2001. FEBRUÁR

EDITOR

Balkán-szindróma

A minap gazdagabb lettem egy kövér trójai programmal.

Kelenhegyi Péter

főszerkesztő

Úgy sejtem, aki hosszabb-rövidebb ideig adatvédelmi kérdésekkel foglalkozik, az előbb-utóbb kissé paranoiás lesz. Mégis merő véletlen lehet csupán, hogy a minap pár órán belül három olyan, se-tárgya-se-feladója-se-mondandója üzenet pottyant be elektronikus postaládámba, amelynek egyetlen valamirevaló tartalma egy kövér Hybris vírus volt.

Persze mi ez ahhoz képest, amit a havonta közel húszmillió online árverést lebonyolító eBay informatikusainak kellett kiállniuk, amikor a cég fő- és tartalék rendszere egyszerre állt le fél napra? Vagy mit mondhatnak magukban annak a bradwelli atomerőműnek a munkatársai, akik a napokban tudták meg, hogy múlt nyáron a létesítmény egyik, korántsem patyolattiszta előéletű biztonsági őre keresztüljutott a számítógépes védelem első szintjén, és kulcsfontosságú adatokat törölt?

És mit szólhattak magukban azok a MatávNet-előfizetők, akik január közepén megkapták nem csupán a szolgáltató online felmérésének kérdőívét, hanem egyik előfizetőtársuk levéllavinát indító válaszát is, mellé a spam ellen tiltakozók figyelmeztető leveleit, két vírusprogrammal megfejelve? Hány szál hajukat vesztették el a cég rendszergazdái, mire leállították a levélfolyamot és betömték a biztonsági rést…?

S ki tudja, hány mailboxon nyitott azóta hátsó ajtót az a jó kövér kaméleon-NPCJMANP.EXE vagy READER_ DIGEST_LETTER.TXT.PIF vírus?

Eszemben sincs szenzációt keresni az efféle hírekben. Ám bármennyire szeretnék is tompítani az új gazdaság szállászcsinálói a biztonság hiányára utaló beszámolók élét, vírusok és hackerek márpedig vannak. Valahogy úgy, ahogy Balkán-szindróma is létezik, jóllehet a betegséget nem urániummagos lövedékek okozzák, hanem környezet- és vegyi szennyezés vagy valami más. A lényeg, hogy nem elég tagadni.

Egyvalamire jók a szaftos hírek: ráirányítják a figyelmet a mulasztásokra. Amit a száraz adatok nem domborítanak ki, az neonfénnyel kezd világítani, ha a maga naturális

módján leírják, ahogy történt.

Sajnos egyes szoftverek mélyen aláásták az informatika biztonságába vetett bizalmat. Megszoktuk, hogy a számítógépek néha lefagynak, s ilyenkor nincs más teendő, mint megnyomni a reset gombot, és elbúcsúzni a képernyőre kimerevült adatoktól. Tudomásul vettük, hogy a szoftverek licencszerződéseiben szó sem esik a gyártó felelősség- és kötelezettségvállalásairól. Míg a háztartásban természetesnek tartjuk, hogy a garanciaidőn belül a gyártó szervizpartnerei felelnek a meghibásodott tévé javításáért, senkinek sem jutna eszébe garanciaidőt vagy jótállást számon kérni a megjelenésük pillanatától fogva elavult és eleve tökéletlen szoftvereken. Legföljebb menti az adatait, ahogy tudja, s ha ez sem elég, biztosítást köt.

Tudniillik az internet második korszaka csakis az adatokról szól. A gyorsaság, a hatékonyság, a belső és külső rendszerek, folyamatok összekapcsolása az információs korszak lényege, ez pedig tisztán pénzügy.

Vegyük például a bankokat, ahol a legtöbb pénz van! Jelenleg négy hazai pénzintézet kínál internetes banki szolgáltatásokat együttvéve körülbelül ötvenezer alkalmi és rendes ügyfélnek, azaz a magyar internetezők legföljebb húsz százalékának. Ám mindaddig, amíg a home banking nem nyújt nagyobb biztonságot, nincs mit csodálkozni azon, ha az ügyfél nem mer beszállni a buliba. A bankkártya-tulajdonosok túlnyomó többsége még mindig csak a bankjegykiadó automatáknál veszi elő a kártyáját, pedig illenék tudnia, hogy a banki tranzakciók költsége réz- és márványburkolatú ügyfélkiszolgálással legalább száz forint, míg internetes banki tranzakcióval csupán a tizede.

A bankoknak tehát látszólag nem érdekük áttérni az online szolgáltatásokra, még kevésbé az intelligens memóriakártyákra. Holott a mágneskártya biztonságáról már ezerszer elmondták, amit lehetett. Persze a chipkártya sem az ultima ratio. Ám – mindaddig, amíg valamely nagy kártyakibocsátó rájuk nem kényszeríti – a bankok inkább vállalják a mágneskártyás visszaélésekből eredő károkat, mint a teljes kártyaelfogadó hálózat átalakításának költségeit.

Sehol a világon nem emelkedhet a levegőbe korszerű repülőgép anélkül, hogy előtte a lehető legalaposabban át ne vizsgálták volna. Az informatikai rendszerek biztonsági átvilágítását végző cégek viszont legföljebb azt tanúsíthatják, hogy azok a következő – mondjuk, fél éven belül esedékes – átvilágításig éppenséggel megfelelnek-e az elvárható követelményeknek. A milliókba kerülő vizsgálat után azonban legalább el tudják mondani magukról, hogy nem elégedtek meg a Balkán-szindróma létének tagadásával. És ez már nem kevés.

HÍREK

E-GAZDASÁG

Compaq

Webszerverek középiskoláknak

Két tucat pályamunka érkezett arra a szakközépiskolai pályázatra, amelyet tavaly decemberben hirdetett meg a Compaq Computer Magyarország Kft. A cég Magyarországon eddig még meg nem valósított webes alkalmazásokra várt eredeti ötleteket. A Compaq szakértőiből álló bírálóbizottság előnyben részesítette azokat a munkákat, amelyek a mindennapi gyakorlatban is használható javaslatokat adnak, megvalósításuk működő üzleti alkalmazás, e-business lehet. Az első kategória nyertesei szervert és PC-t nyertek, a második kategóriás győztesek egy-egy PC-vel lettek gazdagabbak. Az első hasonló pályázatot 1995-ben hirdette meg a Compaq. Az idei pályázat során is kiderült: a diákok nem ismernek lehetetlent, ötleteik nemzetközi mércével mérve is versenyképesek. *www.compaq.hu.*

EAN

A visegrádiak és a B2B

A cseh, lengyel, magyar és szlovák EAN szervezetek az év elejétől együttműködnek a vállalatok közötti elektronikus kereskedelem feltételeinek javításában. A nemzeti adatbankok közös megoldásokat keresnek a termékek, szolgáltatások, szállítási egységek, szervezetek és helyek azonosítására, az adatstruktúrák egységesítésére, az ellátási lánc hatékonyságának javítására. Bíznak abban, hogy az összefogás eredményeként lényegesen javul a beszállítások kultúrája a térségben. Magyarország 1984 óta tagja az adatok szabványosításával és az adatbankok együttműködésével foglalkozó nemzetközi EAN szervezetnek. Csaknem száz ország vállalatai kerültek így kapcsolatba.

Kalapács.hu

Internetes aukció

Máris több aukciós site (Kalapács.hu, Magyaraukció.com, Ecseri.hu, Napfolt Aukció, Prim Árverés, Árverés.hu, Licitcity, Eukcio.hu) verseng a hazai piacon az eBayéhez hasonló pozícióért. A közelmúltban indult Kalapács .hu – amely mögött a NetBridge kockázatitőke-társaság áll – januárban beindította domainnév-aukciós szolgáltatását. Mivel a hazai internetes társadalom még mindig jelentős részben cégalkalmazottakat, programozókat és a technika iránt érdeklődőket foglal magában, ettől a szolgáltatástól nagy érdeklődést és forgalomnövekedést remél a Kalapács.hu. A liberálisabb domainnév-regisztrációs szabályok eredményeként mostanra jószerivel az összes kézenfekvő, egyszerű domainnév elkelt, a hazai brókerek bejegyeztek már majdnem minden igazán érdekesnek hangzó nevet. Így egyfelől piaci hiány, másfelől kínálat alakult ki: megjelentek azok a vállalkozások, amelyek eredetileg értékesítés céljából vásároltak neveket. A Kalapács.hu domainnév-aukciós szolgáltatása kezdettől több mint kétszáz nevet tartalmaz, s folyamatosan keresik az új üzleti partnereket. *www.kalapacs.hu.*

Econet

Portálépítés

Hosszabb távon átfogó pénzügyi portállá fejleszthető alkalmazások új generációjának kidolgozásáról kötött megállapodást az Econet.hu Rt. és a Compaq Computer Magyarország Kft. a közelmúltban. A szerződés értelmében az Econet fejleszti ki az internetes tőzsdei tranzakciókat kezelő szoftvert és az illesztőmodulokat a tőzsdei back-office rendszerekhez, amelyeket a két cég közösen értékesít. A készülő rendszer többek között képes lesz átfogóan értelmezni és megjeleníteni minden tőkepiaci terméket, számlainformációt, valamint alkalmas lesz piaci adatszolgáltatásra és a megbízások állapotának visszajelzésére. A megoldás ügyféloldali része egyszerű internetes böngésző ablak. Az új rendszer az év első negyedévében lesz elérhető. Econet.hu, *www .econet.hu,* tel.: 488-0730. Compaq Magyarország, *www.compaq.hu,* tel.: 458-5541.

Arthur D. Little

TIME

A Euro-Phoenix pénzügyi tanácsadó céget nevezte ki a C-quential hivatalos magyarországi képviselőjének az Arthur D. Little, amely tavaly adta át valamennyi, telekommunikációval, informatikával, médiával és elektronikával (angol betűszóval TIME) kapcsolatos tevékenységi körét a tulajdonában lévő C-quentialnak. A vállalat hozzáfér az Arthur D. Little valamennyi erőforrásához. A C-quential szolgáltatásai: stratégiai és szervezeti design, teljesítményjavítás, elektronikus kereskedelem, vállalati pénzügyek, ügyfélszolgálat vezetése, technológiai és innovációs menedzsment, hálózattervezés, valamint teljes körű tanácsadás a stratégiai tervezéstől a megvalósításig. A budapesti székhelyű Euro-Phoenix Kft. pénzügyi tanácsadó tevékenysége főként közép-európai cégek fúziójára és felvásárlására irányul. Tíztagú csapata meghatározó szerepet játszott a régió közel kétszáz pénzügyi tranzakciójában. Az elmúlt néhány évben a Euro-Phoenix Kft. elsősorban telekommunikációs megbízásokat teljesített Lengyelországban, Bulgáriában és az egykori Jugoszláviában. A C-quential és az Arthur D. Little a GSM, az LMDS, az UMTS és távolsági hívások licenceivel kapcsolatos tanácsadással foglalkozott, segített alternatív szolgáltatók piacra lépési stratégiájának kidolgozásában, távközlési hálózatok tervezésében, műszaki átvilágítás elkészítésében, mobilszolgáltatók WAP- és tartalomszolgáltatási stratégiájának, internetszolgáltatók üzleti stratégiájának és terveinek kidolgozásában. További információ: Némethy László. Tel.: 201-0717.

roWeb

Elkelt az Internetto

Január közepén gazdát cserélt az első magyar online újság. Az Internetto megvásárlásáról az IDG Magyarország Kft. és az EuroWeb Rt. tavaly decemberben írt alá megállapodást, az üzlet előzményeihez azonban kétségkívül hozzátartozik az azóta az Index sorait erősítő szerkesztői gárda korábbi kiválása. A vételárra és a következő időszak fejlesztéseire a kiadott közlemény szerint az új tulajdonos egymilliárd forintot szán. A megújuló Internetto az EuroWeb Rt. leányvállalataként, önálló részvénytársaságként kezdi meg működését, ezt követi azon tartalomszolgáltatási modell kialakítása, amely az új B2B2C koncepció alapján a Pantel–EuroWeb cégcsoport üzleti ügyfélkörének is új lehetőségeket nyújt. EuroWeb Internet Szolgáltató Rt. Tel.: 224-4000.

FotexNet

Karácsonyi csúcs

A FotexNet.hu internetáruház forgalma a karácsonyi időszakban két hét alatt túllépte a 70 millió forintot. Az áruházon kívül nagy sikere volt a kereskedelmi portálon indított játékoknak, amelyek közül a CLIX új rajongótábort teremtett a logikai játékok szerelmeseinek, az Ingyenlottóban részt vevői közül pedig december első húsz napjában közel ezer játékos vehette át nyereményét. A cég januárban a Westel-előfizetőkre is kiterjesztette a játékban való részvétel lehetőségét, akik SMS-ben küldhetik el tippjeiket. A portál látogatóinak száma a várakozások szerint néhány hónapon belül meghaladhatja az egymilliót. A nemzetközi piaci megjelenés előkészítése jegyében megkezdődött az egyes szolgáltatások idegen nyelvekre fordítása, amelyek közül január végéig az angol, német, román és szlovák változatok készülnek el. *www.fotexnet.hu.* Tel.: 487-3713.

KPMG

Tudásmenedzsment Magyarországon

A KPMG tanácsadó cég felmérése szerint a tudásmenedzsment hazai alkalmazásában átfogó, összehangolt stratégiával többnyire még nem rendelkeznek a hazai vállalatok. Az egyik fő akadály, hogy a munkatársak a hatalom és a pozíció megtartása érdekében gyakran inkább visszatartják a megszerzett tudást, mintsem megosztanák egymással. A technológiai háttér kialakításában azonban nincs lemaradás, sőt az internet és a cégen belüli intranet bevezetésében meg is előzzük a nemzetközi átlagot. A KPMG Consulting munkatársai Magyarországon 18 nagyvállalatot kerestek fel. A társaságok 39 százaléka nyilatkozott úgy, hogy rendelkezik tudásmenedzsment-stratégiával. Míg nemzetközi téren a cégek 68 százalékánál már elindult tudásmenedzsment-program, nálunk a megkérdezett vállalatok 57 százalékánál készülnek vagy működnek ilyen programok. A már végrehajtott programok közül a leggyakoribb projekt nálunk a leginkább bevált módszerek, eljárások (best practice) tapasztalatainak szervezett megosztása a munkatársakkal (29 százalék). A cégek 22 százaléka elemezte a tudásmenedzsment-helyzetet (benchmarking) és 11 százaléka tett lépéseket a vállalaton belül a TM jelentőségének tudatosítására. Hat százalékuk válaszolta azt, hogy már létrehozta a cégen belüli tudásközpontot, meghatározta a felelősöket, illetve jutalmazza a tudás megosztását. Arra a kérdésre, milyen problémák nehezítik a tudás hatékony felhasználását, a legtöbben azt válaszolták, hogy nem ismerik a TM előnyeit (86%). További gondként jelölték meg, hogy „nincs idő a tudás megosztására” (78%), „a fejekben lévő tudást nehéz megszerezni” (73%), „a munkatársak újra feltalálják a spanyolviaszt” (67%) és „a munkatársak nem akarják megosztani a tudásukat” (61%). Komoly figyelmet érdemel az utóbbi kijelentés, mert jelzi: nálunk még gyakori a félelem, hogy a tudás megosztásával csökken a befolyás, a hatalom. A nemzetközi felmérésben a cégek mindössze 16 százaléka nevezte gondnak ezt. Ugyanakkor a technológiai háttér kialakításában jól állunk – például minden megkérdezett cégnél van internet-hozzáférés, és már majdnem mindenhol (88 százalék) működik intranet is, bár még nem igazán használják ki a benne rejlő lehetőségeket. Lemaradás tapasztalható viszont az adattárházak (44 százalék) és a dokumentumkezelő rendszerek (35 százalék) alkalmazásában. Bővebb információ: KPMG. Tel.: 237-6536. E-mail: *miklos.scheibelhoffer@kpmg.hu.*

NetSurvey

E-commerce Magyarországon

Noha az első nagy rohamból kimaradtunk, az elmúlt időszakban radikális változásokon ment át a magyar elektronikus kiskereskedelmi piac – állapítja meg a NetSurvey Internetkutató Intézet legutóbbi vizsgálata, amelynek célja elsődlegesen annak a kiderítése volt, van-e már kielégítő választék és van-e számottevő vásárlói és eladói érdeklődés

Magyarországon. A vizsgálatba bekerült az új ágazatban érintett összes (körülbelül 130) vállalkozás. Jóllehet a kutatás egyformán koncentrált a kis, a közepes és a nagy cégekre, az eredmények mégis azt mutatják, hogy minél kisebbek a cégek, annál nagyobb számban vannak jelen e piacon. Örömteli, hogy a válaszadók majdnem 30 százaléka arról számolt be, hogy a bevételek legalábbis fedezik a ráfordításokat. Ám nem lehetetlen, hogy e cégek alulbecsülték e-commerce üzletáguk jövőbeni növekedését. Mindenesetre a válaszadók 61 százaléka vagy már nyereséges, esetleg nullszaldós, vagy pedig arra számít, hogy rövid távon eléri ezt az állapotot. További 39 százalék nincs ilyen kedvező helyzetben: szerintük az e-commerce egyelőre többe kerül, mint amennyit jövedelmez. NetSurvey Internet-kutató Intézet, tel.: 209-1368.

Pixelpark

Iroda Szlovákiában

A stratégiai tanácsadással, designnal, internetes technológiák integrációjával, valamint logisztikai tanácsadással foglalkozó Pixelpark AG megvásárolta a Nex Slovensko szlovák multimédiacéget, s ezzel a budapesti és a törökországi után megnyitotta harmadik irodáját a régióban. *www.pixelpark .com.* Tel.: +43-1-718-7857-137.

WebTime

Vámismeretek az interneten

A Nyitott Szakképzésért Közalapítvány támogatásával Webvám címmel kötetlen tanulási programcsomagot fejlesztett ki a WebTime Kft. A távoktatási programot vállalkozóknak állították össze; célja, hogy a vállalkozók külkereskedelmi tevékenységük során szükséges vámalapismereteket elsajátíthassák. *webvam.webtime.hu.* E-mail: *laszlo.kocso@webtime.net.*

Zeus

Minősítve

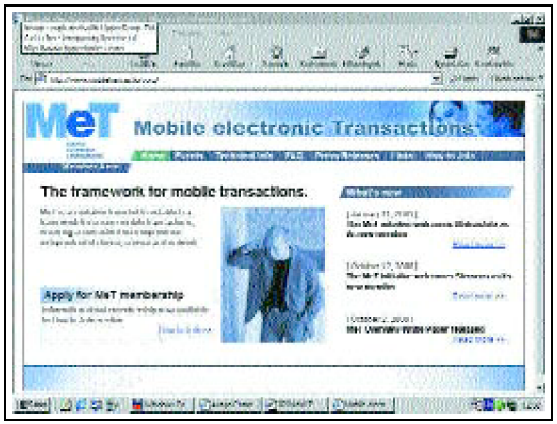
Noha Magyarországon is egyre több cég foglalkozik internetes kommunikációs és üzleti alkalmazások kínálatával, egyre több a csalódott ügyfél. Az olcsó honlapgyártó kisvállalkozások nem vizsgálják meg a megrendelő üzleti stratégiáját, nem elemzik kommunikációs tevékenységét, ráadásul az esetek többségében még gyártási és használati dokumentációkkal sem látják el ügyfeleiket. Multinacionális cégek vezetői is gyakran számolnak be arról, hogy nem készül vállalatuk üzletpolitikájához igazodó webkommunikációs stratégia. Ezért vágott bele – a magyarországi webkommunikációs cégek közül elsőként – a Zeus Tanácsadó és Kiadó Kft. a nemzetközi ISO 9002 minőségbiztosítási tanúsítvány megszerzésébe. A minősítés a felkészüléssel együtt egy évet vett igénybe. Információ: *www.zeus.hu.* Tel.: 312-0302, 474-0291.

TÁVKÖZLÉS

Matsushita

A MeT kezdeményezés új tagja

Az Ericsson, a Motorola, a Nokia és a Siemens januárban bejelentette, hogy a Panasonic márkanévről ismert Matsushita Communication Industrial Co., Ltd. csatlakozott a MeT kezdeményezéshez, amelynek tagjai közösen fejlesztenek nyílt keretrendszert a biztonságos mobiltelefonos e-kereskedelmi tranzakciókhoz. A tavaly áprilisban indult MeT célja, hogy tagjai a meglévő ipari szabványokhoz – például WAP, Wireless Transport Layer Security (WTLS), Wireless Identification Module (WIM), Public Key Infrastructure (PKI) és Bluetooth – illeszkedő m-kereskedelmi technológiákat fejlesszenek ki. A rendszer biztonságát kriptográfiai megoldások és elektronikus aláírások szavatolnák. *www.mobiletransaction.org.*



MatávCom

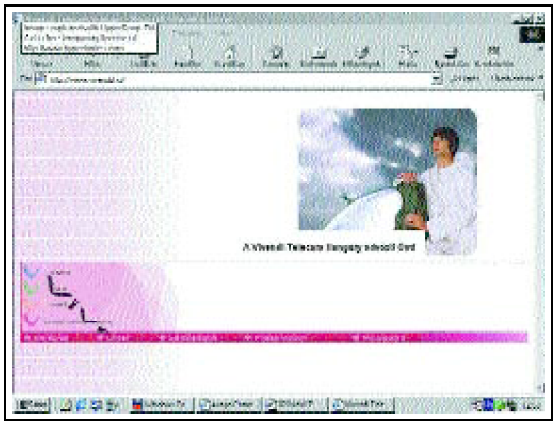
Újabb cégvásárlás

Többségi tulajdont szerzett a MatávCom a CompArgo Számítástechnikai, Távközlési és Szolgáltató Kft.-ben. Közös közleményük szerint az újabb cégvásárlás célja, hogy a MatávCom még szélesebb kompetenciát szerezzen az infokommunikációs piacon, jelen esetben a távfelügyeletben, illetve az informatikai távközlési szoftverek fejlesztésében. *www .matavcom.hu.*

Vivendi

Felkészülés a liberalizációra

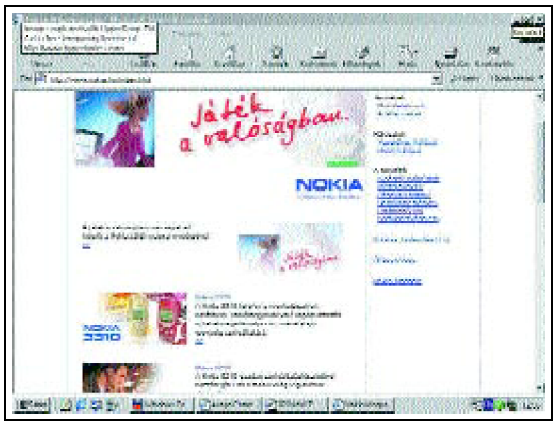
Hárommilliárd forintot fordít idén versenyhelyzetének javítására a Vivendi. A részben koncessziós, részben alternatív távközlési cég a múlt év végén átszervezéssel kezdte felkészülését a liberalizációra. Az újonnan alakult V com és V fon, továbbá a leendő V net versenypozícióinak erősítéséért folyamatosan javítják a szolgáltatások biztonságát, színvonalát. Az új számlázási rendszert a jelenleginél lényegesen nagyobb igények zökkenőmentes kielégítésére tervezik. Hasonló a helyzet a 4,5 millió hívás kezelésére alkalmas új call centerrel. A Sun, az Avaya és az Oracle közreműködésével kialakított szolgáltatásfelügyeleti központ pedig lehetővé teszi, hogy folyamatosan figyelemmel kísérjék és elemezzék az országos hálózat üzembiztosságát és a szolgáltatás színvonalának alakulását. Készülnek – többek közt – az új távközlési technológiák (MPLS/IP-VPN) szolgáltatásszintű felügyeletére, a virtuális ISP, ASP hosting szolgáltatás menedzselésére és egyéb feladatokra is. A Geometria Rt. térképen alapuló rendszere például nemcsak egy-egy térség kapacitásának gyors felmérésére vagy a „gyenge láncszemek” helyéből adódó potenciális problémák előrejelzésére alkalmas, hanem a távközléstől távoli többletszolgáltatásokra is. Vivendi Telecom Hungary, *www.vivendi.hu.*



Nokia

128 millió telefon

Összesen több mint 128 millió mobiltelefont adott el 2000-ben a Nokia, 64 százalékkal többet, mint 1999-ben. A cég becslései szerint tavaly világszerte összesen 405 millió készülék került forgalomba, 45 százalékkal több, mint egy évvel korábban. A mobiltelefon-előfizetők száma így 2000 végére meghaladta a 700 milliót. Nokia Hungary Kft. Tel.: 06-20-977-7797. *www.nokia.hu.*



INFORMATIKA

Bentley

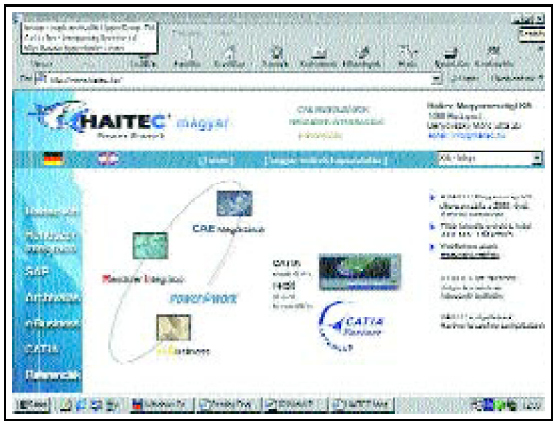
40 millió dolláros felvásárlás

Január elején a Bentley bejelentette, hogy felvásárolja az Intergraph három üzletágát. A Bentleyhez kerül az Intergraph plotserver termékcsaládjába tartozó InterPlot és Digital Print Room sorozat, a raszterkonverziós termékek családja, így az I/RAS Engineer és az I/RAS B, valamint a MicroStation sorozat, az InRoads és InRail tervezőrendszerek. Bentley Europe. Tel.: +3123-556-0560. *www.bentley.com.*

Haitec Kft.

Évzáró és évnyitó

Irodaavatással zárta a múlt évet a Haitec Magyarországi Kft., amelyen közölték: 2001-től e-business Security Services néven új üzletágat indít a vállalat, más divízióikhoz hasonlóan ugyancsak IBM termékekre építve. A cég első negyedévi rendelésállománya már az év végén meghaladta a 200 millió forintot. Haitec Kft. *www.haitec.hu*.



HP Invision

Fotópályázat

Dánia, Franciaország, Svédország, Izrael, Belgium, Hollandia, Spanyolország, Magyarország, Szaúd-Arábia, Oroszország és az Egyesült Királyság fotóművész-hallgatói vesznek részt a HP nemzetközi fotópályázatán. A diákok személyi számítógépből, lapolvasóból, nyomtatóból, CD-íróból és digitális kamerából álló HP digitális fotófelszerelést kapnak, amellyel három hónap alatt négy-négy képet kell készíteniük a következő három kategóriában: „*Az én városom 2001-ben”,* azaz hogyan mutatná meg városát; „*Ihlet”,* azaz mi ösztönözheti a képzelőerőt; végül a „*Vegyél meg!”,* azaz egy termék vagy szolgáltatás reklámkampány stílusú fotózása. Előzetes pályáztatás után a HP Magyarország az Iparművészeti Egyetemet választotta a digitális fotópályázaton való részvételre. Magyarországot *Vinnai Péter,* a *Foto Video Magazin* szerkesztője képviseli a nemzetközi zsűriben. Az eredményhirdetés 2001. április 30-án lesz, a győztes megtarthatja a HP digitális fotófelszerelést, emellett 5000 dollár pénzjutalomban részesül. *www .hpinvision.com.*

HTE-programok

Február 5., hétfő, 14 óra, PT

A Hírközlési és Informatikai Tudományos Egyesület Szenior Klub klubnapján *HIKI születése és megszűnése* címmel előadás hangzik el. Meghívott előadók: *Drabik Illés, Saufert János, Varga Pál.*

Február 7., szerda, 15 óra, Sopron

(Lackner Kristóf u. 7.)

A Hírközlési és Informatikai Tudományos Egyesület Soproni Szervezete látogatást szervez az MTV Soproni Körzeti Stúdiójába, amelyre minden érdeklődőt szeretettel várnak. A rendezvényről érdeklődni lehet *Nagy Tamás* titkárnál.

Február 7., szerda, 16 óra, PT

A HTE DVB Kör, a HTE DRK (Digitális Rádió Kör), a HTE Kábeltelevíziós Szakosztály, a HTE Vételtechnikai Szakosztály és a HTE Stúdiótechnikai Szakosztály együttes szervezésű Médiaklubja. Program: A DVB-T hálózati kiépítése I. Előadók: *Árky Zsolt, Szűcs Ferenc, Ughy Elek.* Vitavezető: *dr. Tormási György.*

Február 8., csütörtök, 16.30 óra, PT

A HTE Számítástechnikai Szakosztály, az EOQ MNB és az ISACA Magyar Fejezete közös szervezésű rendezvénye a *Linux rendszerek nagyvállalati környezetben,* melynek keretében előadások hangzanak el: 1. Linux rendszerek elérhetőségének növelése fürtözéses megoldásokkal. Előadó: *Bodnár Csaba* (Mission Critical Linux Kft.). 2. Formális védelmi modell implementációk Linuxon. Előadó: *Magosányi Árpád* (LME). A rendezvényről érdeklődni lehet *dr. Szenes Katalin* szakosztályi elnöknél a 06-20-331-7438-as telefonszámon vagy a *szenes@nik.bmf.hu* e-mailen.

Február 12., hétfő, 14 óra, TH (III. 337.)

A HTE TETRA Szakosztály szervezésében előadás hangzik el *TETRA fejlesztések és eredmények a Rhode & Schwarznál.* Előadók: *Knut Buerkner* (Rhode & Schwarz Bick Mobilfunk), *Dieter Angerer* (Siemens Austria).

Február 14. , szerda, 14 óra, PT

A HTE Stúdiótechnikai Szakosztály szervezésében előadás hangzik el *Új technológiák a Televízió Stúdiótechnikában* címmel. Vitavezető: *Ágoston György* (MTV Rt.).

Február 15., csütörtök, 17 óra, PT

A HTE Távközlési és Informatikai Projektirányítók (TIPIK) Klubja. Program: *Egy e-business projekt tapasztalatai.* Vitaindító: *Mészárosné Divinyi Mariann* (Inter-Európa Bank).

Február 22., csütörtök, 17 óra, PT

A HTE Távközlési Szakosztályának szervezésében a TÁVKÖZLÉSI KLUB 16–20 óra között várja az érdeklődőket. A klubnap témája: *Az ADSL alapú szolgáltatások bevezetésének jogi-műszaki kérdései.* Vitaindító előadást tart: *dr. Takács György* (HIF). Felkért hozzászólók: *Kocsis Ferenc* (Matáv), *Bárányné dr. Sülle Gabriella* (Pantel), *Birta Bertalan* (Elender). Vitavezető: *Megyesi Csaba* (Siemens telefongyár).

TH: *Budapest, V., Kossuth Lajos tér 6–8.*

PT: *Budapest, VI., Andrássy út 3.*

A rovatot Zákonyi Magdolna gondozza. Bővebb felvilágosítás kérhető: HTE Titkárság,1055 Budapest, Kossuth tér 6–8. Tel.: 353-1027, fax: 353-0451, www.mtesz.hu/hiradastechnika. E-mail: hiradastechnika@mtesz.hu.

NJSZT-hírek

Neumann Üzleti Klub

A közelmúltban félreértésre adhatott okot, hogy társaságunk bevonása nélkül, ám az NJSZT által évek óta használt néven, Neumann Klubként alakult fórum az információs társadalomról szóló rendezvények szervezése céljából. A kormányzati kezdeményezésre megalakult fórum felelőseivel való egyeztetés eredményeképpen a szervezők egy közleményt juttattak el az NJSZT szerkesztőségébe, melyből néhány mondatot idézünk: „Ezúton tájékoztatjuk Önöket, hogy az általunk Neumann Klub néven alapított klub nevét Neumann Üzleti Klubra változtatjuk. A változtatással garantálni szeretné a klub a Neumann Társasággal a kölcsönös megbecsülésen alapuló, hosszú távú kapcsolatot és együttműködést, hiszen céljaik hasonlóak. A társaságnak és az üzleti klubnak is legfőbb törekvése, hogy hozzájáruljon az információs társadalom fejlődéséhez. Rendezvényeivel, munkájával segítse az információáramlást és Magyarország szellemi erőforrásainak kiaknázását.” A Neumann Üzleti Klubbal együttműködve az NJSZT Neumann Újklub néven folytatja klubrendezvényeit, amelyre továbbra is szeretettel vár minden érdeklődőt. (Aktuális program: *www.njszt.hu.*)

Internet Fiesta a könyvtárakban

Könyvtárak az Internet és a digitális kultúra terjesztéséért, 2001. március 2–4. Fővédnök: *Mádl Ferenc* akadémikus, köztársasági elnök. Védnökök: *Kroó Norbert* akadémikus MTA főtitkár, *Pokorni Zoltán* miniszter (OM), *Rockenbauer Zoltán* miniszter (NKÖM), *Sík Zoltán* informatikai kormánybiztos. Az internetkultúra népszerűsítését szolgáló, világméretű rendezvénysorozatot, az Internet Fiestát évente rendezi meg az Internet Society. A 2001. évi Fiesta rendezvénysorozat a könyvtárakra épül. Ezzel arra szeretnénk felhívni a figyelmet, hogy az információs társadalom kialakításában ezen intézményrendszer rendkívül fontos, meghatározó szerepet játszik.

IEEE/IEEE CS-tagság

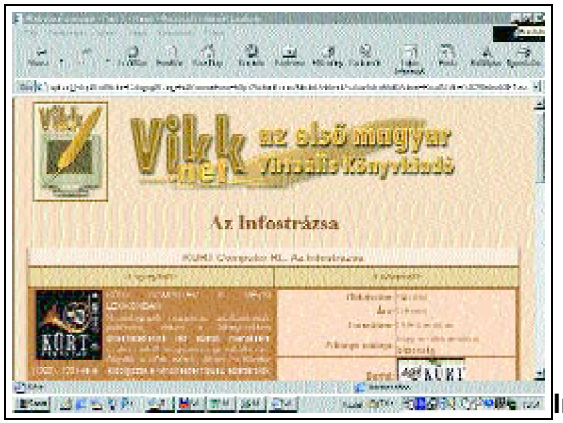
Tájékoztatjuk tagtársainkat, hogy 2001. február 28-ig kapcsolódhatnak be kedvezményes feltételekkel az IEEE/IEEE Computer Society rendkívül aktív szakmai tevékenységébe. További információ: NJSZT honlapja: *www.njszt.hu,* IEEE CS honlap: *www.computer.org,* e-mail: *hpg@ njszt.hu* (NJSZT IEEE CS Budapest Center, tel.: 312-9884). Minden érdeklődőt továbbra is szeretettel várunk az NJSZT IEEE CS Budapest Center olvasótermében a NJSZT Titkárságon. (Folyóirat-tartalomjegyzékek az NJSZT honlapján találhatók).

ECDL-mérleg: „tény-leg” 2000-ről

Magyarországon (beleértve a nemrégiben akkreditált határontúli intézményeket is) 2000 decemberének végéig összesen 28 573-an váltottak vizsgakártyát és 16 245-en szerezték meg a bizonyítványt. Budapesten regisztráltatták magukat a legtöbben, 10 708-an (37,57 százalék), a második helyen Baranya megye (2074 hallgató, 7,28 százalék), a harmadik helyen pedig Komárom-Esztergom megye áll 2022 regisztrációval, ami az összes regisztráltak 7,1 százalékát jelenti. Az ECDL-esek száma világszerte meghaladta az egymilliót, és hazánkban is várható a vizsgázók számának ugrásszerű növekedése: cél, hogy az Európai Unió de facto elvárásaihoz híven Magyarországon is tömegesen szerezzék meg az informatikai írástudást igazoló Európai Számítógép-használói Jogosítványt.

2001. FEBRUÁR / HÍREK / Könyvszemle

Könyvszemle



Infostrázsa

Kiadó: Vikk.net

Ára: ingyenes e-könyv

Elsősorban a hazai alkotóknak kíván publikálási lehetőséget adni az elektronikus könyvek terjesztésére létrehozott Vikk.net kiadó. Virtuális könyvespolcukon a januári nyitáskor öt, lapzártánkkor már tíznél több letölthető e-könyvet kínáltak az érdeklődőknek. Ezek egyike az adatmentéssel, informatikai biztonsággal és kockázatkezeléssel foglalkozó Kürt Computer Rendszerház Rt. *Az Infostrázsa* című kiadványa, amelyet ingyenesen, PDF formátumban lehet letölteni. A könnyed stílusban íródott könyvecskében érdekes történetek olvashatók az informatikai biztonságról. Például: hogyan vesztik el és lopják el az adatokat mások, másoktól. Az itt elsütögetett poénok az olvasóra természetesen nem érvényesek. Ha netán mégis a saját környezetére ismer, legalább megnyugvással töltheti el a tudat, hogy mások is gondatlanok, felelőtlenek. *Az Infostrázsa* legnagyobb fejezetéről, a Kürtölőről így ír a könyv szerkesztője, *Kürti Sándor* vezérigazgató: „Negyvennyolc történet az informatikai biztonságról. Mindegyike két oldal terjedelmű, és mindegyik legalább egy poénnal és egy jó tanáccsal van fűszerezve. E kétperces önálló olvasmányok méltán pályáznak a ‚Bestseller of WC Library’ címre. Kéttucatnyi

történetenként a lecsupaszított jó tanácsokat foglaljuk össze. Mi így kövezzük a pokol felé vezető infosztrádát. Ha sikerre vágysz a munkahelyeden, küldj ezekből hetente egyet-egyet az informatikai főnöknek. Nyert ügyed van.”

A Vikk.net-ről jelenleg letölthető e-könyvek:

Sztolár Miklós: Jelzálog (kisregény);

Nógrádi Gábor: Galambnagymama (gyermekirodalom);

Szilágyi Vilmos: Intim kapcsolatok (szexológia);

Chi Wicca: NemS negyedek (napló);

Gligorics Teréz: Szimultán (kisregény);

Niké: Már vártalak (sci-fi fantasy);

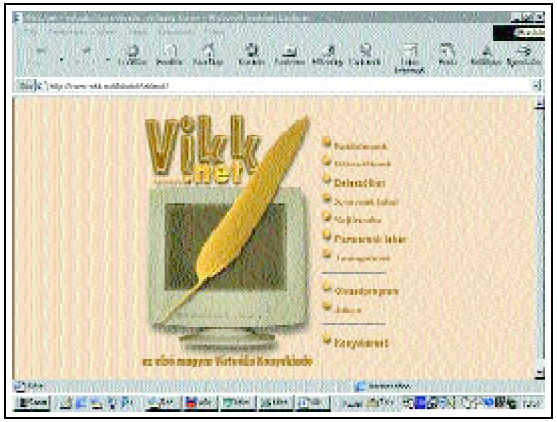
Németh Ibolya: Mexikói üdvözlet (levélregény);

Kurmainé P. Judit: Hobbim a bonsai (szakkönyv);

Reményik László: Akik sötétben is látnak (dokumentumregény);

Perjés László: e-mber (sci-fi);

Kürt Computer Rendszerház Rt.: Az Infostrázsa (informatikai biztonság).



Az Infostrázsa első kiadása 1998 decemberében, második kiadása 2000 decemberében jelent meg papírkötésben. Az e-könyv változatot tavaly december 12-én töltötték fel a Vikk.net oldalaira, ahonnan azután egyetlen hónap alatt 270-en töltötték le. A Vikk.net *(www.vikk.net)* a Lezlisoft Computer Graphics *(www.lezlisoft.com)* és a Kikelet 21 Szellemi Műhely *(www.lezlisoft.com/kikelet)* közös vállalkozása. A kiadó létrejöttében fontos szerepet játszott a Kreatív Kör levelezőlista virtuális közössége is. Sajnos az „első magyar virtuális könyvkiadó” címre pályázó vállalkozás igénytelen, hibákkal csúfított weboldalai rontják az elektronikus könyvekről még ki sem alakult képet. A Vikk.net e-könyvkiadóról *Csapó Ida* szolgál felvilágosítással a 06-30-956-1565 telefonszámon és a *vikk.net@lezlisoft.com* e-mail címen.

INTERJÚ
Sun Microsystems

2001. FEBRUÁR / INTERJÚ Sun Microsystems / Hálón született cégektől a „régi” gazdaságig

Hálón született cégektől a „régi” gazdaságig

Egy kaliforniai sajtószemináriumon John McFarlane-t, a Sun rangidős elnökhelyettesét kérdeztük a Sun internetes stratégiájának néhány részletéről.

Szerző: Hutter Ottó

Napjainkban mindenki internetforradalomról beszél, miközben megkezdődött egy szoftverforradalom is, ami teljesen átrendezheti az informatikai alkalmazások használatával kapcsolatos szokásokat. Kíváncsiak voltunk, vajon egy olyan patinás cég, mint a Sun Microsystems, hogyan reagál ezekre a kihívásokra.

John McFarlane: Amiként az elsők között ismertük fel az internet fontosságát, úgy az elsők között mutattunk rá arra is, hogy az internetforradalom egyik leglátványosabb hatása éppen az informatikai alkalmazások használati módjának átalakulása. Felgyorsult világunkban mindenki szeretne az igazi üzleti problémákra koncentrálni, és ehhez az informatikát ugyanolyan alapszolgáltatásként igénybe venni, mint a villanyáramot vagy a vizet.

Eleinte csupán provokációnak tekintették, amikor *Scott McNealy* elnök-vezérigazgatónk arról beszélt, hogy a valóban üzleti gondolkodású CIO a jövőben nem vásárol már sem számítógépeket, sem szoftvereket, csak üzleti alkalmazásokat bérel egy szolgáltatótól. Ma már sorra jelennek meg az alkalmazásszolgáltatók (ASP-k), amelyek bárki számára elérhetővé teszik ezt a modellt.

Nagyvállalati körben tulajdonképpen mindez akár az internettől függetlenül, saját vállalati hálózatok igénybevételével is megvalósítható. Az internet segítségével azonban olcsóbban és szélesebb körben szerezhetők meg ezek a közműszerű informatikai szolgáltatások. Mi a magunk eszközeivel szintén mindent megteszünk, hogy katalizáljuk ezt az átalakulást, ezért fektetünk komoly energiákat ServiceProvider.com elnevezésű szolgáltatói programunkba. A Sun komoly tapasztalatokkal, sikeres termékekkel, domináns piaci részesedéssel rendelkezik az internetszolgáltatói piacon, és ezt szeretnénk kiterjeszteni a teljes szolgáltatói szektorra.

BYTE Magyarország: *Mit takar ez a program valójában?*

John McFarlane: A Sun– Netscape Alliance – kifejezetten a közműszerű szolgáltatási modellben való értékesítésre optimalizált – termékeire támaszkodva olyan alkalmazásokat kínálunk az üzenetkezelés, a biztonságos távoli hozzáférés és bizonyos személyes hatékonyságnövelő alkalmazások támogatására, amelyek kézzelfogható módon segítik a szolgáltatókat bevételeik növelésében. Speciális szolgáltatásokkal, előre konfigurált és akár egy napon belül szállítható szerverekkel, az új szolgáltatások tesztelését megkönnyítő

kompetencia-központokkal is javítjuk a működés hatékonyságát és a szolgáltatás minőségét. Egyre nagyobb tekintélynek örvend a SunTone Certified hitelesítési rendszerünk, amivel azt a képet szeretnénk erősíteni a felhasználókban, hogy a Sun technológiájára és módszertanára alapozva az interneten keresztül is ugyanolyan robusztus módon kínálhatók az informatikai alkalmazások, amint azt a távközlési szolgáltatások esetében már megszoktuk.

John McFarlane, a Sun elnökhelyettese

BYTE Magyarország: Az internet alapú szolgáltatásokhoz szükséges infrastruktúra garantálása mindig is a Sun egyik fő tevékenységének számított. Az azonban meglepetést keltett, hogy tavaly a StarOffice megvásárlásával megjelentek az irodai szoftverek piacán is. Vannak ezzel kapcsolatban hosszú távú céljaik és ha igen, mik?

John McFarlane: Bizton állíthatom, hogy továbbra sem kívánunk betörni az alkalmazásszerverek piacára, annak ellenére, hogy a StarOffice-szal valóban komoly terveink vannak. Várhatóan 2001 első felében StarPortal néven elindítunk majd egy referenciaértékű szolgáltatást, amely az ASP modell szerint fogja elérhetővé tenni az irodai szoftvercsomagok szokásos dokumentumkezelő, csoportmunka- és üzenetkezelő szolgáltatásait. Ebben számunkra korántsem az esetleges üzleti eredmény a lényeges, hanem az, hogy demonstráljuk: ebben az alapvető alkalmazási szegmensben is életképes a szoftverek szolgáltatás jellegű terjesztési, illetve használati modellje.

BYTE Magyarország: *Hogyan látja ezeken az új stratégiai területeken Európa helyzetét? A Sun számára mennyire fontosak az itteni regionális piacok?*

John McFarlane: Egyáltalán nem udvariasságból mondom, hogy Európa rendkívül fontos nekünk, a bevételek jelentős és egyre növekvő része származik erről a dinamikusan bővülő piacról. Ugyan éppen az ASP területeken érezhető egyfajta idegenkedés, ami miatt egyelőre ennek a szolgáltatási modellnek messze nem alakult ki olyan kultúrája, mint például az Amerikai Egyesült Államokban. Viszont akadnak olyan, szintén lényeges területek – gondolok itt mindenekelőtt az intelligens kártyákra és a mobil technológiákra –, amelyeken Európa számos országa világviszonylatban is az élen jár. Márpedig ezek az említett technológiák számunkra kulcsfontosságúak. Az intelligens kártya kis túlzással a SunRay termékcsaládunk lelke, a mobil területen pedig a múlt év végén jelentettünk be átfogó programot.

BYTE Magyarország: A távközlési és internetes szolgáltatóknak nyilván meghatározó a szerepük az internetforradalom kiteljesedésében, de nem szorulnak a kelleténél jobban háttérbe a hagyományos iparágakban működő cégek internetes lehetőségei?

John McFarlane: Valóban megfigyelhető volt ez a tendencia az elmúlt időszakban, hiszen tulajdonképpen érthető, hogy először a kisebb, rugalmasabb cégek tudnak befogadni egy új technológiát, no és persze azok a szolgáltatói iparágak, amelyeknek az üzlete erre épül. Ma azonban már eljutottunk oda, hogy a tradicionális nagy gyártók, iparvállalatok, energiatermelők és közszolgáltatók, pénzintézetek számára is egyre fontosabb az internet. Ezeket a vállalatokat mindenekelőtt abban kell segíteni, hogy back-office rendszereiket integrálják az internettel. Persze lehet, hogy egy idő múlva ezeknek a cégeknek nem hardvert és szoftvert fogunk eladni, hanem IT-architektúrát, és ők valójában csak szolgáltatást fognak vásárolni a Service Providerektől. Legalábbis erre utal e szolgáltatók exponenciális ütemben fejlődő infrastruktúrája. Ha azonban SP programunk sikeres lesz, és hosszú távon is megőrizzük mostani piaci részesedésünket, akkor azt hiszem, ebben az új korszakban sem kell aggódnunk üzleti eredményeinkért.

Hutter Ottó az Infopen főszerkesztője.

E-mail: **otto@hutter.hu.**

HAZAI PÁLYA
e-üzlet

Alapkövetelmény a növekedés

Csapdába csal, ha a cég e-business megoldásának tervezésekor a puszta funkció lebeg az IT-gárda előtt.

Szerző: Vityi Péter

Nincs olyan, a funkciókra vonatkozó teszt, amely kimutatná, mi történik, amikor az alkalmazások a pilotfázisból a tényleges működés szakaszába lépnek, s robbanásszerűen bővül a potenciális fogyasztók köre. Ha a rendszer tervezésekor erre nem készülnek fel, az elektronikus üzlet lényegét tévesztik szem elől.

Természetesen nem csupán a rendszer hibás méretezése idézhet elő üzletileg kritikus helyzetet. Általános tapasztalat, hogy a mennyiségi jellegű változás minőségieket is megkövetel, azaz a rendszernek esetleg előre nem látott funkciókkal is bővülnie kell. Olyan architektúrára van tehát szükség, amely erre az összetett méretezésre is képes. A Microsoft .Net architektúrájának egyik alapelve éppen az, hogy tartalmazza a minden irányú növekedés lehetőségét.

Konkrét technológiák

Az architektúrák az egyes növekedési irányokat olykor külön termékekben fogalmazzák meg. E rövid cikkben még saját cégünk átfogó termékszemléjére sem törekedhetünk, csak a minőségi, funkcionális méretezés szükségletének példázása céljából idézünk fel, mondjuk, a webes kereskedést szolgáló néhány alkalmazást. A webes kereskedelem microsoftos architektúrájában a perszonalizációtól a katalóguskezelésig egy tényleges nagyáruház minden fontosabb funkciójára képes Commerce Server áll az előtérben, amelynél a szolgáltatások követhetik a vállalkozás méreteit. Emellett a .Net egyik alapkövetelményének is megfelel: XML-képes, ami azért lehet fontos, mert a kereskedelem, a verseny, az árubeszerzés stb. a webes piactereken is folyik, így szükség van saját határaink túllépésére, adatok (árak, kampány- és egyéb információk) differenciált szolgáltatására és fogadására. Egy szinttel hátrább a Microsoft esetében a különböző alkalmazások integrációját végző BizTalk Server áll, amely nem merev architektúrát fog össze, hanem olyat, amelyben váratlan, de az XML-kommunikációra felkészült komponensek is felbukkanhatnak. Csak egy példa az ilyesfajta váratlan szükségletre a labilitást előidéző, kockázatot növelő túlszaladó rendelés esete, amely nincs tekintettel a fizetési folyamatok tempójára vagy a gyártási, logisztikai lehetőségek alakulására.

Összefüggő kulcsszavak

Az internetes architektúrától a felhasználók mindenekelőtt gyorsaságot, méretezhetőséget, kézben tarthatóságot és biztonságot várnak. Ez utóbbi a webes üzletvitel legérzékenyebb kérdése. Idetartozik az üzem- és az adatbiztonság is. Amikor architektúrát választunk, gondolnunk kell arra, mi történik a sebezhetőséggel, ha hirtelen megtízszereződik a felhasználók, ügyfelek száma; új és esetleg külső cégtől származó alkalmazással kell kiegészíteni a rendszert; de arra is, mivel jár, hogyha át kell térni a 7×24 órás folyamatos üzemre. Ilyen helyzetben biztonsági tartalékokat kell beállítani, például fürtözni kell. (A Microsoft-platformban a bővítés biztonságának egyik fő tartozéka az Active Directory, amellyel a különböző, akár újonnan belépő alkalmazások is ugyanazt az operációs rendszerre támaszkodó „securityt” használhatják.)

Különösen a biztonság érdekében a rendszer kézben tartásához megfelelő szakértelemre, a gondosan kidolgozott üzemeltetési és biztonsági házirendek betartására van szükség. Ezek hiányában bármely rendszer nagyjából egyformán sebezhető, ami azonban nem írható a platform vélt gyöngeségének rovására.

Az emberi tényező speciális vonatkozásokban jelenik meg az internetes e-businessben. Az egyik ezek közül a használati színvonal és fegyelem már említett szükségessége. Egy másik pedig a vállalatok e-kereskedelmi fejlesztésével függ össze.

A jéghegy csúcsa

Az internetes korban az architektúra létesítése idején épp csak a jéghegy csúcsa látszik. A szemlélet eme korlátozására esetleg a gazdasági körülmények kényszerítik az üzletépítést. El kell fogadtatni az informatikai beruházás növekedésére számító koncepciót a folyamatos egyensúlyra törekvő gazdasági vezetéssel. Ha a kezdetben választott architektúrát nem lehet megfelelően méretezni, hanem növekedéskor fel kell váltani, az ésszerűnek látszó takarékosság utólag még akkor is pazarlásnak minősül (az is), ha a cégtörténetben megmagyarázható. A tág látókörű IT-menedzsment a közvetlen funkcionális szükséglet mellett gondol a növekedésre is, a gazdasági menedzsment viszont sokszor annak ellenére kénytelen korlátozni az ambíciókat, hogy meg van győződve az üzletvitel dinamikus növekedéséről. A kockáztatás, a hitelből építkezés nem tartozik minden cég háttérlehetőségei közé. Ilyenkor csak az oldhatja fel az ellentmondást, ha az architektúra a kezdeti teljesítményével sem drága, a továbbiakban pedig egyszerűen és fajlagosan olcsón bővíthető. Az ilyen befektetés ésszerűségéről meg lehet győzni a gazdasági vezetést, ha pedig a biztonsági szempontok kezelése is megnyugtató, az adminisztratív döntéshozást is. Az ilyesfajta platformmal tehát a vállalatvezetés minden szintje és területe konszenzusra juthat a cégfejlesztésben, ez az egység pedig az internetes üzletvitel viszonyai között a siker kulcsfontosságú feltétele.

Vityi Péter ***(petervi@microsoft.com)*** *a Microsoft Magyarország Kft. megbízott ügyvezetője.*

HAZAI PÁLYA
Szoftverfejlesztés

Nyújtózkodó szoftverházak

Külön-külön nem érzik magukat elég erősnek a nemzetközi szerephez, ezért szövetségre lépnek nagyobb szoftverházaink.

Szerző: Győrfi Áron

Az informatika legdinamikusabban fejlődő területeinek egyike a szoftverfejlesztés. Az erős nemzetközi verseny miatt azonban a magyar szoftverfejlesztő cégek (legtöbbjük 1990 után alakult) speciális alkalmazások, eszközök kifejlesztésére és bedolgozói vagy szerződéses fejlesztésre kényszerültek. Ez a fajta termékszerkezet nem vezetett kiemelkedő nemzetközi piaci sikerhez, holott a fejlesztők kiváló munkát végeznek. A vállalkozások gazdasági gyengesége, marketingjük és megbízhatóságuk (a hosszú távú terméktámogatás) hiánya a piaci siker gátjává vált. Mindezek ellenére világszerte ismerik és elismerik a magyar informatikai eredményeket, termékeket. Ezt jelzi néhány, nemzetgazdasági szempontból is fontos adat.

Báti Ferenc: Nem leszünk versenytársai a hazai szoftvercégeknek

Míg 1995-ben az akkor vizsgált negyven-ötven vállalat harmincmillió dollár exportot bonyolított, napjainkra ez már több százmillió dollárt tesz ki. A közép-európai technológiai ágazatról szóló legutóbbi felmérés – amelyet a Deloitte & Touche Central Europe az egyes cégek 1997 és 1999 közötti évi átlagos árbevétel-növekedési mutatója alapján állított össze – megállapítja, hogy a vizsgált vállalatok közel felénél az éves árbevétel nem éri el az egymillió dollárt, és legtöbbjük csupán egyetlen országban működik. Felsővezetőik a piaci részesedés növelését, az értékesítés és a marketing erősítését, valamint a tőke és a magasan képzett munkaerő elérhetőségét tekintik a legnagyobb üzleti kihívásoknak.

Rutin és garancia

Nemrégiben néhány független tulajdonosi szerkezetű, magyar szoftverfejlesztő vállalkozás vezetői döntő lépésre szánták el magukat. Erőik egyesítésével olyan társulás létrehozásán fáradoznak, amely számottevő kapacitásával is kitűnhet a régió fejlesztőközpontjai közül. A közös, magyar tulajdonú vállalat kialakításában jelentős szerepet vállalt *Báti Ferenc,* a Magyar–Amerikai Kereskedelmi Kamara Informatikai Bizottságának elnöke.

Mint lapunknak elmondta, a szoftvercéget alapító társaságokkal ellentétben ez a szövetség – amiként minden exportorientált vállalkozás – rá lesz kényszerítve a magasabb minőségi követelményrendszer alkalmazására. A közösség elsősorban olyan megbízásokat akar megpályázni, amelyeket a jól működő mai magyar szoftvercégek igen kis eséllyel pályázhatnának meg, együttes erővel viszont képesek felsorakoztatni megfelelő számú informatikust és kiállítani a megfelelő tudású fejlesztőcsoportot. „Eleinte valószínűleg rutinjellegűnek látszó bérmunkafeladatokat fogunk ellátni – amiben én egyébként semmi szégyellnivalót nem látok.” Báti Ferenc szerint a közös vállalat nem lesz versenytársa a hazai szoftvercégeknek sem a magyar piacon – mivel külföldi megrendeléseket remél –, sem pedig a világpiacon, hiszen nagyobb méretű fejlesztésekre szóló megbízásokat keres.

Vaspál Vilmos: A marketingkihívásnak nem tudunk eleget tenni

A hazai szoftveróriás létrehozásának ötletét támogatta – a szoftverfejlesztés iránti növekvő igényen kívül – a sikeresen működő, magas árbevételt produkáló indiai fejlesztőközpontok példája is. Indiában jelenleg közel hatmilliárd dollár éves árbevétel származik ilyen tevékenységből, ám az előrejelzések szerint a szoftverházak bevétele négy-öt év múlva az ötvenmilliárd dollárt is elérheti. A szövetkezésre készülő magyar szoftverfejlesztők négy-öt év múlva mintegy 500 millió dollár éves árbevétellel számolnak.

Arra a kérdésre, vajon az exportcélú szoftverfejlesztés nem vonja-e el a magyar fejlesztőket a magyar piactól, Báti Ferenc elmondta: „Az, hogy már induláskor körülbelül ezer fővel számolunk, még nem jelenti azt, hogy holnaptól kezdve ezer informatikust kivonunk a magyar piacról. A társaság által foglalkoztatottak száma fokozatosan éri el ezt a létszámot, miközben folyamatosan nő a részt vevő szakemberek tudásszintje és javul tudásuk minősége."

Szoftverház-építőkockák

A hazai szoftvercégek jövedelmezőségének fenntartása komoly feladatot ró a vállalatok felső vezetésére. Mi szólt hát amellett, hogy részt vegyenek az új szoftvercég alapításában? – kérdeztük a központ létrehozásában érdekelt magyar szoftverházak közül háromnak a vezetőit. Mint *Nagy Zsolt,* a Unitis Rendszerház Rt. igazgatótanácsának elnöke elmondta, a kétszáz fővel dolgozó Unitis munkatársai közül 130-140 fejlesztői, tanácsadói tevékenységet lát el. Ez a létszám megfelel a magyarországi projektek méreteinek, ám tapasztalataik szerint a nyugat-európai piacon gyakran kevésnek bizonyul ahhoz, hogy a cég nagyobb léptékű projektekbe is bekapcsolódjon vagy ilyenekben meghatározó szerepet töltsön be.

Vaspál Vilmos, a FreeSoft Kft. ügyvezető igazgatója így fogalmazott: „Nekem elsősorban magyarul kell gyártani. Nagyon speciális helyzet lenne az, ha rögtön a világpiacot céloznám; akkor angolul kellene gyártanom." Ehhez a FreeSoft méretű szoftverházaknak nincsenek meg sem a marketing-, sem az üzleti eszközeik. A nyolcvanfős, majd egymilliárd forint éves forgalmú vállalkozás üzleti eredményei – és különösen marketinglehetőségei – világpiaci méretekben szemlélve kevésnek bizonyulnak. „Szerintem – vélte

Vaspál Vilmos – ha a termékfejlesztés lenne 100 egység, akkor a marketing körülbelül 2000 egység. Ennek a kihívásnak nem tudunk eleget tenni.”

Igaz Gábor, a hárommillió dollár árbevételű VT-Soft Kft. ügyvezető igazgatója úgy véli, cége immár a belföldi piac szűkös méreteivel szembesül. „A hazai piac nagyon korlátozott, bizony elég nehéz stabilan megtartani; ki kell lépnünk a világ felé, azt pedig csak nagyobb méretekben lehet.”

Vajon megéri-e gazdasági érdekszövetséget alakítani, vállalva az új társaság működtetésével járó szervezési, összehangolási feladatokat? Működtethető-e egy ekkora vállalat úgy, hogy az alapítók megosztják erőforrásaikat a saját, illetve a közösen vállalt projektek között? – kérdeztük az érintetteket.

Igaz Gábor: A szoftverpiac nagyon sokféle ismeretet igényel

Abban egyetértenek, hogy nemcsak az igény és a példa van meg a szoftverfejlesztő központ működésére, hanem a szoftverfejlesztéshez szükséges szakmai és szellemi tudás is. „Olyan modellt is el lehet képzelni – vázolta Nagy Zsolt –, hogy a saját fejlődési lehetőségeinket kiaknázva bizonyos idő alatt jutunk el addig az ezerfős kapacitásig, amit ez a huszonöt cég egy hónap alatt közös fedél alá tud hozni. Csakhogy az informatika roppant gyors fejlődése mellett az idő rendkívül fontos tényező. A lehetőségek most vannak itt, és úgy gondoljuk, ezeket most kell kiaknázni. Egyikünk sem várhat addig, amíg vállalkozása a világpiac igényeinek megfelelő kapacitásokat tudhat a magáénak.”

„A szoftverpiac – teszi hozzá Igaz Gábor – annyiban speciális piac, hogy nagyon sokféle tudást és ismeretet igényel. Ezek a kvalitások jelenleg különböző cégekben vannak meg. Egymás felvásárlását nem tekintem lehetséges megoldásnak, hiszen mindenki saját környezetében, a saját cégében érzi jól magát. A tulajdonosváltásokkal vagy a fúziókkal megváltozhatna ez a helyzet, de ha az emberek elhagyják, értéktelenné válna a cég is. A közösen választott megoldással mindenki megőrizheti önállóságát, hosszabb távon mégis kialakulhat az a kritikus tömeg, amiből már komoly cég építhető fel.”

Huszonötből több

Lapzártánk idején huszonöt vállalkozás – az Albacomp, az Axis, a Bancraft, a Banksoft, a B.I.T. Hungary, a Duna Elektronika, az Eurotrend, a FreeSoft, a HLC, az Integra, az

Interface, az Intersoft, az IqSoft, az IT Consult, a MAVI, a MIS, a Montana, a Rakit, a Regens, a Simpletech, a Triad, az Ulissys, a Unitis, a VT-Soft és az X-Prompt – vezetői folytattak tárgyalásokat a legnagyobb magyar szoftvercég létrehozásáról. Leghamarabb februárban derül ki, a tárgyalások kezdetén megjelent érdeklődők közül hányan tartottak ki a jobb piaci pozíció reményében.

Nagy Zsolt: Nem várhatunk, amíg vállalkozásunk a világpiac igényeinek megfelelő kapacitásokat tudhat a magáénak

Báti Ferenc elképzelhetőnek tartja, hogy végül nem huszonöt, mindössze tizennyolc cég fog össze, ám a számuk igen hamar megduplázódhat. „Nem azért, mert mi ezt szeretnénk, hiszen tizennyolcat sem könnyű koordinálni, hanem mert erre igény van.” Ugyanakkor szinte biztos abban, hogy rövid időn belül versenytársat is kapnak, amelynek meglehet, nem harminchat, hanem negyvenöt tagja, társtulajdonosa lesz.

Győrfi Áron a BYTE Magyarország munkatársa.

E-mail: **gyorfi.aron@iquest.hu.**

HOL TALÁLHATÓ?

FreeSoft Kft.

1011 Budapest,

Gyorskocsi u. 5–7.

Tel.: 489-4500

www.freesoft.hu

Magyar–Amerikai Kereskedelmi Kamara
1052 Budapest,
Deák Ferenc u. 10.
Tel.: 266-9880
Unitis Rendszerház Rt.
2040 Budaörs,
Kinizsi u. 2/B
Tel.: 06-23-505-050
www.unitis.hu
VT-Soft Kft.
1036 Budapest,
Pacsirtamező u. 41.
Tel.: 436-0540
www.vtsoft.hu

KÖRNYEZET
e-commerce

Fogyasztói szemmel

Az Országos Fogyasztóvédelmi Egyesület infokommunikációs munkacsoportja tavaly kétszer is vizsgálta az elektronikus kereskedelem hazai állapotát.
Szerző: Varga Miklós

Az infokommunikációs szakértő, *Fischer Gábor* szerint egyetlen negyedév alatt szembetűnő fejlődést tapasztaltak. Szinte ugrásszerűen javult a fogyasztók tájékoztatása, a vásárlás módja, a szállítás ideje és színvonala. Kedvezően változott a vizsgált weboldalak megbízhatósága, képi tartalma is. Igazi áttörést azonban az infrastruktúra, a jogi háttér, a vásárlási és az értékesítési kultúra együttes fejlődése hozhat.

A fogyasztó érezheti már, hogy az e-kereskedelem révén kinyílik számára a tér, s fizikai fáradság nélkül vásárolhat könyvet, CD-t, tartós fogyasztási cikket és még sok egyéb árut az ország bármelyik pontjáról vagy akár távoli világrészekről. A kereskedelmi lánc lerövidítésének költségcsökkentő hatása azonban nem érzékelhető eléggé. A kiadásokra érzékeny, illetve a jól ellátott környékeken élő vásárlók feltehetően még sokáig a „valódi" boltokat részesítik előnyben a virtuális áruházakkal szemben a telefonszámla, az internethasználat díja, a csomagolás és a szállítás pluszköltségei miatt.

A vizsgálatot végző fogyasztóvédők komoly visszatartó tényezőként érzékelték az infrastruktúra hiányosságait. A nap legkülönbözőbb időpontjaiban tapasztaltak lekapcsolódást, időtúllépést, s gyakran fel sem kapcsolódhattak a hálóra. Május 25-én délelőtt például egyetlen vásárláshoz 2,5 óra kellett. Egy másik alkalommal hétköznap este 7 körül 44 perc alatt jutottak a vásárlás megkezdéséig. Igaz, másnap hajnalban már mindössze 7,5 perc is elegendő volt ehhez. Előfordult olyan eset is, amikor az egyik oldalról egyszerűen nem tudtak tovább lépni, mert bármely hivatkozásra kattintottak, az idő túllépése miatt vissza kellett térni a főoldalra. A probléma okain lehet vitatkozni, de ez aligha érdekli a vásárlástól elriasztott potenciális vevőt.

ILLUSZTRÁCIÓ: BUTTINGER GERGELY

A próbavásárlásokat végzők minden esetben korrekt kereskedőkkel találkoztak. Mégis fontosnak tartják, hogy a vásárlók védekezzenek az elektronikus kereskedelemmel – ma még – együtt járó veszélyekkel szemben. Szerintük érdemes megismerni a kereskedőt, keresni a részletes termékleírást, elolvasni a szerződés feltételeit s kinyomtatni vagy elmenteni azokat. Célszerű ellenőrizni, megfelel-e a termék a magyar szabványoknak, rendelkezik-e az eladó minőségbiztosítási tanúsítvánnyal vagy pecséttel, megfelelő-e a szállítási és panaszügyintézés, az eladás folyamata, milyenek a garanciális feltételek, probléma esetén visszavonható-e a rendelés, megvédhetők-e a pénzügyi és személyi adatok.

Ezzel együtt a vevőnek mérlegelnie kell a kockázattal járó veszteségeket, megoldást találni a tömeges reklám e-mail- áradat ellen, képezni a családot a személyes adatok védelmére, valamint az online aukciókat óvatosan kezelve nem szabad pénzt küldeni annak, aki nem bizonyítja, hogy valóban birtokosa a felkínált árunak.

Kétségtelen: a vásárlók többsége ma még világszerte nyűgnek tartja az elővigyázatosság szabályait, s visszaretten az elektronikus vásárlástól, vagy behunyt szemmel fejest ugrik a kedvezőnek ítélt, alacsony kockázatú ügyletekbe. Az Európai Unió ezért ajánlásokkal készteti a kormányokat a fogyasztó védelmét szolgáló intézkedésekre, programokra. Mindenekelőtt fontosnak tartja a kiszámítható és biztonságos kereskedelem feltételeinek megteremtését, az információs infrastruktúra fejlesztésének gyorsítását, a kölcsönös előnyök maximalizálását, a szociális értékek megőrzését, illetve megvalósítását, s mindennek eredményeként a használók és a fogyasztók bizalmának kiépítését. Magyarországon az EU ajánlásainak teljesítése még csak a kezdetén tart. A távollévők kereskedelméről szóló kormányrendelet megjelent, de számos fórumon deklarálta a kormány, hogy ezen a területen is folytatódik az európai uniós jogharmonizáció. A fogyasztóvédők szerint az e-kereskedelem magyarországi elterjesztéséhez tömeges és olcsó PC, illetve internet-hozzáférés, törvényben szavatolt viszonyok, a lehetőségek megismertetése és megismerése, továbbá az információs társadalom más területein való gyorsabb fejlődés szükséges.

Varga Miklós a BYTE Magyarország munkatársa. E-mail: vargam@mail.matav.hu.

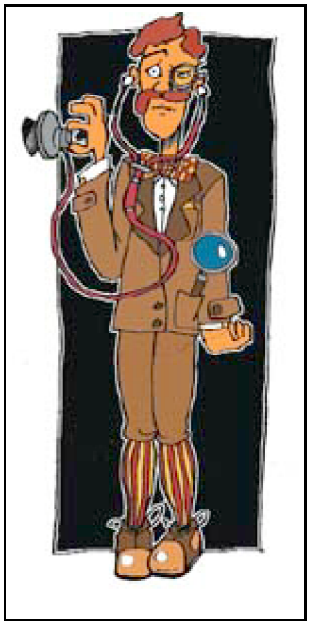
2001. FEBRUÁR / DR. WATSON Fóti Marcell rovata

DR. WATSON
Fóti Marcell rovata

2001. FEBRUÁR / DR. WATSON Fóti Marcell rovata / Technokrimi

Technokrimi

A biztonságtechnikával foglalkozók néha krimibe illő eseménysorozat kellős közepén találják magukat. Életszagú történetünk főhősei sem kerül- hették el a bonyodalmakat.



A következő néhány hónapban egy igaz történetet mesélek el. A cégek és szereplők nevét megváltoztattam, de az érintett vállalatok tevékenységi körét nem. Merítek, ha nem is idézek a nyomozati anyagként felhasznált belső levelezésekből, rendszernaplókból, nyilvános levelezési listák (lyris.netacademia.net) archívumából, ahol például a mai napig megtalálhatók és azonosíthatók az eredeti levelek, felhasználó- és cégnevek. A kíváncsibbak akár meg is kereshetik, az aktív listatagok pedig talán még emlékeznek rá. Hisz mindez nem is oly rég, 2002-ben történt. :) Az ICQ üzenetek sajnos elvesztek, de a történet így is kerek egész. Szolgáljanak az alábbiak tanulságul minden hackernek: a sánta kutyánál is lassabban fut a hazug, csaló ember.

Az alábbi írásban meghagytam azokat a kifejezéseket, amelyeket az elektronikus levelekben olvastam. Ezeket bizony így írják hejesen (ly)! Meg kell különböztetnünk egymástól például a király és a kiráj szót. Míg az előbbi egy főnév, addig pontos j-vel írva jelzőként használatos. Kiráj = jó, nagyszerű. De ilyen a rencergazda szó is, hisz így írva kemény két karaktert meg lehetett takarítani – ez 18 százalékos tömörítésnek felel meg! Később egy szószedetben is elmagyarázom az esetleg teljesen érthetetlen szavakat.

Maga a történet viszonylag egyszerű. Adott a QTV, valamint konkurense, az X-Channel, a másik országos tévécsatorna. Ezek egymástól lopkodják a műsorterveket, amit az is bizonyít, hogy a két csatorna egy időben mindig pontosan ugyanolyan műsort sugároz, nehogy lemaradjon a másiktól. Ha az egyiken vetélkedő megy, akkor a másikon is. Ha a másik csatornán megváltoztatják az esti film kezdési időpontját, a másik azonnal fut utána. Ne firtassuk, ennek az egésznek van-e bármi értelme, mert jómagam például alig nézek tévét. Ha mégis ott ragadnék előtte, s egy műsorról kiderül, hogy sorozat, már kapcsolok is át. Ahol szintén sorozat van. Kikapcs. Egymástól még egy hangyányi eltérést sem mernek kipróbálni sem a kereskedelmi tévék, sem a kereskedelmi rádiók. Viszont ami miatt mégis különös fontosságot tanúsítok a műsorlopási jelenségnek, az az, hogy itt valódi, sőt tipikus ipari kémkedésről van szó. S mindez a szemünk előtt zajlik! S most lássuk a dokumentumokat. Szólaljanak meg végre a QTV rendszergazdái. Az alábbi levelet a vezető rendszergazda küldte kollégáinak:

From: hook@qtv.hu

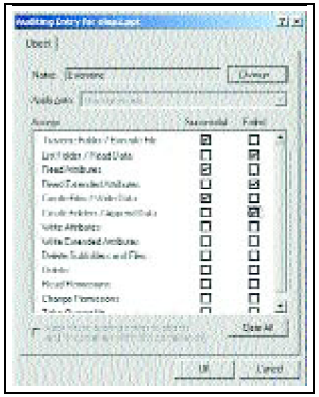
To: IT@qtv.hu

Date: 2002 december 27 wednesday

Subject: Sux az unnepek kozott

Baze fiuk, be kell mennunk a ket unnep kozott. Meglehet, hogy szilveszterkor is. Ilyen legutobb 2 eve volt az emlekezetes 2000 evi hisztinel. De amig akkor csak rohogtunk rajta, s valojaban mindenki tudta, hogy baromsag az egesz, addig most gaz van. Sajnos hiaba vitettuk gepre a musorterveket a szerkesztokkel, igy is elloptak. Lapozzatok fel a teletexteket a 303. oldalon es gyozodjetek meg rola. Szal holnap gyertek be. Sorry.

hook



1. ábra

Ez a dokumentum természetesen nem publikus, így csak itt és most olvasható. Az alábbi azonban a security@lyris.netacademia.net címre érkezett, ennek a levelezési listának a tagjai meg is kapták:

From: hook@qtv.hu

To: security@lyris.netacademia.net

Date: 2002 december 28 Thursday

Subject: Bemutatkozas es 1 kerdes

Hello lista, de jo hogy vagytok! Most talaltam ratok a BYTE-ban lapozgatva. Telleg, hogy kerult az hozzam? No mind1. Bemutatkozom. Hook vagyok a QTV-tol, es az egyik baratomnak az lenne a kerdese, hogy hogyan lehetne megallapitani, hogy egy bizonyos fajlt ki olvasott el, illetve ki tette ki lemezre, kuldte el esetleg emilben. A baratomtol ugyanis nem eloszor elloptak egy fajlt. Valami kis jutiliti jo lenne.

Thx hook

Mivel a két ünnep között nem volt valami nagy forgalom a listákon, személyesen én válaszoltam hooknak, illetve a listának, amit az összes előfizető megkapott:

From: marcellf@netacademia.net

To: security@lyris.netacademia.net

Date: 2002 december 28 Thursday

Subject: Re: Bemutatkozas es 1 kerdes

Hi hook,

Hat utolag gyakorlatilag remenytelen a helyzet-sajnos. Korabban kellett volna ebredned, es akkor beallithattad volna a kritikus fajlokon/konyvtarakon az NT esemenynaplozast. Tudod hogy kell? Jobbklatty a fajlon, properti, security ful, audit. See etecs. (Lásd az 1. ábrát – *A szerk.*)

Ez ugyan W2K-s, de az NT-ben is hasonlo. A lenyeg h csak arra allitsd be, amire telleg kivancsi vagy, mert kulonben belefulladsz a sok Event Log bejegyzesbe. Az Event Logban a Security lapon fog gyulni az info.

fm

Hook valószínűleg még sohasem csinált ilyet, mert visszakérdezett:

From: hook@qtv.hu

To: security@lyris.netacademia.net

Date: 2002 december 28 Thursday

Subject: Re: Bemutatkozas es 1 kerdes

Koszi. NT4 a kornyezet, kicsit szivtam ugyan, mert nem volt security ful, de a kollegak tudtak a megoldast: miutan a FAT-ot NTFS-re konvertaltam a CONVERT D: /FS:NTFS paranccsal, megjelent. Bepipaltam. Kiprobaltam. Nem mukodik, ures az Event Log. Mi a baj? Volt egy hiabuzenet, de nem emlekszem ra.

hook

From: marcellf@netacademia.net

To: security@lyris.netacademia.net

Date: 2002 december 28 Thursday

Subject: Re: Bemutatkozas es 1 kerdes

Hi hook,

A hibauzenet arrol szolt, hogy a naplozast be kell kapcsolni a NAAAAGY fokapcsoloval, a juzer menedzserben. Polici->audit. Itt a file es object accesst kell bepipalni. De ha mar itt vagy, pipald be a sikertelen logon/logoffot is. Hatha valaki probalkozik a jelszavak kitalalasaval. Ez itt a W2K fokapcsoloja, az Administrative Tools->Local Security Policy. See etecs. (Lásd a 2. ábrát – *A szerk.*)

fm

Most már csak röviden, levélfejlécek nélkül írom a lényeget, mintha beszélgetnénk, de természetesen ez is levelezés:

Hook: Aha, megy! 1 gépen. Na de van 155. Hogy lehetne automatizálni?

FM: Sehogy. Különösen a fájlok beállítását tartom reménytelennek. Minden fájl azonos nevű? :)

Hook: Dehogy. Sőt, azt sem tudom, hol vannak. Excel táblák. Na jó, ezzel elleszünk egy darabig. :(

Ezután hook ezt írta kollégáinak:

From: hook@qtv.hu

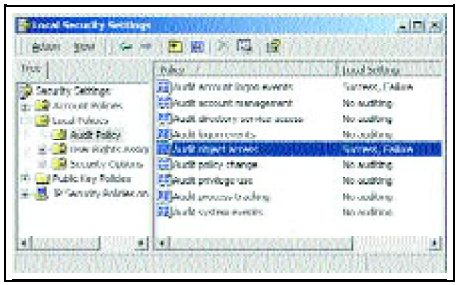
To: IT@qtv.hu

Date: 2002 december 28 Thursday

Subject: Naplozas

Fiuk, ma itt alszunk. A naplozas, amit Petivel kiszenvedtunk, sajnos nem allithato be 155 gepen eccerre. Pizza, kola van, megkerdeztem Andit, fizetik. A csaladotoknak mondjatok jo eccakat.

hook



2. ábra

Ezután néhány napnyi csend következett, a QTV-sek úgy gondolták, felkészülten várták a következő behatolást. Az óriási naplóhadjárat nem várt eredménnyel járt: a következő héten kiderült, hogy maga hook lopkodta le a fájlokat a gépekről. :) Természetesen ez nem igaz. Akkor mi történhetett? Kiderül a folytatásból…

Fóti Marcell (MCT, MCSE, MCDBA, MZ/X).

E-mail: **marcellf@netacademia.net.**

Szótár az e-mailekhez

Szó	Magyarázat	Tömörítés
Baze	Egy közismert, ámde nyomdafestéket nem tűrő káromkodás majdnem kiejtés szerinti leírása.	50% (8 karakter helyett 4)
Sux, suxolás	To suck = szívni (szótár szerint). Meglepő, de az angol nyelvterületen is ezt a szót használják a pórul jár kifejezés helyett.	25%

Szó	Magyarázat	Tömörítés
Szal	Szóval, egyszóval.	33%
Etecs	Attach. Csatolás, csatolt dokumentum.	28%

MÉRLEG
Diskeeper 6.0

Rend a lelke mindennek

A hatos verziószámot megérni elég szép teljesítmény egy szoftver életében: nincs ez másképp a Diskeeperrel sem.

Szerző: Tóth Endre

Vége a merevlemez-töredezettségnek

Diskeeper 6.0

Digital Kft.

www.digital.co.hu

Workstation ár: 50–75 dollár

Server ár: 260–400 dollár

A nagygépes környezetből eredő Diskeeper 6.0 töredezettségmentesítő lényegesen másként viselkedik, mint elődje, az ötös. A közel másfél éves fejlesztésnek köszönhetően má Server változata. Ezek elsősorban abban különböznek egymástól, hogy milyen fájlrendszert hajlandók rendbe rakni, illetve milyenek a képességeik a hálózatos működés terén.

A Workstation minden partíciótípust kezel, de csupán egyes gépeken hajlandó működni. A Server egyedül FAT16 és NTFS partíciókat hoz egyenesbe, illetőleg azon belül az MF és irányíthatja az egyes munkaállomásokon futó Diskeeper példányok működését.

Az 5.0 változat kivette ugyan az MFT-ben tárolt fájldarabkákat, de magát az MFT-t nem tudta folyamatos darabbá rendezni. Az új verzió elboldogul ezzel a problémával, bár kiz Ugyanígy rendbe rakja a page-fájlt és a könyvtárakat a leállított rendszer mellett. Az NTFS könyvtáraihoz ugyanis futó rendszer alatt tilos nyúlni. Ez érvényes FAT16-on is; ho lemezen található adatokat és a rendrakás folyamatát, bár a körítés megváltozott az új funkcióknak megfelelően.

A Server hálózati műveleteinél szintén akad néhány változás: Microsoft Networking munkacsoportonként vagy domainenként, de akár egyes gépekből vagy azok egyes lemez Workstationben egyedül ez a funkció szerepel).

A Diskeeper – szemben a Windows 9x és a Windows 2000 beépített eszközeivel – önállóan képes futni, miután beállította a rendszergazda. Elég csupán elindítani a gépet. A pro sem használnánk ki munkánk során. Újdonság, hogy egy időben akár több lemezen is dolgozhat, persze csak több fizikai egységnél érdemes használni ezt a funkciót.

Az Executive Software egyébként szerényen a „Fastest Windows defragmenter ever built”, vagyis a valaha készített leggyorsabb Windows töredezettségmentesítő kifejezéssel il

OpenVMS és NT-Alpha platformokon, bár az eltérő fejlesztési irányok miatt a fő hangsúly a Windows környezetben futó változatokon van. Olyannyira, hogy jelenleg ez az egyetlen,

Tóth Endre

E-mail: **xorn@matavnet.hu.**

ÉRTÉKELÉS

Technológia	*****
Megvalósítás	*****
ÁR/Teljesítmény	*****

2001. FEBRUÁR / MÉRLEG Diskeeper 6.0 / FÓKUSZ

FÓKUSZ

FragGuard

Három olyan töredezettség létezik, amely csak újraindítás közben, álló rendszernél szüntethető meg biztonságosan: a page-fájlé, az MFT-é és a könyvtárszerkezeteké. A FragGuard könyvtárbejegyzések összegyűjtéséhez kell újraindulni a géppel. Az eredmény: sokkal kevesebb újraindítás és a fájlrendszer nagyobb teljesítménye.

Set it and Forget It – Smart Scheduling

A Set it and Forget It beállítással teljesen automatizálható a töredezettségmentesítés. Ennél azonban tovább lép a Diskeeper 6.0: Smart Scheduling technológiájával analizálja a leme forgalmas időszakban a Diskeeper ne rabolja az értékes erőforrásokat.

2001. FEBRUÁR / MÉRLEG CorelDraw 10 Graphics Suite

MÉRLEG
CorelDraw 10 Graphics Suite

2001. FEBRUÁR / MÉRLEG CorelDraw 10 Graphics Suite / A grafikus bajnok

A grafikus bajnok

A Corel ismét ringbe szállt új, 10-es számot viselő versenyzőjével – igen szép eredményeket érve el.

Szerző: Gigor Csaba

A CorelDraw 10 a vektoros és a bittérképes grafikák mellett animációkkal is elboldogul

FOTÓ: SZEPESI TIBOR

CorelDraw 10 Graphics Suite

Forgalmazó: CODRA Kft.

1119 Budapest, Vahot u. 6.

Tel.: 466-6263

www.corel.hu

Nettó ár: 209 000 Ft

Nettó upgrade ár: 89 000 Ft

A fejlesztők ezúttal elsősorban a professzionális felhasználók kényelmének növelésére, munkájuk elősegítésére összpontosítottak. Addig-addig mesterkedtek, míg végül sikerült egy fürgébben futó, könnyebben kezelhető programegyüttest alkotniuk. Ami lényeges, hogy ezentúl az animációk kezeléséhez is hathatós segítséget kapunk az új családtag, a Corel R.A.V.E. révén.

A CorelDraw 10 vektorgrafikus laptervező és illusztrációs program újdonságai közt szerepelnek az előre programozott beállítások, az úgynevezett presetekkel ellátott funkciók. A felhasználók is készíthetnek ilyeneket, így amikor többször kell azonos paraméterekkel ugyanazon effektet vagy funkciót alkalmazniuk, jelentősen meggyorsíthatják a munkájukat. A formázó opciók és effektek eredménye a valós idejű preview funkcióval kísérhető figyelemmel. A többoldalas dokumentumok tartalmát a Page Sorter használatával, az oldalak nézőképeinek segítségével ellenőrizhetjük, miközben az egyes oldalakat felépítő rétegeket és objektumokat az Object Manager ablakban láthatjuk. A tervezési idő lerövidítését szolgálja a PerfectShapes, amellyel gyorsan készíthetünk komplex alakzatokat, például nyilakat, csillagokat, szövegdobozokat, illetőleg folyamatábra-dobozokat. A körvonal, kitöltés, méret, pozíció, elfordulás és egyéb paramétereket könnyedén változtathatjuk. A textúrakitöltő a többi interaktív effekttel megegyező felbontással renderelődik az egységes látvány érdekében. A finom színátmenetekről gondoskodó interaktív kitöltő eszközben is történtek változások. A kontrollvektorokhoz bármikor létrehozhatunk újabb csomópontokat. A kibővített szövegkezelő eszközök egyetlen dialógusablakba kerültek, a szövegformálás dialógusban egyszerűbb lett a karakterszinten történő formázási opciók változtatása. Helyesírás- és nyelvhelyesség-ellenőrzőt, valamint thesaurust is beépítettek. A QuickCorrect funkcióval a gépelési hibák kijavítása is automatizálható. A programcsomag webgrafikák készítéséhez szükséges segédeszközöket tartalmaz.

Dokumentumunk HTML-oldallá konvertálására külön parancs szolgál, de készíthetünk úgynevezett rollover képeket, gombokat, amelyekhez hangokat is rendelhetünk. Az állományokat több formátumba és sávszélességre is optimalizálhatjuk, és készíthetünk PDF vagy akár Macromedia Flash dokumentumokat is. A nyomtatási funkció továbbra is igen hasznos eszköze a Preflight, amely a művelet előtt ellenőrzi a dokumentumot. Ha hibát talál, tanácsot ad annak kiküszöbölésére.

A Corel Photo-Paint 10 fényképek retusálására, szerkesztésére, bittérképes képek készítésére alkalmas eszköz. Egyes szűrőivel már a kép szkennelésénél javítja a bevitt ábra minőségét, míg másokkal látványos képi megoldások érhetők el. A felhasználói felület ízlés szerint testreszabható, ide értve a színpalettákat és a menüket is. Az egyéni beállítások részben vagy egészben megoszthatók más felhasználókkal. Az új komponensarchitektúrának köszönhetően erősebb lett a program feletti kontroll, mivel a memóriába csak az éppen szükséges alkotóelemek töltődnek be. A program lehetőséget kínál a felhasználónak, hogy kikapcsolja a zavaró vagy szükségtelen figyelmeztető jelzéseket, hibaüzeneteket. Olyan szövegkezelő eszközökkel bővítették a programot, mint a Text-On-A-Path, amely egy általunk megrajzolt görbére illeszti a beírt szöveget, vagy az új Anti-Aliasing a kisebb pontméreteknél is megfelelő minőségű látvány elérésére.

A CorelDraw Graphics Suite család legfiatalabb tagja a Corel R.A.V.E. Felhasználói felülete a CorelDraw-hoz hasonló felépítésű. Tartalmazza az összes megszokott animálási lehetőséget: timeline ablakot, layereket, egymásba tűnési funkciókat és hangokat is képes kezelni. A végeredményt swf (Flash), gif és avi formátumokba is exportálhatjuk.

Gigor Csaba a BYTE Magyarország munkatársa. E-mail: ***gigor@byte.hu.***

ÉRTÉKELÉS

Technológia	*****
Megvalósítás	*****
ÁR/Teljesítmény	****

2001. FEBRUÁR / MÉRLEG CorelDraw 10 Graphics Suite / FÓKUSZ

FÓKUSZ

R.A.V.E.

Az animációt az időtengely hosszában szerkeszthetjük. Ezt a módszert több elterjedt program is alkalmazza, mert így végig átlátható marad a munkafolyamat, bármennyi obj keyframeknek (animációskulcs-kocka). Ez lehet akár egy effekt is, amelyet szintén külön objektumként kezelünk. A Corel R.A.V.E.-ben automatizálhatjuk az effektek létrehoza egyes képkockán külön beállítani.

2001. FEBRUÁR / MÉRLEG Mobiltelefonok

MÉRLEG
Mobiltelefonok

2001. FEBRUÁR / MÉRLEG Mobiltelefonok / Osztálytalálkozó

Osztálytalálkozó

Talán a karácsonyi ajándékozási láz sarkallta rendkívüli aktivitásra a mobiltelefonok gyártóit.

Szerző: Hanácsek István

Az ősz beköszöntével nem csupán a mezőgazdasági termények értek be, hanem a mobiltelefonok is. A nagy gyártók sorra mutatták be legújabb készülékeiket, közülük most két neves cég telefonjait vizsgáltuk meg.

Panasonic GD52 és GD92

Kis méret, pille súly, gazdag szolgáltatás

Panasonic GD92

Panasonic Magyarország Kft.

1117 Budapest,

Neumann János u. 1.

Tel.: 382-6060

www.panasonic.hu

Bruttó ár: 54 900 Ft-tól

ÉRTÉKELÉS

Megvalósítás	*****
ÁR/Teljesítmény	****

Kis pénz, kis készülék, nagy tudás

Panasonic GD52

Panasonic Magyarország Kft.

1117 Budapest,

Neumann János u. 1.

Tel.: 382-6060

www.panasonic.hu

Bruttó ár: 12 900 Ft-tól

ÉRTÉKELÉS

Megvalósítás	*****
ÁR/Teljesítmény	*****

A Panasonic igen jól csengő név a szórakoztató elektronikában. Termékei leginkább a csúcskategóriás készülékek közé tartoznak. Nincs ez másként a telefonjaikkal sem. A GD c
megszokott szolid külsejű, esztétikus berendezés. Pehelysúlyukhoz (99, illetve 77 gramm) nem társul a használhatatlanul kis méret. A tervezők jó érzékkel megtalálták a középutat: kénye

A cég mindkét telefonnal igencsak magasra emelte a mércét, hiszen összességében a legjobb ár/teljesítmény mutatóval rendelkeznek. Jól példázzák a japán mentalitást: olcsó, megbízható

Közös jellemzőjük az átlátszó, műanyag borítású billentyűzet és a négyállású navigációs gomb. A készülékek az ikonos menürendszer és a középen található, négy irányba billenthet
megjelenik. A menüpontok mellett sorszám is feltűnik, amelyet a menübe való belépés után begépelve rögtön a kívánt szolgáltatáshoz jutunk. A kontrasztállítási lehetőségnek köszön
narancs és zöld) is változtatható, ami főként sötétben teszi érdekessé a telefont. A hívócsoportokhoz rendelhető színek alapján már a hívás pillanatában tudhatjuk, mely kategóriából keres

Ezeket a mobilokat különösen azok fogják értékelni, akiknek a kommunikáció mellett a sajátos egyéniségű készülék is fontos. Ez utóbbit elsősorban a csengőhangoknál lehet tapasz
nagyon jó minőségű hangzás és a minden más telefontól eltérő, húszféle csengőhang teljesen egyedivé teszi őket, s mindehhez az egyéni csengőhangot a telefon mikrofonján ker

használhatók: a hátlapba épített kis hangszóróval egyméternyi távolságból is jól hallható a beszéd.

Diszkrét helyzetekben jól jöhet a folyamatos vagy szaggatott üzemmódra állított rezgő hívásjelzés. A beépített óra mellett van ébresztés, de beprogramozhatjuk a telefon be-, ille funkció nincs a készülékben, de az ébresztőórával egy nap akár több időpontra is figyelmeztethetjük magunkat. A saját telefonkönyvbe a SIM kártyán kívül további ötven, illetve fix és egy általunk beírt minta segít a gyors szerkesztésben, illetve angol nyelvet választva a már szabvánnyá váló T9 prediktív szövegbevitelt is használhatjuk. További szolgáltatás a

A GD52 és a GD92 egyelőre nem követi a divatot, nem lehet vele közvetlenül elérni a mobil internetet (WAP). Nincs benne játék és hiányzik az infraport, így a számítógéppel v Ha telefonálás közben éppen nincs kéznél papír, segít a voice memo szolgáltatás, amellyel egy diktafonhoz hasonlóan kétszer 15 másodpercnyi beszélgetést, illetve kétszer 10 másodp

A GD52 vékonyka lítium-ion akkumulátorának egyszeri feltöltésével három órát beszélgethetünk, illetve 150 órán keresztül várhatjuk a hívásokat, míg a GD92-nél ez 3,5, illetve 160

Nokia 6210

Mindenkinek van egy álma

Nokia 6210

Nokia Magyarország Kft.

1092 Budapest, Köztelek u. 6.

Tel.: 06-20-977-7797

www.nokia.hu

Bruttó ár: 79 900 Ft-tól

A finn Nokia sem maradt ki az őszi újdonságokból. Az igazán sikeres 6110-es sorozat nyomdokain haladva piacra dobta 6210 típusjelű, kétnormás (900/1800 MHz) telefonját. egyeznek meg, a tömege azonban kisebb, 114 gramm. A szolgáltatásokban gazdag telefon alkalmas a HSCSD (High Speed Circuit Switched Data, nagy, legfeljebb 43,2 Kbps se Kezelését a Nokiánál megszokott és a 7110-zel szinte teljesen megegyező menürendszer teszi kényelmessé.

A bőkezűen felszerelt, középkategóriásnak szánt telefon számos területen messze kiemelkedik a mezőnyből. Elsőként az ezer név és 150 SMS-üzenet tárolására elegendő memó emlékeztető ikonnal is megtoldható. Üzeneteinket mintegy 150-féle csoportba szervezhetjük. Az SMS-írást a beépített, előre szerkesztett sablonok és a – sajnos magyar nyelve képeket csatolhatunk. A 6210-es tulajdonosa ötféle hívásprofilt készíthet magának. Szintén a használatot könnyíti meg a hangtárcsázás: tíz telefonszám hívható egy-egy szó határidőnaplót, ráadásul az aktuális esemény előtt a beállított időpontban hangjelzéssel és a képernyőn megjelenő üzenettel figyelmeztet minket a teendőre.

Unaloműzésként három játék közül válogathatunk. Ébresztőóra, számológép, valutaátváltó program gazdagítja a szolgáltatások sorát. Az egyedi beállítást a 38-féle beépített és to
könnyíti a beépített infravörös csatlakozó, hiszen ezen keresztül számítógéppel vagy akár egy nyomtatóval is összekapcsolhatjuk a telefonunkat. A 900 mAh-s lítium-ion akkumulátor

Hanácsek István a HiCo Számítástechnika cégvezetője.

E-mail: **hicosz@hotmail.com.**

ÉRTÉKELÉS

Technológia	*****
Megvalósítás	*****
ÁR/Teljesítmény	****

2001. FEBRUÁR / MÉRLEG Mobiltelefonok / FÓKUSZ

FÓKUSZ

SZABVÁNYOK

GPRS

A GPRS (General Packet Radio Services) a mobilkommunikáció új, nagy reményű szabványa. A GPRS igyekszik optimálisan szétosztani a rendelkezésre álló adatátviteli kapacitást a
eljárással 21 Kbps sebességre feltornázott csatornákból legfeljebb nyolcat lehet összefogni, így elméletileg 170 Kbps sebesség érhető el. A telefon bekapcsolásának pillanatától fogv
éppen letöltünk valamit, vagyis adat- vagy honlapolvasás közben nem növekszik a telefonszámlánk. Az eddig említett eljárások közül várhatóan ez lesz az, amely teljes mértékben megvál

UMTS

A harmadik generációs UMTS (Universal Mobile Telecommunications System) szabvány – a GPRS rendszer nagy vetélytársa – igazán használhatóvá teszi a telekommunikációt. Zá
jelenlegi szabványnál. Ez a megoldás már alkalmas a videoképek élvezhető átvitelére is. Ez a merőben új technológia azonban teljesen eltérő infrastruktúrát igényel: az adótornyoktól kezd

A készülékek tesztelését a Westel Mobil Rt. támogatta.

2001. FEBRUÁR / FÓKUSZ Adatvédelem

2001. FEBRUÁR / FÓKUSZ Adatvédelem / A biztonság kilenc pontja

A biztonság kilenc pontja

A Novell adatvédelmi koncepciója az alapelveket foglalja össze.

Szerző: Kelenhegyi Péter

Előrejelzések szerint a tavaly regisztrált 327 milliós on-line felhasználói tábor létszáma 2003-ra 600 millióra nő. És ez még csak a fogyasztói e-kereskedelem. Ám minél aktívabb e-üzleti tevékenységet folytat egy vállalat, annál komolyabban kell vennie mind saját, mind partnereinek adatbiztonságát.

Az *Information Week* felmérése szerint a hálón termékeket vagy szolgáltatásokat kínáló cégek 59 százalékánál fordult elő tavaly egy vagy több biztonsági probléma – ezek többsége azonban nem került nyilvánosságra. Az ismert esetek közé tartozik, hogy augusztusban az egyik brit banknak sikerült nyilvánosan megjelenítenie ügyfelei számlaszámait e-banking webhelyén. Ugyanebben a hónapban az egyik ismert angol nagykereskedő volt kénytelen lezárni webhelyét, mert az egyik vásárló hozzáfért mások hitelkártyaszámaihoz. Új, feltörekvő cégek számára az ilyen galiba végzetes is lehet.

Bár az elektronikus üzletvitel célja, hogy a vállalat ügyfelei, beszállítói közvetlenül elérhessék munkatársainkat, egyes alkalmazásainkat, a valóságban a cégek – legalábbis szándékosan – soha nem engednek a sajátjukkal megegyező szintű hozzáférést a külső felhasználóknak. Nem kerülhetnek napvilágra például a könyvelési vagy értékesítési rendszerek pénzügyi adatai, nem kószálhatnak szabadon az üzleti vetélytársak a személyzeti rendszerekben és nem juthatnak be vírusok, rosszindulatú támadók sem belülről, sem hálózati partnertől, sem az internetről.

A Novell és stratégiai partnerei szerint az átfogó biztonságpolitikai keretrendszer kilenc elemből áll. Ezek közös vonása, hogy a vállalat informatikai rendszerei egyetlen pontból felügyelhetők.

• **Tűzfal.** A tűzfalak védelmet nyújtanak a belső és külső fenyegetések ellen, ugyanakkor biztonságossá teszik az alkalmazottaknak, a vásárlóknak és a partnereknek a vállalati adatok internetes elérését.

• **Egypontos bejelentkezés.** Csökkenti a többféle jelszó használatából adódó felügyeleti terheket, valamint annak a veszélyét, hogy az alkalmazottak jól látható helyre írják le jelszavaikat.

• **Virtuális magánhálózat.** Költséghatékony és biztonságos mód a távoli felhasználók és fiókirodák, valamint a központ összekapcsolására.

• **Feljogosítás és hitelesítés.** Az elektronikus üzletvitel biztonságának lelke, a hitelesítés igazolja, hogy a felhasználók valóban azok, akiknek mondják magukat. A feljogosítás az a folyamat, melynek során hozzáférési jogokat kapnak a számukra meghatározott biztonsági szintnek megfelelően.

• **Biztonságos üzleti kommunikáció.** A csoportos munka során a biztonságos, azonnali üzenettovábbítási környezet elengedhetetlen a csoporttagok hatékony kommunikációjához.

• **Tanúsítványok kezelése.** A PKI (Public Key Infrastructure, nyilvános kulcsú titkosítási infrastruktúra) az adatok védelmének legbiztonságosabb és szabványos módja az interneten. Az adatok titkosítva továbbítódnak, és csak az arra jogosult címzett képes a dekódolásra.

• **Behatolásfelderítés.** A jogosulatlan felhasználók azonosítása, figyelése és kizárása.

• **Vírusvédelem.** Az összes lehetséges támadási felület védelme a vírusok ellen.

• **Hálózatfelügyelet.** Egyszerű felügyeleti eszközök, amelyekkel automatizálhatók a biztonságfelügyelet egyes funkciói.

A biztonságpolitika megtervezése és kialakítása előtt célszerű független céget megbízni a biztonság felmérésével. A hatékony biztonságpolitika kialakítása a vállalat minden egyes részére hatással lesz, ezért elkötelezettséget kíván meg a vezetés legfelsőbb szint-jeitől is.

Kelenhegyi Péter a BYTE Magyarország főszerkesztője.

E-mail: **kelenhegyi@byte.hu.**

Csomagmegoldás elemenként

Nem készül ugyan belőlük dobozos megoldás, de partnerein keresztül elérhetők a Novell kilencpontos biztonsági koncepciójának elemei.

Tűzfal. A Novell BorderManager Firewall Services a csomagszűrő, az áramköri átjárók és az alkalmazásproxyk szintjén kínál tűzfalas védelmet.

Egypontos bejelentkezés. A Novell Single Sign-on az NDS eDirectoryt használja a felhasználói profilok tárolásához.

Virtuális magánhálózat (VPN). A Novell BorderManager VPN Services a felhasználókat az NDS eDirectoryn keresztül hitelesíti; megfelel a beágyazások, a titkosítás és a kulcscsere-mechanizmusok szabványainak.

Hitelesítés és feljogosítás. Az NDS eDirectoryra épülő Novell Modular Authentication Services (NMAS) képes mind a többféle módszeren alapuló, mind a többszintű hitelesítésre.

Biztonságos üzleti kommunikáció. A Novell GroupWise a dokumentumokkal kapcsolatos jogokat – megtekintés, szerkesztés, megosztás – az NDS eDirectoryval felügyeli. A GroupWise 5.5 Enhancement Pack lehetővé teszi a rendszergazda jogainak korlátozását és finom szabályozását.

Tanúsítványok kezelése. A felek azonosítását szolgálja a Novell Certificate Server vagy az Entrust PKI infrastruktúrája; ez látja el a kulcs- és tanúsítványfelügyeleti funkciókat.

Behatolásfelderítés. A hacker- és vírustámadások évente körülbelül 1,6 milliárd dollár kárt okoznak világszerte. A BindView by-Control for NetWare and NDS átfogó rendszerbiztonsági értékelést végez.

Vírusvédelem. A GroupWise ellenáll a makróvírusoknak, a McAfee ActiveVirus Defense-ben alkalmazott ViruLogic technológia pedig felderíti és kiirtja a beférkőzni próbáló újfajta vírusokat is.

Hálózatfelügyelet. A BindView by-Control for NetWare and NDS növeli a NetWare és NDS eDirectory szerverek biztonságát.

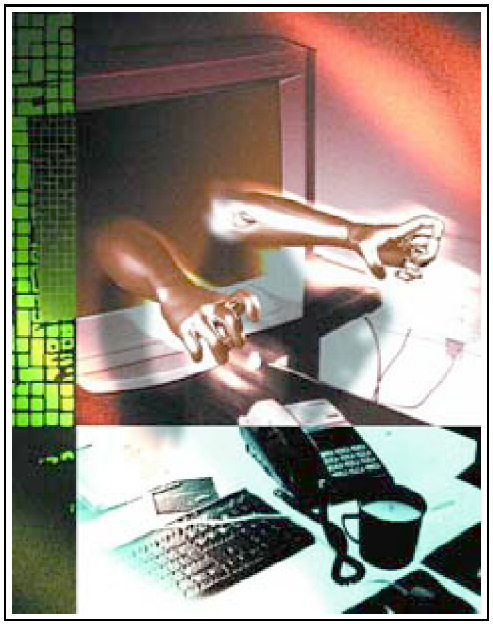
Mindennapi tűzfalaink

Az adatforgalom legkényesebb kérdése az adatok védelme.

Szerző: Simay Endre István

Noha az adatvédelemnek megvannak a maga jogi normái, etikailag és a cégek gazdasági érdekei szempontjából is nélkülözhetetlen az illetéktelen adathozzáférés megakadályozása. Az adatáramlás két végpontja közti útvonalon alkalmazhatók a különböző titkosítási eljárások, amelyek többé-kevésbé képesek a „drót” lehallgatása ellen védeni adatainkat. Az erre a célra használt kódolási eljárásokról sem árt azonban megjegyezni, hogy nem megfejthetetlen titkosításon alapulnak, hanem azon az egyszerű gazdaságossági szemléleten, miszerint a kód megfejtésével elérhető információ megszerzése ne érje meg a dekódolás munka- és energiaráfordítását.

Nem alkalmazható a titkosítás a cégek belső hálózataira csatlakozó munkaállomásokon, minthogy a valós időben elérhető háttértáraikon – általában merevlemezeken – az adatok dekódolt formában, az adott operációs rendszer számára közvetlenül olvasható állapotban vannak jelen. E megállapítás igaz még abban az esetben is, ha a fájlrendszer titkosított formában tartalmazza az adatokat (erre egyelőre főleg a Unix világában találunk példákat). Ilyen körülmények között aki az adott szerver vagy munkaállomás kezeléséhez hozzáfér, gyakorlatilag közvetlen adatelérési lehetőséget szerez a belső információkhoz. Nem véletlen tehát, hogy már az informatika korai szakaszában kialakultak azok a szoftveres és hardveres, valamint a cég munkarendjének kialakításán alapuló megoldások, amelyek az informatikai eszközök fizikai hozzáférését szabályozták például zárható szobákkal vagy jelszavas gépeléréssel. Csakhogy ezzel sem teljes a védelem, mivelhogy nyitva marad a hálózat, illetve azon keresztül a géphozzáférés lehetősége, amelyről a felhasználó a legtöbbször nem is tud. Így a globális hálózatok világában egyre szélesebbre tárulnak a magánemberek és a vállalati hálózatok számítógépei előtti kapuk.



ILLUSZTRÁCIÓ: BUTTINGER GERGELY

Míg korábban csupán a cégek nagy adatkiszolgálói és a szerverekre kapcsolódó munkaállomások adatvédelme volt a feladat, ma már valamennyi, a világhálóra kapcsolódó személyi számítógépet hálózati munkaállomásoknak kijáró védelemmel kell ellátni. Régebben az adatokhoz csak jól körülhatárolt felhasználói kör férhetett hozzá, melynek tagjait a vállalati informatikusok személyesen is ismerhették. A cég képviselője a pusztán IP-címekkel azonosított ügyfelek közül általában az üzleti partnerekkel kerül közvetlenebb érintkezésbe, az elektronikus kereskedelemben viszont velük is mindössze virtuális, habár hitelesített kapcsolatrendszer jön létre.

Hasonló helyzetet teremt a dolgozók körében a távmunka és a virtuális magánhálózatok (VPN-ek) terjedése, hiszen azokban komplex azonosítás előzi meg a tagok adathozzáférését. A cégek és a magánemberek számára azonos IP-szabványú adattovábbítás garantálja, hogy egyező technológiával böngészhessék a cégek weblapjait, mint amivel a más célú, személyes információikat beszerzik.

Sok fejfájást okozhat, ha a személyes információ kifürkészésének megakadályozása kudarcba fullad. Például az üzleti, banki adatok illetéktelen elérése tetemes anyagi és – ha nyilvánosságra kerül – erkölcsi károkat okozhat. Ez a publicitás könnyen megszerezhető a behatolók hiúsága vagy a cég népszerűségének csorbítása okán. Magánemberek esetében, hasonlóan a lakásbetörésekhez, gépük illetéktelen felhasználásakor az egyik probléma pszichológiai, amely a felhasználó elbizonytalanodásában, internetes félelmeiben nyilvánul meg. Létezik azonban egy súlyosabb következménye is: a feltört, de az internetre még felcsatlakozó gép könnyen ugródeszkává válhat más rendszerek feltöréséhez. Ily módon az ártatlan felhasználó IP-címét, hálózati azonosítóját fogják megtalálni a nyomok után kutatva, ami kellemetlen büntetőjogi hercehurcákkal járhat.

A tűzfalak feladata

A fenti problémák elkerülésére születtek meg a különböző hálózatok – általában a magánhálózat és a nyilvánosság – elválasztására alkalmas informatikai eszközök, a tűzfalak. Alapvető feladatuk, hogy az adatáramlásba iktatva megszűrjék az internetes adatcsomagokat, kizárják a behatolókat, valamint a későbbi behatolást előkészítő vagy pusztán

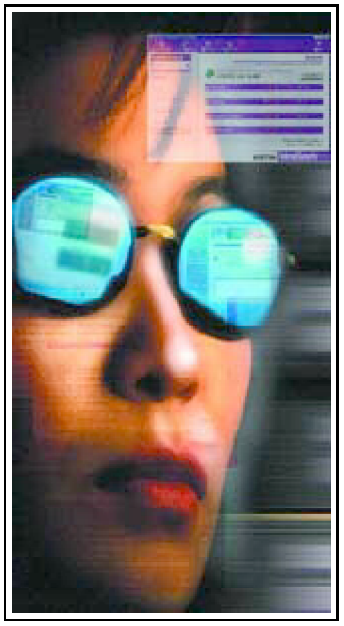
romboló programokat, a trójai falovakat. Gyakorta nehéz elválasztani a tűzfalak funkcióit a többi adatvédelmi célokat szolgáló vagy szintén az internetes adatokat szűrő technológiáktól. Ezért találunk oly sok szoftveres tűzfalmegoldást az antivírus-, illetve tartalomszűrő programokat is fejlesztő cégek kínálatában.

A tűzfalak természetesen más megvalósításban jelennek meg a különböző hálózatokban, és a termékkínálat szintén eltér aszerint, hogy egy nagyvállalat központi szervere(i) köré kell-e védőfalat húznunk vagy a magánfelhasználó gépét szeretnénk megvédeni. Ám mindkét esetben az a cél, hogy az adatok az előre engedélyezett forgalmat követve, előre meghatározott feltételek szerint jussanak át a hálózatok közötti falon. Ennek érdekében a tűzfalak alkalmazhatnak csomag- és alkalmazásszintű szűrést vagy ezek kombinációját.

A különbség az, hogy míg a csomagszűrő eljárás az érkező csomag forrását, portszámát és célját elemzi, addig az alkalmazásszintű szűrés a csomag típusát és a forgalomra használt protokollt is megvizsgálja annak érdekében, hogy valóban csak a megfelelő és a megfelelő alkalmazáskiszolgálást célzó szolgáltatásokhoz tartozó csomagok jussanak át.

Nagyvállalatok védelme

Nagyvállalatoknál mindenekelőtt az igen jelentős üzleti értéket képviselő adatállományt, illetve az ezt tároló gépet kell elkülöníteni, miközben jókora hálózati adatforgalom szűréséről kell gondoskodni. Fizikailag a tűzfal a legritkább esetben kerül a szerverre, inkább külön védelmi egységet célszerű létrehozni. Ily módon a tűzfal sokkalta jobban paraméterezhető a védendő rendszerhez és más funkciók is hozzákapcsolhatók. Például a szerver és a hálózat közötti, nagy mennyiségű adatmozgatás miatt szinte biztosan szükség lesz olyan proxyegységre, amely a terhelések kiegyenlítését, a lekért adatok ideiglenes tárolását és a beérkező kéréseknek megfelelő gyorsított kiszolgálást végzi. Tehát ajánlatosabb inkább a proxy munkájához csatlakoztatni a tűzfalat, mint közvetlenül a szerverhez. A proxy szerepét ellátó eszköz erőforrásait használó megvalósítás általában a szoftveres tűzfalakra jellemző. Az igazi nagyrendszerek tűzfalai a legtöbbször hardveresen is elkülönülő egységek, ezzel a munkájuk függetleníthető a hálózat többi részétől. Így egyfajta célszerszámként építhetjük be azokat a hálózatba, s a proxyk akár saját operációs rendszert, beépített célszoftvert futtathatnak.



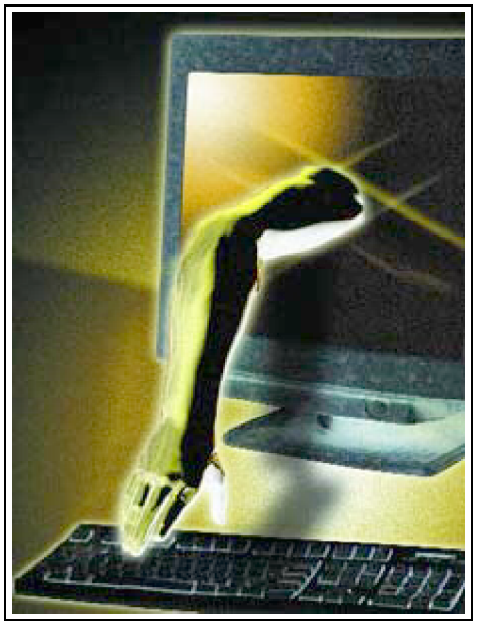
A hálózatba csatlakoztatás helye szintén különböző lehet. Például a Nokia IP440 Router Firewall speciális kapcsolóegységként illeszkedik a hálózatba, és saját, FreeBSD alapú operációs rendszere van. Ezzel gondoskodik más szoftveres tűzfalak, például a Check Point FireWall-1 kiegészítő telepítéséről is. Ezek az eszközök rendszerint a hálózati berendezésekkel, nagy rendszerek telepítésével, rendszerbiztonsággal foglalkozó cégek kínálati listájában szerepelnek (ilyen a Cisco Secure PIX Firewall, a Check Point VPN-1 Appliance 330 vagy az eSoft Interceptor).

A biztonság ára

A fizikailag és logikailag elkülönített tűzfalak hátránya a beszerzéskor, rendszerkiépítéskor jelentkező magasabb költség. Emiatt számtalanszor döntenek más, olcsóbb megoldások mellett, melyek hiányosságai rendszerint csak később, az első komolyabb adatvesztés nyomán válnak nyilvánvalóvá. Előnyük ugyanakkor, hogy külön egységként akár egyedi megoldásokat, csak a mi rendszerünkre jellemző kiépítéseket valósíthatunk meg. Még a gyári rendszerek különböző kombinációja és velük egy többlépcsős védelem kialakítása is olyan egyediséget kölcsönözhet rendszereink határain, amely igencsak megnehezíti a behatolók dolgát. A különböző tűzfalmegoldások egymásra, illetve egymás mögé telepítésével ugyanis kiküszöbölhetjük az egyes rendszerek hiányosságait. Ez egyben a tűzfaltelepítés egyik, egyetemesnek tekinthető szabálya is lehetne: soha ne elégedjünk meg egyetlen tűzfallal, mert annak mindig lehet olyan, akár publikus típushibája, amelyet kihasználva feltörhetik stabilnak hitt hálózatunkat. A nagy rendszerek, illetve a több tűzfal telepítésével járó többletköltséget mindig kalkuláljuk bele a kivitelezés árába, mert a későbbiekben bizony sokszorosan megfizethetünk takarékosságunk miatt. A különböző biztonsági rendszerek összeházasításával a kifelé látszó egyediség mellett a rendszer testre szabása, a nekünk legmegfelelőbb szűrési megoldások beépítése, a szabályrendszerek rugalmasabb kialakítása is egyszerűbb.

Megoldások kis cégeknek

Minél kisebb cégről van szó, annál kevésbé nyílik lehetőség az említettek teljes körű megvalósítására, ugyanakkor a védendő adatok értéke és fenyegetettsége is kisebb. Természetesen nem a támadások száma csökken, hanem a feltörés célja változik meg. Az üzleti adatszerzésre vagy a rendszer puszta működésképtelenné tételére irányuló kísérletek nagyobb anyagi és időáldozatot érnek meg egy nemzetközi banki rendszernél, mint egy helyi kisüzem néhány számítógépes törpehálózatánál. Ugyanakkor az utóbbinál egyre inkább egybe kell építenünk olyan funkciókat, amelyeket nagyobb rendszernél egy dedikált gépre bízunk. Sokszor előfordul, hogy hálózatos operá-ciós rendszerhez integrált tűzfalmegoldást használunk a rendszer internetes kijáratát is garantáló szerveren. Ez természetesen nem feltétlenül azonos a rendszer adatait is tároló szerverrel, bár a hálózat méretében lefelé haladva mind gyakoribb. A kisebb hálózatokban tehát felhasználhatjuk azokat a megoldásokat, amelyek egy nagy rendszer részhálózatainál már beváltak, és egy „dobozos” rendszerrel is integrálhatók. A többnyire szoftveres megoldások szép számmal beszerezhetők a piacon. Köztük találhatók az operációs rendszert is fejlesztők termékei, mint például a Novell BorderManagere, vagy kifejezetten biztonsági szoftverek, amelyekkel megfejelhető egy más forrásból származó operációs rendszer. Az egyéb biztonsági szoftvereket kínáló cégek közül megemlíthetjük a McAfee, a Computer Associates vagy a Symantec termékeit. Ugyanakkor a kisebb hálózatokat üzemeltető cégeknek szánt eszközök között is vannak hardverrel integrált megoldások, amilyen a D-Link DI-701 Residential Gateway, a Linksys Etherfast Cable/DSL Router vagy a NetGear RT311 Gateway Router.



Néhány alternatíva

Természetesen a kis- és középvállalatok hálózataiban szintén szerepet kaphatnak a „házilagos” megoldások. Például úgy, hogy a hálózatos kapcsolatokat olyan gépre bízzuk, amelyet körültekintően „felszerelünk” a külső behatolások megfogására vagy legalább felderítésére. Erre tulajdonképpen a Novell említett BorderManagere is alkalmas, amennyiben NICS (Novell Internet Caching System) alkalmazással használjuk. Ez utóbbi, a NetWare 5.x alapú internetes gyorsítótár-architektúra több hardvergyártótól (Compaq, Dell, IBM) beszerezhető.

Szinte kínálja a lehetőséget ilyen hálózati egység kialakítására a Linux. A jelenleg kapható, illetve összeállítható disztribúciók kivétel nélkül a 2.2.x–es kernelre épülnek, amelyek megengedik a proxy-, illetve tűzfalfunkciók megteremtését. Így a kernel megfelelő fordítási opcióinak beállításával és akár egy szerényebb tudású hardverrel felépíthetjük a hálózatunk határát jelentő gépet, ami befelé már csak a kellően felügyelt forgalmat engedi át. Az IP-chain (Linux IP Firewalling Chains) alapú linuxos tűzfallehetőség kétségtelenül költségkímélő megoldás.

Védtelen kisfelhasználók?

Leginkább a magánfelhasználókra jellemző a költségérzékenység és – tisztelet a kivételnek – a felületesebb hálózathasználat. Rengetegen gondolják úgy, hogy az ő gépükön nincs olyan adat, amelyet érdemes volna megszerezni, tehát nincs igazán miért félniük. Minél védtelenebb a rendszer, annál könnyebb feltörni, és a magánfelhasználók gépei bizony meglehetősen védtelenek. Persze van, aki a rombolás előre megfontolt szándéka nélkül nyúl bele egy ilyen gépbe, majd a hozzá nem értésével okoz komoly felfordulást.

Az interneten például találhatók olyan eszközök, amelyek eredetileg egy hálózat gyenge pontjainak felderítésére készültek, de alkalmasak károkozásra is. Bár ezek a behatolások is igen bosszantóak, mivel személyes adatok juthatnak idegenek birtokába vagy mehetnek tönkre a merevlemezen, az illetéktelen betörés lényegesen kellemetlenebb következményekkel járhat akkor, ha a tulajdonos gépét „zombivá” alakítják. Az ugródeszkává lett számítógép(ek)ről azután a támadók nagyobb rendszereket küldhetnek padlóra

a felhasználó(k) tudomása nélkül. Az ilyen támadások visszakövetésekor a többnyire mit sem sejtő egyén a végállomás. A gyanú tisztázását pedig rendszerint nehezíti, hogy a munkaállomásokra telepített tűzfalak feljegyzik a behatolási szándékot, behatárolják a behatolási kísérlet forrását.

Ötletbörze

Amennyiben a felhasználó gépén Linux fut, élhetünk a korábban taglalt kerneles megoldással. Ennek alapja az „ami nincs kifejezetten engedélyezve, az tiltva van” filozófia. Az IP-chain közvetlen konfigurálása ugyan nem könnyű feladat a járatlanabb felhasználóknak, azonban a Linuxhoz számos, ezt segítő kézi készülék (például a KDE alapcsomagjában megtalálható Kfirewall) áll ingyen a rendelkezésre. Kész szkriptek is letölthetők térítésmentesen az említett kernelmegoldás konfigurálásához, amelyek kezelőfelületükkel megkönnyítik a feladat elvégzését. Ezek közül kifejezetten kezdő linuxosoknak szánták a Guarddogot (Simon Edwards). Természetesen a Linuxhoz is rendelkezésünkre állnak a fizetős termékek, például a LinuxWall (Frank Bernard Informationstechnik GmbH). Általában ez utóbbiak alkalmasak az egyedi szabályrendszerek kényelmes létrehozására, de a Linuxon ezt ki-ki maga is megteheti, lényegesen több tanulás és munka árán.

Alkalmazkodva a magánfelhasználók asztalán található rendszerek sokféleségéhez, a nekik készült tűzfalakból áll rendelkezésre a legnagyobb választék – árban és elérhetőségben egyaránt. Nem véletlenül, hiszen a legelterjedtebb operációs rendszer, a Windows (95, 98 és Me) – a Linuxszal ellentétben – alapbeállításában a „minden meg van engedve” elvét juttatja érvényre, továbbá nem tudunk magunknak új kernelt és/vagy hálózati csatlakozóegységet (Kernel32.dll, Winsock.dll) sem fordítani. Emiatt a határvédelmi programoknak kell megoldaniuk minden kapcsolatszűrési feladatot.

A beszerezhető szoftverek jelentősen eltérnek egymástól terjesztési koncep-ciójukban és funkcionalitásukban egyaránt. Az alkalmazások között megtalálhatók a SOHO-nak szánt programok kistestvérei, mint az ingyenesen letölthető eSafe Desktop és a kifejezetten erre a platformra készült programok. Találunk komplex URL- és protokollszűrést kínáló alkalmazást (ilyen a Norton Internet Security 2001-ben „reinkarnálódott” shareware AtGuard), az alkalmazó programok szerinti beállítású, ingyenes forgalomfelügyelőt (ZoneAlarm) vagy az interneten megvehető, komplex forgalom-, IP- és behatolásfigyelőt (BlackICE Agent).

A windowsos felhasználói tűzfalak közös jellemzője – kevés kivételtől eltekintve –, hogy meglévő, sokszor gyárilag beépített szabályrendszerrel dolgoznak. Ennek előnye, hogy kevés felhasználói ismerettel elérhető a leggyakoribb támadási módok kiszűrése, a támadási kísérletek loggolása, az internetes forgalom figyelése.

Szintén kecsegtető a programok kedvező ára, esetleg ingyenes hozzáférhetősége, ami nem feltétlenül jelent nagy korlátozást a Windowson elérhető funkcionalitásban. Kétségtelen hátrány viszont, és ez nem csak a Windowsra igaz, hogy egy gépen kell megoldanunk alkalmazásaink futtatását, a hálózatos kapcsolatot, valamint annak ellenőrzését. Ez pedig próbára teszi gépünk erőforrásait: a biztonságért bizony memóriából és processzoridőből egyaránt áldoznunk kell. Mi több, érdemes lehet viszonylag csekély beruházással pluszgépet és némi extra szakismeretet beszerezni. Egy olcsóbb számítógéppel kihasználhatjuk a külön linuxos kapcsolati gép előnyeit, amelyhez akár egy mini Linux disztribúciót is ingyenesen letölthetünk.

Simay Endre István az Infopen munkatársa.

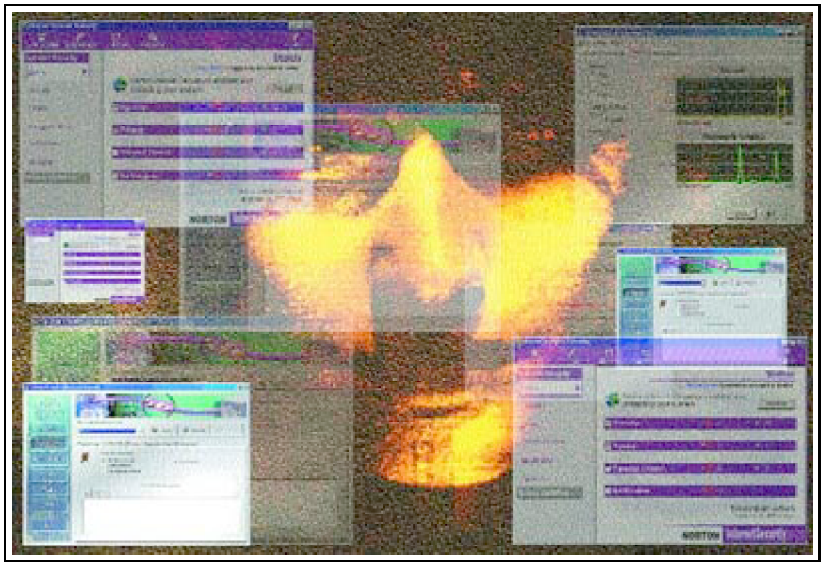
E-mail: **endre_s@infopen.hu.**

2001. FEBRUÁR / FÓKUSZ Adatvédelem / OSI rétegek

OSI rétegek

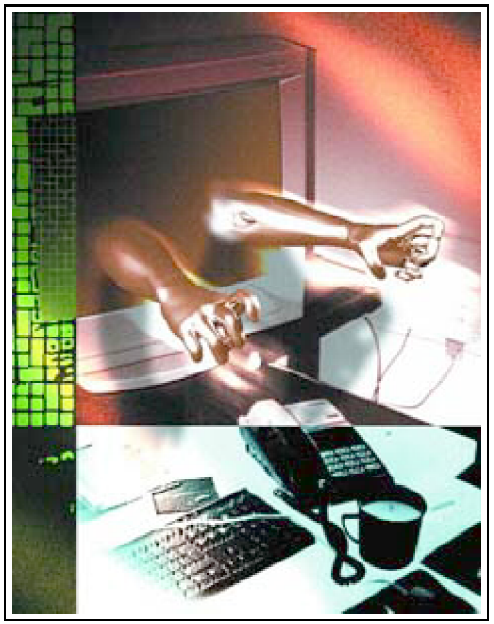
Táblázatunkban összevontan kezeltük a vállalati rendszerekben felhasználható hardveres és szoftveres alkalmazásokat. Ezek közös jellemzője, hogy ellátják a tűzfalak „kötelező” (routerekre, például Linksys), a tűzfalegységekre (például a Cisco Pix termékcsaládjára) és más, appliance jellegű készülékekre (például a Novell ICS-sel és BorderManagerrel telepí

Csakhogy a hardveres tűzfal-, illetve VPN-megoldások sem az OSI (Open System Interconnection) modell szerinti hardverszinten üzemelnek (lásd a Novelltől származó kis rendszerrel kerülnek forgalomba. Ám a nagy rendszerekbe integrált egységek is a rendszergazda munkahelyéről felügyelhetők, ahogy a szűrési feltételeket tartalmazó adatállományok



A Novell programok már jelzik azt a tendenciát, hogy különböző funkciókat integráljanak egy rendszerbe. A vállalatoknak ajánlható tűzfalszoftverek között is találunk több olyan de ilyen a CA eTrust vagy a HP Praesidium programjai között található CA eTrust Firewall és a HP Praesidium Firewall is. További példa a Norton System Worksbe integrálódó N

Mint a táblázatból látható, az OSI modell mind a hét rétegére van megfelelő tűzfal-technológia. A magasabb rétegekben jobban vagy finomabban ellenőrizhetők a hálózatba nagyobb teljesítményért viszont a kisebb biztonság az ár.



OSI réteg	Tűzfal-technológia
Alkalmazás	Virtuális magánhálózat (VPN)
Internetes objektumtárolás	
(Object Caching)	
Prezentáció	VPN
Esemény	VPN
Átvitel	VPN
IPX/IP és IP/IP átjárók	
Csomagszűrés	
Hálózat	VPN
Hálózati címfordítás	
(Network Address Translation, NAT)	
Csomagszűrés	

OSI réteg	Tűzfal-technológia
Adatkapcsolat	VPN
Pont-pont protokoll (PPP)	
Csomagszűrés	
Fizikai	Nem alkalmazható

Ismertebb tűzfalak osztályozása

Gyártó	Vállalati és szervermegoldások	Munkaállomásra, illetve otthonra szóló megoldások
Aladdin Knowledge Systems Ltd. www.esafe.com	eSafe Enterprise	eSafe Desktop
Central Command, Inc. www.centralcommand.com, www.avp.com	AVX Enterprise Management Console	AVX Professional
Check Point Software Technologies Ltd. www.checkpoint.com/products/vpn1/index.html	Check Point VPN-1	
Cisco Systems, Inc. www.cisco.com/univercd/cc/td/doc/	Cisco Secure PIX Firewall series Cisco IOS Firewall Cisco Centri Firewall	
Computer Associates International, Inc. www.cai.com/solutions/enterprise/etrust/	CA eTrust Firewall CA Virtual Private Network	
D-Link Systems, Inc. www.dlink.com/products/broadband/di701/	D-Link DI-701 Residential Gateway	
eSoft, Inc. www.esoft.com/products/	eSoft Interceptor eSoft InstaGate EX	

Gyártó	Vállalati és szervermegoldások	Munkaállomásra, illetve otthonra szóló megoldások
IBM www.ibm.com/software/security/firewall/	IBM SecureWay Firewall	
Internet Security Systems, Inc. ww.iss.net/securing_e-business/security_products/intrusion_detection/index.php	ISS RealSecure	
Hewlett-Packard www.hp.com/security/products/firewall/	HP Praesidium e-Firewall	
Linksys www.linksys.com/	Linksys Etherfast Cable/DSL Router	
McAfee.com Corporation/ Network Associate, Inc. http://software.mcafee.com/products		Internet Guard Dog Pro McAfee.com Personal Firewalls
NetGear, Inc. www.netgear.com/	NetGear RT311 Gateway Router	
NetGuard, Inc. www.netguard.com	Guardian Firewall-5 GuardianPro GuardianPro eNT	
Network ICE Corporation www.networkice.com/products	ICEpac Security Suite	BlackICE Defender
Nokia Corporation www.nokia.com/vpn/firewall_vpn.html	Nokia Firewall/VPN Appliance	
Novell, Inc. www.novell.com/products/	Novell BorderManager Firewall Services Novell FireWALL for NT	

Gyártó	Vállalati és szervermegoldások	Munkaállomásra, illetve otthonra szóló megoldások
Open Door Networks, Inc. www.opendoor.com	DoorStop Server Edition	DoorStop Personal Edition
PGP Security/ Network Associates, Inc. www.pgp.com/products/	PGP e-ppliances Gauntlet Firewall Gauntlet VPN	
Progressive Systems, Inc. www.progressive-systems.com/	Phoenix Adaptive Firewall	
Sonicwall, Inc. www.sonicwall.com	SonicWALL PRO-VX Internet Security Appliance SonicWALL SOHO	
Symantec Corporation www.symantec.com	AXENT Raptor Firewall Intruder Alert	Norton Internet Security 2001 Norton Personal Firewall 2001 Symantec Desktop Firewall 2.0
Watchguard Technologies, Inc. www.watchguard.com/products/	Watchguard LiveSecurity System Watchguard SOHO	
Zone Labs, Inc. www.zonelabs.com		ZoneAlarm Pro ZoneAlarm

Hackervilág Magyarországon

Az 1999-es év orwellinek bizonyult a magyar web történetében. Ebben az évben léptek színre azok a hackerek, akik bizonyították: a magyar rendszerek is feltörhetők, sőt érdemes is feltörni azokat. Az első áldozatok közé tartoztak a Budapesti Rendőr-főkapitányság és a Microsoft Magyarország oldalai.

A 2000. év fejleménye volt az egyik legnagyobb visszhangot keltő betörés: egy magát Phantomnak nevező behatoló (mint kiderült, behatolócsoport) feltörte az Elender internetszolgáltató oldalait, és közszemlére tette a felhasználói név–jelszó párosokat. A rendőrség, illetve néhány szakértő munkájának eredményeképpen a hackereket elcsípték ugyan, ám jogerős ítélet máig nem született. Megfelelő biztonsági intézkedések hiányában a rendszert rövidesen ismét feltörték.

A PentaGuard csoport nevében fellépő Diablo nevű hackerhez fűződik a Külügyminisztérium honlapjának feltörése, majd a Pénzügyminisztérium hivatalos oldalának meglékelése. Az itt közzétett bíráló versike ellenére máig nem sikerült tisztázni az elkövetők személyét: a hivatalos közlemények eleinte magyar, majd román tettesekről szóltak.

A múlt év egyik érdekessége volt Érd város honlapjának feltörése. Viszonylag kevés munkával egy alapbeállítású Linux rendszert cseréltek le ismeretlen tettesek, az új honlapon szintén politikai tartalmú üzenetet hagyva maguk után.

A közelmúltban egy ismeretlen támadó újból az Elendert vette célba. Az Alarmixot törte fel: a megváltoztatott oldal a felhasználói nevekkel és jelszavakkal alig tíz percig volt közszemlén a világhálón.

2000 legvégén forgatták fel a tv2-nél futó *csiszár.hu*-oldalakat, mondván: a műsorvezető megbántotta a hackertársadalmat. Az ebből kibontakozó nyilvános vita egyik érve: a sajtó és a kereskedelmi televíziók rendszerint bűnügyi szenzációként, környezetükből kiragadva tálalják a hasonló eseteket. A tanulság pedig: a többé-kevésbé laikus közvélemény szerint a világháló a bűnök melegágya, ezért szabályozni, cenzúrázni kell.

A leghosszabb lajstrommal egy Obotak nevű behatoló dicsekedhet. Különös ismertetőjegye, hogy a Microsoft rendszerekkel működő hostokra vadászik. Tavalyi trófeái közé tartozik a Bsa.cz, a BRFK, a Számalk, a Spiderweb, az Infotéka és Siófok város honlapja. Idén eddig a Morphologic.hu, az IqSoft.hu, a PublicPress.hu, a Selectrade.hu és az Egyesült Államok agrármarketing-központjának honlapjai *(www.ams.usda.gov)* estek áldozatául. Obotak végül az amerikai honlapon elhelyezett üzenetben tájékoztatta a világot tényked ése okáról: Magyarországon a hackereket bűnözőknek tekintik, míg az Egyesült Államokban nagy képzettségű szakembereknek számítanak.

Kis János

2001. FEBRUÁR / FÓKUSZ Elektronikus aláírás

FÓKUSZ
Elektronikus aláírás

2001. FEBRUÁR / FÓKUSZ Elektronikus aláírás / Törvényre várva

Törvényre várva

Az e-gazdaság biztonságának egyik kulcsa az elektronikus aláírás. Az ennek használatáról szóló törvény kormányzati egyeztetés alatt áll.

Szerző: Bartal Iván

Az Országgyűlés tavaszi ülésszakán várható az 1075/ 2000. (IX. 13.) kormányhatározat előírása alapján készült törvénytervezet parlamenti vitája. A törvény elfogadása, valamint a végrehajtásához és a gyakorlati alkalmazásához szükséges további jogszabályok megalkotása felbecsülhetetlen jelentőségű mind az elektronikus kommunikáció, mind az e-kereskedelem és az internet használatának szempontjából.

Amennyiben a törvény célja megvalósul, az aszimmetrikus kulcspárokon alapuló titkosítási módszerekkel előállított üzenetek és aláírások kizárólagos személyünkhöz kapcsolódását és az elektronikus úton továbbított vagy tárolt dokumentumok jogi hatályát, bizonyító erejét a magyar jogszabályok meghatározott feltételek esetén a papír alapú iratok bizonyító erejével azonosnak ismerik majd el.

Uniós irányelvek

Az elektronikus aláírással kapcsolatos magyar jogalkotási tervek az Európai Unió szabályozásán alapulnak, összhangban Magyarországnak az úgynevezett európai megállapodásról szóló törvényben tett kötelezettségvállalásával, amely szerint jogszabályait az unió jogszabályaihoz és szabályrendszeréhez közelíti.

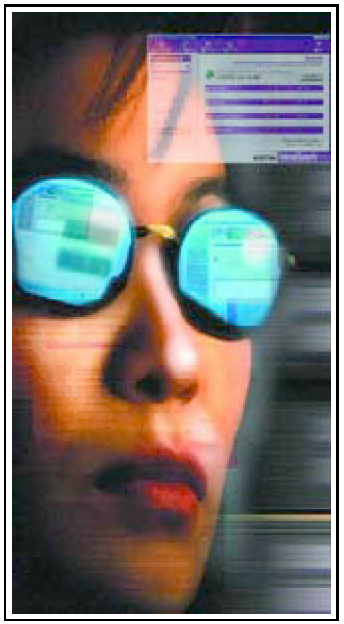
A tervezett magyar szabályozás az Európai Unió Parlamentje és Tanácsa által elfogadott két irányelven – az 1999/93/EK irányelv az elektronikus aláírásról (a továbbiakban: irányelv) és a 2000/31/EK irányelv az elektronikus kereskedelemről – alapszik majd. Az irányelv egyébként csak céljának megvalósítását tekintve kötelező az egyes tagállamokra, a megvalósítás eszközeit és módját a tagok maguk választhatják meg.

Aláírásfajták

Az elektronikus és a digitális aláírás fogalma között nem csupán jogi, hanem gyakorlati különbség van. Az előbbi az elektronikus dokumentum megjelölését, aláírását jelenti (e-mail üzenet végén „aláírt” nevet), míg az utóbbi ennek meghatározott technikával történő elvégzését. Ahhoz, hogy a jog bármilyen elektronikus aláírást hitelesnek tekintsen, olyan biztonságos technikát kell használni, amelynél az aláíró személye, az aláírás helye és ideje (időbélyegző), az irat sértetlensége bizonyítható és az aláírás megtörténte nem letagadható.

Jelenleg a legelterjedtebb módszer az aszimmetrikus (és nyilvános) kulcsú titkosítás. Ennél a küldő az üzenetet saját titkos kulcsával kódolja, míg a fogadó a küldő nyilvános kulcsával dekódolja, vagyis megfejti az üzenetet (lásd *Titkos lépések,* BYTE Magyarország, 2000. november). Fontos, hogy egy üzenetet csak ugyanazon kulcspár kulcsaival lehet titkosítani és megfejteni. A nyilvános kulcs bárki által hozzáférhető, míg a titkos kulcsot a felhasználónak titokban kell tartania. A nyilvános kulcsot a hitelesítésszolgáltatók hitelesítik (Magyarországon például az európai hiteleshelyként működő NetLock Kft.) és erről tanúsítványt adnak ki.

A jogi szabályozás lényege az elektronikus dokumentumok és aláírások jogi hatályának elismerésén túl olyan szabályrendszer kialakítása, amely megnyugtatóan rendezi az elektronikus aláírás egyes fajtáival („egyszerű” és minősített) és felhasználásukkal, az aláírással kapcsolatos szolgáltatások (hitelesítés és időbélyegzés) nyújtásával és igénybevételével, valamint az elektronikus aláírással összefüggő hatósági (felügyeleti, ellenőrző, minősítési) feladatokkal kapcsolatos kérdéseket.



Valószínűleg a magyarországi törvény is alapelvként mondja majd ki, hogy az elektronikus aláírás vagy dokumentum bizonyítási eszközként elfogadását megtagadni nem lehet pusztán amiatt, hogy azok csak elektronikus formában léteznek. Ugyanakkor egyes területeken (válóper, örökbefogadás, öröklés) nem lehet kizárólag elektronikus aláírást, illetve iratokat használni. A magasabb szintű feltételeknek megfelelő (fokozott biztonságú) elektronikus aláírás azonban jogszerűen válthatja fel a papíron történő írásba foglalást, így az ügyvédi törvény esetleges módosításával lehetővé válhat az elektronikus ügyvédi ellenjegyzés is.

A törvény a digitális aláírás kifejezés helyett feltehetően többféle elektronikus aláírást különböztet meg, amelyek között elsősorban az előállításhoz használt eszközök, a tanúsítás és az aláíráshoz fűződő joghatások szempontjából van különbség. Az „egyszerű” elektronikus aláírás a speciális technikai védelem nélkül készült aláírást jelöli majd (szkennelt aláírás beillesztése fax végére). A fokozott biztonságú elektronikus aláírás már alkalmas lesz az aláíró azonosítására is, hiszen olyan (megfelelő hardver- vagy szoftver-) eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll (titkos kulcs), és olyan módon kapcsolódik a dokumentum tartalmához, hogy az aláírást (kódolást) követően az üzeneten végrehajtott módosítás érzékelhető.

A legmagasabb szintű elektronikus aláírás a minősített elektronikus aláírás lesz. Ez olyan fokozott biztonságú aláírás, amely megfelel a jogszabályban előírt technológiai és a tanúsítványt kibocsátó hitelesítésszolgáltatóval szemben támasztott szakmai és megbízhatósági (például felelősségbiztosítás) követelményeknek.

A törvény várhatóan annál erősebb bizonyító erőt fűz majd az elektronikusan aláírt dokumentumhoz, minél magasabb az aláírás előállításának technológiai biztonsága. A fokozott biztonságú elektronikus aláírással ellátott iratok feltehetően megfelelnek a tényleges írásba foglalás követelményeinek, míg a minősített elektronikus aláírású dokumentumok (vagyis amelyeknél az aláírás a hatóságilag engedélyezett eszközökkel történik, és amely esetekben a tanúsítvány az aláíró és a tanúsítvány meghatározott hiteles adatait, például nyilvános kulcsát, nevét, a tanúsítvány értékbeli, idő- és térbeli korlátozását is tartalmazza) a polgári perrendtartásról szóló 1952. évi III. törvény értelmében teljes bizonyító erejű magánokiratoknak minősülhetnek. Nemcsak a polgári, hanem az államigazgatási és a büntetőeljárásban, valamint a cégeljárásban is elképzelhető az

elektronikus aláírás használata.

Szolgáltatások

Feltehetően a magyar törvény is különbséget tesz a hitelesítésszolgáltatás (személyes, névjegykártya típusú, szervezeti vagy szervertanúsítvány), az időbélyegző szolgáltatás (olyan elektronikus aláírás, amely tartalmazza a „lebélyegzés” időpontját és ezáltal az azt követő változások érzékelését), illetőleg az elektronikus aláírási folyamat szolgáltatása között.

Az elektronikus aláírás biztonságát és az aláíró személyazonosságát, valamint szükség szerint további adatait a hitelesítésszolgáltató (certification service provider, CSP) tanúsítja. A tanúsítványok kiállítását meghatározott adatok hiteles igazolása előzi meg. Ezen adatok mennyisége, illetve a bizonyítékként elfogadott dokumentumok minősége a szolgáltató által kiadott, merevlemezre menthető, böngészőbe illeszthető tanúsítványok biztonsági szintjével (és nyilván áraival) együtt változik.

Például lehet, hogy a legalacsonyabb szintű tanúsítvány kibocsátását megelőzően a felhasználónak fizikailag nem is kell megjelennie a szolgáltatónál, elég, ha egy e-mail címmel rendelkezik. Az így kiadott tanúsítvány viszont csak azt fogja tanúsítani, hogy a megjelölt személynek tényleg ez az elektronikus levélcíme. A legmagasabb szintű tanúsítványnál viszont a szolgáltató valószínűleg aláírási címpéldányt, személyit, útlevelet, cégkivonatot vagy egyéb hiteles dokumentumot fog kérni és a személyes megjelenést is előírja. Az irányelvben (és valószínűleg a magyarországi törvényben alkalmazott megoldás szerint is) a hitelesítésszolgáltató jogosult korlátozni az általa kiadott tanúsítvány felhasználását időben, térben, sőt előírhatja, hogy a tanúsítvány kizárólag meghatározott értékű ügyletekben használható fel.

A tanúsítványokat a szolgáltató meghatározott esetekben felfüggesztheti és visszavonhatja. A visszavont tanúsítványokról a szolgáltatók úgynevezett revocation- (visszavonási) listákat vezetnek.

Felügyelet

A kormányhatározat alapján a szolgáltatóknak nem kell hatósági engedélyt beszerezniük az elektronikus aláírással kapcsolatos szolgáltatások nyújtásához. Nyilvánvaló azonban, hogy engedélykérési kötelezettség hiányában mindenképpen szükség van valamilyen állami kontroll gyakorlására. Ezt a feladatot hivatott ellátni a bejelentési kötelezettséggel létrejövő nyilvántartás és az úgynevezett minősítés rendszere.

A jelenlegi álláspont szerint a fokozott biztonságú elektronikus aláírással kapcsolatos hitelesítésszolgáltatási tevékenység megkezdését be kell jelenteni a Hírközlési Főfelügyeletnek (a HÍF-nek), míg a minősített elektronikus aláírással kapcsolatos hitelesítésszolgáltatási tevékenységet csak a HÍF által kiadott minősítéssel rendelkező szervezet folytathat majd. E két aláírásfajtánál csak a HÍF által jóváhagyott eszközök lesznek használhatók, ugyanúgy, mint az internet beszédcélú felhasználása (VoIP) vagy az internetszolgáltatás során.

Feltehetően a HÍF a szolgáltatók nyilvántartásba vételén és minősítésén kívül a szolgáltatók tevékenységét és annak jogszerűségét is ellenőrizni fogja, és hatósági jogkörben eljárva intézkedési, valamint bírságolási joga is lesz – bár elképzelhető, hogy a lapzártánkkor még készülő törvény végül más megoldásokat alkalmaz.

Felelősség

A szolgáltatók felelősségét a törvény a polgári törvénykönyv általános kártérítési szabályai alapján rendezi, vagyis amennyiben a szolgáltató jogellenes magatartásával kárt okozna, köteles lesz azt megtéríteni, kivéve ha bizonyítja, hogy úgy járt el, ahogy az az adott helyzetben elvárható volt. Fontos szabály, hogy kétség esetén valószínűleg a szolgáltatót terheli a bizonyítás kötelezettsége.

A kormányhatározat szerint a külföldi szolgáltatók tanúsítványa a magyarországival azonos hatályú lesz, ha nemzetközi szerződés úgy rendelkezik vagy amennyiben azt egy magyarországi szolgáltató felülhitelesíti. A felülhitelesítést be kell jelenteni a felügyeleti szervnek. Az okozott kárért ilyenkor a külföldi és a magyarországi hitelesítésszolgáltató egyetemlegesen felel.

Az elektronikus aláírás széles körű alkalmazásához természetesen nem elegendő a törvénytervezet elfogadása. Ám az elektronikus aláírás jogi hatályának elismerése gyökeres változásokat hozhat a biztonságos internetes vásárlástól a business-to-business piactereken át az egyes nagyvállalatok belső kommunikációjának biztonságos működéséig az élet számos területén. Ahhoz azonban, hogy az elektronikusan aláírt dokumentumokat a bírósági és az államigazgatási eljárásokban ténylegesen használni tudjuk, alighanem többet kell várnunk, mint az elektronikus aláírásról szóló törvénytervezet hatálybalépéséig hátralévő fél-háromnegyed év.

Bartal Iván az Oppenheim és Társai, Freshfields Bruckhaus Deringer Ügyvédi Iroda ***(www.freshfields.com)*** *munkatársa.*

E-mail: **ivan.bartal@freshfieldsbruckhaus.com.**

HOL TALÁLHATÓ?

NetLock Kft.

www.netlock.net

Hírközlési Főfelügyelet

www.hif.hu

FÓKUSZ
Adatbiztonság

A vállalati hálózatok biztonsági őrei

A biztonságos internetelérés szintjeihez tartozó termékek kombinációja hatékony védelemmel vértezheti föl a vállalatokat.

Szerző: Éberling Tamás

Az internet korában már egyetlen vállalat sem nélkülözheti a zökkenőmentes elektronikus adatfeldolgozás infrastruktúráját. A világhálóra csatlakozás azonban nem csupán az üzletmenet jelentős gyorsítását, hanem ugyanakkora kockázatot is hordoz magában: egy információs rendszer az internet biztonsági problémáiból adódó részleges vagy teljes kiesése olyan anyagi kárt okozhat, ami messze meghaladja a háló eléréséből származó esetleges hasznot. Éppen ezért az a cég, amelyik megfelelő biztonsági rendszer mellőzésével csatlakoztatja hálózatát az internetre, hatalmas kockázatot vállal.

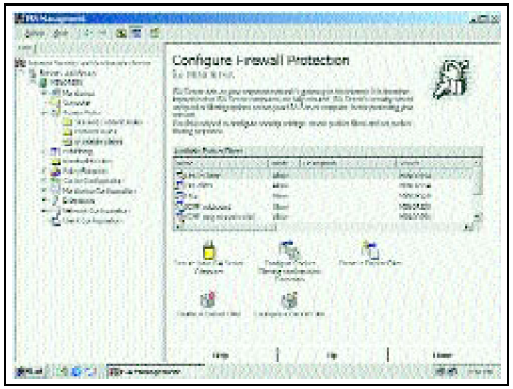
A biztonságos csatlakozásnak többféle módja és szintje van, melyeket az adott vállalat hatékony üzletmenetéhez szükséges informatikai infrastruktúra és a kockázatelemzés kérdései határoznak meg.

Cikkünk a biztonságos internetelérés egy-egy szintjének új termékeit mutatja be, amelyek kombinációja hatékony védelemmel vértezheti fel a vállalatokat. Az egyik termék a Microsoft egységes .NET stratégiájának része. A Microsoft Internet Security and Acceleration Server (ISA szerver) az internetcsatlakozás biztonsági szintjének alapját képező tűzfal és proxy szerver kombinációja. A másik pedig a Computer Associates eTrust biztonságimegoldás-csomagjának, a biztonság magasabb szintjét képező betörészlelő rendszere, az Intrusion Detection (eTrust ID).

ISA szerver

Az ISA szerver – a Microsoft Proxy Server 2.0 újabb verziója – nemcsak nevében, hanem szolgáltatásaiban és kezelésében is jelentősen megváltozott. Már a 2.0-ás változatnál megfigyelhettük, hogy a Microsoft szakítani próbált a hagyományosnak mondható tűzfal-architektúrával, helyette a dinamikus csomagszűrési és transzparens Winsock proxy kombinálásával igyekezett növelni a Windows hálózatok biztonságát és a teljesítmény fokozását. Ez a szemlélet az új verzióban is érezhető: tovább csiszolták az úttörőnek számító architektúrát. A terheléselosztásra, a hibatűrésre és a méretezhetőségre irányuló erőfeszítések mellett mind nagyobb hangsúlyt fektetnek a tűzfal funkciók biztonságos működésére. Ezt látszik alátámasztani az a tény is, hogy tervezik a termék ICSA bevizsgálását.

Az ISA szerver telepítése a Windows 2000 szerver biztonságos konfigurálásával kezdődik. A szoftveres tűzfalak és a proxy szerverek csak akkor lehetnek a hálózatok hatékony átjárói, ha az alattuk futó operációs rendszer – legyen az Unix, Linux vagy Windows – konfiguráltsága eleget tesz a mindenkori maximális biztonsági követelményeknek. Gondoljuk csak el, mennyire hatékony az a tűzfal, amelyik öt-hat betűs, szólista alapján választott rendszergazdai jelszóval rendelkezik! Tehát állítsuk be Windows 2000 rendszerünket úgy, hogy alkalmas legyen a „védőbástya” feladat ellátására! Első teendőnk a rendszergazda felhasználó átnevezése legyen és erős, legalább tíz karakter hosszúságú, speciális karaktereket is tartalmazó jelszó hozzárendelése.



Az ISA szerver kezelőfelülete

Ezután tiltsunk le minden olyan szolgáltatást, ami nem szükséges rendszerünk működéséhez. Ilyenek például az alapbeállításból elinduló – Computer Browser, Distributed File System (DFS), Distributed Link Tracking, Fax Service, License Logging, Telephony – szervizek. A hálózati csatolók konfigurálásának legjobb módja, ha az internet felőli kártyán a TCP/IP protokollon kívül nem engedélyezünk más szolgáltatást (Microsoft kliens-, fájl- és nyomtatómegosztás, NetBios stb.). Mivel az alapértelmezett ISA szerver letiltja telepítésekor a két csatoló között az IP Forwardingot, a belső hálózathoz csatlakozó kártyához a hatékony menedzsment miatt akár SNMP protokollt és Terminal Services

szolgáltatást is rendelhetünk.

Az ISA szerver CD-jének elindítása után kétféle telepítési mód választható: Active Directory integrált vagy standalone. A szerver Active Directory (AD) integrációjával ISA szervertömböket és -láncokat építhetünk fel, amelyek a méretezhetőség, a terheléselosztás és a hibatűrés, valamint a nagyvállalati hierarchikus gyorsítótár kialakításának eszközei. Ha az internethasználatot 60 százalékban gyorsító Web cache funkció bővítést igényel, az új ISA szervert csatlakoztassuk egy, az AD-ban kialakított tömbhöz. A szerver további konfigurálást nem igényel, a korábban kialakított ISA séma fog érvényesülni. Az így szervezett tömbkialakítással két legyet üthetünk egy csapásra: a terheléselosztás mellett a hibatűrés is megoldódik; ha a tömb egyik szervere meghibásodna, a többi zavartalanul megoldja az internetátjárást.

Az ISA szerver háromféle üzemmódban működtethető: tűzfalként, proxyként vagy integrált módban. Ha csak a tűzfal vagy a proxy üzemmódot választjuk, a későbbiekben nincs lehetőség a másik funkció használatára. Ezért érdemes minden esetben az integrált üzemmódra voksolni, mert a szolgáltatások így külön engedélyezhetők vagy tilthatók. Az ISA telepítése során leállítja az esetleg futó WWW service-t és javaslatot tesz az átkonfigurálására vagy megszüntetésére. Ezután a belső hálózati csatoló kiválasztásával felépíti az úgynevezett Local Address Table-t (LAT-ot), ami a transzparens Winsock proxy működéséhez szükséges. Ugyanis a Winsock kliens a munkaállomáson e táblázat alapján dönti el, hogy a kapcsolatot a belső hálózaton belül vagy az ISA szerveren keresztül az internet felé próbálja-e felépíteni.

Az ISA konfigurálása során kiderül, hogy ez az eszköz alkalmas a varázslókkal beállítandó szabályok hatékony létrehozására. Az ISA integrált üzemmódban telepítve háromféle szolgáltatást ad: tűzfalat, proxyt és ütemezett oldalletöltést.

A tűzfal szolgáltatás a többi termékhez hasonlóan csomagszűrést végez a beállítható szabályok alapján. Az ISA tűzfal sajátossága a hagyományos tűzfal funkciókon túl az úgynevezett dinamikus csomagszűrés: a biztonság növelésének érdekében csak a belülről kezdeményezett kérések számára engedélyez kapcsolatot. A TCP portok kizárólag a kapcsolat idejére vannak nyitva, a kommunikáció megszűnte után dinamikusan záródnak. Ez a fajta csomagszűrés a különböző port scanner-behatolások ellen nyújt védelmet. A konfigurálás során, a dinamikus csomagszűrés engedélyezésénél azonban figyelni kell arra, hogy azokat a protokollokat, amelyeket külső gép kezdeményez – tipikusan ilyen az általunk üzemeltetett web- és levelezőszerver elérését célzó HTTP és SMTP protokollok –, a szolgáltatást nyújtó szerverünk felé irányítsuk. Ezt a szerver közzétételi – Web publishing, Server publishing – szabályvarázslókkal tehetjük meg.

A Web publishing szolgáltatás a belső hálózaton üzemelő webszerver képviseletén túl az internet felé fordított gyorstárazást (reverse caching) is végez, tehermentesítve ezzel a belső kérések által amúgy is terhelt webkiszolgálót. A technológia alapja egyébként a proxy szerver fordított működése: az internet felől érkező HTTP kéréseknek az ISA szerver tesz eleget, s csak akkor fordul a belső webszerver felé, ha a kérést saját gyorsítótárából nem tudja teljesíteni.

A tűzfalak és proxy szerverek közti alapvető eltérés a hétrétegű OSI modell különböző szintjén történő működés. A tűzfalak a hálózati rétegen üzemelve csak az IP-csomag fejlécét figyelve döntik el a csomag sorsát, viszont a korlátolt funkcionalitáshoz gyors működés társul. A proxy szerverek viszont az alkalmazási szinten az egész IP-csomag tartalmát vizsgálják, így lehetőség nyílik a tartalomszűrésre és a felhasználói szintű protokollelemzésre – sajnos a sebesség rovására. Látható, hogy külön-külön egyik megoldás sem teljes a vállalat szabályrendszerének és biztonsági szempontjainak érvényesítéséhez. Az ISA szerver azonban egymagában elvégzi mindkét funkciót: a további vizsgálatok szemszögéből érdektelen protokollokat a tűzfal kezeli, a böngészéshez szükséges FTP és HTTP protokollokat pedig a proxy szervizhez juttatja további feldolgozásra. A proxy szerver feladata azonban nemcsak a tartalomszűrésben és a jogosultságok ellenőrzésében merül ki: gyorstárazási funkciójával (cache-eléssel) csökkenti a sávszélesség terheltségét.

Az ISA szerver harmadik szolgáltatása az ütemezett oldalletöltés (Scheduled Content Download), amely a proxy funkciókat teszi hatékonyabbá: a gyakran keresett oldalak előre definiálva az ISA gyorsítótárába kerülnek. Így a vállalati toplistás oldalak felé irányuló forgalom felszabadításával jelentős sávszélesség-csökkentés érhető el.

eTrust ID

Az internetes védőbástyaként szolgálatba állított tűzfalak és proxy szerverek a vállalati hálózatok védelmi vonalának első, külső személy által is jól beazonosítható elemei. Ezek a gépek éppen emiatt válnak az internetes támadások elsődleges célpontjaivá. Képzeljünk csak el egy páncélszekrényt riasztó nélkül! Jól véd, de mégis feltörhető anélkül, hogy értesülnénk róla.

A CA eTrust Intrusion Detection terméke az internet felől érkező betörések egyik „riasztó rendszere”, amely a hálózat számára láthatatlanul telepíthető a bástyaszerepet betöltő hardvereszköz elé vagy mögé. A külső támadások úgy indulnak a bástyagép ellen, hogy nincs tudomásuk a tűzfal előtt megcímezhetetlenül megbújó, betörésészlelő rendszerről. Így az még a károkozás előtt megfelelő lépéseket tehet: riaszt vagy konfigurálja a tűzfalat a betörési minta alapján.

Az eTrust ID-nek frissíthető betörési mintaadatbázisán túl további hasznos funkciói is vannak, például tartalmazza a CA InoculateIT vírusfigyelő rendszerét is. Komplex riportolási szolgáltatásával pedig felhasználói szintre lebontott jelentések készíthetők a forgalmi adatokról. A legapróbb részletekig kiterjeszthető naplózásnak csak a háttértár nagysága szabhat határt. Ha ez is kevés lenne, akár az egész elektronikus levelezés kontrollálható.

Az internet megváltoztatja az emberek és a szervezetek kommunikációját. A különböző méretű szervezetek saját hálózataikat az internetre kötik üzleti sikerük és hatékonyságuk növelése érdekében. A csatlakozás azonban nemcsak előnyöket tartogat, bizonyos veszélyeket is rejt. Az eTrust ID és az ISA szerver a kommunikációs infrastruktúra olyan elemei, amelyek képesek az internetkorszak kihívásaira hatékony és biztonságos válaszokat adni.

Éberling Tamás (MCSE, MCP+I) a Minor Rendszerház Rt. munkatársa.

E-mail: **teberling@minor.hu.**

Kislexikon

Dinamikus csomagszűrés: A csomagszűrés során a TCP portok csak a kapcsolat idejére nyitottak, a kommunikáció befejeztével záródnak.

Transzparens Winsock proxy: Az internet felé Windows socketen keresztül (például ICQ, Telnet vagy FTP kliens) kapcsolatot kezdeményező gazdagép számára a proxy működése láthatatlan.

IP Forwarding: Multihome – több hálózati csatolóval rendelkező – rendszereken a csatolók közötti adatátátvitel (IP-forgalom) engedélyezése.

Web cache: Az internetről letöltött oldalak merevlemezen tárolása. A proxy szerver ebből a gyorsítótárból teljesíti a klienseknek az egyszer már lekért weblapokat.

HOL TALÁLHATÓ?

www.minor.hu

FÓKUSZ
Adatvédelem

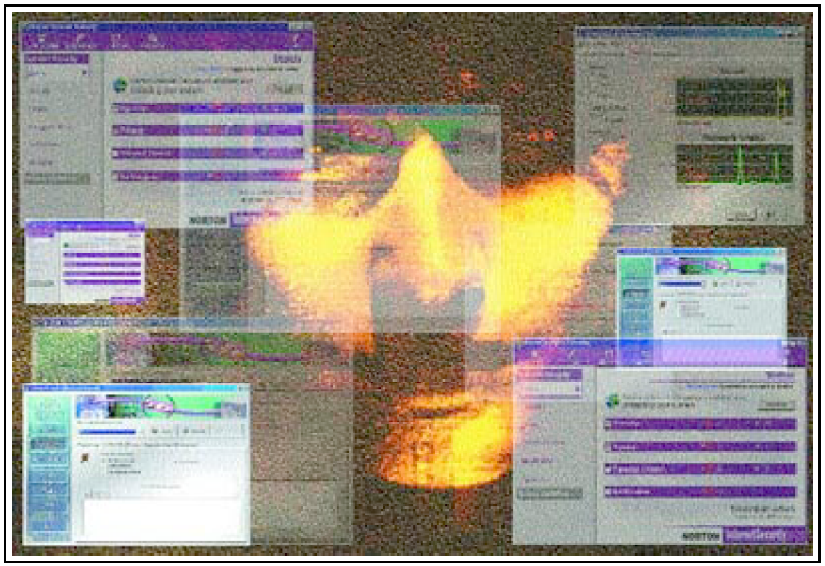
Elvetett kockázat

Élvezzük az informatika térhódításának előnyeit, de ne feledjük: mindennek ára van!

Szerző: Kőrös Zsolt

Az informatikai rendszerek sebezhetőek, és ebből bizony igen sok probléma származhat. Mára eljutottunk arra a pontra, ahol a továbblépés legfontosabb kérdése nem más, mint az ezekben a rendszerekben tárolt, feldolgozott és továbbított adatok megnyugtató szintű védelme.

Az elmúlt években különböző hatékonyságú biztonsági megoldások láttak napvilágot, s mind több cég foglalkozik napjainkban ezek fejlesztésével. Ám valamennyi megoldással van egy közös gond: alkalmazni kell őket! Fontos, hogy a kiválasztott rendszert szakszerűen használják, folyamatosan és kivételezés nélkül. Ez nem is olyan egyszerű feladat. Ugyanis minden védelmi rendszer valamilyen kényelmetlenséggel jár, a felhasználók pedig előbb-utóbb megtalálják az életüket egyszerűbbé tévő kiskapukat (jelszó a billentyűzet alján). Ettől kezdve pedig már el lehet felejteni a védelmi rendszert, akármilyen komoly beruházást igényelt a bevezetése.



Kulcskérdés tehát, miként lehet betartatni a felhasználókkal az előírt követelményeket, folyamatosan és automatikusan ellenőrizni az ennek megfelelő használatot. Az információkockázat-kezelő (Information Risk Management, IRM) rendszerek éppen ezt a feladatot látják el.

IBSZ

Valamennyi informatikai rendszer alapkövetelménye, hogy a benne tárolt információ minden szempontból biztonságban legyen. Ez az a meghatározás, ami (ma már) magától értetődő mindenki számára, ugyanakkor egy gyakorló informatikus nemigen tud mit kezdeni ezzel a definícióval, mivel egy valóban biztonságos rendszer felépítéséhez pontosan meg kell határoznunk, mit tekintünk biztonságos működésnek:

• mi az a működés, amit megengedünk a rendszerünkben és mi az, amit nem;

• milyen megoldásokkal ellenőrizzük, hogy a megengedett működés ténylegesen csak azt csinálja és úgy, amire és ahogy mi gondoltunk, illetve hogy a nem megengedett működések előfordulnak-e a rendszerünkben;

• kik azok, akik használhatják a rendszerünket, és az egyes felhasználók milyen mértékig vehetik igénybe a rendszer szolgáltatásait stb.

Ezek azok az alapkérdések, amelyekre – megfelelő mélységű kockázat- és költségelemzés után – választ kell adni ahhoz, hogy a biztonságos működés kezelhető fogalommá váljék. A válaszok megtalálhatók az adott rendszer Informatikai Biztonsági Szabályzatában (IBSZ). Az IBSZ az információvédelemmel foglalkozó szakembereknek nemcsak újabb dokumentáció a többi között, hanem az informatikai rendszer biztonságának alapja. Igen nagy bátorságra vall, ha valaki (legyen szó felelős vezetőről vagy rendszergazdáról) egy éles informatikai rendszert ilyen szabályzat nélkül, pusztán intuícióra vagy rutinra építve üzemeltet. IBSZ hiányában ugyanis csak ad hoc módszerekkel lehet észrevenni a rendszer megbízhatóságát sértő eseményeket, s utólag (cége válogatja, hány százmilliós kárnál) derülhet ki, hogy a rendszernek létezik gyenge pontja és ezt ki is használták rövidebb-hosszabb ideig.

Természetesen az IBSZ még nem jelenti azt, hogy a védelem terén minden tökéletes és karba tett kézzel ülhetünk; nem is ez a célja. Sokkal inkább az, hogy a rendszer

üzemeltetőinek legyen egy olyan, az üzleti folyamatok elemzésén alapuló kézikönyve, amelyből kiderül: mi az, ami megengedett a rendszerben s mi az, ami nem. Éppen ezért komoly felelősség hárul a szabályzatot összeállítókra. Olyan szabálygyűjteményt kell készíteniük, amely – ha betartják – a rendszer tervezésekor meghatározott szintre tudja csökkenteni a kockázatokat.

Az IBSZ ugyanakkor nem örök érvényű dokumentáció. Az informatika fejlődésével a rendszereknek is újabb és újabb igényeket kell kielégíteniük, így az IBSZ-nek is lépést kell tartania ezekkel a változásokkal. Tehát ne feledkezzünk meg az IBSZ rendszeres felülvizsgálatáról sem!

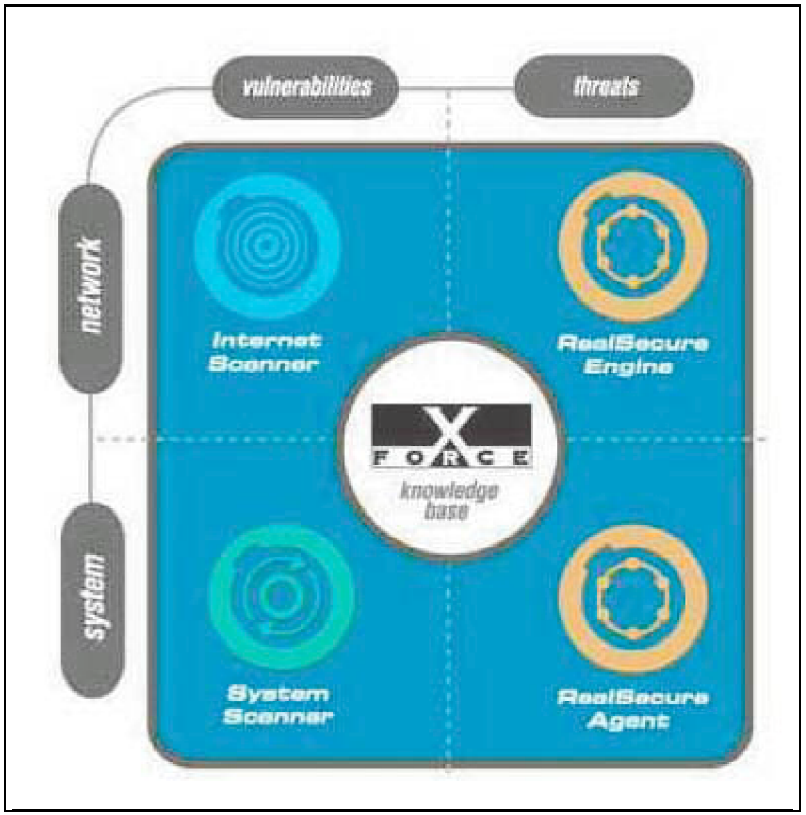
IRM rendszerek

Ha egy informatikai rendszernek már van Informatikai Biztonsági Szabályzata, a következő lépés annak betartatása, amely két párhuzamos feladatból áll:

• Megfelelő gyakorisággal ellenőrizni kell, vannak-e a rendszerünkben biztonsági rések. Erre a célra szolgálnak a különböző szkennerprogramok, amelyek a különböző – a programok minőségétől függő – sérülékenységi adatbázisok alapján felmérik a rendszer egyes elemeinek biztonsági szintjét. Bármelyik gyártó szkennerét használjuk, egy dobozból kivett és frissen telepített rendszeren biztosan találunk számos, kisebb-nagyobb sérülékeny pontot. Azt, hogy ezek közül melyek a potenciálisan problémát okozó sérülékenységek, azt az IBSZ határozza meg.

A szkennerek egy része lehetővé teszi, hogy a vizsgálódást az IBSZ-nek megfelelően, testreszabottan hajtsuk végre. Ekkor a riportok csak azokat a sérülékenységeket fogják tartalmazni, amelyekkel ténylegesen foglalkoznunk kell. Ezeket a sérülékenységeket kijavítva lehet az új eszközt a rendszerünkbe állítani, mert csak így tartható fenn a teljes rendszer védettsége.

Természetesen a behatolási technikák szakterülete ugyanolyan gyorsan fejlődik, mint az informatika. Egy ma sérülékeny pont nélkülinek ítélt rendszeren pár hónap múlva – az akkori legfrissebb sérülékenységi adatbázissal szkennelve – számtalan újabb potenciális támadási felületet találhatunk.



Az ISS SafeSuite család felépítése

Ez egyfelől egyre kifinomultabb támadási technikák megjelenésére utal, ami akár azt is jelenthetné, hogy a támadók nagy része nincs azon a műszaki színvonalon, hogy végre is tudjon hajtani egy ilyen bonyolult behatolást. A tényleges helyzet azonban nem ez: a magasabb tudású hackerek olyan programokba ágyazzák ezeket a technikákat, amelyeket bárki kezelhet és amelyekhez hozzáférhet az interneten. Másfelől számos olyan, nem kellően tesztelt program jelenik meg a kereskedelmi forgalomban, amelyeken néha tényleg ordító biztonsági rések tátongnak. Nem véletlenül terjedt el az a nézet, hogy manapság a kereskedelmi programok legjobban kidolgozott része a licencszerződés, amelyben a gyártó garantálja, hogy semmiért és semmilyen körülmények között nem vállal felelősséget.

A szkennerek megfelelő gyakoriságú és rendszeres használatával azonban esélyünk van arra, hogy még azelőtt felfedezhessük a sérülékeny pontokat rendszerünkben, mielőtt azt bárki meglékelhetné.

• Folyamatosan figyelnünk kell a rendszerünkben zajló eseményeket. Erre a célra szolgálnak a behatolásfelderítő programok (Intrusion Detector Systems, IDS-ek). Ezek az eszközök – szintén az IBSZ alapján – valós idejű üzemben vizsgálják az általuk látott változásokat, majd eldöntik, hogy azok normális vagy biztonságot sértő események. Utóbbi esetben a jobb IDS-ek nemcsak rögzítik a történteket és üzennek a felügyelettel megbízott szakembereknek, de aktív védelmi intézkedéseket is végrehajtanak. Például

kizárják az érintett felhasználót, megszakítják az adott kapcsolatot, átprogramozzák a tűzfalakat.

Az IDS-ek két jellegzetes csoportra oszthatók: host és hálózat alapúakra. A host alapú eszköz adott kiszolgáló védelmét látja el a hoston születő logok folyamatos figyelésével. A hálózat alapú eszközök egy hálózati szegmenst (collision domaint) tudnak védeni úgy, hogy figyelik a hálózaton folyó forgalmat. Mindkét megoldásnak vannak előnyei: a host alapú IDS olcsó és egyszerű; a hálózat alapú IDS nagy hatékonyságú, mert a támadásokat még azelőtt fel tudja ismerni, mielőtt azok eljutnak a támadott eszközig. Persze hátrányok is akadnak: a host alapú IDS csak azt látja, ami a logba kerül, ezt egy ügyes támadó ki tudja kerülni; a hálózat alapú IDS viszonylag drága és erőforrás-igényes, ugyanakkor a switchelt vagy titkosított forgalmú hálózatokban bonyolultabb az alkalmazása.

Optimális megoldások?

Az előnyök összevonására és a hátrányok kiküszöbölésére született meg nemrég az első hibrid IDS, az Internet Security Systems (ISS) RealSecure Server Sensor eszköze. Ez az IDS egyszerre host és hálózat alapú, mert a kiszolgáló logfájljait is tudja figyelni és az adott host hálózati forgalmát is látja az esetleges titkosítás dekódolása után, de még az operációs rendszer előtt.

E két párhuzamos feladat egy kisebb rendszerben viszonylag problémamentesen elvégezhető. A rendszer méretének növekedésével arányosan változik azonban a biztonsággal kapcsolatos információk mennyisége is. Ennek feldolgozása pedig egyre nagyobb terhet jelent a szakembereknek, ami egyre nagyobb hibavalószínűséget feltételez. Ha ehhez még hozzávesszük, hogy a fentieken kívül számtalan más forrásból érkeznek biztonsággal kapcsolatos adatok, akkor beláthatjuk, hogy egy határon túl mindez már „emészthetetlen”. A helyzet persze nem reménytelen, hiszen az IRM vezetői döntéstámogató rendszerek éppen ezen próbálnak segíteni. Ilyen például az ISS SafeSuite Decision is, amely képes – bármilyen, biztonsággal kapcsolatos – információk folyamatos gyűjtésére a rendszerből, majd mindezt el is helyezi egy adatbázisban. Az adatbázisban tárolt adatok elemzésével rengeteg fontos információ tárható fel, segítve ezzel a biztonsági menedzserek munkáját. Ilyen információk lehetnek:

• Melyek azok, a rendszer biztonsági szempontjából leginkább kritikus elemek, amelyek kijavításával a legnagyobb mértékben emelhető az egész rendszer biztonsági szintje? Ehhez nemcsak a sérülékeny pontok meghatározásához szükséges adatokra van szükség, hanem a leggyakoribb támadásokat leírókra is. E kettő összevetésével kiszűrhetjük azokat a sérülékenységeket, amelyeket ténylegesen támadnak.

• Milyen a teljes rendszer biztonsági szintje, hogyan változott ez a szint az elmúlt időszakban?

Ezen információk birtokában a biztonsági szakemberek képesek a felügyeletükre bízott erőforrásokat a lehető leghatékonyabban kihasználni, ugyanakkor a kiadott javítási feladatok elvégzését nyomon tudják követni.

Kőrös Zsolt a Noreg Kft. ügyvezetője.

E-mail: **zsolt.koros@noreg.hu.**

HOL TALÁLHATÓ?

www.noreg.hu

www.iss.net

NEMZETKÖZI HÍREK

2001. FEBRUÁR / NEMZETKÖZI HÍREK / 210 dotcomcsőd 2000-ben

210 dotcomcsőd 2000-ben

Megszűnt tizenötezer munkahely és elveszett 1,5 milliárd dollárnyi beruházási tőke.

A Webmergers.com internetelemző cég tanulmánya szerint 121 vállalkozás (vagyis a befuccsolt cégek 60 százaléka) a negyedik negyedévben ment tönkre; decemberre például negyven áldozat esik, és a Webmergers szerint ezek a cégek legalább 1,5 milliárd dollár befektetési tőkét rántottak magukkal a sírba. A tanulmány hozzáteszi, hogy a bukott vállalkozások legalább egynegyede megpróbálja értékesíteni vagyonát vagy csődeljárás útján újraszervezni önmagát.

A B2C szférában működő cégek közül kerül ki a bukottak 75 százaléka; a B2B cégek adják a 21 százalékot, a maradék pedig jórészt online szolgáltató vagy infrastruktúravállalkozás. Az e-kereskedelemben 55 százalék vett részt, 30 tartalomellátó volt.

Ami a tönkrement cégek területi elhelyezkedését illeti, az Egyesült Államok csúcstechnikai övezeteiben aratott leginkább a „halál": az áldozatok 30 százaléka Kaliforniában maradt a harcmezőn, New York és Massachusetts 10 százalékkal, Nyugat-Európa pedig 11 százalékkal járult hozzá a gyászlistához.

Tim Miller, a Webmergers vezetője szerint a csődök megugrása részben az ünnepek előtti idegfeszültségnek és az év végi könyvelési manővereknek tudható be. Ugyanakkor az is tény, hogy több internetes céget (közkeletű nevén dotcomot) vásároltak fel, mint amennyit becsuktak. „Minden temetésre öt esküvő jutott – véli Miller. – Egyre több cég jön rá, hogy csökkentenie kell a költségeket vagy partner után kell néznie." A szakértő optimista: azt ugyan nem állítja, hogy vége a csődhullámnak, ám úgy gondolja, hogy a nehezén túl vagyunk.

Forrás: Information Week

2001. FEBRUÁR / NEMZETKÖZI HÍREK / Fellendülés előtt a DSL

Fellendülés előtt a DSL

Elemzők szerint a tavaly tapasztalt problémák ellenére a DSL 2001-ben könnyebben elérhetővé és vonzóbbá válik a vállalkozások számára. 2000-ben a DSL-nagykereskedők többször is megégették a kezüket. Néhány, csődbe ment kis internetszolgáltató nem tudta kifizetni a nagykereskedők járandóságát, és a cégek kénytelenek voltak munkásokat

elbocsátani, bővítési terveiket pedig elhalasztani. A nagykereskedők a jövőben óvatosabban fogják megválogatni partnereiket, és inkább a nagyobb, stabilabb vállalkozásokkal kötnek szerződést – vélik az elemzők. Valószínűleg közvetlen kapcsolatokat is megpróbálnak majd kiépíteni a fogyasztókkal, mert így maguk ellenőrizhetik a szolgáltatás színvonalát.

A nagy távközlési cégek általában hiányos szolgáltatásokat nyújtanak a kisvállalkozásoknak, így a DSL-nagykereskedők a siker reményében célozhatják meg az üzleti fogyasztókat. A kábelmodem-szolgáltatások felhasználói bázisa idén várhatóan megduplázódik, az előfizetők száma ötmillióval nő. A DSL nem számíthat ennyi új felhasználóra, de az előfizetők több mint egyharmada kisvállalkozás lesz.

A DSL-lel a fő baj az, hogy viszonylag lassú az igények kielégítése és gondok vannak az együttműködő képességgel – márpedig ez a két probléma 2001-ben sem oldódik meg teljesen. A DSL szolgáltatás bevezetése azért bonyolult, mert a távközlési cégek, az ISP-k és a DSL-nagykereskedők bonyolult egyeztetését és együttműködését igényli. A felek mindegyike másfajta számítógéprendszert használ, és bár szoftvercégek már dolgoznak az ellátók rendszereinek összekapcsolásán, a programok széles körű elterjedése 2002 előtt nem várható. Manapság a DSL működése hálózatspecifikus. Év végére elkészültek az együttműködő képességet szavatoló szabványok, amelyek nagymértékben elő fogják mozdítani a DSL-piac fejlődését, hatásuk azonban 2001-ben még aligha jelentkezik.

2000 ezzel együtt az áttörés éve volt a DSL számára: bár az előfizetések nem érték el az elemzők által megjósolt szintet, a tízszázalékos növekedés így is minőségi ugrást jelentett.

A piac legnagyobb szereplői, például az AOL és a Microsoft az év második felében több pénzt költöttek marketingre, és ennek meg is lett az eredménye: az AOL jelenleg több mint ötezer megrendelést vesz fel hetente, az Egyesült Államok legnagyobb DSL-ellátója, az SBC pedig naponta 3000-4000 új fogyasztónál telepít DSL-kapcsolatot.

Az AOL nemrég bővítette DSL forgalmazási kapcsolatait a Gatewayjel és a Circuit Cityvel. A Gateway hat bevásárlóhelyen kínálja új számítógépeihez a DSL szolgáltatást, az AOL „csináld magad” eszközkészlete pedig tíz bevásárlóközpont Circuit City boltjaiban kapható. Az AOL DSL szolgáltatása csak a Verizon és az SBC fogyasztói számára

hozzáférhetők. Az SBC október óta 516 000 előfizetőről számolt be. Nő a lefedettség, és a vásárlók 70 százaléka saját kezűleg telepíthető megoldást választ, ennek következtében az SBC két héten belül ki tudja elégíteni a megrendeléseket. A cég 2002-re a felhasználók 80 százalékát el akarja érni a DSL-lel – ehhez úgynevezett szomszédsági átjárókat kíván használni, amelyek a központi irodától a jelenlegi 5334 méternél nagyobb távolságokra terjesztik ki a DSL hatókörét. Az átjárók telepítését már meg is kezdte a cég.

Forrás: Information Week

2001. FEBRUÁR / NEMZETKÖZI HÍREK / Fordítás IBM-módra

Fordítás IBM-módra

Az IBM új fordítóprogramja a webhelyek, elektronikus levelek és élő csevegőfórumok tartalmát angolról franciára, németre, olaszra, spanyolra fordítja és vissza. A WebSphere Translation program ezenfelül angolról kínaira, japánra és koreaira is fordít, de ezeknél az ázsiai nyelveknél visszafelé nem működik.

Egy németországi bank intranetjén már tesztelik a programot és az IBM is használja a szoftvert saját webhelyének Developers Cornerében. A teljes változat márciusban jelenik meg. *Brian Garr,* az IBM beszédfelismerő rendszerekkel foglalkozó csoportjának fejlett technológiáért felelős programvezetője szerint az IBM sokat dolgozott azon, hogy a WebSphere Translationt megszabadítsa azoktól a problémáktól, amelyek az úgynevezett univerzális fordítóprogramokat korábban jellemezték. Ezek közé tartoznak például a helytelen szó- és mondatszerkezetek, amelyek sértik a célközönség fülét. Még fontosabb, állítja Garr, hogy a fordítókódokat az adott nyelveket anyanyelvi szinten beszélő fejlesztők írják.

A profi fordítók nem félnek attól, hogy az új program elveszi a kenyerüket. „A gépek alkalmazási lehetőségei korlátozottak, hiszen a nyelvet nem lehet szóról szóra lefordítani" – jelentette ki a Linguistic Systems egyik vezetője. Garr szerint az IBM sem hiszi, hogy a program tökéletes munkát végez. A cég éppen ezért arra buzdítja a felhasználókat, hogy a lefordított anyagokhoz mellékeljenek egy nyilatkozatot, amely tudatja az olvasókkal, hogy amit látnak, csupán fordítás. A WebSphere Translation Windows NT, AIX és Solaris alapú kiszolgálókon fut.

Forrás: Information Week

2001. FEBRUÁR / NEMZETKÖZI HÍREK / Jelszó nélkül, szabadon

Jelszó nélkül, szabadon

A biometrikus azonosítási technikák úttörője, az eTrue a NASA-nál beindította internetes bejelentkező szolgáltatását. A NASA alkalmazottai hazulról az eTrue szolgáltatásán keresztül férhetnek hozzá a hálózati szervereken lévő bizalmas adatokhoz. A rendszer mind a webes, mind a hálózati bejelentkezéseknél többféle biológiai jellemző, köztük az arc

és az ujjlenyomat alapján azonosítja a felhasználót. A szolgáltatásnak az Exodus Communications ad otthont és az eTrue felügyeli.

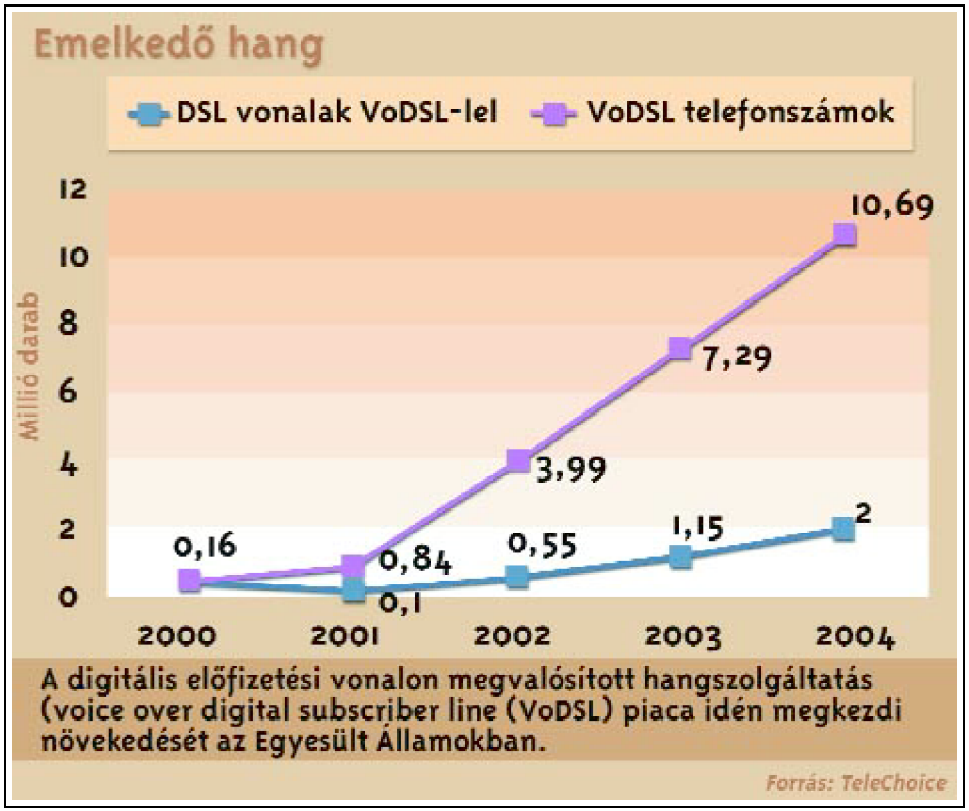
Az eTrue az üzlet részeként kamerával és ujjlenyomat-olvasóval látja el a vásárlót. A cég szerint azok a vásárlók, akik beszállnak az „Első alkalmazók programjába" (a NASA ezt tette), néhány napon belül már használhatják is a rendszert. A szolgáltatás tetszőleges számú felhasználót tud kezelni és éjjel-nappal működik. Az ellenőrzés mellett minden tranzakciót naplóz, és adatai későbbi jelentésekhez, ellenőrzésekhez is felhasználhatók.

Az új rendszerrel az internetes e-üzletben megjelent a biometrikus ellenőrzési technika: nincs szükség jelszavakra, azonosítószámokra, kártyákra, kulcsokra vagy bármire, amit az ember elveszíthet vagy amit ellophatnak tőle – nyilatkozta *David Teitelmann,* az eTrue elnök-vezérigazgatója. A tranzakciók és a tárolt adatok védelméről és biztonságáról többszörös tűzfallal körülvett, SSL szintű internetkommunikációt nyújtó, redundáns kiszolgálókra épülő, hibatűrő rendszer gondoskodik. Az eTrue szolgáltatás Windows 98-at, NT-t és 2000-et futtató ügyfélrendszerekkel, illetve Windowst, Unixot vagy Linuxot futtató szerverekkel működik.

Forrás: Network Magazine

2001. FEBRUÁR / NEMZETKÖZI HÍREK / Emelkedő hang

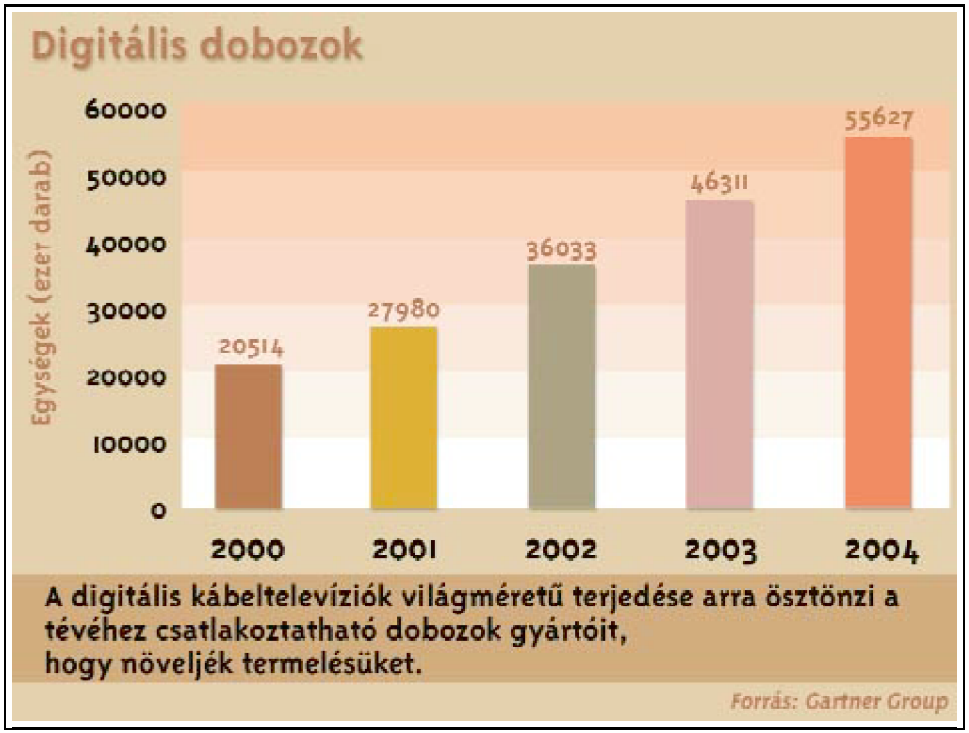
Emelkedő hang



A digitális előfizetői vonalon megvalósított hangszolgáltatás, a voice over digital subscriber line (VoDSL) piaca idén megkezdi növekedését az Egyesült Államokban.

2001. FEBRUÁR / NEMZETKÖZI HÍREK / Digitális dobozok

Digitális dobozok



A digitális kábeltelevíziók világméretű terjedése arra ösztönzi a tévéhez csatlakoztatható dobozok gyártóit, hogy növeljék termelésüket.

2001. FEBRUÁR / NEMZETKÖZI HÍREK / Kihelyezett biztonság

Kihelyezett biztonság

A legalább 100 millió dolláros árbevétellel rendelkező amerikai cégek kihelyezett biztonsági szolgáltatásokra (tűzfalra, virtuális magánhálózatra és vírusok elleni védelemre) szánt kiadásai évente 165 százalékkal nőnek a következő öt évben.

Az IP hatodik fokozata

Az IPv6 egy olyan kor követelményeit elégíti ki, ahol még a hűtőszekrényeknek is lehet saját IP-címük.

Szerző: Kelly Jackson Higgins

Az IP Version 6, az internet protokoll új generációja végre felkészült, hogy átvigye az internetet abba a fázisba, ahol gyakorlatilag bárminek lehet saját IP-címe. Az IPv6 tágas címzéstartományának akkora a térfogata, hogy el tudja látni címmel a webtelefonokat, a kábelmodemeket, a DSL csatlakozókat, sőt akár a repülőgépüléseket is.

„A címzés a fő ok, amiért az IPv6-ot kifejlesztették – mondja *Robert Hinden,* az IETF IP Next-Generation munkacsoport társelnöke. – Elsősorban azért hozták létre, hogy

nagyobbá tegye az internetet.”

ILLUSZTRÁCIÓ: BUTTINGER GERGELY

Mindamellett nem tűnik úgy, hogy a vállalkozások különösképpen sietnének bevezetni az IPv6-ot. A legtöbb egyesült államokbeli cég egyelőre csak halmozza a meglévő IPv4-címeit vagy belső, „álcímeket” gyárt, és közömbös az IPv6 iránt. Az IPv4-es címhiányban szenvedő régiók, mint Ázsia és Európa, valamint a mobil hálózatok gyártói, üzemeltetői támogatják az IPv6-ot, hogy több címhez jussanak. Az IPv4-es rendszer kapacitásának már mintegy a felét elhasználta, ami kevés teret enged az új hálózatoknak és a kapcsolt eszközöknek.

A mobil világ lehet az IPv6 első átütő erejű alkalmazása: a Third Generation Partnership Project (Harmadik generációs együttműködési projekt, 3GPP) az IPv6-ra szavazott a mobil hálózatok új hullámának. Ez oda vezethet, hogy a következő néhány évben robbanásszerűen megnő az IPv6 nyelvét beszélő mobilkészülékek száma, ami érdekeltebbé teheti Amerika vállalatait is. Egyes európai országokban, például az Egyesült Királyságban már megkezdődött az új generációs mobil hálózatok árveréses kiosztása. Az Egyesült Államokban, amely a mobiltelefóniában legalább egy generációval le van maradva Európától, 2002-ben lesz az első árverés.

128 biten

Az új korszak internetje is mozgékonyabb lesz az IPv6-tal, mivel az IP csomagok ide-oda ugrálnak majd a mobil és a vezetékes hálózatok között. Az IPv6 128 bites címzésstruktúrája képes lesz befogadni a mobil kézi készülékek új generációját. Az IPv6-nak 128 bites címei vannak, szemben az IPv4 32 bites címeivel, ami gyakorlatilag végtelen címzésterületet jelent, hiszen ez exponenciális növekedés.

„A vezeték nélküli technológia lesz az IPv6 motorja – vélekedik *Art Souza,* az interaktív- és videokonferencia-szerverszoftvereket fejlesztő cég, az Ezenia külföldi forgalmazásért felelős alelnöke. – Lényegesen több a mobil telefon, mint a PC.”

Ezenközben azért a Net nagy nevei már a fedélzeten vannak kereskedelmi IPv6-termékeikkel. A Cisco, amely már két éve forgalmaz egy letölthető IPv6-tárkezelőt, az első negyedévben az IOS 12.2.1t verziójába beépítve kínálja majd az IPv6-ot. A Sun Microsystems Solaris 8.0 szoftvere már kezeli az IPv6-ot, akárcsak az IBM az AIX 4.3-as és újabb verzióiban. A Microsoft a Windows 2000 bedolgozóprogramját valódi termékké alakítja a Windows 2000 idén megjelenő új verziójában. A Novell az év közepén jelenik meg a NetWare 5-ös és 6-os verziójához letölthető IPv6 bedolgozóprogrammal. A Nortel az IPv6-ot beépíti feladatorientált integrált áramkörébe a készülő harmadik generációs mobilberendezéseihez. Már piacon van a cég IPv6-ot használó AGS útválasztója és Passport 5430-as hang-adat váltója. A BSD shareware Unix és Linux operációs rendszerei már kezelik az IPv6-ot.

Egyelőre nem sürgős

Az IPv6 korai felhasználóinak többsége az amerikai kutatók és az egyetemek

köréből kerül ki. Az IPv6 eladói azt állítják, hogy bár a cégek egyre nehezebben találnak nagy IPv4-es címmezőket, semmi sem sürgeti a dolgot. Az IPv4, az IP első verziója még várhatóan elél 10-15 évig, párhuzamosan az új IPv6-os mobilkészülékekkel, útválasztókkal és hálózati kiszolgálókkal.

Szemben az Egyesült Államokkal, amely felépítette és kiterjesztette az internetet és idejekorán jókora szeletekhez jutott az IPv4-ből, Ázsiának és Európának nehéz időkkel kell szembenézniük az IP-címek tekintetében. Az egyenlőtlenség megrázó: a Stanford Egyetem, ahol az internet született, körülbelül 17 millió IPv4-címet birtokol, míg a teljes kínai nemzet körülbelül 9 millió IPv4-címmel rendelkezik. Japán és az Európai Bizottság – mindkettő belefáradva, hogy úgy kell összelopkodniuk egy kis címhelyet – ebben az évben az IPv6-ot leendő IP-terjeszkedésük fontos tényezőjének nevezték. Az IPv6-címeket már elkezdték juttatgatni a szolgáltatóknak a regionális internet-nyilvántartók, mint például az American Registry for Internet Numbers (ARIN), valamint a hasonló ázsiai és európai intézmények. A japán ISP Internet Initiative Japan már kínál egy eredeti IPv6-szolgáltatást Japánban. Az Egyesült Államokban pedig az internetszolgáltatók közül elsőként a Qwest Communications, a WorldCom és a Zama Networks nyújtanak IPv6-os transzportszolgáltatást.

Még egyik amerikai szolgáltató sem szárnyal, de a Qwest erőteljesen gyűjti próbawebhelyeit az új kereskedelmi IPv6 hálózati szolgáltatásához, amelyet külön OC3-as gerincvezetéken továbbít New York-ból Denverbe, majd onnan tovább San Franciscóba.

„Az IPv6 világméretű mozgalommá kezd válni – jelenti ki *Guy Cook,* a Qwest internetszolgáltatásért felelős alelnöke. – Az internet eddig erősen Amerika-központú volt."

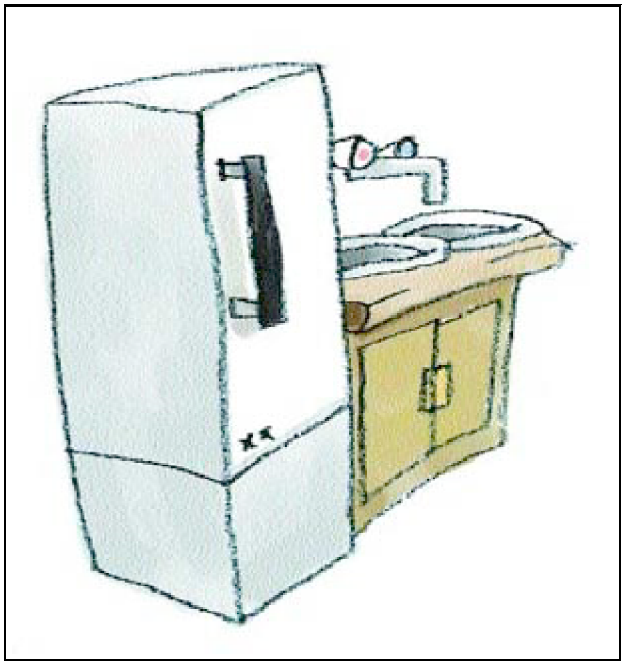
A dolog iróniája, hogy az IPv6 nem igazán észbontó sebességgel kezdte pályafutását. A protokoll több mint tíz évig készült, és a hajdan csak rá jellemző különleges tulajdonságai – mint a szolgáltatásminőség és a biztonság – bekerültek az IPv4-be. De nagyobb címzéskapacitása és egyes tulajdonságai – mint a hálózati eszközök önkonfigurálhatósága és a mobil IP – életben tartották.

„Ha azt akarjuk, hogy az internetkísérlet egy fokkal magasabb szintre lépjen, akkor lennie kell egy IPv6-infrastruktúrának" – vélekedik *Mark Silverberg,* a Compaq IPv6-képességekkel rendelkező Tru64 Unix operációs rendszerét forgalmazó szervezeti egység vezető üzletkötője.

Nincs elég cím

A fennmaradó IPv4-címek nem elegendőek a várhatóan egymilliárd új csomóponthoz, beleértve azokat a mobil készülékeket, amelyek becslések szerint a hálóra lépnek az elkövetkező néhány évben. „Az IPv6 személyenként egymilliárd címet nyújt" – tájékoztat *Thomas Narten,* az IBM vezető szoftverfejlesztője.

Itt van az IP-címzés rejtélyének a lényege. Az IPv4 olyan, mintha egy bizonyos mennyiségű telefonszámunk lenne ennél jóval több telefonhoz. Az IPv6 pedig ahhoz hasonlítható, mintha a szükségesnél lényegesen több számjegyünk lenne a telefonszámokhoz, vagyis több cím jut a hálózati eszközöknek.



Bár a tipikus vállalkozások nem készültek még fel az IPv6 használatára, a nagy vállalat-összeolvadások és -felvásárlások már fejfájást okozhatnak az IP-címek tekintetében, például ha a vevőnek le kell mondania a megvásárolt cég IP-címeiről és újakat kell hozzárendelnie az eszközeihez.

„Meglátják, hogy ezen cégek közül sokan megkezdik majd az áttérést az IPv6-ra, mihelyt megfogalmazzák a jövőstratégiájukat" – véli *Graham Lovell,* az IPv6-kompatibilis Solaris 8.0-t árusító Solaris értékesítési igazgatója.

Egyelőre még nem sok vizet zavarnak az IPv6-ot tesztelő vállalatok, és kevés egyesült államokbeli cég törődik egyáltalán az IPv6-tal. Még azután is, hogy a Bank of America összeolvadt a volt NationsBankkel, a banknak változatlanul van elegendő IP-címe. Egy nagy DHCP architektúrát üzemeltet, amely kezeli az összeolvadásból kimaradt több százezer IPv4-címét.

„Az IPv6 egyelőre még a radarképernyőinken sem látszik. Van címünk bőven" – nyilatkozza *Rick Ingrassia,* a San Franciscó-i Bank of America nyílt hálózatokért felelős elnökhelyettese.

Egyéb előnyök

A címzéstartomány mellett az IPv6-nak akad még néhány előnye. Az IPv6-világban könnyebb lesz internetszolgáltatót váltani, mivel a cégeknek ekkor sem kell lemondaniuk IP-címükről. „Ha elhagyja a hálózati szolgáltatóját, megtarthatja az eszközéhez rendelt címet és nem kell átszámoznia a hálózatát" – mondja *Orv Cooper,* a Zama Networks alelnöke és műszaki vezetője.

Ez a szolgáltatás az IPv6 önkonfiguráló képességének köszönhető, ami tulajdonképpen önálló felkutatás. Az alkalmazott módszerek egyike az állapot nélküli önkonfigurálás, ami

összehozza a gép meglévő MAC címét a helyi útválasztó hálózati prefixumával, ahelyett hogy azt az IP-címet használná, amit a DHCP kiszolgáló osztott ki.

„Így időt takarítunk meg, és a kevés hálózatiinfrastruktúra-ismerettel rendelkező felhasználó is úgy konfigurálhatja az eszközét, hogy nem is tud róla" – nyilatkozta *Susanna Wood,* a Nortel IPv6-programjának vezetője. Ekként elkerülhető a DHCP kiszolgálók adminisztrálásának szakemberigényes módja, amit a legtöbb nagy szervezet használ IPv6-címeinek kezelésére. Tehát a 6-os verzióban is használhatók maradnak a DHCP kiszolgálók, ha egy cég nem akarja kiselejtezni ezeket. És az IPv4-gyel ellentétben a felhasználónak nem kell újraindítania az asztali számítógépét vagy noteszgépét, ha IP-címet vált.

„Az önkonfigurálás sokkal okosabbá teszi a hálózatot" – véli *Shanen Boettcher,* a Microsoft Windows 2000-kiszolgálókat forgalmazó részlegének vezető termékmenedzsere. Állítása szerint a kiszolgáló a bejelentkező címből azt is tudni fogja, hogy a felhasználó az otthoni vagy a munkahelyi gépéről jelentkezett-e be.

A beépített biztonság ugyancsak az IPv6 egyik előnye. Bár az IPSec hozzáférhető a 4. verziós hálózatokon is, a néhány nagyvállalat hálózatának peremén ülő címfordító (Network Address Translation, NAT) átjárók lelassíthatják a titkosítást. A címfordító átjárónak az a feladata, hogy a saját vagy egyedi IP-címet átfordítsa azon kevesebb címek egyikére, amit a Net megért és viszont. „Az IPv6-tal a biztonság a kapcsolat teljes hosszán működik, hála a globális, egyetlen címnek" – mondja az IBM-es Narten.

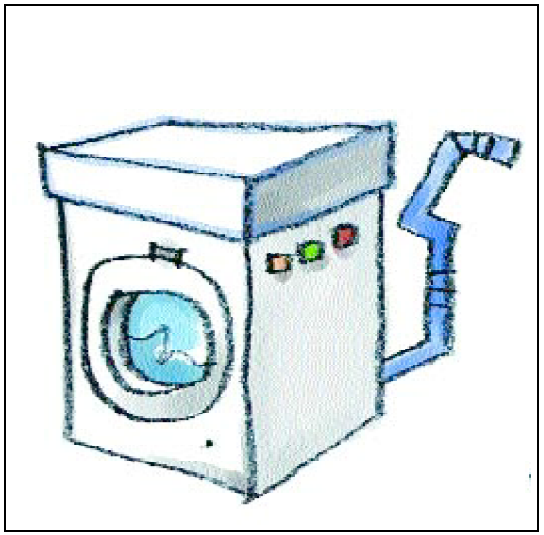
A 3GPP 2000-es specifikációjában azt igényli, hogy az IPv6-ot építsék be a 2002-ben induló mobil IP multimédia-alrendszerbe, vagyis azokba a kiszolgálókba, amelyek szétválasztják a hangot és az adatot, amikor az információ belép a hálózatba.

„Az IPv6 valószínűleg benne lesz a mobilkészülékekben, így vagy lesz, vagy nem lesz szükség csatornakeresésre vagy címfordításra az információkezelő rendszer előtt" – vélekedik *John Donaldson,* az IPv6-ot mobilkészülékeibe beépítő Nortel stratégiai igazgatója.

Ez persze nem jelenti azt, hogy két esztendő múlva minden mobilkészülék kizárólag IPv6-használó lesz, sem azt, hogy ilyen lesz az internet infrastruktúrája. Akárcsak az

IPv6-ot már gyakorlatban tesztelő helyeken, a mobilkészülékek valamiféle „becsatornázást” fognak végezni az IPv6-forgalomnak a meglévő IPv4-be tereléséhez, akárcsak egyes NAT-ok.

Megoldandó feladatok



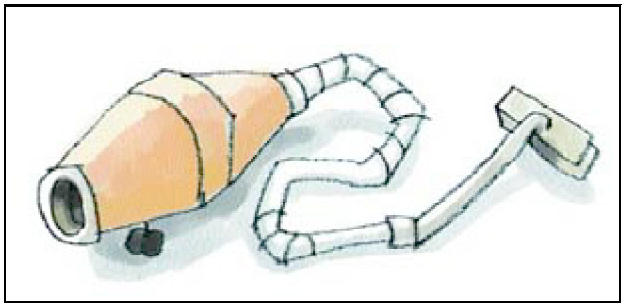
Az IPv6 mobil IP-infrastruktúrájával a felhasználó fenntarthatja a kapcsolatot, miközben cellákat vált. „Lehetőség van a kapcsolatátadásra a tornyok közt, így fennmarad az IP-kapcsolat” – jelenti ki Donaldson. Van azonban valami, amit a mobil IP nem tesz meg, vagyis megszakad a kapcsolat akkor, amikor a felhasználó a vezetékes hálózatról átlép a vezeték nélkülibe. A Nortel ennek a kiküszöbölésére építette bele ezt az új szolgáltatást a mobil szoftverébe.

Egyelőre azonban rengeteg olyan infrastruktúra létezik, amit hozzá kell illeszteni az IPv6-hoz, mielőtt az széles körűen beindulna. „Nincsen olyan (kereskedelmi forgalomban kapható) tűzfal vagy csomagszűrő eszköz, ami IPv6-ot használna” – állítja Lovell a Suntól.

Ráadásul a szoftver alapú IPv6-kezelés elég lehet a korai megvalósítások esetén, de hosszú távon elégtelen lesz a nagy internetszolgáltató hálózatokhoz. „A szoftver most még megfelel, ám ahogy cégünk ezen szektorának növekedését figyeljük, hosszú távon szükség lesz a szilíciumra” – említi Cooper a Zamától.

Arról nem is beszélve, hogy az internetszolgáltatók miként lesznek képesek támogatni azokat a mobilkészülékeket, amelyek a nyilvános kapcsolt telefonhálózatról átugranak az internetre.

„Jó néhány trükkös eset várható, amikor ötszázmillió mobilkészülék úgy barangol majd, hogy a hívásnak egy vezetékes helyen kell végződnie – közli *Charles Lee,* a WorldCom kormányzati eladásokért felelős vezetője. – Az IP-hez még kifejlesztésre várnak azok a számlázási módok és vevőtámogatások, amelyeket az emberek a telefóniában már megszoktak.”



Alkalmazások gyakorlatilag még nem készültek az IPv6-hoz. De egy alkalmazás IPv6-ra való alkalmassá tétele rendszerint csak annyiból áll, hogy hozzáadunk egy IPv6-protokolltárat, amit felkészítünk a 128 bites cím megértésére. Egyes alkalmazásoknak egyáltalán nem is kell együttműködniük a protokollokkal, míg másoknak igen. „Egyes alkalmazásokat könnyű lesz átírni a 128 bit használatához, de lesznek olyanok is, amelyek valamivel több munkát igényelnek majd" – jelenti ki *Bob Fink,* az Energy Sciences Network helyettes kutatásifőosztály-vezetője a UC-Lawrence Berkeley National Laboratorynál.

És bár számos amerikai cég elégedett egyelőre meglévő IPv4-infrastruktúrájával, a vezető hálózatiberendezés-gyártók szép ütemesen rakják le a következő generációs IP alapjait. Más nagy műszaki fordulatokhoz hasonlóan az IPv6 is fokozatosan fog felemelkedni, különösebb hűhó nélkül, a végfelhasználók többsége pedig észre sem veszi, hogy valami változott.

Kelly Jackson Higgins ***(kjhiggins@aol .com)*** *szabadúszó újságíró.*

Forrás: Internet Week, a CMP Media, Inc. kiadványa.

2001. FEBRUÁR / CÍMLAPSZTORI

CÍMLAPSZTORI

2001. FEBRUÁR / CÍMLAPSZTORI / LELAKATOLT CÍMTÁRAK

LELAKATOLT CÍMTÁRAK

A címtárszolgáltatások páncéltermeiben egyre értékesebb adatok rejtőznek, de néha nem könnyű észrevenni a hívatlan látogatót.

Egy nagyvállalati számítógéprendszer minden sarkában és szegletében található valamilyen információ, beleértve az adatbázisokat, a szövegszerkesztő állományokat és az intranetet. A legtöbb vállalatnál a földrajzilag vagy szervezetileg elkülönülő dolgozók vagy csoportok sok időt pazarolnak arra, hogy redundáns információkat gyűjtsenek össze. A címtárszolgáltatások azért születtek, mert a vállalatok felismerték, hogy ez a gazdag adattömeg még sokkal értékesebb lehet, ha rendszerezett módon gyűjtik össze és teszik elérhetővé egy kereshető adattárban.

A redundancia csökkentésével és a hozzáférhetőség növelésével a címtárszolgáltatások ígéretes módon szervezik az adatokat a vállalat által könnyebben felhasználható módon. A címtár-szolgáltatási architektúra egy vagy több címtáradatbázist (a címtárszervert) és ügyféloldali szoftveralkalmazásokat (címtárügyfeleket) tartalmaz. Az X.500-as so-rozatú szabványok, amelyeket 1988-ban tett közzé az ISO és az ITU, gyakorlatilag referenciaként szolgálnak a címtárszolgáltatások számára.

Akárhogy is, a látomás, amit ezek a szabványok előre vetítettek, sosem valósult meg. A vállalatok lassan haladtak előre az X.500 elfogadásával, mivel az meglehetősen összetett. A Lightweight Directory Access Protocol (LDAP), amelyet az X.500 leszűkítésével készítettek, megfelelt a komplexitással kapcsolatos kérdésekre, az e-kereskedelem terjedésével pedig a politikai kérdések jelentősége is számottevően csökkent. Az elektronikus kereskedelem versenyhelyzetben előnnyé változtatta az információelérést.

Ahogy a címtárak mindinkább kifinomult és értékes adatok kincstáraivá váltak, a bennük tárolt adatok biztonságának veszélyeztetettsége a dolog természeténél fogva úgy lett egyre komolyabb. Cikkünk fölvázol néhány lehetséges módszert, amellyel a szervezetek tőkét kovácsolhatnak a címtárhasználatból, majd folytatjuk a telepítés rizikófaktorainak tárgyalásával, levonjuk következtetéseinket, különös tekintettel a sebezhető pontokra és azok védelmére, végül bepillantunk a jövő fejlesztéseibe.

A kezdetek

Bármely szervezetben számos lehetőség kínálkozik tőkét kovácsolni a címtárak használatából. Bizonyosfajta informá-ciók jobban illeszkednek a címtárszolgáltatásokhoz. Általában ez az információ kereshető is lesz, amiként kereshető minden információ, amelyet logikus rendszerbe foglaltak vagy amely ilyen rendszerbe foglalható. Azok az

adatok, amelyek közvetlen jelentést hordoznak, jobban működnek egy címtárban. Ilyen például a kollégánk telefonszáma vagy egy alkatrész katalógusszáma. A ritkán változó adatok is igen alkalmasak címtárban tárolásra. A gazdanevek és az IP-címek ugyan változhatnak, ám nem túl gyakran.

A címtárak leginkább nyilvánvaló felhasználási területe a telefonkönyv, amely a dolgozók nevét, címét, telefonszámát és e-mail címét tartalmazza. A telefonkönyv után egyszerűen hozzáadhatók a címtárhoz a számítógépes infrastruktúra adatai, például a DNS-táblázatok, valamint a leltár- és felhasználólisták.

Egyetlen címtárat használva – amelyben a felhasználóknak a vállalat minden rendszeréhez, adatbázisához és alkalmazásához létezik bejegyzésük – a vállalat rengeteg időt takaríthat meg ahhoz képest, hogy ezeket az adatokat egyedi adatbázisokban, külön-külön tárolnák. A megtakarítás elérheti akár a 30 százalékot is. Természetesen a másik oldalról ez veszélyes is lehet: ha a központi információ elvész, az súlyosan érinti az egész céget (gondoljunk csak az ellopott belépési kódokra).

Fokozódó félelmek

A vállalatok akkor nyerhetik a legtöbbet a címtárak használatával, ha érdemi üzleti adatokat, például táblázatokat, vevőlistákat, viszonteladók adatait tárolják bennük. Így az adatok sokkal könnyebben hozzáférhetők és megszűnik a redundancia. Magától értetődik: ahogy a vállalat egyre értékesebb és kifinomultabb módon használja a címtárakat, úgy a benne tárolt adatok értéke is egyre nő – no meg a veszély is, amely az adatok biztonságát fenyegeti.

Sajnos éppen az elérhetőség, amely ezeket az adatokat oly hasznossá teszi, fokozza a legjobban a sebezhetőséget. Rigorózus és paranoiás biztonság alkalmazása híján változatos veszélyek fenyegetnek. Még riasztóbb, hogy nem könnyű észrevenni, ha egy sebezhető ponton valaki bejutott a rendszerbe. A sikeres betörések és az ellopott adatok azután könnyen súlyos üzleti problémák forrásaivá válhatnak, beleértve a vevők bizalmának elvesztését. Ha ugyanis nyilvánosságra kerül az információlopás ténye, versenyhelyzetben ez az előny elvesztésével járhat, sőt még bírósági ügy is lehet belőle, amelyet az adatok bizalmas kezelésének megsértése miatt indíthatnak.

A vállalatnak számos kockázatot kell felvállalnia a címtárak bevezetése során. Az egyik, hogy az adatok innentől kezdve nyíltan elérhetők, nem megfelelő személy is hozzájuk férhet. Szinte mindig az a helyzet, hogy a címtárakban tárolt adatoknak többszintű titkossági minősítéseik vannak. A másik rizikó az adatvesztés, amikor az információ törlődik. Azt hihetnénk, hogy a törlést könnyű észrevenni, de amikor több millió rekord változásait kell figyelemmel kísérni, ez szinte lehetetlen. A harmadik veszély az adatok módosítása, akár oly módon, hogy nem kellő hozzáértéssel teszik, akár úgy, hogy szándékos rosszakarattal változtatják meg azokat. Ez azonnal érzékeny módon befolyásolja a címtár értékét, hiszen az egyenes arányban áll a benne lévő adatok pontosságával.

Elő a pajzsokkal!

A továbbiakban azokra a sebezhető pontokra mutatunk rá, amelyekre minden címtárhasználónak figyelnie kell és meg kell tennie a megfelelő lépéseket a védelmükre.

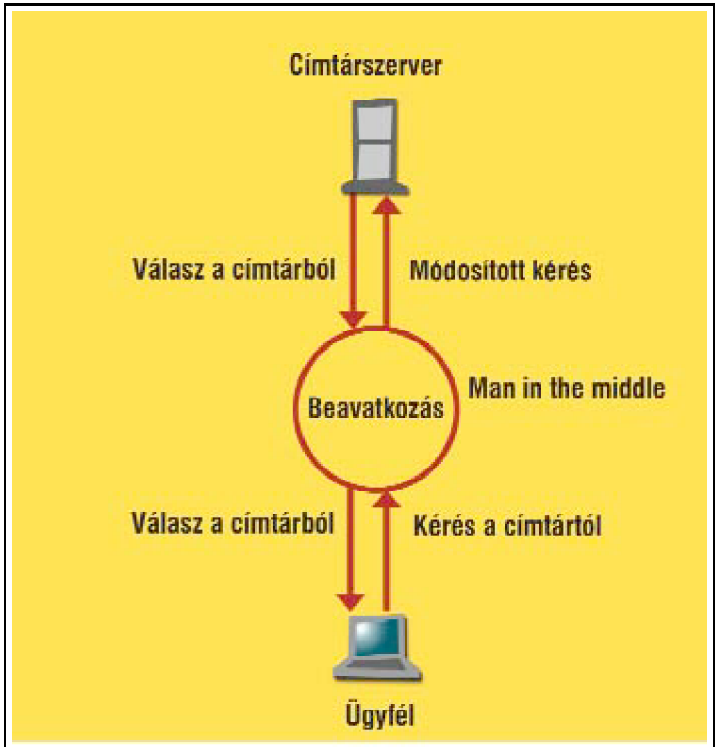
A címtárakat fenyegető veszély rengeteg összetevőtől függ, többek között attól, hogy a címtár milyen információt tartalmaz, ki férhet hozzá és hol található (a hálózatban, illetve fizikailag). A veszélyek azonban enyhíthetők, ha a címtár tervezésekor megfelelő hangsúlyt helyezünk a biztonságra. Természetesen nagyvállalatoknál, ahol több tucat címtár van üzemben, ez valószínűleg nem valósítható meg. Ugyanakkor már azzal is csökkenthetjük vállalatunk sebezhetőségét, ha gondosan kiértékeljük a rizikófaktorokat, amelyek kulcsfontosságú címtárainkat veszélyeztetik.

A konkurencia többféle módon érheti el információinkat. Komoly veszélyt jelent a lehallgatott kommunikáció, amelynél a hálózaton mozgó informá-ciót csípik el menet közben. Ezt a veszélyforrást később részletesen fogjuk tárgyalni. Ennél hétköznapibb eset a közvetlen, jogosulatlan hozzáférés a címtárhoz. Ez ellen az első lépés az, hogy minden felhasználónak azonosítania kell magát és hogy a hozzáférési jogosultságokkal megfelelő korlátozásokat léptetünk életbe.

Azonosította magát?

Magától értetődik: a címtár védelmében az első lépés, hogy mindig tudjuk, ki akar hozzáférni. „De nálam már van felhasználóazonosítás” – válaszolja erre. Azonban valószínűleg csupán név–jelszó párost használ. Az egyszerű név–jelszó alapú azonosítás persze többet ér, mint ha nem lenne semmi – de a védelem, amit nyújt, erősen korlátozott, ha a jelszavakat nem kódolt formában küldik át a hálózaton (és ez gyakorta így történik).

A betolakodó figyeli a hálózati forgalmat a nyílt szövegben továbbított jelszavakért, és így „jogszerű” címtárhozzáférésre tehet szert. Nyílt szövegű jelszavakkal csak igen alacsony biztonsági szintű hozzáférést engedhetünk, például a munkatársak módosíthatják elérhetőségeiket a vállalat telefonkönyvében, de ez a megoldás nem alkalmas az értékes információ biztonságának szavatolására.



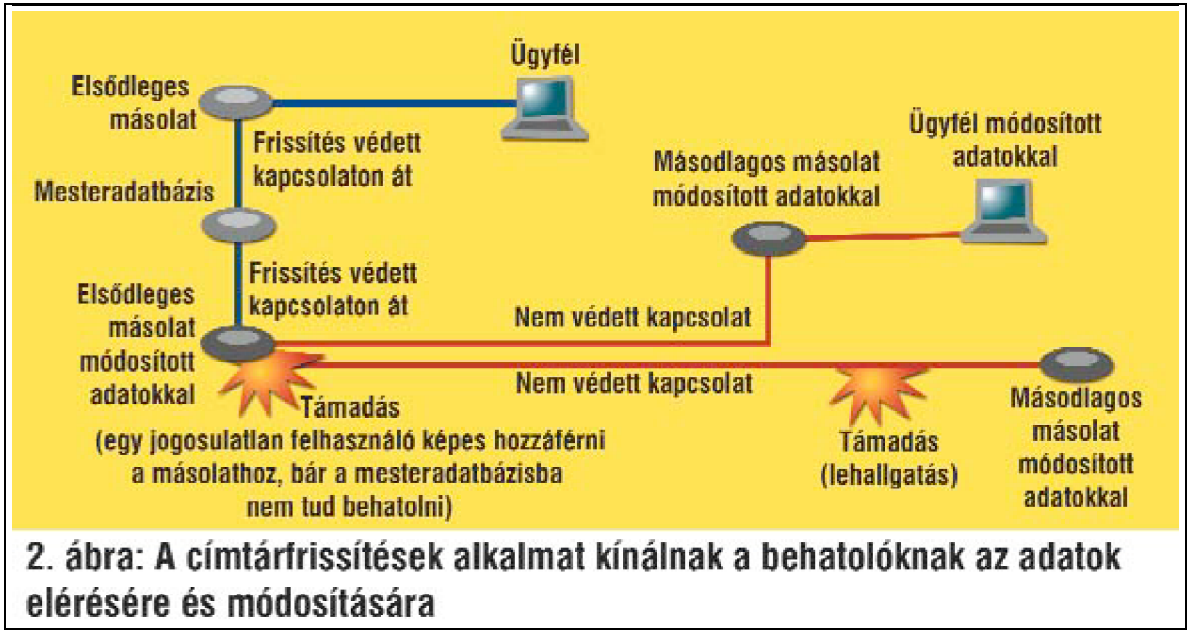
1. ábra: A man in the middle támadásnál a címtár és a felhasználó közé furakszik harmadiknak a betolakodó

A felhasználói nevek azonosításának biztonsága a Secure Sockets Layer (SSL) használatával javítható. Az SSL maszkolja a jelszót a hálózati forgalomban, így csökkenti a jelszólopás lehetőségét. Szintén segíthet, ha ezen kívül olyan jelszókezelő szoftvert használunk, amellyel különböző követelmények állíthatók be a jelszavakkal kapcsolatban (minimális jelszóhossz, betű–írásjel kombinációk stb.). A támadó sokféle jelszótörő programot és szótárt tölthet le a hackerek weboldalairól, így biztosra kell mennünk, hogy a felhasználóink nem használnak könnyen kitalálható jelszavakat. Fontos továbbá, hogy olyan jelszavakat lehessen előállítani, amelyek mindezek ellenére könnyen megjegyezhetők, tehát a felhasználók nem fogják őket sehová leírni. A teljesen véletlenszerű jelszó első megközelítésben jónak tűnik biztonsági szempontból, a gyakorlatban azonban azt szokta eredményezni, hogy a felhasználók leírják a jegyzetfüzetükbe (esetleg alkoholos filccel a monitor szélére), s ezzel nagy esélyt adnak a behatolásra.

Az SSL és egy megbízható jelszókezelő szoftver együttes használata a legtöbbször valószínűleg elegendő lesz. Noha ez a biztonsági szint közel sem tökéletes, könnyen megvalósítható, mégis nehéz feltörni. Ha ennél magasabb szintű biztonságra van szükségünk, használhatunk digitális tanúsítványokat vagy külső szolgáltató nyújtotta azonosítást.

Az SSL és a digitális tanúsítványok használata kellő biztonságot nyújt. A tanúsítványokkal igen magas szinten garantálható a biztonság és a felelősségre vonhatóság, a felhasználók nem tudják letagadni, mit csináltak. Ennek azonban megvan az a hátránya, hogy a növekvő funkcionalitás jelentősen növeli a szolgálati forgalmat, ami a teljesítmény rovására mehet. A tanúsítványok kezelése is több időt vesz igénybe. Ezzel együtt a digitális tanúsítványok használata megalapozott lehet, ha a címtár valóban érzékeny adatokat tartalmaz; amennyiben a biztonsági problémából adódó várható pénzügyi vagy jogi következmények ezt igazolják; ha a felhasználók olyan nagymértékben veszélyeztetett hálózaton keresztül érik el a címtárat, mint az internet; vagy ha a címtárat használók száma kevés. Amennyiben tanúsítványokat használunk, ajánlatos lehet beszerezni kriptográfiai gyorsítókat a teljesítmény növelése érdekében. (Ezek általában kiegészítő hardvereszközök, például különleges hálózati kártyák beépített kódoló funkcióval.)

Ha a vállalatnál már bevezettek biometriai vagy ujjlenyomat-azonosításon alapuló, fejlett azonosítási rendszereket, használhatják azokat a címtárak hozzáférésének szabályozásához is. Csupán ezért egy nagyvállalat valószínűleg nem vezeti be ezt a technológiát, de ha egyébként is használnak ilyet, megérheti a teljes integrációt elvégezni.



2. ábra: A címtárfrissítések alkalmat kínálnak a behatolóknak az adatok elérésére és módosítására

Természetesen a felhasználók azonosításának a célja nemcsak az, hogy tudjuk, ki dolgozik a címtárban, hanem az is, hogy megadhassuk, mihez férhet hozzá és mit csinálhat az adatokkal. A felhasználói jogosultságok kiosztása és a hozzáférés-ellenőrzés használata mellett biztosak lehetünk abban, hogy mindenki csak az őt illető információhoz juthat hozzá. Minden címtárrendszer gyártójának megvan a saját hozzáférés-ellenőrzési rendszere. Az IETF dolgozik az LDAP-kompatibilis címtárak szabványán, de ez egyelőre vázlatos állapotban van (megtalálható a www.ietf.org /internet-drafts/draft-ietf-ldapext-acl-model-06.txt címen Access Control Model for LDAP 3 név alatt). Ez a szabványjavaslat azonban aligha készül el 2001 közepénél előbb, így a címtár-hozzáférési és -jogosultsági beállítások tanulmányozása és a jogosultsági rendszer megfelelő összeállítása addig is a címtár tervezésének fontos eleme.

Kémelhárítás

A címtárhoz hozzáférést kérő felhasználók azonosítása fontos lépés, ám közel sem elég. Ahogy a vállalat elérhetővé teszi a címtárakat a belső hálózaton vagy az interneten (ez sok alkalmazásnak alapvető szükséglete), a rizikófaktor meredeken nőni kezd.

A várható támadások között van a „szaglálás”, angol nevén *sniffing,* ami tulajdonképpen a hálózati forgalom folyamatos lehallgatását jelenti. Ami adat a dróton áthalad, azt a támadó begyűjtheti: jelszavakat vagy bármi mást. A repülőgép-eltérítés mintájára itt a hálózati kapcsolatokat téríthetik el a támadók, a *connection hijacking* egy jogosult felhasználó forgalmának elterelése a támadóhoz, aki így a már feljogosított, kész kapcsolat fölött veszi át a hatalmat. A harmadik támadási forma a *man in the middle:* ennél a címtár és a felhasználó közé furakszik be harmadiknak a támadó, és miközben kínos pontossággal továbbít mindkét irányba minden adatot, hogy észre ne vegyék, az adatokat maga is elraktározza. Komolyabb esetben pedig bele is nyúlhat a kommunikációba és megváltoztathatja a felhasználó lekérdezését vagy a címtár válaszát (lásd az 1. ábrát).

E támadások bármelyike esetén a megfelelő figyelő-felügyelő rendszer nélkül a vállalat tulajdonképpen észre sem veszi, hogy támadás áldozata lett, vagyis információit úgy veszítheti el vagy úgy módosíthatják, hogy a támadón kívül senki nem tud róla.

A vállalat természetesen harcba szállhat ezekkel a veszélyekkel, ha kapcsolati szintű protokollokat használ, például az SSL-t, hogy biztonságossá tegye a kommunikációt. Ez a lépés felhasználói azonosítással is együtt jár, és használhatatlan vagy legalábbis nem azonnal rendelkezésre álló információt lehet csak lehallgatni a kommunikáció közben. A kódolószoftverek használatának árát persze meg kell fizetni időben, sávszélességben, így számos vállalatnál úgy vélik, a tűzfalon belül nincs szükségük ilyesmire. E döntés számos tényezőtől függ, és bár nem feltétlenül helytelen, a cégeknek nagyon is tudatában kell lenniük annak, milyen kockázatot vállalnak. Ahogy azt korábban már említettük a címtárakkal kapcsolatos aggályaink felsorolásakor, a vállalatnak jól meg kell fontolnia, kinek milyen információhoz ad hozzáférést, mekkora annak az esélye, hogy valaki más hozzá szeretne ehhez jutni – és hozzá tud-e jutni – és vajon mik lehetnek a következményei, ha ez sikerül neki.

A tervezési fázisban a vállalatnak át kell gondolnia azt is, hol legyen a címtár a hálózatban. Hol fog elhelyezkedni, hogyan fogják a rajta lévő adatokat frissíteni? A mestercímtár frissítése és az azt követő automatikus másolatkészítés újabb lehetőség a támadónak, hogy információkhoz jusson, így ezeket a pontokat jól kell védeni. Az elővigyázatosságot a konkrét helyzet határozza meg. A támadások az adatok megbízhatóságát és integritását egyaránt megzavarhatják (lásd a 2. ábrát). Hasonló támadások történhetnek más lehallgatási és kapcsolódási fenyegetések esetében. A biztonságos kommunikáció használata általában e veszélyeket a töredékére csökkenti, akárcsak a másolatkészítéshez használt dedikált vonalak.

A másolatkészítés biztonságának szavatolása mellett észre kell vennünk azt is, ha valaki a mestercímtárban módosít vagy töröl adatokat, hiszen ezek a változások a másolatokban is meg fognak jelenni, függetlenül attól, mennyire biztonságos a kommunikációs csatorna. Hasonlóképp a mestercímtárban tárolt információ is csak annyira jó, amennyire a forrása: ha a vállalat a címtárat például a dolgozók munkaügyi adatbázisából frissíti, az információforrás integritása is legalább annyira fontos, mint a biztonságos kapcsolat. Hogy milyen sebességgel terjednek a változások a frissítések során, az attól függ, milyen gyakori frissítéseket terveznek – ez pedig vállalatonként óriási eltéréseket mutathat.

Külön aggodalomra adnak okot a metacímtárak. Hiteles központi adattárként játszott szerepük rendkívül fontos, ráadásul összeköttetést teremtenek az eltérő címtárkörnyezetek között. Ha egy információ módosul valahol a címtárban vagy éppen a metacímtárban, a sérülés könnyen továbbterjedhet a különböző címtárakban, amelyek között ez a metacímtár szolgáltat összeköttetést.

További támadási pont – bár ezt gyakran elfelejtik –, hogy ha egy címtár helye fizikailag nem biztonságos, akkor a hálózattal kapcsolatos semmilyen biztonsági intézkedés nem lesz képes megakadályozni, hogy valaki egyszerűen kisétáljon az épületből a merevlemezzel… Hasonló a veszély akkor, ha akár csak egy terminál is szabadon hozzáférhető: bárki magasabb szintű jogosultságot szerezhet, mint ami jár neki. A múlt legendás hackerei sokszor meséltek olyan történeteket, amikor egyszerűen kértek valakitől egy jelszót vagy besétáltak az épületbe, és a kívánt információt az egyik ott lévő számítógépet használva szerezték meg. A fontos címtárakat biztonságosan őrzött szobában kell tárolni, célszerűen beléptető rendszerrel, belépési engedéllyel.

A biztonságiak

Még a legjobb biztonsági előírások és termékek sem garantálhatják, hogy a rendszer sosem fog betörési kísérlet áldozatául esni. Ezért figyelőszoftverekre, például egy megbízható behatolásérzékelő rendszerre, valamint hatékony auditálásra és analízisre van szükség. A megfigyeléssel kifürkészhetők a potenciális támadási pontok, az audit és az analízis a megtörtént incidensek elemzését, a biztonság kijátszásának lehetőségeit fülelheti le. A két módszer kombinációja segíthet kiértékelni a helyzetet és így javítani a biztonsági rendszeren. Számos gyártó ajánl menedzselt megfigyelési és audit szolgáltatást.

A vállalatok többnyire eldöntik, hogy házon belül üzemeltetik a megfigyelő és audit rendszert vagy hálózati alkalmazásaikat kiadják üzemeltetésre külső cégnek – nemcsak a címtárat, hanem egyben az egészet. Ahogy azt már számos cég felfedezte, jó biztonsági szakértőket nem könnyű találni. Az általános IT-szakemberhiányban jó néhány vállalat inkább kiadja ezzel foglalkozó szakértőknek a biztonsági funkciók egy részét, mint hogy házon belül próbáljon megoldást találni rájuk.

Konyhakész szoftverek

A címtárszolgáltatások gyártói várhatóan a jövőben megjelenő „konyhakész” szoftvereik biztonsági szolgáltatásait is folyamatosan fejlesztik – beleértve a biztonságos kommunikációs kapcsolatokat és a másolatkészítést. Ahogy a biztonságot a kommunikáció elválaszthatatlan részévé teszik, a címtárak sebezhetősé-ge a korábban említett támadásokkal szemben nagymértékben csökkenthető. A másik reménysugár, hogy a Microsofton kívül mások is megjelennek Kerberos alapú azonosítási eljárásaikkal.

Ugyanakkor egyre több gyártó ismeri fel, hogy a címtárak kiválóan illeszthetők a vállalat biztonsági architektúrájához, ahol segíthetnek megvédeni az alkalmazásokat és az információs erőforrásokat. A legtöbb cégnél a címtárak a felhasználói információk és profilok tárolásának eszközei. Ebben a helyzetben a címtár kulcsszerepet tölt be a biztonság felhasználókra „kényszerítésében”, minthogy a címtár tárolja a felhasználó adatait és jogosultságait.

Az olyan gyártók, mint a Tivoli, az Entegrity, a Securant, a Netegrity vagy az Entrust, mind ajánlanak termékeket a hozzáférés ellenőrzésére és a jogosultságok kezelésére a vállalat hálózatának tetszőleges részeire vonatkoztatva. A címtár tárolja a felhasználói profilokat és olykor a tanúsítványokat és a jogosultsági információt is. Valamely hozzáférés-vezérlő döntéshozó mechanizmus elérheti ezt az információt, hogy megnézze, engedélyezheti-e a felhasználó hozzáférését, amikor az egy másik erőforráshoz próbál kapcsolódni. Így a címtár kulcsszerephez jut a vállalat biztonsági információinak tárolásában. Számos cég már jelentős felhasználói címtárakat épített fel, ezek a termékek pedig lehetővé teszik számukra, hogy a befektetést kihasználhassák a web és a hálózati hozzáférés biztonságosabbá tételére.

*Robin Mejia **(rjmejia@pacbell.net)** biztonsági szakértő. Peter Lindstrom (plindstrom@hurwitz.com) vezető analitikus a Hurwitz Group Security Strategies Service-énél.*

Forrás: Network Computing, a CMP Media, Inc. kiadványa.

HOL TALÁLHATÓ

Rengeteg hasznos biztonsági információval szolgál a Security Portal *(www.securityportal.com)*.

Gyakran előforduló kérdésekre kaphatunk választ a Password Cracking honlapján *(www.password-crackers.com),* amely egyszersmind ugródeszkául szolgál az újdonságokhoz és a letölthető jelszótörő programokhoz.

A négy LDAP modellt *Tim Howes, Mark Smith* és *Gordon Good* könyve, az *Understanding and Deploying LDAP Directory Services* alapján készült kivonat segítségével idéztük fel. Mindhárom szerző a Netscape munkatársa. A kivonat a *developer.netscape.com/viewsource/ldap_models/ldap_models.html* címen található.

Jeff Hodges bemutatója az LDAP címtárak biztonságáról és egy kiváló hivatkozásgyűjtemény található a *www.stanford.edu/~hodges/talks/WebSec99/DirectoryServiceSecurity-1999-08-11/* címen.

2001. FEBRUÁR / CÍMLAPSZTORI / Címtárak a biztonságért

Címtárak a biztonságért

A vállalatok jó néhány biztonsági területen használják a címtárakat mint egyedüli megoldást. A címtárak valószínűleg legismertebb felhasználási módja a biztonsági területen a PKI.

A digitális tanúsítványok titkosítással védett, online bizonyítványok, amelyek egyfajta kitűzőként vagy útlevélként viselkednek. E tanúsítványoknak kezelhetőeknek és elérhetőeknek kell lenniük, hogy hasznukat lehessen venni. A PKI a digitális tanúsítványokat teljes életciklusukban menedzseli, online regisztrációt, kulcskészítést, tanúsítványfrissítést és -visszavonást kínálva. A PKI címtárakat használ a tanúsítványok közzétételére és hitelesítésére oly módon, hogy ellenőrzi a hitelesítő hatóságot (Certificate Authority, CA) és átnézi a visszavont tanúsítványok listáit (Certificate Revocation List, CRL). A PKI és a címtár-technológiák együtt gondoskodnak a megfelelően bizalmas kezelésről (titkosítás) és az integritásról (digitális aláírások), a meg nem tagadhatóságról (digitális aláírások) és a hitelesítésről (felhasználói bejelentkezés). Amikor a címtár részeként fontolóra vesszük a PKI-t, figyelembe kell venni a címtár hierarchiájára gyakorolt hatását is. Egy több szinttel és tárolóval ellátott hierarchikus struktúra megkönnyíti a feladatok elkülönítését (a fa egy ágának kezelése, és átláthatóbbá teszi a kezelést, ha a vállalat szervezeti vagy földrajzi felépítésével összhangban építik azt fel.

Ugyanakkor a vállalatoknak gyakran kell módosítaniuk a hierarchikus struktúrát kisebb szervezeti változások esetén, felvásárlások, eladások alkalmával. Minthogy a PKI címtár függ a CA helyétől a fában, állandó, egyszerű struktúrát igényel. A fastruktúra módosítása akár a vonatkozó tanúsítványok visszavonásával és ismételt kiadásával is járhat.

2001. FEBRUÁR / CÍMLAPSZTORI / Encryption Plus for Hard Disks

Encryption Plus for Hard Disks

A vállalati szintű titkosítás hasznos, könnyen kezelhető eszköze a PC Guardian programja. Nem minden cégnek van szüksége az általa kínált magas szintű biztonsági

szolgáltatásokra. Ha azonban bizalmas információkat tárolunk nem külső támadásnak kitett helyeken (például noteszgépeken), az Encryption Plus for Hard Diskssszel egyszerűen védhetjük meg adatainkat.

Ha egy noteszgép rossz kezekbe kerül, azzal a vállalat belső adatai is kiszivároghatnak. A merevlemez tartalmának titkosítása, kódolása segíthet, de vajon megbízhatunk-e alkalmazottainkban, hogy rendszeresen cserélik a jelszót, olyan jelszót választanak, amelyet nem lehet egykönnyen kitalálni és nem utolsósorban hogy emlékezni fognak a jelszavaikra?

A PC Guardian Encryption Plus a rendszer-adminisztrátorok munkáját segíti, megfelelő jelszókezelés használata írható elő vele a windowsos gépeken. A programot igazán egyszerű beállítani – akár a rendszergazdáknak, akár az egyszerű felhasználóknak – és munka közben tapintatosan félrehúzódik az útból.

Decemberben kiadták az Encryption Plus for Hard Disks 6.1-es változatát. A Windows 2000 kezelésén kívül semmi igazán új nincs benne.

KONFIGURÁLÁS

Adminisztrátorként telepítjük a főprogramot a saját számítógépünkre, majd egy varázsló futtatásával állíthatjuk be a vállalati szintű alapértelmezett értékeket. Ezek magukban fog kiválasztásakor.

Például kiköthetünk minimális jelszóhosszt a felhasználóknak, kötelezően előírhatjuk valamilyen különleges karakter (például a @ vagy a #) használatát a jelszóban, beállíth próbálkozhat jelszavának kitalálásával a feledékeny felhasználó.

Végül a varázsló teljesen új példányt készít a programból, amely a választott beállításokat tartalmazza. Ha a felhasználók ezt telepítik a gépükre, máris szabad a pálya merevlemezük

Az Encryption Plus a Blowfish eljárást használja az adatok kódolására, amely hangzásában akár egy James Bond-filmben szereplő név is lehetne, valójában azonban a ma létező elemzője.

DEKÓDOLÁS A HÁTTÉRBEN

Indítsunk el egy, az Encryption Plus által védett merevlemezű gépet hajlékonylemezről, és az a háttértárolón nem talál semmit a digitális szemeten kívül. De indítsuk el magáról a mer

Az Encryption Plus háttérprogramja – amely menet közben, „röptében” kódol és dekódol – a mester rendszerindító rekordból indul még a Windows előtt. A Windows teljesen normál

Minden olyan programnak, amely ennyire hardverközelben dolgozik, vannak kompatibilitási problémái. Az Encryption Plus összeütközésbe kerülhet azokkal az alkalmazásokkal, am

Ha a gépben egynél több merevlemez van, akkor egyiket sem fogja kódolni a program. Ha a lemez titkosított, egy második lemez hozzáadása a rendszerhez már nem fog problémát je

Miként befolyásolja ez a háttérkódolás a teljesítményt? A logikus gondolkodás szabályai szerint az ilyen alacsony szinten futó programnak, amely minden olvasást és írást feldolgoz,

Saját méréseink szerint az Encryption Plus for Hard Disks igazából javított a teljesítményen – körülbelül 8 százaléknyit! A PC Guardian ugyan nem tudott magyarázatot adni a dolog

Egyetlen dologra nem alkalmas az Encryption Plus: internetes biztonsági eszköznek. Nem lehet ugyanis azt megállapítani, hogy egy állománykérés a billentyűzeten dolgozó 1 amelyeknél az irodán belüli „leskelődés” problémát okozhat vagy ahol a számítógépek ki vannak téve a lopás veszélyének. Ezek után nem túl meglepő a PC Guardian azon bejelentés

GYORS HELYREÁLLÍTÁS

A védelemnek mindig megvan az ára: ha egy felhasználó elfelejti a jelszavát, nem tud hozzáférni a kódolt adatokhoz. Az Encryption Plus erre két megoldást kínál: egy vállalati az adatok. Használható ezenkívül még egy One-Time Password program az egyszeri alkalomra szóló jelszóval, amelyet az Encryption Plus adminisztrátori változatával lehet elk felhasználón.

Nem minden számítógépben van szükség ilyen szintű védelemre – és szinte nincs olyan vállalat, amelyiknek minden gépét így kellene védeni. De ha van olyan érzékeny informá

ezek biztonságba helyezésének.

Lincoln Spector

Forrás: Network Computing, a CMP Media, Inc. kiadványa.

2001. FEBRUÁR / KERESŐ Mobiltelefónia

KERESŐ
Mobiltelefónia

2001. FEBRUÁR / KERESŐ Mobiltelefónia / Szabványok háborúja

Szabványok háborúja

Az Egyesült Államok mobiltelefon-szolgáltatói háborúban állnak Európával és Japánnal a mobilszabványokkal kapcsolatban, de a kínai kártya mindegyiküket lesöpörheti.

Szerző: Jonathan Collins

Az amerikai mobilszolgáltatók árgus szemekkel figyelik Kínát, hogy saját jövőjükbe láthassanak. A hidegháborúban méretével és erejével erős tényezőként szerepet játszó birodalom most hasonlóan központi szereppel bír a mobiltelefóniás világ versenyében. A verseny kimenetele mind az Egyesült Államokban, mind világszerte átrajzolhatja a nagy mobilszolgáltatók küzdőterét.

A harcot az amerikai, illetve a japán és az európai tábor mobiltelefónia-szabványainak eltérése határozza meg. Ha nem is annyira végzetes fontossággal, mint a nukleáris fegyverek felhalmozása, Kína mobiltechnológiai választása keményen meghatározhatja a mobiltelefónia-szolgáltatók és -berendezésgyártók kiadásainak és bevételeinek sorsát. Bármelyik technológiát választja is Kína kormánya, a felhasználók óriási száma miatt az lesz gazdaságos a szolgáltatóknak, figyelembe véve a nagyobb termelési volument és a nagyobb piaci lehetőségeket. A tét óriási a mobiltelefóniás verseny amerikai résztvevői számára: Kína megnyerése nélkül számos egyesült államokbeli szolgáltató elveszítheti nemzetközi jelenlétét.

Különösen nagy aktualitást ad a témának, hogy a mobilvilág a harmadik generációs technológia felé halad. Miközben a harmadik generációs mobilhálózatok azt ígérik, hogy a technológiák száma négyről kettőre fog csökkenni, addig egy újabb globális ellentétpár jelenik meg.

Riválisrendszerek

Az egyik oldalon áll a CDMA2000, a CDMA, a kódosztásos többszörös hozzáférés legújabb változata, amelyet a San Diegóban székelő Qualcomm fejlesztett ki és az Egyesült Államok vezető szolgáltatói alkalmaznak. A másik oldalon a Nemzetközi Távközlési Unió (ITU) keretében kifejlesztett, szélessávú CDMA (W-CDMA) áll. Ez utóbbi két európai szabvány – a GSM (Global System for Mobile Telecommunications) és a TDMA, az időosztásos többszörös hozzáférés –, valamint a japán PDC (Personal Digital Cellular) technológia továbbfejlesztése. A két oldal között nincs átjárás, bár mindkét technoló-giát Qualcomm-szabványok alapozták meg.

Ennek a világszínpadon zajló politikai háborús előadásnak nem lett volna szabad bekövetkeznie. Arra számítottunk, hogy a harmadik generációs technológia bevezetése a

mobiltelefóniát a teljes körű harmónia felé vezeti. A Nemzetközi Távközlési Unió égisze alatt az üzemeltetők és a berendezésgyártók olyan csatolószabványt határoztak meg, amely globális hézagmentes hozzáférést képes nyújtani a nagy sebességű adat- és hangszolgáltatásokhoz.

Az egységes szabvány azt jelentené, hogy a K+F forrásokat egyetlen, nagy felvevőképességű piacra lehetne összpontosítani, kisebb fejlesztési kiadásokkal terhelve a gyártókat. A szolgáltatók a hálózataikon barangolásból eredő nagyobb bevételben reménykedhetnének, hiszen a felhasználók külföldi útjaikon is használhatnák mobilkészülékeiket. Több lehetne a felhasználó is, hiszen csökkenne a készülékek ára, a teljes körű hozzáférés pedig vonzóbbá tenné ezt a technológiát.

Egyes gyártók és üzemeltetők ellenállása azonban akkorának bizonyult, hogy az egységes szabvány helyett harmadik generációs technológiacsalád született, és két kihívó áll szemben egymással. Annak ellenére, hogy több szervezet is, legalább öt évig, próbálkozott az elhárításával. „Egy sor politikai ügy volt, olyan ügyek, amelyek az egységes szabványba az Európa kontra Egyesült Államok gondolatát látták bele, és megakadályozták, hogy egységes szabvány jöhessen létre” – állítja *Bharat Shah,* a Qualcomm fejlesztési igazgatója.

Harc a piacokért

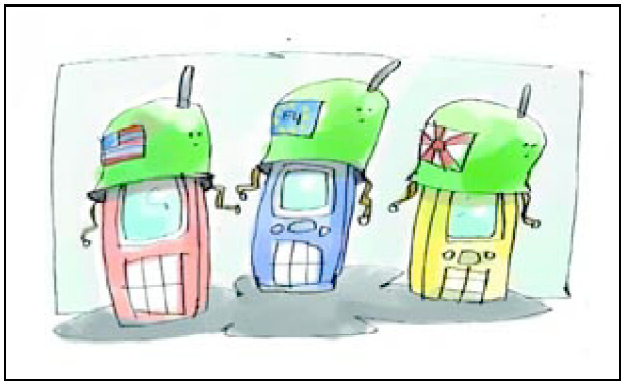
Most, a két szabvány korában, csökkent a globális barangolás lehetőségének valószínűsége, és mindkét fél a még döntés előtt álló piacokra hajt. Az a technológia élvezi majd a kisebb gyártási költségek előnyeit, amelyik több piacot és több felhasználót szerez.

„Ha növekszik a forgalom, olcsób-bak lesznek a berendezések. Ehhez jön a berendezést fejlesztő üzemeltetők növekvő tapasztalata” – véli *Ake Persson,* a Texas állambeli Ericsson mobilkommunikációs ágazatának elnöke.

Ezért figyelnek Kínára az Egyesült Államok szolgáltatói. „Kína az utolsó nagy piac – jelenti ki *Kelly Quinn,* a bostoni Aberdeen Group vezető elemzője. – Ha a CDMA-nak nem sikerül itt megkapaszkodnia, ez a CDMA mint világszabvány végét jelenti.”

Kína két szempontból is jelentős. Egyrészt több mint egymilliárdos lakosságával a világ potenciálisan legnagyobb mobilpiaca. A prognózisok szerint a felhasználók száma ez év elején 70 százalékkal nőhet. Másrészt – ellentétben a jelenleg nagyobb két piaccal, Japánnal és az Egyesült Államokkal – Kína még éppen hogy elindult a mobillefedettség irányába. S mivel gyenge a vezetékes ellátottsága, jóval nagyobb igénye lesz a mobilkommunikációra.

Bár nagyjából ugyanannyi mobil-előfizető van az Egyesült Államokban és Kínában, az utóbbinak tágabb tere van növekedni: 2000 végére várhatóan 70 millió mobil-előfizetője lesz. Az Egyesült Államokban az előfizetők száma az évezred végére éppen meghaladja a 100 milliót, de ez száz lakosra harminc készüléket jelent. Kína 70 millió felhasználója csak a lakosság 5,6 százalékát fedi le. Ha majd 2005-ig Kínában újabb 162 millió előfizető jelenik meg, az akkor is csak 17,8 százalékos lefedettséget fog jelenteni. A kínai piac méretéből fakadóan amely cég technológiájával az ország szövetkezik, döntő előnyt szerezhet a vezeték nélküli világuralomért vívott csatában.



Bár az elemzők szerint ha Kína a másik tábort választja, az Egyesült Államok szolgáltatói és a CDMA technológia veszítheti a legtöbbet, az érintett szolgáltatók, nem meglepő módon, cáfolják a veszélyeket. „Tekintettel Kína nagyságára, jól jönne, ha a CDMA-t fogadnák el, de az sem zavarna minket, ha nem – mondja *Oscar Valente,* a Montana állambeli Sprint PCS vezető műszaki szakembere. – A CDMA a leggyorsabban fejlődő technológia, és túllépte már a kritikus tömeget, hogy profitálhasson a piac méretéből." A számok mindamellett nem feltétlenül támasztják alá Valente kijelentését. Az átfogó mobilpiac máris aszimmetrikus. A massachusettsi Cahners In-Stat Group elemzése szerint három GSM bázisállomás jut egy CDMA bázisállomásra. Ez azt jelenti, hogy a W-CDMA teljesen a CDMA2000 fölé kerekedik, hacsak a Qualcomm CDMA-ja nem kapaszkodik meg a kínai piacon.

Területi megosztottság

Az Egyesült Államokban működő TDMA-üzemeltetők, az AT&T, a BellSouth és az SBC Communications mind a W-CDMA felé tartanak. Ráadásul a saját PDC technológiáját használó japán NTT Mobile Communications Network is már régóta a W-CDMA erős támogatója, akárcsak az európaiak. Mindez nem jelenti azt, hogy a CDMA-nak nincs jövője. Jelenleg jó néhány előfizetője van, és a berendezések árai együtt haladnak a GSM- és a TDMA-infrastruktúráéival.

A CDMA különösen erős az Egyesült Államokban és Koreában, de elterjedt Latin-Amerikában is. A legnagyobb piac Korea, ahol a kormány előírja, hogy az országban minden mobilhálózatot CDMA alapon kell kiépíteni. Ez azonban megváltozhat, amikor a hálózatok a harmadik generációs technológiákhoz idomulnak. A harmadik generációs frekvenciasávok három fő várományosa – az SK Telecom, a Korea Telecom és az LG TeleCom – már felvetette, hogy átáll a W-CDMA-t alkalmazó harmadik generációs szolgáltatásra. Az Egyesült Államokban mindeközben a Sprint PCS és a New York állambeli Verizon Wireless – az ország legnagyobb mobilüzemeltetője 25 millió előfizetővel – CDMA technológiát használnak digitális előfizetőiknél. Mindkét cég kinyilvánította elkötelezettségét a CDMA2000 kibontakoztatására a következő néhány évre, és mindketten a CDMA legerősebb támogatói.

„Reméltem, hogy a Vodafone befolyása a Verizon Wirelessben (a Vodafone birtokolja a cég 45 százalékát) elmozdítja a Verizont a W-CDMA irányába. Ezzel a cég megszerezhetné azt a mintegy 40 ezer európai üzletember-előfizetőt, aki hetente megfordul az Egyesült Államokban. De reményem elhalt, amikor a cég bejelentette a CDMA2000 lelkesült támogatását" – nyilatkozza *Ray Jodoin,* a Cahners elemzője.

Jodoin szerint a Verizon tévedése alkalmat teremt a Washington állambeli VoiceStream amerikai GSM-üzemeltetőnek. A VoiceStream nemrégiben beleegyezett, hogy felvásárolja a Deutsche Telekom, amely agresszíven fejleszti W-CDMA hálózatait európai piacain. Hasonló várható az Egyesült Államokban is, ha az eladási tender sikerre vezet. „Ha szokásom lenne fogadásokat kötni, egy csomó pénzt tennék a VoiceStreamre" – nyilatkozza Jodoin.

A dolgok jelenlegi állása nem valami rózsás az amerikai szolgáltatók számára. Kínában most hetvenmillió előfizetőből jóval kevesebb mint egymillió használ CDMA alapú hálózatot. A meghatározó technológia a GSM. A Qualcomm azonban, amelynek a legtöbb nyernivalója van a CDMA technológián, keményen dolgozik, hogy elfogadják és Kína-szerte alkalmazzák azt. A Qualcomm erőfeszítéseit támogatja az Egyesült Államok kormánya is, és úgy látszik, a cég időnként már a siker küszöbén áll.

Az év elején az Egyesült Államok kormánya Kína azon kívánságának támogatását, hogy bejusson a Világkereskedelmi Szervezetbe (WTO), számos feltételhez kötötte. Az egyik a Qualcomm CDMA technológiájának engedélyezendő frekvenciasáv volt. A megegyezés biztosnak tűnt, mivel a Qualcomm el-fogadta az engedélyezési feltételeket. Mindazonáltal kevesebb mint két héttel azután, hogy Kína elnyerte az Egyesült Államok támogatását a WTO-ba való felvételhez, a pekingi székhelyű, kínai állami tulajdonú China Unicom megerősítette, hogy minden CDMA-fejlesztést leállítottak.

Előnyök, hátrányok

Egyelőre nem világos, hogy végül is min alapul a kínai döntés és mennyire megalapozott, hogy más piacról vegyenek technológiát. A különféle technológiák támogatói szívesen jelentik ki, hogy az ő technológiájuk a legjobb: a hatékonyabb spektrumhasználattól az olcsóságon át a gyorsabb és könnyebb telepíthetőségig. A PCS-es Valente szerint a CDMA „jobb spektrumkihasználású" versenytársainál, és túl hosszadalmas a W-CDMA telepítése annak ellenére, hogy a mérnökök több mint öt évig dolgoztak rajta.

Ha viszont *John Zeglist* hallgatjuk meg az AT&T Wirelesstől, akkor egészen más képet kapunk. Szerinte nem igazak a rossz spektrumkihasználásról szóló állítások, és az embereknek nem szabad elhinniük a „hittérítést" arról, hogy a CDMA olcsóbb, mint a TDMA. Mindkét technológia az internetprotokoll (IP) felé tart, és – állítja Zeglis – itt a W-CDMA lesz a jobb.

Bármennyire valósak a technológiák különbségei, egy sereg elemző véleménye szerint nem ezek a kulcstényezők az üzemeltetők vásárlási döntéseiben. „Jelenleg a CDMA és a GSM/TDMA berendezések ára nagyjából azonos, a spektrumkihasználás teljesen megegyezik és a hívások minősége is egyforma. Nem a technológia a vita igazi tárgya. Ez inkább politikai játszma a gyártók között" – véli a Massachusetts állambeli Pyramid Research igazgatója, *Godfrey Chua*.

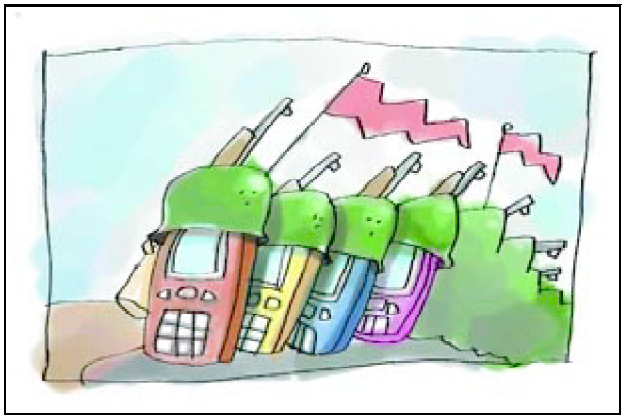
Megszerezni a technológiát

Kína következő lépése várhatóan az lesz, hogy javítsa jövőbeli helyzetét. „Minden harmadik generációs ügyben arra törekszenek, hogy a szolgáltatások legfejlettebb szintjén legyenek" – jelenti ki Chua.

Kína választása attól is függ, mennyire veszi figyelembe a nemzetközi barangolást, ami sokak számára a nemzetközi szabvány lényege. A W-CDMA azt ígéri, hogy használói hozzáférhetnek a szolgáltatásokhoz egész Európában, Japánban és Ázsia nagy részén. Mivel az Egyesült Államok GSM-szereplőinek többsége a VoiceStreamre tett, és várhatóan ezt a céget megveszi a Deutsche Telekom, bizonyosra vehető, hogy létrejön egy országos W-CDMA hálózat az Egyesült Államokban. Ezenfelül a TDMA szereplői elindultak a W-CDMA felé vezető úton, miután felfejlődnek az Enhanced Data GSM Environment (EDGE) szabványra.

A második generációs GSM szolgáltatás bázisáról a W-CDMA-ra lépve Kína jövedelemhez jut a GSM/W-CDMA telefonjaikat használó utazóktól, és telefonjai használhatók lesznek a tengerentúlon is. „Bár igencsak különbözők a piacok, mind Korea, mind Kína erősen törekednek harmadik generációs rendszerek kiépítésére, amelyek teljes körű barangolást nyújtanak. Ez a W-CDMA-nak kedvez" – említi meg Jodoin.

Chua szerint viszont Kínának nem a barangolás, hanem az alaptechnológia megszerzése a célja. Kína kétségbeesetten szeretné alkalmassá tenni magát a mobilberendezés-gyártó üzletre. Ennek sikeréért pedig alkalmasnak kell lennie arra, hogy hozzáférjen a külföldi gyártók által kifejlesztett technológiákhoz.



ILLUSZTRÁCIÓ: BUTTINGER GERGELY

„Valószínűleg az a fél nyer, amelyik hajlandó lesz a legtöbb technológiát átadni Kínának. A csapda abban rejlik, hogy ha Kínának meglesz a technológiai tapasztalata, arra használhatja olcsó munkaerejét, hogy ő legyen a legolcsóbb telefonkészülék-gyártó, amivel éles versenyt támaszt a többi gyártónak. Ha Kína a CDMA-t választaná, elsősorban azok a koreai és egyesült államokbeli üzemeltetők húznának hasznot az olcsó készülékekből, amelyek már kiépítették CDMA-hálózataikat. A CDMA-piac szereplőinek telefonkészüléket gyártók száma igencsak korlátozott, szemben a sokkal nagyobb számú GSM telefongyártóval. A sok gyártó segíti a felhasználói választást. A CDMA-nak egyszerűen nincsenek gyártói."

Feltehetően ezért törekszik a Qualcomm arra, hogy gyorsan bejusson Kínába. Egy, a China Unicommal aláírt szerződés részeként a Qualcomm licencelte a CDMA szellemi tulajdonjogát 12 kínai gyártónak. Közülük tíz hálózati berendezéseket és telefonkészülékeket is fog gyártani, kettő pedig csak készülékeket. Mivel telefonkészülék és hálózati berendezés üzletágát már eladta a japán Kyocerának és az Ericssonnak, a Qualcomm nem sokat veszíthet azon, ha megnő a kínai berendezésgyártás. A cég a minden CDMA termékre vonatkozó jogaiból és a W-CDMA termékekből fog hasznot húzni.

Kínának már 23, hivatalosan bejegyzett mobiltelefon-gyártója van: 2000 első negyedévében 9,08 millió készüléket gyártottak, amelyből 8,82 milliót adtak el. Ez az előző évihez képest 177, illetve 162 százalékos növekedés. A kínai piacot azonban egyelőre három külföldi gyártó uralja: a Nokia, az Ericsson és a Motorola együttesen a mobiltelefon-piac 90 százalékát birtokolja.

Hintapolitika

Minden mérlegelés és spekuláció mellett az amerikai szállítók már láthatták, Kína milyen gyorsan lendült oda-vissza a döntései között. A kínai kormány el sem fogadta és el sem vetette a CDMA-t. És az elemzők erősen aláhúzzák, hogy bármilyen, CDMA-t elutasító döntés visszavonható. Kína olyan döntési helyzetben van, hogy – Chua szerint – „bármikor kiugorhat. Az eladók tudnak várni." Sőt, az is elképzelhető, hogy a kínai kormány beleegyezik mindkét technológia elterjesztésébe.

Annak egyik útja, hogy az Egyesült Államok és más országok szolgáltatóit a legkevésbé érintse Kína döntése, az lehetne, hogy kezdjenek önkéntesen technológiát váltani és egy csapatba tömörüljenek. Egyesek úgy vélik, hogy a már piacon lévő GSM és TDMA mobilüzemeltetők hajlanának arra, hogy CDMA2000-re váltsanak, amikor bevezetik harmadik generációs szolgáltatásukat. „Akárhogy is nézzük, ez nem stabil piac. Az üzemeltetők vallásos hittel választanak technológiát: a beruházás legjobb megtérülését várják. Akadnak például olyan európai GSM-szolgáltatók, amelyek Latin-Amerikában CDMA hálózatot építenek" – említi meg az ericssonos Persson.

Más elemzők viszont azt állítják: igencsak valószínűtlen, hogy bármely üzemeltető a rivális technológiára való átállást válassza. „A technológiaváltás túl költséges, különösen ha azt már bevezették és a piac növekedőben van” – véli Chua.

Az Ericsson elismeri magáról, hogy bár a technológiaváltás lehetséges, jelenleg nem fejleszt ezt lehetővé tévő terméket.

Mivel Kína döntésének nincs ismert határideje, a világ lélegzet-visszafojtva figyel, és a szolgáltatók azt lesik feszülten, hogy piacuk fellendül vagy hanyatlik. Egy dolog semmiképpen nem fog hamar megváltozni: az, ahogy a felek a tétjüket védelmezik. Amíg a tétnek marad esélye, a zavaros helyzet fennmarad.

Jonathan Collins **(johncollins@cmp .com)** a wireless for tele.com főszerkesztője.

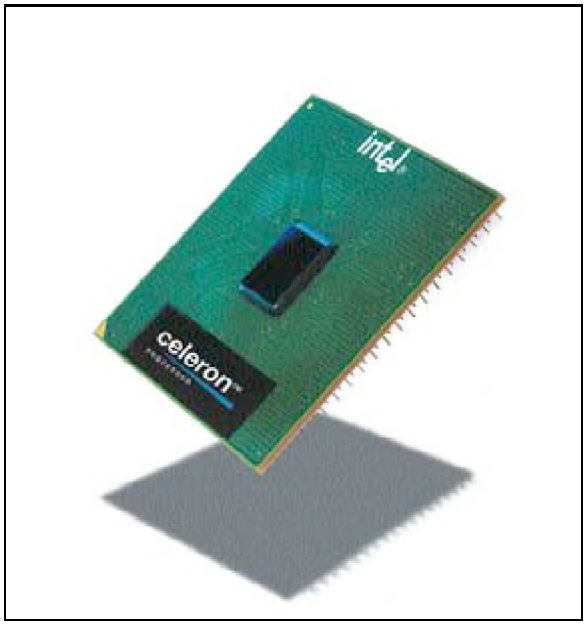
Forrás: tele.com, a CMP Media, Inc. kiadványa.

ÚJDONSÁGOK

HARDVER

800 MHz-es Celeron

Olcsó PC-khez szánt új processzort és lapkakészletet fejlesztett ki az Intel. A 800 MHz-es lapka az első olyan Celeron, amely a szélesebb kommunikációs csatornát nyújtó 100 MHz-es rendszersínt használja. A 810E2 jelű lapkakészlet kezeli a nagy sebességű sínt és lehetővé teszi új technológiák bevezetését az alsó kategóriájú PC-knél. Ezek közé tartoznak a továbbfejlesztett I/O hub, az ATA-100 Ultra DMA merevlemez-meghajtók, valamint az új USB vezérlők, amelyek négy plug-and-play kaput kezelnek különféle rendszereszközök csatlakoztatásához. Az Intel bejelentett két új alaplapot – a microATX D810E2CA3-at és a FlexATX Desktop Board D810E2CB-t – is OEM-gépekhez. Az alapkártyák a Pentium III és a Celeron lapkákat egyaránt fogadni tudják. A Celeron processzorok jelenleg 800 (100 MHz-es rendszersín), 766, 733, 700, 667, 633, 600 és 566 MHz-es változatban kaphatók.



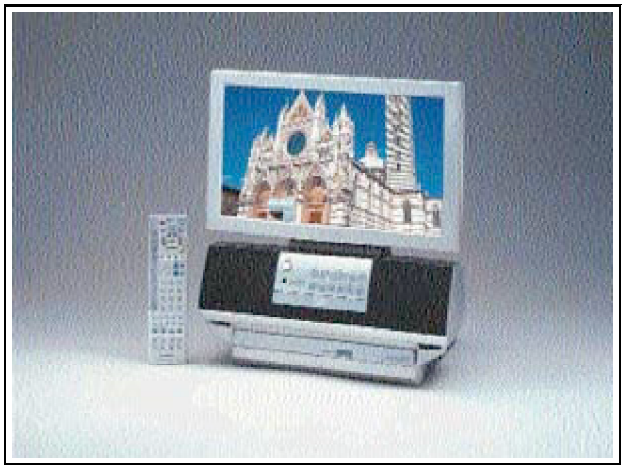
MP3 lejátszó az Inteltől

MP3 és Windows Media Audio (WMA) formátumú, négyórányi zenei programot és több mint húszórányi beszédhangot képes tárolni 128 MB-os flash me-móriájában a Pocket Concert Audio Player. Opcionális kiegészítőként otthoni sztereó dokkot és autós audioadaptert tartalmazó Audio Accessory Kit vásárolható hozzá.

www.intel.com

Netezés távvezérlővel

DVD-lejátszóval és internetböngészővel ellátott LCD-képernyős digitális tévérendszert dob piacra a Panasonic. A 15,2 hüvelykes képátmérőjű berendezés februárban jelenik meg a japán piacon. HDTV-műsorokat, datacastingot és BS digitális rádióműsorokat, valamint a kézi távvezérlővel internetes szolgáltatásokat lehet elérni vele. Az e-mailek küldése, fogadása és a webböngészés a távvezérlővel bonyolítható, billentyűzetre nincs szükség. A tévé D-VHS videomagnóhoz csatlakoztatható, a beépített i.LINK terminál segítségével a BS digitális műsorok egyszerűen felvehetők és visszajátszhatók. A DVD-kamkorderek és a digitális kamerák állóképeinek rögzítése ugyancsak az i.LINK csatolóval történik.



Információ: Panasonic Magyarország Kft.

Tel.: 382-6060.

Power Mac G4

A januári Macworld Expón az Apple bemutatta a 133 MHz-es rendszerbuszra épülő Power Mac G4 termékcsaládot. A Power Mac G4 képes a CD-RW lemezek kezelésére, a legnagyobb teljesítményű változatban található SuperDrive meghajtó pedig még DVD-t is képes írni. A gépekhez adott iDVD szoftverrel egy gombnyomással készíthetők DVD-Video lemezek mindenféle iMovie, Final Cut Pro és QuickTime anyagból. A konverziót az iDVD végzi el. Az iTunes szoftverrel az MP3 állományok rendszerezhetők, CD-ről vett dalok kódolhatók MP3 formátumban, dalok tölthetők fel MP3 lejátszó készülékekre. Az új modellek négy konfigurációban lesznek kaphatók Magyarországon.

Apple Hungary IMC (HDSys Kft.) Tel.: 250-3260 www.apple.hu

X-box

Januárban *Bill Gates* mutatta be az X-Box játékkonzolt, amelyet több mint ötezer videojáték-rajongó és játékprogram-fejlesztő visszajelzéseinek figyelembevételével terveztek. A konzolon egyebek közt négy vezérlőbemenet, hang- és videokimenet, az online játékhoz szükséges csatlakozó, NVIDIA grafikus egység található; lelke az Intel 733 MHz-es

processzora. A Microsoft játékkonzolt Magyarországon és Mexikóban fogják gyártani. A magyar üzem hozzávetőleg hárommilliárd dolláros GDP-növekedést jelent az ország számára. Az X-box 2001 őszén lesz kapható az Egyesült Államokban és Japánban, míg az európai megjelenésre 2002 első negyedévében lehet számítani.

Microsoft Magyarország. Tel.: 437-2800

E-mail: ***petker@mic***

rosoft.com

2001. FEBRUÁR / ÚJDONSÁGOK / SZOFTVER

SZOFTVER

Ingyenes PalmOS 3.1H

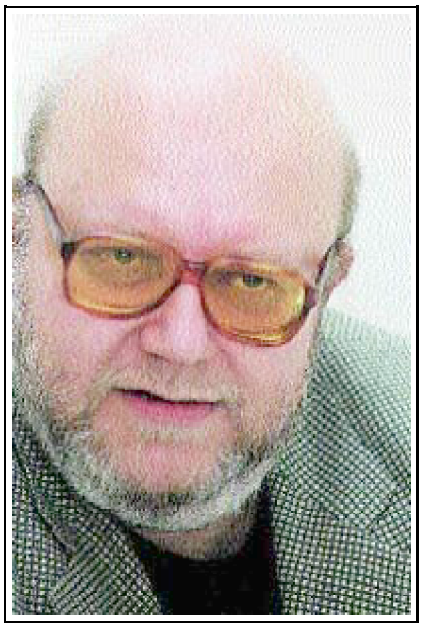
A HDSys Kft., a Handspring magyarországi képviselete és a Paragon Ltd. *(www.penreader.com)* magyarította a Handspring Visor tenyérszámítógépek PalmOS 3.1H operációs rendszerét. A szoftver és a telepítési leírások a *www.handspring.hu* oldalról tölthetők le. A szoftver ingyenes minden Handspring Visor-tulajdonos számára, de ez a változat nem fut a Palm, IBM, TRG pro vagy Sony tenyérszámítógépen. A PalmOS 3.5H magyar verzió Handspring Visor Platinum és Prism gépekre februárban jelenik meg.

Hungarian Data Systems Kft., Tel.: 250-3260 www.hdsys.hu

SZABAD SZEMMEL
Kis János rovata

2001. FEBRUÁR / SZABAD SZEMMEL Kis János rovata / Mennyi is az ingyen?

Mennyi is az ingyen?



FOTÓ: SEBESTYÉN JENŐ

Magyarországon több testhosszal győzött az ingyen-Net, miután elindította szolgáltatását két ingyenes internetszolgáltató. A Kiwwi nagy dolmánnyal és némi amatörizmussal

terhelt szolgáltatása a vidékiek egy részének hozott enyhülést, míg a Freestart a mögötte álló Pantel professzionalizmusával nyúlt a hazai felhasználói körhöz. Így a harmadik út, amelyet informatikai kormánybiztosunk jelölt ki „lottóirodájával" – mint ismeretes, a fizetőképes jelentkezők között kisorsolták a PC-ket –, elsikkadt a semmiben. Hiszen ha megnézzük, ki tett többet a Net-kultúra elterjesztéséért, egyértelmű, hogy az ingyenes szolgáltatók, legyenek bár sok szempontból amatőrök. Amatörizmusuk információhiányát ugyanis a háló közössége igen gyorsan pótolta.

A felhasználóra pedig maradt a telefonszámla nyűge, amelynél szeretett monopolszolgáltatónk további komoly alapdíjemelést tervez. Itthon immár nem a telefonhiány, hanem a magas költség az alacsony internethasználat oka. Persze mások is jeleskednek az ár felhajtásában. A UPC kábeles árai a nevetségesség határait súrolják, és néhány internetszolgáltatóról sem mondható semmi jó. Pedig a hazai Net-kultúrát, későbbi jövedelmeiket ölik meg ezzel a lépéssel.

Az internetes üzlet alapja az ingyenes szolgáltatás, habár a nemzetközi szakirodalmat látva ennek ellenkezőjére is találhatunk hivatkozásokat. A Yahoo! például most tette fizetőssé internetes aukcióit. Más portálok szintén azzal fenyegetőznek, hogy pénzt kérnek szolgáltatásaikért, és egyes internetszolgáltatók, melyek korábban ingyenesek voltak, átmentek a fizetős kategóriába. Ezt a Kiwwi szolgáltatási szerződése sem zárja ki, de ez lenne számukra a legfájdalmasabb öngyilkosság. Ugyanakkor a távközlési szolgáltatást nyújtó cégek minden idők legnagyobb profitját vágják zsebre.

Magyarországon átalakul a ViaNovo. Önálló politikai webújság lett a Euroastra, míg a Travelport, a Netpincér inkább saját szolgáltatási területeire korlátozva hirdeti a profizmust. Az egyetlen tudományos portál, a Jövőnéző beolvadt az STP portálba. Az Index a komplex szolgáltatók közül kezd egyre inkább kitűnni, megtalálva a webes hangot. A szaklapok is mind jobb portálokkal várják az olvasókat és a hirdetőket.

Miközben nem veszik észre, hogy a sikeresnek tűnő ágazatnak mások el kívánják vonni a létalapját. Újra visszaszorítani az internetezők számát egyszerű gazdasági eszközökkel. A szerzői jogvesztő irodák meg akarják sarcolni – és részben meg is teszik – a webtartalmakat. Mások szeretnék szabályozni és újabb adókkal sújtani a szolgáltatókat: a hangadótól a reklámadóig mindent a szerencsétlen tartalomszolgáltatók nyakába varrnak. Arra senki sem gondol, hogy újfajta forrásmegosztás kellene: a hozzáférés-szolgáltatók és a tartalomszolgáltatók képezik a két nagy tábort. Ugyanis a jó tartalom hozadéka a még több netező, akik kifejezetten a hozzáférés-szolgáltatók bevételeit gazdagítják. Hiszen az internet lassan egyetemes kultúránk része: egyre több az eredeti magyar tartalom, és kezdenek felébredni azok is, akik eddig nem voltak jelen a Neten. Az eredmény természetesen ugyanolyan ellentmondásos kutyulék, mint a szabályozás körüli hatalmi harc.

Azaz az ingyen még így is sokba kerül, nagyon sokba, amit a felhasználók fizetnek meg. Európában – és talán az egész világon – nálunk a legdrágább a távközlés. Ráadásul hiányzik a kultúra, amelynek alapján a fogyasztóvédők vagy a felhasználók meg tudnák ítélni, mi az olcsó és mi a drága.

A Családnet PC-akció szakértői szemmel nézve nagyon drága – a keresetekhez képest. Ám hogyha megnézzük egyik népszerű diszkontáruházunk ISDN-akcióját, akkor láthatjuk, hiba van az értékarányos szolgáltatások körül. Az egyik levelezési listán olvastam, hogy egy noname monitorral felszerelt, AIDA „márkájú" számítógép ötórás matávnetes internetcsomaggal, 14 900 forintos Eicon Divasszal, ISDN-csomaggal együtt 190 000 forintba kerül (figyelmeztetés a számítógépdobozon: csak a Matávval való szerződéskötés után vihető), míg majdnem ugyanez a számítógép márkás monitorral, internetcsomag nélkül, viszont két kis hangfallal 150 ezerért megvásárolható. Valaki nagyot szakít…

Az olcsó valóban olcsó lenne, ha nem drágítanák meg egyes monopolszereplők, amelyek törvény adta monopolhelyzetük miatt nem kerülhetők ki. Így lesz az ingyenes is megfizethetetlen. Hacsak nem változtat ezen a politika. Ennek rég eljött az ideje.

Kis János szabadúszó informatikai szakújságíró. Szakterületei: adat- és vírusvédelem, DTP, hálózatok, számítógépes etika, gépemberi jogok.

E-mail:

johannes@mail.datanet.hu.

Ha valaki a fentiekkel nem ért egyet (vagy akár nagyon is egyetért), írjon a BYTE Interaktív levelezőlista Vita rovatába: vita@byte.hu. Más levelezőlistára feliratkozás: www.byte.hu.