szerint az e-learning legfontosabb drivereit a vállalatok számára a rugalmasság, az információk elektronikus elérhetősége, a költséghatékonyság és a munkavállalói produktivitás növelése jelenti. Ugyanakkor a cégek négyötödénél mutatható ki valamilyen konkrét indok arra vonatkozóan, hogy miért nem alkalmazzák egyáltalán vagy nagyobb arányban az e-learninget. A leggyakoribb elutasítási indoknak – minden harmadik cégnél – a munkatársi igények [vélt] hiánya számít. Ezek a döntéshozók úgy gondolják, hogy a munkatársak számára valójában nem jelentene értéket, vagy csak marginális hasznot hozna az online oktatás, továbbképzés. Egyébként a nemzetközi tapasztalatok azt mutatják, hogy jóval nagyobb arányban igénylenék a munkatársak az e-learninget, mint azt a vállalatvezetők feltételezik.
A vállalati döntéshozók részéről magával a megoldással kapcsolatos szkepszis érződik akkor is, amikor arra hivatkoznak, hogy a tudás ilyen módon nem adható át, vagy nem hatékony, illetve drága. Fontos azonban, hogy e vélekedések többsége alapvetően csak percepció, jellemzően hiányoznak az alátámasztó tárgyi elemek, hatásvizsgálatok, tanulmányok, elemzések.

Energiadilemma az adatközpontban

Az International Energy Agency szerint 2008-ban a világ energiafogyasztásának 4 százaléka IT-vonatkozású volt, azonban az energiaigény évi 15 százalékos növekedése mellett ez az arány 2030-ra 40 százalékra nőhet. Ennek mérséklésére a jelenleg elérhető technológiákkal is van lehetőség – az energiahatékonyság javításával. Ezt – amint az az első példák láttán valószínűsíthető – törvények is előírhatják már a közeli jövőben. Írta: Kis Endre

A Schneider Electric több mint száz országban kínál integrált energiamenedzsment megoldásokat az energia és infrastruktúra, az ipari folyamatok, az épületautomatizálás, az adatközpontok és -hálózatok területén, valamint a lakossági piacon. A több mint 100 ezer főt foglalkoztató, közel 16 milliárd euró éves árbevételű cég saját becslése alapján, ügyfelei jegyzik a világ villamosenergia-fogyasztásának 72 százalékát.

Ezek a szervezetek és magánszemélyek – a Schneider Electric szerint – a fejlett energiafelügyeleti megoldásokkal átlagosan 30 százalékos megtakarítást érhetnek el az energiafogyasztás terén.

EGY AVATAR KARBONLÁBNYOMA

Az utóbbi években minden képzeletet felülmúló információrobbanásnak lehettünk tanúi. **Egyedül 2006-ban 3 milliószor több információt rögzítettünk, mint amennyit a könyvnyomtatás kezdetétől számítva összesen kinyomtattak, és ez az információmennyiség idén megkilencszereződik. Ezzel arányosan növekszik a hálózati sávszélesség iránti igény, miként az információt kezelő rendszerek, alkalmazások és eszközök üzemeltetéséhez szükséges energiafogyasztás is.** Az élet minden területére jellemző információközpontúságból fakadó igények kiszolgálására egyre nagyobb kapacitású adatközpontok épülnek. Az Egyesült Államok energiafogyasztásának 2 százalékát már jelenleg is ezek a létesítmények adják.

A felhasználók napi 3 milliárd percet töltenek a Facebookon, naponta több mint 1 milliárd videót néznek meg a YouTube-on, és ugyanennyi képet tekintenek meg a Google weboldalán. A mobilinternet elterjedésével az ilyen számok egyre gyorsabb ütemben nőnek a lakosság és az üzleti felhasználók körében egyaránt. A napjainkban piacra kerülő mobileszközök funkcióinak zöme hálózati adatforgalmat feltételez.

A világhálóra csatlakozó felhasználók ugyanakkor nem gondolnak arra, hogy ez a foglalatosság mennyire energiaigényes. A weben töltött minden másodperc 20 milligramm szén-dioxid kibocsátásával jár. Tíz éven belül az üvegházhatást kiváltó gázok 20 százalékát az internethasználathoz szükséges energia előállítása fogja termelni. A Second Life virtuális világát benépesítő avatarok például – átlagos életciklust alapul véve – ma már akár több elektromos energiát is fogyaszthatnak, mint egy hús-vér ember.

Stefan Nordenfors
vezérigazgató
Schneider Electric Hungária Villamossági Zrt.

Az IT mellett más területeket is ideszámítva, a világ energiafelhasználása 1980 óta 45 százalékkal nőtt, ami azt jelenti, hogy a jelenlegi szinthez képest 2050-ben már 100 százalékkal több energiára lesz szüksége az emberiségnek.

A növekvő energiafogyasztás káros környezeti hatásainak mérséklése érdekében a nemzetközi közösség célul tűzte ki, hogy ez idő alatt felére csökkenti szén-dioxid-kibocsátását, és a továbbiakban az elektromos energia egyre nagyobb részét megújuló energiaforrások felhasználásával állítja elő. Országonként eltérő, hogy a helyi adottságok függvényében erre milyen lehetőség kínálkozik. Magyarország például a szélenergia és a föld hőenergiájának hasznosításától várja a legnagyobb eredményt. **Egyelőre azonban kétséges, hogy az ambiciózus célok és határidők mennyiben lesznek tarthatók. A megújuló energiaforrások jelenleg a világ áramtermelésének elenyésző hányadát adják.**

ENERGIAINTELLIGENCIA

Ezért fontos, hogy az energiafelhasználás hatékonyságán javítsunk; ezen a téren sokkal gyorsabban és olcsóbban érhető el előrelépés, mint az energiatermelés és -elosztás módjának megváltoztatásában. E mellett szól az a körülmény is, hogy a jelenlegi áramelosztó hálózatok nagy energiaveszteség mellett működnek. Ez azt jelenti, hogy a fogyasztói oldalon megtakarított minden 1 kilowatt áram után 3 kilowattal kevesebb elektromos energiát szükséges termelni.

– Vállalatunk a felhasznált energia mennyiségének csökkentésében és annak hatékonyabb hasznosításában látja a környezetvédelem jövőjét – fejtette ki *Stefan Nordenfors*, a Schneider Electric Hungária Villamossági Zrt. vezérigazgatója. – Véleményünk szerint ez az első és legfontosabb lépés a fenntartható fejlődés felé. Ezért olyan eszközöket és megoldásokat kínálunk, amelyek segítségével a végfelhasználók hosszú távon is fenntartható hatékonyságot érhetnek el az energiafelhasználás terén.

Az IT-vel összefüggő energiaköltségeken elérhető megtakarítást azonban nehezíti, hogy a vállalatok általában nem tudják pontosan kimutatni, IT-eszközeik mennyit fogyasztanak. Ez az energiaköltség becslések szerint a vállalat bevételének 6–20 százalékát is elérheti 2020-ra. Mivel a villanyszámla alapján nem derül ki az IT-re eső fogyasztás mértéke, az energiahatékonyság érdemi javításához több és részletesebb információ szükséges.

– Ezért kidolgoztunk egy általános, az IT mellett más területeken is alkalmazható modellt, amely négy lépésben segíti a fogyasztót a hatékonyabb energiafelhasználáshoz – mondta Stefan Nordenfors. – Mindenekelőtt **részletesen mérjük a fogyasztást, hogy pontosan kiderüljön, hol menynyi elektromos energiát használunk, és miért. Ennek alapján a második lépésben a nagy fogyasztású eszközöket energiahatékony változatokra cseréljük.** Ezt a két szakaszt a passzív energiahatékonyság területeként határoztuk meg, mert ha egy alacsony fogyasztású eszközt akkor is használunk, amikor ez valójában nem szükséges, még mindig energiát pazarolunk. A következő két lépés az aktív energiahatékonyság területére vezet. Kö-

zülük az első az automatizálás – a világítás, a fűtés, a légkondicionálás és a különböző eszközök automatikus lekapcsolása a szenzorok által továbbított információk alapján. Ezek az adatok a meghibásodások gyors észlelését és javítását is segítik. A negyedik lépés az energiafogyasztással kapcsolatos információk elemzésén keresztül biztosítja az elért energiahatékonyság hosszú távú fenntarthatóságát és további javítását.

A Schneider Electric a hozzá tartozó APC-vel együtt olyan menedzsment megoldást szállít, amellyel az adatközpontokban is részletekbe menő módon monitorozható, elemezhető és optimalizálható a hatékonyság az IT-eszközök, a hűtés és az egész létesítmény energiafogyasztása terén.

– A Schneider Electric Power Logic EEM (energy management information system, EMIS) és az APC InfraStruXure Central funkcióit ötvöző megoldás, amely a más szállítóktól származó felügyeleti eszközökből érkező adatokat is integrálja, holisztikus képet ad az adatközpont energiafogyasztásáról és -hatékonyságáról – emelte ki *Szarka Attila*, a Schneider Electric IT Hungary Kft. vezető rendszermérnöke. – Többek között valós idejű adatokat mutat be a folyamatok mentén, támogatja a költségelszámolást és -tervezést, virtualizációs környezetre is optimalizálva segíti az elemzést és a riportolást. Az adatközpont élő modellje is felépíthető ezzel a megoldással, amelyen minden tervezett változtatás és bővítés hatása szimulálható és ellenőrizhető az energiafogyasztás szempontjából. A kaliforniai Raging Wire sacramentói adatközpontja például – amely az egyik legnagyobb a San Franciscó-i öböl térségében –, évi 1 millió kWh áramot takarít meg pusztán a meglévő infrastruktúra jobb felügyelete által. A vállalat ezt úgy érte el, hogy minden rackszekrénybe szenzorokat telepített, majd a mért hőmérsékletértékek alapján optimalizálta a vízhűtést és a légkondicionálást.

A Schneider Electric szerint az ilyen információgyűjtés és -elemzés kulcsfontosságú az energiahatékonyság javítása szempontjából, és az automatizálással együtt a fejlődés fő irányát mutatja az energiafogyasztás felügyelete területén. Ha tetszik, az energiaintelligencia megoldások megjelenéséről beszélhetünk.

ZÖLD PÉLDÁK

Az Európai Bizottság kutatóközpontjának energetikai intézete 2008 végén ajánlást készített az adatközpontok kialakítására és üzemeltetésére nézve *(Code of Conduct on Data Centers)*, amelyet számos szállító és felhasználó támogat. Aki ezt aláírásával önként vállalja, annak az energiahatékonyság terén bevált gyakorlatot kell alkalmaznia, eleget kell tennie a legjobb TCO-val bíró eszközök beszerzésére érvényes követelményeknek és évente jelentést készítenie energiafogyasztásáról.

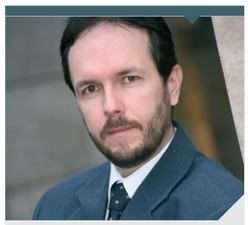
> A felhasználók napi 3 milliárd percet töltenek a Facebookon, és több mint 1 milliárd videót néznek meg a YouTube-on...

Az Egyesült Királyság azonban, ahol az adatközpontokra az összes áramfogyasztás 3 százaléka esik, már törvényi erejű szabályozást is bevezetett ezen a téren annak érdekében, hogy vállalása szerint 2050-re 80 százalékkal csökkenthesse az üvegházhatást kiváltó gázok kibocsátását. Várható, hogy a jövőben más európai országok is követik majd ezt a példát.

– Magyarországon többek között a régió legnagyobb adatközpontját működtető Dataplex használja az APC szünetmentes áramforrásait az energiahatékony üzemeltetés megoldására – mondta Szarka Attila. – A frankfurti repülőtér Schneider Electric eszközökkel optimalizálja a hűtést adatközpontjában, ahol Európa egyik legnagyobb hőszigete található. A Ferrari és a Renault Forma–1-es csapata szintén az APC megoldásával biztosítja nagy számítási kapacitású szerverparkjának áramellátását.

Az adatközpontok energiafelügyelete területén a Schneider Electric olyan partnerekkel is együttműködik, mint az IBM. Az egyesült államokbeli Bryant University az IBM Scalable Modular Data Center megoldásával konszolidálta és virtualizálta szerverparkját, amely addig három különböző helyszínen működött. Ennek az IBM BladeCenter platformra épülő megoldásnak az APC InfraStruXure architektúra és az ún. célzott hűtést biztosító InRow-technológia is integráns része. Segítségével az egyetem 75-ről 40-re csökkentette a szerverek számát, ami 40-50 százalékkal kisebb helyigényt és becslés szerint 30 százalékkal nagyobb energiahatékonyságot eredményezett.

Az adatközpontok energiahatékonyságának mérésére a Green Grid szövetség, amelyben a Schneider Electric elnökségi tag, kidolgozta a PUE (power usage efficiency) mérőszámot. Ez azt mutatja, hogy a létesítmény egészének energiafogyasztása miként viszonyul az IT-eszközök energiafogyasztásához (a számítási kapacitástól függetlenül).



Szarka Attila
vezető rendszermérnök
Schneider Electric
IT Hungary Kft.

– Az ideális PUE 1,0, az Egyesült Államokban az átlag 2,5, Európában 2,2 körül alakul – tette hozzá Szarka Attila. – A Budapest Bank adatközpontja, ahová hűtési megoldást szállítottunk, ehhez képest várhatóan kiemelkedő, 1,4 PUE energiahatékonysággal fog működni.

Itt érdemes megemlíteni, hogy a Schneider Electric látta el épületautomatizálási és -felügyeleti termékekkel a koppenhágai Bella Centert is, amely otthont adott az ENSZ tavalyi klímakonferenciájának. A projekt során a 122 ezer négyzetméter alapterületű épületben a világítást, a szellőztetést, a légkondicionáló rendszert, a keringetőpumpákat, valamint a biztonsági és beléptető rendszereket cserélték a Schneider Electric megoldásaira. **Az új világítástechnikának köszönhetően az épület 300 ezer kWh-val kevesebb energiát használ, a keringetőpumpák pedig 30–50 százalékos költségmegtakarítást tesznek lehetővé. Az épület üzemeltetője összességében évi 268 ezer eurót takarít meg,** így a beruházás kevesebb mint 8 év alatt megtérül. Az átalakítás eredményeként a központ 2009 decemberéig 1150 tonnával kevesebb szén-dioxidot termelt.

Figyelmet érdemel az Antarktiszon 2008 óta működő Princess Elisabeth kutatóállomás is, amelynek áramelosztó és energiafelügyeleti, valamint automatizálási megoldásait a Schneider Electric szállította. A kutatóállomás évi 54 MWh energiaigényét teljes egészében megújuló energiaforrásokból, napelemek és szélerőművek segítségével biztosítja – így az energetikai szempontból önellátó, a természeti környezetet nem terhelő létesítmények lehetséges jövőbeni elterjedését vetíti előre.

Energiaakadémia

Energiahatékonyságot javító megoldásait a Schneider Electric saját gyáraiban is alkalmazza világszerte. – A 2004–2008-as időszakra célul tűztük ki, hogy gyárainkban az egy főre jutó energiafelhasználást 10 százalékkal csökkentjük az azt megelőző szinthez képest – mondta *Stefan Nordenfors*. – Ezt sikerült túlteljesítenünk, és hogy megmutassuk az energiamegtakarításban rejlő lehetőségeket, 2011-ig további 10 százalékkal kívánjuk csökkenteni fogyasztásunkat. A projekthez Magyarországon elsőként 2008-ban a Schneider Electric zalaegerszegi kismegszakítógyára, az MG Zala Kft. csatlakozott. Az átalakítás révén a gyár 2009 novembere és 2010 januárja között átlagosan 73 kWh-ról 39 kWh-ra, azaz csaknem a felére csökkentette a termeléshez kapcsolódó energiafelhasználást.
A téma iránt érdeklődők számára a Schneider Electric központi weboldalán elérhető Energy University számos tanfolyamot kínál. Ezeken egy regisztrációt követően bárki ingyenesen elmélyítheti ismereteit az energiafogyasztás felügyelete és az energiahatékonyság javítása terén.

ÖSSZEÁLLÍTOTTA: Kelemen Gábor

Csökkenő árak, növekvő verseny

Az Európai Unió 2007 júniusában alkotott először részletes szabályokat a hanghívások roamingdíjának leszorításáért. A cél az egységesebb távközlési piac kialakítása, a fogyasztóvédelem erősítése, valamint a verseny és az átláthatóság fokozása volt. A siker felemás.

A kezdeti célok csak részben valósultak meg. Egy az első roamingrendelet hatását vizsgáló jelentés szerint a verseny nem a kívánt mértékben erősödött, így az Európai Bizottság tavaly júniusban módosította a vonatkozó szabályokat, továbbá kiterjesztette az addig csak hanghívásra vonatkozó rendelkezéseket az SMS-küldésre és az adatroamingra is. A 2009 júniusában elfogadott, módosított barangolási szabályozás szerint 2009. július 1-jétől a fogyasztók által a barangolásos hanghívásokért fizetett maximális (áfa nélküli) díjak percenként 0,46-ról 0,43 euróra mérséklődtek, és ezek 2010. július 1-jétől tovább, percenként 0,39 euróra csökkennek. A szöveges üzenetek maximális díja 2009. július 1-től 0,11 euró lesz. A szolgáltatók által egymásnak kiszabott adatátviteli barangolási díjak 2010 júliusától feltöltött vagy letöltött megabájtonként 1 euróról 0,8 euróra csökkennek. *Neelie Kroes*, a bizottság digitális menetrendért felelős alelnöke hangsúlyozta: bár a barangolásról szóló első szabályozás elfogadása óta folyamatosan csökken az EU-n belüli külföldi mobiltelefon- vagy mobileszköz-használat díja, a nagyobb verseny jobb választási lehetőségeket és még kedvezőbb díjakat jelentene a fogyasztók számára.

Az idén július elején közzétett időközi bizottsági jelentés szerint az EU mobilszolgáltatói az uniós szabályok által meghatározott maximális percdíjaknak megfelelően csökkentették barangolási díjaikat, és az árak átláthatósága is javult. A barangolásos hívások díja 2005 óta több mint 70 százalékkal csökkent, a szöveges üzenetek EU-tagállamok közötti küldése 60 százalékkal kerül kevesebbe. A külföldön való internetezés nagykereskedelmi árai is jelentősen, több mint 50 százalékkal csökkentek, így az árak jóval az európai uniós maximum alatt vannak. Mindez azonban még nem mutatkozik meg teljes mértékben a kiskereskedelmi árakban. 2009 végén a szolgáltatók egymás felé megabájtonként átlagosan 0,55 eurós díjakat alkalmaztak. Az átlagos fogyasztói ár a 2009 elején mért megabájtonkénti 3,62 euróról 2009 végéig 2,66 euróra csökkent. A nagykereskedelmi és a végfelhasználói árak közötti különbség tetemes, így a bizottság azt várja a szolgáltatóktól, hogy a nagykereskedelmi szinten elért megtakarításokat adják tovább a fogyasztóknak.

A fogyasztók számára a díjak a fentiek ellenére sem csökkentek jelentősen az uniós szabályok által előírt szint alá. A kiskereskedelmi árak továbbra is az uniós szabályok által meghatározott maximális díjak közelében találhatók. A bizottság jelentése ezért arra a következtetésre jutott, hogy az EU-n belüli barangolásos hívások piaca még nem elég erős ahhoz, hogy jobb választási lehetőségeket és kedvezőbb tarifákat kínáljon a fogyasztók számára.

A bizottság elemzése továbbá arra is rámutat, hogy a szabályozásnak és az árak csökkenésének köszönhetően annak ellenére növekedett a roaminghasználat szerte az unióban, hogy az elmúlt két évben az utazások száma hozzávetőlegesen 12 százalékkal visszaesett. 2009 nyarán, az Európai Unió egészére kiterjedő 11 centes maximális SMS-díj bevezetését követően az előző év hasonló időszakához képest 20 százalékkal több szöveges üzenetet küldtek a felhasználók. Az adatátviteli barangolási szolgáltatások forgalma 2009-ben pedig 40 százalékkal nőtt.

A bizottság jövő nyáron vizsgálja felül teljes egészében a 2009. évi barangolási szabályokat. Megnézik, hogy sikerült-e elérni a jogszabályban foglalt célkitűzéseket, továbbá, hogy a barangolási szolgáltatások piaca az egységes digitális piaccal szembeni elvárásoknak megfelelően működik-e. (További részletek: computerworld.hu/cikk/roaming2010)

Rekordösszeg kutatás-fejlesztésre

Az Európai Bizottság csaknem 6,4 milliárd eurót kíván kutatási és innovációs célokra fordítani a 7. Kutatás-fejlesztési Keretprogram (FP7) keretében 2011-ben – jelentette be *Máire Geoghegan-Quinn* uniós biztos. Ez rekordösszeg a K+F területén. Az EU kb. 16 ezer kutatóintézetre, egyetemre és ipari szereplőre számít, köztük 3000 kkv-ra. A támogatások odaítélésére az elkövetkezendő 14 hónapban kerül sor. Az unió azt várja, hogy e csomag hatására több mint 165 ezer álláshely keletkezik.

Számos szakterületről lehet majd támogatásra pályázni a program keretében. Az egészség témakörére például több mint 600 millió eurót fordítanak. Az információs és kommunikációs technológiák kutatására további 1,2 milliárd euró áll rendelkezésre, ami lehetővé teszi, hogy a bizottság teljesítse az európai digitális menetrendben vállalt ígéretét az IKT támogatásának éves növelésére.

Az európai vállalkozások 99 százalékát kitevő kkv-k is kitüntetett figyelmet kapnak. Számukra csaknem 800 millió euró válik elérhetővé. Lesznek olyan kutatási területek – például az egészség, a tudásalapú biogazdaság, a nanotechnológia egyes témakörei –, ahol a kkv-k részvétele el kell, hogy érje az adott összköltségvetés 35 százalékát.

Az IKT költségvetésből hozzávetőleg 600 millió eurót az új generációs hálózati és szolgáltatási infrastruktúrákra, robotrendszerekre, elektronikus és fotonikus alkatrészekre, valamint digitális tartalmakhoz kapcsolódó technológiákra szánnak. Több mint 400 millió euró pályázható annak kutatására, hogy az IKT hogyan segítheti elő az alacsonyabb szén-dioxid-kibocsátású gazdaság megteremtését, valamint a lakosság elöregedése jelentette kihívás kezelését. A jövő internetjével foglalkozó magán-állami partnerség céljára 90 millió eurót különítenek el 2011-re.

A hetedik keretprogram 2011. évi pályázati költségvetése 12 százalékkal több a 2010. évinél (5,7 milliárd), és 30 százalékkal haladja meg a 2009-est (4,9 milliárd). A pályázati felhívások részben előkészítik az „Innovatív Unió” kezdeményezést is, amelyet 2010 őszén indít útjára az EU. (További információ: ec.europa.eu/research/fp7/index_en.cfm)

Aktuális

- Egy 6,2 millió eurós kutatási projektnek köszönhetően az európai polgároknak ezen a nyáron vasúti utazásaik során kevesebb forgalmi zavarral kell számolniuk. Az ARRIVAL projekt keretében olyan szoftvert fejlesztettek ki, amely hatékonyabban tervezi a vonatok menetrendjét, valamint valós időben, eredményesebben kezeli a forgalmi zavarokat. A projekt eredményeit Európa-szerte már most alkalmazzák egyes vasúttársaságok annak érdekében, hogy a vasúthálózat használata a menetrendkészítés és a váratlan forgalmi zavarok kezelését tekintve egyaránt hatékonyabb legyen.

- Az Európai Unió a 2011-es évre 1,2 milliárd euró értékben hirdetett meg kutatás-fejlesztési pályázatokat. A pályázatok témái között szerepel a „jövő internetje”, az energiahatékonyság javítása, valamint a gépjárművek tisztán elektromos árammal való meghajtása is.

- Egy uniós támogatással megvalósuló kutatási projekt, a Workpad olyan számítógépes alkalmazásokat fejlesztett ki, amelyek lehetővé teszik a természeti katasztrófákhoz kirendelt csapatok gyors és hatékony koordinációját és kommunikációját az életmentés érdekében. Az EU 1,85 millió euróval támogatta a projektet. A fő cél az volt, hogy megvizsgálják, hogyan lehet a különböző mentésre szakosodott szervezetek több tucat adatbázisát a tartalommegosztó technológia segítségével összekapcsolni. A módszert már sikeresen használták Dél-Olaszországban és ma már a világ bármely pontján elérhető.

Szoftverek magyarul

Fontos az angol nyelv ismerete, de természetesen a magyar felhasználó dolgozhasson magyar nyelvű szoftverekkel. Legyen szó akár a kereskedelmi forgalomban kapható termékekről, akár a szabad szoftverekről. Írta: Mallász Judit

Jogos, hogy a hazai végfelhasználó a magyar nyelvű szoftvereket részesíti előnyben. Magyar nyelvű felületen, ékezetes karakterekkel szeret dolgozni, a dátumot, a pénznemeket és egyéb jelöléseket az anyanyelvén megszokott formában akarja használni. Mindez ma már természetes is, hiszen a külföldről származó szoftverek döntő többségét a piaci bevezetés előtt honosítják.

JAPÁNBAN IS MAGYARUL

A szoftverek különböző nyelvi változatait vizsgálva mindenekelőtt fontos megkülönböztetni egymástól a *globalizációt* (vagy internacionalizációt) és a *lokalizációt* (vagy honosítást).

A szoftverek globalizációja azt jelenti, hogy bármilyen nyelvű szoftverrel dolgozik is a végfelhasználó, használhatja a saját anyanyelvét.

– A globalizáció a szoftver minden nyelvi változatára érvényes, alapját maga az operációs rendszer adja – tájékoztatott *Antunovics Mónika*, a Microsoft szakértője. Miről is van itt tulajdonképpen szó? Gondoljuk el, hogy egy japán egyetemre a világ minden tájáról érkeznek vendégoktatók. A helyi számítógépeken értelemszerűen japán Windows fut, ám mindenki szeretné a dokumentumokat és az e-maileket a saját anyanyelvén írni, a dátumokat, a pénznemeket a saját hazájában megszokott módon használni. Ez – a szoftverek globalizációjának köszönhetően – minden további nélkül megtehető, pusztán a területi beállításokat kell elvégezni (hol vagyok, mi az anyanyelvem).

Antunovics Mónika

szakértő
Microsoft

NINCS FORRÁSKÓDFORDÍTÁS

A szoftverhonosítás alapvetően két elemből tevődik össze: egyrészt a felhasználói felületet lefordítják az adott ország (vagy piac) nyelvére, másrészt pluszszolgáltatásokat építenek be a szoftverbe (például az adott országra jellemző háttérképeket). Általában a honosítás már a szoftverfejlesztés egy bizonyos szakaszában elkezdődik, majd azzal párhuzamosan folyik.

Honosításkor soha sincs forráskódfordítás. Ez meglehetősen szigorú követelményeket támaszt a fejlesztőkkel szemben: a honosíthatóság érdekében a forráskódba szöveget beírni szigorúan tilos, a képernyőn megjelenő minden felhasználói felületi erőforrást (párbeszédpaneleket, menüket, linksorokat, állapotsorokat, lefordítandó szövegeket stb.) külön fájlokban (resource DLL) kell gyűjteni.

> A szoftver üzeneteit, menüit félreérthetetlenül és minden nyelvre lefordíthatóan kell megfogalmazni...

A honosítás első lépéseként a honosító eszköz értelmezőmodulja (parser) kiolvassa a megadott fájlokból az erőforrások összes paraméterét, majd beteszi azokat egy adatbázisba. Gyakorlatilag egy olyan táblázat jön így létre, amelynek egyik oszlopa a forrásszöveget, másik oszlopa a célszöveg felhasználói felületének erőforrásképét mutatja. Ezt követően – a lokalizáció költségeinek csökkentése érdekében – a fordítómemória jut szerephez: megpróbálnak minden olyan elemet felhasználni, amelynek már létezik a fordítása. Az így előkészített adatbázist kapja meg a fordító.

Mivel a szoftverfejlesztés és a -honosítás párhuzamosan folyik, a fordítási adatbázist időnként frissíteni kell. A honosító eszköz automatikusan megjelöli a különbségeket, így a fordítást végző szakembernek csak a változásokkal kell foglalkoznia.

A Microsoft belső fejlesztésű honosító eszközökkel dolgozik. Ezek gyakorlatilag ugyanazon az elven működnek, mint a többi, piacon található eszköz.

SERVER, KISZOLGÁLÓ VAGY SZERVER?

– Honosításkor vannak olyan kényes kérdések, amelyeket szoftverenként és országonként nagyon körültekintően kell kezelni – hívta fel a figyelmet Antunovics Mónika. – Megfontolandó, hogy minden szöveget le kell-e fordítani vagy sem. Lehet például olyan kompromisszumot kötni, hogy az elrejtett, csak a rendszergazdák számára hozzáférhető üzenetek maradjanak meg angolul.

Sok vitát váltanak ki a terminus technicusok. Franciaországban például minden nyelvi kérdésben az akadémia dönt, ezért a honosítást végző szakembereknek állandó kapcsolatban kell állniuk a nyelvi hatóságokkal. Komoly problémát okozhatnak a nyelvi reformok. Egy 3-4 éves fejlesztési ciklusú szoftvernél tulajdonképpen előre kellene látni a változásokat, illetve azt, hogy az új szabályok mennyire terjednek el a köznapi használatban.

Országa válogatja, hogy hol húzódik a határ a lefordítandó és az

angolul hagyható kifejezések között. Az egyik véglet, hogy gyakorlatilag mindent le kell fordítani (még a walkmant is), a másik, hogy minél több kifejezés maradjon angolul (ennek főként a rendszergazdák a szószólói).

„Mi minden esetben próbálunk kompromisszumot találni, és ha egy kifejezés nem válik be, megváltoztatjuk a korábbi gyakorlatot. Itt van például a *server*, amit sokáig *kiszolgálónak* fordítottunk. Hiába írtunk azonban 10 évig kiszolgálót, kénytelenek vagyunk elfogadni, hogy nem vált be. Így aztán áttértünk a *szerverre*, így, *magyarosan írva*. **Személyes tapasztalatom, hogy a latin eredetű szavakat könnyebb átültetni a magyar nyelvbe. A regisztráció vagy a kliens-szerver kifejezések igen jól meghonosodtak, míg például a firewall vagy a cookie sokkal kevésbé"** – mutatott rá a Microsoft szakértője.

Tímár András
szoftverhonosítási szakértő
FSF.hu

FUNKCIONALITÁS ÉS NYELVHELYESSÉG

Tudvalevő, hogy az angol rendkívül kompakt nyelv, ezért a honosítás – angol forrásnyelv esetén – óhatatlanul problémákat rejt magában. Ezek egyike a helyszűke, aminek kiküszöbölésére a Microsoft fejlesztői szigorú, írásos utasításban kapják, hogy a párbeszédpanelekben plusz 30 százaléknyi helyet kell hagyniuk a honosított szöveg számára. Ennek ellenére előfordul, hogy a fordított szöveget képtelenség beszorítani a rendelkezésre álló felületre. Ilyenkor a honosítónak lehetősége nyílik a hely megnövelésére, vagy esetleg a lefordított kifejezés rövidítésére (ez utóbbi kerülendő).

Az angolban nincsenek toldalékok, nincs a főneveknek nemük, nincs különbség a tegezés és a magázás között. Ennek következtében minden célnyelv esetében meg kell hozni a vonatkozó szabályokat. Magyarul például a Microsoft-alapú rendszerekben a felhasználó és a számítógép kölcsönösen magázza egymást, sok szláv nyelvben viszont a felhasználó tegezi a számítógépet, míg a számítógép magázza a felhasználót. A stílust mindig a célnyelv országának kultúrája határozza meg.

„Cél, hogy a funkcionalitás és a nyelvhelyesség egyaránt tökéletes legyen. Sajnos vannak technikai korlátok, amelyek időnként megakadályozzák az elegáns megoldást. Természetesen a fordítók képességei is eltérőek. Az azonban biztos, hogy a honosítást mindig olyanok végzik, akiknek a célnyelv az anyanyelvük, és akiknek van némi szoftverismeretük" – hangsúlyozta Antunovics Mónika.

TÖMEGIGÉNY

Tágabb értelemben a honosítás is a fejlesztés része. A szoftverfejlesztőknek minden esetben figyelembe kell venniük a honosítók igényeit, olyan kódot, illetve szoftvert kell fejleszteniük, amit könnyű átültetni más nyelvekre. Az első lépés tehát a termék nemzetköziesítése. Ennek részeként úgy kell felkészíteni a szoftvert (például a dátumkezelést, a mértékegységeket), hogy az minden nyelvi beállítást kezelni tudjon. A szoftver üzeneteit, menüit félreérthetetlenül és minden nyelvre lefordíthatóan kell megfogalmazni. Ezután kerülnek ki a lefordítandó erőforrásfájlok a fordítóhoz, aki valamilyen honosítást támogató eszköz segítségével lefordítja a szövegeket – mondta *Tímár András* szoftverhonosítással foglalkozó szakember, a Free Software Foundation Hungary Alapítvány (FSF.hu) tagja.

Az, hogy egy szoftverben menynyire kell a teljes fordításra törekedni, nagymértékben a felhasználói körtől függ. **Egy rendszergazdáknak szóló szoftver fordításánál mások a szempontok, mint például egy szórakoztatóelektronikai készüléknél, aminek a kezelését egy laikusnak is tökéletesen meg kell értenie.**

„A honosítással a tömegek számára is elérhetővé válnak a szabad szoftverek. Labdába sem rúghat az a termék, aminek nincs magyar verziója. Ezt követeli meg a piac. Ugyanakkor nem értek egyet azzal, hogy minden szoftvert feltétlenül honosítani kell. A szakember esetenként jobban jár, ha például az eredeti, angol szerverszoftvert használja. Ahhoz könnyebben talál irodalmat is az interneten. De egy böngészőt vagy szövegszerkesztőt feltétlenül le kell fordítani magyarra" – hangsúlyozta Tímár András.

MINŐSÉGI KÜLÖNBSÉGEK

A szoftvereknél – a szöveg jellegéből fakadóan – sok az ismétlődés, elég kötött a szókincs. Ezért adja magát, hogy a honosítók célszoftverekkel dolgozzanak.

Az alapanyag (a forrásszöveg) formája az adott projekttől, a megrendelő kívánságától függ. Lehet közvetlenül az erőforrásfájlokból dolgozni, vagy kigyűjteni az összes szöveget egy Excel táblázatba (ez a legegyszerűbb). A szabad szoftvereknél, ahol nincs megrendelő, csak a forráskódból lehet kiindulni; ott a fordító dönti el, hogy milyen utat választ.

„Fordítója válogatja, hogy ki milyen alapanyagból, illetve milyen segédeszközzel dolgozik szívesebben. A technikailag kevésbé képzettek jellemzően egy sima Word vagy Excel dokumentumot részesítenek előnyben, a professzionális fordítók azonban előszeretettel használnak honosító célszoftvereket, például Tradost vagy Passolót. Ez utóbbiak fizetős eszközök. **Mivel a szabad szoftvereknél gyakorlatilag a PO fájlformátum az uralkodó, e szoftverek honosítására vannak szabad szoftveres segédeszközök is. Léteznek webes és nem webes fordítók, fordítómemória- és technológiakezeléssel, minőségellenőrzéssel vagy anélkül.** Ezen eszközök színvonala ugyan még nem érte utol a kereskedelmi termékekét, de az utóbbi pár évben nagy volt a fejlődés, és előbb-utóbb behozzák a lemaradást" – mutatott rá Tímár András.

A szakember elmondta: a honosítás minőségét illetően a magyar nyelvű szabad szoftverek meglehetősen vegyes képet mutatnak. Vannak azonban olyan kiemelt projektek, így például a Mozilla Firefox, az OpenOffice.org vagy a Gnome, amelyeknél fokozott hangsúlyt kap a minőség, és szigorú az ellenőrzés.

A nyelv nem szoftver

Hiába ítélnek a nyelvészek egy-egy kifejezést kevésbé szerencsésnek, a webbel nem tudják felvenni a harcot. Manapság, amikor az interneten pillanatok alatt milliókhoz jutnak el a különféle írásos és képi anyagok, szinte lehetetlen megakadályozni, hogy az azokban használt szavak és kifejezések bekerüljenek a köztudatba – véli *Prószéky Gábor*, a MorphoLogic ügyvezető igazgatója. A szoftverek világában a Microsoft hasonlóan meghatározó erőt képvisel, mint a hétköznapi emberek körében az internet. Nem meglepő tehát, hogy a Microsoft által elfogadott és bevezetett magyar kifejezések képezik a szoftvervilág terminológiájának alapját.

Prószéky Gábor
ügyvezető igazgató
MorphoLogic

Manapság a nagy szoftvercégek egyre inkább egy központi helyen végzik szoftvereik honosítását. Ennek – Prószéky Gábor szerint – vannak veszélyei. Nem elég ugyanis, ha a honosítást végző fordító anyanyelve a célnyelv, az is fontos, hogy az illető az adott nyelvi közegben éljen. Ellenkező esetben a fordítás, jóllehet nyelvileg tökéletes, nem életszerű. Szoftvert fejleszteni lehet néhány kijelölt nagy központban, a szoftverek honosítására azonban nem feltétlenül ez a kívánatos út.

Tanúsítványt ellenőrző szerver

A Windows 2008-as OCSP válaszadó szolgáltatással kialakíthatunk egy online tanúsítvány-ellenőrzési rendszert, amely révén ügyfeleink, külső partnereink, akik tanúsítványalapú hitelesítéssel érnek el bizonyos erőforrásokat cégünknél, az ellenőrzést gyorsan, könnyedén biztonságosan el tudják végezni. Írta: Takács János

Egyre többen használnak nyilvános kulcsú infrastruktúrára épülő (Public Key Infrastructure – PKI) szolgáltatásokat az online kommunikációkban és az üzleti tranzakciókban, amelyekben elektronikus tanúsítványok (IETF: X.509. v3) segítségével azonosítjuk a részt vevő feleket. A tanúsítványokat egy ún. megbízható harmadik fél, a hitelesítésszolgáltató (*továbbiakban: HSZ*) állítja ki és menedzseli, továbbá felel a tanúsítványok ellenőrzéséért, illetve a törölt vagy visszavont tanúsítványok állapotának publikálásáért.

A nyilvános kulcsú infrastruktúrán alapuló szolgáltatások használatának talán a legfontosabb része a megbízható ellenőrzési eljárás, amelyet alapos körültekintéssel kell elvégezni, ha például, elektronikus dokumentumok alapján szeretnénk döntéseket hozni. Az ellenőrzési procedúrát mindig a HSZ által meghatározott hitelesítési rend alapján kell végeznünk, máskülönben a szolgáltató nem vállal semmilyen felelősséget, garanciát. A HSZ-ek a felelősek a lejárt tanúsítványok listájának kiadásáért (CRL-listák), amelyet a szolgáltatási szerződésben is rögzítenek, hogy milyen formában és milyen gyakorisággal teszik ezt, illetve az ebből származó károkért anyagi felelősséggel tartoznak.

A visszavonási információk birtokában tudjuk eldönteni, hogy a tanúsítvány az aláírás pillanatában érvényes volt-e, illetve a visszavonási információk segítségével igazolhatjuk, hogy az aláírást valóban megalapozottan fogadtuk el.

A tanúsítványok állapotának és érvényességének ellenőrzésekor két fő szempontot kell figyelembe vennünk: a lejárati időt és a visszavonási állapotot. A szolgáltatók a tanúsítványokat rögzített időtartamra adják – ez általában 1 év –, de bármely okból időközben is visszavonhatják. Ezt olyan esetben szokták megtenni, ha például a kulcs kompromittálódott, az alkalmazott elhagyta a céget, vagy ha elvesztette az intelligens kártyáját. Mint az előbbiekben említettük, ezek a szolgáltató által közreadott visszavonási listákból ellenőrizhetők. Van azonban egy online ellenőrzési protokoll is, az ún. OCSP (Online Certificate Service Protocol),

> A nyilvános kulcsú infrastruktúrán alapuló szolgáltatásoknál nagyon fontos a megbízható ellenőrzési eljárás...

amely valós időben ellenőrzi a kérdéses tanúsítványt, és az eredményt egyből láthatjuk. Ezt a megoldást főleg ott érdemes használni, ahol a visszavonási listák használata nem megfelelő vagy nem kielégítő.

VISSZAVONÁSI LISTÁK VAGY ONLINE ELLENŐRZÉS (OCSP)?

A hitelesítésszolgáltatók visszavonási listái az összes visszavont és felfüggesztett tanúsítvány sorozatszámát tartalmazzák. Ezzel szemben **az OCSP csak az ügyfél által kért egyedi tanúsítvány állapotával kapcsolatos információkat közli valós időben, azaz sokkal kisebb adatforgalmat (néhány KB-ot) generál,** egy lista pedig akár több megabájt is lehet, így a távoli ügyfeleknek, akiknek nincs nagy sebességű kapcsolatuk, elég nehézkes, lassú lehet egy visszavonási listán alapuló ellenőrzési procedúra. Ennél is nagyobb probléma a visszavonási listáknál a kivárási idő (grace-period): ha a szolgáltató a napi lista kiadása után von vissza egy tanúsítványt, akkor az csak a következő listában jelenik meg. Ezzel szemben az OCSP-nél azonnal a legfrissebb információt kapjuk a tanúsítvány állapotára vonatkozóan.

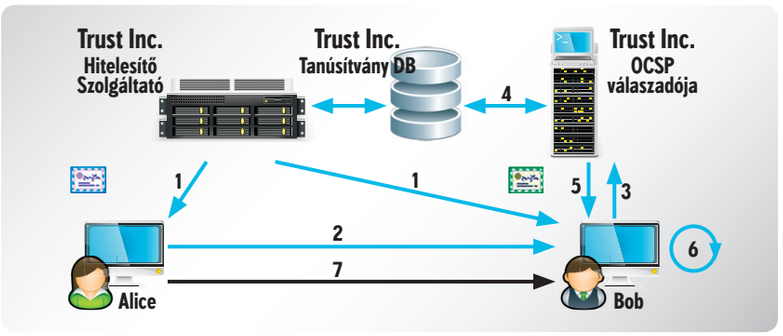
Az OCSP tanúsítvány-ellenőrzési szolgáltatást használhatjuk minden olyan rendszerben, ahol az ügyfelek tanúsítványokkal hitelesítik magukat. Használhatjuk például webalapú rendszerekben, ahol SSL/TLS-alapú kapcsolatokat használunk, intelligens kártyás bejelentkezésnél, az S/MIME-alapú titkosított levelezésnél, a titkosított fájlrendszernél (EFS) vagy akár az olyan VPN-kapcsolatoknál, ahol EAP/TLS-alapú hitelesítést használunk.

Szerveroldalról a Windows Szerver 2008-tól natívan támogatja az OCSP válaszadó szolgáltatást, amely gondoskodik a visszavonási állapotadatok kezeléséről és szétosztásáról. Ügyfél operációs rendszer oldalon a Windows Vistának és a Windows 7-nek része a támogatás, a korábbi verzióknál azonban csak a visszavonási listákat lehetett használni.

MŰKÖDÉS KÖZBEN

Hogyan működik a nyilvános kulcsú infrastruktúrában az OCSP-szolgáltatás? Nézzünk egy egyszerű példát Bobon és Alice-on keresztül, akik szeretnének egymással lebonyolítani egy üzleti tranzakciót. Az ehhez szükséges tanúsítványokat a Trust, Inc. biztosítja számukra, mint hitelesítő hatóság. A folyamat a következő:

1. A Trust, Inc. kiadja az igényelt tanúsítványokat Bob és Alice számára.
2. Alice végre akar hajtani egy tranzakciót Bobbal, ezért elküldi neki a nyilvános kulcsát.
3. Bob, miután megkapja Alice nyilvános kulcsát, egy OCSP-kérésben ellenőrzi, hogy nem kompromittálódott-e Alice titkos kulcsa. Az OCSP-kérésben megtalálható Alice tanúsítványának sorozatszáma, lényegében Bob ezt elküldi el a Trust, Inc. OCSP-válaszadójának.
4. A Trust, Inc.-hez tartozó OCSP-válaszadó a sorozatszám segítségével kikeresi Alice tanúsítványának visszavonási állapotára vonatkozó adatokat az adatbázisából. Ha a kulcs kompromittálódott, akkor az ebben az adatbázisban rögzítve lenne.
5. A Trust, Inc. OCSP-válaszadó szolgáltatója megerősíti Bob számára egy aláírt válaszban (OCSP response), hogy Alice tanúsítványa rendben van.
6. Bob ellenőrzi az aláírt választ, ez biztosítja a fogadó felet, hogy tényleg a megfelelő OCSP-válaszadó szolgáltatótól kapta-e a választ. (Mivel Bobnak megvan a Trust, Inc. nyilvános kulcsa, így ezt könnyedén ellenőrizheti.)
7. Bob végrehajthatja a tranzakciót Alice-szel.



OCSP-szolgáltatás működése

A WINDOWS 2008 OCSP-SZOLGÁLTATÁS

Természetesen ez a szolgáltatás azon cégeknél alkalmazható, ahol már működik a PKI infrastruk-

túrán alapuló szolgáltatás, vagy ahol tervezik az ilyenfajta szolgáltatás bevezetését. Az online válaszadó bevezetésével növelhetjük PKI-infrastruktúránk rugalmasságát, méretezhetőségét. Hiszen az online válaszadók bevezetésével leegyszerűsíthetjük, felgyorsíthatjuk és kényelmesebbé tehetjük ügyfeleink számára a tanúsítványok ellenőrzésével járó, néha eléggé összetett folyamatokat.

A Microsoft OCSP-támogatás kliensszerver felépítésű. A szerverkomponenst az Active Directory tanúsítványszolgáltatások szerepkör által biztosított új szolgáltatásként tudjuk telepíteni. A hitelesítő szolgáltatás feltelepítése után telepíthető az OCSP-szolgáltatás, még mielőtt elkezdenénk tanúsítványokat kiállítani az ügyfeleknek. A kliensoldal lényegében a CryptoAPI 2.0 függvénytárba van beépítve.

Ahhoz azonban, hogy egy ilyen szolgáltatást be tudjuk indítani, van néhány feltétel. Mindenekelőtt rendelkeznünk kell IIS-szolgáltatással. Utána telepíteni kell egy hitelesítésszolgáltatót, majd engedélyezni az OCSP-válaszadó sablont. Be kell állítanunk az automatikus igénylést erre a sablonra, valamint a hitelesítési szolgáltatón be kellene állítani a kiadott tanúsítványok terjesztési pontját. Ez utóbbi egy URL-cím, amely alapján az ügyfél (az-az a böngésző) megtalálja az adott tanúsítványhoz tartozó OCSP-válaszadót.

Az OCSP-szolgáltatás telepítése után szintén fontos lépés, hogy létrehozzuk a visszavonási konfigurációt minden általunk üzemeltetett hitelesítőszolgáltatóhoz. Erre azért van szükség, hogy az általuk kiadott tanúsítványok állapotára vonatkozó kéréseket megválaszolhassuk. Amikor ugyanis az ügyfél megkapja az adott tanúsítvány állapotára az OCSP-választ, ott nemcsak a kérdéses tanúsítványnak, hanem az azt kiállító összes olyan közbenső hitelesítésszolgáltatónak érvényesnek kell lennie, amely a tanúsítási láncban szerepel.

A visszavonási konfiguráció tartalmazza a hitelesítésszolgáltató tanúsítványát, az OCSP-válaszok aláíró tanúsítványát, valamint a visszavonási szolgáltató egyedi beállításait. Azt figyelembe kell venni, hogy a Windows Server 2008 OCSP-válaszadója csak egy alapértelmezett, a visszavont tanúsítványok listáján alapuló visszavonás-szolgáltatót biztosít, és nincs lehetőség új szolgáltatók felvételére.

A WINDOWS 2008 OCSP-VÁLASZADÓ

A következőkben megnézzük a Windows 2008 OCSP-válaszadó főbb szolgáltatásait.

Webproxy-gyorsítótárazás: az OCSP-válaszadó webproxy-gyorsítótára lényegében az OCSP szolgáltatási felülete, amely egy IIS-szolgáltatás által működtetett.

A NONCE és nem NONCE típusú kérelmek támogatása: az ilyen típusú kérelmek konfigurációs beállításaival biztosíthatjuk az OCSP-válaszadó válaszainak ismétlésvédelmét.

Speciális titkosítás támogatása: a válaszadók úgy konfigurálhatók, hogy ECC és SHA–256 titkosítást használjanak a titkosítási műveletekhez.

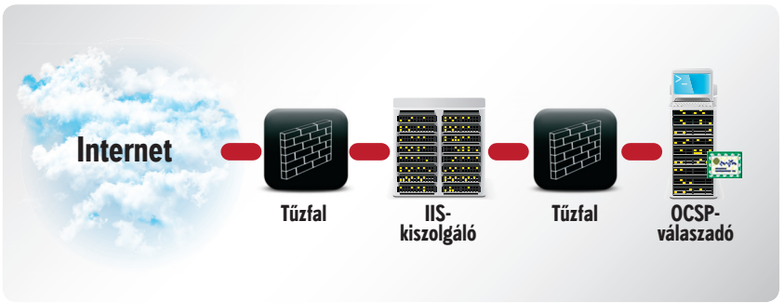
Előre definiált OCSP-tanúsítványsablonok: ezek egyszerűsítik a telepítést.

Kerberos protokoll integrációja: az OCSP-válaszadó kérelmei és válaszai bejelentkezésnél feldolgozhatók a Kerberos jelszó-hitelesítéssel együtt (a Windows bejelentkezésnél), ezáltal gyorsabban ellenőrizhetők a kiszolgálók tanúsítványai.

Az OCSP-válaszadó szolgáltatás telepíthető egy önálló számítógépre vagy több önálló gépre, amelyekből ún. tömbkonfigurációkat hozzunk létre. A tömbkonfigurációban több gépet tehetünk, így a redundancia révén a hibatűrés és a magas rendelkezésre állás követelményeinek is megfelelnek. A tömbkonfigurációban a tömbtagokat külön-külön konfigurálhatjuk, menedzselhetjük, illetve szükség van egy tömbvezérlőre, amely elhárítja az esetleges ütközéseket. Az Windows 2008 OCSP-válaszadó az MMC beépülő moduljának köszönhetően több OCSP-válaszadó önálló entitásként kezelhető.

Az *alábbi képen* az OCSP-válaszadó a védett belső hálózaton (LAN) belül található. Az ügyfelektől érkező kérelmeket egy IIS fogadja, amely a DMZ-ben (demilitarizált zóna) foglal helyet, így a kérelmeket átirányítja az OCSP-válaszadó felé. Nagy előnye ennek a megoldásnak, hogy „tűzfalbarát" megoldás, így a tűzfalon csak átjárást kell biztosítanunk a 80-as porton keresztül.

A másik lehetséges megoldás, amikor egy ISA szerveren (Microsoft Internet Security and Acceleration) keresztül kapcsolódnánk az OCSP-válaszadóhoz.



OCSP-válaszadó a védett belső hálózaton

Miért jó a tömbkonfiguráció? Azért, mert a válaszadó tömbhöz folyamatosan adhatunk új tagokat, amelyeket akár földrajzi szempontok alapján, hálózattervezési, méretezhetőség vagy esetleg hibatűrési okok miatt kényszerülünk beiktatni.

OCSP-VÁLASZADÓ TELEPÍTÉSI MODELLJEI

A válaszadót telepíthetjük egyetlen gépre vagy akár több gépből álló fürtre is. Önálló OCSP-válaszadó megoldás lehet olyan kisebb környezetekben, ahol nem okoz komolyabb gondot a válaszadó kiesése, véleményem szerint főként tesztkörnyezetekben lehet jelentősége. A fürtözött megoldás már alkalmazható vállalati közegben, ahol fontos a megfelelő teljesítmény és rendelkezésre állás.

Nézzük meg az extranetes környezetek számára lehetséges kiépítéseket! Itt lényegében az OCSP-válaszadók kapcsolatban állnak az extranettel; egyik szempont lehet, milyen szintű védelmet szeretnénk biztosítani az OCSP-válaszadó aláíró kulcsának.

Ezeknek a kiépítéseknek az előnye, hogy viszonylag kevés portot kell kinyitnunk, így nagyobb ellenőrzést gyakorolhatunk, ami biztonsági szempontból egyáltalán nem elhanyagolható.

KONKLÚZIÓ

A Windows 2008 szerver OCSP-szolgáltatásával támogathatjuk a tanúsítványok állapotára vonatkozó kéréseket, ezzel is megkönnyítve és felgyorsítva a validációs folyamatot. **Az OCSP használatával levesszük az ügyfelek válláról a néha bonyolult ellenőrzési procedúrát, így most ezt egy kattintásra elvégzi helyettünk a böngésző, és nem kell visszavonási listákat nézegetnünk, ahol számtalan hibalehetőség becsúszhat.** Láthattuk, hogy a tömbkonfigurációk kiépítésével jelentősen növelhetjük infrastruktúránk méretezhetőségét és hibatűrését, amelyek megléte elengedhetetlen a vállalati közegben.

OCSP-t támogató böngészők

A Microsoft az Internet Explorer 7-től kezdve építette be a böngészőjébe az OCSP-támogatást. Legalább Windows Vistát kell használnunk hozzá, mert XP-n ez a funkció még nem működik.
A Mozilla Firefox minden verziója támogatja az OCSP-t, a böngésző 3-as verziójától kezdve az OCSP-ellenőrzés alapértelmezett beállítás lett a böngészőben. Az Apple Safarija és a Mac OS X szintén támogatja ezt a funkciót, az Operába a 8.0-tól építették be, és a Google Chrome is alkalmas erre, ha legalább Windows Vistára telepítettük.

Anonimitás az interneten

Ha böngésszük a netet, alapjában nem figyel ránk senki. Ez egészen addig igaz, amíg nem a cégünknél netezünk, és esetleg nem olyan híreket teszünk közzé, amelyek valakiknek kimondottan kellemetlenek lehetnek. Ilyenkor várható, hogy online tevékenységünkre felfigyelnek. Ennek egyes vállalatoknál elbocsátás is lehet a vége. Írta: Horváth Ádám

Ha érzékeny tartalmakat olvasgatunk vagy teszünk közzé a neten, jó megoldás lehet az ingyenes, nyílt alapokon fejlesztett *Tor hálózat* használata (a bűnözők kiválóan el tudnak rejtőzni az interneten e nélkül is, így a Tor nem sokat segít a cyberbűnözőknek). Bár az elosztott hálózatként működő Tor 2003 októberében indult, nincs óriási felhasználói tábora. Az alapelgondolás rém egyszerű: az adatforgalmat több számítógépen át küldi titkosítva a célpontnak, így nem vagy alig lehet visszakövetni, hogy az az adat honnan származik.

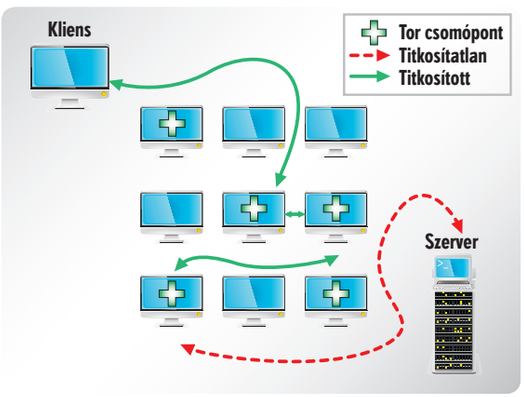
A Tor hálózat alapjában TCP-csomagok küldésére alkalmas, és ezt egy helyi, speciális SOCKS PROXY indításával éri el. Nem HTTP proxyként működik, így nemcsak böngészők használhatják, hanem tetszőleges, SOCKS-ot támogató alkalmazások is (pl. chatprogramok).

Többféleképpen is csatlakozhatunk a rendszerhez: lehetünk egyszerű kliensek, akik csak névtelenül szeretnének valamilyen szerverhez csatlakozni. Lehetünk átjátszók (relay), akik a kliens-szerver között továbbítanak, végül lehetünk rejtett szolgáltatás, amely azonosíthatatlan végpontként jelenik meg, így téve közzé tartalmakat, szolgáltatásokat.

Átjátszót némileg kellemetlen üzemeltetni, hiszen rajtunk keresztül elvileg illegális forgalom is bonyolódhat, ám mivel a Digital Millennium Copyright Act's a szolgáltatókat, így végül az átjátszókat is védi, ezért jogilag nem aggályos (számos esetben ejtették az eljárást Tor-felhasználók ellen). Még nagyobb biztonságban vagyunk, ha beállítjuk a kilépési szabályokat, azaz hogy átjátszónkon keresztül milyen forgalmakat lehet bonyolítani. Fontos kiemelni, hogy a Tor a hagyományos nyomozás ellen nem védi meg a felhasználókat – a tanúkat ki tudják hallgatni, az írásokat lehet elemezni, így végül az elkövető is azonosítható, ha az ügy súlya olyan.

MŰKÖDÉS

A Tor hálózathoz csatlakozni úgy lehetséges, hogy a kliens kér egy Tor-listát a központtól, majd csatlakozik valamelyik csomóponthoz. A kifelé irányított kommunikáció titkosított, sőt a Tor átjátszók is titkosítva küldik a forgalmat, csak a kilépő csomópont adja át a szervernek (például weboldalnak) titkosítatlanul a forgalmat. A titkosításhoz TLS-t (RSA1024 és AES128 titkosítás) használ a rendszer, így állíthatjuk: nem a titkosítás lesz a rendszer gyenge pontja.



Tor kliens-szerver kapcsolódás

Bár a TCP-forgalmat megfelelően elrejti, a benne futó forgalommal nem foglalkozik. Ha tehát böngészőnk sütiben elküldi azonosítóinkat, akkor értelmetlen Tor hálózaton keresztül kapcsolódni egy oldalhoz. Ezért a Tor használata előtt törölni kell böngészőnkből a sütiket és a cache-t. Az anonimitás persze így sem tökéletes, hiszen az épp online lévő átjátszók listája nyilvános. Ha minden átjátszót figyelnek/lehallgatnak (erre van elméleti lehetőség), akkor statisztikai elemzéssel kikövetkeztethető, hogy milyen forgalmat bonyolítottunk.

TESZT

A Tor igényes telepítőcsomagja Windowsra, Macre és Linuxhoz is elérhető. Alapjában kétféle csomagból választhatunk – az egyik csak maga a Tor, a másik pedig előre csomagolt, amely Firefox böngészővel (legtipikusabb használat) vagy csevegőprogrammal (Pidgin) érhető el. **Akik nem akarnak sokat konfigurálni, nyugodtan választhatják a böngészős csomagot, egyszerűen működik és kész! Bár a telepítés nem nehézkes, a manuális telepítésnél proxy portszámokat kell tudni. Ezt viszont a leírás nem rágja a felhasználó szájába, sőt a beállítások között sem látszik.**

A Tor SOCKS proxyként működik, ezért a csomag telepíti a Polipo webproxyt (HTTP proxy) is, amihez a böngészőnk csatlakozhat, majd pedig a Polipo csatlakozik a SOCKS-hoz. Ez bonyolultnak hangzik, ám valójában arról van szó, hogy más portszámokat kell megadni böngészőben (8118), és mást egyéb SOCKS-ot használó szoftverben (9050).

A rendszer sajnos igen lassú, inkább valamilyen modemes kapcsolatnak érződik, de legalább működik. Tesztjeinkben a látogatott weboldalak csak a Tor kilépő IP-címét látták, amit bármikor, egyetlen kattintással tudunk váltani (így RapidShare letöltésre vagy torrentezésre aligha érdemes használni a Tort).

A teszt alatt több mint 1700 átjátszó volt online, többségük Európában, így bőségesen lehet a csomagokat továbbítani a csomópontok között. Ha aktívan használjuk a Tort, nekünk is érdemes átjátszót indítani, amit egyszerűen, grafikus felületen állíthatunk be. Könnyen konfigurálható, hogy milyen sávszélességet és milyen típusú eléréseket vagyunk hajlandók forgalmazni. Itt érdemes figyelni, hiszen alapértelmezettként miden forgalmat (SMTP-t is, azaz lehetséges spamforgalmat is) vállalunk, ezt érdemes szűkíteni.

REJTETT SZOLGÁLTATÁS

Ez igazán érdekes ötlet: úgy tudunk szolgáltatást, például weboldalt üzemeltetni, hogy a hozzánk csatlakozók nem tudják, a szolgáltatás honnan származik. A folyamat viszonylag bonyolult, ám a beállításról részletes leírással szolgálnak a Tor lapján. Az elmélet a következő: létrehozunk egy szolgáltatást, például weblapot, aminek a szolgáltatásazonosítóját leadjuk a központnak, és eltároljuk egy központi DHT-tárban. Ha valaki keresi a mi szolgáltatásunkat (például egy fórumhirdetés alapján), akkor a DHT-tárból megkapja a szolgáltatásleírót, amelyben jelölték, hogy a szolgáltatás milyen bemutatkozó pontokon keresztül (introduction point) érhető el. Ezek a pontok maguk sem tudják, hogy a szerver hol érhető el, csak azt, hogy milyen további csomópontnak kell továbbítani az üzenetet, amely vagy kapcsolatban van a szolgáltatással, vagy maga a szolgáltatás, vagy csak egyszerűen továbbítani tudja a szolgáltatás felé az üzenetet.

A kliens elküldi a bemutatkozó pontokon keresztül, hogy mely adott csomóponton át szeretne kommunikálni a szerverrel (rendezvous point). **A szerver felkeresi ezt az adott csomópontot (valahány átjátszón keresztül), és elindul az adatfolyam. Sem a szerver, sem a kliens nem tudja, hogy a másik fél ki, csak azt, hogy valamilyen útvonalon keresztül az adatfolyam létrejött.** Így például közzétehetünk érzékeny fotókat anélkül, hogy azokat bárhová fel kellene tölteni, így cenzúrázni sem lehet őket.

ÖSSZEGZÉS

A Tor hálózat kiváló megoldás lehet akkor, ha adott feladatokhoz követhetetlenek szeretnénk lenni az interneten; bár lassú, működik, és csak nagyon nagy apparátussal lenne (elvileg) visszakövethető a forgalmazó. Olyan esetben is érdekes lehet, ha közzé szeretnénk tenni valamilyen szolgáltatást, ám nem akarjuk, hogy a kliensek tudják, ez honnan származik. Rejtett szolgáltatást is igen egyszerűen indíthatunk!

Felelősen, fenntarthatóan

Társadalmi felelősségvállalás, röviden CSR, az angol Corporate Social Responsibility kifejezésből. Parképítés, kórházaknak juttatott adományok, az él- vagy éppen a tömegsport támogatása. Nap mint nap hallani ilyen és hasonló kezdeményezésekről. Kérdés, hogy mindez valójában mit takar, illetve a vállalatok mennyire átgondoltan, milyen arányban és mértékben járulnak hozzá a fenntartható fejlődéshez. Írta: Mallász Judit

Tavaly Magyarország száz legjelentősebb vállalatának egyharmada számolt be ún. nem pénzügyi teljesítményéről – derül ki a KPMG felméréséből. **Egy év alatt a kép gyakorlatilag nem változott: amíg 2008-ban 34 vállalat készített jelentést a fenntartható fejlődés érdekében tett lépéseiről, addig 2009-ben 33.** Közülük 17 vállalat különálló CSR/fenntarthatósági jelentést készített, 12 cég éves jelentésébe foglalta a CSR/fenntarthatósági tartalmat, míg 4 vállalat mindkét megoldással élt. A 33 jelentés közül nyolcnak van külső kontrollja; ez számottevő visszaesés az előző év adataihoz képest (2008-ban 15 vállalat auditáltatta jelentését).

A KPMG felméréséből megállapítható, hogy a jelentéskészítést elsősorban a márkaépítés és az etikai megfontolások motiválják. A gazdasági szempontok és a számszerűsíthető eredmények még csak néhány jelentésben tűnnek fel.

HOL VANNAK A VÁLSÁGHATÁSOK?

A különálló jelentést készítő vállalatok 80 százaléka a Global Reporting Initiative (GRI) irányelveit alkalmazza. Ez elősegítheti a vállalatok jelentéskészítési gyakorlatának egységesítését, a nem pénzügyi teljesítmények összehasonlíthatóságát.

Bár a GRI egyik tartalmi alapelve a vállalat működését befolyásoló lényeges körülmények számbavétele, a vizsgált 100 hazai cégből mindössze 6 ítélte a gazdasági válság hatásait olyan fontosságúnak, hogy azokat jelentésében szerepeltesse. (A 6 cég közül 4 – nem meglepő módon – a pénzügyi, illetve biztosítási szektorból került ki.) E tény kétségtelenül elgondolkoztató, hiszen 2009-ben a vállalatok többségét már érintette a válság, illetve annak hatásai előre láthatók voltak. Ez is azt igazolja, hogy a jelentések tartalmát és minőségét célszerű volna felülvizsgálni, javítani – állapította meg *Szabó István*, a KPMG vezető tanácsadója, a kutatások vezetője.

Figyelemre méltó, hogy **a klímaváltozás elleni küzdelem, a szénlábnyom mérése, valamint a víz védelme a jelentések közel felében már megjelenik, de például a roma integráció kezelésére tett vállalati intézkedések még hiányoznak a jelentésekből,** illetve a cégek tevékenységéből.

Amíg a világ vezető vállalatainál a legmagasabb szintű átláthatóságot biztosító A+ és B+ alkalmazási szint a legelterjedtebb, addig Magyarországon a C és C+ szintű riportok teszik ki a GRI szerint készített jelentések több mint 40 százalékát. A KPMG szakértőinek véleménye szerint a C szintű jelentések számának érzékelhető növekedése biztatónak tekinthető, amennyiben az újonnan jelentést készítő vállalatok a C szintet az első lépésként, nem pedig végállomásként tekintik.

ELEKTRONIKA – CSUPÁN 15 SZÁZALÉK

A KPMG felmérésében szereplő 100 nagyvállalat 16 iparágat képvisel, köztük az elektronikai és számítástechnikai gépgyártást, valamint a telekommunikációt és médiát.

Az elektronikai iparágban vizsgált 13 vállalat közül mindössze 2 készített társadalmi/környezeti tevékenységéről jelentést: egy különálló vezetői összefoglalóban, egy pedig éves jelentésében, külön fejezetben. A 15 százalékos arány azt jelzi, hogy ebben a szektorban még kevéssé elterjedt a CSR-tevékenységekről való beszámolás gyakorlata.

Az elektronikai iparág legnagyobb hazai szereplőinek további 23 százaléka jelentést ugyan nem készít, de honlapján beszámol társadalmi, környezeti tevékenységéről. Közel 70 százalékra tehető azon vállalatok aránya, amelyek egyáltalán nem bocsátanak közre CSR-rel kapcsolatos információt.

Csupán egyetlen elektronikai vállalat számol be arról, hogy társadalmi és környezeti tevékenységeit meghatározott stratégiai célok mentén hajtja végre, valamint a célok elérésének mérésére valamilyen indikátorrendszert használ. Ugyanakkor egyetlen vállalat sem készít beszámolót az elért eredményekről. Biztató jel, hogy a felmérésben részt vevő elektronikai vállalatok 15 százaléka már felismeri, sőt meg is határozza a fenntartható fejlődésben rejlő üzleti és pénzügyi lehetőségeket.

Az elektronikai iparág szereplői körében még nem terjedtek el a nemzetközi szervezetek (OECD, ILO) által kiadott iránymutatások, ugyanakkor a vizsgált cégek közül kettő beszámol az ISO 14001 kör-

Első a stratégia

A 2008-as és 2009-es évre vonatkozó kutatások eredményei alapján a KPMG a következő főbb javaslatokat teszi a vállalatoknak:

- Alakítsanak ki az üzleti stratégiából levezethető fenntarthatósági stratégiát; határozzanak meg indikátorokat, mérhető rövid és hosszú távú célokat.
- Határozzák meg, mely érintett csoportokkal állnak kapcsolatban, és milyen célból kezdenek párbeszédet velük; alakítsák ki a strukturált párbeszéd kereteit, folyamatát.
- A csoport szinten jelentést készítő vállalatok mutassák be a helyi szintű gazdasági, környezeti és társadalmi hatásokat, kezdeményezéseket és azok eredményeit is.
- A jelentések tartalmazzák az adott időszakra meghatározott célkitűzéseket, a mért eredményeket, dilemmákat, fejlődési területeket.
- A vállalatok elemezzék a fenntarthatóságban rejlő kockázatokat és lehetőségeket, továbbá mutassák be azok pénzügyi hatásait.
- Az átláthatóság, a hitelesség és a megbízhatóság javítása érdekében ajánlott, hogy a jelentéseket külső, független fél tanúsítsa.

nyezeti menedzsmentrendszer alkalmazásáról. A szektor legnagyobb hazai képviselői még egyáltalán nem alkalmazzák a GRI jelentéskészítési útmutatóit.

Megjegyzendő, hogy **a hazai elektronikai ipar két vállalata említést tesz a vállalatirányítás jelentőségéről, egy pedig már összeköti azt a fenntarthatóság, a társadalmi felelősség fogalmával. Elgondolkoztató, hogy csupán egyetlen iparági szereplő számol be a belső ellenőrzés fontosságáról, valamint a kockázatmenedzsment fenntartható fejlődésre gyakorolt hatásáról.** Szintén figyelemre méltó, hogy a vizsgált vállalatoknak kevesebb mint egytizede készít antikorrupciós szabályzatot, és teszi lehetővé, hogy az észlelt szabálytalanságokat a dolgozók – névtelenül – bejelenthessék.

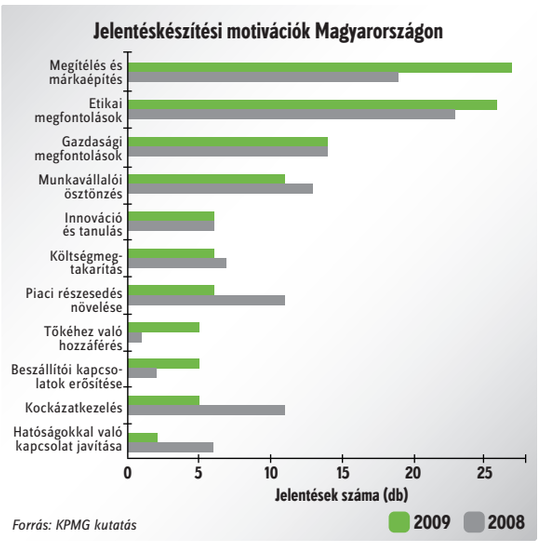
A magyar elektronikai ipar meghatározó képviselőinek a fele foglalkozik beszámolójában a klímaváltozás kérdésével, az abban rejlő üzleti lehetőségekkel, illetve a klímaváltozással kapcsolatos vállalati teendőkkel. Ez utóbbiak között említik a felhasznált energia csökkentését, a termékinnovációt, valamint az újrahasznosítási lehetőségek felkutatását és kihasználását.

A felmérésben szereplő elektronikai gyártók egyike sem hitelesítteti jelentését tanúsító szervezettel.

NÉGYBŐL HÁROM...

A telekommunikáció és média az egyik legérettebb iparág fenntarthatósági és átláthatósági szempontból – derül ki a KPMG felméréséből. Jóllehet a vizsgált 100 nagyvállalat közül mindössze 4 tartozik a szektorba, közülük 3 készít jelentést, ráadásul a többi vállalat számára is példaértékű tartalommal és minőségben.

Mi állhat a jó gyakorlat hátterében? A vállalat (vagy anyavállalatának) tőzsdei jelenléte, a külföldi tulajdonosok szemlélete, a tudatos márkaépítés, a megkülönböztetésre való törekvés a hazai piacon tapasztalható egyre élesebb versenyben – vélik a KPMG szakértői. „A telekommunikációs eszközök széles körű alkalmazása, a szolgáltatások elterjedtségének magas foka, az iparágban rejlő folyamatos megújulási képesség, a kreativitás, továbbá a lakossági és vállalati ügyfelek magas száma hatalmas potenciált rejt magában, amit a CSR/fenntarthatóság szolgálatába tudnak állítani. A telekommunikációs iparág szereplői felismerték a termékekből, szolgáltatásokból származó előnyöket, amelyek egyszerre szolgálják az üzleti növekedést, valamint megoldást kínálnak a klímaváltozás hatásainak csökkentésére. Elég például arra gondolni, hogy a távközlési szolgáltatásokkal kiváltott utazások mennyire csökkenthetik a közlekedésből származó környezetterhelést, de említhető a megújuló-energiák mind szélesebb körű alkalmazása is" – fogalmazott Szabó István.



Forrás: KPMG kutatás

A korrupció és a csalás megelőzésére két vállalat mutatja be intézkedéseit, de konkrét esetekről, a megelőzést segítő csatornákról ezek sem adnak tájékoztatást. Ugyancsak két vállalat foglalkozik a vállalatirányítás, a megfelelőség és a klímaváltozás összefüggéseivel.

A telekommunikációs és médiaszektor jelentései a GRI irányelvei alapján készültek, A+ és B alkalmazási szinten. A három jelentéskészítő vállalat közül egy tanúsíttatta jelentését külső független féllel.

Brúnó, a vakvezető kutya

A vízilabdások és a Vodafone összefogtak a látássérült emberekért. Olimpiai bajnok vízilabdásaink csatlakoztak főszponzorukhoz, és nemcsak bemutatták a vakvezető kutyák kiképzésével foglalkozó Somlai Angyalka Alapítvány munkájának fontosságát, hanem egy kiképzés előtt álló kiskutyát is örökbe fogadtak.

INTELLIGENS ÉS DÖNTÉSEKET HOZ

A magyar vízilabda-válogatott négy tagja nemes tettre vállalkozott annak érdekében, hogy felhívja a figyelmet látássérült embertársaink megsegítésére és az ő életüket megkönnyítő vakvezető kutyák kiképzésének fontosságára. *Varga Dénes*, *Varga Dániel*, *Madaras Norbert* és *Gergely István* bekötött szemmel, vakvezető kutyákra hagyatkozva haladtak végig, és álltak hősiesen helyt az utcai akadálypályán, amely a világtalan emberek mindennapi életének egy kis szeletét hivatott bemutatni. Ennek során rádöbbenhettek arra, hogy a látássérültek számára a legegyszerűbbnek tűnő feladatok – mint például a vásárlás egy virágárusnál vagy egy lépcső megmászása – is komoly gondot jelenthetnek, amelynek leküzdésében nagy segítségükre lehet egy vakvezető kutya.

A fiúk örökbe fogadtak egy kiképzés előtt álló kiskutyát, Brúnót, aki immár a válogatott ajándékaként nevelkedik, és kap kétéves kiképzést, hogy annak befejeztével segíthesse a látássérült embereket. Brúnó társát, Szászt pedig a hosszú, sok türelmet és kitartást igénylő tréning után *Kemény Dénes* szövetségi kapitány adta át új gazdájának, akinek mindennapi életét mostantól nagyban megkönnyíti a kutya.

A vakvezető kutyák nemcsak fantasztikusan intelligensek, de nagyon fegyelmezettek és türelmesek is; gazdáiknak a mindennapokban elengedhetetlen segítséget és biztonságot nyújtanak. A vakvezető kutya az egyetlen olyan állat, „akire" döntést bízhat a gazdája. Az egyetlen élő rehabilitációs „eszköz", amelynek segítségével partnere munkába járhat, oktatási intézménybe juthat el, biztonságban töltheti napjait. Mindemellett lelki társa, barátja, szinte családtagja a látássérült embernek. Egy vakvezető kutyus kiképzése legalább két évet vesz igénybe, és nem kevesebb mint 2 millió forintba kerül.

TOVÁBBI ADOMÁNYOZÓK KERESTETNEK

A Vodafone – felelős társadalmi szereplőként – elkötelezett támogatója olyan programoknak és szervezeteknek, amelyek a közösségek építését, az oktatást vagy a biztonságos életet segítik. A Vodafone Magyarország több mint hat esztendeje támogatja a látássérült emberek megsegítéséért küzdő Somlai Angyalka Alapítványt; eddig 30 millió forinttal járult hozzá a kincset érő kutyák kiképzéséhez. Hazánkban mindössze 100-120 speciálisan kiképzett kutya „dolgozik". A kiképzés magas költsége miatt ez a segítség csak keveseknek adatik meg, több száz látássérült várólistán van.

A legutóbbi, 5 millió forintos támogatás kifejezetten azt a célt szolgálja, hogy egy adományszervező alkalmazásával minél többen értesüljenek erről a nehézségről, és minél többen járuljanak hozzá a kutyusok kiképzéséhez. ■

ÚJ TANULMÁNYOK!

Közel 20 milliárd forintot költöttünk arra, hogy megtaláljuk a megoldást a jövő adatközpontokkal kapcsolatos problémáira

White Paper #141 (WP-141)
"Data Center Projects: Project Management"

~~€95,00~~ INGYENES

White Paper #42 (WP-42)
"Ten Steps to Solving Cooling Problems Caused by High-Density Server Deployment"

~~€55,00~~ INGYENES

Új

White Paper #117 (WP-117)
"Network-Critical Physical Infrastructure: Optimizing Business Value"

~~€95,00~~ INGYENES

Új

White Paper #37 (WP-37)
"Az adatközpont és hálózati terem infrastruktúra túlméretezéséből eredő többletköltségek elkerülése"

~~€55,00~~ INGYENES

White Paper #40 (WP-40)
"Cooling Audit for Identifying Potential Cooling Problems in Data Centers"

~~€95,00~~ INGYENES

Új

White Paper #6 (WP-6)
"Determining Total Cost of Ownership for Data Center and Network Room Infrastructure"

~~€55,00~~ INGYENES

White Paper #18 (WP-18)
"The Seven Types of Power Problems"

~~€95,00~~ INGYENES

Új

White Paper #102 (WP-102)
"Monitoring Physical Threats in the Data Center"

~~€55,00~~ INGYENES

White Paper #82 (WP-82)
"Physical Security in Mission Critical Facilities"

~~€95,00~~ INGYENES

Ön már megtalálta a megoldást?

Több ezer ügyfelünket kérdeztük meg Birminghamtől Pekingig, hogy egészen pontosan megismerjük az adatközpont-tervezéssel kapcsolatos jó és rossz tapasztalatokat egyaránt. Azt tapasztaltuk, hogy sok esetben költségcsökkentésre hivatkozva a teljes adatközpont-tervezés elmaradt.

Ön ismeri a tervezés során elkerülendő 10 legnagyobb hibát? Tudja, hogyan lehet a hűtési teljesítményt további ráfordítás nélkül növelni?

Ezekre, és számos más adatközpontokkal kapcsolatos kérdésre talál választ legújabb tanulmányainkban. Használja fel Ön is kutatásaink eredményeit, hogy cégének pénzt, magának pedig elkerülhető problémákat takarítson meg.

Töltse le az APC ingyenes tanulmányát az elkövetkezendő 30 napban és lehetősége lesz nyerni egy iPad™ készüléket!

Látogasson el a www.apc.com/promo weboldalra és írja be a következő kódot: 76649v Tel 06 40 200 262 • e-mail apchutech@apcc.com

APC™ by Schneider Electric

©2010 Schneider Electric, minden jog fenntartva. A Schneider Electric és az APC védjegyek tulajdonosa a Schneider Electric vagy az USA-ban és más országokban lévő leányvállalatai. Minden egyéb védjegy a tulajdonosa kizárólagos birtokában áll. HU APC by Schneider Electric, 1117 Budapest Hauszmann Alajos u. 3/B. HUNGARY APC3F6EF_HU_B