e-CRIME

A globális üzleti világ tapasztalataiból ítélve a cyberbűnözők aggasztó mértékben veszélyeztetik a vállalatok működését. 14. oldal

MOBILITÁS

A mobilitás komoly kihívás a vállalatok IT-részlegeinek: nehezebb megvédeniük a határkörükből kikerülő eszközöket. 21. oldal

395 forint

SZÁMÍTÁSTECHNIKA

ICT-STRATÉGIA DÖNTÉSHOZÓKNAK • WWW.COMPUTERWORLD.HU
ALAPÍTVA 1969 • 2009. ÁPRILIS 28. • XL. ÉVFOLYAM 18. SZÁM

IDG Communications HUNGARY

COMPUTERWORLD

Az együttműködés képessége

A felhasználó a hálózatból most sem lát többet, mint tegnap, ám közben a hálózati rendszerekben mégis óriási változás zajlott és zajlik. Ez a változás közel sem csak kvantitatív (gyorsabbak lettek), hanem kvalitatív is: új tudás, új jellemzők jelentek meg a hálózat aktív elemeiben. Helyzetjelentés a hálózati eszközökről.

Összeállításunk a 8-11. oldalon

9 770587 151006 09018

TARTALOM

AKTUÁLIS

FÓKUSZ

ÜZLET

TECHNOLÓGIA

HORIZONT

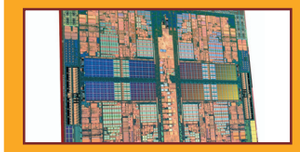
ÁLLANDÓ ROVATAINK

2009.04.28.

WWW.COMPUTERWORLD.HU

Olcsóbban telefonálhatunk külföldről

Júliustól ismét csökken az SMS roaming szolgáltatás díjszabása az EU-n belül, miután erről törvényt fogadott el szerdán az Európai Parlament. computerwold.hu/cikkek/sms-rom



Ambiciózus AMD-tervek

Az AMD az Opteron processzor hatodik születésnapján a következő két évet érintő terméktervéről beszélt. Komoly ambíciók, sok mag egyetlen processzorban. computerwold.hu/cikkek/amd-plan

Boldog születésnapot, Apple!

Egy francia fejlesztőcég olyan megoldással rukkolt elő, amelynek révén központosított, vállalati szintű virtualizált böngészés valósítható meg. computerwold.hu/cikkek/virtualweb

Megújuló IVSZ

Megválasztották az IVSZ új elnökségét. A tizenhat fős testület két évre szóló mandátumot kapott. A szövetség elnöke továbbra is *Keresztesi János*. computerwold.hu/cikkek/ivsz09

IMPRESSZUM COMPUTERWORLD-Számítástechnika
ICT-stratégia döntéshozóknak • alapítva 1969 • 2009. április 28. • XL. évfolyam 18. 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
Felelős kiadó Bíró István ügyvezető – ibiro@idg.hu
Lapigazgató Melovics Csaba – csmelovics@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 Csontos Péter – pcsontos@idg.hu
Főszerkesztő-helyettes Dervenkár István – idervenkar@idg.hu
Lapszerkesztő Barabás Balázs – bbarabas@idg.hu
Online-szerkesztő Tököli Gábor – gtokoli@idg.hu
Olvasószerkesztő, korrektor Sz. Erdős Judit – jerdos@idg.hu
Munkatársak Horváth Ádám – ahorvath@idg.hu
Kis Endre – ekis@idg.hu
Kodolányi Balázs – bkodolanyi@idg.hu
Makk Attila – amakk@idg.hu
Mozsik Tibor – tmozsik@idg.hu
Samu József – samu.jozsef@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 osztályvezető Radácsy Katalin – kradacsy@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
Rendezvényszervező Bödör Eszter – ebodor@idg.hu

Jogi közlemények
Szerkesztőségünk a kéziratokat lehetőségei szerint gondozza, de nem vállalja azok visszaküldését, megőrzését.

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 kézbesítőknél (06/80-444-4444; hirlapelofizetes@posta.hu, fax: 303-3440)
Előfizetési díj egy évre 15 720 forint, fél évre 7860 forint, negyed évre 3930 forint.
Lapunkat a MATESZ auditálja
Olvasóink szokásait a Nemzeti Médiaanalízis méri fel.
A Computerworld az IVSZ hivatalos médiapartnere.

Samu József
újságíró

Harcos, fejjel a homokban

Első fokon elítélték a Pirate Bay torrentoldal alapítóit – börtön néz ki nekik és pénzbüntetés. A hanglemez- és filmipar képviselői üdvözült mosollyal az arcukon ünnepelnek, miközben az oldal zavartalanul működik tovább. Most komolyan! Tényleg ennyire nem látják a fától az erdőt?!

Vajon milyen lehetett a nagy sarkantyúgyárak utolsó éve? Vagy azok a hónapok, mielőtt a papírgyárak leálltak a lyukkártyagyártással? Be kéne ültetni a nagy filmstúdiók és hanglemezkiadók embereit egy időgépbe, és visszaröpíteni őket ezekhez az eseményekhez, hátha rájönnek arra, hogy a hang- és mozgóképhordozó korongok sokkal inkább a közelmúltat képviselik, mintsem a jövőt. Merthogy más jelekből nem tűnnek tanulni.

Tavaly a HD DVD eltűnt a színről, a győztes pedig a Blu-ray lett, hip-hip hurrá! Ja, hogy azóta sem tudott a győzelmével mit kezdeni, és nem terjed el? Persze, egyfelől mert drágák a lejátszók, és pont mostanában jutott el a kiadók tudatáig, hogy a DVD-ből is akkor lett sláger, amikor az asztali lejátszók ára elérte a 100 dolláros szintet. Úgyhogy igyekszenek 99 dolláros eszközöket kifacsarni az elektronikai cégekből. Másfelől: a fejlett piacokon elérhetők a legálisan letölthető, HD-felbontású filmek, illetve a HD-felbontásban sugárzó fizetős kábelcsatornák. Ki a csuda akar lemezekért szaladgálni és akár drága, akár olcsó lejátszókat venni, ha fogja a meglévő laptopját, ráköti a tévéjére, és megnézi rajta a neki kedves sorozatot, talkshow-t, mozifilmet?! Sőt! Nem is biztos, hogy a laptopjával kell babrálnia! Az új generációs játékkonzolok HD-minőségben képesek filmeket lejátszani. Mind a Sony, mind a Microsoft kínál letölthető filmeket – az utóbbi még 14 nap után lejáró, kvázi kölcsönözhető néznivalót is kínál. Csak éppen nem nekünk! A mi piacunkat sem az Xbox Video Marketplace, sem a PlayStation Store nem szolgálja ki.

Csak nekem tűnik a képmutatás csúcsának, hogy a kiadók a „csak tiszta forrásból” szlogent kiabálják, közben meg nincs lehetőség arra, hogy kényelmesen, az internetről letölthető filmeket, játékokat vásároljunk hivatalosan? A PlayStation 3-tulajdonosok – de akik az agyonhypolt iTunes zene-, szoftver- és filmboltot szeretnék magyar állampolgárként hivatalosan használni, szintén hasonló cipőben járnak – kénytelenek térképről kinézett, amerikai címekre regisztrálni kamu felhasználókat, és próbálgatni, hogy a hazai bank által kibocsátott hitelkártyáikat megeszi-e a PlayStation Store, amit meg értelemszerűen azért akarnak használni, hogy ott vásárolhassanak, azaz ott pénzt költhessenek el. Ők valóban pénzt akarnak elkölteni, csak éppen nem szolgálják ki őket! Persze azzal, hogy nem létező amerikaiak nevében regisztrálnak, máris nem jogtiszta az, amit vásároltak. Igazi 22-es csapdája, amit csak úgy lehet kikerülni, hogy az online vásárlás helyett vehetnek lényegesen drágábban filmeket és játékokat, fizikai adathordozó korongokon. Hú, de jól jártunk!

Kedves kiadók! Tessenek már észrevenni, hogy az emberek rákaptak a letölthető tartalmakra, mert kényelmesek. Nem kell értük elmenni a nem is biztos, hogy olyan közeli plázába, ott vannak kényelmes, pár kattintásnyi távolságra a neten. Ha az illegális letöltéssel kaptak rá, hát azzal, de ez mit sem változtat azon, hogy jelenleg Magyarországról hivatalosan, jogtisztán elérhető, HD-filmek letöltését lehetővé tévő internetes forrás nincs. (Zene téren nem ilyen reménytelen a hazai helyzet, létezik DRM-mentes forrás, de hogy az árképzésük hogyan viszonyul az iTunes 0,69, 0,99, 1,29 dolláros dalonkénti árához, illetve az ott meglelhető tartalmakkal mennyire versenyképes vagy sem a kínálat, az már más kérdés.)

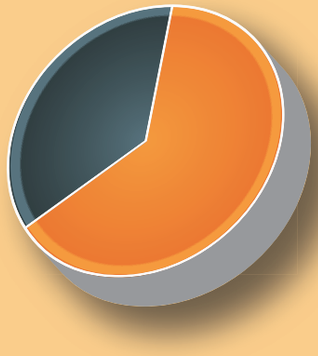
Remek ötlet volt ez a harc a Pirate Bay ellen! Ha hosszú pereskedés árán – ugye világos, hogy az első fordulón vagyunk csak túl, az ítélet nem jogerős és az egész ügy nyilvánvalóan évekig húzódik majd? – el is érnék, hogy bezárjon az oldal, akkor is számtalan alternatíva marad. Btjunkie, Mininova, Torrenthound, Seedpeer, Btmon, Fenopy, Monova – csak hogy az első párat említsem, amit egy kereső kiköpött. Addig, amíg a per zajlik – főleg most az ítélettel – meg csodás, ingyen reklámot tetszettek csinálni a vidáman működő oldalnak. Telitalálat!

Változnak az idők, változnak a felhasználók, a fentebb citált, működő példáknál nem kell jobb ennek alátámasztására. De mindaddig, amíg a világ nagyobbik felét nem szolgálják ki jogtiszta letölthető tartalommal, addig felesleges erőfeszítés az amúgy is ezerfejű, minden leszegett helyébe újat növesztő sárkány lenyakazása.

> *Az emberek rákaptak a letölthető tartalmakra...*

Olvasóink szerint...

Előző lapszámunkban a válságból való kilábalás lehetőségeivel foglalkoztunk, valamint azzal, hogy válsághelyzetben miként változik a piacot meghatározó cégek felelőssége a felhasználókkal szemben. Ezzel kapcsolatban megkérdeztük olvasóinktól, hogy szerintük képesek lesznek-e az egymással versengő nagy világcégek kooperálni a válság túlélése céljából.



- Nem, mert megpróbálják kihasználni a helyzetet konkurenseik piacról történő kiszorítására vagy bekebelezésére (64%)
- Igen, mert így csökkenthetik a válság okozta veszteségeiket (36%)

Az e heti véleményről a computerworld.hu/cikkek/velemeny0918 weboldalon szavazhatnak.

Hyde Tech Corner

Ismét felkértük a hazai IT-szektor három személyiségét, hogy kommentálja a közelmúlt híreit, eseményeit.

[Összeállította: Barabás Balázs]

Összeállításunkból kiderül, hogy a hordozható számítógépek helyét lassan átveszik az okostelefonok, továbbá, hogy mekkora veszteséget okoz mindannyiunknak minden egyes kéretlen levél, és arra is fény derül, hogy lehet-e összefüggés a Skype és a Pirate Bay között.

Kalózok–Pandúrok: sok-egy
A Pirate Bay torrentoldal alapítói ellen indított perben elítélték a kalózokat. A pandúrok nyerték ezt a fordulót, az ítélet nem jogerős.
computerworld.hu/cikkek/pirbay

Suhajda Attila
elnök
Magyar Outsourcing Szövetség

SUHAJDA ATTILA ELNÖK, MAGYAR OUTSOURCING SZÖVETSÉG

Új és szélesebb alapokra kell helyezni az értékesítési csatornákat. Érdekes lenne annak vizsgálata is, hogy az illegálisan, saját használatra letöltött tartalmak hány százalékát vásárolják meg aztán legálisan is, ha az adott szoftver például beválik, vagy a zenét igazán jó minőségben akarják hallgatni. Úgy vélem, a mai világban, amikor szinte elmerülünk a ránk zúduló információkban, egyre nehezebb megtalálni a számunkra tetsző, értékes tartalmakat, legyen az zene vagy éppen egy jó kis program. Ha megtalálásához, kipróbálásához néhány kattintásnál több időre van szükség, a legtöbb ember soha nem is fogja megnézni. Ezért aztán ezek a fájlcserélő, letöltő szájtok végső soron az ismertség és az ismertté válás egyik fontos csatornájává is váltak. Ki kell találni azokat az új értékesítési formákat, amelyek a sok kicsi sokra megy elve alapján juttatják bevételhez a jogtulajdonosokat, szemben a jelenlegi 1 eladott termék utáni drágább jogdíj modellel.

Tudomásul kell vennünk, hogy a világ globalizálódott, annak minden előnyével és hátrányával. Ugyanakkor a globális piac hatalmas lehetőségeket is rejt magában, de a sikerhez reális helyzetértékelésre és innovatív ötletekre van szükség. Ezért nem értem például az adathordozók árát növelő Artisjus-sarcot itthon, mert ennek az lesz az eredménye, hogy aki teheti, külföldről fogja ezeket megrendelni. Vagy nézzünk egy másik példát, a telefontársaságokat. Milyen szép kerek bevételre tettek szert monopóliumaik révén! Aztán jött a Skype, és ki gondolta volna, hogy a világ legnagyobb ügyfélkörrel rendelkező telefonszolgáltatójává válik pár év alatt? Azért persze a telefontársaságok is megvannak, igaz, rákényszerültek üzleti modelljük átalakítására. Véleményem szerint ez vár a tartalomszolgáltatókra is. Ezt a csatát lehet, hogy megnyerik, de a háború már eldőlt.

Jól fogynak a laptopok
A globális fogyasztói elektronikai piac növekedését három termékkategória, a mobil- és okostelefonok, az LCD TV-k és a laptopok generálták 2008-ban.
computerworld.hu/cikkek/tce09

ANDERS JENSEN VEZÉRIGAZGATÓ, PANNON

A gazdasági válság hatása kettős: egyrészt valóban csökkenti a növekedést, másrészt a költségkímélő megoldások előtérbe kerülésének hatására új fejlesztéseket is eredményez. Elmondható, hogy az elektronikai termékek esetén is megfigyelhető, hogy a felhasználóknak igényük van a mobilitásra, és a számítógépek piacán is elértük azt a pontot, amikor több hordozható eszköz fogy, mint asztali. Ebben a trendben fontos szerepe van a mobil széles sávnak is, aminek segítségével a felhasználók gyakorlatilag bárhol és bármikor kapcsolódhatnak a világhálóhoz.

A mobilpiacon a növekvő okostelefon-arány is fontos trend. Habár az okostelefonok többnyire nagyobbak egy átlagos telefonnál, a legkisebb hordozható számítógépnek számítanak: szinte minden funkció elérhető róluk, amire az embereknek menet közben szükségük lehet, legyen szó e-mailről, egy fontos információ weben való megkereséséről, vagy akár a szórakozásról.

Anders Jensen
vezérigazgató
Pannon

Óvni kell az e-mail címeket!
Büntethető lesz az e-mail címekkel való kereskedelem. *Jóri András* adatvédelmi biztos a Büntető Törvénykönyv módosítását kezdeményezte.
computerworld.hu/cikkek/btkemail

Gacsal József
üzletfejlesztési igazgató
Intel Hungary

GACSAL JÓZSEF ÜZLETFEJLESZTÉSI IGAZGATÓ, INTEL HUNGARY

A minden levelesládát elöntő spam nem csak azzal okoz kárt, hogy feleslegesen bosszantja és fárasztja a felhasználókat, szakembereket. A világnak az ilyen forgalom továbbítása és szűrése is komoly költségeket okoz. Egy számítás szerint minden egyes kéretlen levél mindennel együtt (felhasznált energia, szoftver, munkaerő) kb. 30 dollárcentünkbe kerül. Ezenfelül foglalja a sávszélességet is, ami vissza nem hozható veszteség.

Ma a világ szervereinek kb. 80 százaléka Intel-alapú, tehát joggal érezzük a felelősségünket, hisz az internetes spam forgalma is nyilván ezeken a kiszolgálókon nyugszik. A mi becslésünk szerint ma a működésben lévő kiszolgálók 40 százaléka egymagos, 40 százaléka kétmagos és mindössze 20 százaléka négy- vagy többmagos processzorokat használ. A most megjelent Xeon 5500-as sorozat tagjai átlagosan 50 százalékkal kevesebbet fogyasztanak az előző nemzedéknél. Közben legalább 200 százalékos teljesítménynövekedést várhatunk tőlük. Azt mondhatjuk, hogy átlagosan 9 darab régi 2005-ös szerver helyett csak egy újat kell üzembe helyezni. Így minimálisan 8 hónapos megtérüléssel számolhatunk, ami még a mai körülmények között is megfontolandó befektetés, ha valamit tenni akarunk a helyzet javítása érdekében. Talán valamit visszahozhatunk abból, amit a spammerek elvesznek tőlünk.

HÍRMOZAIK

A Ciscóé a Tidal

A Cisco Systems felvásárolja a Tidal Software nevű vállalatot, amely intelligens alkalmazásfelügyeleti és automatizálási megoldások fejlesztésével foglalkozik. A Tidal Software megoldásai a szerverektől a hálózaton át a munkaállomásokig terjedő költséghatékony felügyeletet biztosítanak az alkalmazások teljesítményének gyors, pontos és automatikus szabályozásával. A megállapodás értelmében a Cisco megközelítőleg 105 millió dollárt fizet a Tidal Software cégért.

ENIAC ERP hosting

Segíthetik a vállalatok háttérrendszereinek automatizálását az ERP-rendszerek. Az ENIAC ehhez kínál teljes szolgáltatáscsomagot: egyrészt biztosítja az OMF szoftver bevezetését, másrészt annak hostingját is. A mostani, válságoktól terhes piaci környezetben szinte minden cégnél a költséghatékonyságot elősegítő megoldások kerülnek előtérbe, segítségükkel a cégek egyrészt pénzt tudnak megtakarítani, másrészt energiát átcsoportosítani bevételszerző tevékenységeikre. Egy jól felépített ERP-rendszerben mindkét dolog elérhető. A hosting szolgáltatás keretében igénybe vett ERP-rendszerrel pedig tovább csökkenthetők a költségek, mert nem kell foglalkozni a drága és folyamatos fejlesztést igénylő szerverek üzemeltetésével.

Synergon az Invitelnél

Az Invitel Zrt. legújabb adatközpontjának teljes aktív és passzív hálózati infrastruktúra kialakítására tendert írtak ki, amelynek győztese, a Synergon valósította meg az Invitel 2009. évi legnagyobb informatikai beruházásának első fázisát. A projekt értéke meghaladja a 100 millió forintot. A megbízás keretében a Synergon Rendszerintegrátor – Magyarországon elsőként – a Cisco célmegoldásaival, a Nexus 7000 és a Nexus 5000 termékek alkalmazásával alakította ki az Invitel adatközpontját, illetve a befogadó épület teljes strukturált kábelezését.

Mindenki elégedett

Barabás Balázs ▪ 7,4 milliárd dollárt fizet készpénzben a Sun részvényeiért az Oracle, vagy 5,6 milliárdot és az adósságait is átvállalja. Bár korábban is felmerült, hogy az Oracle megvenné a Sunt, ez a lehetőség először nem tűnt komolynak, mert az Oracle – a HP-vel közösen kifejlesztett Exadata tárolószervert leszámítva – eddig még nem lépett be a hardverpiacra. A megegyezést követően azonban a Sun hátterével az Oracle ezen a piacon is komoly pozíciókat szerezhet magának.

Az Oracle–Sun egyesülés kapcsán már megszülettek az elemzések, feltételezések: mindenki jól járt, de lehet, hogy a dolgozók kevésbé. Az egyesülést bejelentő hír után kiadott közleményben *Safra Catz*, az Oracle elnöke úgy fogalmazott, hogy a következő pénzügyi évben a tranzakció másfél milliárd dollárral növelheti a vállalat pénzügyi eredményeit, míg a második évben az összeg elérheti a 2 milliárdot. Ez azt jelenti, hogy az üzlet nagyobb nyereséget hoz az Oracle-nek, mint a BEA-, PeopleSoft- és a Siebel-felvásárlások együttvéve. A Sanford C. Bernstein elemző cég kutatója szerint ez a nyereség reális lehet, de csak nagyarányú leépítésekkel. Számításai szerint ugyanis a 2010-es pénzügyi évben a Sun nyeresége 800 millió dollár körül lesz, szemben az Oracle által említett 1,5 milliárddal. A hiányzó 700 milliót csak úgy lehet kigazdálkodni, ha legalább 5500, de inkább 10 ezer embert elbocsátanak (időzítéstől függően). A Sunnál jelenleg is létszámleépítés van folyamatban, ami a dolgozók 15–18 százalékát érinti.

Az IBM ugyanakkor csöppet sem bánkódik a Sun elvesztése miatt. Habár az első negyedéves eredményei 11 százalékos árbevétel-csökkenést mutatnak az előző év azonos időszakhoz képest, az 1,70 dolláros részvényenkénti nyereség 4 százalékos növekedést jelent 2008 első negyedévéhez képest. Az egyesülő cégektől sem tart az IBM. Mint *Mark Loughridge*, a vállalat pénzügyi vezetője nyilatkozta: „Ha rágondolok, és azt kérdezem magamtól, hogy alapvetően mi változott ezzel, akkor semmi sem jut eszembe." Loughridge hozzátette: „Ez ugyanaz a két csapat, amelyekkel eddig is versenyeztünk, és mindig is nyertünk."

„1,5 milliárd dollárral növelheti az Oracle eredményeit a Sun-akvizíció már a következő évben..."

Safra Catz
ORACLE

Ha az Oracle és a Sun felől érkező korábbi támadásokat vesszük alapul, akkor az IBM mellett egy másik cég is aggódhatna az egyesülés miatt, mégpedig a Microsoft. Ennek ellenére az elemzők inkább arra számítanak, hogy ez jót fog tenni a redmondi vállalatnak. Érvelésük szerint ugyanis, ha az Oracle ezután rendszerszállítóvá pozicionálja át magát, akkor ez arra kényszerítheti a nagyobb hardvergyártókat, például a Dellt vagy a HP-t, hogy erősítsék együttműködésüket a Microsofttal. A HP eddig az Oracle egyik legnagyobb partnere volt, de miután az Oracle mostantól egyben hardverszállító is lesz, a HP feltehetően alternatívákat fog keresni az Oracle-lel szemben. A Microsoftnak az is kapóra jön, hogy miután a Sun korábban felvásárolta a MySQL-t, és az most az Oracle-é lesz, a továbbiakban eggyel csökken adatbázisszállító konkurenseinek száma.

ESEMÉNY-NAPTÁR

Április 28–29. BUDAPEST
Korszerű Közigazgatás. (Köz)-adatok aranykalitkában. Adatvédelem – Információszabadság – Információbiztonság
WWW.IIR-HUNGARY.HU

Április 29. BUDAPEST
DigitalFestival09
WWW.DIGITALFESTIVAL.HU

Április 30. BUDAPEST
Game Developers Forum 2009
WWW.GDF-HU.COM

Május 1–3. BUDAPEST
9th BME International 24-hour Programming Contest
WWW.CHALLENGE24.ORG/2009/

Május 5. BUDAPEST
Adattárház Fórum 2009
WWW.ADATTARHAZFORUM.HU

Internethajó – tizedszer

Computerworld.hu ▪ Immár tizedik alkalommal indul útjára a Dunán az Internethajó. A jubileumi Internethajó idén is a döntéshozók közös vitafórumát teremti meg, egy korszakhatárt nyitó nemzeti programmal, a Nemzeti Digitális Közművel kapcsolatban. Az „Átstartolás! – Nemzeti Digitális Közmű" mottó alatt induló rendezvényen a szervezők a tavalyihoz hasonlóan ismét nagy érdeklődésre számítanak. Szakértők szerint a Nemzeti Digitális Közmű program – amennyiben tényleg elindul – felbecsülhetetlen előnyöket jelenthet Magyarországnak. A Nemzeti Digitális Közmű a legkorszerűbb, optikai összeköttetésen alapuló informatikai infrastruktúra lenne Magyarországon, amely a legkisebb településekre is elvinné az internet előnyeit. Az ezzel kapcsolatos részletek megbeszélésére kerül sor az Internethajón, ahol a szakmai vezetők értékelik közösen a helyzetet.

A dunai hajózással egybekötött, az informatika fontos kérdéseit érintő jubileumi rendezvényen a központi témát kormányzati, e-közigazgatási, piaci szempontból érintett szereplők vitatják meg kerekasztal-beszélgetések formájában. A meghívottak között szerepel többek között *Bálint Ákos*, a Nemzeti Fejlesztési Ügynökség főigazgatója, *Bódi Gábor*, az Elektronikuskormányzat-központ szakállamtitkára, *Paál Péter*, az IBM Magyarországi Kft. vezérigazgatója és *Maradi István*, a Magyar Telekom műszaki vezérigazgató-helyettese.

Az esemény előtt a szervezők – immár negyedik alkalommal – ismét kiadják a Kék Noteszt. Az információs társadalom éves helyzetjelentése várhatóan áprilisban jelenik meg – áll a szervező cég, az eWorld közleményében.

Felhő a dobozban

A HP a szervereket, a tárolórendszereket és a hálózati eszközöket, valamint a felügyeletüket segítő szoftvert egységbe foglaló, konvergens platformot jelentett be, amellyel a szolgáltatások automatizálhatók az adatközpontokban. [Írta: Kis Endre]

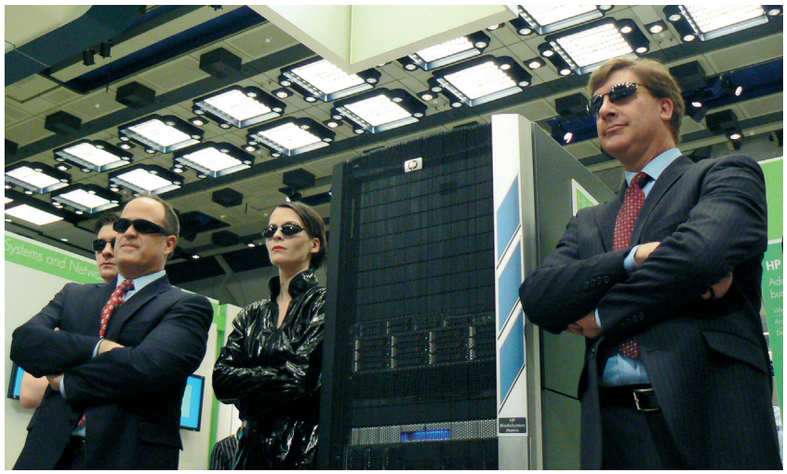
A HP BladeSystem Matrix platform a gyártó múlt héten megrendezett *Technology@Work 2009* kiállításán mutatkozott be Berlinben. A rackszekrényben érkező megoldás részét képező Orchestration Environment egységes managementfelületet biztosít az alkalmazás-infrastruktúra rendkívül gyors tervezéséhez, konfigurálásához, üzemeltetéséhez és optimalizálásához. Ez a platform lehetővé teszi, hogy a vállalat a meglévő fizikai erőforrásait zökkenőmentesen összekapcsolja a virtualizált erőforrásokkal, és a teljes környezetet ugyanarról a felületről menedzselje.

Ebben a felügyeleti környezetben – ahogyan azt a HP a kiállításon demonstrálta – a vállalat előre konfigurált virtuális gépeket talál, illetve ilyeneket maga is egyszerűen, *húzd és ejtsd* módszerrel létrehozhat. Ezek a gépek adott feldolgozási teljesítményt, tárolókapacitást, sávszélességet tartalmaznak. Konfigurálásukat az OE azzal is segíti, hogy grafikus felületen jelzi, milyen fizikai erőforrások érhetők el, illetve azt is, ha az igények lefedéséhez újabb kapacitás beszerzése és beüzemelése szükséges. A menedzsment megoldás arra is lehetőséget ad, hogy az IT-igazgató a virtuális gépet adott időre bocsássa valamely alkalmazás vagy a fejlesztés, tesztelés rendelkezésére. A határidő leteltével az OE ezeket a virtuális gépeket automatikusan visszavezeti, és visszahelyezi az elérhető erőforrások közé. Mindez jelentősen megkönnyítheti az erőforrások használatával járó költségek követését és elszámolását a vállalaton belül.

ALKALMAZÁS-INFRASTRUKTÚRA PERCEK ALATT

Az OE-ben előkonfigurált virtuális gépeknek köszönhetően, az üzleti igények lefedése rendkívüli módon felgyorsul. Az alkalmazás-infrastruktúra a konferencián bemutatott példa – egy többrétegű architektúrára épülő e-kereskedelmi alkalmazás bevezetése – alapján mindössze 108 perc alatt felállítható, míg ez a hagyományos módszerekkel 33 napot venne igénybe. Ezért a dobozban érkező vagy vállalaton belüli Mátrix privát felhőként is értelmezhető, amely házon belül is a *cloud computing* szolgáltatásait, gyors és rugalmas erőforrás-hozzárendelését kínálja. Mindez a vállalati IT-erőforrások jobb hasznosítását eredményezi, ami a beruházások és az üzemeltetés terén is nagyobb költséghatékonyságot ad.

A HP saját számításai szerint – amelyeket 320 darab, rackszekrénybe szerelt szerver BladeSystem Matrix környezetbe történt konszolidálása alapján végzett – a vállalatok a platform bevezetésével három évre vetítve 78 százalékkal csökkenthetik a birtoklás összköltségeit (TCO), és 323 százalékos megtérülést érhetnek el beruházásukon (ROI). A hagyományos kialakítású IT-környezethez képest a BladeSystem Matrix bevezetési költségei 40 százalékkal alacsonyabbak, míg az energiafogyasztással és a hűtéssel összefüggő költségek 92 százalékkal is kisebbek lehetnek. A platform beszerzési ára így mindössze 8 hónap alatt megtérülhet a vállalat számára.



HP BladeSystem Matrix: előkonfigurált virtuális gépek – kattintásra

A Matrix kapcsán a HP olyan alkalmazásszállító partnerekkel is együttműködik, mint a Microsoft, az Oracle és az SAP annak érdekében, hogy a platformon előkonfigurált virtuális gépek minél jobban illeszkedjenek a vállalatok által használt alkalmazásokhoz, az azok által kiszolgált folyamatokhoz. A Matrix beszerzési ára egyébként teljes körű projektmenedzsment támogatást, valamint egyéves, napi 24 órás, heti hétnapos műszaki támogatást is tartalmaz, amely 4 órás válaszidőt garantál a felhasználóknak.

SZOLGÁLTATÁSALAPÚ VÁLLALATI INFORMATIKA

A HP szerint a jövőben a vállalatok az üzleti informatika valamennyi komponensét szolgáltatás formájában fogják használni. Ehhez az infrastruktúra olyan mértékű szabványosítása és megnyitása, automatizált felügyelet szükséges, amilyet a BladeSystem Matrix platform is kínál. *Francesco Serafini*, a HP technológiai szolgáltatások csoportjának (TSG) európai, közel-keleti és afrikai regionális igazgatója kérdésünkre elmondta, hogy a most bemutatott megoldások az eredetileg 2005-ben bejelentett adaptív infrastruktúra portfólió természetes továbbfejlődését képviselik, de a jelenlegi gazdasági körülmények között még kifejezettebb felhasználói igényekre válaszolnak. Serafini szerint a továbbiakban különösen a kis- és középvállalatok körében terjedhet gyorsan az IT-szolgáltatások használata. A nagyvállalatokra ma még inkább jellemző, hogy informatikai környezetüket sokkal inkább egyedi igényeik szerint alakítják. A jelenlegi gazdasági körülmények között azonban nyomós érvek szólnak amellett, hogy ezek a szervezetek is mindinkább szabványosítsanak, és IT-szolgáltatásokat vegyenek igénybe házon belüli vagy külső szolgáltatótól. Maga a HP is átalakította saját IT-infrastruktúráját ebben a szellemben, és számos nagy ügyfelének is ad szolgáltatásokat a létrehozott adatközpontokból. Ez a terület a cégen belül várhatóan egyre dinamikusabban fog bővülni, összekapcsolva az ügyfeleknél kialakított fizikai és virtualizált erőforrásokat a HP által adott szolgáltatásokkal.

A kiállításon tartott nyitó előadásában *Ann Livermore* alelnök, a HP TSG vezetője is utalt arra, hogy ez a divízió már jelenleg is akkora, több mint 40 milliárd dolláros éves bevételt hoz, mint a vállalat PC üzletága, megelőzve a nyomtatókat fejlesztő és értékesítő divíziót, amely a másik, hagyományosan erős terület a gyártó portfóliójában. Livermore azt is kiemelte, hogy a világon értékesített szerverek közül minden harmadik a HP terméke. Ezt a kompetenciát a cég az adatközpont- és hálózatfelügyeleti, valamint alkalmazáskihelyezési szolgáltatásokat adó EDS tavaly májusi felvásárlásával erősítette. Az akvizíció a világ második legnagyobb IT-szolgáltatójává tette a HP-t, amely a múlt év októberében a tárolórendszerek virtualizálása és az iSCSI SAN technológia terén élenjáró LeftHand Networks nevű céget is felvásárolta. Mindehhez a gyártó meglévő System Insight Manager rendszerfelügyeleti megoldását a virtualizálás és automatizálás irányában fejlesztette tovább – és ezzel előállt az adaptív infrastruktúra következő nemzedékét képviselő megoldások valamennyi eleme.

Duncan Campbell, a HP TSG-csoportjának adaptív infrastruktúráért felelős alelnöke kérdésünkre elmondta, hogy a gyártó olyan eszközöket is kifejlesztett, amelyekkel fel tudja mérni, hogy egy vállalat informatikai környezete mennyire képes rugalmasan, gyorsan és költséghatékony módon reagálni a változásokra. A HP tanácsadói az eredmények alapján segítenek kijelölni a továbbfejlesztés irányát és lépéseit, ezek mentén a vállalat meglévő rendszereinek integrálásával fokozatosan is áttérhet a virtualizált erőforrásokra épülő IT-szolgáltatások használatára.

A tárolórendszerek tankhajója

A BladeSystem Matrix mellett a HP olyan tárolómegoldásokat is bemutatott Berlinben, amelyekkel a vállalatok nagyobb adatsűrűséget és költséghatékonyabb üzemeltetést érhetnek el.
A HP LeftHand P4000 – szabványos x86-alapú SAN-megoldás, amely a hagyományos, Fibre Channel-alapú hálózati tárolórendszerekhez képest 33 százalékkal jobb kapacitáshasznosítást és 50 százalékkal alacsonyabb üzemeltetési költséget kínál.
A LeftHand Virtual SAN Appliance segítségével pedig a vállalatok egyetlen virtualizált tárolómegoldássá szervezhetik az IT-környezetükben meglévő, közvetlen csatlakozású (DAS) tárolórendszereiket.
A Tanker becenevű HP StorageWorks MDS 600-as pedig olyan sorosan kapcsolt SCSI (SAS) moduláris diszkrendszer, amellyel maximum 100 merevlemez is adott szerverhez rendelhető. Ezzel a megoldással a hagyományos DAS tárolórendszerekhez képest 230-szor nagyobb adatsűrűség és 70 százalékos költségcsökkenés érhető el.

CÉL: az együttműködő képesség

Noha a felhasználók számára a hálózat ma is olyan, mint tegnap volt vagy pár éve, a hálózatok alapjául szolgáló eszközök sokat változtak. Ez nemcsak kvalitatív változás (gyorsabbak lettek), hanem kvantitatív is, új tudás, új jellemzők jelentek meg bennük. [Írta: Makk Attila]

Megjelenésükkor nem szoktak nagy nyilvánosságot kapni az új hálózati eszközök, még egy-egy vírus is fényesebb karriert fut be – legalábbis ami a sajtóvisszhangot illeti. Pedig az alapvető hálózati megoldások az utóbbi években többször is jelentős változásokon mentek át, különösen, ha visszatekintünk az első időkre. A hálózatok által kínált lehetőségek is jelentősen megváltoztak. Ezzel nemcsak a hálózatok tervezőinek, üzemeltetőinek kellene tisztában lenniük, hanem a cégek vezetésének is. Hiszen a jól megválasztott hálózati eszközök hosszabb távon is segítik az adott vállalat fejlődését, mivel az egyes alkalmazások, szolgáltatások új beruházás nélkül vagy minimális ráfordítással megvalósíthatók. A lehetőségek ismeretében el tudjuk kerülni a felesleges beruházásokat.

A gyakorlatból rengeteg példát lehet sorolni: **ha megvesszük az első kezünk ügyébe akadó hálózati kapcsolót, lehet akármilyen olcsó vagy éppen drága, közel sem biztos, hogy hosszabb távon megfelel;** ha később IP-kamerákat szeretnénk üzemeltetni róla, esetleg vezeték nélküli hálózat hozzáférési pontjait, akkor PoE-képes kapcsoló kell. Ha beszerzéskor erre nem figyeltünk, nem gondoltunk, akkor vagy újabb felesleges költségekbe verjük magunkat, vagy kerülő megoldást választunk. Hasonlóképpen buktató lehet a VLAN-ok kezelésének hiánya. Esetleg a hálózat bővülésekor szembesülünk azzal, hogy kell még kapcsoló, de a vásárolt típusból többet nem lehet egy komplexummá összekötni – tehát vagy a hálózat struktúrájával alkuszunk meg, vagy újra fizetünk.

A QoS-képesség, amikor a forgalom jellege szerint egyes késleltetésre érzékeny típusok előnyt élveznek (videó, hang) is jól jön, ha hangot, képet kell továbbítani. A hálózati eszközök sok fajtájának számtalan tulajdonsága van, és mivel ezen eszközöknek együtt kell működniük, lehetőség szerint együtt is kell kiválasztani őket. Ha ez nem megy, akkor legalábbis valami stratégiát kell alkotni, aminek mentén az új beszerzések megvalósíthatók. Ekkor nem fordul elő, hogy egy új eszköznek hiába van valamilyen ügyes funkciója, a többivel nem képes együttműködni.

Hogy egy hálózat tervezésénél mire érdemes figyelni, annak összefoglalása nem férne jelen cikk terjedelmébe. Ezért felvázoljuk, hogy ma a számítógépes hálózatok terén mi a helyzet, milyen irányban folynak a fejlesztések, milyen jellegű termékek várhatók. Talán kissé önkényesen, de az egyszerűbb áttekinthetőség miatt négy területre osztottuk a hálózatokat: 1. vezeték nélküli megoldások, 2. hagyományos tűzfalak – ide vettük az ezeket felváltó, felváltani kívánó megoldásokat is, 3. hagyományos hálózati eszközök, 4. új, főleg az összetett hálózatok által megkívánt felügyeleti, elemző eszközök.

VEZETÉK NÉLKÜLI HÁLÓZATOK

Ezekre nagyon nagy igény volt, ám megjelenésükkel igen sok problémát is előhoztak. A két legnagyobb közülük a sávszélesség – ami soha nem elég, a vezetékes hálózatoknál sem –, illetve a biztonság. Otthoni vagy korlátozott használatra a jelenlegi 802.11b és 802.11g szabványú eszközök is alkalmasak, ám nagy tételben vállalati, különösen nagyvállalati alkalmazásra már nem.

A 802.11n szabványnak már létezik egy piszkozata (vázlata); bár az IEEE – mai ismereteink szerint – csak 2010 januárjában véglegesíti. A 802.11n szabványú hálózat 54 megabit/s sávszélességtől 600 megabit/s-ig lesz használható. (Ezek a sávszélességre vonatkozó adatok persze kicsit csalókák, mert a sávszélességből elég sokat lefoglalnak maguk a hálózati eszközök, a felhasználó számára a TCP/IP kapcsolat sávszélessége jóval kisebb.)

Noha a szabvány még nincs kész, többen gyártanak már 11n szabvány szerint működő hálózati eszközöket. Ezeket a Wi-Fi Alliance 2007 óta minősíti, hogy megfelelnek-e a 802.11n szabvány jelenleg élő tervezetének. Tehát nem arról van szó, hogy a szabványtól teljesen elrugaszkodott eszközöket gyártanának.

A vezeték nélküli hálózat eszközeit sokan gyártják, de van egy másik irányzat is, amely a vezeték nélküli hálózatok felügyeleti és biztonsági problémáira is megoldást kíván adni. Ezek a gyártók teljes rendszert kínálnak, hardvert és szoftvert egyaránt. Ilyen termékcsaládja van például az Aruba Networksnak. A hozzáférési pontok vezérlését központilag felügyelik, így nagyon jól szabályozható, hogy hol ki férjen hozzá a hálózathoz, s aki hozzáfér, annak mit szabad – lehet – csinálnia. Ebben a struktúrában a felhasználó profilja követi a felhasz-

11n és antennák

A 11n szabványú készülékek az átvitelhez egyszerre több csatornát képesek használni: a MIMO-technológia (multiple input, multiple output) használatával az adatfolyam egyszerre két csatornában halad, mindegyiknek saját kódoló/dekódolója, saját adó- és vevőantennája van. Ezért a 11n készülékek drágábbak, mint a 11b/g szabványúak.

A 11n szabványú eszközök jele: a×b:c. Ahol az *a* az adóantennák számát jelenti, azazhogy hány csatornán tud adni, a *b* a vevőantennák száma, a *c* pedig azt jelenti, hogy az eszköz egyszerre hány adatfolyamot képes kezelni. Ma a 2×2:2; 2×3:2 és 3×3:2 készülékek kaphatók, a készülő szabvány 4×4:4-et is megenged.

nálót, ahol rácsatlakozik a hálózatra, akár vezeték nélkül is; és pontosan ugyanazok lesznek a jogai a hálózatban, mint bármelyik más ponton. A másik hasonló széles körű megoldást kínáló gyártó a Symbol, illetve most már az utóbbit megvásárló Motorola. Ők szintén teljes rendszert kínálnak – hozzáférési pontokat, s az azokat vezérlő központi eszközöket. Többen gyártanak 11n szabványú eszközt: Intel, D-Link, SMC, HP ProCurve, Cisco. Ezek előnye akkor használható ki, ha a teljes hálózat 802.11n szabványú eszközöket használ: a régiekkel kompatibilis, de akkor csak azon a sebességen, azokkal a képességekkel működik.

UTM-TŰZFALAK

A hagyományos tűzfalaknak volt néhány jó évük. Üstökösként robbantak be a hálózati piacra – mindenki megjelent saját tűzfalával, talán tucatnyi, kifejezetten tűzfal gyártására szakosodott új cég is felbukkant. Ma már minden gyártó kínál UTM-tűzfalakat (Unified Threat Management), amelyek több funkciót egyesítenek. A felépítés általában moduláris, azaz az egyes funkciók kikapcsolhatók, illetve külön licenc megvásárlása után kapcsolhatók be. A tűzfal (nevezzük határvédelemnek) funkció mellett VPN-végződtetésre, IDS/IPS feladatokra, webes tartalomszűrésre, URL-szűrésre, e-mail szűrésre, levélszemét detektálására, a forgalomban való víruskeresésre, illetve a tapasztalt események naplózására való képességekkel ruházzák fel az UTM-tűzfalakat. Ma már nagyon nehezen lehet kapni olyan vállalati kategóriába tartozó tűzfalat, amely ne kínálna a fentiek közül egyszerre több szolgáltatást is. **Nyilván nagyon praktikus, ha csak egy eszközt kell beszerezni, üzemeltetni –, de azért az is nyilvánvaló, hogy egy univerzális eszköz nem tudja a speciálisan egy-egy célra készített készülékkel annak területén felvenni a versenyt.** Ráadásul a fenti feladatok meglehetősen erőforrás-igényesek. Egy tavalyi tesztben az UTM-tűzfalak átlagos áteresztőképessége volt a vizsgálat tárgya *(lásd Legyen egy modullal több? – Computerworld 2008/17. szám)*. Ez igen jelentősen csökkent minden egyes újabb funkció aktiválása után – 25–30 százalékos csökkenés volt a legjobb érték.

Lényegében minden gyártó UTM-tűzfalakat kínál: a sebesség és a minőség megőrzése miatt egy-egy modult a terület szakértőjével készíttetnek el. Tipikusan ilyen a víruskereső rész, amelyek általában a jól ismert, víruskeresőket készítő cégek termékei. A webtartalomszűrésre a nagy mintával rendelkező szolgáltatókat használják.

Ezt a tendenciát jól mutatja, hogy az összes nagy és kisebb tűzfal gyártója UTM-eszközökkel jelent meg, régi, jó bevált termékvonalakat adtak föl emiatt. Jó példák erre a Cisco ASA (ami három termékvonalat szüntetett meg), a Juniper Netscreen készülékei, de a Fortinet, a Sonicwall és Checkpoint választékában is ilyen univerzális készülékek vannak. A kisebb gyártók is követik ezt az irányt: a Zyxel ZyWALL családjában is ilyen összetett eszközök találhatók, Kaspersky vírusvédelemmel, IDP-képességgel.

Mindenesetre ma még mindenképpen érdemes egyes feladatokra arra specializálódott eszközt használni: a VPN kezelését a határvédelem mellett az UTM-tűzfalak jól és hatékonyan végzik. Viszont a víruskeresés és az IDS/IPS működtetése erősen visszafogja a teljesítményüket. Spamszűrésben pedig egyelőre jobb, ha a speciálisan arra felkészített eszközöknél maradunk.

Ez az irányzat azt is jelenti, hogy **amit ma a tűzfalak piacának tekintünk, egyre szélesedik. Azok a gyártók, amelyek valamelyik területen erősek, ezen az UTM-piacon is meg tudnak majd jelenni:** valamiben erős eszközüket felvértezik más képességekkel. Például errefelé mutat a McAfee Content Security eszköze. Ez levél- és spamszűrésben, illetve a hálózatos forgalomban való víruskeresésben igen hatékony, proxyként is használható, ráadásul penge szerver kivitelben is kapható.

Úgy néz ki, hogy egyelőre az UTM-tűzfalak megmaradnak a hálózati forgalom hatékony kezelésénél (VPN, IDS/IPS stb.), és a víruskeresést, spamszűrést egy másik eszközcsalád fogja hatékonyan végezni. Várható, hogy a két fél közül (tűzfalak gyártói, illetve víruskeresők/spamszűrők készítői) egyik felvásárolja a másikat, így olyan eszközt alkothat, amely több funkciót is magas minőségben tud ellátni. Erre a technikai lehetőség megvan, inkább a gyártóknak hiányzik az egyik vagy a másik oldal tapasztalata.

ÚJ HÁLÓZATI ESZKÖZÖK

Időről időre megjelennek újfajta hálózati eszközök is. Régen a hub volt az egyetlen lehetőség egy hálózat kiterjesztésére – emlékszik ma már valaki ilyen eszközre? Hasonló az analóg modem, amely erősen kiveszőben van, szerepét átveszik a VPN-ek, saját vonalak.

Ugyanakkor a hálózatok igen nagy iramban bővülnek. Egyre több végpontot kezelnek, egyre több a számítógép, de újabb és újabb eszközök jelennek meg végpont szerepben: hálózati nyomtatók, lapolvasók, biztonsági eszközök (mozgásérzékelők, kamerák, beléptető rendszer eszközei stb.). Nemcsak a végpontok száma növekszik, hanem a forgalom is színesedik: ma már régen nem arról van szó, hogy egy-egy fájlt lemásolnak a hálózaton. Hang, videó, nyomtató adatfolyam, épületfelügyeleti eszközök jelei közlekednek ugyanazon a hálózaton. És mivel a felhasznált adatok értékesebbek lettek – károsodásuk, elvesztésük, illetéktelen kezekbe kerülésük a felhasználó cég számára komoly veszteséget jelent –, a különböző támadások is felértékelődtek. Egy régi struktúrában, ha leáll a belső hálózat, legfeljebb nem ment a netezés, esetleg leállt az elektronikus levelezés – amit amúgy is csak mellékesen használtak. Ha viszont ezen a hálózaton működik a telefon is, a faxok is itt jönnek-mennek, hálózati nyomtatókat használunk, esetleg még a kamerák és a beléptető rendszer is ezen keresztül működik, akkor a leállása megengedhetetlen.

Persze a hálózatok felügyelete a sokféle forgalom, a nagyszámú végpont miatt nem éppen egyszerű, ezért rengeteg eszközt készítettek ehhez – nagy (és kisebb) felügyeleti rendszereket, hiszen a nagy forgalmat figyelni, az eseményeket elemezni ma már nem lehet kézzel, miután a hatalmas adatmennyiségben könnyen elvész egy-egy rosszindulatú próbálkozás, gyanús jel. Ezért megjelentek azok az eszközök, amelyek a hálózat biztonságát hivatottak szavatolni, ezek folyamatosan figyelik a hálózati forgalmat – ide értendő a legszélesebb körű monitorozás – és gyakorlatilag azonnal képesek akár beavatkozni is. Talán azon utópisztikus közterületi kamerákhoz lehetne hasonlítani mindezt, amelyeken olyan szoftver fut, amely a képből képes kiszűrni a gyanús eseményeket.

Ezek az eszközök megkapják az aktív hálózati eszközök naplóit, a hálózati forgalmat figyelik, és így a hálózatra vonatkozóan minden pillanatban teljes képük van. Természetesen ilyen eszközt nem lehet úgy beilleszteni a hálózatba, mint egy egyszerű végpontot: a felügyelt eszközök naplóit rá kell irányítani, illetve látnia kell a hálózat forgalmát. Általában ez okozza a fejtörést, hiszen nehéz olyan pontot találni egy nagy hálózatban, ahol minden látható – ezért a gyakorlatban ezek a felügyeleti eszközök több ponton elhelyezett szenzorral működnek. Ezeket az eszközöket a SIEM (Secutrity Information and Event Management) névvel illetik.

Zöld D-Link

A D-Link régóta jelen van az otthoni és kisvállalati eszközök piacán, néhány éve piacvezető is volt a hálózati termékek piacán, majd a Wi-Fi termékek piacán is. Emellett komoly fejlesztésekbe kezdett, hogy a nagyobb vállalatok számára is megfelelő eszközöket kínáljon – már hazánkban is vannak olyan nagy hálózatok, amelyeket D-Link eszközökre építettek. A cég nagy hangsúlyt fektetett arra, hogy termékeiben maximálisan érvényesítse a környezetvédelmi követelményeket. Mind a kis, mind a nagy cégek számára kínál energiatakarékos hálózati eszközöket. A nagy választékot legutóbb április elején bővítették, amikor is a 16 portos felügyelhető gigabites kapcsolójuknak jelentették be az energiatakarékos változatát. A D-Link „zöld" hálózati eszközei a nem használt portok áramköreinek fogyasztását a minimumra csökkentik, a hűtést optimalizálják, hogy a feleslegesen működő ventilátor se fogyasszon áramot. Rövid hálózati kábelt használva a D-Link zöld eszközei kevesebb energiát használnak.
Jelenleg a D-Linknek teljes választéka van alacsony fogyasztású hálózati eszközökből: kapcsolók minden kategóriában, Wi-Fi eszközök, NAS-ok – és hamarosan megjelennek a Powerline hálózati adapterek zöld változatai is.

Ilyen eszköz a Cisco MARS naplóelemzője, a Juniper STRM – neve szerint Security Threat Response Manager –, a célt tekintve nagyon hasonló a Novell Sentinel, de ide sorolható a Mirage és a ProCurve felügyeleti szoftvere is. Mivel ezek viszonylag új, de mindenképpen kevéssé ismert eszközök, érdemes róluk, a lehetőségeikről néhány szót szólni.

JUNIPER STRM

A Juniper OEM-szerződés keretében jut ehhez az eszközhöz a fejlesztő Q1 Labstól. Az STRM hálózatba beillesztve képes figyelni a forgalmat. Ha megkapja az egyes eszközök naplóit (azaz hozzá irányítjuk a syslogot), valamint a hálózati eszközök Netflow adatait, akkor az azo-

kon történt eseményeket képes figyelni. Ezért **célszerű valami központi helyre telepíteni, a számunkra kritikus hálózati részek flow adatait ráirányítani.** Három méretben kapható, ezekben a fő különbség a másodpercenként feldolgozható események száma, ami 500-tól 10 000-ig terjed.

A beérkező adatokat rengeteg szempontból képes feldolgozni, a fenyegetéseket, rendellenes viselkedéseket felismeri. Itt elsősorban nem a letöltött állományokban és a megnyitott weboldalakon megbúvó vírusokra kell gondolni, mert ezek megtalálása és kiirtása más eszközök feladata, de persze a Juniper STRM ezekről az eseményekről is értesül a vírusirtók naplóiból. Inkább a hálózatban fellelhető anomáliákra, gyanús viselkedésekre kell gondolni, mondjuk egy végpont rövid időn belül többször megváltoztatja az IP-címét, adott végpontról jellegének (nyomtató, levelezőszerver, adatbázis-szerver...) nem megfelelő intenzív vagy a hálózatban nem engedélyezett forgalom észlelhető, mondjuk, videostream. Rengeteg előre gyártott szabály van, de létre lehet hozni saját szabályt is, hiszen elképzelhető, hogy egy hálózatban sajátos működésű, és ezért sajátos igényű eszközök vannak. Alapvetően természetesen a Juniper-termékek naplóállományait ismeri föl, azok forgalmi adatait kezeli, de több más hálózati eszköz adatait is képes értelmezni. A lista kicsit az Egyesült Államok IT-szakembereinek az ízlését tükrözi: azok az eszközök vannak benne, amelyeket a tengerentúlon nagy mennyiségben használnak, azért megtalálható benne többek között a Windows és Linux kiszolgálók naplóinak értelmezése is. Vegyes hálózati környezetben nem egyszerű beállítani, de ha már működik, gyors választ tesz lehetővé a hálózatban megjelenő gyanús eseményekre. Ez általában is igaz ezekre az eszközökre: a beállításuk nem megy automatikusan, hiszen hozzá kell szabni a saját felügyelt hálózathoz, és az igényekhez.

CISCO MARS

A Cisco MARS nagyon hasonlóan működik. Neve mozaikszó: Monitoring, Analysis, and Response System *(A MARS-ról korábban: Tudjuk, mit csináltak tavaly nyáron – Computerworld 2008/10. szám)*. A készülékre kell irányítani a különböző hálózati eszközök riportolását, amit az megemészt, és ha bizonyos események (a Cisco szóhasználatával *eventek)* együtt következnek be, akkor egy esemény generálódik. Ezt akár a hálózat topologikus rajzán is meg lehet jeleníteni.

A készülék többféle kapacitással készül: másodpercenként 50-től 15 ezer esemény feldolgozásáig képes.

NOVELL SENTINEL

A Novell Sentinel nem dobozos termék, hanem egy szoftver. (Ahogy lényegében az előzők is, csak a gyártó azt egy előre konfigurált hardveren teszi elérhetővé.) A Sentinel a 6.1-es változatnál tart, **a szerver része lényegében minden elterjedtebb operációs rendszeren fut, Linuxoktól Windowsig. Kell alá adatbázis-kezelő is: Oracle vagy MS SQL.** Ezekből látható, hogy a Novell Sentinel igen jól méretezhető, tetszés szerinti hardverre telepíthető, ám az árát jelentősen emeli a szükséges hardver és adatbázislicenc beszerzése. Ugyanakkor kiválóan együttműködik a Novell más termékeivel, azaz nemcsak a hálózati eszközök jelentéseit fogadja, hanem például a Novell Identity Managerét vagy a Novell ZenWorksét. A syslog, snmp mellett számtalan más kapcsolaton keresztül is képes adatokat gyűjteni. A támogatott eszközök listája (amelyekről az érkező adatokat értelmezni tudja) meglehetősen hosszú.

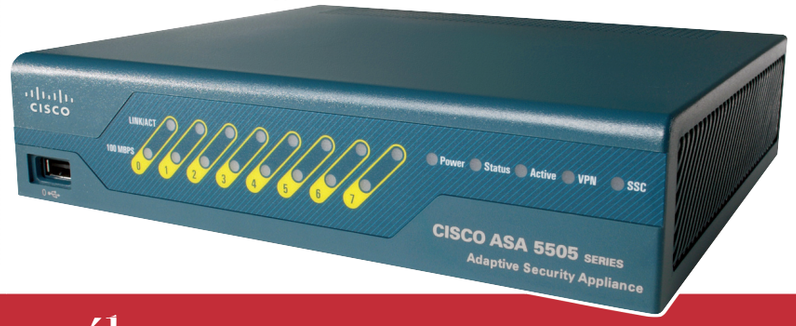
Az említett három eszköz nagyon hasonló: az üzemeltetőnek ad egy felületet, ahol a hálózat különböző jellemzőit megtekintheti, ha nem támogatott eszköze van, akkor kisebb-nagyobb munkával annak üzeneteit megértetheti a SIEM-rendszerrel. Mindegyik képes a biztonsági szabványok által megkövetelt jelentések elkészítésére – ez elsősorban a pénzügyi szektorban fontos.

MIRAGE

A Mirage Network Access Control kicsit megelőzte korát. Amikor a piacra került, a hálózatos fenyegetések még nem voltak sem annyira elterjedtek, sem annyira veszélyesek, mint manapság. Az eszköz a hálózatot figyeli, és a beállított szabályok szerint azonnal figyelmeztetést küld, illetve aktívan képes beavatkozni.

Ez is egy hardvereszköz, amit a hálózatba kell illeszteni, semmi más külön szoftver telepítését nem igényli, semmiféle ügynökre nincs szüksége – emiatt természetesen ez is platformfüggetlen. Passzívan figyeli a hálózatot, az adatforgalmat nem befolyásolja, ám képes beavatkozni, azaz a szabályokat megsértő hálózati eszközöket képes kizárni a hálózatból, ebben kétségtelenül többet nyújt azoknál a megoldásoknál, amelyek csak figyelmeztetést adnak.

A fenyegetettségeket nem szignatúra alapján (hasonlóan a többi eszközhöz) ismeri fel, hanem a viselkedésből,



350 km magasan és 100 méter mélyen

A HP úgy véli, a vezeték nélküli változatok új lendületet adhatnak a ProCurve kapcsolók piaci sikereinek. A ProCurve eszközök népszerűek: azok működnek a nemzetközi űrállomáson, ahogy a CERN-ben, a föld alá épített óriási részecskegyorsítóban mért adatokat is a HP ProCurve eszközein keresztül rögzítik, és azok feldolgozásához a világ minden részéről fizikusok ezreinek kell hozzáférést biztosítani. Az eszközök sikerében egy sor saját fejlesztésű technológia is közrejátszik, például az Adaptive EDGE leegyszerűsíti a hálózat üzemeltetését, jó eséllyel képes megelőzni a váratlan leállásokat.

A 2008-as év a HP ProCurve számára meglehetősen mozgalmas volt, több kisebb bejelentés után nagy lépést tettek: felvásárlásaikkal a WLAN-területen is terjeszkedésbe kezdtek. A Wi-Fi megoldások iránt itthon elég nagy a bizalmatlanság, de a tengerentúlon, Európa nyugati felén, illetve a világ keleti felén igazi sikertörténet, igen nagy Wi-Fi rendszereket telepítenek, és használnak. Az új vezeték nélküli megoldások már megfelelő biztonságot adnak, és közben megőrzik a nagy rugalmasságot.

A nagy bevásárlások nem véletlen események: a HP ProCurve intenzív munkába fogott. Ennek már 2008 végén megjelent az eredménye, amikor bejelentették a HP ProCurve harmadik negyedévi eredményeit. Az előző év hasonló időszakához viszonyított növekedése sok területen jelentősen meghaladja az ipari átlagot – a Dell'Oro Group által végzett felmérés szerint.

A világszerte eladott layer 2-től 7-ig terjedő, kapcsolókba épített portok számában 25,8 százalékos növekedést értek el, míg az iparág növekedése átlagosan csupán 6,6 százalék volt. A bevételt tekintve is jelentős a növekedés: az előző év harmadik negyedévéhez képest 14,1 százalék, míg az iparág átlaga 4,5 százalék volt. Egy elég speciális területen, a PoE (PowerOnEthernet) portok eladásában 51,7 százalékkal nőttek (a piaci átlag 13,7 százalék volt).

Termékei a hálózati terület egyre nagyobb részét fedik le, ezeket röviden a következőképpen lehet összefoglalni:

- LAN Edge 2/3/4 layer, 10–1000 megabites és 10 gigabites portokkal;
- LAN Core 2/3/4 layer, 10–1000 megabites és 10 gigabites portokkal bővíthető;
- WLAN: vezérlők, AP-k, szoftverek, például RF-tervező, Wi-Fi hálózathoz mobility IDS/IPS;
- WAN: a választékban találunk routert is;
- felügyelet: ProCurve Manager szoftver minden kapcsolóhoz jár, ennek sok bővítőmodulja van. A ProCurve Network Immunity Manager 1.0 a hálózatban fellépő fenyegetésekre képes reagálni, külön modul készült a WLAN-környezethez, azaz a LAN kiterjesztésével nem kell új felügyeleti eszközhöz nyúlni, a meglévő eszköz alkalmas Wi-Fi hálózat kezelésére is;
- hálózati biztonság: erre a felügyeleti rendszer bedolgozó modul-jai szolgálnak. A Network Access Controller egy RADIUS-alapú kiszolgáló, amivel a hálózatba csak autentikált eszközt engedhetünk be, ami elég széles szabályrendszerhez köthető. Megadott szoftver, megadott javításokkal legyen a gépen, esetleg másik szoftver nem lehet rajta;
- a termékekhez a felhasználó kaphat oktatást, konzultációt is.

A HP ProCurve jelentős változáson megy keresztül. Régebben mostohagyermek volt a HP-n belül, mostanra viszont változott a helyzet. Erről kérdeztük *Bolla Szilárdot,* a HP ProCurve üzletágának új vezetőjét.

a tünetekből következtet a betegségre. A gyártó 11 szabadalommal rendelkezik a hálózathoz való hozzáférés vezérlésének témakörében. A rendszer két részből áll, egy vagy több szenzorból, valamint a kiszolgálóból, ami a szenzorok adatait feldolgozza. A szenzorok több méretben léteznek: a legkisebb 50 hálózati végpontot képes felügyelni, a legnagyobb 2500 darabot.

HP PROCURVE

A HP ProCurve ugyan nem gyárt SIEM-eszközt, de hasonló funkcionalitást meg tudunk valósítani ProCurve eszközökkel is. **A ProCurve Proacitve Defense megoldása a ProCurve eszközök képességeire épül, és a hálózati eszközök többrétegű védelmét biztosítja: észreveszi a fenyegetéseket, és szükség esetén beavatkozik.** A ProActive Defense két elemből áll: a hozzáférés-vezérlés a felhasználókat szabályozza, ki mit érhet el – ezt vezetékes és vezeték nélküli hálózaton belül is tudja. A Network Immunity Manager figyeli a hálózati forgalmat, anomáliákat keresve. Elsősorban a ProCurve eszközök adatait képes feldolgozni, amelyek hardvere erre fel van készítve, de az sFlow adatok más eszközről is megkaphatók. A védelem másik eleme a hozzáférés-vezérléshez kapcsolódik, ez a Network Access Controller 800 hardver, amely egy RADIUS szerver, kibővített képességekkel, és a hálózathoz kapcsolt eszközöket ellenőrzi. Meg lehet akadályozni, hogy nem engedélyezett eszközt kössenek a hálózatra, például egy akárhonnan behozott kapcsolót, noteszgépet. Olyan szempontokat adhatunk meg, hogy a felcsatlakozott gépen az operációs rendszer milyen legyen, milyen foltnak (patch) kell rajta lennie, milyen szoftver nem futhat rajta – ha megadott trójait talál, nem engedi be a hálózatba.

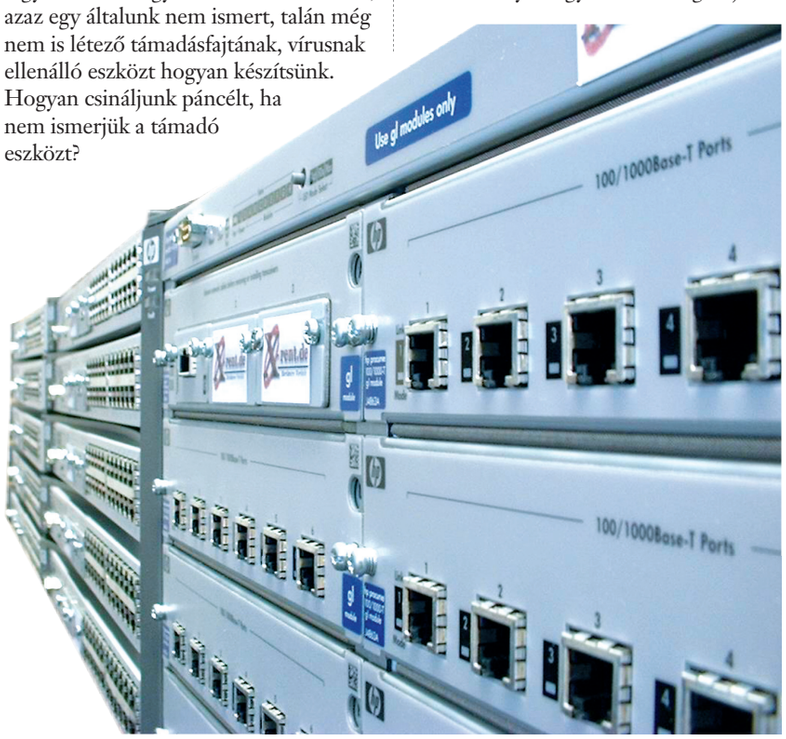
FIGYELMEZTETÉSEK

Nyomatékosítanunk kell: egy ilyen eszköz bevezetése nem azonos azzal a feladattal, hogy veszünk egy szervert, és feltelepítjük rá az operációs rendszert, vagy hogy új hálózati kapcsolót helyezünk üzembe. Ezek az eszközök egyértelműen egy specializált feladatra valók, mondjuk, ha a hagyományos szerverek-munkaállomások, akár a tűzfalak is a konfekcióruháknak felelnek meg, akkor ezek a SIEM-eszközök a szabónál rendelt, egy-egy alkalomhoz készített öltönyök. Az üzembe helyezéshez sok-sok próba kell. Ismerni kell az eszközt, ismerni kell a saját hálózatot, tudni kell, mit szeretnénk figyelni, mely eszközök forgalmát, állapotát. Ennek megfelelően lehet kiválasztani az eszköz, illetve a szenzorok helyét. A hálózat aktív eszközeit úgy állítsuk be, hogy a szenzorok megkapják az adatokat. Ez a határvédelmi eszköz, víruskereső, hálózati kapcsolók, forgalomirányítók konfigurálását jelenti, de Windows szerverekre esetleg alkalmazásokat is kell telepíteni, amelyek az állapotukról adatokat közölnek (például a Windows eventek sysloggá alakítására).

Ezeken aztán az első eredmények alapján finomítani kell: **egy SIEM-eszköz üzembe állítása alapesetben is hetek kérdése, de egy több száz végpontos, országot-világot átfogó hálózat esetében több hónapos projekt is lehet.**

A SIEM-eszközök arra a nagyon régi problémára próbálnak megoldást adni, hogy egy várható, ám teljesen ismeretlen fegyver ellen hogyan védekezzünk előre, azaz egy általunk nem ismert, talán még nem is létező támadásfajtának, vírusnak ellenálló eszközt hogyan készítsünk. Hogyan csináljunk páncélt, ha nem ismerjük a támadó eszközt?

A SIEM-eszközök a normálistól eltérő viselkedést veszik észre, amelyek közt vannak igen egyszerűek – megszűnt vagy végtelenre nőtt hálózati forgalom, hibás csomagok tömeges megjelenése –, és vannak általánosan nem megfogalmazhatók, amelyek egy-egy hálózatban, egy-egy alkalmazás esetében anomáliának számítanak. A testre szabás azt is jelenti, hogy a sajátos igényeknek megfelelő események figyelését is megoldják.



Computerworld-Számítástechnika: A HP ProCurve hosszú évek óta a jobb sorsra érdemes termékekkel együtt meghúzódott a háttérben, afféle mostohagyerekként. Tavaly pedig megtáltosodott, igen dinamikusan fejlődik, a WLAN-piacon egyenesen a legnagyobbak közt kíván megjelenni.

Bolla Szilárd: Valóban, a 90-es évek végén a HP ProCurve bevételt tekintve még csak a 12. helyen állt, és ez nem is igazán változott egészen 2002–2003 környékéig, amikor is egy hosszas audit procedúrán esett át az üzletág. Az auditot stratégiai döntés követte, amelynek értelmében újjászervezésre és invesztícióra került sor, majd a 2008-as évet már a bevételeket tekintve második helyen zárta a ProCurve. Minek köszönhető a változás? Erre egyszerű a válasz: a HP teljes mellszélességgel kiáll az üzletág mellett és ennek megfelelően szerveződnek folyamataink cégen belül és kívül egyaránt.

CW-SZT: A fejlődés igen jelentős, de alacsony értékről indulva ez még érthető. Mennyire tartható ez a fejlődési ütem, a piac átlagát jelentősen meghaladó növekedés?

B.L.: Azt gondolom, hogy rövid távon ez a dinamika folytatódhat, hiszen valóban van honnan fejlődni, és nem titkoltan „duplázni" szeretnénk a hazai piacon, nemzetközi viszonylatban pedig a gazdasági válság ellenére is erőteljes expanzió előtt állunk.

CW-SZT: Ehhez nagy fejlesztési kapacitás kell.

B.L.: Azt gondolom, hogy a ProCurve termékeket korábban is a megbízhatóság és a minőség fémjelezte, amelyet kitartó és lojális partneri körünk is alátámaszthat, de ambiciózus terveink megvalósításához valóban további akvizíciós és erőteljes R&D tevékenység kapcsolható a jövőben. A ProCurve nagy lendületet kapott *Marius Haas* kinevezésével, aki korábban az EDS akvizícióval hívta fel magára a figyelmet, majd gyorsan letette névjegyét, amikor a Colubris akvizíciót hozta tető alá. A Colubris piacvezető wireless megoldásokat kínál most már a HP támogatását is élvezve. Úgy látom, hogy a HP ProCurve-nak soha nem volt ekkora tekintélye a HP-n belül, és soha nem is vártak tőlünk ennyit.

CW-SZT: A hazai piacon a ProCurve meglehetősen gyengén szerepel. Mi az oka?

B.L.: A számok ismeretében sajnos nem tudok ezzel vitába szállni, és több tényezőt is fel lehetne sorolni, de azt gondolom: most minden együtt áll ahhoz, hogy kibontakozzon egy sikersztori. Nyugat-Európában 12–15 százalék a részesedésünk, de például Finnországban ez a 35 százalékot is eléri, itthon mindössze 5 százalék körül mozgunk. Ezen az idén jelentősen változtatni kívánunk és ennek érdekében a helyi szervezetet is bővítjük. A HP ProCurve bekerült a TSG-üzletágba (szerverek, tárolórendszerek), s hogy ennek az üzletágnak a részévé váltunk, azt jelenti: a projektekben van lehetőség ProCurve-t ajánlani.

CW-SZT: A gazdasági káosz, válság nem torpedózza meg a nagyra törő terveket?

B.L.: Természetesen mi is érezni fogjuk a válság hatásait, mint mindenki más, de a ProCurve előnyösebb helyzetben van versenytárainál, hiszen a méretünkből adódóan rugalmasan tudunk alkalmazkodni a piaci kihívásokhoz, és a jelenlegi piacon mi vagyunk az első számú alternatíva a Cisco mellett. Nem utolsósorban a jó áraink miatt a kisebb költségvetésből gazdálkodó vezetők számára jó választás vagyunk.

Követelmény-keretrendszer a közlekedésben

Jó példája az infokommunikációs alkalmazás fejlődésének az az út, amelyet a vállalatirányítási rendszerek bejártak az üzleti felhasználóknak szánt első számítógép piacra kerülésétől máig. [Írta: Vargha Márton]

Kezdetben még külön volt a számlázás, a főkönyv, a leltár és a többi, és ha adatot kellett átadni egyik adatrendszerből a másiknak, az papíron történt: az egyik kinyomtatta, a másikba a rögzítők beírták. Ma pedig már összeolvad az operatív irányítás az egyik, és az elemzés, tervezés a másik oldalról, és ugyanazt az adatot látja szinte a keletkezése pillanatától a maga gépén a megrendelő, az eladó, az eladó beszállítója, az, aki a terméket eljuttatja a gyárból a vevőnek, és az, aki a változásokra, tendenciákra kíváncsi. **Ha a felhasználó felől nézzük, talán a felhősödés az a szó, amely legjobban fedi az infokommunikáció fejlődésének ezt a folyamatát.** Egy felhőben gomolyognak ki tudja hol, ki tudja hogyan az adatok és az alkalmazások, amelyekkel dolgozni tudunk. Előtérbe kerülnek a funkciók, egyszerűsödik a használat. Mindennek az alapja egy (vagy több) mesterséges nyelv, ami biztosítja, hogy ne torzuljon az adatok által hordozott információ.

A közös nyelvet a vállalatirányításban egyrészt a programok kényszerítették rá a világra – talán az SAP alapítóinak, *Dietmar Hoppnak* és *Hasso Plattnernek* az érdemei a legnagyobbak e téren –, másrészt a bonyolódó gazdaság átláthatóságát biztosítani próbáló törvénykezés. A telefontársaságok viszont már a kezdet kezdete óta egy nyelven beszélnek. Nemzetközi hívás nem létezett anélkül, hogy ne értette volna meg egymást a magyar és a francia telefonoskisasszony, majd ne lett volna később a közös SS7 jelzésrendszer. Már több mint egy évtizede szó van a konvergenciáról, a telefon- és az adathálózat összeolvadásáról, és mégis, a vártnál jóval lassabban történik, pedig itt csak két, jól szabványosított rendszert kell egységesíteni vagy felhősíteni.

KÖZLEKEDNI BONYOLULT

Nagyságrendekkel nagyobb feladat nemhogy egy kontinens, de még egy ország közúti közlekedési infrastruktúrája teljes menedzsmentjének a megvalósítása! Probléma a korábban kialakult szigetrendszerek integrációja, az alrendszerek közötti kommunikáció, a gyűjtött adatok átjárhatósága és átláthatósága, de gond az is, hogy rengeteg az érintett, akire figyelni kell. (Már csak azért is, mert az adatcsomaggal ellentétben az autós bele tud, és bele is szól.) Még szerencse, hogy a többség érdekelt minden, a forgalom folyamatosságát erősítő szolgáltatásban.

Elengedhetetlen volt, hogy az integráció érdekében beinduljon egy szabványosítási folyamat. Előbb Amerikában és Japánban a nyolcvanas évek végén, majd más kontinenseken is. Európában a kilencvenes évek közepe táján vált anyagi erővé a gondolat, hogy követelményleíró keretrendszer kialakításával elő kellene segíteni a közlekedési infokommunikáció felhősödését. Neki is láttak a közös szerkezetek kialakításának, és **általános követelményrendszereket dolgoztak ki, amelyekből mindenki kiindulhat, amikor egy közlekedési folyamatot támogató infokommunikációs rendszer tervezésébe fog.** A részt vevő szervezetek, egységek felhasználói igényeiből kiindulva felépített struktúrára az angol a „frame", a magyar terminológia a „keretszerkezet" szó használja, és a közúti ITS-alkalmazások, rendszerek rendszertervét érti rajta. A keretterv egységes szerkezetben írja le és összegzi a közúti ITS-fejlesztésekkel szemben támasztott felhasználói követelményeket, valamint az átjárhatóság érdekében megkövetelt funkciókat és alapvető rendszertulajdonságokat. Segítségével országos, regionális vagy helyi, koncepcionális szintű ITS-fejlesztési terv készíthető, annak funkcionális és fizikai szerkezetével együtt.

EURÓPAI TÖREKVÉSEK

Európában a kezdet a kilencvenes évek végén induló KAREN kutatás-fejlesztési program volt, ennek eredményeire támaszkodik a FRAME projekt (www.frame-online.net), melynek feladatául a finomítást, a nemzeti adaptációk kialakításának támogatását, és az European ITS Framework Architecture (EITSFA), magyarul Európai ITS Keretszerkezet véglegesítését szabták. Alapelv volt, hogy a már meglévő megoldások ne szigetelődjenek el, a rendszertervet az Európában folyó fejlesztésekből és már működő megoldásokból kiindulva készítették.

2002 márciusában publikálták az interneten a FRAME kiválasztó szoftverének 1.1-es változatát, 2006 végén pedig a 3.0-st, amely a magyar szoftverhonosítás alapja lett. Az előzményanyagok feldolgozásával, az eredeti Selection Tools lefordításával, majd a magyar követelmények beillesztésével és kitartó marketingmunkával a COWI Magyarország Kft. alakította ki és tette szakmai körökben ismertté a Magyar Nemzeti ITS Keretszerkezetet, a HITS-et.

A KERETRENDSZER

A HITS felhasználói igények alapvető készletét ajánlja fel a közúti ITS-ekhez, és segít hozzárendelni a kiválasztott igényekhez a kielégítésükre alkalmas funkciókat és a megvalósulásukhoz szükséges adatfolyamatokat. Használatával egy koncepcionális logikai rendszerterv állítható elő. **Ez az első szint, a funkcionális szerkezet, amelynek a funkcióihoz alrendszerek, modulok és logikai, adatáramlási kapcsolatok hozzárendelésével alakul ki a fizikai szerkezet.** Alapvető tulajdonsága valamennyi általános közúti ITS-rendszertervnek, tehát a HITS-nek is, hogy miközben végigsegít a rendszertervezés lépéseihez hasonlító úton, gondoskodik az együttműködést és a szolgáltatások integrációját biztosító feltételek beépítéséről.

A keretszerkezet olyan váz, amellyel könnyen és gyorsan beépíthetők a felső vezetői – akár politikai, társadalmi – célok a rendszertervbe. Annak érdekében támogatja az Európai Unió a használatát, hogy a közúti ITS-megoldások Európa-szerte nyíltak, modulárisak, továbbfejleszthetők legyenek, és együtt tudjanak működni akár kontinentális szinten is. Magyarországon a HITS keretszerkezet használata a biztosíték arra, hogy egy közlekedési infokommunikációs fejlesztés eredménye nyílt, az európai ITS-piaccal konform termék legyen. Segít a felhasználónak és a fejlesztőnek a követelmények megfogalmazásában, hidat képez az ITS-t használó közösség, a felső vezetői szint és a rendszerfejlesztők, valamint a régebbi és új rendszerek között és inspirálja az új fejlesztéseket, kutatásokat és kísérleteket.

Funkcionális terület	Rövidítés	Magyar elnevezés
Area 1	pepf	Elektronikus díjfizetés lehetőségének biztosítása
Area 2	psef	Biztonsági és segélykérő berendezések biztosítása
Area 3	mt	Forgalom kezelése, forgalommenedzsment
Area 4	mpto	Közösségi közlekedés menedzselése
Area 5	padas	Fejlett vezetőtámogató rendszerek biztosítása
Area 6	ptja	Utazás közbeni támogatás biztosítása
Area 7	psle	Támogatás az előírások érvényesítésében
Area 8	mffo	Szállítmány és flottamenedzsment

Az Európai ITS Keretszerkezet és a HITS által lefedett területek

Több intelligencia, mint beton

Az ITS Hungary egyesület főtitkára, *Lindenbach Ágnes* egyike azoknak, akiknek a legszélesebb áttekintésük van az EU-programokhoz, projektekhez kapcsolódó magyarországi kezdeményezésekről. Arra kértük, emeljen ki néhányat a terítéken lévő témák és eredmények közül.

Computerworl-Számítástechnika: Kihasználjuk a lehetőségeket?
Lindenbach Ágnes: Nyíltak lehetőségeink az ITS magyarországi lehetőségeinek kutatására, fejlesztésekre a csatlakozásunk után az Európai Unióhoz, és ezeket szerintem ki is használtuk. A CONNECT projektnek már a harmadik fázisát zárjuk le a közeljövőben.
CW-SZT: Mi a legnagyobb eredménye a CONNECT-nek?
L. Á.: Egymásra épülő szakmai területeken készültek pilot projektek, megvalósítási tanulmányok. Fontos az európai ITS keretrendszer magyarítása, a HITS, ami – ha mindenki használja – azt teszi lehetővé, hogy térben egymás mellett, időben egymást követően használatba kerülő alkalmazások kommunikálni tudjanak egymással. A legnagyobb eredménye pedig szerintem az, hogy intézmények, szervezetek – például a főváros és az Állami Autópálya Zrt.(ÁAK Zrt.) – elkezdtek egymással együttműködni, adatot cserélni. A projekt keretében központot korszerűsített az ÁAK Zrt., és érzékelőket, változtatható jelzésképű táblákat tett ki, ami látványos ITS-alkalmazás. A Fővárosi Közterület-fenntartó Zrt. parkolási információs rendszert és internetes útvonalajánló programot fejlesztett. Elindult Magyarországon a navigációs eszközök valós idejű információval való ellátása a Petőfi Rádió műsora alatt.
CW-SZT: Mi lesz a lezáruló projekt után?
L. Á: 2007 óta létezik az EASYWAY program, amelynek indításakor az Európai Bizottság kikötötte, hogy a megvalósításokra kell koncentrálni, elsősorban az információszolgáltatásra országokon belül, és a tagállamok között. Négy szakmai területe van, ezekbe kellett besorolni a kiválasztott magyarországi fejlesztéseket.
CW-SZT: Az EU-programok főként az európai közlekedési folyosókra vonatkoznak?
L. Á.: Részben. De ahogy a CONNECT-ben benne volt Budapest, ebben a programban is részt vesz, hiszen az autópályák befutnak a fővárosba, az ÁAK Zrt.-vel közösen kell biztosítani az autók folyamatos haladását. A Budapesttel való együttműködésért dicséretet is kapott Magyarország! Az Európai Bizottság egyértelműen azt szorgalmazza, hogy az ITS-eszközök még nagyobb figyelmet kapjanak. Már a közlekedéspolitika 2001-es fehér könyvében ott van: „Itt az ideje a kevesebb betonnak és a több intelligenciának a közlekedési rendszerben.” Látszik ez a nemrég az Európai Parlament elé terjesztett direktívában is, amely pontosan a közlekedési informatika fejlesztésének gyorsítását, a rendszereknek a tagállamok közötti összehangolását, azaz az interoperabilitást írja majd elő.
CW-SZT: Mennyire mérhető az informatikai közlekedési rendszerek hatása?
L. Á.: Rendszere válogatja. Legjobban akkor lesz mérhető az egyes ITS-alkalmazások hatása, ha működni fog a forgalmi adatok folyamatos mérésére szolgáló ITS-megoldás. De úgy tudom, hogy például az autópályákon elhelyezett táblákon megjelenített üzenetekkel máris sikerült javítani a haladási sebességen.
CW-SZT: Az eCall, az automatikus vészjelzőrendszer ügye hogyan áll?
L. Á.: Ezt láthatóan igen fontosnak tartják az Európai Unióban, de a gazdája nem a közlekedésért, hanem az információs társadalomért felelős hivatal. Ezért aztán nálunk is a MEH Informatikai Szakállamtitkárságán foglalkoznak vele. Bár még nem csatlakoztunk az eCall szándéknyilatkozathoz, aktívak vagyunk a vele kapcsolatos kutatásokban. Indult egy EU-s projekt arról, hogy melyik tagállamban hogyan állnak hozzá az eCallhoz, mit várnak tőle, milyen gondokat látnak tornyosulni előtte. Minden tagállam ad be adatokat, de négy országban, köztük Magyarországon részletes tanulmány készül, én vagyok a magyar konzorciumi partner. Határozottan nő a fogadókészség és az eCall infrastruktúra kialakítása melletti elkötelezettség. Azért is fontos az eCall, mert az Európai Bizottság éppen a közlekedési baleset okozta halálozások drasztikus csökkentése végett pártolja az ITS-fejlesztést. A baleset következményeinek elhárításában van egy jól definiált mentési lánc. Ha jó az informatikai, irányítási háttér és jó a kommunikáció, akkor ebben a láncban végrehajtási időket lehet leszorítani, illetve egyes következményeket, például a torlódást a közlekedők informálásával meg lehet előzni.
CW-SZT: Mit vár a közeljövőtől?
L. Á.: Úgy látom, hogy az ITS ügye egy szintváltási lehetőséghez érkezett Magyarországon, eljött az ideje a stratégiakészítésnek. Mert eddig volt ugyan szó a közlekedésfejlesztési tervekben, koncepciókban az informatikai megoldásokról, de csak alárendelt szerepkörben.
CW-SZT: Jól látszik ez például Budapest Közlekedési Rendszerének nemrég elfogadott Fejlesztési Tervében, ahol még mindig hátrasorolódtak az ITS-alkalmazások.
L. Á.: Én éppen egy korszakváltásról beszélek; lehet, hogy a fővárosban ez még nem látszik, de a központi irányításban mindenképpen megnőtt az ITS elfogadottsága. Ezért is vágtunk bele néhányan a stratégia megfogalmazásába, és tettünk le egy horizontális szemléletű tanulmányt az ITS Hungary tagjai, és persze a közlekedési tárca illetékesei elé.

A pontos fordítás és a diagramok átvétele mellett a HITS-projekt résztvevői alaposan megvizsgálták, hogy a hazai körülmények igénylik-e a bővítést új felhasználói követelményekkel, funkciókkal. 2002-ben az ÁKMI Kht. a CONNECT projekt keretei között állt a hazai fejlesztések élére, és utódja, a Magyar Közút folytatta a munkát. A COWI Kft., a Topolisz Kft. és a Hétpont Kft. szakemberei vizsgálták az EITSFA magyarországi alkalmazhatóságát és alakították ki a magyar változat alapelemeit. Először kiválasztották az autópályák forgalomirányításához elengedhetetlennek vélt felhasználói igényeket a forgalomirányításban, az eseménykezelésben és az útközbeni információs támogatásban, és elemezték az ezekhez illeszkedő funkcionális szerkezetet. A következő lépésben megkerestek közlekedési cégeket, és kérdőívekkel felmérték az ITS-alkalmazások magyarországi helyzetét. Az összegyűlt információ birtokában fogtak hozzá a HITS kialakításához. Tehát nem egyszerűen lefordították magyarra az EITSFA-t, hanem beillesztették azt a magyar környezetbe. Ezt a FRAME projekt szakemberei természetesnek tartják, de igyekeztek előre gondoskodni arról, hogy a nemzeti sajátosságok figyelembevétele ne vezessen a nemzeti változatok elszabadulásához, és ezzel ne szűnjön meg a keretrendszer páneurópai jellege. Amit egy országban a kereteken belül maradva kidolgoznak, azt a FRAME projektben mint egységet vizsgálják és megfelelő formában az EITSFA kiegészítéseként megjelentetik a keretrendszer újabb kiadásaiban. Ez történik a magyar hozzáfejlesztésekkel is.

Szakemberek nagy áttörésnek tartják a HITS Kiválasztó Eszköz magyar nyelvű szoftverének véglegesítését, ahogy *Hladon Andrea* (COWI Kft.) megfogalmazta: „Használatával egy dohányzóasztalt közel fél méter magasságban beborító dokumentáció, ismertetés és összerendelő tábla váltható ki.”

A HITS-ben végbemenő ITS-koncepciófejlesztést segíti a frame-online.hu honlapról letölthető szoftver, amely a kiválasztott felhasználói igényekhez automatikusan és a felhasználó igénye szerint rendel funkciókat, adatbázis-fajtákat és funkcionális adatfolyamatokat. A programmal bárki összeállíthat magának egy keretrendszert, kidolgozhatja egy régió vagy vállalat közlekedési informatikai fejlesztés EITSFA (HITS) kompatibilis követelmény-specifikációját. A HITS megalkotásának céljai, a pozitív hatások akkor érvényesülhetnek legjobban, ha a lehető legtöbb közúti ITS-fejlesztésnél használják. Ezt elősegítendő, 2010-re várhatóan Útügyi Műszaki Előírás is támogatni fogja.

Egyre veszélyesebbek a cyberbűnözők

A globális üzleti világ tapasztalataiból ítélve a cyberbűnözők aggasztó mértékben veszélyeztetik a vállalatok működését. Gaidosch Tamás, a KPMG IT-tanácsadás részlegének partnere szerint az internetes bűnözők könnyedén ki tudják kapcsolni és meg tudják kerülni a legtöbb védelmet, illetve igényük szerint manipulálni is tudják azt, így az installált védelmi technológiák egyre kevésbé bírnak elrettentő erővel. [Írta: Mozsik Tibor]

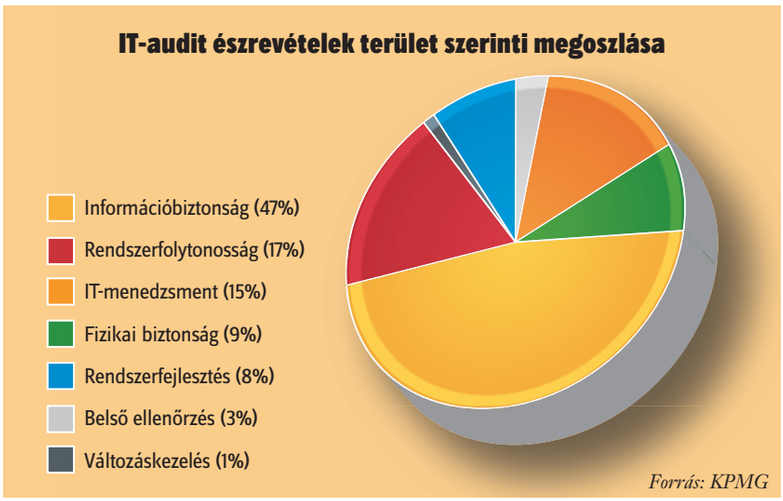
Már régen nem magányos hackerek állnak az elektronikus úton elkövetett bűncselekmények hátterében – vélik az internetes bűnözéssel foglalkozó szakemberek. A különböző típusú támadásokat ma már jellemzően szervezett bűnözői csoportok érdekében követik el. Az internetes bűnözés méreteivel kapcsolatban már eddig is több elrettentő szám látott napvilágot: a Symantec 2008-as felmérése szerint például a rosszindulatú számítógépes programok (malware) miatti fenyegetések száma 2006–2008 között több mint a felével nőtt, és ma már több – a 2,4 milliót is meghaladja a rosszindulatú szoftverek száma –, mint az ismert legitim alkalmazásoké.

Egy másik kutatás szerint **tavaly az előző évhez képest közel megháromszorozódott az adathalász (phising) támadások áldozatainak száma.** Eközben csak az Egyesült Királyságban kétszeresére nőtt a számlaelbirtoklási csalások mennyisége is.

zombihálózatot (botnet) már néhány száz dollárért lehet bérelni is. Az egyre jobb szoftvereknek köszönhetően a támadások minden korábbinál kifinomultabbak és célzottabbak; a létező rendszerek jobb felhasználásával ezzel együtt a legtöbb támadás még mindig detektálható lenne.

MÁR NEM ELÉG A HAGYOMÁNYOS VÉDELEM

A KPMG és az AKJ Associates a 7. nemzetközi e-Crime kongresszus kapcsán felmérést végzett több mint 300, többségében európai nagyvállalat és egyéb szervezet körében a biztonsági tudatosságról. A *2009 e-Crime* című felmérés válaszadóinak majdnem 80 százaléka vélekedik úgy, hogy **a lenyomatfelismerésen alapuló biztonsági szoftverek nem nyújtanak megfelelő szintű védelmet az internethasználók részére** – tudtuk meg *Gaidosch Tamástól*, a KPMG partnerétől, aki szerint a vírusirtóknál ma már kulcskérdés a minél gyorsabb frissítés, továbbá a még nem ismert támadásokkal szembeni védekezést lehetővé tevő heurisztikus detektálás. A felmérésben idézett egyik válaszadó így vélekedett: „Jelenleg a vírusellenes termékek védelmi mechanizmusként nagyjából semmit nem érnek. Olyan új típusú vírusellenes termékek megjelenésére van szükség, amelyek valóban hatékonyan tudják kezelni a problémát.”



Mindeközben egyre szélesebb körben elérhetők a szofisztikált céleszközök, amelyek révén már nincs szükség komoly ismeretekre a számítógépes betörésekhez. Becslések szerint ma már a támadások többségét olyanok végzik el, akiknek nincs is elmélyült technikai tudásuk. Ráadásul az elkövetéshez már nincs szükség komoly forrásokra sem – egy

Az említett problémát súlyosbítja, hogy a jelenlegi gazdasági környezetben megnövekedett számú munka nélkül maradt IT-szakértő közül egyre több csatlakozik a cyberbűnözői érdekszférához; a válaszadók kétharmada véli úgy, hogy a válság következtében elbocsátott IT-szakértők egy része a cyberbűnözésnél köthet ki. A válaszadók 45 százaléka már az elmúlt időszakban is az ügyfeleiket ért támadások számának növekedését tapasztalta, a cégek fele szerint pedig a támadások technikailag egyre kifinomultabbak. **A KPMG ügyfelei körében végzett felmérésben a válaszadók közel kétharmada vélte úgy, hogy a jövőben a fertőzött honlapok, a webes alkalmazások jelenthetik azt a támadási módot, amely leginkább kompromittálhatja az ügyfelek online biztonságát.**

Gaidosch Tamás
partner
KPMG

ÉSZRE SEM VESZIK

Gaidosch Tamás szerint a cyberbűnözőknek nem számít többé, van-e installált védelmi technológia a társasági rendszereken vagy az otthoni számítógépen; ennek nincs többé elrettentő hatása. Az internetes bűnözők ki tudják kapcsolni, meg tudják kerülni a legtöbb védelmet, illetve igényük szerint manipulálhatják is azt. Az e-Crime felmérés válaszadóit nagyon aggasztja, hogy a hagyományos védelem nem hatékony a célzottabb fenyegetésekkel szemben – a jó fiúk kezdenek mesterlövészek ellen csúzlival védekező gyerekekhez hasonlítani. Mindeközben a malwarerel és az emberi hiszékenység kihasználásával (social engineering) elkövetett csalások 80 százaléka eredményesen végződik.

A 2009 e-Crime felmérés válaszadóinak 62 százaléka úgy gondolja, hogy vállalata nem szán elegendő időt, anyagi forrást és erőforrást a gyenge pontok meghatározására. A felmérésben részt vevő egyik vállalat így nyilatkozott: „Már ért bennünket támadás, amely 10 hónapon át nem detektált alvó fertőzéssel járt. Hány ilyen lehet már számítógépeinken?” A biztonság komolyan vételének mértéke a múltban adott esetben attól függött, milyen fokban volt a támadásoknak üzleti hatásuk. Lassan véget ér az az időszak, amikor a legnagyobb fenyegetést a cél nélküli, de az üzletre negatív hatást gyakorló támadások jelentették. Ezeket egyre inkább felváltják a szofisztikált, szervezetek ellen irányuló, megrendelésre végrehajtott, célzott támadások, különböző ágazatokra kialakítva.

SOK A PROBLÉMA AZ INFORMÁCIÓKKAL

– Nem meglepő módon arra a megállapításra jutunk, hogy a maximálisan naprakész védelem fenntartásának precíz megközelítését valló és abba beruházó szervezetek sokkal kevésbé aggódnak, mint azok, amelyek nem ruháztak be, vagy nem tudják, menynyire naprakészek – tette hozzá Gaidosch Tamás. – Az underground gazdaságban az adat – pénz, és valós annak a veszélye, hogy az üzleti világ, a biztonsági szolgáltatók, a kormányok és az igazságszolgáltatás lemaradnak az ellenőrzés kézben tartására irányuló versenyben. Védelmi képességeik egyre kevésbé hatásosak a gyorsan növekvő kockázatok ellen. Sok társaság az alapvető védelmi intézkedéseket sem hozza meg, pedig a legtöbb sikeres támadás alapszintű hibákat használ ki.

A nemzetközi kutatás keretében itthon is elvégzett felmérés azt mutatja, hogy **a vállalatoknál elvégzett IT-auditok során leggyakrabban az információbiztonsággal (47 százalék), valamint a rendszerfolytonossággal kapcsolatos problémák szoktak felmerülni.** A KPMG szerint néhány fontos lépést mindenkinek meg kell tennie a nagyobb informatikai biztonság érdekében, így meg kell hozni az alapvető védelmi intézkedéseket, és az ügyfeleket is fel kell világosítani a legjellemzőbb támadási módokról, valamint az azok elleni védekezési lehetőségekről. Ezzel párhuzamosan a saját rendszerek védelmét is meg kell erősíteni és meg kell vizsgálni az új, biztonságosabb e-kereskedelmi működési modelleket is.

Fókuszban a gyors megtérülés

elemzés

Idén a GDP csökkenése a szoftverpiac zsugorodását is generálja. A költségcsökkentést, illetve a hatékonyságnövelést támogató alkalmazások azonban keresettek. [Írta: Barabás Balázs]

Rendszeresen felülvizsgálja előrejelzéseit az IDC. A legutóbbi korrekció során a januárban kiadott prognózishoz képest még alacsonyabbra módosították a szoftverpiacra vonatkozó előrejelzéseket. A januári prognózis is negatív volt, ám azóta napvilágra kerültek az új GDP-előrejelzések, amelyek január óta tovább romlottak: akkor még 3,5 százalékos csökkenéssel számoltak a gazdaságkutatók, **most inkább 5-6 százalékra számítanak, és ezt a romlást várhatóan követi az informatikai ipar is.** Ennek fényében az IDC 2009-re a szoftverlicenc- és karbantartási költések 3-4 százalékos csökkenését prognosztizálja Magyarországon.

Az IDC által vizsgált első csoport az infrastruktúra szoftverek (operációs rendszerek, menedzsment szoftverek, virtualizációs, biztonsági és tárolószoftverek). – Ez a szegmens lesz a válság legnagyobb vesztese, a visszaesést leginkább az operációs rendszerek piacának nagyarányú beszűkülése generálja – mondta *Marosvári Gábor*; az IDC Magyarország vezető elemzője. Drasztikusan csökkennek Magyarországon a PC- és szervereladások, márpedig a csökkenő hardvereladások mellett az operációsrendszer-eladások sem nőnek. A cégek a platform szintű migrációkat csak akkor fogják idén meglépni, ha ez üzletileg kritikus fontosságú; inkább megvárják a Windows 7 megjelenését. Bár a Linux terjed, még nincs akkora piaci részesedése, hogy látványosan befolyásolja a piacot *(lásd cikkünket a 12. oldalon)*.

Az operációs rendszer annyira markáns szelete az infrastruktúra szoftvereknek, hogy ennek a piacnak a beszűkülése magával rántja a teljes infrastruktúraszoftver-szektort, ami az IDC jelenlegi becslése szerint értékben 4-5 százalékkal fog csökkenni az idén.

KÖLTSÉGCSÖKKENTÉS VIRTUALIZÁCIÓVAL

– Az infrastruktúra szoftverek többi alcsoportjában – a biztonsági szoftverek, a virtualizáció, a tárolószoftverek területén – jobb a helyzet, ez a három szegmens átlagon felül fog nőni idén is, akár két számjegyű növekedéssel – mondta Marosvári Gábor. – A biztonsági szoftvereknél az informatikai vezetők nem merik csökkenteni a büdzsét. A válsághoz szorosan kapcsolódó tömeges leépítések és átszervezések a magyarországi cégeket is nagymértékben érintik. Ennek kapcsán egyre több szabotázs esetről lehet hallani. Az ilyen fenyegetések ellen védekezni kell, például jogosultságkezelő rendszerek bevezetésével, különböző adatlopás elleni védelmi eszközökkel.

A tárolószoftvereknél a törvényi szabályozás „hajtja" a piacot, különösen a pénzügyi szférában. A szigorodó EU-s és nemzetközi direktívák mind abba az irányba hatnak, hogy az ügyféladatokat védeni kell, kötelezően meg kell őrizni, archiválni, és ez növekedést gerjeszt ebben a szegmensben. A virtualizáció is jó lehetőségeket kínál. Ha egy virtualizációs projekt konszolidációval párosul, akkor az egyértelmű, kézzelfogható hatékonyságnövelő előnyöket hoz, főként a nagy és közepes cégek IT-szervezeteinél. A meglévő IT-erőforrások jobb kihasználását teszi lehetővé egy alacsonyabb működési költségszint mellett. Minden olyan informatikai beruházás, amely gyors megtérülést hoz és kézzelfogható üzleti hatékonyságnövekedés érhető el vele, idén is keresett lesz.

VÉGZETES A ROSSZ DÖNTÉS

A következő nagy kategória az alkalmazásfejlesztő szoftvereké; ide tartoznak az adatbázisok, a fejlesztőeszközök, a köztes szoftverek és az üzleti intelligencia. Itt is árnyalt a kép. A relációs adatbázis-kezelők határozzák meg ennek a piacnak a fejlődését, de ez a szegmens idén Magyarországon nem kecsegtet sok jóval. **Elmaradnak ugyanis a nagy alkalmazásbevezetési projektek, leszámítva néhány, EU-s forrásból megvalósuló kiemelt e-kormányzati tendert.** Jellemzően karbantartás típusú lehetőségek lesznek az adatbázispiacon, de ez kevés lesz ahhoz, hogy kompenzálja az új licenceladások csökkenése miatti bevételkiesést. Egy másik nagy vesztes lehet idén a fejlesztőeszközök szegmense. Az okok nagyjából ugyanazok, mint az adatbázisoknál: csökkenő alkalmazásfejlesztési kedv, kevesebb alkalmazásimplementáció. Jobb lehetőségek mutatkoznak a köztes szoftverek szegmensében, ezen belül is az automatizációs middleware-ek terén, amelyek képesek az üzleti folyamatokat automatizálni, és optimalizálják a cégek üzleti működését. Különböző BPM-, BPA-alapú alkalmazásintegrációs törekvések, az üzleti szolgáltatások összekapcsolása előremenekülési lehetőséget jelenthetnek a nagy szolgáltató cégeknek.

Az üzleti intelligencia is kitörési pont lehet – elsősorban a felső vezetői igényeket lefedő jelentéskészítő-elemző eszközök esetében. Ezek szintén kézzelfogható hatékonyságnövelő előnyökkel járnak, kkv-knál és nagyvállalati szinten egyaránt. Az üzleti intelligencia alkalmazásával ugyanis jobban előkészített, megalapozottabb döntéseket tud hozni a cégvezetés. Ennek mindenképpen lesz keletje Magyarországon: itt is két számjegyű piaci bevételnövekedés várható. Ez még egy viszonylag alulfejlett piac, főként a kkv-k szintjén. Azoknál a cégeknél azonban, ahol már van valamilyen back-office rendszer, logikus fejlődési fázis egy ilyen rendszer bevezetése.

KIAKNÁZATLAN PIAC A KKV-SZEKTOR

A szoftverpiac harmadik nagy pillére az üzleti alkalmazások szegmense. Ez is ambivalens képet mutat: vannak olyan alkalmazástípusok, amelyek lendületesen növekedni fognak, és olyanok, amelyek visszaesnek. Az már látszik: a szállítók úgy próbálnak védekezni a válság okozta bevételkiesés ellen, hogy megemelik az alkalmazásokhoz kapcsolódó karbantartási díjakat. De ez kevés ahhoz, hogy kompenzálják az új alkalmazások bevezetésének elmaradásából származó bevételkiesést. Itt is legalább 3-4 százalékos bevételzsugorodásra lehet számítani. A válság nagy vesztesei a nem üzletkritikus alkalmazások lesznek (például a levelező- vagy mérnöki tervezőrendszerek). Emellett sok nagyvállalati, stratégiai ERP- vagy vertikális alkalmazásbevezetési projektet már a tavalyi év végén töröltek vagy átütemeztek.

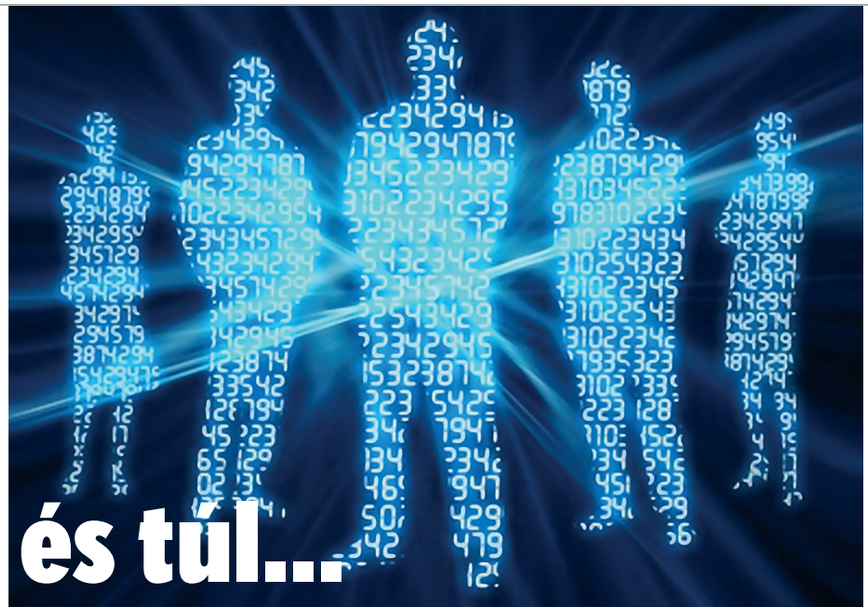
Az alkalmazáspiacon azok a csoportmunka-eszközök terjedhetnek, amelyek csökkentik a cégek járulékos költségeit, például az utazási kiadásokat, telefonköltségeket – népszerűek lehetnek a videokonferencia- vagy aunified communication alkalmazások. A nagyvállalati ERP-piac stagnálni fog, de a low-end piacon vannak lehetőségek. ERP-fejlesztésre lehet számítani olyan kkv-któl, amelyek elnyernek egy-egy EU-s támogatást, illetve azoktól, amelyek felismerik, hogy egy jól előkészített ERP-projekt hosszabb távon hatékonyságnövelést tud hozni. Látni kell azonban, hogy **a kkv-k nagy része komoly likviditási gondokkal küzd, ráadásul itt az informatikai kultúra is hagy kívánnivalókat maga után:** sok cégnél az IT egyszerűen nem prioritás. Vagy ha meg is fogalmazódik az igény, akkor elvárják, hogy személyre szabott megoldást kínáljanak nekik nyomott áron, de nem biztos, hogy a szállítónak így már megéri a befektetést. Az IDC nemrég készített egy modellt, amely azt mutatta, hogy Magyarországon több tízezer olyan kkv van, ahol lenne létjogosultsága valamilyen ügyviteli vagy ERP-rendszer bevezetésének. Ez hatalmas potenciál, de a szállítóknak még nagyon sokat kell dolgozniuk ahhoz, hogy megismertessék ennek előnyeit.

Szintén fontos terület a CRM. A nagy bankok, pénzügyi szolgáltatók és közműcégek várhatóan folytatni fogják idén ügyfélszolgálataik korszerűsítését, főleg elektronikus ügyfélszolgálati csatornáik fejlesztését. Számítani lehet kontaktcenter- és e-banking-fejlesztésekre, valamint az elektronikus számlázás bevezetésére annak érdekében, hogy a vevőkiszolgálásban maximális hatékonyságot érjenek el, és megtartsák meglévő ügyfeleiket. Egy másik fontos fejlesztési terület a sales: minden olyan megoldás, amely az értékesítési csapat hatékonyságát növeli, növekedésre számíthat idén is. – A meglévő vevők megtartása, lehetőség szerint új vevők megszerzése, átcsábítása a konkurenciától létkérdéssé vált – mutatott rá Marosvári Gábor.

Idén csökkennek a szervereladások

Az IDC március végén jelentette meg negyedéves prognózisát az idei x86 szerver operációs rendszereinek eladásaira a világon. A Microsoft Windows Server és a Linux szervereladásokat egyaránt sújtja a válság, az IDC szerint mindkettő esetében visszaesés várható.
Néhány nappal korábban jelent meg a Linux elfogadottságáról készült IDC-felmérés. A Novell támogatásával készült tanulmányt 300 informatikai vezető megkérdezésével állították össze. Közel háromnegyedük nyilatkozta, hogy cégüknél folyamatban van Linux szerver tesztelése, vagy már eldöntötték, hogy nagyobb mértékben alkalmazzák idén a vállalati IT-rendszerben. Ami a desktop verziót illeti, a válaszadók kétharmada közölte, hogy tesztelnek vagy nagyobb arányban alkalmaznak Linuxot. Az okok között első helyen szerepeltek az alacsonyabb támogatási költségek.
Matthew Eastwood, az IDC vállalati platformkutatásokért felelős alelnöke szerint a két tanulmány között nincs ellentmondás. „Rövid távon a Linux is, a Windows is visszaeséssel számolhat. Idővel azonban a Linux-eladások továbbra is növekedni fognak, mint ahogy a Windows is" – mondta.

Biztonság a gépeken innen és túl...



Szerencsére egyre több az olyan cégvezető, aki felismerte, hogy a biztonsági kérdések már rég túlmutatnak a cég biztonsági főnökének és informatikai vezetőjének a felelősségi körén, és adott esetben a cég üzleti eredményeit is képesek befolyásolni. [Írta: Csörgő László]

Mivel a cégek informatikai és biztonságtechnikai feladatainak a megoldása mára az IT-iparág egyik legjelentősebb üzleti szegmensévé nőtte ki magát, a felelős döntéshozók és szakemberek – gyakorlatilag pillanatok alatt – a különböző megoldások hirdetéseinek erdejében találhatják magukat. Ráadásul, mivel a legtöbb felső vezetőnek sem ideje, sem kedve nincs a számára túlságosan száraz vagy a marketingszempontokat előtérbe helyező anyagok böngészéséhez és szelektálásához, ezek az anyagok először jobb esetben a biztonságért felelős, rosszabb esetben az IT-vezető asztalára kerülnek. Ha belegondolunk, hogy a terület átlátását mennyi régi időkből származó (mára legalábbis újragondolásra érdemes) elv és a cégek mérete és/vagy felépítése miatt előforduló gyakori integrációs és bevezetési probléma nehezíti, és ehhez hozzátesszük, hogy a biztonságért vagy az IT-ért felelős vezető csak a saját szakterületén van otthon, akkor a problémák csúcsát már láthatjuk.

ÖNTSÜNK TISZTA VIZET A POHÁRBA!

Először is tisztázni kell, hogy egy jól működő – a valós életben is bizonyító – teljes biztonsági rendszer nem olcsó befektetés. Csakhogy még mindig olcsóbb lehet, mint egy komolyabb biztonsági probléma okozta kár, ami az üzleti eredményeket is befolyásolja. Ráadásul az ilyen károk a mai gazdasági helyzetben a piaci lehetőségek általános zsugorodásával egyre gyakoribbak is lehetnek. Ha rendszerben gondolkodunk, akkor a biztonsági kérdéseknek az IT-n kívül is meg kell jelenniük, többek között a HR-ben és a fizikai biztonságban is. Érdekes megfigyelés, hogy kevés az a cég, amelynél hatékonyság szempontjából a biztonságért és IT-ért felelős vezető a vállalati hierarchiában a megfelelő helyen van. Nézzünk egy példát: hazánkban **a legtöbb komoly cégnél a marketing végre nem csak egy felirat a cég 23. irodájának ajtaján, és nem olyan emberek gyűjtőneve, akik a hirdetésekkel foglalkoznak, hanem alapvető és meghatározó funkciója van a cég piaci stratégiájában** – tehát ma már nem is kérdés, hogy a marketingvezetőnek a csúcsmenedzsmentben a helye. Ilyen fokú kiemelésre a biztonsági területen természetesen nincs szükség, de az mindenesetre elengedhetetlennek tűnik, hogy a biztonsági főnök közvetlenül a vezetőnek számoljon be, és az is fontos, hogy az IT- és biztonsági vezető között a vállalati hierarchia szintjén ne alá-fölérendeltségi viszony legyen.

Kiemelten fontos az is, hogy a biztonsággal, az információ- és adatvédelemmel kapcsolatos előírásokat lehetőség szerint gyakorlatiasan, minden (akár rendkívüli) helyzetre alkalmazhatóan és naprakészen kivétel nélkül minden dolgozó számára elérhetővé kell tennünk – természetesen egyénre szabott formában. A régiónkban működő cégek egyelőre ilyen téren meglehetősen el vannak maradva a világ élvonalától. Éppen ezért rendkívül fontos a HR-részleg szerepe is, ugyanis az ő feladatuk az, hogy a biztonság növelését célzó képzéseket bevezessék egy vállalatnál. Több szakértő egybehangzó véleménye szerint egyelőre kivételnek kell tekintenünk azokat a cégeket, amelyeknél az információbiztonság oktatási oldalát a HR az elvárt szinten és megfelelően hatékony formában végre tudja hajtani.

GYAKORLATI PÉLDA AZ ELINDULÁSHOZ

Ha egy cégnél egy átlagos középvezetőnek lehetősége van arra, hogy egy aprócska, 16 gigabájtos USB-kulcsra vagy egy hasonlóképpen kevéssé feltűnő, irattárca méretű, de fél terabájt kapacitású külső merevlemezre a cég számára komoly értéket képviselő adatok szinte teljes körét lemásolja pár óra alatt anélkül, hogy ezt a műveletet még a kezdetekkor automatikusan leállítaná a rendszer, és biztonsági riasztást jelentene, akkor a cég gondban van. Ekkora kapacitású háttértáron ugyanis szinte bármit el lehet lopni: kiadatlan könyvek kéziratait, bizalmas gazdasági, eladási adatokat, e-maileket, címlistákat, vásárlói adatbázisokat, fejlesztői projekteket, szabadalmak dokumentációját és így tovább. Az alkalmazottak lojalitásába vetett feltétlen bizalom nem tűnik túl szerencsésnek. Manapság különösen nem, hiszen annak fényében, hogy 2008-ban számtalan cég tőzsdei részvényértéke feleződött, szinte biztosra vehető, hogy az illegális információszerzés gyakorisága radikálisan nő.

> **Régiónkban sok cégnek az a szerencséje, hogy errefelé még nem általános gyakorlat a konkurens cégnél dolgozók megkörnyékezése...**

Régiónkban sok cégnek egyszerűen az a szerencséje, hogy errefelé még nem általános gyakorlat a konkurens cégnél dolgozók megkörnyékezése átigazolás előtt azért, hogy ezen az úton szerezzenek fontos információkat a konkurensről. Ez a helyzet azonban két-három éven belül akár 180 fokos fordulatot is vehet. A régebbi IT-kultúrájú (és demokráciájú) országokban egyébként már igencsak konkrét eszközökkel próbálja meg az állam presszionálni a cégeket és intézményeket arra, hogy az általuk kezelt adatokra vigyázzanak. **Angliában például gyakorlatilag automatikusan küldik a pénzbüntetést abban az esetben, ha bizonyíthatóan illetéktelenek kezébe kerültek egy-egy intézmény adatai.** Mivel a büntetést adatbázis-rekordonként kell fizetni, már egy pár százas rekordot tartalmazó információvesztés (pontosabban: információszivárgás) is komolyabb összegű bírságot vonhat maga után. A helyzet kétségkívül lehangoló, ha az előbbi megközelítésben vizsgáljuk meg a kérdést.

KOMPLEX MEGOLDÁSOK

Ugyanakkor szerencsés helyzetben is vagyunk, hiszen a számunkra új keletű fenyegetés Nyugat-Európában és a tengerentúlon már régen jelen van. Ezért jó pár cég foglalkozik a mind teljesebb körű biztonsági megoldásokkal. Ennek egyik előnye az, hogy az ilyen cégek portfóliója nincs szorosan limitálva,

magyarán, nemcsak egy bizonyos biztonságtechnikai megoldásszállítót vagy rendszert tartalmaz. Az sem elhanyagolható, hogy **az ilyen biztonsági integrátor cégek olyan hiányosságokra is rá tudnak világítani, amelyekre egy adott speciális területtel foglalkozó cégnek általában nem terjed ki a figyelme.** Például egy hackertámadások elleni eszközöket szállító valószínűleg nem fogja megjegyezni az egyeztetésen, hogy a megrendelőnek – tapasztalata szerint – nincs jól működő biztonsági gyakorlata a telephelyére látogató vendégekkel, partnerekkel és a kiszolgáló személyzettel szemben, és hogy első körben (vagy párhuzamosan) erre is figyelmet kellene fordítani. Azaz bármilyen jó is lesz ezek után a hackerek elleni védelem IT-fronton, ha például a szerviztechnikusként bemutatkozó illegális behatolót a portás maga kíséri fel az irodákhoz.

Az információ védelmének jelenleg is számtalan módozatát ismerjük, és az sem titok, hogy ezek különböző hatékonyságú módszerek. Régi igazság, hogy egy rendszer annyira erős, mint a leggyengébb láncszeme. Ma már a behatolók (melyek a statisztikák szerint többnyire belső dolgozók) adatlopási kísérleteinek legidőigényesebb része az, hogy megtalálják ezt a leggyengébb láncszemet. Éppen ezért azok a védelmi rendszerek a leghatékonyabbak, amelyek minden részfeladat megoldására és összekapcsolására képesek, és ezáltal teljes körű védelmet nyújtanak. Ezeket a rendszereket egyszerűbb menedzselni is, beleértve itt a komplett port- és eszközkontrollt, a hozzáférések információszintű lebontását és menedzsmentjét. Az információvédelem frontján például a legnagyobb gyártók, a Symantec, a McAfee, a Websense megoldásaival (csak hogy a legismertebb konkurens gyártókat említsük) lehetőség van a hatékony védekezésre.

Az egyik legdivatosabb hívószó a biztonság terén jelenleg a DLP, amely a Data Loss Prevention rövidítése *(lásd bővebben Féken tartott adatok, Computerworld 2009/11. szám)*. Hatalmas előnye a megközelítésnek, hogy hatékonyan járul hozzá az egyenszilárdságú védelem megvalósításához, hiszen a technológia alkalmazásával az adatokhoz való hozzáférés, azok feldolgozása és továbbítása is csak a megfelelő jogosultságok birtokában lehetséges. Így **a védelmi rendszerben esetleg meglévő hiányosságok a DLP bevezetésével adott esetben nagyságrenddel csökkenthetők.** Egy DLP-rendszer minimálisan a végpontokon, fájlszervereken, a web- és e-mail átjárókon elemzi az átáramló információt, de a legjobb rendszerek képesek a nyomtatószervereken OCR-technológiával, a Sharepoint-szervereken, sőt akár a hálózat tetszőleges pontján, áramlás közben felismerni (és szükség esetén blokkolni) az érzékeny adatokat.

Az egyes rendszerek között perdöntő különbség lehet az érzékeny információ meghatározásának, majd felismerésének módszere és hatékonysága, különösen igaz ez az állítás a magyar nyelvi környezetre. A területen vezetőnek számító Websense DLP-technológiája például szöveges állományokat is képes felismerni akár egyetlen bekezdés egyezése esetén, de meghatározható az is, hogy egy adatbázisból hány rekord vagy rekordrészlet továbbítására van jogosultsága egy felhasználónak. Mi több, nem szükséges a copy/paste metódust vizsgálni, mivel ha az adattolvaj az információt egyszerűen újragépeli, akkor is megállítható az adatszivárgás.

JOGSZABÁLYI PROBLÉMÁK

Ha kicsit eltávolodunk az IT nézőpontjától, akkor tapasztalhatjuk, hogy a hazai jogi szabályozás és a céges biztonsági főnökök viszonya is meglehetősen érdekes képet mutat. Mivel a terület jogi szabályozás szempontjából eléggé általánosra sikerült, sok esetben a biztonsági vezetők érdeklődési köre és a jogi előírások által lefedett terület nem mindig esik egybe. Például születhet olyan döntés, hogy bár az előírások miatt az egyik biztonsági terület megoldása fontos lenne, mégsem foglalkoznak vele, mert azt nem tartják a cég számára valós biztonsági kockázatnak. Ezért adott esetben olcsóbb büntetést fizetni, mint azzal a területtel foglalkozni. A jogilag nem szabályozott másik terület viszont már jelenthet biztonsági kockázatot a vállalatnak, és azzal – előírások ide vagy oda – már komolyan foglalkoznak. Természetesen a cégek biztonsággal kapcsolatos, alapvetően költségszempontú hozzáállása is érthető, de együtt tudunk érezni a jogalkotókkal is. Az ideális állapot mégis az lenne, ha egyrészt a szabályozás is életszerűbb és naprakészebb lenne a jelenleginél, másrészt a cégek is megtalálnák a maguk sebezhetetlen megoldásait.

Az elkövetkező évek fontos kihívása az lehet a biztonságtechnikai területen, hogy mennyire lesznek képesek a cégek a saját adataikra úgy tekinteni, mint egy állandóan védendő, értékes információra, és a döntéshozók mennyire tudnak majd az egyes részmegoldások helyett hatékony rendszerben gondolkozni. **Az információbiztonság sokkal inkább egy általános, mindenre kiterjedő vezetési elv, mint egy szimpla szakterület, és mára jóval fontosabbá vált annál, hogy azt teljes egészében egy IT-vezetőre merjük bízni.** Hiszen már maga a szó is túlmutat a számítógépeken, a kábeleken és a programokon, bár kétségkívül ezek jelentik az alapot. A biztonsági disztribúcióval foglalkozó cégeknek mindenesetre elég komoly jövőt jósolhatunk az elkövetkező években csakúgy, mint az új szemléletű, teljes körű, kimondottan információbiztonsági rendszereknek.

Fontosabb adatvédelmi jogszabályok

A 2001. évi CVIII. törvényt 2003-ban egészítették ki adatvédelemmel kapcsolatos funkciókkal. (Az elektronikus kereskedelmi szolgáltatásokkal és információs társadalommal kapcsolatos kérdéseket szabályozza.) A 2003. évi XCVII. törvény rendelkezéseinek többsége jelenleg is hatályos.

1992. évi LXIII. törvény – A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról (2005. június 1-jétől hatályos)

Adatbiztonság:

– 10. § (1) Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

(2) Az adatokat védeni kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.

Macre is épül

A Mac OS X operációs rendszerekre épülő számítógépek között egy olyan trójai kezdett terjedni, amelynek célja botnet hálózat kiépítése, és elosztott szolgáltatásmegtagadási támadások kezdeményezése. [Írta: Kristóf Csaba]

A rosszindulatú programok jelentős részének alapvető célja, hogy fertőzött számítógépekből álló, jól irányítható, kártékony botnet hálózatokat építsen ki. Az elmúlt években mindezt olyan intenzitással tették, hogy napjainkra már PC-k millióit képesek bevetni a támadók a különféle kártékony tevékenységeik végrehajtásakor. A botnetek a legtöbbször kéretlen elektronikus levelek nagy mennyiségű küldésére, valamint elosztott szolgáltatásmegtagadási támadások kezdeményezésére alkalmasak, és adott esetben jelentős anyagi haszonszerzéssel kecsegtetik az üzemeltetőiket. Ők sokszor bérbe is adják a számítógépes károkozóikkal kiépített hálózatokat, illetve az azok által biztosított erőforrásokat.

A botnetek létrehozóinak és üzemeltetőinek célja, hogy hálózataikat minél decentralizáltabban működtessék, ugyanis a múlt évben – egyes szolgáltatók tevékenységének beszüntetésével – több olyan szerver is leállt, amelyet nagy kiterjedésű botneteket vezéreltek. Jó példa volt erre a McColo internetszolgáltató működésének felfüggesztése is – ennek hatására a kéretlen levelek terjedése globális szinten jelentős mértékben visszaesett. A spamek számának csökkenése azonban átmeneti volt, ugyanis a botnetek újraéledtek, és napjainkban már ismét rekordokat döntöget a levélszemét mennyisége. A problémát tovább fokozza, hogy a mostani botnetek már sokkal inkább alkalmasak arra, hogy egy-egy szolgáltató leállítását átvészeljék, ezért a hatóságok, illetve a biztonsági cégek feladata is egyre nehezebbé válik.

TELHETETLEN BOTNETÉPÍTŐK

Az elmúlt időszakban a botnetek kapcsán az is kiderült, hogy e kártékony hálózatok mögött álló csoportok meglehetősen telhetetlenek. Legalábbis ezt tükrözi a Conficker féreg irtó hadjárata is, amely tavaly november óta terjed, elsősorban egy windowsos sebezhetőség kihasználásával, valamint a cserélhető adattárolók adta lehetőségek kiaknázásával. A féreg egyes becslések szerint több mint tízmillió rendszerre került fel, és jelenleg is készen áll arra, hogy teljesítse a támadók parancsait. A Conficker terjesztői azonban még ennyivel sem érték be, hiszen a Trend Micro szerint most azon mesterkednek, hogy a saját botnetjüket összeolvasszák a Waledec nevű hálózattal.

Az nem kérdés, hogy a botnetek mögött álló személyek minden lehetőséget megragadnak arra, hogy a lehető legtöbb rendszert uralják. A legfrissebb biztonsági jelentések szerint most már azzal sem elégednek meg, hogy „csak” a Windows operációs rendszerekre épülő számítógépeket kebelezik be, ugyanis a Macintosh platform felhasználásával is elkezdtek kiépíteni egy botnetet, amely iBotnet néven kezdte meg a működését.

TEREBÉLYESEDIK AZ IBOTNET

Az iBotnet tulajdonképpen egy Mac OS X-kompatibilis trójai tevékenykedésére alapozza a működését, amelyről a Trend Micro, a Symantec és egyéb biztonsági cégek már az év elején beszámoltak. A legtöbbször iService-ként emlegetett kártékony program januárban elsősorban fájlcserélő hálózatokon kezdett terjedni, és napjainkban is fellelhető azokon. Többnyire a fájlcserélőkön megosztott iWork ’09 és Adobe Photoshop szoftverek kalózmásolataiba rejtve kerül rá a számítógépekre. Amikor a felhasználó letölt egy ilyen fertőzött szoftvert, majd elindítja azt, akkor a trójai azonnal aktiválódik. **Ezt követően egy hátsó kaput nyit a rendszereken, amelyeken keresztül a támadók jogosulatlanul férhetnek hozzá a számítógépeken tárolt adatokhoz, illetve egyes esetekben kártékony műveleteket hajthatnak végre.** A trójai általában az 1024-es TCP-porton keresztül kapcsolódik az internethez. A kártevő állományai variánstól függően az alábbi könyvtárak valamelyikébe kerülhetnek be:

/System/Library/StartupItems/DivX
/System/Library/StartupItems/iWorkServices

Arról, hogy az iService által kialakított botnet aktivizálódott, két kutató, *Mario Ballano Barcena* és *Alfredo Pesoli* számolt be. A szakemberek szerint az eddig két variáns formájában terjedő trójai a jövőben új változatokban is felbukkanhat, ugyanis a kódját úgy alakították ki a készítői, hogy az rugalmasan legyen módosítható.

A Symantec szerint a kártékony program a felfedezése előtt néhány ezer számítógépet fertőzhetett meg, és mostanra pár tízezerre tehető azon Mac számítógépek száma, amelyeken jelenleg is megtalálható. Ez ugyan jó néhány windowsos botnet méretéhez képest nem tűnhet figyelemre méltónak, azonban az iBotnet jelentősége elsősorban abban rejlik, hogy ez az első olyan kártékony program, amely komolyabb, Mac-alapú botnetet kezdett kiépíteni.

Az iBotnet létezését a McAfee is megerősítette. *Joris Evers*, a McAfee szóvivője szerint a januárban felfedezett Mac-kompatibilis trójai program olyan szoftvert telepített a számítógépekre, amely távoli hozzáférést, illetve vezérlést tett lehetővé. Ezt követően a saját P2P hálózatán keresztül további rendszerekhez kezdett kapcsolódni, és parancsokat fogadni. A McAfee úgy látja, hogy az iBotnetet elsősorban szolgáltatásmegtagadási támadásokhoz lehet felhasználni, amelyek weboldalak, illetve webszerverek megbénulásához vezethetnek.

A *Washington Post* információi szerint az iBotnet a szolgáltatásmegtagadási támadások terén már megkezdte tevékenységét. Elsőként a dollarcardmarketing.com weboldalt vette célba, amelynek üzemeltetője megerősítette, hogy az oldalt valóban DoS-támadás érte, és az adatforgalom jelentősen megnőtt. Ez azonban nem vezetett a webhely megbénulásához vagy összeomlásához.

VÉDTELENÜL HAGYOTT RENDSZEREK

Az iBotnet kapcsán az ESET cég is megszólalt. *Randy Abrams*, az ESET egyik igazgatója az *SC Magazine* amerikai kiadásának elmondta, hogy a maces közösség még mindig azt hiszi, nincs szüksége antivírusalkalmazásokra. Ezért a Mac OS X esetében a víruskereső szoftverek elterjedtsége kisebb a windowsos világhoz képest.

Botnet neve	Számítógépek száma	Spamkapacitás (milliárd/nap)
Conficker	10 000 000+[	10
Srizbi	315 000	60
Bobax	185 000	9
Rustock	150 000	30
Cutwail	125 000	16
Storm	85 000	3

Forrás: SecureWorks (árpilisi statisztika), F-Secure

Vitathatatlan, hogy a Mac OS X-kompatibilis vírusok száma jóval csekélyebb, mint a Windows platformon működőképes kártevőké. Ennek ellenére – ahogy azt az iBotnet tevékenykedése is alátámasztja – napjainkban már a Mac OS X védelmét sem érdemes félvállról venni. *Graham Cluley*, a Sophos szakértője a trójai januári felfedezésekor úgy vélekedett, hogy ugyan a Macintosh számítógépek ritkán esnek áldozatául kártékony programoknak, mindez nem jelenti azt, hogy a probléma nem is létezik. „Az Apple-felhasználók nem dughatják a fejüket a homokba, amikor a biztonság kerül szóba” – tette hozzá Cluley.

VÉDEKEZÉS EGYSZERŰEN

Az iService trójait tulajdonképpen az összes Mac OS X-kompatibilis vírusvédelmi alkalmazás képes felismerni és eltávolítani. Ezért a rosszindulatú program elleni védekezés egyik leghatékonyabb módja a megfelelően frissített víruskeresők használata, illetve a fájlcserélők megfontolt kezelése. Ugyancsak fontos, hogy a Macintosh számítógépek esetében is mind az operációs rendszer, mind az azon futó alkalmazások biztonsági frissítése rendszeresen megtörténjen. A támadók ugyanis az Apple és a különféle Mac OS X-kompatibilis szoftvereket fejlesztő cégek által közzétett sebezhetőségek kihasználására is egyre nagyobb figyelmet fordítanak, ami kockázatot jelent.

Isten veled, Silicon Graphics!

Április 1-jén kért csődvédelmet az a cég, amelynek neve a 80-as, 90-es években egyet jelentett a 3D-s animációval. Összeállításunkban sorra vesszük a Silicon Graphics történetének legfontosabb eseményeit. [Írta: Samu József]

A Silicon Graphics vagyonáért 25 millió dollárt fizet a Rackable Systems, és a cég gyakorlatilag megszűnik. Ez a második eset a Silicon Graphics történetében, hogy csődöt jelent, de úgy fest, ez alkalommal nem lesz folytatás. **A Rackable Systems a számítógéppel segített tervezés területén szeretne terjeszkedni, így a beruházással leginkább a Silicon Graphics szolgáltatásaira és ügyfélkörére utazik, mintsem a cég termékeire.**

1981-ben egy évre voltunk attól, hogy piacra dobják a korszak meghatározó mikrogépeit: a Sinclair Research a ZX Spectrumot, a Commodore pedig a Commodore 64-et. *Jim Clark* és *Abbey Silverstone* ekkor alapította meg a Silicon Graphics Incorporatedet (SGI) eredetileg azért, hogy 3D-s grafikus terminálokat gyártsanak.

A MOTOROLA 68000-ES IDŐK

A cég első generációs termékei az IRIS 1000 (Integrated Raster Imaging System) sorozatú, nagy teljesítményű grafikus terminálok voltak, amelyek Motorola 68000-es processzorokra épültek – ugyanarra a CPU-ra, mint a korszak legendás gépei, például az Atari ST, az Apple Macintosh vagy a Commodore Amiga. A későbbi IRIS 2000 és 3000 modelleket már teljes értékű Unix munkaállomásokká fejlesztették.

Az IRIS 1000-es sorozat első tagjai általános célú számítógépekhez csatlakoztak; a Digital Equipment Corporation VAX-ai, a későbbi 2000-es, 3000-es gépek abban az időben nagyon vonzók voltak. A 3130-as például elég nagy teljesítményű volt ahhoz, hogy teljes 3D-animációs és leképezési (rendering) feladatokat lásson el anélkül, hogy ehhez a háttérben egy nagygépnek (mainframe) kellett volna dolgoznia. Nagy kapacitású merevlemezekkel – két 300 megabájtos meghajtó –, streamerrel és Ethernet hálózati csatlakozással akár egy teljes animációs művelet központi gépe is lehetett. A sorozatot 1989-ig gyártották, és összesen körülbelül 3500 darab 2000-es és 3000-es IRIS-t értékesítettek.

Az SGI legjobb éve az 1995-ös volt:

a cég értéke a 7 milliárd dollár közelében járt, és közel 10 ezer főt foglalkoztatott.

RISC-ÉRA

Az 1980-as évek közepén piacra dobott IRIS 4D sorozattal az SGI átnyergelt a MIPS Computer Systems RISC mikroprocesszor-architektúrájára. Ezek a gépek nem csak nagyobb teljesítményűek voltak a korábbi, Motorola-alapú termékeknél, de több memóriát voltak képesek megcímezni. Az SGI alapvetően ezeknek köszönhette hírnevét, no meg annak, hogy a 3D-s animációk használata egyre népszerűbbé vált a televíziós közvetítésekben és a filmekben.

A cég kiterjedt MIPS-alapú munkaállomás- és kiszolgálókínálattal volt jelen a piacon az 1990-es években, ezek az SGI saját, IRIX nevű Unix System V változatára épültek. Köztük voltak a masszív, háztartási hűtőgép méretű Onyx vizualizációs rendszerek, amelyek akár 64 processzort is tartalmazhattak, és képesek voltak megbirkózni három, nagy felbontású 3D-s grafikai streammel is.

1992-ben a MIPS piacra dobta első 64 bites mikroprocesszorát, az R4000-et, ami az első, szabad kereskedelmi forgalomban is kapható – értsd: nem katonai célú vagy célhardverbe épített – 64 bites RISC CPU volt. (Ezt aztán hamarosan követte a Digital Alphája és mások is.) Az IRIX 6.2 lett az első teljesen 64 bites IRIX-változat, beleértve a 64 bites pointerek használatát is. Az SGI 2006-ban fejezte be a MIPS/IRIX rendszerek forgalmazását.

IRIS GL ÉS OPENGL

Egészen a második generációs Onyx gépekig, amelyekben az SGI a Reality Engine grafikus alrendszert használta, a cég gépeinek grafikus alrendszerei az IRIS GL-en (IRIS Graphics Language) keresztül voltak programozhatók. Ahogy az évek során egyre több szolgáltatással vértezték fel a hardvereket, egyre nehezebb volt a cég saját alkalmazásprogramozói interfészét (API) fenntartani – és még nehezebb használni.

1992-ben az SGI úgy döntött, hogy itt az ideje tisztába tenni az alaposan felszemetesedett IRIS GL-t, és létrehozták az OpenGL-t. Az API-t olcsón licencelhette bárki, a szabvány karbantartásának feladatára pedig létrehozták az OpenGL Architecture Review Board nevű szervezetet. Az OpenGL lett az első gyors és hatékony, operációs rendszertől független, valós idejű 3D-s grafikai szabvány. Manapság legfőbb konkurense a Microsoft Direct 3D-je, de az csak a Windowsokat futtató számítógépekkel kompatibilis.

TÜNDÖKLÉSE ÉS...

A cég a 90-es években volt a csúcson. **A filmipar nagy fogyasztója volt a cég termékeinek, a Terminator 2, a Jurassic Park, de a Gyűrűk Ura**

SGI O2, belépő szintű Unix munkaállomás 1996-ból, minden idők egyik legszebb asztali gépe

trilógia speciális effektusainak elkészítéséhez is SGI-gépeket használtak. Más filmek mellett a Jurassic Parkban fel is bukkan egy SGI-gép – itt hangzik el az a legendás mondat a tizenkevés éves karakter szájából, hogy: „Ezt ismerem! Ez Unix!" – amin nem átallottunk hangosan röhögni a moziban.

Az SGI legjobb éve 1995 volt, amikor a cég értéke a 7 milliárd dollár közelében járt, és közel 10 ezer főt foglalkoztatott. Azonban ahogy az SGI-gépeknél sokkal megfizethetőbb PC-k grafikus teljesítménye megközelítette a cég legfontosabb üzletágának számító grafikus munkaállomások teljesítményét, úgy esett vissza a kereslet iránt. Valahol morbid, de számos, grafikai hardverfejlesztéssel foglalkozó mérnök hagyta ott a céget, és ment át olyan vállalatokhoz, mint a 3dfx, az ATI vagy az NVIDIA, hogy ott éppen az SGI sírját megásó, PC-s 3D-s fejlesztésekkel foglalkozzon.

Az SGI ezért igyekezett a grafikus munkaállomások helyett a nagy teljesítményű, digitális videózást és webes alkalmazásokat kiszolgáló szerverek felé fordulni, de az ezen a területen is erős konkurenciával kellett volna felvennie a versenyt. Az SGI megoldásainál lényegesen olcsóbb Linux- és BSD-alapú, x86-ra épülő szerverek, fürtözött gépek tovább erodálták a cég piacát.

SGI Octane, 1997–2000

ELHIBÁZOTT MANŐVEREK

A piac zsugorodása mellett az SGI több – fogalmazzunk így – rosszul sikerült akvizíciót és eladást is végrehajtott. 1995-ben felvásárolta a 3D-s modellező szoftvereket készítő Alias Research-öt és a Wavefront Technologiest, egy vállalatban egyesítve a kettőt Alias Wavefront néven. (A formációt jelenleg Alias Systems Corporationnek hívják.) 2004-ben az SGI az Accel-KKR nevű magántőke-befektető társaságnak 57,1 millió dollárért adta el a céget, amit az 2005 októberében 182 millióért adott tovább az Autodesknek.

1996 februárjában az SGI felvásárolta az ismert szuperszámítógép-gyártó Cray Researchöt 740 millió dollárért. A lépést már akkor értetlenül fogadta a piac, hiszen a két cégben nem sok közös volt: eltérő technológiákat alkalmaztak, és különböző piacokat céloztak. Három hónappal később a cég eladta a Cray SPARC/Solaris részét a Sun Microsystemsnek egy nem nyilvános összegért – ezt a széles körben elfogadott pletyka 50 millió dollárra teszi. 2000 márciusának végén az SGI a Cray márkanevet és termékvonalat eladta a Tera Computer Companynak – utóbbi később Cray-re nevezte át magát –, cserébe 35 millió dollárt és 1 millió dollár értékű részvényt kapott.

2000 szeptemberében az SGI átvette az Intergraph Computer Systems Windows-alapú Zx10 munkaállomás- és szervertermékeit, hogy azokat saját márkaneve alatt értékesítse, de végül 2001 júniusában felhagyott a próbálkozással.

SGI Iris Indigo R3000, Elan grafikus opcióval a kilencvenes évek elejéről

HOSSZAN TARTÓ, SÚLYOS BETEGSÉG UTÁN...

1998-ban a Cray bejelentette, hogy többé már nem fejleszt saját processzorokat, és Intel Itaniumra épülő rendszerek fejlesztésébe fog. Az átállás azonban óriási késéssel jött csak létre, és az Itanium teljesítménye is elmaradt a várakozásoktól, így az ügyfelek érdeklődése erősen megcsappant. A cég csak 2001-ben dobta piacra első ilyen rendszerét, addig MIPS-alapú fejlesztésekkel próbálta fenntartani piaci jelenlétét. Ezek iránt igencsak kicsi volt a kereslet, hiszen az ügyfelek tudták, hogy hamarosan bekövetkezik az Itaniumra váltás. A MIPS-ről való átállás egyben az IRIX végét jelentette: a cég gépei SUSE Linuxszal érkeztek, a régi alkalmazásokat pedig egy valós idejű fordító végezte.

2005 novemberében az SGI-t a New York-i értéktőzsde kivezette, mert a cég papírjainak árfolyama nem érte el a szükséges minimumot. Az SGI értéke tíz év alatt 7 milliárd dollárról 120 millióra zuhant.

2006 májusában a cég csődvédelmet kért, a mély gödörből csak őszre tudott kilábalni. Új stratégiája szerint általános célú szerverek előállítása jelentette volna az SGI jövőjét, de az amúgy is telített piacra a hitelét vesztett SGI-nek már nem sikerült visszakapaszkodnia. 2008-végén a cég értékpapírjait ismét kiebrudalták a tőzsdéről, bevételei tovább csökkentek, a veszteségek nőttek, és nagyjából 1000 alkalmazott maradt a 35 millió dolláros piaci értékű cégnél.

A válság az utolsó szöget is beverte az SGI koporsójába. Jelenleg a vállalkozás továbbviteléhez olyan tőkeinjekció kellene, amelynek a kockázatát nem merik vállalni a befektetők. A mérnöki és tudományos célú clusterekre szakosodott, nagyjából háromszáz főt foglalkoztató Rackable Systems most 25 millió dollárt ad az SGI-ért, ami még így is 15 százalékkal több, mint ami a szebb napokat látott SGI piaci értéke.

Internetszolgáltatások – mobil internet

Az internet mára univerzális kommunikációs infrastruktúra lett. Cégeknek és magánszemélyeknek is fontos, hogy hozzáférjenek – ám közel sem mindegy, hogy milyen módon. [Írta: Makk Attila]

A hálózatok, majd az internet mára gyakorlatilag egyetlen csatornába terelte a kommunikáció különféle módjait. Egyetlen infrastruktúrát kell fenntartani egyetlen belépési ponttal. Ez persze kockázatot is jelent: egyetlen vonal elvágása minden kommunikációt megszüntet. Ez ellen lehet, és kell is védekezni, tartalék vonalak beállításával –, ahogy egy kórháznak vagy más folyamatos működést megkövetelő üzemnek is van megfelelő eszköze az áramellátás megszűnése esetére.

Az internet modellje a felhasználó szempontjából: van egy nagy kapcsolóközpont, egy fekete doboz, a szélén konnektorokkal, amelyeken keresztül a felhasználó igénybe veheti a kapcsolóközpont szolgáltatásait. Azaz más végpontokkal – ez esetben a konnektorokhoz csatlakozó felhasználók – kapcsolatba léphetnek az internet által adott szabályokkal (protokollok). A felhasználó szempontjából a konnektorok az érdekesek: mi módon tud hozzájuk kapcsolódni, hol, milyen szolgáltatásokat tud igénybe venni, és nem utolsósorban mennyiért?

Az internetszolgáltatást kínáló cégek az ISP-k. Vannak globális, nemzeti, valamint regionális és helyi szolgáltatók. A végfelhasználó általában a helyi szolgáltatóval kerül kapcsolatba, ott fizet elő, a helyi szolgáltató „köti be" az internetet. A hierarchia magasabb szintjén lévő szolgáltatók a hierarchia alacsonyabb szintjén álló szolgáltatók számára biztosítják a kapcsolatot, de előfordul, hogy egy-egy helyen egy globális vagy országos szolgáltató közvetlen kapcsolódási lehetőséget nyújt a végfelhasználóknak.

Ez a klasszikus struktúra az utóbbi időben kicsit átrendeződik. A GSM-hálózatokat üzemeltető cégek is megjelentek országos vagy globális szolgáltatóként.

Az árak szempontjából nehéz az összehasonlítás:

a mobil netelérés és a vezetékes szolgáltatások költségeit is sok tényező befolyásolja.

Ma alapvetően kétféle módon csatlakozhatunk az internethez: vezetékkel vagy vezeték nélkül. A vezetékes megoldások alapulhatnak ADSL-en, nagy sávszélességű kábelen, vezeték nélküli megoldásokon, hagyományos telefonvonalon. Az analóg modemest is sok helyütt használják, de inkább két gép, telephely közti adatkapcsolatra. Az ADSL a hagyományos, már kiépített telefonvonalakat használja: a már kiépített vonalhálózat és az elérhető sávszélesség miatt ez a legelterjedtebb, és akár cégek számára is alkalmazható. A sávszélesség 8 megabit/s-ig terjedhet. A nagy sávszélességű kábeles megoldást külön ki kell építeni – elméletileg 30 megabit/s sávszélességre képes. A szolgáltatók 1–6 megabit/s között kínálják, és ugyanezen a kábelen telefont, tévéadást is tudnak adni. Szélessávú kapcsolat lehetséges vezeték nélkül is. Ekkor a szolgáltató építi ki a mikrohullámú láncot – ezzel a felhasználónak nem kell törődnie, ő a kábelvégződéshez csatlakozik.

A GSM-szolgáltatók a mobil internet bevezetésével komoly szeletet hasítottak ki maguknak a piacról, de megfelelő eszközök híján nem értek el jelentős áttörést. Mára viszont összejött minden: van megfelelő sávszélesség a 3G-s hálózatokon, valamint vannak megfelelő eszközök: okostelefonok, noteszgépek. Ez utóbbi növelte meg a mozgékonyság iránti igényt, amit a vezetékes szolgáltatók nem tudtak kielégíteni. A 3G-s elérés ebben verhetetlen: ahol van térerő, ott el lehet érni a leveleket, meg lehet nézni a menetrendet, vagy egy rendszergazda be tud jelentkezni távolról a szerverre. Ugyanakkor a vezetékes kapcsolat sokkal stabilabb, általában nagyobb sávszélességű – igaz, hogy csak ott, ahová bekötötték. A mobil internet sávszélessége erősen helyfüggő, és időben is változik: ha egy helyen nagy a GSM-hálózat terheltsége, akkor a válaszidő nagyon megnő, az ilyenre érzékeny alkalmazásokkal bajok lehetnek.

A mobil internet ráadásul kötődik a földi szolgáltatókhoz: a végpont kapcsolata csak a legközelebbi bázisállomásig terjed a levegőben, onnan már a szolgáltató kábelén megy a központba, ahonnan átkerül az internetre.

Az üzemeltetőknek, a folyton mozgásban lévő dolgozóknak kifejezetten megéri. Egy másik kedvező alkalmazási lehetőség a céges internetelérés mellett tartalék vonalnak fenntartani. Bár ez utóbbi nem ad teljes biztonságot, mivel az adatcsomag csak a legközelebbi bázisállomásig megy a „levegőben", onnan vezetéken folytatja az útját – és elég egy túlbuzgó markológép-kezelő, hogy az elsődleges és másodlagos vonal is megszűnjön. Az ISP-k és GSM-szolgáltatók gerincvonalai ugyanis sok helyen együtt futnak. Ezért tartalék vonalnak inkább valami nagy sávszélességű vezeték nélküli megoldást válasszunk, amely független a GSM-hálózat terheltségétől, és igen messzire elvihető a „levegőben".

Az árakat tekintve nehéz összehasonlítani a mobil netelérést a vezetékes szolgáltatásokkal. Akinek a mobilitás szükséges, annak nyilván hiába az olcsóbb vezetékes megoldás. A hazai kínálatban az a sajátos, hogy megszüntették a korlátlan forgalmú csomagokat. Bár az egyik szolgáltató a weboldalán még hirdet ilyen csomagot, ő is csak megszorítással: havi 5 gigabájt forgalom átlépése után lassíthatja az adatforgalmat. A mobil internetelérés sávszélessége helytől/időtől függ, ára pedig a havi forgalomtól.

A Computerworld A mobilitás kockázatai mellékletét hirdetőink támogatták.
Elkészítésében közreműködtek: Makk Attila szerkesztő, Sz. Erdős Judit olvasószerkesztő, Berényi István tördelőszerkesztő.
Felelős kiadó: Bíró István, az IDG Magyarország Lapkiadó Kft. ügyvezetője.

Laptopok védelme, nem részlegesen

Ma már egyre gyakoribb, hogy a cégek noteszgépeket vesznek asztali munkaállomások helyett, a munkatársak rugalmasabb munkavégzése érdekében. Ez azonban egy sor új biztonsági problémát vet fel. Mobil eszközök védelme Alcatel-Lucent módra.

Attól a pillanattól kezdve, hogy egy felhasználó, hóna alatt a noteszgépével, kilép a vállalat kapuján, máris nagy kockázatot jelent a cég IT-rendszere számára. Nagyjából ahhoz hasonlíthajuk ezt a helyzetet, mint amikor egy GPS-szel követett szállítmány alagútba, aluljáróba kerül. Az IT-részleg ugyanis attól a pillanattól semmit sem tud a gépről egészen addig, amíg a felhasználó újra be nem jelentkezik róla – mondjuk VPN-en keresztül. Ám jó lenne tudni a következőket:

- Hol van a noteszgép?
- Ki használja?
- Védettek-e a háttértárán lévő adatok?
- A felhasználó tudatában van-e annak, hogy kikerült a céges védőernyő alól?
- Mikor és hogyan kerülnek a noteszgépre a frissítések?
- Miként történik a fontos adatok mentése?

A noteszgép elvesztése, ellopása sajnos mindennapos eset. Csakhogy ez az IT-vezetés, a biztonságért felelős személyek és a felhasználók számára is rémálom, hiszen majdnem biztos, hogy a saját céggel, valamint harmadik féllel kapcsolatos bizalmas adatok is voltak a gépen.

MOBILITÁS VAGY BIZTONSÁG?

Az örök kérdés, hogy pontosan hol is van a kényelem és a biztonság közti egyensúly. A noteszgépeket illetően rengeteg biztonsági módszer, eljárás van, amelyek mindegyike részmegoldást ad. A Bell Laboratories és az Alcatel-Lucent közös fejlesztése egy olyan kártya, amely éppen azt célozza, hogy tökéletes egyensúlyba kerüljön a mobilitás és a biztonság. Vegyük sorra, hogy a OmniAccess 3500 nevű kártya mely funkciói biztosítják e két követelmény harmóniáját.

Lemeztitkosítás támogatása: a kártya SmartCardként integrálható a McAfee Safeboot Full Disk Encryption- és FDE-megoldásokkal, emellett azonban a Truecrypt kötet titkosító megoldásokkal is együttműködik.

GPS: a beépített GPS úgy működik, hogy a kártya helyzete a noteszgép kikapcsolt állapotában is pontosan követhető, mivel van benne egy akkumulátor, amely 120 óra készenléti időt biztosít számára.

Távoli zárolás (remote lock): a noteszgéphez való hozzáférés a gép kikapcsolt állapotában is zárolható.

Távoli végleges lezárás: ha a noteszgép elveszett (vagy ellopták), a *remote kill* paranccsal az NLG-kártyán tárolt kulcsok távolról is törölhetők, ezáltal a titkosított kötetek biztosan elérhetetlenné válnak, titkosítottak maradnak. Ez azonban nem végleges törlés, hiszen ha szerencsés esetben megtaláljuk a laptopot, akkor távolról fel is lehet oldani a lezárást, és a titkosító kulcsok visszatöltésével az információk újra elérhetők lesznek.

> **Elsősorban olyan helyekre jó az OmniAccess 3500, ahol az állampolgárok vagy a vállalatok bizalmas, titkos információit kezelik.**

Kétkomponensű hitelesítés: a bejelentkezéshez az NLG-kártyára és a felhasználónév/jelszó párosra vagy a kártya PIN-kódjára van szükség. A kártya–noteszgép–felhasználó hármas bármely elemének cseréje esetén megakadályozható a használat.

Automatikus VPN: távoli használatkor már a Windowsba való bejelentkezés előtt felépül a VPN, és ezt még a rendszergazda sem tudja megkerülni. Ez rendkívül hatásos, mert a távolról dolgozó munkatárstól is kikényszeríthető a vállalati policyk betartása.

Tűzfal és proxy: az NLG-kártyában csomagszűrő és proxy funkció is található, ami a hálózati átjáróról programozható. Az NLG kliensszoftvere tűzfalat is tartalmaz, de az NLG-átjáró maga is tűzfal.

Módosítástól védett: az NLG ügyféloldali részét a számítógép rendszergazdai jogokkal felruházott felhasználója sem módosíthatja. Emellett felügyeli a Windows rendszer integritását, sérülése esetén riaszt, és távolról lehetőséget ad a beavatkozásra.

3G-modem: a vezetékes hálózattól távol is használható a beépített 3G-modemmel; természetesen ezen az interfészen is VPN-kapcsolatot épít fel. Itt fontos megjegyezni, hogy a kártya automatikusan mindig a legolcsóbb VPN-kapcsolatot építi fel: azaz, ha van LAN (például ADSL-en), akkor azt használja, ha az nincs, megpróbál WLAN-hálózatot keresni, és csak harmadsorban fordul a GSM-hálózathoz.

Mentés távolról, holtidőben (off-peak backup load): a noteszgépről az adatok a kártya memóriájába menthetők, ahonnan holtidőben, például hajnalban 3G-modemen keresztül feltölthetők a cég mentőszerverére. A kártya több mentőszoftvert is támogat. A mentés úgy működik, hogy ha a szinkronizálásra kijelölt könyvtár(ak)ban adatot módosítunk, mentünk, az azonnal replikálódik a kártyán, és onnan másolódik majd fel – akár kikapcsolt noteszgép esetén is – a backup szerverre.

Frissítés távolról, holtidőben (off-peak patch download): a kártya ugyanezt a folyamatot el tudja végezni visszafelé is. Letölti a frissítéseket, és amikor a felhasználó bekapcsolja a gépet, akkor azokat érvényesíti. Ezzel megoldódik az az egyébként nagyon gyakori gond is, hogy a noteszgépek használói esetleg hetekig nem dugják a céges hálózatra a gépüket, és ezért a víruskeresők, valamint az alkalmazások biztonsági frissítései sem települnek a gépükre. Ezt bővíti ki a cég, várhatóan már ez év második felében például egyik újdonságával, az e-mail prefetching szolgáltatással.

Távoli elérés: a felhasználó az AutoVPN-nek köszönhetően az üzemeltetők számára mindig elérhető, így probléma esetén könnyen be tudnak jelentkezni a gépére.

Leltár: a gép komponenseinek teljes leltára megtalálható a kártyán – beleértve a szoftverek, szolgáltatások, védett köteten tárolt állományok listáját is –, mégpedig úgy, hogy ezek az információk a kártyán keresztül bármikor lekérdezhetők a vállalat NLG-gateway-én keresztül.

DÍJAZOTT BIZTONSÁGI MEGOLDÁS

Aki szembesült már a noteszgépek üzemeltetési problémáival, annak nem kell ecsetelni ennek a kártyának az értékét. Nem véletlen tehát, hogy az OmniAccess 3500 számtalan díjat nyert: szerepelt többek között a 2008-as Global Excellence legjobbjai között, valamint elnyerte az *Internet Telephony* magazintól a Product of the Year díjat 2007-ben; a *Windows IT Pro* szerkesztősége 2008 legjobb termékének választotta, valamint elnyerte a Tomorrow's Technology Awards Winner 2008-at és az *Information Security* magazintól az Editor's choice 2008-at.

A gyártó elsősorban olyan helyekre ajánlja, ahol az állampolgárok vagy a vállalatok bizalmas, titkos információit kezelik. Kicsit meglepő talán, de a kártyának kifejezetten a javára válik, hogy az első hat támogatott nyelv között a magyart is megtaláljuk. Magyarországon nagy mennyiségben először az Országos Egészségbiztosítási Pénztár vezette be noteszgépeinek, munkatársai adatkommunikációjának védelmére.

Alcatel·Lucent

OmniAccess 3500 Nonstop
Laptop Guardian

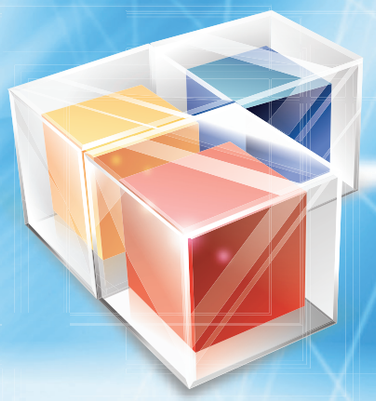
SOHA TÖBBÉ NEM LESZEK ÁLDOZAT
CUREINSECURITY.COM

Látogassa meg a www.cureinsecurity.com oldalt!

Találkozzon néhány védtelen laptoppal, akik elmondják
a történetüket és az igazi megoldásról beszélnek

Regisztációval ingyenes korlátozott idejű tesztelésre jelentkezhet

Közép-Európa legnagyobb játékfejlesztői konferenciája.



GAME DEVELOPERS FORUM

GDF2009

2009 • 04 • 30

Gyere és hallgasd meg
a legnagyobb játékfejlesztők előadásait!

Időpont: 2009. április 30, csütörtök
Helyszín: Budapest, Cinema City Aréna

Részletek: www.gdf-hu.com

Támogatók:

CRYTEK

1C COMPANY

mesh array digital media school

Autodesk

XBOX 360

GIGABYTE

Szervezők:

GameStar MCB

Kiemelt médiatámogatók:

index

PC Dome

GAMEKAPOCS online superkapocs magazin

2009. április 30. • Cinema City, Arena Plaza