Computer PANORÁMA

Computer Panoráma
XIV. évfolyam 6. különszám, 2003. május
Ára: 695 Ft

ADATBIZTONSÁG

Információvédelem mindenkinek KÜLÖNSZÁM

CD-melléklettel

Fertőzők osztálya
Vírusok, férgek, trójaiak

Windows, ami biztos
Windows Server 2003

Titkosügynök a PC-n
Megatrend ISee

Szabványos biztonság
IT biztonsági audit

Digitális pecsét
Elektronikus aláírás

Szoftverek résen
Tűzfalak

Megbízható mobilok
Nyilvános kulcsú titkosítás

Romboló impulzusok
Szünetmentes áramforrások

Jól tartott szerverek
Szerverfarmok

A CD tartalmából:
ZoneAlarm 3.7
(teljes verzió)
Norton Antivirus 2003
(30 napos próbaverzió)
Ashampoo Mail Virus Blocker
(teljes verzió)

Járja be velünk az információbiztonság világát!

03006
9 770865 524126

ELEMZÉS

TECHNOLÓGIA

SZOFTVER

SZOLGÁLTATÁS

HARDVER

MOBIL

ALKALMAZÁS

HÍREK, ÚJDONSÁGOK

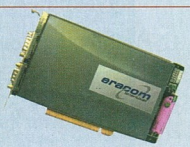
SZOFTVER

Windows Server 2003 30

A Microsoft április 24-én, San Franciscóban jelentette be legújabb operációs rendszerét, a Windows Server 2003-at. A termék a műszaki újítások százainak köszönhetően adatközpont-szintű megbízhatóságot kínál a felhasználóknak. Írásunkban a Windows Server új biztonsági szolgáltatásait tekintjük át.

TECHNOLÓGIA

Elektronikus aláírás 16



Évek óta várjuk, hogy elérkezik a papír nélküli irodák kora, de az irodai papírfogyasztás nemhogy csökkent volna, inkább nőtt az irodai számítástechnika terjedésével. Ha előbb-utóbb mégsem kell majd minden hivatalos ügyet személyesen intéznünk, az csakis az elektronikus aláírási rendszernek lesz majd köszönhető.

HARDVER

Szünetmentes áramforrások 42

A vírusok, hackerek és más internetes fenyegetések elleni védekezésben sokan hajlamosak megfeledkezni a sokkal hétköznapibb veszélyekről. Ilyen például az áramkimaradás, vagy – ami még rosszabb – a villámcsapás. A tápellátásban bekövetkező zavarok ellen a szünetmentes energiaforrások jelentik a megoldást.

IMPRESSZUM

ADATBIZTONSÁG
A Computer Panoráma különszáma
XIV. évfolyam 6. különszám,
2003. május

Felelős szerkesztő: Bányai Ferenc
Művészeti vezető: Iszkra Ildikó
Titkárságvezető: Szőke Erika
Címlap: Szincsák László

Szerkesztőség:
1091 Budapest, Üllői út 25. I. em.
Telefon: 456-6888, fax: 456-6970
E-mail: c.panorama@cpanorama.hu
Internet: http://www.computerpanorama.hu
Kiadó:
Felelős kiadó: Dely Tamás ügyvezető igazgató

Kiadó: A HVG Kiadó és a WEKA Computerzeitschriften-Verlag GmbH közös vállalata, a Computer Panoráma Kiadói Kft. Computer Panorama Verlag GmbH

1091 Budapest, Üllői út 25. I. em.
Telefon: 456-6888
Terjesztés:
Mosolygó Kitti marketing- és terjesztési vezető
1091 Budapest, Üllői út 25. I. em.
Telefon: 456-6964, fax: 456-6970, e-mail: terjesztes@cpanorama.hu
Ügyfélszolgálat hétfő–péntek: 9–17 óráig
Terjeszti: a Hírker Rt., az NH Rt. és alternatív terjesztők

Hirdetésfelvétel:
hirdetési vezető: Tasnádi Rózsa
hirdetésszervező: Háder Judit, Kuba Ilona
1091 Budapest, Üllői út 25. I. em.,
Telefon/fax: 456-6974, fax: 456-6970
E-mail: c.panorama@cpanorama.hu

Hirdetésfelvétel Németországban:
Telefon: 0049-8121-95-1182
Telefax: 0049-8121-95-1627
E-mail: Akieger@wekanet.de

A Computer Panoráma különszámai megrendelhetők:
a kiadónál személyesen, levélben, e-mailben, weboldalunkon vagy a postahivatalokban, a hírlapkézbesítőknél és a Hírlap-Előfizetési és Elektronikus Posta Igazgatóságon (HELP)
1900 Bp. XIII., Lehel út 10/A, a Postabank Rt. 219-98636/021-12799 pénzforgalmi jelzőszámon. A különszámok megvásárolhatók a hírlapboltokban, könyvesboltokban, a kiadónál. A régebbi számokat keresse a kiadóban, telefon: 456-6964, 1091 Budapest, Üllői út 25. I. em.

Az Adatbiztonság különszámot készítette:
Levilágítás: GMN Repro Stúdió
Nyomtatás: Pauker Nyomdaipari Kft.
1044 Budapest, Baross u. 11-15
Felelős vezető: Vértes Gábor ügyvezető igazgató

ISSN 0865-5243

Fertőzők osztálya

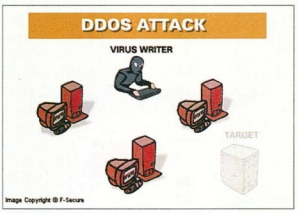
A számítógépes vírusok újabb és újabb, egyre globálisabb fertőzési hullámokkal hívják fel magukra a figyelmet. A maga korában elhíresült LoveLetter vagy a máig felbukkanó Code Red lassan már csak gyenge próbálkozásoknak tűnnek napjaink egyre összetettebb kártevőihez képest.

Máig igaz, hogy a legveszélyeztetettebb platformok a *Microsoft* gyártotta rendszerekkel felszerelt gépek, közülük is azok, amelyekre elfelejtik naprakészen feltenni a javításokat, így védtelenül állnak a támadások keresztüzében. Ahogy az is igaz, hogy a számítógépes vírusok jelenléte korántsem új fejlemény.

A mai vírusok ősei már a *Commodore* és *ZX* gépek térhódításával megjelentek. Első virágkoruk azonban a DOS-korszakra tehető, és a vírusoknak máig leggyakrabban otthont adó *Intel* PC-k gyors elterjedésével jött el. A gépindításra használt flopik *bootszektorának* fertőzésével a vírusok terjesztése lényegében a felhasználó aktív közreműködésével valósult meg.

A boot-vírusok mellett azután sorra megjelentek a fájlokat fertőző, illetve magukat álcázó másfajta vírusok is. A gépen tárolt állományokba beépülő, méretnövekedést okozó, szemetet termelő vírusok felbukkanása azonban csak a nagyobb merevlemezekkel, virágkoruk pedig az egyedileg is igen sok állományból álló programrendszerekkel jött el, amelyek fájlrendszere amúgy is nehezen áttekinthető.

A nagyobb merevlemezek eljövetelével a partíciók „buherálása" is gyakorlattá vált, aminek egyik leghírhedtebb, de mindenképpen egyik legnagyobb kárt okozó példája a *OneHalf* nevű vírus volt. Az ősvírus-csoportok egyikeként megjelent *Trójai faló* jellegű kártevőkről annyit érdemes még megjegyezni, hogy a magukat valamilyen hasznos funkcióval álcázó állományként elbúvó kártevők máig megvannak, de manapság már nem őket, hanem a „művészbejárót" létrehozó kártevőket illetik ezzel a meghatározással.



A féregszerű terjedés és a DoS kialakulása

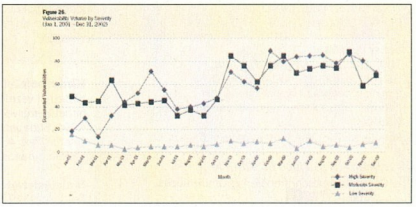
Veszélyes internet

Ahogyan a DOS, mint operációs rendszer visszaszorult, úgy csökkent a DOS-specifikus vírusok jelentősége. Ugyanakkor más eszközök bukkantak fel, a terjesztésre és a víruskészítésre egyaránt. Erre jó példát mutathatnak a *Word makróvírusai*, mivel a Microsoft Wordbe épített Basic nyelv új programozási felületet kínált, és a dokumentumok cseréje is új terjedési módot szolgáltatott. Nem véletlen, hogy volt idő, amikor a legnagyobb veszélyt ezek a vírusok jelentették.

Az újabb minőségi ugrást a világ internetesedése jelentette, amely új lehetőségeket teremtett a kártevők számára mind a terjedésre, mind a kártételre. Az egymással szinte folyamatos kapcsolatot tartó számítógépek alkotta rendszeren az egyes vírusok terjedése igen gyors lehet. Erre jó példa a lassan már szintén emlékké fakuló *SirCam*, amely egy kisebb hálózaton az első fertőzést követően perceken belül teljes fertőzöttséget volt képes előidézni.

Ehhez azonban már több kell, mint egy fájlhoz hozzáragasztani a víruskódot. Az internetes kártevőnek a hálózatkezeléshez is konyítania kell, tehát az adott gép kommunikációs rendszerébe kell integrálódnia. Az internetes kártevők összetettsége egyre növekszik, és sokszor elmosódik a határ a „csak" közvetlen kárt okozó és gyorsan szaporodó vírusok, az idegen behatolást könnyítő trójaiak, valamint a kommunikációs rendszert kihasználó, a kommunikáció parazitálásával ható férgek között. Olyannyira, hogy egy jobb vírusirtó alkalmazás ma már nem is tesz különbséget ezek között, és kivétel nélkül mindeniket eltávolítja. Az azonban továbbra is igaz, hogy a gyors terjedési lehetőség ellenére a „gyors halált" okozó vírus továbbra sem sikeres. Ennek egyszerűen az az oka, hogy amennyiben egy vírus a szaporodása előtt okoz könnyen észrevehető kárt, illetve rendszerösszeomlást, akkor már nem is lesz esélye szaporodni.

Az internet szerepe ebben a folyamatban az, hogy a gyors terjedési lehetőség felkínálásával a „lappangási idő" nagyon lerövidül. Ehhez elég áttekinteni azokat a statisztikákat, amelyek például a már említett – és a fertőzések java részét egyfajta fertőző memóriatartalomként közvetítő – Code Red, a nem sokkal utána felbukkant *Nimda*, vagy a közelebbi múlt *Slammer* járványát írják le. A világhálón órák alatt szétterjedő járvány gyorsan okozhat igen nagy károkat, amelyeket már dollármilliókban-milliárdokban lehet csak mérni. Talán az sem véletlen, hogy ezek többsége



A program-sérülékenységek és súlyosságuk alakulása a Symantec felmérése alapján (Symantec Internet Security Threat Report – Attack Trends for Q3 and Q4 2002)

valamely programhibát – sérülékenységet – használ ki, és tulajdonképpen a féregszerű viselkedésük dominál.

A sérülékenységek szerepét azért is említjük, mert az internetes támadásoknak általában sokszor célpontjai a programok ilyen fogyatékosságai. Márpedig – mint azt a *Symantec* egyik tanulmánya *(Symantec Internet Security Threat Report – Attack Trends for Q3 and Q4 2002)* – kimutatta, ezeknek a problémáknak a száma és súlyossága növekvő tendenciát mutat az utóbbi időkben. A gyors nagytömegű fertőzés pedig az internetes kiszolgálókon előidézett szolgáltatás-megtagadáson *(Denial of Service, DoS)* keresztül okoz jelentős kárt.

Bár az említett trió tagjai a Windows-rendszert károsítják, a vírusokról azt is érdemes tudni, hogy elvileg szinte bármely operációs rendszerre írható vírus. Ilyen például a Linuxra írt *Slapper*, amely az OpenSSL egyik 2002. szeptemberében felfedezett és azóta kijavított problémájához kötődött. Itt jegyezzük meg azt is, hogy bár felbukkantak már platform-független, Linux-on és Windows-on is megélő vírusok, a legjelentősebbek még mindig az egyes operációs rendszerekhez, programkörnyezetekhez kötődnek.

Szkriptvírusok

A terjedési közeghez való alkalmazkodás egyik jó példája volt a *Hybris*, amely önállóan tudta frissíteni moduljait a világhálóról. Ám a közegen kívül természetesen a vírusírás eszköztárának változása is hatott a vírusokra. A Word makróvírusainak kapcsán már szó esett arról, hogy a Windows-alkalmazások viselkedésébe belenyúló *Basic* nyelv alkalmas az adott alkalmazáshoz kötődő, illetve a *Visual Basic for Applicaton (VBA)* kódjait értelmezni képes kártevők előállítására.

A jobb sorsra érdemes és a rendszergazda kezében igen hatékony eszközzé tehető Windows *Scripting* rendszerrel is gyorsan és nem is túl nagy szakismerettel fejleszthetünk a rendszerek mélyére is behatolni képes kódot. Nem véletlen tehát, hogy a Visual Basic alapján fejlesztett *szkriptvírusok*, a szkriptrészleteket is használó vírusok egyre sűrűbben bukkannak fel a kártevők világában.

A vírusírókon kívül azonban továbbra is lényeges a felhasználó vírusterjedést segítő viselkedése. Ez sokszor nem más, mint az egészséges félelemszint hiánya, a levelekben kapott programok gyanútlan és kritikátlan elindítása. Ebben az olyan levelezőprogram is ludas lehet, amely szinte kínálja a felhasználó becsapását, és lehetővé teszi a csatolt állományok egyszerű kattintással való aktiválását.

A vírusok és rokonaik világa folyamatosan alakul, a kártevők száma úgyszólván napról napra nő. Így egyre nagyobb jelentőségű, hogy a vírusirtó alkalmazás ne csak ott legyen a gépünkön, hanem napra, vagy szükség esetén órára készen frissített állapotban is legyen.

Simay Endre István

10 jótanács a Symantectől

10 Használd a józan eszed! Még mindig az a jobb, ha a biztonság javára tévedsz. Ha bizonytalan vagy egy csatolmány felől, inkább töröld, főleg akkor, ha az egy azonosíthatatlan helyről származik! Ha csalogató animációk vannak egy egyáltalán nem hivatalosnak tűnő helyen, ne töltsd le őket!

9 Vizsgáld meg a flopikat használat előtt! Ez mindig lényeges, de különösen akkor, ha két számítógép közötti információcserére használod a lemezt. Könnyen bekaphatsz egy védtelen hálózatról származó vírust és beviheted a saját hálózatodba. A lemezen levő bármely program elindítása előtt lefuttatott vírusellenőrzés megelőzi a fertőzést.

8 Ne kölcsönözz flopikat! Még a legjobb akaratú barátodtól is kaphatsz tudtán kívül vírust, trójait vagy férget. Címkézd meg egyértelműen a flopijaidat, hogy tudd, azok a sajátjaid, és ne add kölcsön őket. Ha a barátod idegen flopit akar adni neked, javasolj más fájlcsere módszert!

7 Flopiról ne indíts rendszert! A flopikon keresztül lehet talán a legegyszerűbben vírust kapni. Ha a munkád közben flopit használsz, vedd ki, mielőtt kikapcsolnád a gépedet, mert az önműködően a flopiról próbálja majd elindítani a rendszert, és az esetleges vírus máris a gépedre kerülhet.

6 Ne tölts le programokat az internetről! Az internetes hírcsoportok vagy a sosem hallott webhelyek, mint megannyi megbízhatatlan forrás, számítógéped fő vírusbeszerzési forrásai lehetnek. Óvakodj az olyan fájlok letöltésétől, amelyekről nem tudod kétséget kizáróan, hogy biztonságosak. Ide tartoznak a freeware-ek, a képernyővédők, a játékok és minden egyéb program – minden fájl, amelynek a kiterjesztése „.exe" vagy „.com", például olyasmi, hogy „coolgame.exe". Győződj meg arról, hogy a túloldalon fut-e víruselhárító program. Ha le kell töltened valamit az internetről, ellenőrizz minden egyes programot, mielőtt futtatnád azokat! Az összes letöltést egy könyvtárba gyűjtsd, és használat előtt annak teljes tartalmán futtasd le a víruskeresőt!

5 Frissítsd gyakran a víruselhárító programodat! Egy víruselhárító program éppen annyira hatásos, amilyen sűrűn frissíted. Nap mint nap születnek új vírusok, férgek és trójaiak. A nem napra kész szoftver mellett átcsúszhat valamelyik variánsuk.

4 Légy azonnal védve! Úgy állítsd be a víruselhárító szoftveredet, hogy a rendszerindításkor az is elinduljon és folyamatosan fusson! Ez biztosítja az esetlegesen elfelejtett, vagy szándékosan kihagyott csatolmányvizsgálat esetére a védelmi tartalékodat. Azáltal, hogy a víruselhárító szoftveredet önindítóvá teszed, mindenképpen biztosítod az azonnali védelmedet, még ha el is felejtenéd elindítani azt.

3 Vizsgálj meg minden érkező e-mail csatolmányt! Feltétlenül küldd át a vírusellenőrzésen az összes, megnyitni szándékozott csatolmányt! Tedd meg ezt még akkor is, ha ismered a feladót, és megbízol benne. A rosszakaratú programok, például a trójaiak a baráti forrásból is beszivároghatnak a rendszeredbe.

2 Ne nyisd meg automatikusan a csatolmányokat! Feltétlenül akadályozd meg, hogy a levelezőprogramod magától nyissa meg a csatolmányokat! Ezzel gondoskodsz arról, hogy futtatásuk előtt meg tudd őket vizsgálni. Nézz utána a levelezőprogramod biztonsági beállításainál, vagy a beállítások menüpontjában, hogy mit kell tenned!

1 Telepíts megbízható víruselhárító programot! A víruselhárító program rendszeresen átnézi a fájlokat, hogy nem változott-e a hosszuk, nincsenek-e benne az ismert vírusok listájában, nem gyanús-e a csatolmány, vagy nem mutatkozik-e valami riasztó jel. Ez a legfontosabb dolog, amit a számítógéped vírusmentessége érdekében megtehetsz.

Auditorium Maximum

Az IT biztonság, annak folyamatos menedzsmentje, illetve auditálása egyelőre még gyerekcipőben jár mifelénk, de a szakértők szerint látványos fejlődés előtt áll ez a szakterület. Cikkünkben a módszereket, szabványokat járjuk körül, és vázlatosan bemutatjuk az IT audit piac szereplőit is.

A címben szereplő latin név a Budapesti Műszaki Egyetem egykori és mostani hallgatói számára ismerősen cseng: a patinás központi épületben található legnagyobb előadótermet hívják így. Cikkünk élére azonban nem csak a szójáték kedvéért került: az információtechnológia biztonságáról szóló átfogó ellenőrzés és az arról szóló minősítés, más néven *az IT biztonsági audit* szerepe az elkövetkező években egyre nagyobb lesz. Ismerkedjünk meg tehát a szakmai háttérrel, az eljárásokkal, az egyelőre még nem világszerte elfogadott szabványokkal és a bimbózó hazai piac szereplőivel.

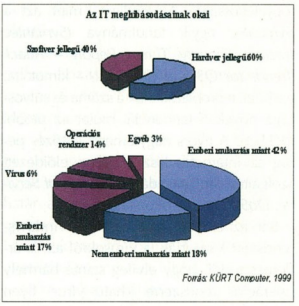
Szabályok és szabványok

Az egyre kiterjedtebb cégen belüli hálózatok, az internet, a kettő kombinációjaként elterjedt *VPN (Virtual Private Network)*, azaz virtuális magánhálózati megoldások elterjedésével a rendszerek nyitottsága, a kívülről jövő rosszindulatú behatolásokkal szembeni kiszolgáltatottság egyre nő. A bonyolultság növekedése magában rejti a meghibásodások kockázatának a növekedését. A cégek, állami szervek terebélyesedésével nő a munkatársak esetleges félrelépésének a kockázata is. Ugyanakkor az informatika egyre inkább átszövi életünket, egyre több kritikus *(mission critical)* rendszer működésétől függ a gazdálkodók és a hatóságok működőképessége. Az informatikai rendszerek adatbázisaiban felhalmozott információ értéke is egyre nő, és nem csak a reprodukálásukhoz szükséges munkamennyiség nagysága miatt.

Az említett okok miatt az informatikai biztonság kérdése szükségszerűen egyre inkább az érdeklődés homlokterébe kerül. A kockázatok sokfélék, a legtöbb helyen a heterogén, több éves fejlődés során kialakult informatikai rendszerek, hardver- és szoftvermegoldások számos rést kínálnak a támadások vagy a véletlen meghibásodások számára.

Közben egyre több felelős vezető teszi magáévá a gondolatot, hogy az IT biztonságával folyamatosan törődni kell. Az információtechnológiai (IT) rendszer valamennyi elemét külön-külön és együtt is folyamatosan vizsgálják azok működése során az informatikai biztonsági eljárások szempontjából. A vizsgálatok eredményétől függően a legjelentősebb veszélyforrásoknál a költségkereteken belül korrigálják a rendszert. Az itt leírt folyamat az IT rendszer üzemeltetésének része, vagy részévé kell, hogy váljon. E belső vizsgálatokkal párhuzamosan időszakonként célszerű a teljes vizsgálatot egy informatikai biztonságra szakosodott külső *auditáló céggel* (is) elvégeztetni, amely a független vizsgáló szemszögéből összehasonlítja a megfogalmazott biztonsági eljárásokat a szabványelemekkel és a gyakorlati alkalmazással. Mindezen vizsgálatok célja az, hogy rávilágítsanak az informatikai biztonság gyenge pontjaira, az adatvesztés kockázatára és még egy sereg kézzelfogható paraméterre, amelyek a felelős vezetők számára világos képet festenek a pillanatnyi helyzetről, és kiindulópontot adnak a jövő stratégiai döntéseinek meghozatalához. A hangsúly a rendszeres (belső/külső, valamint részleges/teljes) vizsgálaton és ez alapján az informatikai biztonsági rendszer folyamatos módosításán, javításán van.

Az informatikai biztonság speciális szakismereteket kíván. Érdekes aspektusa ennek a potenciális külső támadók, a *hackerek* esete. A rendszereket vizsgálatuk során valódi, de „megszelidített" hackerek támadásainak teszik ki. Ezek a többnyire tinédzserkorú vagy alig idősebb szakemberek rablóból lettek pandúrrá, és tevékenységüket, az úgynevezett *„etikus hackelést"* a vizsgálatok során szigorúan dokumentálják és bizalmasan kezelik.



A felmérés óta eltelt időben a vírusok, illetve a külső behatolások súlya tovább nőtt

Kis-közepes nagyságú, szakosított tanácsadó cégek
(a teljesség igénye nélkül)

EMIB Tanácsadó Kft. – AS/400 rendszerek biztonsági szakértői

Hunaudit Kft. – Az APEH „hosszú bájtok éjszakája" körüli auditálás főszereplője

Hunguard Kft. – többek között a MEH/ITB szellemi háttere e témában

IMSys Kft. – főleg bankok és biztosítók partnere

Metacom – referenciák: minisztériumok, önkormányzatok, állami nagyvállalatok

Nektor IT Security

Noreg Információvédelmi Kft. – a Montana csoport tagja, bankok/pénzintézetek, a telekommunikáció partnere

FAX MEGRENDELŐLAP

Computer Panoráma Kiadói Kft.
Terjesztési Osztály
1091 Budapest, Üllői út 25.
Tel.: 456-69-63

Fax: 456-69-70

Minden 3. DVD-s Computer Panoráma AJÁNDÉK!

MOST MÉG JOBBAN MEGÉRI!

Ha az alábbi DVD-mellékletes Computer Panorámákból legalább hármat megrendel, akkor az egyiket ajándékba adjuk!

Válasszon legalább három Computer Panorámát és fizessen 7170 Ft helyett **CSAK 4780 Ft-ot!**

Ezzel 2390 Ft-ot takarít meg!

Megtakarítása hat darab megrendelt DVD-s Computer Panoráma esetén 4 780 Ft, 9 darab esetén már 7 170 Ft!

Ne késlekedjen, rendeljen még most!

☐ CP 2002/6

☐ CP 2002/7

☐ CP 2002/8

☐ CP 2002/9

☐ CP 2002/10

☐ CP 2002/11

☐ CP 2002/12

☐ CP 2003/1

☐ CP 2003/2

☐ CP 2003/3

☐ CP 2003/4

☐ CP 2003/5

SZÁMLÁZÁSI CÍM:

Cégnév: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Ir.sz: ☐☐☐☐ Helység: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Út/utca/tér: ☐☐☐☐☐☐☐☐☐☐☐☐☐
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐,

hsz. ☐☐☐, em./ajtó: ☐☐/☐☐

Telefon (napközben): 06 ☐☐☐☐☐☐☐☐

E-mail: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Kérjük, a kézbesítés megkönnyítése és a gyors ügyintézés érdekében minden adatot feltétlenül adjon meg!

POSTACÍM:

Cégnév: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Ir.sz: ☐☐☐☐ Helység: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Út/utca/tér: ☐☐☐☐☐☐☐☐☐☐☐☐☐
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐,

hsz. ☐☐☐, em./ajtó: ☐☐/☐☐

Telefon (napközben): 06 ☐☐☐☐☐☐☐☐

Mobilszám: 06 ☐☐☐☐☐☐☐☐☐

Aláírás

AJÁNLATUNK A KÉSZLET EREJÉIG ÉRVÉNYES.

Átfutási idő körübelül 2 hét.

Internet: www.computer panorama.hu/megrendeles,
E-mail: **megrendeles@cpanorama.hu**

A megrendelt újságokat utánvéttel küldjük, áraink a postaköltséget nem tartalmazzák! (A postaköltséget az érvényes postai díjszabás szerint számoljuk.)

100%-os biztonság nincs. De mennyit ér meg a biztonság adott szintű emelése? Egy példával élve: ha a hűtőszekrényünkkel mondjuk kétévente történik valami, és éppen a nyaralás alatt olvad le áramkimaradás vagy műszaki hiba miatt, körülbelül 15 ezer forint értékű mélyhűtött áru megy tönkre. Ha 300 ezer forintért vehetnénk saját áramfejlesztőt, nem érné meg, mert aránytalanul nagy a befektetés a veszteséghez képest. Más lenne a helyzet, ha hetente olvadna le a hűtő, vagy ha milliós értékű kaviárt tárolnánk benne. A biztonsági intézkedések meghozatalának tehát fontos része a *költség/haszon elemzés.*

Minden információbiztonsággal foglalkozó tanácsadó egyetért abban, hogy a cégek, illetve hatóságok informatikai rendszereinek működését egy *Informatikai Biztonsági Szabályzatban* (rövidítve IBSz) kell szabályozni. Ez a többi szabályzathoz hasonlóan rögzíti a folyamatokat, a dokumentálás rendjét, de tartalmazhat például konkrét terveket a bekövetkezhető informatikai katasztrófahelyzetek kezelésére, „túlélésére" is. Érdemes belegondolni persze abba is, hogy egy ilyen gyorsan változó területen, az újabb és újabb veszélyek, támadások közepette hogyan lehet a működés egyszerre szabályozott és dokumentált, ugyanakkor rugalmas és képes gyorsan reagálni a kihívásokra...

Amíg például a minőségbiztosítás terén nemzetközileg elfogadott, egyeduralkodó szabványok vannak (az *ISO 9000* család), az informatikai biztonság területén a szabványosodás szintje egyelőre még sokkal alacsonyabb.

A terület szakértőinek nemzetközi szervezete az *ISACA (Information Systems Audit and Control Association – Nemzetközi Informatikai Auditorok Egyesülete).* Ez kidolgozott egy ajánlást, egy IT szabályozási szabvány- és célgyűjteményt *COBIT (Control Objectives for Information and Related Technology – irányítási célok az információs és rokon technológiák számára)* néven.

Egy további irányelv-gyűjtemény az úgynevezett *Common Criteria.* Ezt egy Egyesült Államokbeli kutatóintézet dolgozta ki az USA központi kormánya megbízásából, majd számos állam csatlakozott hozzá, és kialakult a nemzetközi minősítés szervezete is. Hazánkban a *Miniszterelnöki Hivatal* égisze alatt működő *Informatikai Tárcaközi Bizottság* ajánlások keretében állt e rendszer mellé.

Talán a legnagyobb esélye a teljes körű nemzetközi elfogadtatásra az *ISO17799* – „leánykori" nevén *British Standards BS7799* – szabványnak van. A GKM ez évi pályázatai is ezt a szabványt támogatják.

A szakértőcégek ezen szabványok, illetve ajánlások egyike-másika, vagy az ezekből kialakított mix alapján dolgoznak. Természetesen a minősítők is minősítve vannak: a szakembereknek az ISACA jogosult a *CISA (Certified Information Systems Auditor – minősített információs rendszer auditor)* címet adományozni. Hazánkban egyelőre nem túl nagy a CISA minősítésű szakértők száma.

A támadások következményei

Amint azt a legutóbbi, 2002 októberében megjelent „Adatbiztonság" különszámunkban részletesen bemutattuk, a *BellResearch* kutatócég 2002-es – 400 cég körében végzett – telefonos felmérései alapján Magyarországon az informatikai biztonság fontosságát közepesnek, az ötfokozatú skálán 3 és 4 közötti pontszámmal értékelték a megkérdezettek. Tették ezt annak ellenére, hogy az elmúlt két évben a hazai cégek közel 20%-át érte közvetlen anyagi kár valamilyen informatikai biztonsági probléma miatt. A kérdést annál fontosabbnak ítélték meg, minél nagyobb volt a képviselt cég.

A hazainál jóval fejlettebb és nyitottabb amerikai gazdaságban a veszélyek már sokkal nagyobbak. Amint azt a *Computer Security Institute* és a *Szövetségi Nyomozóiroda (FBI)* közös kutatása kimutatta, a tavalyi évben az amerikai cégek 85%-át érte vírusfertőzés, körülbelül 40%-uk szenvedett el kívülről vagy belülről indított rendszerbetörést, illetve „Denial of Service" (szolgáltatás megtagadás) típusú támadást.

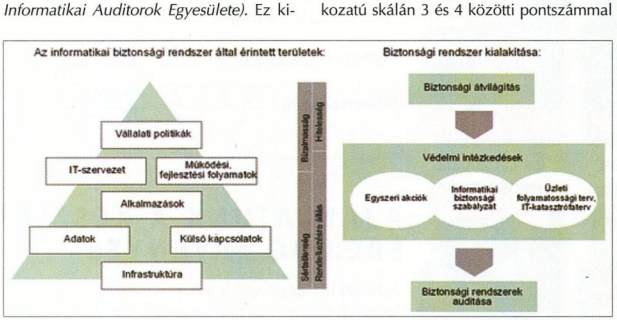
Hogy az anyagi következményeket is érzékeltessük, álljon itt néhány kiragadott példa: a *Code Red* vírus, pontosabban féreg csupán 9 óra alatt több mint 250 ezer rendszert fertőzött meg világszerte 2001. július 19-én, és 18 óra alatt érte el a globális telítettséget. A *Computer Economics* becslése szerint ennek az egyetlen támadásnak a gazdasági hatása összesen 2,6 milliárd dollár volt. Egy másik vírus, a *Sircam* által okozott kár összességében 1,3 milliárd dollárt tett ki.

A hazai példatárból is említsünk egy esetet: az anyagi következmények ismerete nélkül is bizton állíthatjuk, hogy súlyos gondokat okozott az *OEP* (régebben TB) néhány évvel ezelőtti adatvesztése, amikor is a gazdálkodóktól újra bekért papír-alapú saját bevallási példányok alapján rögzítették újra bizonyos adatokat.

Kis Miklós

Többféle profilú, nagyobb tanácsadó cégek, rendszerintegrátorok

AAM – referenciák nagyvállalatoktól minisztériumokig
MCS – német tapasztalatok hazai forrása
STRATIS – a Meta Group tagja
FreeSoft Kft. 3A - Audit, Adatbiztonság, Alkalmazásfelügyelet üzletág
ICON Számítástechnikai Rt. Informatikai Biztonság Üzletága
KÜRT Rt. – saját fejlesztésű IBiT Informatikai Biztonsági Technológia
Synergon Informatikai Rt. Üzleti és Biztonsági Tanácsadás Üzletág
telnet Magyarország Rt. Informatikai Biztonság divíziója



Az AAM így szemlélteti az informatikai biztonság elemeit és a menedzsment folyamatát

FAX MEGRENDELŐLAP

Computer Panoráma Kiadói Kft.
Terjesztési Osztály
1091 Budapest, Üllői út 25.
Tel.: 456-69-63

Fax: 456-69-70

Igen, utánvéttel megrendelem az alábbi 2002-es és 2003-as különszámokat:

- ❐ 2003/1 Tesztgyőztesek (495 Ft)
- ❐ 2003/2 CAD/CAM (695 Ft)
- ❐ 2003/3 PC-Házimozi (1990 Ft)
- ❐ 2003/4 Download (695 Ft)
- ❐ 2002/17 Távközlés (595 Ft)
- ❐ 2002/16 Hálózatok (695 Ft)
- ❐ 2002/15 Tesztek (695 Ft)
- ❐ 2002/14 Monitorok (495 Ft)
- ❐ 2002/13 Arany Válogatás III. (1 690 Ft)
- ❐ 2002/12 Mobil Világ 2. (495 Ft)
- ❐ 2002/11 Windows XP (595 Ft)
- ❐ 2002/10 Adatbiztonság (695 Ft)
- ❐ 2002/9 CAD/CAM Trendek 2. (695 Ft)
- ❐ 2002/8 Arany Válogatás II. (1 495 Ft)
- ❐ 2002/7 Notebook (695 Ft)
- ❐ 2002/6 Mobil Világ 1. (495 Ft)
- ❐ 2002/5 Monitorok 1. (495 Ft)
- ❐ 2002/4 CAD/CAM Trendek 1. (695 Ft)
- ❐ 2002/3 Internet 1. (595 Ft)
- ❐ 2002/2 Nyomtatók (595 Ft)

SZÁMLÁZÁSI CÍM:

Cégnév: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Ir.sz: ☐☐☐☐ Helység: ☐☐☐☐☐☐☐☐

Út/utca/tér: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐

hsz. ☐☐☐, em./ajtó: ☐☐/☐☐

Telefon (napközben): 06 ☐☐☐☐☐☐☐☐☐

E-mail: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Kérjük, a kézbesítés megkönnyítése és a gyors ügyintézés érdekében minden adatot feltétlenül adjon meg!

POSTACÍM:

Cégnév: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Ir.sz: ☐☐☐☐ Helység: ☐☐☐☐☐☐☐☐

Út/utca/tér: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐

hsz. ☐☐☐, em./ajtó: ☐☐/☐☐

Telefon (napközben): 06 ☐☐☐☐☐☐☐☐☐

Mobilszám: 06 ☐☐☐☐☐☐☐☐☐

Aláírás

A megrendelés átfutási ideje körübelül 2 hét.
Internet: www.computer panorama.hu/megrendeles,
E-mail: **megrendeles@cpanorama.hu**
A megrendelt különszámokat utánvéttel küldjük, áraink a postaköltséget nem tartalmazzák! (A postaköltséget az érvényes postai díjszabás szerint számoljuk.)

Nyakunkon az ellenség

Egyre gyakrabban hallunk híreket vírustámadásokról, új és egyre veszélyesebb vírusok felbukkanásáról. Elemzésünkben a vírusvédelem különböző aspektusait járjuk körül, a 2F tapasztalataira alapozva.

Miért kell védekeznünk?

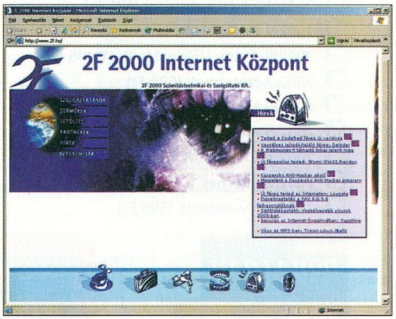
Nem árulunk el titkot azzal, hogy a víruskereső programok feladata a vírusos programok (valamint a trójaiak, dokumentum-makrók és társaik) felderítése és ártalmatlanná tétele. Ha csak annyit megteszünk, hogy használjuk, és rendszeresen frissítjük őket, máris sok veszélyforrást hatástalanítottunk: a flopikon és CD-ROM-okon terjedő, e-mailben érkező, letölthető fertőzéseknek vége. A gépünket fenyegető veszélyeknek azonban, sajnos, nem.

Számítógépünk képes az internetre csatlakozni, vagy már eleve egy cég hálózatába van kötve, ez pedig igen komoly veszélyforrás. Több tanulmány egybehangzóan állítja, hogy az adatokat ért támadások nagyjából 80 százalékáért saját munkatársaink a felelősek. A támadók véletlenül vagy szándékosan akaszkodnak mások gépére, hogy ott, szintén véletlenül vagy szándékosan, adatvesztést okozzanak. Néha elég egy lelkes kolléga, aki csak „segíteni" akart. De előfordulnak komolyabb esetek is, amikor szándékosan egymás adatait lopták, törölték alkalmazottak vagy egykori alkalmazottak. Közvetlenül az internetre csatlakozva pedig még hatványozottabban fordulhat elő ilyesmi.

Egy új korszak kezdete

Érdekes példa az alig pár hete megjelent *Slammer* (vagy *Sapphire*) vírus.

Az *SQL-Slammer* néven is ismeretes Sapphire féreg, amely január 25-én jelent meg az interneten, új korszakot nyitott a gyorsan terjedő internetes vírusok történetében. Egy neves elemzőcég felmérése szerint a megfertőződött SQL szerverek 90%-a a járvány első 10 percében esett áldozatul a Slammernek. Az általuk nemrég publikált jelentés szerint a Slammer féreg közvetlenül megjelenése után már minden 8,5 másodpercben megduplázta a fertőzött gépek összlétszámát, és három percen belül elérte aktivitása csúcspontját, amikor is másodpercenként 55 millió adatcsomagot küldött szét a Világhálón. A Slammer terjedése két nagyságrenddel (!) gyorsabb volt a 2001 nyarán megjelent *CodeRed* vírusénál, amely átlagosan 37 percenként duplázta meg a fertőzött gépek számát.



A 2F 2000 Kft. szolgáltatásai között kiemelkedő helyet foglal el az adatvédelem

A Sapphire férget készítő rosszindulatú hacker kifinomult, kézzel optimalizált gépi kódban írta meg a kártevőt. Emiatt annak mérete a memóriában mindössze 250 bájt (és az adathálózatban is csak 376 bájt), így szinte korlátlan példányszámban tud terjedni szerverről szerverre, a modern nagy sebességű hálózatokon keresztül. Mivel a féreg egyáltalán nem tartalmaz közvetlenül a gépeket pusztító rutint, a kódja igen kis méretű lehetett, és a további terjedés alapjául szolgáló fertőzött szerver-állománya is folyamatosan növekedett. A kisméretű, körülbelül 300 bájtos kártevő programkódja ugyanis annyira egyszerű, hogy csak a működéshez szükséges információkat hordozza.

Mivel a Sapphire féreg létezése a Windows memóriájára korlátozódik, a kód nem kerül kiírásra a háttértárolókon. A ma létező víruskereső szoftverek rajtuk kívülálló okokból nem képesek a teljes rendszermemóriát ellenőrizni, így a Sapphire hatékony felismerését nem lehet beépíteni az adatbázisaikba. A megfelelő védelmet

Mobil tartalomszűrő

Az *F-Secure Corporation* bejelentette az *F-Secure Mobile Filter* termékét, a világ első tartalombiztonsági megoldását a vezeték nélküli letöltő-rendszerekhez. A termék tartalomszűrési lehetőséget kínál a szolgáltatók számára a kártékony szoftverek és az inkompatibilis Java alkalmazások kiszűrésére, még mielőtt azok letöltődnének a mobiltelefonokra. A megoldás a szűrési feltételek automatikus frissítésének a szolgáltatását is tartalmazza. Emellett a szolgáltató rugalmasan definiálhat szabályokat a nem kívánt tartalom blokkolásához.

Az F-Secure Mobile Filter Java bájtkódelemzést és víruskeresést végez az inkompatibilis Java szoftverek és más káros tartalmak kiszűrésére a hálózaton, még a letöltés előtt. A transzparens proxy felépítés megkönnyíti az integrációt a letöltő-platformokkal, a szolgáltató oldalán található felhasználói felület pedig lehetővé teszi a nemkívánatos funkciók és akár az egyes inkompatibilis Java függvények kiszűrését is. Az *F-Secure Anti-Virus Research* központ automatikus, napi 24 órás szolgáltatást nyújt a tartalomelemző adatbázis frissen tartásához.

az operációs rendszer és az alkalmazások gyártói által kiadott biztonsági frissítések telepítése és a tűzfalak megfelelő konfigurálása jelenti.

Okulva a korábbi vírusok írói által elkövetett hibákból, a Sapphire féreg a rendszer órajelciklusát használja a célpontként szolgáló véletlen IP-címtartományok generálására, így bár az erőforrásokat nagyon pazarló módon, de korlátlan mértékben tud terjedni. Ennek egyik mellékhatása, hogy a kiküldött csomagok gyakran „multicast packet" típusú címmel rendelkeznek, vagyis a legrosszabb esetben egyetlen csomag is egy egész alhálózatnyi kiszolgálót fertőzhet meg! Ez a technika eddig ismeretlen volt.

A Slammer vírusról szóló jelentésben a *CAIDA* munkatársai kifejtik, hogy ez a féreg alapul szolgálhat olyan jövőbeli változatok kifejlesztéséhez, amelyek még gyorsabban terjednek, és nagyobb káoszt hagynak maguk után. „Ha a Slammer írói elterjedtebb szoftvert vagy biztonsági hiányosságot választanak célpontjuknak, és pusztító rutinnal egészítik ki a féregvírust, minden bizonnyal sokkal komolyabb kárt okozhattak volna" – áll az elemzésben.

A Microsoft 2002 júliusa óta ismerte azt az SQL 2000 biztonsági hibát, amelyet a Sapphire kihasznált, és amelyre a javítás meg is jelent júliusban. Sajnos jellemző, hogy mind a különböző operációs rendszerekre, mind pedig az alkalmazásokra kiadott hibajavító biztonsági javításokat NEM futtatják le a rendszergazdák, csak miután azok hiánya problémát okozott.

A Vírus Híradó portál hiteles és naprakész tájékoztatást nyújt a vírusokról, és hasznos információkkal látja el a PC-felhasználókat

A Slammer írói – valószínűleg szándékosan – kihagyták a büntető rutinjukat, igazság szerint a tömeges fertőzésen túlmenően jelentős adatvesztést okozó pusztítást is véghez tudtak volna vinni. Az is szándékosnak látszik, hogy éppen a hétvégére időzítették a támadást, amikor a munkavállalók és a számítástechnikai szakemberek jó része nincs a munkahelyén.

A Slammer leglényegesebb tulajdonsága, hogy viszonylag könnyen lehet védekezni ellene – de nem víruskeresővel. A víruskeresők ugyanis merevlemezünk állományait vizsgálják folyamatosan, ez a vírus azonban sohasem ölt állományformát. Jelen lehet a gép memóriájában és a hálózaton is, fájlként azonban sosem találjuk. Fertőzési módja a számítógépeket feltörő crackerek, illetve az egymás adatait lopkodó kollégák módszereit idézi: a hálózatot felhasználva támadja és fertőzi meg célpontjait, a víruskeresők számára mindvégig láthatatlanul.

Mire jó a tűzfal?

Hogyan védekezzünk akkor? Mit tehetünk a Slammerhez hasonló járványok, a gépünket célzó ismerősök és kollégák, ismeretlenek ellen? A megoldás a hálózati forgalom elemzése. Ezt legtöbbször a tűzfalak végzik, amelyek a vállalati hálózatok ki- és bejövő forgalmát ellenőrzik. Saját kollégáink ellen azonban nem védenek meg, és ugyanez a helyzet akkor is, ha például egyszerű internet-felhasználóként otthonunkból kapcsolódunk a hálózatra. Nincs mit tenni, saját gépünk védelmére egyedi tűzfal kell. Ezeknek két fő fajtája is ismeretes, a vállalati és otthoni felhasználás igényeihez igazodva. A személyi tűzfalak a nagy és bonyolult vállalati tűzfalak védelmét adják – egyetlen gépnek. Feltelepítve a felhasználó szabályozhatja, ki és hogyan férhet a gép adataihoz, erőforrásaihoz. Mivel beállítása a felhasználó aktív közreműködését igényli, a dokumentáció tanulmányozására nagy szükség lesz.

Vállalati környezetben az igények és az elvárások is mások az effajta eszközökkel szemben. Itt rendszerint elosztott tűzfalakat használnak. Ezek hasonló elven működnek, mint a személyi tűzfalak, ám felügyeletüket, beállításukat, karbantartásukat a vállalat rendszergazdája végzi. Ily módon a felhasználók védetté válnak egymással és a külső veszélyekkel szemben, miközben egyáltalán nem kell bonyolult hálózati fogalmakkal megismerkedniük, érthetetlen műszaki kérdésekre hasukra ütve válaszolniuk.

Az elosztott és a személyi tűzfalak egy lépéssel tovább viszik a számítógépek védelmét. A statikus, állományokban kereső vírusvédőkre továbbra is szükség lesz – ám a dinamikus, a hálózatot aktívan felhasználó támadások, fertőzések ellen csakis ezekkel védekezhetünk hatékonyan.

Fórján Tamás, Csizmazia István
2F 2000 Kft.

Veszélyesebb vírusok 2003-ban

Veszélyesebb és nehezebben detektálható vírusok megjelenését helyezte kilátásba 2003-ra *Kimmo Alkio*, az *F-Secure Corporation* alelnöke.

2002-ben új típusú fenyegetések jelentek meg: a vírusok terjedése Linux rendszereken, a nyílt forráskódot kihasználó támadások, az otthoni számítógépekbe való betörések egyre gyakoribbá válása és az ázsiai vírusírók egyre növekvő aktivitása rengeteg munkát adott az adatbiztonsággal foglalkozó cégeknek.

Az új technológiák, a sok platform, valamint a mobil- és a vezeték nélküli eszközök rohamos terjedésével együtt nő a potenciális támadások száma is.

Mindezek a fenyegetések nagy lehetőséget, komoly piaci potenciált tartogatnak a biztonsági cégek számára. Kimmo Alkio szerint azonban a megfelelő megoldás kiválasztásánál ma már egyre nagyobb szerepet kapnak a könnyen menedzselhető, „mobil vállalati" biztonsági rendszerek, és egy ilyen komplex biztonsági szolgáltatás esetében a márkanév és a hozzá fűződő tapasztalat is egyre inkább meghatározó szempont.

Az F-Secure – melynek magyarországi disztribútora a *2F 2000 Kft.* – 10%-os piaci részesedéssel bír a magyar piacon.

A hazai felhasználók informálása érdekében a 2F 2000 Kft. munkatársai 2002 novemberében elindították a *Vírus Híradó* portált (**www.virushirado.hu**), amely magyar nyelven nyújt hiteles és naprakész tájékoztatást a vírusokról, s hasznos információval látja el a PC felhasználókat.

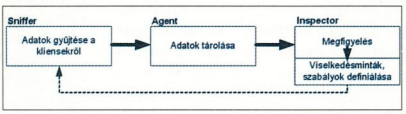
Titkosügynök

Lassan átalakul társadalmunk szemlélete az informatikai biztonság mibenlétét és felelősségét illetően. Immár nálunk is elérkezett az idő egy minden részletre kiterjedő adatvédelmi termék megjelenésére. Ez a termék a Megatrend Rt. által kifejlesztett ISee.

Röviden összefoglalva az *ISee* funkcióit: a termék mindent megfigyel, rögzít, az engedélyezett akciókat hagyja, a tiltottakat nem hagyja végbemenni, összegzi a tapasztalatokat, a kockázatot viselkedési modellek alapján a *mesterséges intelligencia* segítségével menedzseli. Vagyis az IT szakképzettséggel nem rendelkező főnök is tud értékelni és beavatkozni, azaz képes az „elvárható" tevékenység végrehajtására, a biztonság érdekében. Ezáltal mentesül az esetleges nem kívánt jogkövetkezményektől, amelyektől azok tarthatnak, akik a mai üzleti és egyéb területeken felértékelt informatikai rendszerek kockázatait nem, vagy nem megfelelően kezelik.

Mivel az IT támadások túlnyomó többsége még az internet mai fejlettsége mellett is elsősorban a belső munkatársak részéről érkezik, *az ISee logikus módon a kliensekre koncentrál, és IP alapú kommunikációt használ,* tehát bármilyen nagygépes erőforrásra támaszkodó hálózaton is életképes. Jelenleg teljes körűen a *Microsoft,* a *Unix,* a *Novell* és a *Banyan Vines* hálózatokon tudja ellátni a szerverek védelmét.

Az ISee moduljai – a *Sniffer,* az *Agent* és az *Inspector* – különálló egységek, amelyek önállóan, azaz off-line üzemmódban is működőképesek.



Az ISee működési modellje

Sniffer

A Sniffer a kliensgépeken futó kisméretű és kis erőforrás-igényű, *a háttérben észrevétlenül működő* alkalmazás, amely – egy speciális megoldás révén – láthatatlan a fájlrendszerben. A Sniffer az alábbi aktivitásokról szolgáltat az *Inspector* által meghatározott módon és mélységben információt:

1. Képernyőtartalom
2. Perifériák aktivitása (billentyűzet, flopi, printer, CD-ROM stb.)
3. Fájlaktivitás
4. Szoftveraktivitás (operációsrendszer, alkalmazás)
5. Hálózati aktivitás

A Sniffer hálózat nélküli, *off-line üzemmódban is működőképes.* Ekkor a helyi adattárolóra dolgozik (a létrehozott adatállomány rejtett), és ha újra online állapotot észlel, azonnal szinkronizál az *Agenttel,* s átküldi az off-line állapot alatt keletkezett adatokat. Az Inspector a Sniffer off-line állapotáról értesül.

A felügyelet módja a képernyő esetében: a képernyő grafikus tartalmáról teljes másolatot készít, hasonlóan a PrintScreen utasításhoz.

A képmásolat jellemzői:

- Egyedi képformátum
- Digitális vízjellel (rejtett digitális információkkal) ellátott
- Digitális pecséttel (név, dátum, idő) ellátott
- Részletgazdag, nagyítható, változtatható a felbontása
- Tömörített és titkosított.

Az ISee különleges *digitális vízjel* alapján azonosítja a képeket. A digitális vízjel a képet leíró bináris állományba rejtett információ, amely tartalmazza többek között a digitális pecsétet és a fájl *bináris ellenőrző összegét.* Az ISee a bináris ellenőrző összeg révén győződik meg arról, hogy a képet nem próbálták retusálni. Az ISee teljes mértékben kizárja a törlés, módosítás vagy a másolás lehetőségét, ha a menedzsment ezt is előírja. Hasonlóképpen kézben tartható a billentyűzet és az alkalmazások is, így azután gyakorlatilag csak ez engedélyezett tevékenységekre van lehetőség a felügyelt gépen.

Agent

Az *Agent* modul tevékenységének fókuszában az adattárolás, az Inspector utasításainak a végrehajtása *(Parancs-végrehajtó),* a rendszer integritásának állandó monitorozása, illetve a *Digitális Integrátor* által létrehozott külső kommunikációk menedzselése áll.

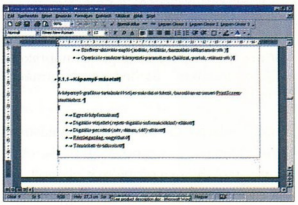
Parancs-végrehajtó

A Parancs-végrehajtó az Inspector utasításainak szakszerű végrehajtásáról és a műveletek visszaigazolásáról gondoskodik. A végrehajtás jellege lehet azonnali, eseményvezérelt, időzített és ciklikus, illetve manuálisan vagy automatikusan kezdeményezett. Főbb funkciói: a riasztási utasítások és beavatkozások végrehajtása és nyugtázása.

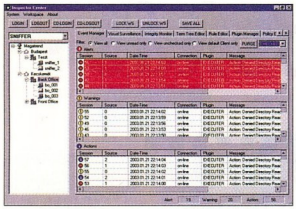
Integritás monitor

A *Rendszer-integritás* monitor feladata az ISee rendszer moduljainak, a modulok legkritikusabb funkcióinak, a megfigyelés alá vont kliensek megfelelő működésének, illetve a különböző rendszerelemek kapcsolatának állandó felügyelete.

- *Sniffer:* online, off-line állapot figyelése, Sniffer aktiválás/deaktiválás, a telepítési vagy illegális eltávolítási kísérletek naplózása stb.



Képernyő felügyelet



Az eseménykezelő (Event Manager)

- *Inspector:* az adatbázis hozzáférések naplózása, a vezérlő paraméter-állományok létrehozásának és módosításának naplózása stb.
- *Agent:* Fekete Doboz adatbázis-konzisztencia vizsgálat, behatolási kísérletek naplózása, utasítások nyugtázásának nyomon követése stb.

Digitális Integrátor

Az ISee speciális része a *Digitális Integrátor,* amelynek segítségével a külső intelligens biztonságtechnikai berendezések kétirányú információs és vezérlési szintű kommunikációját valósíthatjuk meg. Segítségével megoldható a külső digitális biztonsági eszközök vezérlése, illetve az adatok fogadása ezekből a rendszerekből. Ilyen például egy kamera, amely a belépési jelszó begépelésekor vagy más programozott esemény bekövetkezte esetén rögzíti a képet.

Inspector

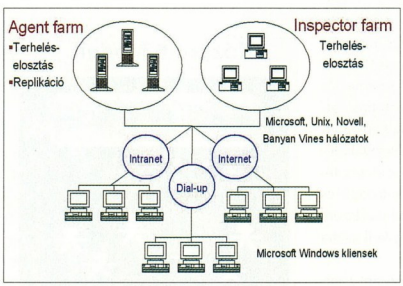
Az Inspector Center (IC) alkalmazás szolgál a kliens felügyeleti, elemzési és beavatkozási tevékenységek, funkciók ellátására. Az IC interaktív és ergonomikus kezelői felületet biztosít nagy felhasználószámú és kiterjedt informatikai rendszerek megfigyeléséhez.

Event Manager

Az *Event Manager* a rendszer eseményeinek magas szintű feldolgozására készült felület. A rendszerben zajló eseményeket három szinten *(Alerts, Warnings, Actions)* kezelve kínál a megfigyelő személyzetnek gyors és hatékony beavatkozási lehetőséget. Az egyes bejegyzésekre kattintva részletes információt kapunk az adott eseményről, illetve a rendszer az azonnali beavatkozási lehetőségekről is tájékoztatja a kezelőt. A képernyőn a bal oldalon látható hálózati tallózó panelen találjuk az aktív és passzív klienseket. A vizuális segédeszköz segítségével akár távolról is telepíthetünk Sniffer alkalmazásokat a kliensekre.

Rule Editor

A *Rule Editor* segítségével komplex „ha ez-és-ez bekövetkezik, akkor tedd ezt-és-ezt" típusú mondatok *(scriptek)* fogalmazhatók meg, amelyek összességükben egy-egy csoportra vagy egyénre jellemző viselkedésmintákat határoznak meg. Az ISee számos beépített fájl-, alkalmazás-, biztonsági, hálózati és kulcsszó típusú szabályt tartalmaz, amelyek a felhasználók által szabadon bővíthetők. Programozni is egyszerű, és a scriptek tárházát kapják a felhasználók, amely még mesterséges intelligencia nélkül is hatékony. Az egyik legfontosabb alkalmazása a vizuális felügyelet és a távbeavatkozás.



ISee topológia

A *Visual Surveillance* funkció lehetővé teszi bármely kliensen folyó tevékenység online megfigyelését. Tetszőlegesen beállítható a képernyő-frissítési frekvencia, de akár teljes képernyős valós idejű megfigyelés is lehetséges. A felület lehetőséget kínál több kliensen folyó munka egyidejű ellenőrzésére, kicsinyített képfotók segítségével.

A *Remote Console* funkció terminálkapcsolatot inicializál a kijelölt klienssel, amelynek segítségével az adott távoli fájlrendszerben böngészhetünk. A videóberendezésekhez hasonlóan az észlelt események rögzíthetők, visszajátszhatók.

Topológiai jellemzők

Az ISee alkalmas nagy kiterjedésű és felhasználószámú heterogén LAN és WAN hálózatok megfigyelésére. A terhelés elosztására mind az Agent, mind pedig az Inspector farmokba szervezhető. Távoli telephelyeken önálló Agent telepíthető, amely folyamatosan replikál a központi Agenttel. A Sniffer minimális sávszélességet igényel, így akár vékony modemes vagy internet-kapcsolaton keresztül is biztosítja az online adatszolgáltatást.

A rendszer biztonságáról

A rendszer egésze és a rendszer komponensei önmagukban is képesek eleget tenni a fokozottan kritikus környezetek biztonsági elvárásainak. A rendszer készítői a különböző kockázati szinteknek megfelelően több módszert is alkalmaztak.

1. *Minden modul képes az önreprodukcióra.* Technikailag ezt az úgynevezett *Shadow* (árnyék) teszi lehetővé, amely rejtett alkalmazásként állandóan figyeli az adott modul státuszát, illetve értesül arról, ha valaki „közelébe kerül" a kritikus alkalmazásoknak, fájloknak, és beavatkozik, mielőtt a működésben zavar támadna. Az önreprodukcióra kidolgozott egyedi technológia lehetővé teszi, hogy a folyamat alatt is működőképes maradjon a rendszer.
2. *Minden modulnak saját szabályrendszere van* arra az esetre, ha valamilyen okból elszigetelődne a többi modultól. A Sniffer esetén beállítható például, hogy off-line esetben helyi adattárolóra dolgozzon, vagy felfüggessze a gépet, amíg újra online állapotot nem észlel.

A biztonság biztonságáról

Elsőre úgy gondolnánk, hogy egy ilyen hatékony és kisméretű szoftver, amely gyorsan távolba is juttatható, nem más, mint egy vírus. Természetesen az eddigi felhasználók és a termékkel ismerkedők fő kérdése az, hogy vajon biztosítható-e ennek a hatalmas „erőforrásnak" a kordában tartása. A válasz: szerencsére igen. A Sniffer csak ellenőrzötten és azonosítottan kerülhet bármely számítógépre. A „terjesztőket" pedig ugyenez a rendszer felügyeli, akik így nem menekülhetnek.

Hecks Ferenc

Hálózati azonosítás – biztosan és gyorsan

A hálózati kommunikáció egyik legfontosabb kérdése a felhasználók biztonságos azonosítása, s lehetőleg minél gyorsabb beléptetése a rendszerbe. Erre nézve több cég is kidolgozta a maga legjobbnak vélt megoldását. Írásunkban a Sun idevágó technológiai eljárását mutatjuk be, amely máris elnyerte több nagyvállalat tetszését.

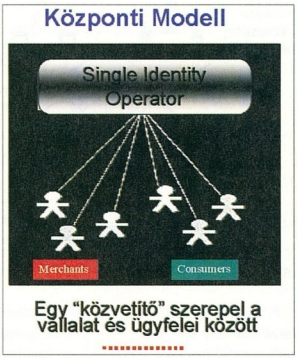
Mr. Smith vagy Kovács úr, mint minden reggel, ma is besétál munkahelyére. Leül számítógépe elé, és bejelentkezik a vállalati hálózatba. Mivel adatai védelme érdekében az általa használt alkalmazások jelszóval védettek, vállalatirányítási, döntéselőkészítési-elemző programja, adatbázis-kezelő és webes alkalmazásai vagy e-mail rendszere használatához újra és újra meg kell adnia felhasználónevét és jelszavát.

A *Gartner* tavalyi felmérése szerint a jelszómódosítások költsége átlagosan 51 és 147 dollár között mozog cégenként, csak az ezzel eltöltött munkaidőre számolva. Az átlagosan több mint tíz különböző rendszert működtető vállalatok háromnegyede nem rendelkezik a felhasználók adatait szinkronizálni képes eszköztárral, illetve a webalapú szolgáltatásaik hozzáférés-védelmét többségüknél egyáltalán nem szabályozzák.

A *Meta Group* tanulmánya arra mutatott rá, hogy a 10 ezer főnél több alkalmazottat foglalkoztató vállalatok helpdesk hívásainak 45%-a jelszavak módosításából áll. A legtöbb esetben a vállalati adatkezelés nem egységes, a különböző információkat több helyen tárolják, visszakeresésük sokszor rendkívül nehézkes vagy menedzselhetetlen. A szabályozatlan adatkezeléssel törvényi, illetve személyiségi jogi előírások sérülnek.

Hálózati azonosítás

A *hálózati azonosítás* az évtized, vagy inkább az évszázad legmeghatározóbb kérdése, amely a vállalat legfontosabb értékéről szól – a közösségekről. Ügyfelekről, részvényesekről, partnerekről vagy alkalmazottakról, akiket a vállalati versenypozíciók megtartása érdekében idejüket jelentősen kímélő szolgáltatásokkal kell támogatni. Nem is szólva arról, hogy az egységes azonosítási infrastruktúra megteremtésével, az egyes külső és belső felhasználók adatainak egységesítésével és a különböző hozzáférések szabályozásával a napi működés sokkal költséghatékonyabbá válik.



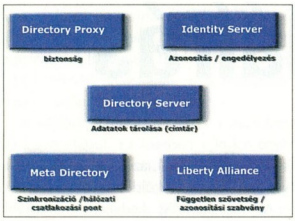
A központi modell kiépítése a hálózati azonosítás alapja

Liberty Alliance

Legutóbbi Adatbiztonság különszámunkban már írtunk arról, hogy a *Sun Microsystems* vezetésével jelentős lépésekre került sor az egységes és biztonságos adatkezelés megteremtése érdekében, a tavalyi év őszén megjelent úgynevezett *Liberty Alliance* szabvány új specifikációjával.

A szabvány a Sun frissen kiadott szervertechnológiai újdonságában – a *Sun One Identity Server 6*-os verziójában – már helyet kapott. A felhasználói azonosítást és az egyes adatok hálózaton keresztüli elérhetőségét még hatékonyabban menedzselő új technológia már nem csupán a vállalaton belüli adatforgalom karbantartási feladatait, hanem a vállalatközi információáramlást is lehetővé teszi.

Az elosztott modellben már minden résztvevő egyenrangú félként vesz részt



Az azonosítást végző rendszer összetevői

A rendszer alapja a Sun Microsystems már működő *Directory Servere*, a címtár, amely az azonosítás alapjául szolgál. Itt egy helyen tárolják valamennyi felhasználói adatot. Erre épül fel az azonosítást és az engedélyezést végző *Identity Server*, illetve az egyes szolgáltatások futását lehetővé tevő egyéb interfészek. A rendszer igen nagy előnye, hogy az egyes elemeket nem kell külön megvásárolni, hanem az alapcsomag részeként mindegyikük azonnal rendelkezésre áll.

Identity Server

Az Identity Server szabványos internetes környezetben (HTTP, XML, SOAP, UDDI, WSDL, Java) működik. A felhasználók azonosítása és engedélyeik kiadása az úgynevezett *SAML (Security Assertion Markup Language)* segítségével történik, amellyel a felhasználói jogok egyénileg testreszabhatók. A felhasználók egyszerűen igénybe vehetik a vállalati hálózat vagy most már akár a teljes közösség online szolgáltatásait, és mindössze egyszer kell megadniuk a felhasználói azonosítót és jelszót. A számukra engedélyezett szolgáltatások beállításait saját maguk is el tudják végezni, jelentősen csökkentve ezzel a központi rendszeradminisztrációs költségeket.

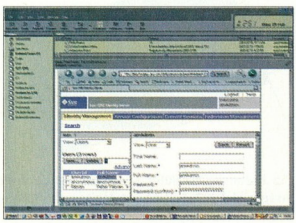
Amit azonban a felhasználó nem lát az az, hogy a rendszert kialakító hálózati szakember milyen modellt választ az azonosítási feladatok ellátására. A hagyományos *központi modellben* a szerver feladata a „közvetítő" szerep ellátása a vállalat és ügyfelei között. Itt minden adat a vállalaton belül és kívül a szerveren fut keresztül. A másik modellben, az úgynevezett *elosztott modellben* az adatforgalom több egyenlő rangú partner bevonásával történik: itt a hálózat már nincsen egy kézben, az azonosítási és az engedélyezési folyamatok menedzselése már nem oldható meg az egységes használatot lehetővé tevő szabványok, mint a Liberty alkalmazása nélkül.

Hasznos linkek

www.sunonetools.com
www.sun.com/software
www.sun.com/identity
www.sun.hu/products/sunone
www.sun.com
www.projectliberty.org

Elosztott modell

Az elosztott modell működése legjobban a pénzautomaták szolgáltatásainak fejlődéséhez hasonlítható. Először minden bank kiépítette saját ATM rendszerét, ahol az egyes automaták csak az adott bank által kiadott kártyákat fogadták el. A következő lépésben olyan hálózatok épültek ki, amelyek kártyatípus szerint csoportosították az automatákba behelyezett bankkártyákat. A mai fejlett rendszerek pedig már teljesen átlátható módon azonosítják és engedélyezik a készpénzes tranzakciókat bármely hálózat vagy akár a kiadó bankok szerint. A Sun szakemberei szerint az elosztott azonosítási rendszert több lépcsőben kell kiépíteni, különös tekintettel a hazai hálózatokra, ahol az online kommunikáció fejlettsége még sok kívánnivalót hagy maga után.



Az Identy Server webes felületein a különféle beállítások egyszerűen és gyorsan elvégezhetők

Az elosztott modell szerint létrehozott hálózatban tehát Mr. Smith vagy Kovács úr mindössze egyszer jelentkezik be, ha például üzleti útjára interneten rendeli meg a repülőjegyét és bérelt autóját. Ferihegyen minden gond nélkül felszáll Frankfurt felé. A baj akkor kezdődik, amikor átszálláskor üzemzavar miatt 2 órával később indul tovább, ezért 2 órával később érkezik meg a tengerentúlra. Az előre lefoglalt bérelt autó a késés miatt nem áll többé rendelkezésére, és a cégével kapcsolatban álló autókölcsönző nem tud másik autóval szolgálni. Mr. Smith vagy Kovács úr a késés miatt fontos üzleti tárgyalástól esik el.

Elosztott hálózatok

Nézzük, hogyan is jutnak el egyes hálózatok a központi azonosítási rendszerből a korszerű elosztott hálózatok kialakításához.

Azonosítási infrastruktúra kialakítása:

Az első lépcsőben a vállalati intranet működésének vizsgálatára, a leltárra és az igények felmérésére kerül sor. Ezután terveket dolgoznak ki a hálózati azonosítás infrastrukturális felépítésére.

Azonosítási szolgáltatások:

A tervezés eredményeként kiterjesztett intranetes hálózat már biztonságosabb és egyszerűbb hozzáférést tehet lehetővé a felhasználók számára. A megoldással nő az ügyfelek elégedettsége, mert gyorsabban, egyszerűbben és biztonságosabban vehetnek igénybe meglévő és új szolgáltatásokat. A rendszer szolgáltatásait ekkor már külső partnerek is igénybe vehetik, akik rákapcsolódnak a zárt hálózatra.

Elosztott internetes hálózat kialakítása:

A meglévő zárt intranetes szolgáltatást kiterjesztik az internetre is. Az elosztás azonosítást nem egy, hanem egyszerre több cég szerverei látják el.

A Liberty Alliance lényege éppen az előbbi probléma elhárításában rejlik: a szabványt alkalmazó egyes szolgáltatók állandó kapcsolatban állnak egymással, és ilyen esetben automatikusan értesítik egymást. Ha a felhasználó úgy dönt, hogy két szolgáltatást össze kíván kapcsolni – esetünkben a repülőjegy foglalást és az autókölcsönzést –, akkor a két, különben teljesen különálló rendszer egy rendszerként kezd működni.

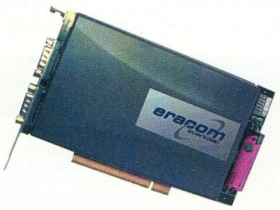
A Liberty létrejöttét, mint a fenti példa is megvilágítja, inkább üzleti szempontoknak köszönheti. Láthatjuk, hogy a mára már mintegy 150 nagyvállalat által támogatott szabvány elterjedése igen nagy jövő áll, hiszen az azonosítási procedúra jelentős leegyszerűsítésén túl az új partnerek vagy hálózatok bekapcsolása a meglévő szolgáltatási infrastruktúrába minden egyes résztvevő elemi érdeke.

Kemény László

Tinta, pecsét, aláírás

Dédapáink, nagyapáink, ha adásvételre került a sor, vették a kalapjukat, és elsétáltak a jegyzőhöz. Ott illő tisztelettel előadták mondandójukat, a jegyző pedig tintába mártogatott tollal elkészítette a szerződést, amelynek az aljára őseink és a tanúik odakanyarították a kézjegyüket. Az utóbbi száz évben vajmi kevés változott: a kézjegy, a papír maradt, csak a tintatartó és a kalap tűnt el.

Évek óta várjuk, hogy elérkezik a papír nélküli irodák kora, de a papírgyárak a megmondhatói, hogy az irodai papírfogyasztás nemhogy csökkent volna, inkább nőtt az irodai számítástechnika terjedésével. Ha előbb-utóbb mégsem kell majd minden hivatalos ügyet személyesen intéznünk, tanúk előtt, saját kezű aláírásunkkal igazolva, hogy az iratot elolvastuk, annak tartalmával egyetértünk, az csakis az *elektronikus aláírási* rendszernek lesz köszönhető.



Az Eracom CSA8000 adaptere mindenben megfelel a minősített hitelesítés-szolgáltatás követelményeinek

Fokozott biztonság

Számos, itteni leányvállalattal rendelkező multinacionális cégnél működik saját használatú belső tanúsítványrendszer, amely az alkalmazottak belső és külső levelezését, illetve a cég állandó partnereivel folytatott üzleti ügyek – megrendelések, számlák stb. – tanúsítását szolgálja. Ám ezek a vállalatok közül is több érdeklődik megbízható harmadik fél – azaz csúcshitelesítő – szolgáltatásai iránt. Az elektronikus adóbevalláshoz és elektronikus számlázáshoz ugyanis a pénzügyi jogszabályok értelmében minősített aláírásra van szükség. Az első minősített hitelesítésszolgáltató Magyarországon a *NetLock Kft.*, amely nemrég kapta meg az idevágó jogosítványokat. Fokozott biztonságú tanúsítványokat öt hazai szolgáltató bocsáthat ki: a *Giro Rt.*, a *Matáv Rt.*, a *MÁV Informatika Kft.*, a *Microsec Kft.* és a már említett NetLock Kft. Ez utóbbi eddig körülbelül százezer tanúsítványt bocsátott ki.

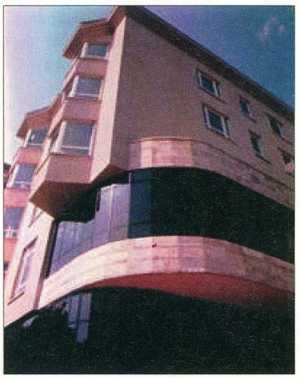
Ugye az már nemcsak a gyerekeink számára természetes, hogy telefonon rendeljenek pizzát vagy mozijegyet, fizetni pedig ráérnek a mozipénztárban, illetve a pizzafutárnál? (A „jobbak" már az interneten nézik meg a moziműsort, és pizzát sem telefonon, hanem a netpincéreknél rendelnek.) Ám a „vérbeli" netezők sem boldogulnak minden ügyes-bajos dolgukkal online. Vegyük például a következő esetet! Valamelyik internetszolgáltató előfizetőiként van egy „rendes" postafiókunk, amelyik vígan betölti a szerepét mindaddig, amíg csak a család egyik tagja használja levelezésre. A gyerekek azonban nőnek... Minthogy a csomag négy postafiókra ad lehetőséget, nosza, kérjük el a többi hármat is! A kérelem benyújtható telefonon és e-mailben egyaránt, az előfizető-azonosító szám, a bejelentkezési azonosító és a titkos belépési kód megadásával, az új postafiók jelszavát azonban faxon küldi el a szolgáltató.

Az egyszerűség kedvéért maradjunk annyiban, hogy az e-mailben megadott információk nem kerülnek rossz kezekbe, csakis az ISP ügyfélszolgálatához jutnak el. Ott a kérést iktatják, intézkednek, és hamarosan megérkezik a jelszó – faxon. Persze érkezhetne e-mailben is, de a biztonság kulcsa ezúttal a fax: nehezebb röptében lehallgatni. A másik lehetőségbe – hogy az e-mailes üzenetváltást elcsípi valaki – rossz belegondolni.

Védett levelek

Vajon hányan tartanak otthon faxkészüléket? A szolgáltató nem kockáztat. Mi igen. Igaz, hogy az e-mail alján szereplő aláírást is elektronikus aláírásnak nevezik, de az nem bizonyítja sem azt, hogy a levelet valóban a postafiók előfizetője írta, sem azt, hogy abba más nem kontárkodhatott bele. Hogyan lehetne mellőzni a jó öreg faxot?

A nyilvános hálózaton úgy lehet szavatolni a felek személyazonosságát, valamint az adatok sértetlenségét, ha a küldeményeket digitális pecséttel, hitelességigazoló tanúsítvánnyal látják el. Példánknál maradva tehát az internetszolgáltató és ügyfele akkor rendezheti az érzékeny levélvál-



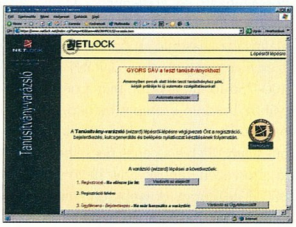
A NetLock székháza – egyedüliként a magyar piacon

tást online, ha *mindkét fél rendelkezik ilyen tanúsítvánnyal*. Ezt a tanúsítványt természetesen független, hiteles szervezetnek – a hitelesítő hatóságnak vagy hitelesítési szolgáltatónak – kell kiállítania.

A legelterjedtebb megoldás a *nyilvános kulcson* alapul. Ez esetben a kulcs egyik fele a feladónál van, azt elvileg csak ő használhatja, a másik, nyilvános kulccsal viszont a címzettnek kell ellenőriznie az üzenet hitelességét. Egyezés esetén biztos lehet abban, hogy a levelet (megrendelést, számlát, adóbevallást stb.-t) valóban a feladó küldte. A nyilvános kulcs tanúsítvány ugyanis a nyilvános kulcs tulajdonosának azonosítására szolgáló adatokból (név, országkód, város stb.), a hitelesítő hatóságot azonosító adatokból és magából a nyilvános kulcsból áll, de tartalmazza a tanúsítvány lejárati idejét, típusát is. Hitelessége annak köszönhető, hogy a kibocsátó hiteles szervezet titkos kulcsával is alá van írva, ezért az ellenőrzés során történő felfedés nélkül nem változtatható meg.

Aláírásgyár

Hogyan készül az elektronikus aláírás? A feladat látszólag egyszerű: a dokumentumról hash algoritmus segítségével fix hosszúságú, 128 vagy 160 bites lenyomatot állítunk elő, majd a privát kulcs a lenyomat kódolásával generálja az eredeti szöveghez és annak előállítójához, pontosabban privát kulcsához tartozó elektronikus aláírást.



A Tanúsítvány-varázsló lépésről-lépésre végigvezet a regisztráció, a bejelentkezés, a kulcsgenerálás és a belépési nyilatkozat készítésének folyamatán

A fogadó oldalán ennek a fordítottja megy végbe: az elektronikus aláírás ellenőrzéséhez szükség van az eredeti szövegre, az aláírásra, az aláírás-ellenőrző algoritmusra, az aláírás készítéséhez használt privát kulcs nyilvános párjára, illetve a tanúsítványra és a hash algoritmusra. Az aláírás segítségével állapítható meg a küldő személyazonossága. Az aláírásban lévő hash, illetve az üzenetből készíthető lenyomat összehasonlítható. Amennyiben a két lenyomat megegyezik, biztosak lehetünk abban, hogy a szöveg az elektronikus aláírás óta nem változott.

Amennyiben hivatali és pénzügyeinket is a világhálón intézzük, szükségünk lesz fokozott biztonságú elektronikus aláírásra, ha pedig teljes bizonyító erejű aláírásra volna szükségünk, amilyen a két tanú előtt kézjegyünkkel ellátott irat, *minősített tanúsítványt* kell szereznünk. A magyar törvények értelmében a minősített elektronikus aláírás olyan elektronikus aláírás, amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki. A biztonságos aláírást létrehozó eszköznek kell szavatolnia, hogy az aláírás készítéséhez használt privát kulcs aláírónként más és más, továbbá titkos, nem rekonstruálható, az aláírás nem hamisítható. Vagyis a privát kulcs tárolására nem alkalmas holmi öreg PC. Minősített eszközzel Magyarországon eddig két cég rendelkezik: a *NetLock Kft.* és a *MÁV Informatika Kft.*

Az eszköz persze még nem minden: a minősített aláírás-hitelesítési szolgáltatás-

Az elektronikus aláírás kisszótára

Elektronikus aláírás

Elektronikus adatok hitelesítésére szolgáló, matematikai algoritmussal készített, s az elektronikus üzenetek, dokumentumok végéhez csatolt kódsorozat. Lehetővé teszi, hogy minden elektronikusan aláírt üzenet olvasója ellenőrizni tudja az üzenetküldő személyazonosságát, az üzenet sértetlenségét. A küldő magánkulcsával készül, és annak nyilvános kulcsával (illetve az azt tartalmazó tanúsítványával) lehet ellenőrizni hitelességét. Dokumentumfüggő, azaz az aláírt üzeneten történt bármilyen változás ténye az ellenőrzéskor egyértelműen kiderül.

Fokozott biztonságú elektronikus aláírás

Olyan elektronikus aláírás, amely alkalmas az aláíró azonosítására, és egyedülállóan hozzá köthető; olyan eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll; a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető. A fokozott biztonságú aláírás az aláíró fél fokozott biztonságú tanúsítványával ellenőrizhető. Ilyen igazolásokat az aláíró félnek fokozott biztonságú hitelesítésszolgáltatók állíthatnak ki. A fokozott biztonságú aláírással ellátott elektronikus irat a magyar jog szerint írásbeli dokumentumnak számít.

Időbélyegző

Elektronikus irathoz, illetve dokumentumhoz az időbélyegző-szolgáltató által csatolt, a bélyegzés időpontját is tartalmazó elektronikus aláírás. Feladata bizonyítani, hogy az adott elektronikus dokumentum a bélyegzés időpontjában már létezett.

Minősített elektronikus aláírás

Olyan elektronikus aláírás, amelynek létrehozásakor az aláíró fél biztonságos aláírás-létrehozó eszközt használt, és hitelesítése céljából minősített tanúsítványt bocsátottak ki az aláírónak. Ilyen igazolást az aláíró félnek minősített hitelesítésszolgáltatók állíthatnak ki. A minősített elektronikus aláírással ellátott elektronikus irat a magyar jog szerint teljes bizonyító erejű magánokiratnak számít, amilyen a papír alapú világban a két tanú előtt történő aláírással hozható létre.

RSA

Az egyik legelterjedtebb nyilvános kulcsos titkosító algoritmus.

Tanúsítvány

A hitelesítésszolgáltató által elektronikusan aláírt igazolás, amely megbonthatatlanul tartalmazza a tanúsítvány tulajdonosának azonosítására szolgáló adatokat (pl. nevét, elektronikus címét) és a tulajdonos nyilvános kulcsát. Az elektronikus aláírások ellenőrzésekor használjuk.

Visszavont tanúsítvány

Amennyiben a felhasználó magánkulcsa kompromittálódik (például ellopják, elveszítik, a felhasználó elfelejti a jelszavát), úgy a hozzá tartozó tanúsítvány használatát megakadályozandó, a tanúsítványt vissza kell vonni. Ezzel a tanúsítvány és a visszavonás oka felkerül a visszavont tanúsítványok listájára.

hoz a sok millió forintos beruházáson, jól védett számítógéptermen, megbízható célhardveren kívül sokéves működési garanciákra van szükség. Például arról is gondoskodni kell, hogy a szolgáltató csődje esetén a nála tárolt tanúsítványokat másik szolgáltató vegye át. A minősítést megelőző audit hónapokat vesz igénybe: az auditorok több száz szempont alapján vizsgálják meg a pályázó cég működését, eljárásait, eszközeit, szabályzatait és szakemberhátterét.

Közép-Európa első minősített hitelesítésszolgáltatójánál, a budapesti NetLock Kft.-

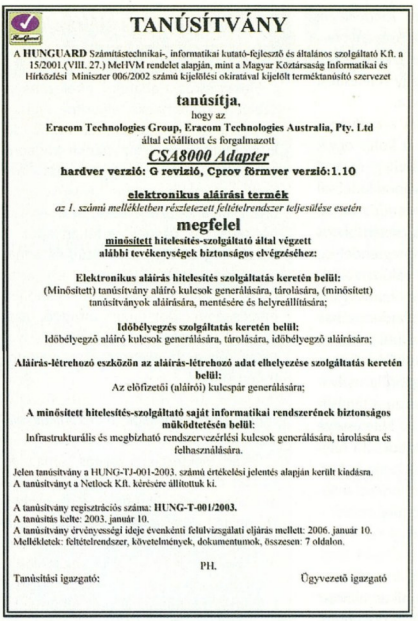
Minősített NetLock

Az elektronikus aláírás hosszú évekre visszatekintő hazai szabályozásának egyik legjelentősebb mérföldkövéhez érkeztünk nemrég: a *NetLock Kft.* 2002. november 4-én beadott minősítési eljárás lefolytatására vonatkozó kérelmét a *Hírközlési Felügyelet* sikeresnek minősítette, így a NetLock Kft. 2003. március 19-től Magyarországon elsőként jogosult minősített tanúsítványok kibocsátására.

A NetLock Hálózatbiztonsági Kft. Magyarország első nyilvános szolgáltatásokat végző, fokozott biztonságú hitelesítés szolgáltatója. A cég szakembergárdájával a szükséges eljárások bevezetése és felügyelete mellett az infrastruktúra technológiai fejlesztését, honosítását és működtetését is végzi. Kis- és közepes vállalatok teljes nyilvános kulcs infrastruktúrájának (PKI) kiépítése mellett technológiája alkalmas akár országos méretű rendszerek kiépítésére is.

A magyar nyilvános kulcs infrastruktúra első hitelesítés szolgáltatójaként foglalkozik a tanúsítványok biztonságos kommunikációban való felhasználását végző tranzakció titkosító eszközök telepítésével és folyamatos támogatásával, teljes, kulcsrakész rendszerek fejlesztésével, azok biztonságos aláíró eszközökkel (pl. intelligens kártyákkal) való kiegészítéseivel.

A cég négy éve egyedüli közép-európai hitelesítés szolgáltatóként szerepel a *Microsoft* operációs rendszereiben az ajánlott tanúsítványkiadók listáján. A *Magyar Posta Rt.*-vel való együttműködésnek, illetve a *Közjegyzői Kamara* közjegyzői hálózatának köszönhetően szolgáltatásai az országban bárhol elérhetők.



TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 15/2001.(VIII. 27.) MeH IVM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Minisztere 006/2002 számú kijelölési okiratával kijelölt terméktanúsító szervezet

tanúsítja,

hogy az

Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd

által előállított és forgalmazott

CSA8000 Adapter

hardver verzió: G revizió, Cprov förmver verzió:1.10

elektronikus aláírási termék

az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel

minősített hitelesítés-szolgáltató által végzett alábbi tevékenységek biztonságos elvégzéséhez:

Elektronikus aláírás hitelesítés szolgáltatás keretén belül:
(Minősített) tanúsítvány aláíró kulcsok generálására, tárolására, (minősített) tanúsítványok aláírására, mentésére és helyreállítására;

Időbélyegzés szolgáltatás keretén belül:
Időbélyegző aláíró kulcsok generálására, tárolására, időbélyegző aláírására;

Aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás keretén belül:
Az előfiztetői (aláíróí) kulcspár generálására;

A minősített hitelesítés-szolgáltató saját informatikai rendszerének biztonságos működtetésén belül:
Infrastrukturális és megbízható rendszervezérlési kulcsok generálására, tárolására és felhasználására.

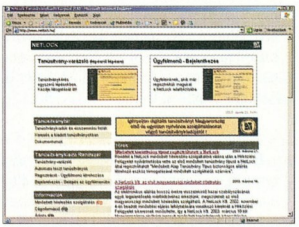
Jelen tanúsítvány a HUNG-TJ-001-2003. számú értékelési jelentés alapján került kiadásra.
A tanúsítványt a Netlock Kft. kérésére állítottuk ki.

A tanúsítvány regisztrációs száma: **HUNG-T-001/2003.**
A tanúsítás kelte: 2003. január 10.
A tanúsítvány érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2006. január 10.
Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen: 7 oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

Az Eracom adapter tanúsítványa részletesen leírja az eszköz alkalmazhatósági körét



A NetLock honlapján minden a tanúsítványokról „szól"

nél a *ProtectServer Orange CSA8000*-es kriptográfiai adapter feladata a minősített tanúsítvány-aláíró kulcsok generálása, tárolása, a minősített tanúsítványok aláírása, mentése és helyreállítása, az időbélyegző aláíró kulcsok generálása, tárolása, az időbélyegző aláírása.

Saját pecsét

A kiemelt adózóknak tavaly már elektronikusan kellett benyújtaniuk a bevallásokat. Egy lépés a papírhegyek felszámolása felé. A következő lépések egyikét talán éppen az olvasó teszi meg. A tanúsítvány megszerezhető online, csak ki kell választani a megfelelő tanúsítványfajtát, és végig kell haladni a regisztrációs pontokon. E folyamat során a böngésző, illetve – ha van – intelligens kártyánk segítségével elektronikustanúsítvány-kérelem készül. Végül, a kiválasztott tanúsítvány fajtájától függően, vagy elektronikus levéllel, vagy közjegyző előtti személyes megjelenéssel kell igazolnunk kilétünket. A tanúsítvány ezután tölthető le.

Mint említettük, az egyszerű elektronikus aláírás mellett még két típust különböztet meg a törvény: a *fokozott biztonságú* és a *minősített* elektronikus aláírást. A fokozott biztonságú aláírásnak a NetLock Kft.-nél három aláírási osztálya van: *expressz* (e-mailben plusz faxon szerezhető meg), *üzleti* (ehhez személyesen kell megjelenni a szolgáltatónál vagy valamelyik postahivatalban, s fényképes iratokkal kell igazolni a személyazonosságunkat) és *közjegyzői* (az igazolás közjegyző előtt történik). A kézzel írott aláíráshoz hasonló módon használható személyes tanúsítvány fajtától függően 400–750 forintba kerül, míg a névjegykártyához hasonló szerepet betöltő, az illető beosztását is tartalmazó névjegykártyás tanúsítvány, illetve a céges pecséthez foghatő szervezeti tanúsítvány nettó havi ára 800–1500 forint. A webszerverekkel folytatott kommunikációban használható szerver tanúsítványért 1600– 2600–3000 forintot kell fizetni, osztálytól függően.

Előfordulhat, hogy a tanúsítványt az érvényességi idő lejárta előtt vissza kell vonni, például azért, mert a magánkulcs elveszett, felmerült a visszaélés gyanúja, avagy a kulcsbirtokos adataiban változás következett be. A visszavont tanúsítványok a szolgáltató nyilvános tanúsítvány-visszavonási listáján szerepelnek.

-i

Hogyan

takaríthat meg

33%-ot?

Rendelje meg a CD-melléklettel megjelenő Computer Panorámát a következő három hónapra, kéthavi áron 2590 Ft-ért!

** Az akcióban kizárólag olyan kedves vásárlóink vehetnek részt, akik még nem voltak előfizetőink.*

Megrendelem a Computer Panorámát a következő 3 hónapra 2590 Ft-ért.

Név: _____

Cím: ☐☐☐ _____

út / utca / tér *hsz.*

Telefon, Fax: _____

E-mail: _____

Információ: www.computerpanorama.hu

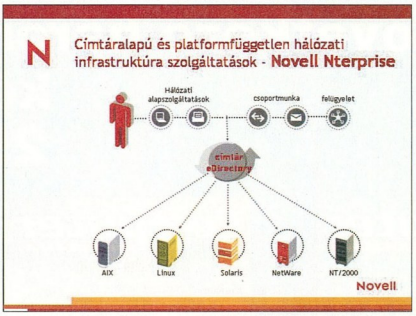
Biztonságos személyazor

Az informatikai rendszerek biztonságának az alapja a személyazonosság-kezelés. A Novell biztonságos személyazonosság-kezelési megoldása a cégek számára lehetővé teszi, hogy alkalmazottaik, ügyfeleik és partnereik egyszerűen és gyorsan hozzáférjenek a munkájukhoz szükséges adatokhoz és alkalmazásokhoz, miközben a cég információi és erőforrásai minden részletre kiterjedően biztonságosan védettek.

eDirectory

A címtárak segítségével biztonságos, mindent átfogó, egyszerűen használható hálózatot építhetünk ki. A címtár alapú struktúra egyik nagy előnye, hogy az összes hálózati erőforrás (adatok, alkalmazások, nyomtatók, internet stb.) mindenki számára könnyen elérhető, és a felhasználóknak nem kell azzal törődniük, hogy hol is vannak a szükséges erőforrások, vagy hogy azok éppen szabadok-e. Mindez láthatatlan lesz számukra, egyben sokkal átláthatóbb lesz a rendszergazdák számára, így az egész rendszer sokkal könnyebben menedzselhetővé és biztonságosabbá válik. A címtár alapú rendszerek legnagyobb előnye az, hogy egyre több alkalmazást, funkciót, illetve szolgáltatást tudunk erre ráépítve viszonylag könnyen bevezetni, és így hálózatunk egyre intelligensebbé válik.

A Novell címtárszolgáltatása, az *eDirectory* (korábban *NDS*) egy skálázható, biztonságos, kiforrott, többplatformos eszköz, amelynek használatával egységes informatikai infrastruktúrát tudunk kialakítani.



A Novell Nterprise integráltan tartalmazza a címtár-alapú és platform-független hálózati szolgáltatásokat

Platformfüggetlenség

Az eDirectory több platformot támogat, mint bármely más címtárszolgáltatás, hiszen az alábbi operációs rendszereken használható:

- IBM AIX
- Linux
- Microsoft Windows NT 4.0
- Microsoft Windows 2000 Server, Advanced Server
- Novell NetWare 5.x és 6
- Sun Solaris.

Egységes jogosultságkezelés

Az eDirectory-t telepítve nincs többé szükség arra, hogy a programok bonyolult algoritmusokkal, külön jelszavakkal ellenőrizzék a hozzájuk forduló felhasználó jogosultságát. Elegendő, ha a címtárhoz fordulnak információért. Különösen előnyös ez a megoldás a belső vállalati információs rendszerben, mert egyfelől a felhasználót nem terheli felesleges adatokkal (nem kóborolnak sajtcédulák a számítógépek körül bejelentkezési azonosítókkal, jelszavakkal), másfelől egy központi adatbázisban áttekinthetően mutatja meg, ki mihez férhet hozzá, s mihez nem. Erre a nyilvántartásra ráépíthető a folyamatos követés is, s rögzíthető, kiről mikor melyik program kért a címtárból adatot, azaz ki mikor mivel dolgozott.

Rugalmas és skálázható felépítés

Az eDirectory mögött álló hierarchikus adatbázis *rugalmas* és *skálázható*. Rugalmas, mert ráilleszthető a vállalat működési modelljére. A cég a fizikailag más-más helyen található egységeit ugyanúgy képes leírni, mint a vállalat különböző osztályait, munkacsoportjait. A címtár skálázható is, mert az egyszerveres, öt munkahelyes vállalati hálózat adatait éppen úgy tudja kezelni, mint a multinacionális nagyvállalatok több száz irodájának és gyárának összes erőforrását és a hozzájuk kapcsolódó információkat.

Biztonsági szolgáltatások

A teljes vállalatot átfogó hálózat esetén a menedzselhetőség mellett a *biztonság* a legfontosabb kérdés. Az eDirectory alapú rendszerek biztonságára utaló legjellemzőbb tény az, hogy az eDirectory-ra épülő és a rendszer biztonsági funkcióit használó hálózatokkal kapcsolatban semmilyen betörési módot nem sikerült még kidolgozni, pedig a Novell címtárszolgáltatása, mint technológia már tíz éve a piacon van.

Az eDirectory esetében minden jogosultság, így a felügyeleti jogok is finoman szabályozhatók. Könnyen kialakíthatók különböző üzemeltetési funkciók, és minden rendszergazda csak azokhoz a beállításokhoz férhet hozzá, amelyekre szüksége van a munkájában.

Az eDirectory a *Novell Modular Authentication Services (NMAS) Standard*

osság-kezelés

Edition változatát is tartalmazza, fejlett jelszókezelési funkciókkal és a tanúsítvány alapú bejelentkezés támogatásával. Az eDirectory másik fontos biztonsági komponense a *NICI (Novell International Cryptographic Infrastructure)*.

A NICI úgy segíti elő a globális hálózat kialakítását, hogy nem kell aggódni a helyi titkosítási törvények miatt. A NICI moduláris megközelítése miatt a titkosítás erősségét, vagy akár az alapját adó algoritmust egyszerűen módosíthatja a Novell vagy más szoftverfejlesztő cég. Bármilyen alkalmazás használhatja a NICI által nyújtott titkosítási szolgáltatásokat egy megfelelő csatoló segítségével, és a NICI moduláris architektúrája a törvények vagy a követelmények változásának megfelelően módosítható, az ezt használó alkalmazás módosítása nélkül.

SecureLogin

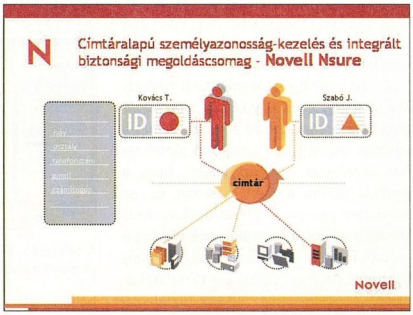
A Novell *SecureLogin* megoldása számos biztonsági rendszer integrálásával kínál egypontos bejelentkezést a hálózat legkülönbözőbb erőforrásaihoz és alkalmazásaihoz. A megoldás segítségével kialakítható az egypontos beléptetési rendszer, növelhető a biztonság, továbbá megvalósíthatók és alkalmazhatók a vállalat különböző biztonságpolitikai előírásai.

Egyszerűbb jelszóhasználat

Napjainkban a legtöbb vállalatnak és szervezetnek egy alapvető biztonsági problémával kell megküzdeniük: a különféle alkalmazások és rendszerek mind saját azonosítóval és jelszóval rendelkeznek, arra kötelezve ezáltal a felhasználókat, hogy nagyszámú információt tartsanak fejben. Ez a probléma a jövőben még mélyülhet is, az internetes alkalmazások gyors elterjedésével. Mivel a technológia villámgyorsan fejlődik, az újabb és újabb alkalmazások jelszavainak ismerete egyre nagyobb terhet ró a felhasználókra, és nem várható el tőlük, hogy valamennyit meg tudják jegyezni.

Mivel a felhasználó egy idő után a különféle alkalmazásokhoz és rendszerekhez tartozó adatokat nem tudja megjegyezni, biztonságosnak egyáltalán nem mondható megoldásokhoz folyamodik: kiragasztja a jelszavát a monitorra, elmenti a bejelentkezéshez szükséges adatait egy szöveges állományba, vagy éppen ugyanazt a könnyen megjegyezhető jelszót használja minden rendszerében.

A Novell SecureLogin használatával a felhasználók biztonságosan, egyetlen



A biztonságos személyazonosság-kezelés eszköze a Novell Nsure

eDirectory-jelszón keresztül férhetnek hozzá valamennyi hálózati alkalmazáshoz – függetlenül attól, hogy ezek az alkalmazások milyen platformon futnak, és hol tárolják a felhasználói azonosítókat és jelszavakat. A Novell SecureLoginnel a teljes hitelesítési folyamat láthatatlanná, ugyanakkor sokkal hatékonyabbá válik.

A SecureLogin működése

A SecureLogin a bejelentkezéshez szükséges adatokat vagy közvetlenül egy tetszőleges LDAP címtárban vagy a *Secret Store* technológiával megerősített Novell eDirectory-ban tárolja. Futás közben automatikusan észreveszi a bejelentkezésre vagy azonosításra szolgáló felületeket, majd kikeresi és megadja az authentikációhoz szükséges adatokat. A SecureLogin script-nyelve a termék lényeges komponense. Az egypontos beléptetés támogatására fejlesztett speciális nyelv jóvoltából a termék közel valamennyi hálózati környezetben és alkalmazással használható. Az egyszerűen megtanulható programozási nyelvnek köszönhetően a beléptető környezet könnyen implementálható és módosítható, illeszkedve a gyorsan változó vállalati környezethez.

A SecureLogin segítségével központilag határozhatjuk meg azt is, hogy mely alkalmazások kerüljenek be az egypontos bejelentkezésbe, és melyek legyenek azok, amelyek továbbra is azonosítót és jelszót kérnek a felhasználótól. Az olyan alkalmazások esetében, amelyeknél időről-időre jelszót kell változtatni, központilag meghatározható, hogy a SecureLogin a háttérben változtassa-e meg a jelszavakat automatikusan, amikor erre szükség van, vagy a felhasználót kérje meg új jelszó megadására. Jelszó-irányelvek megadásával pedig az adminisztrátorok a különböző alkalmazásokhoz használt jelszavak bonyolultságát is szabályozhatják.

A SecureLogin minden működési adatát az LDAP címtárban, illetve – titkosítva – a kliens gyorsítótárában (a cache-ben) tárolja. Ezeknek az adatoknak a központi felügyelete a címtárban oldható meg, mégpedig a Novell eDirectory alkalmazása esetén a Java-alapú *Novell ConsoleOne* termékkel, egyéb címtár használata esetén a címtárhoz adott felügyeleti eszközzel.

- f

Támogatott alkalmazások

A Novell SecureLogin jól integrálható a vállalatoknál meglévő különféle alkalmazásokkal. A termék többek között az alábbi program típusokat támogatja:

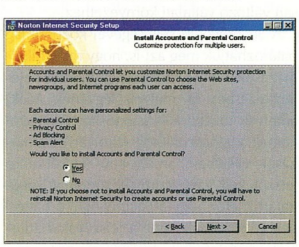
- 32 bites Windows-os alkalmazások
- Terminálszerveres környezetek (pl. Microsoft Windows 2000 Terminal Services)
- E-mail programok (Novell GroupWise, Lotus Notes, MS Outlook stb.)
- IBM nagygépes alkalmazások
- Unixos alkalmazások
- Több mint 30-féle terminálemulátor
- Webes alkalmazások
- Közel 100 alkalmazáshoz biztosít előkészített beléptető scripteket
- Varázslók új alkalmazások integrálásához.

Dobozba zárt biztonság

A Windows operációs rendszer – miközben igen elterjedt a munkaállomásokon és az otthoni gépeken – meglehetősen védtelen a rosszindulatú vírusos, illetve hálózatos támadásokkal szemben. A fenyegető veszélyek közepette hatékony védelmet kínálnak a Symantec biztonsági csomagjai, a Norton Internet Security és a Symantec Client Security.

A munkaállomásokat, otthoni gépeket védő szoftveres tűzfalak nem számítanak már újdonságnak az ingyenesen vagy dobozosan elérhető szoftverkínálatban. Az egykor jó csengésű *AtGuard* shareware terjesztésű személyes tűzfalként élte meg a *3.22*-es verziószámot, amikor is a jól paraméterezhető programot megvásárolta a *Symantec*, és most annak termékeiben él tovább. A Symantec dobozos termékei közül a kisebb cégek, otthoni irodák és „szabadidős" számítógépek számára a *Norton Internet Security 2003*, míg a nagyobb hálózatok munkaállomásainak integrált biztonságának megteremtésére a *Symantec Client Security* csomag telepítése szolgáltatja a védelmet.

Ezek közül a Norton Internet Security modulként tartalmazza a *Norton Personal Firewall 2003* személyes tűzfalat, s a dobozban megtalálható még a *Norton Antivirus* legújabb, *2003*-as verziója is. Az utóbbi lényeges kiegészítő eleme a gép védelmének, beleértve a levelekben terjedő kártevők elleni védelmet is. Az említett programok önálló modulként képesek integrálódni a Symantec Windows-os gépekre fejlesztett karbantartócsomagjánál, a *Norton SystemWorks*-nél megszokott keretrendszerbe, mely utóbbi csomag szintén elérte a 2003-as verziószámot.



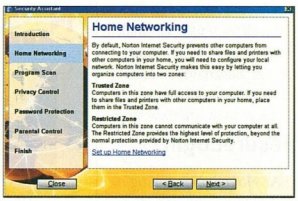
Telepítésekor az extra komponenseket is felvehetjük a rendszerbe

A személyes tűzfal legújabb változatában kivétel nélkül megtaláljuk a korábban megszokott biztonsági elemeket. Így például azt is, amely az internetes kapcsolatok egyik leglényegesebb pontján őrködik, a kapcsolat felépítésének ellenőrzésével. A NPF ugyanis – a tűzfalakra jellemző szabályrendszeren alapulva – minden új hálózati kapcsolat kialakulásakor ellenőrzi a tűzfalszabályok listáját, s ennek alapján eldönti, hogy az adott kapcsolat engedélyezhető-e, netán meg kell akadályozni. Ez egyben azt is jelenti, hogy az illetéktelen kapcsolatoktól való védettség mindkét irányban megoldott.

A tűzfalszabályok megalkotását több tényező segíti. Ezek egyikét az *előrekonfigurált biztonsági szintek* alkotják. A másik jelentős segítség az *önműködő tűzfalszabály-létrehozás*, ami azt jelenti, hogy a legtöbb széles körben használt és az interneten jogosan közlekedő alkalmazás számára a NPF automatikusan kialakítja a szóban forgó alkalmazásra szabott és annak működéséhez szükséges tűzfalszabályokat. Ugyanakkor az *egyedi tűzfal-szabályrendszer* kialakítása is megoldható, amelyet külön varázsló támogat. Ezzel az elsősorban némi hálózati ismeretekkel rendelkezőknek szánt lehetőséggel a hálókapcsolati irányok, a kapcsolati protokollok (TCP, UDP, ICMP), a kapcsolódó alkalmazások, valamint a kapcsolati kapuk (portok) szerinti hangolást oldhatjuk meg.

A számítógépek közötti kapcsolat ellenőrzésére különféle zónák alakíthatók ki, és a Norton Personal Firewall által védett számítógéppel való kapcsolatok tekintetében akár *tiltott zóna* is kialakítható. Az otthoni hálózat kezelését, illetve felismerését külön varázsló, a *Home Network Wizard* támogatja, és ez segít abban is, hogy a saját gépeket a megbízható zónához rendelhessük.

Ami a külső próbálkozásokat illeti, ebben jelentős segítségünkre lehet a portok vizsgálatának automatikus felismerése. Így abban az esetben, ha valaki kívülről próbálja megtalálni a rendszer sérülékenységeit, az *AutoBlock* funkció önműködően megakadályozza a rendszerhez való hozzáférését. Működésekor az AutoBlock önhelyesbítést idéz elő a tűzfal működésében, és a támadó IP-címével fél óráig minden kapcsolatot megakadályoz.



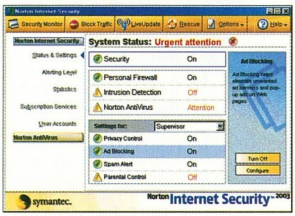
A telepítést követő első induláskor varázsló gondoskodik a helyi beállításokról

A behatolások védelmével kapcsolatban további védelmi rétegként az internetes forgalom tartalmának vizsgálata is bekerült a kínálatba: az NPF felismeri az olyan nethasználó támadókat, mint amilyen a méltán elhíresült *CodeRed* is volt, és amelyik nem maradt sajnos követők nélkül. Behatolás gyanúja esetén ebben az esetben is a további adatforgalom megakadályozása a legjobb védekezés.

Az illetéktelen behatolások megakadályozásán kívül az NPF a digitális magánéletet is védi, így például kirekeszti a *sütiket*. Ezek kiszűrése egyébként webhelyenként beállítható, ami azt is jelenti, hogy az említett webhelyek nem követhe-

tik nyomon a böngészési szokásokat. A magánélet védelmének továbbfejlesztett lehetőségeként a bizalmas információ kijutását a szabványos POP3-as levelezőprogramok, a *Microsoft Office* csatolmányok, az *MSN Messenger*, a *Windows Messenger* és az *AOL Instant Messenger* esetében is megakadályozza.

Több védelmi, illetve olykor kényelminek tekinthető szolgáltatás a böngészéssel kapcsolatos. A szülők például továbbra is megtilthatják csemetéiknek bizonyos weboldalak látogatását, a napi munkában pedig jó szolgálatot tesz a felugráló ablakok kiszűrése. Ezeknek az opcióknak a rendszerbe iktatásáról a programcsomag



A beállítópanelen figyelmeztetést kapunk a kikapcsolt funkciókról

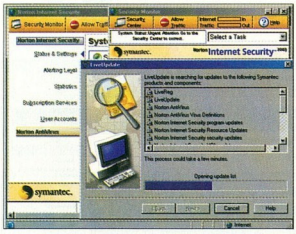
telepítésekor intézkedhetünk.

A hálózati munkaállomások, illetve a vállalati rendszerbe távolról, virtuális magánhálózati (VPN) kapcsolaton keresztül bejelentkező asztali rendszert természetesen azokkal az egyedi eszközökkel is megvédhetjük, melyek általában is alkalmasak az otthoni gépek, illetve az izolált munkahelyek megvédésre. Egy központilag felügyelt rendszerben azonban még akkor is hátrányosak lehetnek az izolált megoldások, ha azokat egy gyártótól szereztük be. Mert minél nagyobb egy hálózat, annál körülményesebb az egyes gépeken elvégezni a telepítéseket, nem is szólva a folyamatos karbantartásról. A biztonsági rendszerek esetében ugyanakkor a napra, vagy rázósabb helyzetben akár órára készen tartás különösen lényeges, aminek az illusztrálására elegendő az órák, napok alatt a földkerekség gépszázezreit fertőző vírusjárványokra gondolnunk.

A céges rendszerek munkaállomásainak központilag felügyelhető megóvására szolgál a *Symantec Client Security*. A VPN-kapcsolatok megvédésére ugyancsak alkalmazható csomag integráltan nyújt vírusvédelmet, személyi tűzfalat és behatolás-érzékelést (IDS), ami a rejtettebb fenyegetések ellen is hatékony segítséget jelent. Márpedig a nagyobb rendszerek esetében erre azért is szükség van, mert itt elég lehet egy-egy munkaállomás áldozattá válása ahhoz, hogy onnan kiindulva az egész rendszer összeomoljon, vagy támadhatóvá váljon.

A felhasználó, amikor a Symantec Client Security telepítését követően a gépe elé ül, hasonló képernyővel találja magát szemben, mint a NIS telepítését követően. A tűzfal tevékenységét ugyanúgy kísérhetjük nyomon egy kis földgömb segedelmével, és a tűzfallogót is hasonlóan érhetjük el. Ami azonban lényeges különbség, hogy míg a különböző zónák beállítása a szóló otthoni gép esetében nem létkérdés, a hálózati munkaállomás esetében a rendszerelérés egyik feltétele. A rossz beállítások hatása itt azonnali, mert a net is elérhetetlenné válik.

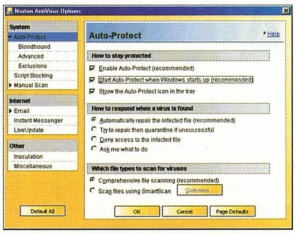
A Symantec Client Security telepítésekor felkerülő vírusvédelem is kicsit más, mint a szokványos, otthon megszokott NAV. Nem a védelem bináris képességeit tekintve, hiszen védelmi képességei természetszerűen éppen úgy kiterjednek valamenynyi kártevőre, hanem olyan szempontból, hogy a *Symantec Antivirus Corporate Edition* esetében a hálózati meghajtókat is végigkutathatjuk a nem éppen szívesen lá-



Külön monitorral folyamatosan figyelemmel kísérhetjük a biztonságunkat, illetve a Live Update-tel menet közben frissíthetjük a biztonsági alkalmazást

tott vendégek után, és a levelezés ellenőrzése is kézben tartható. Ugyanakkor jelentős segítség lehet a biztonságtechnikai háttér megteremtésében a behatolási kísérletek felderítése.

A *Symantec Client Firewall* kezelőpaneljén engedélyezhető behatolás-felderítő és behatoló-blokkoló funkció azt jelenti, hogy a hálózati forgalom nem csak szűrésre, hanem elemzésre is kerül. Így a szokványos tűzfalfunkciók mellett egyfajta forgal-



A Norton Antivirus funkcionalitását is finoman hangolhatjuk kívánságaink függvényében

mi minta is vizsgálhatóvá válik, ami például a portfürkészés leleplezésének a legegyszerűbb módja. Az IDS-modul által tapasztalt mintázat összehasonlítható azzal, amit korábban a *Symantec Security Response* csapata azonosított. Ezeket a mintaállományokat a *LiveUpdate*, a vírusadatbázishoz hasonlóan, folyamatosan frissíteni képes. A naprakész mintakészlet alapján pedig az újabb, a szimpla portfürkészésnél lényegesen kifinomultabb betörési módszerek is lefülelhetők. Az azonosított behatolási kísérlet nyomán az AutoBlock modul veszi át a támadó IP-címét, és 30 percre leállítja a vele folytatott kommunikációt. Például az ilyen „félreértések" miatt is célszerű jól beállítani a bizalmi zónákat a kliens tűzfalán.

A rendszerszintű funkciókat az említett központi menedzsment infrastruktúra teszi elérhetővé a biztonságért felelős rendszergazda számára. Erre azért is szükség van, hogy a teljes rendszerben *egységes biztonsági szemlélet* alakulhasson ki.

Ennek az átfogó rendszernek az egyik vetülete a cég információbiztonsági szabályzata, amelyet be is kell tartatni. Ehhez gondoskodni kell a szükséges eszközök központi felügyelhetőségéről. De arról is, hogy a szükséges eszközök központilag „leoszthatók" legyenek a munkaállomásokra.

A Symantec Client Security telepítésekor komplett készletből választhatunk, így az egyetlen menedzsmentkonzolon keresztül a munkaállomásokon teljes egészében telepíthetők, beállíthatók és kezelhetők a biztonsági komponensek. A telepítendő egységcsomagok természetesen egyedileg is összeállíthatók, de támaszkodhatunk a gyári mintacsomagokra is. A Symantec Client Security telepítésekor a programütközések elkerülése végett célszerű a NAV és a NIS korábbi telepítéseit eltávolítani.

Simay Endre István

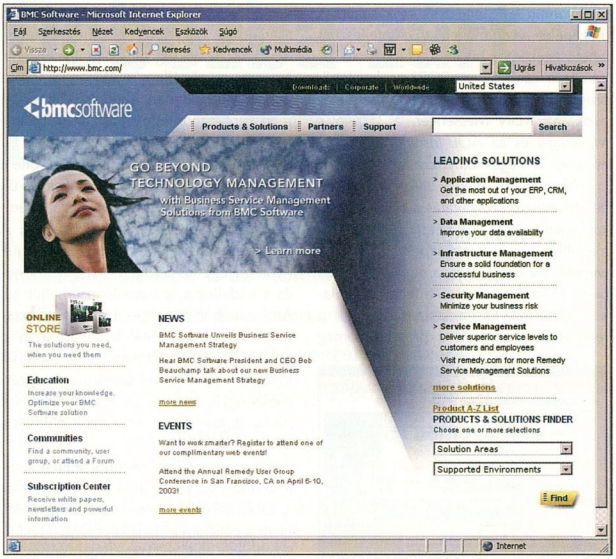
Bővített felügyelet

A BMC Software továbbfejlesztette Control-SA nevű províziós megoldását, amelynek ügyfelei – a nyílt API-knak köszönhetően – immár összekapcsolhatják a biztonsági felügyeletet a munkafolyamat automatizálását szolgáló üzleti alkalmazásokkal.

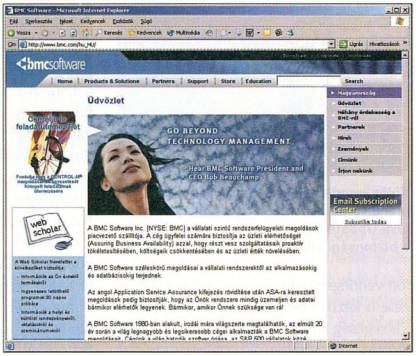
A *BMC Software Inc.*, a vállalati szintű rendszer-felügyeleti megoldások piacvezető szállítója továbbfejlesztette felhasználói províziós megoldását: a *Control-SA* ágens nélküli felügyelettel, webkonzollal, multiregionális *Enterprise SecurityStationnel*, valamint új, nyílt províziós API-kkal és egy virtuális könyvtárral bővült. Az újítások az eddigi sikeres alkalmazásokon és az ügyfelek visszajelzésein alapulnak; ezeknek köszönhetően a Control-SA rugalmas telepítési feltételeket kínál, fokozottan bővíthető, tároló részlege pedig elérhető hagyományos LDAP hívások útján. Ezen kívül az új változat nyílt API-kat is kínál, amelyek által a Control-SA ügyfelek összekapcsolhatják a biztonsági felügyeletet egyéb, a munkafolyamat automatizálását szolgáló üzleti alkalmazásokkal.

Rugalmas telepítési feltételek

A Control-SA *XpressAgent* módszere egyszerű telepítési feltételeket kínál az ügyfeleknek. Az ágens alapú és az ágens nélküli felügyelet közötti választásnak köszönhetően az ügyfelek optimálisan alakíthatják ki környezetüket. Míg az ágensek egyes területeken nélkülözhetetlen valós idejű felügyeleti lehetőségeket biztosítanak, az ágens nélküli felügyelet csökkenti a megvalósítás és a karbantartás bonyolultságát azáltal, hogy távolról képes nyomon követni a folyamatokat. Az ügyfelek igényeik szerint válogathatnak e technológiák közül, és vegyesen alkalmazhatják őket. Az alkalmazást tovább egyszerűsíti az új webalapú biztonsági konzol, a *Control-SA/Web Console*, amely gyorsítja a biztonsági adminisztrátorok munkáját, böngésző jellegének köszönhetően pedig minimalizálja a szükséges betanítást.



A BMC Software honlapja...



...és a magyar oldal

Páratlan bővíthetőség

Mivel a Multi-Region Enterprise SecurityStation a nagyobb globális vállalatok igényeit célozza meg, különböző földrajzi területekre és régiókra kiterjedően valósít meg biztonsági felügyeletet. Ez lehetővé teszi, hogy a különböző régiók a saját helyi szabályozásuknak megfelelően fel-

Control-SA a bankban

A *Kereskedelmi és Hitelbank Rt. (KHB)* nagy számú és rendkívül összetett alkalmazói rendszert működtet, melyeknek folyamatosan meg kell felelniük banki és informatikai biztonsági előírásoknak. A feladat jelentékeny részét képezi (és ennek megfelelően komoly emberi erőforrásokat igényel) a felhasználói jogosultságok kiosztása, ellenőrzése. A KHB a kialakult helyzet értékelését követően e folyamatok erőteljes központosítása és egy igényeik szerint felépített jogosultság-kezelő rendszer bevezetése mellett döntött.

A bank 2002. évi meghívásos pályázatára négy ajánlat érkezett, melyekből három a *BMC Control-SA* szoftverre alapozta megoldását. Az ajánlott technológiát tekintve a Control-SA banki környezetbe történő illeszthetősége, már rendelkezésre álló kiterjedt alkalmazás-integrációs lehetőségei és továbbfejleszthetősége bizonyult meghatározó jelentőségűnek. Az értékelés szerint az azonos technológiát kínáló cégek közül a *VT-SOFT* javasolt megközelítése, tervezési, fejlesztési és implementációs szolgáltatásai és projekt feltételei álltak a legközelebb a KHB elvárásaihoz, követelményeihez, így a projekt megvalósítására a VT-SOFT kapott megbízást.

A jogosultság-kezelő rendszer bevezetése a tervek szerint két fázisban valósul meg. A 2002. novemberében megkezdődött első fázisban a decemberben már jóváhagyott implementációs terv alapján a VT-SOFT üzembe helyezi a rendszer központi elemeit (Enterprise SecurityStation, adatbázisok), illetve a Control-SA meglévő interfészei és egy egyedileg fejlesztett alkalmazás segítségével felépíti a kapcsolatokat a bank kijelölt platformjai és rendszerei felé. A 2003. április végéig tartó első fázis alapvető célja, hogy a kiemelt rendszerek jogosultságai központilag lekérdezhetők és beállíthatók legyenek, a további rendszerek adatai pedig lekérhetővé váljanak.

A második fázisban a feladat valamennyi KHB által kijelölt alkalmazás és platform kétirányú elérése további BMC komponensek felhasználásával, illetve egyedi kapcsolati alkalmazások fejlesztésével. A Control-SA a kiépítendő rendszerben együttműködik a KHB *SAP* humán erőforrás rendszerével és a *Lotus Notes* workflow alkalmazással is.

A VT-SOFT a Control-SA képességeit egy úgynevezett *historikus lekérdező modullal* is kiterjeszti, amelynek feladata a pénzintézeti környezetben (is) elengedhetetlen auditálhatóság támogatása: a rendszer így képes visszamenőleg is kimutatni, hogy kinek mely alkalmazásban milyen jogosultságai voltak adott időszakban. Miután a KHB informatikai rendszerét alkotó közel negyven alkalmazást a bank közel 4 ezer munkatársa használja, ezért roppant lényeges a jogosultságok központi nyilvántartása, valamint a mindenkori hatósági és belső auditálhatóság.

ügyeljék a biztonságukat, ugyanakkor a központi konzol gondoskodik arról, hogy az információk összehangoltan jussanak el az ügyfelekhez, akik így átfogó képet kapnak a rendszerükről. Minden terület kizárólag a saját adatait kezeli, aminek köszönhetően a rendszer jóformán határtalanul bővíthető. A Multi-Region Enterprise SecurityStation alkalmazásának néhány további előnye:

- Jelszavak régiókon átnyúló összehangolása
- Biztosítja az adatok sértetlenségét, amihez a központi konzol szolgál háttértárként
- A Central Console távoli háttértárként funkcionál.

LDAP interfész

A Control-SA fejlesztése lehetővé teszi az LDAP hozzáférés alkalmazását. Ezáltal a Control-SA tárolójában levő felhasználói adatokhoz LDAP parancsokkal férhetünk hozzá. Az LDAP kompatibilitás biztosítása érdekében a *Radiant Logic Inc.*, a könyvtárszoftverek piacvezető szállítója *RadiantOne Virtual Directory Server* termékét kapcsolták össze a Control-SA-val.

A BMC Software eredetikészülék-gyártóként (OEM) kínálja a RadiantOne Virtual Directory Servert minden új Control-SA ügyfélnek, illetve egy karbantartási kiadás részeként mindazoknak, akik már rendelkeznek e termékkel.

Ily módon a különböző LDAP alapú alkalmazások, mint például a jelentéskészítő és auditáló eszközök felhasználói adatokat szűrhetnek ki a Control-SA tárolójából, és jelenthetik a felhasználói visszaéléseket.

A VT-SOFT a BMC egyik legfontosabb magyarországi partnere

Nyílt architektúra

A BMC Software célkitűzése, hogy előmozdítsa a nyitottságot és az interoperabilitást a Control-SA és a munkafolyamat automatizálását szolgáló üzleti alkalmazások között, vállalati környezetben. Ennek eredményeként az ügyfelek, akik üzleti folyamataik feltérképezésében alkalmazzák a munkafolyamatot, akár a BMC Software-ét, a sajátjukat vagy egyéb forrásból származót, nagyobb értéket tudnak majd termelni a Control-SA biztosította fokozott automatizálás és hatékonyság, valamint mérsékelt adminisztrációs költségek révén.

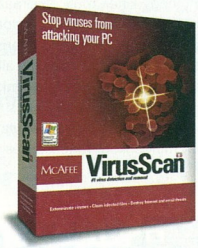
A BMC Software a szakterület vezető szereplőivel együttműködve olyan ipari szabványok kialakításán és terjesztésén munkálkodik, mint például az OASIS Service Provisioning Markup Language (SPLM).

(-)

Harcban a vírusokkal

A Network Associates (NAI) regionális igazgatója, Renske Galema asszony, februári budapesti látogatása során megosztotta velünk cége elképzeléseit az új hálózati biztonsági korszakról. Nyilatkozatából megismerhetünk továbbá néhány különleges védelmi eszközt és terméket, és bepillanthatunk a kulisszák mögé is.

Napjainkban a hálózatok és a számítógépek használói egyre több fenyegetésnek vannak kitéve: a tapasztalatok szerint a világméretű hackerhálózat, az ennél is rosszabb cyberterroristák mellett a legtöbb galibát a felkészületlen, képzetlen felhasználók okozzák. Ez kétféle igényt támaszt a biztonsági megoldásokkal szemben: egyfelől tökéletes biztonságban akarjuk magunkat érezni bármilyen informatikai fenyegetéssel szemben, másfelől viszont elvárjuk, hogy ezt a biztonságot számunkra költséghatékony módon menedzseljék – fejtette ki az igazgató asszony. Ugyanakkor mindenki azt kívánja, hogy neki, végfelhasználónak ne kelljen mindezzel törődnie, hanem végezhesse a maga dolgát. A felhasználók úgy gondolják, hogy elég lenne a védelmet csak egyszer felrakni és beállítani a gépükre, hogy aztán hadd feledkezhessenek meg róla – a gép pedig kifogástalanul működjön a háttérben.



A McAfee VirusScan komplett védelmet kínál mindenfajta támadással szemben

Renske Galema, a Network Associates regionális igazgatója

A fordulat éve

A *Network Associates* szakemberei szerint az informatikai biztonság menedzselésében 2002-ben fordulat következett be, az úgynevezett *reaktívtól* a *proaktív* megközelítés irányába.

Mit is jelentenek ezek a kifejezések?

A reaktív stratégia alkalmazása esetén, ha megjelent egy vírus, akkor azonosították, majd kifejlesztették az ellenszerét, ezután pedig a rendszerekbe bevitték a frissítést – és helyreállt a biztonság. Ezt a ciklust a vírusirtó kutatók és cégek fejlesztéseikkel egyre jobban felgyorsították, a vírusokat egyre hamarabb azonosították, a védelem is egyre hamarabb a helyére kerül. Közben azonban a vírusok terjedése is felgyorsult, a belső hálózatok és az internet fokozódó elterjedése miatt.

Az új, proaktív stratégiában a forgalomelemző szoftverek folyamatosan figyelik a hálózati forgalom alakulását, mintázatait akkor is, amikor még nincs tudomásunk valamely vírus megjelenéséről. A behatolásjelző rendszer gyanú esetén riadót fúj, és elszigeteli a gyanús kódokat, amelyek nagyon sokfélék lehetnek, ártalmasak, de ártalmatlanok is. A rendszerért

Villámkérdések...

...a Network Associates európai regionális igazgatójához.

- *Sokszor vádolják a számítógépek biztonságával kapcsolatban magukat az őröket, az ellenszert kifejlesztő cégeket azzal, hogy ők írják a vírusokat, a károkozó kódokat is. Mi itt az igazság?*

– Ezek teljesen alaptalan pletykák, semmilyen valóságalapjuk nincs. A vírusirtással foglalkozó programozók, még a sokat emlegetett elbocsátottak is, úgy gondolkoznak, hogy még véletlenül sem jut eszükbe a károkozás. Őket is érdekli egy-egy vírus forráskódja, de azt csak programozóként, mint megoldandó feladatot tudják tekinteni, nem pedig élvezni a károkozást. A versenytársak is együttműködnek: többek közt vírusmintákat cserélnek egymással. Szóval rablóból lehet pandúr, de *vírusirtóból* nem lesz *vírusíró*... Ugyan melyik nagy szoftverfejlesztő cég engedhetné meg magának ebben a kiélezett versenyhelyzetben, hogy jó hírét, megbízhatóságát akár egyetlenegy ilyen próbálkozással tönkretegye? – oszlatta el *Renske Galema* az egyik legmakacsabb informatikai tévhitet.

- *Hogyan tesztelik a vírusirtó szoftvereket?*

– A cég minőségbiztosítási részlege az Egyesült Királyságban van. Azonban itt tulajdonképpen csak koordinálják azt a világméretű hálózatot, amelyet a tesztelők alkotnak. A szoftverek úgynevezett béta-verzióját nem csak angol nyelvterületen élő kiválasztott fogyasztói csoportok tesztelik egy 6 hetes időszakban (Magyarországon például a MOL Rt.-nek is van egy tesztelő csoportja a NAI-nál). A visszajelzéseket a fejlesztők beépítik a készülő termékbe. A minőségbiztosítás fontosságát jelzi, hogy inkább későbbre halasztják az új program megjelenését, de a tesztelés eredményét mindenképpen figyelembe veszik.

A VirusScan Professional 7.0 a McAfee Firewall tűzfalprogramot is magában foglalja

felelős szakemberek ezzel időt nyernek. A rendszer az alatt is biztonságban van, amíg a vírust azonosítják, és elkészítik a megfelelő ellenszert. Kulcsfontosságúak ebben a rendszerben a sérülékenységelemző eszközök.

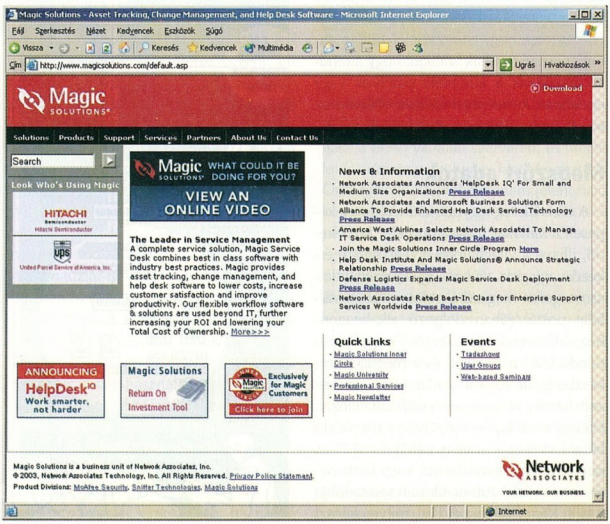
Miért vegyek vírusirtó programot?

A kelet-európai régió helyzetéről szólva az igazgató asszony elmondta, hogy a nagyvállalati szektorban 45%-ra becsülik a NAI piaci részesedését, a kis- és középvállalati szektorban 20%-ra, az otthoni felhasználók körében pedig ennél is kevesebbre. A *McAfee* vírusirtók ebben a körben is elterjedtebbek, de nagyon sokan használnak ingyenes próbaverziókat. A dobozos szoftverek piaci sikerét az azokhoz kapcsolt szolgáltatásoktól (rendszeres online frissítéstől, hírlevéltől, vészhelyzetben azonnali védelemtől stb.) várják. Hasonlóan előnyös, ha például az internetszolgáltatókhoz telepítik a vírus-, illetve spamellenőrző szoftvereket: ilyenkor a felhasználó némi többletköltségért biztonságosabb internet-kapcsolatot választhat a piacon szépen szaporodó ajánlatok közül.

A NAI nemrég vásárolta meg a *Dell Software* nevű céget, amelynek levélszemétszűrő technológiáját ezután saját termékeiben is alkalmazhatja. A *Spam Killer* nevű NAI szoftver már a piacon van, és hatékony védelmet jelent a kéretlen levelek letöltése ellen. A Network Associates már megkezdte az európai régióban a helyi nyelvű termékek bevezetését az otthoni és a kisvállalati felhasználók számára. Elsőként, idén májusban a lengyel nyelvű *McAfee VirusScan* jelenik meg, és azt hamarosan követi majd a cseh, a magyar és a többi verzió is.

Mindezt a régióban tapasztalható rohamos fejlődés is indokolja. A régió átlagában évente 25%-os forgalombővülést terveznek, Magyarországon évi 18%-ot.

F. Fülöp Hajnalka



A Magic Solutions termékcsomag menedzsment eszközök gazdag választékát kínálja a vállalatoknak

A leggyengébb láncszem – az operátor

A NAI is felismerte, hogy milyen nagy arányban a felhasználók a felelősek a legbosszantóbb biztonsági hibákért. A felhasználók informatikai biztonságának tudatossá tételére a NAI egy *online akadémiát* hozott létre, ahol biztonságos körülmények között tudják átadni a stratégiai-szemléleti tudásanyagot, amelynek végfelhasználói szintű alkalmazásával a legtöbb támadás, illetve adatvesztés kivédhető. Hasonló célt szolgálnak a tartalomszűrő szoftverek, amelyek a gyanús és veszélyes, valamint nem munkához illő webhelyek látogatását teszik lehetetlenné. A regisztrált McAfee használók egyébként úgynevezett *extra DAT*-ot és/vagy *super DAT*-ot (azaz különleges vírusdefiníciós fájlt) kapnak e-mailben, amely részletes információt és védelmi megoldást nyújt, ha bárhol a világon felüti a fejét egy kódolt kórokozó. Ekkor még van idő lezárni bizonyos portokat, vagy egyéb módon védekezni a kórokozók ellen.

A kaliforniai központú Network Associates Inc. a hálózati biztonságtechnikai és hozzáférhetőségi megoldások vezető szállítója. A hálózatkezelési és biztonsági mérnöki tudás mellett a NAI–hez tartozik az *AVERT (Anti-Virus Emergency Response Team)* is, az a csapat, amely a *LoveLetter*, a *CodeRed* és a *Nimda* vírusokat is megfékezte.

A Network Associates három megoldáscsomagot kínál. Ezek: a *McAfee Security*, amely a vírusirtó és biztonságtechnikai termékeket foglalja magában, a *Sniffer*, amely a hálózati hozzáférhetőség és rendszerbiztonság területén kínál védelmet, valamint a *Magic Solutions*, amely az innovatív szolgáltatás-menedzsment megoldások piacvezető terméke. A Network Associates stratégiai partnerei között egyaránt megtaláljuk a nagy rendszerintegrátor cégeket, mint például Magyarországon az *ICON*-t és a *HP*-t, valamint a kisebb, egyes területekre fókuszáló cégeket is, mint amilyen a *PiKSYS* vagy a *Schöller Network Control*.

2000 óta a Network Associates képviseleti irodát tart fenn hazánkban.

www.networkassociates.com
www.mcafeesecurity.com
www.sniffer.com

Mindig résen

Az internet hőskorában bonyolult feladat volt még az Unix rendszereken futó tűzfal-szerverek kezelése. A helyzet mára gyökeresen megváltozott: a rendszergazdák jobbnál-jobb, ráadásul egyszerűen kezelhető termékek közül választhatnak. A tűzfalak kínálatát újabban a WatchGuard termékcsalád is színesíti, a PiK-SYS Kft. jóvoltából.

Az „ősidőkben" a programozóknak még nem állt rendelkezésére barátságos felhasználói felület, a tűzfalak beállításához komoly rendszergazdai szaktudásra volt szükség. A technológia ráadásul sokáig elérhetetlenül drága volt. A trend mára megfordult. A vállalkozások nagy többsége – a kisvállalkozásoktól a multinacionális nagyvállalatokig – kiemelkedő figyelmet fordít webes és hálózati adatai védelmére, és ma már nem az a kérdés, hogy telepítsünk-e tűzfalat, hanem

A Firebox hardveres tűzfalak az 1-2 gépes kisvállalatoktól a sokgépes nagyvállalatokig hatékony védelmet nyújtanak

az, hogy melyik cég termékét válasszuk, és a választott rendszer mennyire felel meg a hatékony vállalati védelem követelményeinek.

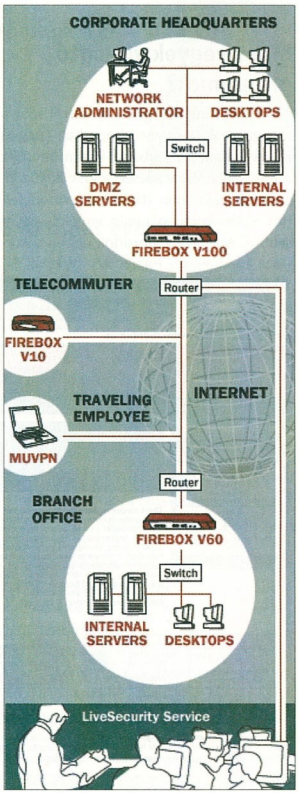
A megfelelő tűzfal használatakor nem fordulhat elő az az eset, hogy egy adott biztonsági hiányosság felfedezésekor a vállalati operációs rendszert karbantartó rendszergazda átháríthassa a felelősséget a tűzfal gyártójára és fordítva. Elfordulnak a vásárlók attól a gyártótól is, amely nem rendelkezik bővíthető termékkörrel, hiszen már egy-két év alatt is előfordulhat, hogy a felhasználó cég új alkalmazásokat telepít, új hálózatokat épít, de természetesen ezért nem akarja eldobni védelmi eszközeit, hanem arra törekszik, hogy jóval költséghatékonyabban adaptálja újdonságait meglévő rendszerébe.

A tűzfal fizikai része csak minőségi és megbízható alkatrészekből állhat annak érdekében, hogy állandó hibamentes, illetve lefagyásmentes védelmet nyújtson. A hibás tűzfal jobb esetben lezárja a vállalati hálózatot, de az is előfordulhat, hogy védelem nélkül hagyja a belső adatokat. A jobb tűzfalaknál azt is be lehet állítani, hogy a rendszer – amennyiben hiba keletkezik – pontosan mit is tegyen. Nagyobb vállalati hálózatokon a tűzfal funkcióit több szerver látja el, az első gép maga a tűzfal, egy másikon lehet elvégezni a beállításokat, egy harmadik gép feladata a logok tárolása, és akár egy negyedik számítógép látja el az engedélyezés feladatait. Sokszor egy második szervert is üzembe helyeznek, amely akkor lép működésbe, ha az első meghibásodik.

Túl a fizikai megbízhatóságon, nem kerülhető el a szoftveres környezet állandó frissítése, fejlesztése sem, hiszen az internet biztonsági réseit azonnal kihasználják a hívatlan látogatók. A gyártók ezért akár heti rendszerességgel újabb és újabb szoftververziókat bocsátanak ki. Ma már természetes, hogy a frissítések letöltése automatikusan történik anélkül, hogy a rendszergazdának a különféle patch-ek vagy update-ek keresésével kellene töltenie az idejét.

Megszűrt adatok

A tűzfalak legnagyobb előnye, hogy képesek a vállalati hálózaton belül közlekedő, illetve a világhálóról a szerverekre érkező vagy oda távozó úgynevezett adatcsomagokat megszűrni. Hasonlóan a vállalat postázójában dolgozó alkalmazotthoz, aki szelektálja a bejövő vagy elküldendő küldeményeket, és a megfelelő rekeszbe gyűjti azokat: a tűzfal az úgynevezett *header* alapján azonosítja adatainkat. Ha egy adott küldeményt nem a megfelelő helyre címeztek, vagyis például a 121-es portra, amely nem üzemel, vagy korlátozva van, a tűzfal automatikusan visszadobja a fájlt. Képzeljük el például, milyen káoszt okozna, ha egy adminisztratív dolgozó kis teljesítményű gépére nagy multimédia fáj-



A frissítésről a rendszer automatikusan gondoskodik

lok kerülnének véletlenül. Mivel a szűrő csak a header adatait vizsgálja, hatékonyan mentesíti a hálózatot a forgalom okozta lefagyástól vagy lelassulástól. A csomagok szűrésén túlmenően az úgynevezett *biztonsági proxy* nem csak a headert vizsgálja meg, hanem a csomag tartalmát is. Ha a csomag potenciális veszélyforrást, például exe kiterjesztésű fájlt vagy scriptet tartalmaz, a tűzfal közbelép és a fájl a felhasználó számára elérhetetlenné válik.

A cégek többségénél ezért igen komoly biztonsági rendszabályok léteznek, amelyek alapján a tűzfal-rendszereket konfigurálják. A ma kapható hardveres tűzfalmegoldásokkal szemben ezért alapkövetelmény, hogy a felhasználói interfész beállításai könnyen áttekinthetők legyenek, de tartalmazzák mindazokat az árnyalt beállítási lehetőségeket is, amelyeket az adott egyedi vállalati hálózati környezet megkíván.

Tegyük fel, hogy Kovács urat azonnali hatállyal elbocsátották munkahelyéről. A döntés után fontos, hogy a számítógépén tárolt bizalmas vállalati adatokhoz való hozzáférését azonnal korlátozzák. A vállalati rendelkezések gyors alkalmazása érdekében a modern tűzfal-rendszerek bármely funkciója bárhonnan, akár távolról is könnyen adminisztrálható, így egy adott hálózati konfigurációs beállítás, például a hozzáférések engedélyezése és tiltása felhasználói csoportokra, illetve egyéni felhasználókra szűkítve azonnal elvégezhető. Adott esetben Kovács úr e-mailjeit azonnal letilthatják, illetve egyes alkalmazásokhoz vagy fájlokhoz való hozzáférését akár percek alatt is korlátozhatják.

A vállalati filozófiának megfelelően ma már sok helyen azt sem nézik jó szemmel, hogy az alkalmazottak munkaidejükben magáncélra használják az internetet. A modern tűzfal-rendszerek olyan kifinomult szűrőrendszerekkel rendelkeznek, amelyek tökéletesen képesek szelektálni a felhasználók által látogatni kívánt webes tartalmakat, amennyiben az internetet nem a munkájuk miatt használják. A log fájlok elemzésével továbbá az is nyomon követhető, hogy ki honnan, hogyan, mikor mit töltött le, és milyen fájlokat továbbított vagy fogadott, illetve milyen alkalmazásokat nyitott meg.

Az is pontosan kimutatható, ha valaki kívülről vagy belülről próbál illetéktelenül adatokhoz jutni, vagy számára nem engedélyezett fájlokat megnyitni. Az ártó szándék nélküli alkalmazottak csupán „kutatnak" a belső vállalati szerveren, és megfelelő védelem nélkül nagy kárt okozhatnak. Önmagában a tűzfal még nem jelent hatékony védekezést, így együtt kell működnie például az antivírus szoftverekkel vagy egyéb hardverekkel.

Néhány évvel ezelőtt, még az internet elterjedése előtt a vállalatok titkos adatait hagyományos módon, saját futár segítségével továbbították, így biztosították azt, hogy illetéktelen kezek ne férhessenek hozzá a bizalmas információkhoz. Ma már a világháló jelentősen gyorsítja üzeneteink célbajutását, azonban a védelemről feltétlenül gondoskodni kell, mivel a hagyományos e-mail önmagában még nem biztonságos. Egyre jobban elterjed az úgynevezett virtuális magánhálózat *(Virtual Private Network, VPN)*, ahol a közvetítő közeg a világháló, de a titkosított adatok csak a küldő és a fogadó számára elérhetők.

Tűzfal vásárlása előtt először is azt kell megvizsgálni, hogy az adott cég milyen internetes kapcsolattal rendelkezik. Nyilván más tűzfal szükséges a kisebb és más a nagyobb sávszélességhez. Fontos felmérni, hogy a vállalati felhasználóknak munkájukhoz sokat kell-e használni az internetet, illetve a belső vállalati hálózaton belül milyen adatforgalom várható. Az amerikai *WatchGuard* cég, amely az idei év tavaszától Magyarországon is forgalmazza a VPN-re épülő tűzfal-megoldásait, az úgynevezett *IPSec* szabvány szerint titkosítja az információt. A szabvány gyártótól függetlenül kódolja a két vagy több egymáshoz kapcsolódó szervezet tűzfalai közötti adatforgalmat.

A WatchGuard Magyarországon

A *WatchGuard Technologies, Inc.* egyik kiemelt partnerén keresztül megkezdte termékeinek magyarországi forgalmazását. Az Egyesült Államokbeli, Seattle-i székhelyű, 1996-ban alapított WatchGuard az informatikai biztonsági megoldások egyik vezető szállítója a nemzetközi piacon. A társaság több mint 300 alkalmazottat foglalkoztat, s 1999 óta jegyzik a tőzsdén. A WatchGuard 2002-ben nemzetközi szinten 75,5 millió dolláros árbevételt ért el. A társaság termékeit elsősorban azok a vállalatok használják, amelyek üzletmenetében meghatározó az e-business és az internet biztonságos használata.

A WatchGuard főbb termékei a következők:

WatchGuard Firebox Vclass: nagyvállalati felhasználásra szánt csomagszűrő tűzfal és VPN-eszköz, Quality-of-Service funkciókkal. A hardver *RapidStream* fejlesztés, amely a hardveres tűzfalak között jelenleg az egyik leggyorsabb. Két Vclass (v80–v100) készülékből egy virtuális, dupla áteresztőképességű és magas rendelkezésre állású tűzfal állítható össze.

WatchGuard Firebox System: hardveralapú biztonsági megoldás, amely a legkülönbözőbb méretű vállalatok számára nyújt integrált tűzfal- és VPN szolgáltatásokat. A rendszer tartalmaz egy *Firebox* hardveres tűzfalat, egy irányító és monitoring szoftvert, valamint a *WatchGuard LiveSecurity* szolgáltatását, amely folyamatosan biztosítja a hálózatok biztonságát és a hálózati szoftverek legújabb verzióit.

WatchGuard Firebox SOHO: modelljei a kisvállalkozások és a kis méretű irodák számára nyújtanak tűzfal- és VPN megoldásokat, továbbá mindazoknak, akiknek DSL-, modem- vagy IDSN-kapcsolatuk van az internettel.

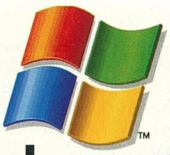
WatchGuard ServerLock: a szerverek operációs rendszereinek adminisztratív és biztonsági célzatú védelem-kiegészítő szoftvere. Az operációs rendszerbe épülve védi azt bármilyen változtatástól, legyen az belső vagy külső támadás, új program telepítése, fájlok törlése vagy megváltoztatása.

WatchGuard AppLock/Web: a Microsoft IIS webszerverek védelmére specializált, a ServerLock-hoz hasonló alkalmazás, amely elsősorban a nyilvános webszerverek védelmének elengedhetetlen kiegészítő szoftvere. Automatikusan védi a webtartalmat, a Windows operációs rendszert és az IIS webszerver szoftvert.

A WatchGuard hazai professzionális partnere, a *PiK-SYS Kft.* végzi Magyarországon a forgalmazás mellett a WatchGuard termékeinek implementálását, karbantartását és terméktámogatását.

Forrás: PiK-SYS Kft., www.watchguard.com

Kemény László



Microsoft® Windows® Server 2003

A Microsoft április 24-én, San Franciscóban jelentette be legújabb operációs rendszerét, a Windows Server 2003-at. A termék a műszaki újítások százainak köszönhetően adatközpont-szintű megbízhatóságot kínál a felhasználóknak. Írásunkban a Windows Server új biztonsági szolgáltatásait tekintjük át.

Windows, ami biztos

Napjainkra a vállalkozások kiterjesztették helyi hálózataikat: egyesítették az intraneteket, az extraneteket és az internetes helyeket. Ebből fakadóan minden eddiginél nagyobb lett a biztonság jelentősége. A számítógépes környezet biztonságának növelése érdekében a *Microsoft Windows Server 2003* operációs rendszer számos új biztonsági funkciót tartalmaz, valamint továbbfejlesztve veszi át a Windows 2000 Server rendszer részét alkotó biztonsági funkciókat.

A vírusok folyamatos fenyegetése, a szoftverek biztonsága állandó kihívást jelent. A Microsoft válasza ezekre a kihívásokra a *Megbízható számítástechnika (Trustworthy Computing)* nevű kezdeményezés, amely keretrendszerül szolgál olyan, számítógépeken és szoftvereken alapuló eszközök kialakításához, amelyek annyira biztonságosak és megbízhatók, mint napjaink bármely háztartási eszköze és berendezése.

A *közös nyelvi futtatókörnyezet (Common Language Runtime, CLR)* szoftvermotor a Windows Server rendszer kulcseleme, amely javítja megbízhatóságát, és elősegíti a számítástechnikai környezet biztonságossá tételét.

Előnyök

A Windows Server biztonságosabb és gazdaságosabb üzleti platformot kínál, amelynek az előnyei a következők:

Alacsonyabb költségek: az alacsonyabb költségek az egyszerűbb biztonság-felügyeleti folyamatokból – hozzáférés-vezérlési listák, Hitelesítő adatok kezelője, nyilvános kulcsú infrastruktúra – fakadnak.

Nyílt szabványok megvalósítása: az IEEE 802.1X protokoll révén könnyebben megóvhatók az üzleti környezetbe tartozó vezeték nélküli helyi hálózatok a lehallgatással szemben.

A hordozható számítógépek és az egyéb új eszközök védelme: a titkosított fájlrendszer *(EFS)*, a tanúsítványszolgáltatások, az intelligens kártyákhoz történő automatikus tanúsítványigénylés és más biztonsági szolgáltatások segítségével sokféle eszköz biztonságos használatának feltételei teremthetők meg.

Hitelesítés

A *hitelesítés* során a rendszer ellenőrzi, hogy egy adott felhasználó vagy objektum valóban az-e, akinek vagy aminek vallja magát. Ilyen művelet az adatok forrásának és sértetlenségének, például a digitális aláírásnak az ellenőrzése, valamint a felhasználók és a számítógépek azonosítása. A Windows Server hitelesítő mechanizmusai révén a teljes hálózat összes erőforrása egyszeri bejelentkezéssel érhető el.

Hitelesítéskor a rendszer – különféle tényezőktől függően – számos szabványos hitelesítéstípus közül választhat. A Windows Server család tagjai által támogatott hitelesítéstípusok a következők:

Kerberos V5 hitelesítés: jelszóval vagy intelligens kártyával egyaránt használható, interaktív bejelentkezés céljára szolgáló protokoll. Szolgáltatások esetén ez az alapértelmezett hálózati hitelesítési módszer.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) hitelesítés: biztonságos webkiszolgálóhoz való hozzáféréseknél használt protokoll.

NTLM hitelesítés: akkor jut szerephez, ha az ügyfél vagy a kiszolgáló a Windows valamely korábbi verzióját használja.

Kivonatoló hitelesítés: a kivonatoló hitelesítés MD5 kivonat vagy üzenetkivonat formájában továbbítja a hitelesítési adatokat a hálózaton keresztül.

Passport-hitelesítés: a Passport-hitelesítés olyan felhasználókat hitelesítő szolgáltatás, amely csak egyetlen bejelentkezést tesz szükségessé.

Az *Internet Information Services (IIS)* használatakor a hitelesítés a biztonság alapvető feltétele.

Az *IIS 6.0* egy széleskörű szolgáltatásokat nyújtó webkiszolgáló, amely biztosítja a hátteret a *Microsoft .NET*-keretrendszer és a már meglévő webalkalmazások és webszolgáltatások számára. Az IIS 6.0-t a webalkalmazások és webszolgáltatások kiszolgálói környezetben való futtatására optimalizálták.

Interaktív bejelentkezésnél a rendszer a

felhasználó azonosítását annak helyi számítógépe vagy *Active Directory*-beli fiókja alapján végzi.

A *hálózati hitelesítés* azon hálózati szolgáltatás számára végzi el a felhasználó azonosítását, amelyet a felhasználó megpróbál elérni. Az ilyen típusú hitelesítéshez a biztonsági rendszer az alábbi hitelesítési módszereket használja:

- Kerberos V5
- Nyilvános kulcsú tanúsítványok
- Secure Sockets Layer/Transport Layer Security (SSL/TLS) kivonat
- NTLM (a Windows NT 4.0 alapú rendszerekkel való együttműködés lehetősége érdekében)

Az *egyszeri bejelentkezés* révén a felhasználók hitelesítő adataik ismételt megadása nélkül férhetnek hozzá a különféle hálózati erőforrásokhoz. A Windows Server család hitelesítési rendszere *kétté-nyezős hitelesítésre* is képes, például intelligens kártyák használatával.

Az *intelligens kártyák* hamisítástól védett, könnyen hordozható eszközök, amelyek biztonságos megoldást jelentenek a különböző feladatokban, mint amilyen az ügyfélhitelesítés, a Windows Server tartományba történő bejelentkezés, a kódaláírás vagy az elektronikus levelek védelme. Az intelligens kártya rendkívül megbízható hálózati hitelesítési forma, mivel a tartományba bejelentkező felhasználót a titkosított azonosító adatok és a kártya jelenlétének egyidejű vizsgálatával hitelesíti.

Objektum alapú hozzáférés-vezérlés

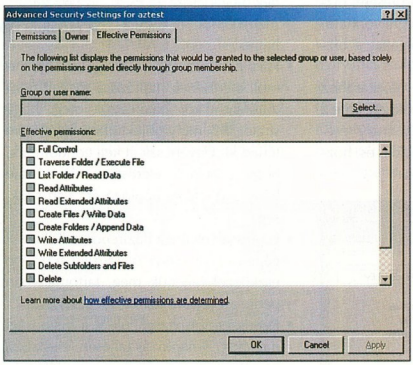
A felhasználói hitelesítés mellett a rendszergazdák az erőforrásokhoz vagy objektumokhoz történő hálózati hozzáférést is szabályozhatják. Ehhez a rendszergazdáknak biztonsági leírókat *(security descriptor)* kell hozzárendelniük az objektumokhoz – a leírók tárolását az *Active Directory* végzi. Az objektumok tulajdonságainak kezelésével a rendszergazda beállíthatja az engedélyeket, elvégezheti a tulajdonos hozzárendelését és figyelheti a felhasználói hozzáférést.

A rendszergazda nem csak egy adott objektum elérését, hanem az objektum egyes attribútumainak elérését is szabályozhatja. Adott objektum biztonsági leírójának helyes konfigurálásával a felhasználó hozzáférést kaphat az információk valamely részhalmazához, például az alkalmazottak nevéhez és telefonszámához, de lakáscíméhez nem.

Az *engedélyek* határozzák meg, hogy az adott felhasználó vagy csoport milyen típusú hozzáféréssel rendelkezik az adott objektumhoz vagy objektumtulajdonsághoz.

Az úgynevezett *általános engedélyek* az objektumok túlnyomó részéhez hozzárendelhetők. Ide tartoznak az olvasási engedélyek, a módosítási engedélyek, az új tulajdonos beállításának engedélye, valamint a törlés engedélye.

Az *engedélyek beállításakor* megadható



A hatályos engedélyek megadása

a csoportok és a felhasználók hozzáférési szintje. Például beállítható, hogy az egyik felhasználó olvashassa a fájl tartalmát, egy másik módosíthassa stb. Hasonló engedélyek állíthatók be a nyomtatókra is.

Objektum létrehozásakor a rendszer egy *tulajdonost* rendel az objektumhoz. Alapértelmezés szerint a tulajdonos az objektum létrehozója. A tulajdonos az objektumra megadott engedélyektől függetlenül bármikor megváltoztathatja az objektumhoz rendelt engedélyeket.

Az *öröklődés* révén a rendszergazdák egyszerűen megadhatják és kezelhetik az engedélyeket. Ezzel a szolgáltatással a tárolóban lévő objektumok automatikusan öröklik a tároló örökölhető engedélyeit.

A *Hatályos engedélyek* lap a Windows Server egyik új szolgáltatása. Segítségével megtekinthetők azok az engedélyek – köztük a biztonsági csoportoktól származtatott engedélyek is –, amelyek adott objektum valamely rendszerbiztonsági tagjára vonatkoznak.

A *felhasználói jogok* a számítógépes környezet felhasználói és csoportjai számára biztosítanak bizonyos bejelentkezési és egyéb engedélyeket.

Naplózhatjuk is az objektumokhoz történő felhasználói hozzáféréseket. A biztonsággal kapcsolatos naplózott eseményeket a biztonsági naplóban tekinthetjük meg az *Eseménynapló* segédprogrammal.

Biztonsági házirend

A helyi számítógép vagy számítógépek valamely csoportjának biztonságát a következő *házirendekkel* tarthatjuk kézben: jelszóházirendek, fiókzárolási házirendek, Kerberos házirendek, naplórendek, felhasználói jogok és egyéb házirendek.

Ha olyan házirendet szeretnénk létrehozni, amely a teljes rendszerre vonatkozik, a következő lehetőségek közül választhatunk: biztonsági sablonok használata, biztonsági sablonok alkalmazása a *Biztonsági konfiguráció és analízis* segédprogram segítségével, valamint a helyi számítógép, a szervezeti egység vagy a tartomány biztonsági házirendjeinek szerkesztése.

A *Biztonsági beállítások kezelője* eszközkészlet segítségével a helyi számítógépre, a szervezeti egységre vagy a tartományra vonatkozóan hozhatunk létre, léptethetünk életbe és szerkeszthetünk biztonsági változókat. Az eszközkészlet elemei a következők:

Biztonsági sablonok: biztonsági házirendet definiál egy sablonban. Ezeket a sablonokat a Csoportházirendben vagy a helyi számítógépen lehet alkalmazni.

A Csoportházirend Biztonsági beállítások bővítménye: tartomány, hely vagy szervezeti egység biztonsági beállításainak egyedi módosítása.

Helyi biztonsági házirend: a helyi számítógép biztonsági beállításainak egyedi módosítása.

Secedit parancsok: biztonsági beállítási feladatok automatizálása a parancssorból.

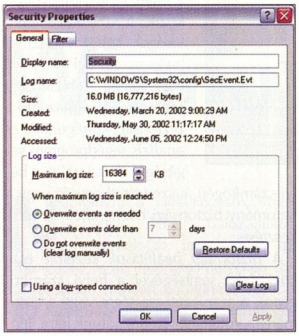
A modul lehetővé teszi a biztonsági elemzés eredményeinek gyors áttekintését. Az aktuális rendszerbeállítások mellett ajánlásokat jelenít meg, és ikonokkal vagy

megjegyzésekkel hívja fel a figyelmet azokra a területekre, amelyek nem felelnek meg az ajánlott biztonsági szintnek.

Naplózás

A *naplózás* lehetőséget nyújt a potenciális biztonsági problémák felderítésére, biztosítja a felhasználók felelősségre vonhatóságát, és bizonyítékokat szolgáltat a biztonság megsértése esetén.

A hatékony naplózás megvalósításához naplózási *házirendre* van szükség. Ehhez meg kell határoznunk, hogy mely eseménykategóriákat, objektumokat és hozzáféréseket kívánjuk naplózni.



A biztonsági napló méretének és megőrzési házirendjének megadása

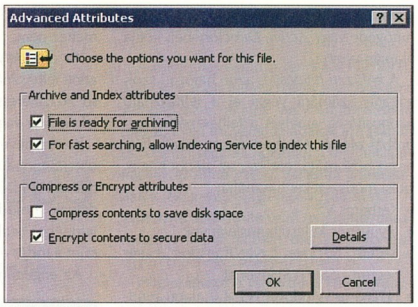
A házirendnek valamilyen átgondolt stratégián kell alapulnia. Például rögzíthetjük, hogy ki fért hozzá a rendszerhez vagy annak bizonyos adataihoz, esetleg azt, aki jogosulatlanul kívánta módosítani az operációs rendszert.

A leggyakrabban naplózásra kerülő eseménytípusok a következők:

- A felhasználók bejelentkezése a rendszerbe, illetve kijelentkezése a rendszerből
- Felhasználói és csoportfiókok kezelése
- Objektumokhoz, például fájlokhoz és mappákhoz való hozzáférések.

A naplózási házirend kidolgozásakor:

- Hozzunk létre saját naplózási stratégiát. Határoljuk körül a naplózandó magatartásokat.
- Válasszuk ki a naplózási stratégiájának megfelelő naplókategóriákat, ügyelve a felesleges kategóriák elhagyására.
- Megfelelő méretet és megőrzési házirendet szabjunk meg a biztonsági napló számára. A biztonsági napló megtekintésére, valamint a napló méretének és megőrzési házirendjének megadására az *Eseménynaplót* használhatjuk.



A tartalom titkosítása az adatok védelme érdekében

- Ha a címtárszolgáltatás vagy az objektumok elérésének naplózása mellett döntöttünk, akkor határozzuk meg, hogy stratégiánk mely objektumok figyelésére terjed ki. Ugyancsak át kell gondolnunk, hogy céljainak elérésére minimálisan hány hozzáférés naplózására van szükség.
- Léptessük életbe a házirendet. Különálló gépen ezt a *Helyi biztonsági házirend* eszközzel tehetjük meg, tartományban pedig a *Csoportházirend* segítségével.
- Rendszeresen vizsgáljuk át a biztonsági naplókat. A naplózás teljesen felesleges, ha soha nem vizsgáljuk át a naplókat.
- Szükség szerint finomítsunk a házirenden. Előfordulhat, hogy bizonyos objektumokat vagy hozzáféréseket hozzá kell adnunk vagy el kell távolítanunk a naplórendből, illetve engedélyeznünk vagy tiltanunk kell bizonyos naplózási kategóriákat.

Az Active Directory és a biztonság

Az *Active Directory* szolgáltatás segítségével a rendszergazdák könnyen és hatékonyan felügyelhetik a felhasználók hitelesítését és a hozzáférés-vezérlést. Az Active Directory az objektumok hozzáférés-vezérlése és a felhasználói azonosító adatok segítségével lehetővé teszi a csoportokkal és a felhasználói fiókokkal kapcsolatos adatok védett tárolását. Mivel az Active Directory nem csak a felhasználói azonosító adatokat tárolja, hanem a hozzáférésvezérlésre vonatkozó adatokat is, a hálózatba bejelentkező felhasználók egyszerre nyernek hitelesítést és kapnak engedélyeket a rendszer erőforrásaihoz történő hozzáférésre.

Mivel az Active Directory lehetővé teszi, hogy a rendszergazda csoportfiókokat hozzon létre, a biztonsági rendszer kezelése sokkal hatékonyabbá válik. Egy fájl tulajdonságainak beállításával például a rendszergazda egy adott csoport minden felhasználójának engedélyezheti a fájl olvasását. Ily módon az Active Directoryban lévő objektumokhoz történő hozzáférés a csoporttagságon alapul.

Adatvédelem

A rendszerben – online vagy offline – tárolt adatok a *Titkosított fájlrendszer (EFS)* és a digitális aláírások segítségével védhetők. Az EFS nyilvános kulcsú titkosítást használ a helyi NTFS fájlrendszer adatainak titkosítására.

Az EFS az alábbi szolgáltatásokat nyújtja:

- Segítségével a felhasználók titkosíthatják a lemezen tárolt fájlokat. A titkosítás nagyon egyszerű: be kell jelölni egy jelölőnégyzetet a fájl *Tulajdonságok* párbeszédpanelén.
- A titkosított fájlokhoz gyorsan és könnyen hozzá lehet férni. A felhasználó nyílt formátumban tekintheti meg saját, lemezen tárolt adatait.
- Az adatok titkosítása automatikusan, a felhasználó számára láthatatlanul történik.
- A fájl visszafejtéséhez törölni kell a jelet a fájl *Tulajdonságok* párbeszédpanelén a *Titkosítás* jelölőnégyzetből.
- A rendszergazdák más felhasználók által titkosított adatokat is visszafejthetnek. Ezáltal az adatok akkor is hozzáférhetők maradnak, ha a titkosítást elvégző felhasználó már nem elérhető, vagy elvesztette személyes kulcsát.

Az EFS csak a lemezen tárolt adatokat

titkosítja. *TCP/IP* alapú hálózaton keresztüli átvitel idejére kétféleképpen titkosíthatók az adatok: az IP-biztonság (IPSec) és a PPTP-titkosítás használatával.

Az EFS-sel összefüggő legfontosabb felügyeleti műveletek a következők:

- Titkosított fájlok biztonsági mentése és visszaállítása
- Titkosított adatok helyreállítása
- Helyreállítási házirend beállítása

A *digitális aláírás* az adatok épségének és eredetének egyik ellenőrzési eszköze. A Windows Server támogatja a *CAPICOM 2.0*-t. E támogatás révén az alkalmazásfejlesztők egy könnyen használható COM felület segítségével aknázhatják ki a *CryptoAPI* robusztus tanúsítvány- és titkosítási szolgáltatásait. Mivel a CAPICOM megoldás COM-alapú, a fejlesztők számos különböző programozási környezetből – Visual C# fejlesztőeszköz, Visual Basic .NET fejlesztőrendszer, Visual Basic, Visual Basic Script, Jscript stb. – is elérhetik szolgáltatásait.

Hálózati adatvédelem

Adott helyen a hálózati (helyi és alhálózati) adatok védelmét a *hitelesítési protokoll* biztosítja. A biztonság további fokozása érdekében a hálózaton továbbított adatok a telephelyen belül titkosíthatók is. Az *IPSec* (IP-biztonság) használatával bizonyos ügyfelek részére, vagy a tartományban lévő összes ügyfél részére minden hálózati kommunikációt titkosíthatunk.

A bejövő és kimenő (intraneten, extraneten vagy internetátjáró keresztüli) hálózati adatok a következő segédprogramokkal védhetők:

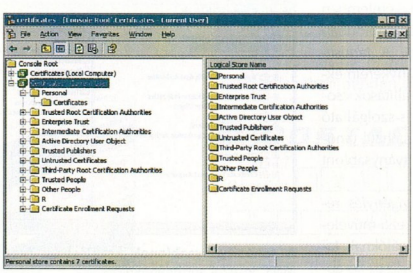
- *IP-biztonság (IPSec).* Titkosításon alapuló védelmi szolgáltatásokból és biztonsági protokollokból álló együttes.
- *Útválasztás és távelérés.* A távelérési protokollokat és az útválasztást konfigurálja.
- *Internetes hitelesítési szolgáltatás (IAS).* Biztonságot és hitelesítést nyújt a telefonos felhasználók számára.

A biztonságos hálózati technikák jövőjeként számon tartott *IPSec* titkosításra épülő védelmi szolgáltatások és biztonsági protokollok együttese. Mivel használata nem igényli az alkalmazások, illetve a protokollok módosítását, könnyen telepíthető meglevő hálózatokon is.

Az IPSec számítógépszintű hitelesítést, valamint adattitkosítást kínál az L2TP alapú virtuális magánhálózati (VPN) kapcsolatok számára. Az IPSec egyeztetés a számítógép és az L2TP alapú VPN-kiszolgáló között történik, az L2TP kapcsolat létrejötte előtt. Az egyeztetés a jelszavak és adatok védelmét egyaránt biztosítja.

A Windows Server rendszerek *Útválasztás és távelérés (Routing and Remote Access, RRAS)* szolgáltatása egy minden feladat ellátására képes szoftveres útválasztó, amely nyílt platformot biztosít az útválasztáshoz és az összekapcsolt hálózatokhoz. A szolgáltatás biztonságos virtuális magánhálózati (VPN) kapcsolatok alkalmazásával kínál útválasztási lehetőséget a vállalkozások számára a helyi hálózatokban (LAN), a távadatátviteli hálózatokban (WAN), illetve az interneten keresztül. A szolgáltatás a Windows Server család tagjaival való integrációra is alkalmas.

A Windows Standard Serverben található *Internetes hitelesítési szolgáltatás (IAS)* a



A tanúsítványok kezelése a Tanúsítványok MMC konzol segítségével

RADIUS kiszolgáló és proxy Microsoft általi megvalósítása. *RADIUS kiszolgálóként* az IAS központi kapcsolathitelesítést, engedélyezést és számlázást végez számos különböző (vezeték nélküli, hitelesítő kapcsoló, távoli telefonos és VPN alapú) hálózati kapcsolathoz. *RADIUS proxyként* az IAS más RADIUS kiszolgálók felé továbbítja a hitelesítési és számlázási üzeneteket. A RADIUS szabványt az *Internet Engineering Task Force (IETF)* dolgozta ki.

Nyilvános kulcsú infrastruktúra (PKI)

A *nyilvános kulcsú infrastruktúra (PKI)* a digitális tanúsítványok, hitelesítés-szolgáltatók (CA) és más regisztrációs szervezetek (RA) rendszere, amely nyilvános kulcsú titkosítás segítségével ellenőrzi és hitelesíti az elektronikus tranzakciókban részt vevő felek jogosultságait. A PKI szabványait folyamatosan fejlesztik, ugyanakkor az elektronikus kereskedelem nélkülözhetetlen elemeiként már jelenleg is széles körben használják őket.

A Windows Server család tagjai különféle szolgáltatásokkal segítenek a nyilvános kulcsú infrastruktúra létrehozásában.

A *tanúsítvány* lényegében egy *digitális nyilatkozat*, amelyet a tanúsítvány tulajdonosának kilétét szavatoló szervezet bocsát ki. A tanúsítvány a nyilvános kulcsot a hozzá tartozó titkos kulcsot birtokló személyhez, számítógéphez vagy szolgáltatáshoz köti. Tanúsítványokat számos olyan nyilvános kulcsú titkosítást használó szolgáltatás és program alkalmaz, amely a hálózatokon, például az interneten keresztül folytatott kommunikáció hitelesítéséről, biztonságáról, valamint az adatok integritásáról gondoskodik.

A Windows tanúsítvány alapú folyamatai az *X.509v3* szabványos tanúsítványformátumot alkalmazzák. Egy X.509 formátumú tanúsítvány adatokat tartalmaz a tanúsítvánnyal rendelkező személyről vagy entitásról, a tanúsítványról, valamint a tanúsítványt kibocsátó hitelesítésszolgáltatóról. A tanúsítványban foglalt adatok között szerepelhet az entitás neve, a nyilvános kulcs és a nyilvános kulcsú algoritmus azonosítója. A tanúsítványt megkapó entitás a tanúsítvány tulajdonosa. A tanúsítványt kiállító és aláíró szervezet a hitelesítésszolgáltató.

A felhasználók a *Microsoft Management Console (MMC)* segítségével kezelhetik tanúsítványaikat. Az automatikus igénylés engedélyezésével a felhasználók automatikussá is tehetik a tanúsítványok kezelését.

Egy tanúsítvány csak a benne meghatározott időtartamra érvényes. Minden tanúsítvány tartalmazza az érvényességi periódus kezdő és lezáró dátumát. Ha az érvényességi idő lejárt, az érvényét vesztett tanúsítvány tulajdonosának új tanúsítványt kell igényelnie.

Abban az esetben, ha szükségessé válik a tanúsítvány által igazolt kapcsolat megszüntetése, a kiállító visszavonhatja a ta-

Microsoft Windows Server 2003

núsítványt. Minden kiállító listát vezet a visszavont tanúsítványokról, melyet a programok a tanúsítványok érvényességének vizsgálatakor használnak.

A *Tanúsítvány-szolgáltatások (Certificate Services)* a Windows Server család hitelesítés-szolgáltatók *(Certificate Authority, CA)* létrehozására és kezelésére szolgáló összetevője. A hitelesítés-szolgáltató feladata a tanúsítványtulajdonosok azonosságának megállapítása és igazolása. Emellett gondoskodnia kell az érvénytelenné vált tanúsítványok visszavonásáról, és közzé kell tennie ezek listáját, amelyet majd a tanúsítványt ellenőrző programok használni fognak.

A tanúsítványokat a hitelesítés-szolgáltató bocsátja ki a tanúsítványkérelemben szereplő adatok és a tanúsítványsablonban megadott beállítások alapján. A *tanúsítványsablon* a bejövő tanúsítványkérelmekre vonatkozó szabályok és beállítások csoportja. Egy vállalati hitelesítés-szolgáltató esetében minden általa kibocsátható tanúsítványtípushoz egy tanúsítványsablont kell rendelni.

Az *automatikus tanúsítványigénylés* révén a rendszergazdák a következő műveleteket engedélyezhetik a felhasználóknak: tanúsítványok automatikus igénylése, korábban kiadott tanúsítványok lekérdezése, lejáró tanúsítványok megújítása a tulajdonos közbeavatkozása nélkül. A műveletek végrehajtásához a tulajdonosnak a tanúsítványokkal kapcsolatos semmilyen ismerettel nem kell rendelkeznie – hacsak a tanúsítványsablon elő nem írja a tulajdonossal folytatott interaktív párbeszédet, vagy a kriptográfiai szolgáltató (CSP) meg nem követeli azt (például intelligens kártyát illesztő CSP).

A *webes igénylőoldalak* a Tanúsítványszolgáltatások különálló összetevője. E weblapok a hitelesítés-szolgáltató üzembe helyezésekor alapértelmezés szerint automatikusan telepítésre kerülnek, ha engedélyezzük, hogy a tanúsítványok igénylői webböngészőn keresztül küldjék el igényléseiket.

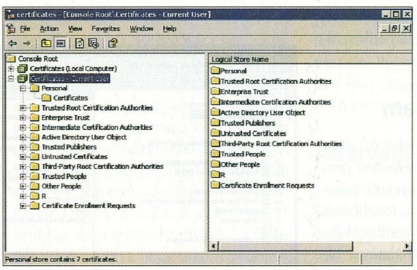
A Windows támogatja az *intelligens kártyán* tárolt tanúsítvány használatával végzett bejelentkezést, illetve az intelligens kártyák tanúsítványok és titkos kulcsok tárolására történő használatát.

A Windows *csoportházirendjével* a tanúsítványok automatikusan eljuttathatók tulajdonosukhoz, mindenki által megbízhatónak tekintett hitelesítésszolgáltatók hozhatók létre, illetve kezelhetők az EFS helyreállítási házirendjei.

Bizalmi kapcsolatok

A Windows Server család tartományi és erdő szinten támogatja a *bizalmi kapcsolatokat*. A tartományok közötti bizalmi kapcsolat lehetővé teszi a felhasználó hitelesítését más tartományban lévő erőforrások használatához.

A bizalmi kapcsolatok típusa és iránya jelentős hatással van a hitelesítésre használt bizalmi útvonalak működésére. A bizalmi útvonal bizalmi kapcsolatok sorozata, amelyet a hitelesítési kérelemnek be kell járnia a tartományok között.



A tanúsítványsablonok kezelése a Tanúsítványsablonok MMC konzol segítségével

A tartományok közötti kommunikáció bizalmi kapcsolatokon keresztül történik. A bizalmi kapcsolat olyan hitelesítési csatorna, amely arra szolgál, hogy az egyik tartományhoz tartozó felhasználók elérhessék egy másik tartomány erőforrásait.

Az *egyirányú bizalmi kapcsolat* két tartomány között létrejött egyirányú hitelesítési útvonal. Ez azt jelenti, hogy ha az A és a B tartomány között egyirányú bizalmi kapcsolat áll fenn, akkor az A tartomány felhasználói elérhetik a B tartomány erőforrásait, ám a B tartomány felhasználói nem férhetnek hozzá az A tartomány erőforrásaihoz.

Bizonyos egyirányú bizalmi kapcsolatok a kapcsolat típusától függően *tranzitívak* és *nem tranzitívak* lehetnek.

Adott Windows erdőn belül minden tartományi bizalmi kapcsolat *kétirányú* és tranzitív. Ha új gyermektartomány jön létre, akkor a gyermektartomány és a szülőtartomány között automatikusan kétirányú tranzitív bizalmi kapcsolat jön létre. Kétirányú bizalmi kapcsolat esetén az A tartomány megbízik a B tartományban, és a B tartomány megbízik az A tartományban.

A Windows tartományok az alábbi tartományokkal képesek egy- vagy kétirányú bizalmi kapcsolatot kialakítani:

- Ugyanazon erdő Windows tartományai
- Más erdő Windows tartományai
- Windows NT 4.0 tartományok
- Kerberos V5 területek

A Windows Server rendszerek erdőjében a rendszergazda erdőszintű bizalmi kapcsolatot hozhat létre, ezáltal a kétirányú tranzitivitást egyetlen erdő hatóköréből egy másik Windows Server erdőre terjesztheti ki. Más szavakkal élve, az erdőszintű bizalmi kapcsolatok segítségével két különálló Windows Server erdő is összekapcsolható, ezzel kétirányú tranzitív bizalmi kapcsolat jön létre a két erdő összes tartománya között.

Összegzés

A vállalatok versenyképességének megőrzése minden eddiginél jobban függ a hatékony és biztonságos hálózati informatikától. A Windows Server segítségével megnövelhető a korábbi informatikai beruházások által nyújtott előnyök köre, az erdők közötti bizalmi kapcsolatokhoz és a Passport szolgáltatás integrálásához hasonló kulcsfontosságú funkciók révén pedig kiterjeszthetők ezek az előnyök a partnerek, az ügyfelek és a beszállítók körére is.

A Windows Server olyan szolgáltatásokat nyújt, amelyekkel biztonságosabb környezet alakítható ki az üzletvitel számára. A bizalmas adatok egyszerűen titkosíthatók, a szoftverkorlátozó házirendek segítségével pedig megelőzhetők a különféle vírusok és trójai falovak által okozott károk. A Windows Server a legjobb választás akkor is, ha nyilvános kulcsú infrastruktúra kialakítása a cél. Automatikus tanúsítvány-igénylési és -megújítási funkcióinak köszönhetően egyszerűen lehet az egész vállalaton belül bevezetni az intelligens kártyák és a tanúsítványok használatát.

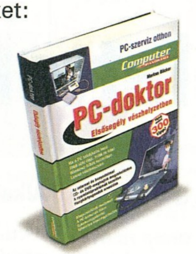
(-)

FAX MEGRENDELŐLAP

Computer Panoráma Kiadói Kft.
Terjesztési Osztály
1091 Budapest, Üllői út 25.
Tel.: 456-69-63

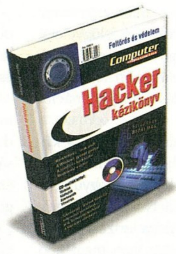
Fax: 456-69-70

Igen, utánvéttel megrendelem
az alábbi könyveket:

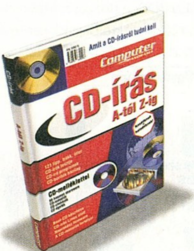


❐ PC-doktor
(3 990 Ft)

❐ PC-tuningolás 2003
(4 990 Ft)



❐ Hacker kézikönyv
(4 990 Ft)



❐ CD-írás A-tól Z-ig
(3 490 Ft)

❐ PC-doktor
e-book – CD-ROM
(3 990 Ft)

SZÁMLÁZÁSI CÍM:

Cégnév: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Ir.sz: ☐☐☐☐ Helység: ☐☐☐☐☐☐☐

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Út/utca/tér: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐,

hsz. ☐☐☐, em./ajtó: ☐☐/☐☐

Telefon (napközben): 06 ☐☐☐☐☐☐☐☐

E-mail: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Kérjük, a kézbesítés megkönnyítése és a gyors ügyintézés érdekében minden adatot feltétlenül adjon meg!

POSTACÍM:

Cégnév: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Ir.sz: ☐☐☐☐ Helység: ☐☐☐☐☐☐☐

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Út/utca/tér: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐,

hsz. ☐☐☐, em./ajtó: ☐☐/☐☐

Telefon (napközben): 06 ☐☐☐☐☐☐☐☐

Mobilszám: 06 ☐☐☐☐☐☐☐☐☐

Aláírás

Átfutási idő kb. 2 hét!
Internet: www.computer panorama.hu/megrendeles,
E-mail: **megrendeles@cpanorama.hu**
A megrendelt könyveket utánvéttel küldjük, áraink a postaköltséget nem tartalmazzák! (A postaköltséget az érvényes postai díjszabás szerint számoljuk.)

Biztonságos hálózatok – távfelügyelettel

Az internet terjedésével nő a fenyegetések száma is – mondják-mondogatják egyre többen. Éppen csak tenni nem akarózik semmit e veszélyek ellen. Az ICON Rt. távfelügyeleti központja nagymértékben tehermentesíti a vállalati IT-szakembereket a hálózati biztonsággal kapcsolatos feladatoktól.

Világszerte egyre növekszik a hálózatokba való illetéktelen behatolások száma. 2002-ben az adatbiztonság világát új típusú fenyegetések határozták meg. Az otthoni számítógépekbe való betörések egyre gyakoribbá válása és az ázsiai vírusírók egyre növekvő aktivitása rengeteg munkát adott az adatbiztonsággal foglalkozó cégeknek. Az új technológiák, a sok platform, valamint a mobil- és a vezeték nélküli eszközök rohamos terjedésével egyidejűleg nőtt a potenciális támadások száma is.

Előrejelzések szerint 2003-ban még veszélyesebb és még nehezebben azonosítható vírusok megjelenésére lehet számítani. A nemzetközi tendenciák hatására ugyanakkor a hálózatbiztonsági kérdések Magyarországon is egyre inkább előtérbe kerülnek.

Távfelügyelet

A biztonsággal összefüggő események a nagyobb informatikai rendszerekben olyan mértékű adatmennyiséget és munkát eredményeznek, amelyet manuálisan kiértékelni, feldolgozni reménytelen. Gondot okozhat a vakriasztások nagy aránya is, ami az emberi felügyelet munkáját jelentős mértékben nehezíti. Ezért egyre több cég ismeri fel a *távfelügyelet* szükségességét, a módszer kínálta előnyöket.

A távfelügyelet azoknak a hardver- és szoftvereszközöknek az interneten vagy bérelt vonalon keresztül való felügyeletét jelenti, amelyek önmagukban vagy a rájuk telepített megfelelő *felügyeleti szoftverek* révén képesek működésükről információt szolgáltatni.

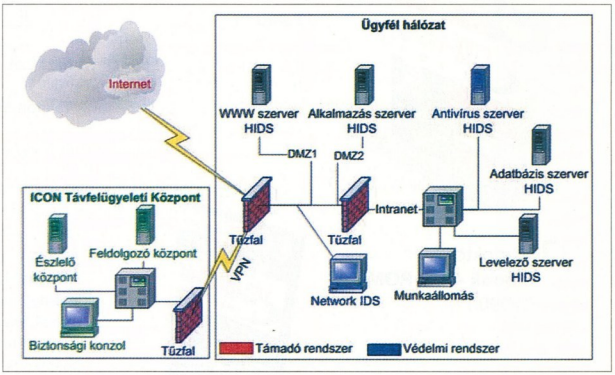
A távfelügyeleti rendszer feladata a különböző biztonságtechnikai eszközökből kinyerhető információ helyi összegyűjtése, szűrése, archiválása, illetve központi feldolgozása, természetesen a veszélyt jelentő események felismerése és a megfelelő mechanikus ellenintézkedések megtétele.

Alkalmazási területek

A távfelügyelet még viszonylag új módszernek számít a hagyományos informatikai biztonságban: csak napjainkban kezd terjedni a különböző pontokon elhelyezett biztonsági eszközök centralizált megfigyelése, illetve az érkező jelzések egységes kiértékelésére kifejlesztett megoldás.

A biztonsági távfelügyeleti szolgáltatások az alábbi területeket ölelik fel:

- Konfigurációkövetés, amely a biztonsági eszközök szoftver- és hardvernyilvántartásának a kezelését jelenti.
- Szerveroldali és átjáró jellegű vírusvédelmi rendszer felügyelete, amely a védelem működőképességének, aktualitásának és aktivitásának követését jelenti.
- Kliensoldali központosított vírusvédelmi rendszer felügyelete, amely alatt a védelem működőképességének és aktualitásának ellenőrzését, aktivitásának követését és az általa szolgáltatott események feldolgozását értik a szakemberek.
- Szerver- és hálózatoldali behatolásdetektáló (IDS) rendszer felügyelete, amely a behatolás-detektáló rendszer működőké-



Az ICON Távfelügyeleti Központja gondoskodik az ügyfelek biztonságáról

Az ICON portfoliójában központi helyen szerepelnek az adatbiztonsággal kapcsolatos megoldások

pességének biztosítását, aktivitásának követését takarja.

- Tűzfal távfelügyelete, azaz a tűzfal működésének felügyelete.
- Rendszeres külső és belső aktív audit (scan), vagyis az informatikai rendszert a külső hálózatok irányából és a belső hálózatról fenyegető sérülékenységek feltárása.
- Rendkívüli események jelzése a felügyelt rendszerek aktivitása és naplóinformációi alapján.
- Rendkívüli események kezelése, beavatkozás, problémakezelés.
- Rendkívüli események bekövetkeztekor a történtek felmérése, az okok meghatározása és a veszély elhárítását célzó lépések megtétele.
- Rendszeres biztonsági összefoglaló jelentés készítése, trendek értékelése.
- A felügyelt biztonsági rendszerek paramétereit, jellemzőit és a megfigyelés során kapott információkat figyelembe véve összefoglaló jelentés készítése a biztonsági eseményekről, rövid és hosszú távú javaslatok készítése a rendszerek biztonsági szintjének emelésére vonatkozóan.
- Katasztrófa-elhárítási akciótervek kidolgozása.

IT-biztonsági piac

A biztonsági távfelügyeleti szolgáltatásoknak megvannak az előfeltételei, ezek közül is a legfontosabb az IT biztonsági stratégia és szabályzat megléte, az üzleti kockázati tényezők szervezeti szintű definiálása, valamint az IT infrastruktúra előzetes biztonsági felmérése.

Egyes felmérések szerint a hazai IT-biztonsági piac (termékek és kapcsolódó szolgáltatások) nagysága eléri az *5 milliárd* forintot. A megfelelő biztonsági megoldás kiválasztásánál ma már egyre nagyobb szerepet kapnak a könnyen menedzselhető rendszerek, adott esetben az erre specializálódott cégek megbízása és egy-egy komplex biztonsági szolgáltatás esetében a tapasztalat is egyre inkább meghatározó szempont.

„A távfelügyeleti rendszer előnyeit hosszan sorolhatnám, de amit elsőként kiemelnék az az, hogy a meglévő emberi erőforrásokat tehermentesíti, ezáltal több időt biztosít az alapvető üzemeltetési és fejlesztési feladatok ellátására. Az *ICON Rt.*-nél folyamatosan képzett, tapasztalt szakemberek figyelnek ügyfeleink rendszereinek biztonságára. Rugalmas, egyedi igényekhez illeszkedő szolgáltatási csomagjaink kulcseleme a *Budapesti Műszaki Egyetemmel* közösen fejlesztett csúcstechnológiájú management szoftver" – foglalta össze a távfelügyeleti szolgáltatás előnyeit *Keleti Arthur*, az ICON Rt. biztonsági üzletágának üzletfejlesztési igazgatója.

Szüksége van-e önnek távfelügyeleti rendszerre?

A dilemmát ki-ki eldöntheti, ha megválaszolja az alábbi kérdéseket.

- A jelenlegi rendszerükben van-e erejük a naplóállományokat figyelni, vagy már rég kikapcsolták a részletes naplózást?
- A meglévő embereik rendelkeznek-e megfelelő szakértelemmel az újonnan megjelenő sérülékenységek elleni védekezés megoldására?
- Tudják-e szakembereik rendszeres informatikai biztonsági képzését és tanulmányaikat finanszírozni?
- Biztonsági incidensek esetén tudják-e, hogy miként kell cselekedni a veszély elhárítása érdekében?
- Munkaidőn kívül felügyeli-e valaki a rendszerüket?
- „Csak" a fentiekért megéri szakembereket felvenni?

Ha az alábbi kérdések közül legalább 1-re NEM a válasza, már érdemes elgondolkodni a távfelügyelet bevezetésén.

„Annak, aki nem csupán vásárolni, de hosszú távon üzemeltetni is akarja a biztonsági rendszert, a 7 x 24 órás távfelügyeleti szolgáltatást érdemes igénybe vennie. A fent felsorolt érvek mellett a szolgáltatásnak megvan az az előnye, hogy szakembereink együtt élnek a cég informatikai rendszerével, így hatékony tanácsot tudnak adni a felmerülő fejlesztési kérdésekben, legyen szó akár az architektúra vagy a teljes informatika átalakításáról."

(–)

Adatok vészhelyzetben

A Kürt Némethonban

Az egyre nagyobb németországi ügyfélkör könnyebb és rugalmasabb kiszolgálása érdekében a *Kürt Computer Rendszerház Rt.* irodát nyitott *KUERT Datenrettung Deutschland GmbH* néven a németországi Bochumban. A professzionális adatmentési és informatikai biztonsági technológiájáról világszinten elismert Kürt 100 százalékos tulajdonosa a német cégnek, amely a tervek szerint szakembereivel és szaktudásával a régióba tartozó más országok adatvesztést szenvedett számítógép-felhasználóit is kiszolgálja majd.

A kezdetben 6 főt foglalkoztató németországi iroda megnyitásának gondolata a Kürt németországi üzleti kapcsolatainak, a német piaci helyzetnek és egy komoly helyi kapcsolatokkal rendelkező német menedzser személyének ismeretében vetődött fel. *Ernst Eder* ügyvezető igazgató mellett a cég kereskedelmi és technológiai tevékenységét magyar szakemberek látják el, míg a marketing és pénzügyi feladatokat külső erőforrásokkal oldja meg az iroda. A helyszínválasztás okai közé sorolható a német műszaki kultúra, a magas fizetőképesség és az a tény, hogy Németországon belül a „leggazdagabb" és legsűrűbben lakott terület a Ruhr-vidék (100 kilométeres körzetben 17 millió ember él).

Németország mellett szólt az a körülmény is, hogy a Kürt évek óta kiállít a világ legnagyobb informatikai és telekommunikációs seregszemléjén, a hannoveri CeBit-en. Hannover szintén az új iroda vonzáskörzetébe esik.

A KUERT GmbH 2003. január közepén történt megalakulásától márciusig nyolc adatmentésre kapott már megbízást, köztük 200 CD nagy értékű adatainak helyreállítására. A cég az első évben 200-250 esettel és 300-350 ezer euró értékű bevétellel számol, az első 3 évben pedig 1,5 millió euróval. A tervek között szerepel még, hogy – a hazai üzleti modellt követve – működésének első szakaszában az adatmentés, azt követően pedig az adatbiztonság is a cég profiljának homlokterébe kerül.

Aki számítógéppel, vagyis digitális adatokkal dolgozik, bizonyára találkozott már az adatvesztés hátborzongató élményével. A Kürt Computer Rt. arra vállalkozik, amire Magyarországon rajtuk kívül senki: megpróbálják az elveszettnek hitt adatokat úgyszólván a sírból visszahozni.

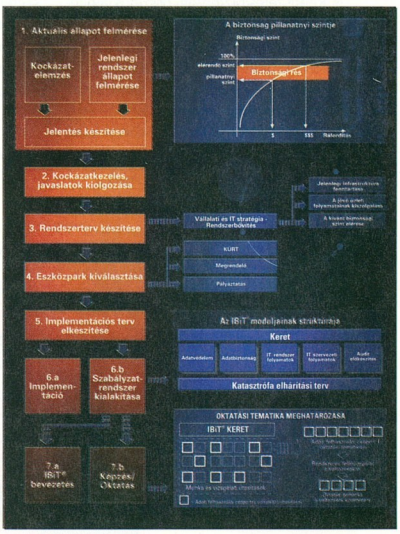
A vállalatok, vállalkozások számítógép-használata mára hétköznapi, megszokott, nélkülözhetetlen dologgá vált. A menedzsereknek és az alkalmazottaknak azonban újfajta kihívásokkal kell szembenézniük: nem elég gondoskodni az adatok, programok, elektronikus termékek tárolásáról, áramoltatásáról, hanem azokat meg is kell védeni. Egy–egy laptopon vagy asztali gépen ugyanis sokszor a „vas" többszörösét érő állományok találhatók: operációs rendszer, adatbázisok, programok, kapcsolatok. Ezeket többféle támadás is fenyegeti: vírusok vagy férgek behatolása, hackerek vagy felhasználók jogosulatlan adatkezelése, adatlopás, vagy akár a képzetlen felhasználók hibájából eredő adatvesztés, sérülés.

Kollektív felelősség

Az internet robbanásszerű elterjedésével megjelent a világban az informatikai biztonsággal kapcsolatos kollektív felelősség gondolata. A felelősség saját magunkért és egymásért is, hisz a hálózaton mindenki kapcsolatban van mindenkivel. Ennek jegyében be kell tartani bizonyos szabályokat, ha nem akarunk sem kárt okozni, sem kárt szenvedni. Hasonlít ez a helyzet a közlekedésre: ott sem lehet fittyet hányni a szabályokra, az őrült autósok nemcsak magukra jelentenek veszélyt, hanem autóstársaikra is.

A magyarországi költségvetési intézmények 2001-ben 50-60 milliárd forintot fordítottak az informatikára (forrás: *Bell Research*). Szakértők szerint Magyarországon jelenleg 10-12 százalék lehet az informatikai biztonságra költött összegek aránya.

Az informatikai biztonság feladatkörét Magyarországon elsőként a *Kürt Rendszerház Rt.* foglalta integrált adatvédelmi, adatbiztonsági rendszerbe: ez az *IBiT*, azaz *Informatikai Biztonsági Technológia*. A jól működő informatikai biztonsági rendszer megteremtése több lépésből álló, összetett feladat. A rendszer kiépítésének különböző fázisai számos olyan járulékos információt szolgáltatnak, amelyek a döntéshozók számára megkönnyítik a vállalati stratégia, az



Az IBiT projek folyamatábrája

üzleti folyamatok és az informatika közötti – sokszor nehezen átlátható – kapcsolatok jobb megértését, s ezáltal segítséget nyújtanak a döntések előkészítésében.

Az IBiT felépítése

A első lépés az *aktuális állapot felmérése:* milyen gépeken, milyen programokkal dolgoznak a cégnél, mekkora a hálózat, hogyan kapcsolódnak az internethez, milyen a jelenlegi IT-biztonság, és mik az elképzelések? A vállalat működése mennyire van veszélyben?

A következő lépés a *kockázatkezelés,* ami azért különösen fontos, hogy kialakuljon a helyes arány: nehogy olyan védelmi intézkedést alkalmazzanak valahol, amelyik többe kerül, mint az általa elhárított kár mértéke!

A következő lépésben elkészített *rendszerterv* tartalmazza a kívánt biztonsági szint eléréséhez szükséges rendszerbővítés műszaki paramétereit és az ehhez tartozó becsült költségeket. Az eszközpark kiválasztása teljesen önállóan végezhető el, és ez többnyire az eszközök szállítójának a feladata. A komplex IT biztonsági rendszer kialakításához a megfelelő minőségről is gondoskodni kell, ami a Kürt feladata.

Arra is volt már példa a Kürt praxisában, hogy csak a szabályzatrendszert kellett kialakítani a meglévő infrastruktúrához, eszközrendszerhez. Természetesen a rendszer megismerése feltétlenül szükséges, tehát ilyenkor az egyszerűbb felmérés mindenképpen része a projektnek. Ezzel az implementációs terv és az implementáció fogalmát is megmagyaráztuk.

Következik az informatikai biztonság megteremtésének egyik legfontosabb lépése: az eddig megfogalmazott elvárásoknak megfelelő egységes IBiT szabályzatrendszer kialakítása és bevezetése.

A szabályok azonban köztudottan annyit érnek, amennyit betartanak belőlük. Nagyon fontos tehát, hogy minden felhasználó – és ne csak a rendszergazda – a megfelelő ismeretekkel rendelkezzen a bevezetendő rendszerrel kapcsolatban, és pontosan ismerje az ehhez kapcsolódó feladatait, lehetőségeit és felelősségét. Az IBiT projekt utolsó modulja tehát a felhasználók és az informatikai dolgozók oktatása az informatikai biztonsági rendszer általános és speciális kérdéseire.

F. Fülöp Hajnalka
kivancsi@vnet.hu

Adatbiztonság a háborúban

Az Irak elleni amerikai hadjárat nemcsak a közel-keleti térségre, hanem az egész világra hatással van. A bevetésre kerülő arzenálban ugyanúgy ott szerepelnek az informatikai támadóeszközök, mint ahogyan a célpontok között is ott vannak a számítógépek és egyéb infokommunikációs objektumok. Az adatbiztonság és adatmentés tekintetében világhírű *Kürt Rt.* szakembereinek segítségével kerestük a választ a háború által felvetett kérdésekre.

A híradásokban ugyan még nem szerepelt, de létezik már olyan bomba is *(EMP – Matrix),* amely az elektronikus szerkezeteket bénítja meg. Képes a becsapódás helyétől mért 10-15 km-es sugarú körben – mikrohullámú rezgés kibocsátásával – minden elektronikus szerkezetet megbénítani, az autók gyújtásától kezdve a mobiltelefonokig, és természetesen a PC-ket, radarokat, GPS-eket is tönkreteszi.

A másik fegyver, amelyet már többször bevetettek, a *mikroszkopikus szénszálak* szórása villanyvezetékre, erőműtelepre, trafótelepekre. Ezek tulajdonképpen hajszálvékony, de 10-20 cm hosszúságú szénszálak, amelyek rövidzárlatot okoznak. Ilyen értelemben tényleg veszélyt jelentenek a számítógépekre, illetve az adatokra (például a felhasználó éppen írni akar, amikor elmegy a villany, ezáltal sérül az adat stb.). Közvetlenül azonban nem okoznak kárt az adatállományban: a winchestert nem károsítják. Hátrányuk, hogy nemcsak az ellenség, hanem a támadók rendszereit is veszélyeztetik.

Az egész világon pusztító vírusok nemcsak a háborúban ütik fel a fejüket és támadnak orvul a rendszerekre, hanem békeidőben, civilek között is bombaként rombolnak, ha nem védekezünk ellenük megfelelően. Az iraki-amerikai konfliktus miatt azonban ismét felszínre került a *kiberterrorizmus* veszélye: a terroristák megbéníthatják a katonailag fontos szervereket, a hírközlő rendszereket, az internetes hálózat egyes részeit.

„Természetesen a terroristák is használják az internetet. Fontos leszögeznünk azonban, hogy a terroristák a békés felhasználókhoz hasonlóan elsősorban információszerzésre és az egymással történő kommunikálásra használják a világhálót, és nem foglalkoznak azzal, hogy hogyan támadják meg azt. Véleményünk szerint a terroristák nem szándékoznak nagyszabású internetes támadásokat indítani" – nyilatkozta az üggyel kapcsolatban *Rainer Fahs,* a NATO egyik biztonsági szakértője A biztonság kedvéért azonban az USA egy külön – sokmilliós – projektet indított, nemcsak a védekezésre, hanem az ellentámadásra való felkészülésre is. A kiberkalózok elleni védekezés egyébként többszintű lehet: a védett eszközök és állományok minél tökéletesebb elszigetelése, a többszintű védelem, a nyílt forráskódú eszközök (pl. *Linux*) használata (a kiskapuk felszámolására), a felhasználók és a civilek oktatása, tájékoztatása.

Valós, hétköznapi veszélyt jelenthet a világ minden felhasználója számára, hogy a vírusok írói kihasználják az emberek érdeklődését a háborús hírek iránt. Olyan vírusokat írnak, amelyek a háborúhoz kapcsolódó híreknek, képeknek álcázzák magukat. Ezek az elektronikus levelek valójában csatolt fájlként magát a vírust tartalmazzák, nem pedig George W. Bush legújabb bejelentését. Az elmúlt egy-két évben nagyon elterjedt ez a fajta vírusírás, a ferde jellemű programozók rájöttek, hogy könnyű terjesztési módszerre leltek. Az iraki háború márciusi kitörése után pár nappal jelent meg az alacsony károkozású fokozatba sorolt *Ganda* féreg, amely valószínűleg Svédországból indult. A Ganda aktivizálódása után kiolvassa az Outlook címjegyzékét, és továbbküldi magát az abban található címekre. A vírus annyiban veszélyes azonban, hogy ismeri a népszerűbb antivírus alkalmazásokat, és amennyiben futnak a fertőzött rendszeren, leállítja azokat.

A háborús térség kommunikációs vonalait nyilvánvalóan zavarják (a műholdat, a GPRS-t, a műsorszóró rendszereket, a mobiltelefóniát stb.). A szakértők szerint ennek komoly informatikai vonatkozásai is lehetnek. Ezek kihatásai a környező államokban is érzékelhetők, illetve az érintett államok (így hazánk is) bevezetik e csatornák fokozott ellenőrzését, ami egyes esetekben teljesítménygondokat is jelenthet. Stratégiailag célszerű a vonalak más technológián alapuló backup vonalakkal való helyettesítése (ezt egyébként a katasztrófa elhárításra való felkészülés szabályai is indokolhatják).

Jól tartott szerverek

Sok vállalkozásnál a szerver még mindig ott áll, ahol akad számára hely. Sufnikban, raktárhelyiségekben, poros, meleg helyeken működnek a gépek, ez pedig erősen rontja a meghibásodási arányokat. Ám a rendszerek folyamatos működése egyre több cég számára létkérdés, így a szerverek elhelyezése és üzemeltetése is mind fontosabb. Erre kínálnak megoldást a szerverfarmok.

A cégek többsége már kiépítette a maga internetes hídfőállását, amelyek a korábban oly jellemző PR-szagú lapocskákból lassacskán komoly, valódi szolgáltatást nyújtó oldalakká fejlődtek. Mind több vállalat használ például internet-alapú kommunikációs rendszereket, adatbázisokat, üzemeltet portál-szolgáltatásokat, esetleg nyújt chat-szolgáltatást.

A minőségi váltással a webszerverekkel szembeni elvárások is nőttek, hiszen az interneten elérhető szolgáltatásoknak a nap 24 órájában, zavarmentesen kell működniük, miközben mind több felhasználót kell kiszolgálniuk. Ehhez elengedhetetlen, hogy szerverünket megfelelő körülmények között, állandó technikai felügyelet mellett tároljuk, amit házon belül megoldani nem csak munkaigényes, de költséges feladat is. Olcsóbb és biztonságosabb megoldást jelent, ha szerverünket a működő *szerverfarmok* valamelyikében helyezzük el, ahol fix havidíj ellenében megfelelő körülmények között tárolják azt.

Gyors hozzáférés

Az olyan interaktív szolgáltatásoknál, mint az online vásárlás, lényeges, hogy a felhasználók minél gyorsabban kommunikálhassanak a webszerverekkel. Ha a számítógép a saját telephelyen üzemel, a cég bérelt vonala jelenti az elérhető legnagyobb sebességet, ezzel szemben a *szerverhostingnál* a szolgáltató hazai és nemzetközi sávszélessége a határ. A *BIX (Budapest Internet Exchange)* szolgáltatási ponthoz *1 Gbps* sávszélességgel kapcsolódó, úgynevezett BIX szolgáltatókra jó példa a *Novacom Kft.*, amely *InternetNetWorks* redundáns hálózatával kapcsolódik a nemzetközi IP gerinchálózatokhoz, valamint a BIX-hez. Ez utóbbira a farmjukon lévő webszerverek egy közös *FastEthernet* kapcsolón keresztül *10/100 Mbps* sávszélességgel csatlakozhatnak.

A Dataplex kolokációs létesítményében akár 100 négyzetméteres különálló termet is bérelhetünk

Az olyan gigászok esetében, mint amilyen például a *Dataplex*, a rendelkezésre álló sávszélesség gyakorlatilag korlátlan.

Éppen a nagysebességű adatkommunikáció miatt a nagyobb szerverfarmokon a jelentősebb telekommunikációs cégek *közvetlen optikai kábeles* csatlakozást használnak, így az egyes hálózatok akár közvetlenül is összekapcsolhatók.

Intelligens épületek

A Dataplex szerverfarmjának otthont adó épület jó példája a korszerű *épületmenedzsmentnek*. Ez egy önállóan is működőképes, úgynevezett *intelligens létesítmény*, amelyet kifejezetten az üzleti szempontból kritikus berendezések és alkalmazások elhelyezésére terveztek. A központ „intelligenciájáról" fejlett épületgazdálkodási rendszer *(Building Management System, BMS)*, üzemeltetést támogató rendszer *(Operational Support System, OSS)* és kábelmenedzsment rendszer *(Cable Management System, CMS)* gondoskodik.

A szerverfarmokat működtető cégek egyik érdekes szolgáltatása, hogy akár a szervereinkkel egy épületbe is költözhetünk, így gépeinket elérhető közelségben tudhatjuk. Ez a megoldás elsőként az Egyesült Államokban vált népszerűvé, hiszen így a kezdő vállalkozások egy kézből kaphatnak meg minden szükséges szolgáltatást anélkül, hogy különösebb beruházásra kényszerülnének.

Fő a biztonság

Az első és legfontosabb szempont kétségtelenül a biztonság. A *co-location* szolgáltatók szervertermei zárt, őrszolgálattal védett, bekamerázott területek, ahová csak a szolgáltató szakemberei léphetnek be. Nem csak az illetéktelen behatolók, de az elektromos tüzek is veszélyt jelentenek, így a szervertermek mindegyikét a legkorszerűbb füst- és tűzérzékelő rendszerek védik, az oltáshoz pedig az elektronikus eszközöket megóvó oltógázt használnak.

Hiába azonban a szigorú őrizet, ha áramkimaradás miatt leállnak a rendszerek, így a szerverfarmok általában két, egymástól független elektromos hálózattal vannak kapcsolatban, a rövidebb kimaradások, illetve feszültségingadozás ellen pedig szünetmentes tápegységeket állítanak hadrendbe. A nagyobb létesítmények a hosszabb kimaradásokra is felkészültek, így szükség esetén az alagsorban álló dízel

Szervereinket zárt helyen is tárolhatjuk

Az Interware Data Centerének polcain több száz szerver számára van hely

generátorral látják el árammal a szerverfarm gépeit.

A 2001. szeptember 11-i New-York-i merényletek óta – amikor a World Trade Center ikertornyaiban számos bank, bróker- és informatikai cég szervere is odaveszett – a természeti csapások mellett a terrorista merényletekre is próbálnak felkészülni. Az *Infigate* éppen ezért egy régi, egy méter vastag falú épület alagsorában és pincéjében rendezte be *Telehoteljét*, amely akár komolyabb földrengéseknek is képes ellenállni.

Kicsiknek és nagyoknak

A maga 8800 négyzetméteres nagyságával a Dataplex létesítménye igazi kolosszus, amely mellett az Infigate 1500 négyzetméteres Telehotelje, az *Interware* 200 négyzetméteres *Data Centere*, de főként a *Telnet* 50 négyzetméteres *Webfarmja* szinte eltörpül. Az alapterületek közötti különbség azonban nem véletlen, ugyanis a cégek más-más célcsoportok számára kínálják szolgáltatásaikat.

A Telnet, a Novacom és az Interware főként a tartalomszolgáltatókat és a kisebb vállalkozásokat célozza meg, így nem meglepő, hogy például az Interware Data Centerének polcain több száz vállalkozás PC-alapú szerverei sorakoznak. Ám ha úgy kívánjuk, választhatjuk a *rackes* megoldást is, amikor szerverünk több más masinával egy szekrényben „duruzsol". Azoknak, akik a későbbiekben több rackszekrényt vagy salgó-polcot kívánnak még elhelyezni, érdemes önálló területet kérniük. Az Interware-nél már 1,2 x 2,4 méteres helyet is bérelhetünk.

Az Infigate és a Dataplex már nagyobb „falatokra" pályázik, ügyfeleik között így távközlési cégeket, bankokat és tartalomszolgáltatókat egyaránt találunk. Ezeknél a szolgáltatóknál rack-szekrénynél kisebb szerverrel ne is próbálkozzunk, hiszen szolgáltatásaikat kifejezetten nagyfogyasztóknak kínálják. Ha például nem kívánunk közösködni, a szervertermen belül zárt „lakosztályokat" is bérelhetünk magunknak, ahová csak a mi szakembereink juthatnak be. A Dataplex épületében – akár 100 négyzetméternél nagyobb – különtermet is bérelhetünk, amelynek alapszolgáltatásait – a légkondicionálást, a be- és kiléptetést, a felügyeletet – egyéni igényeink szerint alakítják ki.

Elérhető szolgáltatások

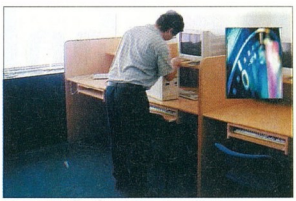
A kolokációs szolgáltatások fix havi díjáért szerverünket megfelelően tárolják, működését monitorozzák, illetve ha szükséges, kikapcsolják és újraindítják. Az Interwarenél az úgynevezett *szolgáltatás monitoring* is benne foglaltatik az árban, amikor az egyes szerveroldali szolgáltatásokat – http-t, mailt stb. – figyelik. Ami az energiaellátást illeti, a legtöbb helyen választhatunk, hogy az eszközök által fogyasztott áramért külön fizetnünk-e, vagy inkább az átalánydíjas megoldást választjuk, amely kiszámítható, fix havi díjat jelent.

A folyamatos energiaellátásról szünetmentes tápegységek gondoskodnak

Amennyiben híján vagyunk a szerverkarbantartásban jártas szakembereknek, vagy egyszerűen nem szeretnénk erre külön erőforrásokat lekötni – természetesen felárért – akár teljes körű rendszeradminisztrációt is kérhetünk. Ebben az esetben a szervermentések, a naplóállományok átkitintése és elemzése, a szoftverfrissítések, a biztonsági beállítások, az új szolgáltatások telepítése és konfigurálása, valamint a karbantartás a szolgáltató feladata, így mi a tevékenységi körünknek megfelelő feladatokra koncentrálhatunk.

Árözön

Az, hogy a szerverünket mennyiért szállásolják el, természetesen az igényelt szolgáltatás függvénye. Amennyiben egyetlen PC-alapú szerverünket szeretnénk jó helyen tudni, és nem zavar minket, hogy a polcon többedmagával csücsül majd, akkor nettó 9 ezer forint körüli havi díjért már találhatunk megoldást. Amennyiben több gép számára szeretnénk polcot, az már drágább, hiszen például az Interwarenél egy 930 x 450 centiméteres hely – ahol négy gép fér el egymás mellett – nettó 29 ezer forintot kóstál. Ha egy egész blokkot bérlünk – a rajta lévő összes polccal egyetemben – akkor a havi 114 ezer forintos számlára készülhetünk.



Szerverünket a helyszínen is javíthatjuk

Az előbbi árak átalánydíjas áramellátásnál érvényesek, ám a rackeknél áramellátás nélkül is kérhetjük a szolgáltatást. Meglévő rack-szekrényünk számára – átalánydíjas áramellátással – nettó 114 ezer forintért bérelhetünk helyet, míg áramellátás nélkül ugyanez 89 ezer forintba kerül. Ha magát az 1/1-es zárható szekrényt is béreljük, akkor átalánydíjas áramellátással 129 ezer forintot kell fizetnünk, míg áramellátás nélkül ugyanez 104 ezer forintot kóstál. Az 1/2-es szekrényért 68 ezer, az 1/4-es szekrényért pedig 37 ezer forintot számláz ki a szolgáltató. Amennyiben átalánydíjas áramellátás nélkül kérjük a szolgáltatást, önálló mérőórára is szükség van, amelynek egyszeri díja – beszereléssel együtt – 120 ezer forint, számlánk pedig minden elfogyasztott kWh után 27,3 forinttal nő.

Már említettük, hogy egyes szolgáltatók kifejezetten a nagyobb cégek – például távközlési és multinacionális vállalatok, bankok, biztosítók, áruházláncok – számára kínálják szolgáltatásaikat. Mivel ezek szerverei több tíz- vagy százmillió forintot is érhetnek, a hosting költségei is nagyobbak, ám ezért cserébe számos különleges szolgáltatást is kínálnak. A számítógépes rendszerek folyamatos működése sok cég számára létkérdés, hiszen képzeljük csak el, hogy például egy banknál milyen problémákat okozhat egy-egy kimaradás.

Fülöp Norbert

Romboló impulzusok

A vírusok, hackerek és más internetes fenyegetések elleni védekezésben sokan hajlamosak megfeledkezni a sokkal hétköznapibb veszélyekről. Ilyen például az áramkimaradás, vagy – ami még rosszabb – a villámcsapás, amely a gép érzékeny részeit teheti tönkre. A tápellátásban bekövetkező zavarok ellen a szünetmentes energiaforrások jelentik a megoldást.

A számítógépeinket működtető elektromos áram ingadozásaival szemben ma már a védekezés több mint kötelező, jóllehet sokan gondolják úgy, hogy a mindennapi életünk részét képező elektromos hálózat önmagában véve ártalmatlan. Pedig elektromos hálózati problémák gyakrabban érnek minket, mint ahogy azt gondolnánk. Minél nagyobb egy hálózat, annál nagyobb az esélye a hálózat által generált feszültségingadozásnak is. Erre csak akkor döbbenünk rá, amikor – derült égből villámcsapásként – modemünk meghibásodik, vagy súlyosabb esetekben a PC-nk merevlemezén tárolt adatok használhatatlanná válnak, sokszor felbecsülhetetlen károkat okozva a tulajdonosnak. Számítógépeink igen gyakran, akár naponta többször is sérülhetnek, kezdve a géplefagyásoktól a különböző hibaüzenetek megjelenéséig vagy a számítógép váratlan leállásáig.

Hogy elejét vegyük a feszültségingadozás miatt bekövetkező hardveres sérüléseknek, és az ezekből következő adatvesztésnek, gyakorlatilag bármely számítástechnikai eszköz használata esetén gondoskodnunk kell a megfelelő védelemről, legyen szó otthoni PC-ről vagy kisebb-nagyobb vállalati hálózatokról.

Az MGE Pulsar termékcsalád megfelelő védelmet kínál a meglepetésszerű áramingadozásokkal szemben

A piacon nagy választékban találunk különféle *UPS (Uninterruptable Power Supply)* berendezéseket, azaz szünetmentes tápokat, amelyek mára első vonali védelmet nyújtanak az áramellátás problémái ellen. A mai szünetmentes tápoknak nem csak az áramellátás a feladatuk, de arról is gondoskodnak, hogy az áramingadozás kiküszöbölésével a megfelelő feszültség jusson el a számítógépünkbe.

Természetesen ezek a berendezések sem ugyanarra a célra készültek. Más és más berendezés vásárlása javasolt az adott probléma vagy a fogyasztott áram mennyisége szerint. Általánosságban elmondható, hogy az egyedülálló PC-k kevés áramot fogyasztanak, ezért az erre a célra szánt szünetmentes tápok úgynevezett *off-line* technológiát igényelnek. Ez azt jelenti, hogy a készülék áramkimaradás esetén automatikusan rákapcsol saját akkumulátorára, és biztosítja a PC folyamatos tápellátását az akkumulátor lemerüléséig.

A következő szintet a *hálózatra kapcsolható* eszközök alkotják. Az off-line technológiával ellentétben ez a készüléktípus már figyeli és beállításainak megfelelően automatikusan korrigálja a beérkező elektromos áram ingadozásait. Ha áramszünet következik be, a szünetmentes táp automatikusan átkapcsol az akkumulátorra, amelyet működés közben folyamatosan feltöltve tart.

A védelem legmagasabb szintjét az úgynevezett *online* UPS technológia jelenti,

Kettős konverziós Smart-UPS

Az *American Power Conversion (APC)* bejelentette rack-es és tornyos kivitelű, kettős konverziós online szünetmentes tápegységeinek új *Smart-UPS RT* családját. Az új termékek kiváló minőségű tápellátás-védelmet kínálnak, áthidalási idő nélkül, a létfontosságú vállalati szerverek és számítógép-hálózatok részére.

Az 1000–10000 VA teljesítménytartományt lefedő, nagy energiasűrűségű Smart-UPS RT tápegységek hosszabb akkumulátoros üzemidőt tesznek lehetővé. A nagy energiasűrűséget mutatja, hogy egy 19 hüvelykes szekrényben az 5000 VA-es tápegység mindössze 3U (1U = 1,75 hüvelyk = 44,45 mm) helyet, a 10 000 VA-es egység pedig mindössze 6U helyet igényel.

Az új Smart-UPS RT főbb előnyei a következők: nagyobb rendelkezésre állás, nulla átkapcsolási idő akkumulátorról vagy akkumulátorra, automatikus és kézi áthidalás, széles bemeneti feszültségtartomány kezelése akkumulátor igénybevétele nélkül (a bemeneti feszültség jellemző terhelések mellett 100-280 V lehet), szoros frekvencia- és feszültségszabályozás, továbbá beépített vészkikapcsoló. Minden egységben beépített akkumulátor van, amelyet a felhasználó üzem közben cserélhet. A Smart-UPS RT termékcsalád minden tagjához tetszés szerinti számú külső – rack-be vagy toronyba szerelt – akkumulátorcsomag csatlakoztatható a kívánt áthidalási idő biztosítására.

Az 1000–5000 VA közötti Smart-UPS RT egységek alaptartozéka a *PowerChute Business Edition* szoftver, felügyeletüket pedig külön megrendelhető *Smart-Slot* kártyák teszik lehetővé. Az 5000-10 000 VA közötti Smart-UPS RT termékeknek alaptartozéka még a beépített webes/SNMP alapú felügyeleti kártya.

amely amellett, hogy gondoskodik a folyamatos áramellátásról, távolról is adminisztrálható. Ez azt jelenti, hogy a rendszergazdák az interneten keresztül akár a város másik pontjáról is lekapcsolhatnak funkciókat, amelyek veszélyeztetik a hálózat legfontosabb berendezéseinek a működését. Ezek a legújabb készülékek úgy is konfigurálhatók, hogy az adott probléma típusa szerint riasztják a rendszergazdát, aki még azelőtt elháríthatja a bajt, mielőtt az bekövetkezne.

A számunkra megfelelő szünetmentes táp beüzemeléséhez feltétlenül javasolt tervben rögzíteni a feszültségingadozás vagy áramszünet esetén szükséges beállításokat, már amennyiben több berendezés igényel védelmet. Először a szünetmentes táp méretét határozzuk meg; a méret itt a fogyasztott áram mennyiségének a függvénye. Aztán arról kell döntenünk, hogy melyik gyártó terméke biztosítja a legmegfelelőbb védelmet számunkra. A beszerzés másik szempontját az egy területen adott, egy hálózatban használt berendezések száma határozza meg. A harmadik szempontot a használt elektromos berendezések típusa határozza meg.

Összefoglalva tehát a következő tervezési szempontokat kell figyelembe vennünk:

- A számítógépes rendszer teljes áramellátásának átlátása
- Az áramellátásban bekövetkező hibák ismerete és problémamentes kezelése
- A szünetmentes tápok karbantartása és a lehetséges hibák felmérése
- Egyes hálózati eszközök ki- vagy bekapcsolhatósága
- Kontrollált számítógép leállások

Vásárláskor győződjünk meg arról, hogy új szünetmentes tápunkban könnyű-e az akkumulátor cseréje. A megvásárolt berendezést mindenképpen a rendszergazda vagy hozzáértő személy konfigurálja. Amennyiben nagyobb hálózatról kell gondoskodni, akár több szünetmentes táp beszerzése is szükségessé válhat. A berendezésekben lévő akkumulátort rendszeresen tesztelni kell, erre a célra a gyártók külön programokat is mellékelnek. Azért, mert beszereztünk egy szünetmentes tápot, ne feledkezzünk meg adataink rendszeres elmentéséről. Bár ezek a berendezések hatékony védelmet nyújtanak, 100%-os adatvédelem nincs!

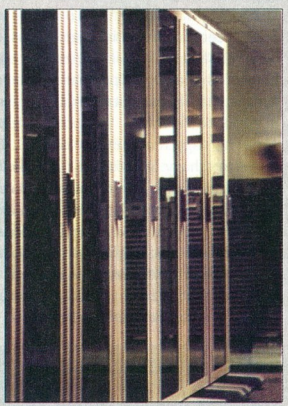
Forrás: www.liebert.com, www.mgeups. com.

Kemény László

Helyhiányos adatközpontok

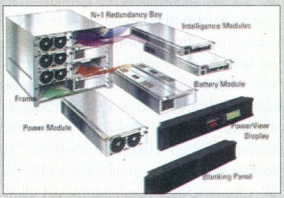
Hasonlóan az egyes számítógépek vagy vállalati hálózatok biztonsági igényeihez, a nagyobb vállalatok, bankok, informatikai cégek adatközpontjai számára is alapkövetelmény a megfelelő minőségű és zavartalan áramellátás. Bár a cégek rendszerint beszerzik az áramellátásról és védelemről gondoskodó berendezéseket, gyakran a rendszeren belüli rendkívüli belső terhelés, illetve az emberi mulasztás is hibajelenségekhez vezethet. Az igazi problémát az UPS nagy helyigénye jelenti, mivel az elmúlt évek technológiai fejlődése ellenére sem csökkent ezeknek az eszközöknek a mérete.

A hagyományos adatközpont áram elleni védelmét úgy oldják meg, hogy vagy szekrényenként egy-egy szünetmentes táp gondoskodik az azonos helyen tárolt berendezések védelméről (rack-es elhelyezés) vagy egy UPS gondoskodik minderről (központi elhelyezés), amely magában az adatcentrumban található, de legtöbbször valahol máshol az épületben kerül elhelyezésre.



Nagy adatközpontokban a helyhiány okozza a legnagyobb problémát

Az egyik vezető gyártó – nevezetesen az *American Power Conversion (APC)* – a két meglévő elhelyezési módon túl egy harmadik megoldást (úgynevezett sávos kiépítést) fejlesztett ki, illetve mindhárom elhelyezési módot egyszerre alkalmazza. Az áramfelvétel alapján határozzák meg, hogy melyik módszer vagy módszerek együttes alkalmazásával kerüljön sor az új rendszer telepítésére. A megoldás a rugalmas elhelyezhetőségnek köszönhetően akár a rendelkezésre álló hely 20%-át is felszabadíthatja, átadva a helyet az adatközpont működését hatékonyabbá tevő fontos egységeknek.

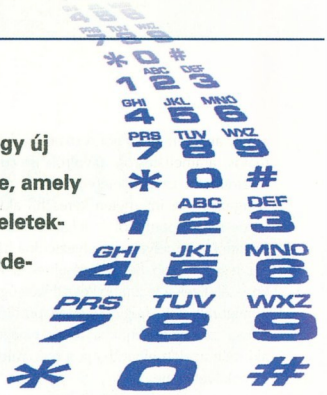


A moduláris felépítés hatékonyabb működést tesz lehetővé

Az *InfraStruXure* néven bejelentett architektúra egy vagy több UPS segítségével oldható meg. Egy UPS esetén a bejövő áramra csatlakozó táp egy forrásból biztosítja a zavartalan áramellátást. A belső feszültség-ingadozások okozta hibák egy század százalék alatti előfordulási esélyét belső rendszere garantálja. A második módszer alkalmazásakor már két külön áramforrást kötnek egy UPS-re. Ebben az esetben már beépített kapcsolót helyeznek el, amely automatikusan vált a két áramforrás között, amennyiben áramingadozás vagy a terhelés miatt szükségessé válik. Ez a felépítési mód egy ezrelék alatti hibalehetőséget okozhat. A harmadik esetben két áramforrásra két külön UPS berendezést kötnek, amellyel még jobban leszorítják a hiba lehetőségét, a gyártó itt már gyakorlatilag kizárja a hiba előfordulását (99,99999%).

Az adatközpontok vásárlása előtt a szakemberek tervet készítenek, amelyben meghatározzák az adatközpont berendezéseit, például áramfelvétel szerint (mondjuk 230V, 3 fázis), felállítják a rendszer prioritásait: ha helyhiány van, melyik az az eszköz, amely feltétlenül védelmet kell kapjon, és melyek azok, amelyek kiépítése várhat. A védelem típusának a meghatározása után a gyártó szoftvere további segítséget nyújt a megfelelő berendezések kiválasztásában.

Forrás: www.apc.com



Az ipar és a tudomány szakértői egy új biztonsági rendszert jelentettek be, amely a bevásárlásoknál és a banki műveleteknél gondoskodhat majd az adatvédelemről. Az úgynevezett nyilvános kulcsú titkosítás új fejezetet nyithat a mobil kereskedelemben.

Megbízható mobilok

A *Trierben* működő *Institut für Telematik* nemzetközi konferenciát rendezett a mobil kereskedelem *(m-commerce)* új fejlesztéseiről. A találkozó fő témája az volt, hogy mi módon lehetne gondoskodni a vezeték nélküli elektronikus üzleti forgalom biztonságosságáról.

Az intézet szerint a mobil kereskedelem további fejlesztéseinek elfogadásához elsősorban bizalomra és egységesítésre van szükség, ami egyben azt is jelentené, hogy jogi értelemben minden mobil-kereskedelmi folyamat támadhatatlan lenne. Garantálni kellene ezen felül a vírus-támadások elleni védelmet is. A fórum lehetőséget adott arra, hogy a tudósok, a gazdaság és igazgatás jeles képviselői megismerkedhessenek az ezen a területen megjelenő új információs és kommunikációs technológiák adta lehetőségekkel, ezenkívül alkalmat adott a gyakorlati tudás megvitatására és kicserélésére is.

Fizetés telefonnal

Az egyik fő témát a *fizetési rendszerek* és a belőlük fakadó lehetőségek képezték. A jövőben az internetet elérő mobilterminálok olyan többletszolgáltatásokkal is bővülnek, mint például a bankautomata keresése mobiltelefonon keresztül, a mobil fizetési lehetőségek, valamint a mobil tranzakciók. Ez bővítené a *WAP (Wireless Application Protocol)* alkalmazásokat, és a többletinformáció-szolgáltatáson felül lehetővé tenné a tranzakciók biztonságos lebonyolítását is. A felhasználó ezentúl bárhonnan és bármely időpontban kezdeményezhet majd banki átutalásokat, akár mobiltelefonon, PDA-n (Personal Digital Assistent) vagy mobil PC-n keresztül. Ez azt jelenti, hogy lehetőség nyílik a bankszámla állásának lekérdezésére, annak megterhelésére, jóváírások kiválogatására, bankkártya-folyamatokat ellenőrzésére, saját folyószámlák közötti pénzáramoltatásra, illetve átutalás kezdeményezésére. A *Paybox* mobil fizetési rendszer alapjait szintén bemutatták az értekezleten.

Aktív SMS

A biztonságos mobilhasználatra jó példa a *Westel* és az *OTP Bank* SMS alapú szolgáltatása. Az *OTPdirekt aktív SMS* olyan korszerű megoldás, amely egy speciális SIM kártya segítségével gondoskodik arról, hogy a mobiltelefonról közvetlenül, könnyen, gyorsan és biztonságosan lehessen pénzügyi tranzakciókat lebonyolítani. A számlaegyenleg és az árfolyamok lekérdezése mellett átutalásra, bankkártyához tartozó vásárlási-limit módosítására, betétlekötésre, számlaforgalom lekérdezésére és OTP bankkártyával végzett tetszőleges Domino kártya egyenleg feltöltésére van lehetőség.

A szolgáltatáshoz speciális SIM kártya szükséges, amelyen olyan alkalmazás található, amely könnyűvé, egyszerűvé és biztonságossá teszi a banki műveleteket, sőt a SIM kártyán 5-5 különböző számla, bankkártya, célszámla és közlemény adatai is tárolhatók.

Segít a Location kereső

Akinek készpénzre van szüksége, azt nem kaphatja meg a mobiltelefonjától. Ilyen jellegű kívánságok esetében is azonban nemsokára segítséget nyújtanak a mobil eszközök: a *Location* keresővel gyerekjáték lesz megtalálni a legközelebbi banki automatát vagy éjszakai trezort. A felhasználó a kijelzőn nemcsak a címet, hanem egy kis térképet is lát majd, amely egy későbbi fejlesztés eredményeként esetleg még a legrövidebb odavezető utat is képes lesz majd megmutatni.

A mobil bank mellett az *M-Brokerage* is megváltoztathatja a bankok és a pénzügyi szolgáltatók világát. Az M-Brokerage egy új és hasznos WAP funkciót kínál a befektetők számára, amelynek segítségével helyhez kötöttség nélkül kereskedhetünk értékpapírokkal. Az egyes értékpapírokhoz nemcsak a vétel, illetve eladás parancsok rendelhetők hozzá, hanem az azok eladásáról, illetve vételéről szóló visszaigazolás is megtörténik. Mód nyílik tovább a tőzsdei árfolyamok lekérdezésére, a piaci meghatározó jegyek figyelemmel kísérésé-

re, vagy a teljes portfolió megtekintésére. A kínálat állandóan friss. A mobilkereskedelem előnyeit főként a folytonosan időhiánnyal küszködő brókerek fogják majd értékelni.

Titkos kapcsolatok

A szimpózium elsősorban a biztonságot érintő témákkal foglalkozott. Szóba került a vállalatok összekapcsolódásának problémája is. Máris számos vállalat és hivatal élvezi a közös kapcsolat előnyeit, amellyel lehetővé vált a kódolt és az aláírással ellátott e-mailek belső elküldése, illetve fogadása. Ezeket azonban szeretnék a külső kommunikációban is alkalmazni.

A nyilvános kulcsú *(Public Key Infrastructure, PKI)* kapcsolatok feltétele, hogy a tanúsítványokat mindkét fél elismerje. Azonban mind az infrastruktúrák gyártói, mind pedig azok értékesítői számára felmerül a kérdés, hogy a különböző kulcsokat miként lehetne egymással összekapcsolni, hogy a felhasználók ne ütközzenek akadályokba.

A *Bridge CA (Certification Authority)* megoldása lehetne ennek a problémának. Meglevő biztonsági struktúrákat köt össze egymással, így különböző szervezetek között is gondoskodik a biztonságos kommunikációról. Az egyes biztonsági struktúrákat összekötő hídként a Bridge CA ezek alkalmazási területét bővíti. Nem lesz szükség a tanúsítványok kicserélésére, a már meglévő beruházások nem vesznek kárba, sőt egy újabb résztvevő csatlakozásakor a haszon arányosan megnő minden tag számára.

Egy semleges bizottság dönt egy meglevő Public Key infrastruktúra Bridge CA-re történő csatlakoztatásáról. Hardver és szoftver tanúsítványok is elfogadottak. Az ajánlások hosszú távon támogatják a chipkártyákra való átállást, hogy ezzel meg tudjanak felelni az aláírási törvény elvárásainak is.

GPRS = nagyobb veszély

Míg a korábbi mobiltelefon-generációnál gyakorlatilag nem állt fenn vírusveszély, addig a *GPRS* és az *UMTS* mobil szabványoknál egészen más a helyzet. Amilyen mértékben növekszik a mobiltelefonok tudása és processzorkapacitása, úgy lesznek egyre inkább érzékenyek a készülékek a támadásokra is. Az új mobiltelefon-szabványok megnövelik a hacker-támadások lehetőségét.

A GPRS mobiltelefonok legújabb generációja magával hozza a mobilvírusok első hullámát. Ennek oka, hogy a GPRS-nél használják először a *WML (Wireless Markup Language) 1.2*-es verzióját. Ezzel lehetővé válik, hogy számítógép programokat wapos mobiltelefonokba töltsünk. A programokkal változtatni lehet a telefonkönyvet: számokat törölni, megváltoztatni vagy beírni. A többi telefonfunkció manipulálása is lehetséges lenne anélkül, hogy azt a tulajdonos észrevenné. Az első vírustámadások még aránylag ártalmatlanok lesznek, mert a különböző WAP gateway-ek, szerverek, telefonkészülékek és WAP-böngészők még nagyon eltérnek egymástól. Ezért az első WAP-vírus generációnak nehéz lesz nagy területen elterjednie. A növekvő szabványosodással azonban javulni fognak a vírusok terjedési feltételei is. A *WML 2.0* közelgő bevezetése megnyitja a kapukat a digitális kártevők előtt.

Vezeték nélküli koncepciók

A *Baltimore Technologies* biztonsági szakcsoportjának fejlesztési témája a biztonságos kapcsolatok megoldásainak átvitele a vezeték nélküli világra. A meglevő internet szabványok és formátumok nem a legkedvezőbbek a mobil kommunikáció számára: a mobil kapcsolatban alkalmazott sávszélesség túl alacsony, a végberendezések pedig csak kevés processzor- és memória-kapacitással rendelkeznek. Az újonnan definiált „keskeny" titkosítási kulcsok inkompatibilisak a meglevőkkel, és ez ahhoz vezet, hogy a vezetékes és a mobil felhasználóknak különbözőek a kulcsaik.

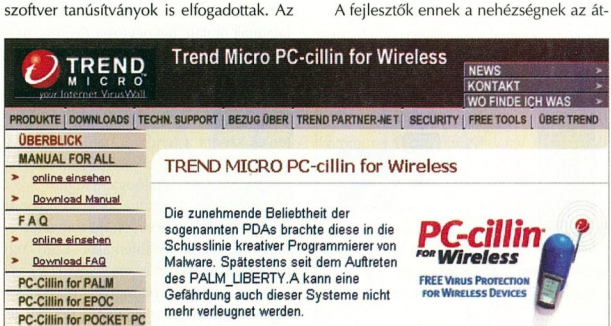
A fejlesztők ennek a nehézségnek az áthidalására olyan azonosítók használatát javasolják, amelyek a tanúsítványokra hivatkoznak. A mobil területén belül nem a valódi tanúsítványt küldik el, hanem egy úgynevezett *Certificate ID*-t, mégpedig egy *URL (Uniform Resource Locator)* sztring formájában. Ennek az az előnye, hogy csak minimális sávszélességre és memóriakapacitásra van szükség, az adatátvitelnél nem adódhat probléma, és több Certificate ID tárolására is lehetőség nyílik.

A vezeték nélküli és a vezetékes világ kulcsai közötti kapcsolatról egy *PKI portál* gondoskodik. A PKI portál a regisztrációs bejelentkezéseket egy szabványos PKI-nek továbbítja. A szoftverrel a mobil szolgáltatásokkal foglalkozó vállalatok alacsony anyagi ráfordítással és rövid idő alatt képesek Public Key infrastruktúrájukat egy új vezeték nélküli készülékre kiterjeszteni.

Ennek az elvnek az alapján a Baltimore már be is mutatott egy szoftveres megoldást, amellyel digitális tanúsítványokat lehet szétküldeni, és a vezeték nélküli felhasználókat gyorsan és egyszerűen lehet azonosítani. A *Telepathy* regisztrációs rendszerrel tömegesen lehet tanúsítványokat kiállítani a mobil hálózaton keresztül. Ez különösen jelentős fejlemény a mobil kereskedelemben érdekelt szolgáltatók, nagyvállalatok, brókerek számára.

Az új megoldás támogatja a fórumon megállapított legújabb vezeték nélküli biztonsági szabványokat: a *Wireless PKI*-t *(WPKI)*, a *Wireless Identity Modult (WIM)* és a *SignTextet* (digitális aláírásokhoz használt WAP standard).

Gyarmati László



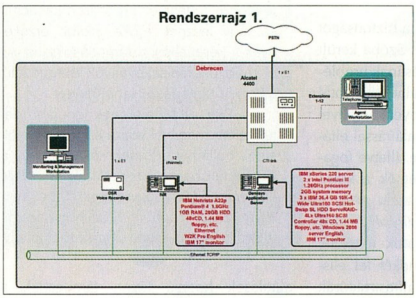
Nehogy gáz legyen...

A biztonságról más fogalmai vannak egy gázszolgáltató cégnek, mint egy informatikai vállalatnak. És megint más szempontok merülnek fel, ha két ilyen cég találkozik. Cikkünkben a Mol-Gáz gázszolgáltató óriáscég informatikai-távközlési hálózatát vesszük szemügyre – különös tekintettel az adatbiztonságra.

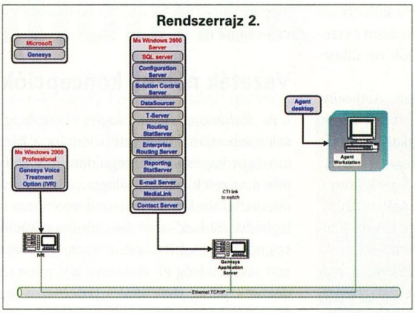
A *Mol-Gáz Kereskedelmi Kft.*, mint vezetékes gázszolgáltató számára elengedhetetlenül fontos, hogy a rendszerében előforduló hibákról – amelyek akár tényleges veszélyt is jelenthetnek a lakosságra nézve – haladéktalanul értesüljön. Sőt, a hibabejelentésnek akkor kell csak igazán a helyzet magaslatán lennie, amikor bármilyen oknál fogva zavar támad a rendszerben. Az *Euronet Rt.* által megvalósított, szolnoki központú, tizenkét telephelyes integrált hang- és adatforgalmi hálózat, valamint az erre épülő ügyfélkapcsolati megoldás gondos tervezéssel és számos kézenfekvő megoldással gondoskodik arról, hogy ne fordulhasson elő, hogy nem értesülnek időben valamely problémáról.

„A biztonság megteremtése nem varázslat – mondja *Járosi Miklós*, az Euronet Rt. kereskedelmi igazgatója – hanem figyelem, átgondolt tervezés eredménye. A Mol-Gáznál a biztonság kulcsa a *redundancia*, illetve a 'menekülő utak' kiépítése, de kihasználtuk természetesen az alkalmazott szoftvermegoldásokba beépített lehetőségeket is."

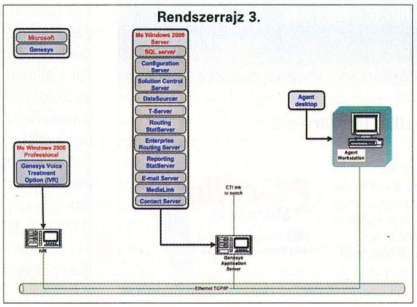
Rendszerrajz 1.



Rendszerrajz 2.



Rendszerrajz 3.



Csökkenő költségek

A rendszer megvalósításának alapvető célja az volt, hogy a Mol-Gáz Kereskedelmi Kft. telefon- és adatforgalmi költségei csökkenjenek és kiszámíthatóbbá váljanak, a vállalati struktúra lényegi átszervezése nélkül. Az új debreceni központot és a tizenkét telephelyet bérelt vonallal kötötték össze, és egy rendszerbe integrálták. Hét telephelyen az adatkommunikációt biztosítja a rendszer, hatnál pedig a hang- és adatintegrációra, azaz a *Voice over IP* technológiára is megoldást kínál.

Az alkalmazott technológia alapja az úgynevezett *frameflex* béreltvonali összeköttetés, amelynek a lényege az, hogy a szolgáltatóval kötött megállapodás alapján egy megadott garantált minimális és maximális érték között mozoghat a sávszélesség. Így egy, két vagy akár több beszélgetés és ezzel párhuzamosan adatforgalom folyhat.

A hálózatra a *Genesys* kis- és középvállalatinak titulált, úgynevezett *Express* megoldása épül, amely az ügyfélszolgálati és hibabejelentő munkát támogatja. A Genesys contact center fő feladata a telefonos ügyfél-kapcsolattartás segítése, de a tervek szerint a rendszer hamarosan a faxon és e-mailen érkező megkeresések megválaszolását is támogatni fogja.

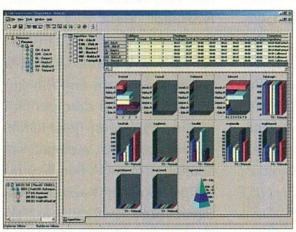
A Mol-Gáz kívánsága az volt, hogy az ügyfél minden esetben elérje a kezelőt, és bejelenthesse a problémáját. Ezért úgy tervezték meg a rendszert, hogy ha a kritikus elemei közül bármelyik meghibásodik, akkor azt haladéktalanul pótolni lehessen.

Rendszerelemek

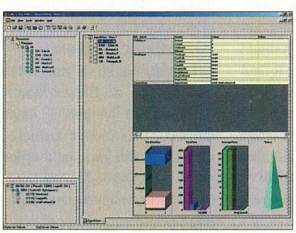
A rendszer kritikus elemei a telefonközpont, az IVR megoldás és a Genesys ügyfélszolgálati rendszer, valamint a központi router. Emellett tartozik hozzá egy hangrögzítő rendszer is, amely a dokumentálást végzi a későbbi ellenőrizhetőség érdekében, és természetesen ott vannak még a szolgáltató által biztosított – és azért az Euronet hatáskörén kívül eső – telefonkapcsolatok is.

A betelefonálás folyamatát tekintve az első feladat, hogy a hívó eljusson a céghez – azaz létrejöjjön a telefonos kapcsolat. A Mol-Gáznál több kerülőutat építettek ki, mindegyik telephely elérhető akkor is, ha a központ és a telephelyek közötti bérelt vonal megszakadna. A bérelt vonal meghibásodása esetén automatikus riasztást küld a szolgáltató és a felhasználó felé, és a szerepét a privát hálózaton belüli adat- és hangkommunikációra egy ISDN (back-up) vonal veszi át, de legtöbb helyen a korábbi analóg vonalak is megmaradtak, így ezek a telephelyek közvetlenül is elérhetők maradnak ebben az esetben az ügyfelek számára.

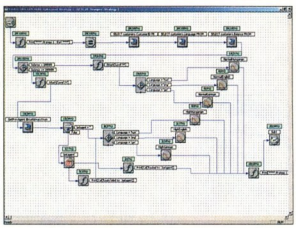
Ha az ügyfél már eljutott a Mol-Gázhoz, akkor a következő feladat, hogy eljusson a kezelőig. A telefonalközpont hibája esetén – egy vészkapcsolási rendszerrel – előre definiált menekülési útvonalra kerül a hívás, automatikusan egy olyan mellékre fut ki, ahol biztosan választ kap. Hasonlóképpen az IVR-be és a Genesys ügyfélszolgálati rendszerbe is beállítottak meghibásodás esetén közvetlenül kapcsolt mellékeket, a contact center szerver hibájától pedig a hardver megfelelő részeinek redundanciája véd.



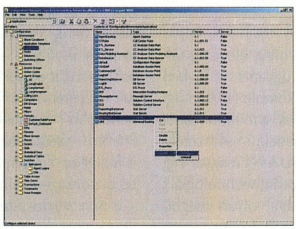
CC Pulse: az operátorok aktuális állapota



CC Pulse: az egyik operátor aktuális állapota



Interaction Routing Designer: integrált stratégia-menedzsment



CME: a contact center centralizált kontrollja

Első az ügyfél

A hardveres védelem mellett több szoftveres megoldás segíti a zavartalan működést. Az integrált hálózatban például prioritás-beállítások gondoskodnak a forgalom zavartalanságáról. Első helyen az ügyfélszolgálat IP mellékeinek hangforgalma áll, második a hozzájuk tartozó belső adatforgalom, amely a belső rendszerek által használt információkat jelenti (például: több telephelyen működő, egymással kommunikáló pénzügyi vagy ügyfélszolgálati megoldás), és csak a harmadik az internetes letöltéseké. A dinamikus sávszélesség kiosztás és vezérlés így gondoskodik arról, hogy míg az ügyfél éppen az ügyintézővel beszél, ugyanazon a kapcsolaton egy nagy internetes letöltés vagy adatforgalom nehogy elnyomja a beszélgetést.

A Genesys ügyfélszolgálati megoldást a telephelyek feléről használják az operátorok – természetesen megfelelő jelszavas védelemmel és jogosultságkezeléssel. A rendszer a vállalat központi vevőadatbázisát használja.

„Gyakran elmondjuk, hogy a biztonság kulcsa a folyamatos figyelem, karbantartás, ami nem az ügyfél lelkének 'ápolgatását' jelenti, hanem azt, hogy a munkatársunk időről időre ellenőrzi a rendszert, elvégzi a szükséges javításokat, frissítéseket, megnézi, hogy rendben vannak-e a beállítások – mondja Járosi Miklós. Tapasztalatunk, hogy az ügyfél számára előnyösebb a karbantartási szerződés, bár ezt sajnos még nem mindenki érti meg. Persze nincs rendszer váratlan hiba nélkül. Meghibásodás esetén – a vállalt rendelkezésre állástól függően mielőbb megkezdjük a hiba elhárítását, a Mol-Gáz hálózat egyes elemeire például azt vállaljuk, hogy négy órán belül akár a helyszínen vagyunk – az országban bárhol – és 24 órán belül cserealkatrészt biztosítunk."

(-)

Innovatív vírusvédelem

Stratégiai együttműködési megállapodást kötött a *ZORP* tűzfal-technológiát fejlesztő *BalaBit* és a vírusvédelmi rendszereket fejlesztő *VirusBuster*. A két magyar tulajdonú cég megosztva nyerte el az „év innovatív megoldása" díjat a 2003. április 9-én és 10-én az MTA székházában megrendezett „Informatika a hatékonyságért" konferencián. A rendezvény fővédnöke az Informatikai és *Hírközlési Minisztérium* és a *Vezető Informatikusok Szövetsége* volt, kiemelt szakmai támogatója pedig az *Informatikai Vállalkozások Szövetsége (IVSZ)*.

A megállapodás értelmében a két hazai fejlesztőcég a jövőben felhasználja egymás technológiáját kereskedelmi termékeiben.

A technológiai szövetséget a

A ZORP professzionális szintű tűzfalvédelmet kínál a világhálózatra csatlakozó rendszerek számára

piaci igény hívta életre, a felhasználók ugyanis előnyben részesítik a komplex biztonsági megoldásokat, a több forrásból származó védelmi rendszerekkel szemben. A két magyar cég reményei szerint technológiáik kombinálásával olyan megoldásokat tudnak kínálni, amelyek világviszonylatban is egyedülállónak számítanak.

Deloitte & Touche a Dataplexnél

A *Deloitte & Touche Üzletviteli és Vezetési Tanácsadó Rt.* a *Dataplex* budapesti nagybiztonságú adatközpontjában helyezte el 16 közép- és kelet-európai államban működő üzletkritikus informatikai és adatforgalmi berendezéseit. A közvetlen és nagy sávszélességű összeköttetést Budapest és a régióban működő Deloitte & Touche irodák között az *AT&T Global Network Services Hungary* biztosítja a Dataplexnél elhelyezett POP-ja révén. A piacot meghatározó, Big Fournak is nevezett üzleti tanácsadó vállalatok közül Magyarországon jelenleg egyedül a Deloitte & Touche rendelkezik az adatforgalom extrém biztonságát nyújtó, rugalmas infokommunikációs infrastruktúrával.

A Deloitte & Touche, az AT&T és a Dataplex szakemberei a berendezések áttelepítésénél Magyarországon korábban még nem alkalmazott, megkülönböztetett IT biztonsági megoldásokat alkalmaztak. A Deloitte & Touche berendezéseit három, egymástól mindenben szeparált biztonsági térben helyezték el: külön redundáns tűzszakasz, redundáns klíma és redundáns áramforrás gondoskodik a szerverkiszolgálás, a storage és a backup működésének folyamatosságáról. A Deloitte az *EMC* terabájt méretű *Symmetrix* high-end storage rendszerét használja tárolásra.

A Deloitte & Touche adatainak szupergyors továbbításáról az AT&T Global Network Services EVPN végpontja gondoskodik, azaz a Deloitte nem fizet más szolgáltatónak összekapcsolási díjat, sem más adatforgalmi költséget. Az AT&T az előző év végén helyezte el hálózati adatkommunikációs eszközeit a Dataplexnél, ügyfelei innen közvetlenül kapcsolódnak a cég globális hálózatához.

Biztonságos ujjlenyomat

Adataink megvédésére rengeteg jelszót, PIN kódot, belépési azonosítót használunk, de ma már léteznek sokkal biztonságosabb módszerek is, amelyek az emberi test természetes jellemzőire épülnek. Az ujjlenyomat viszonylag régóta ismert – elsősorban a bűnüldözésben – de újabban egyre elterjedtebb módszernek számít például az írisz-, a retina-, az arc-, a hang- vagy a kézírásfelismerés is. Ezeket a biológiai azonosítókat egyfelől nem tudjuk elfelejteni, másfelől sokkal nehezebb visszaélni velük. Három személyazonosítással is foglalkozó informatikai, illetve biztonságtechnikai világcég – a *Sun Microsystems*, az *AC Technology* és a *Cross Match Technologies* – most a világon elsőként kínál olyan személyazonosítási megoldást, amely a biometriai adatokat *Smart Card* (intelligens kártya) technológiával egyesíti.

Az új személyazonosítási megoldás lényegi eleme a Cross Match Technologies Verifier E ujjlenyomat-olvasója

Az AC Technology *BiObex* nevű, biológiai azonosítási szoftveréből, a Cross Match Technologies *Verifier E* ujjlenyomat-olvasójából és a *Sun Microsystems* úgynevezett vékonykliens asztali munkaállomásaiból álló rendszer az első olyan, törvényszéki előírásoknak is megfelelő, biometriai alapú hitelesítési megoldás, amely megfelel az *FBI NIST (National Institute of Standards and Technology)* előírásainak.

A megoldás eredetileg a szövetségi kormány számára készült, de igen jól használható olyan, nagy biztonságot igénylő területeken is, például az egészségügyben vagy a bankvilágban, ahol kulcsfontosságú a személyazonosság megállapítása, a különféle csalások és számítógépes terrorcselekmények megakadályozása.

Az új BiObex szoftver segítségével nemcsak az asztali gépekhez, hanem bármely más fizikai vagy digitális portálhoz és más belső céges hálózatokhoz vagy az internethez való hozzáférés is szabályozható.

Mivel helyileg nem tárolnak semmilyen bizalmas adatot, a Sun Microsystems *Sun Ray* kliensek biztonsági szempontból ideális megoldást jelentenek, és hatékonyan védenek az adatlopás ellen. A Sun Ray intelligens kártyák használatával úgynevezett „virtuális asztal" *(hot desk)* architektúrát valósít meg: a felhasználók a kártyájukkal kezdeményezhetnek biztonságos kapcsolatot a hálózat bármely helyéről.

Tovább növeli a megoldás biztonságát a Cross Match Technologies Verifier E nevű terméke. Szemben a kisméretű, olcsó, szilícium alapú ujjlenyomat-olvasókkal, a Verifier E igen tartós, nagyméretű lapja nagy pontossággal képes leolvasni az FBI előírásainak megfelelő nyomatokat is.

Damovo: NetScreen támogatóközpont

A *Damovo* globális kommunikációs szolgáltató Európában az elsők között elnyerte a *NetScreen Technologies* engedélyezett támogatóközpontja *(NetScreen Authorised Support Centre, NASC)* minősítést. Az együttműködés keretében a Damovo új, a NetScreen berendezéseire épülő felügyelt biztonsági szolgáltatást vezet be ügyfelei számára. A NetScreen az integrált hálózati biztonsági megoldások vezető fejlesztője. A cég olyan kulcsfontosságú technológiákat fejleszt, mint a virtuális magánhálózatok (VPN), a szolgáltatásvédelem megtagadása, a tűzfalak és a behatolás elleni védelem, és mindezeket könnyen üzemeltethető berendezések és rendszerek formájában teszi elérhetővé a felhasználók számára.

Az NASC minősítés megszerzését követően a Damovo szorosan együttműködik a NetScreen regionális műszaki támogató központjával, ezáltal a végfelhasználók egyszerűen és rugalmas módon férhetnek hozzá a teljes körű terméktámogatási szolgáltatásokhoz az európai, közel-keleti és afrikai régió területén bárhol. A támogatás kiterjed a NetScreen infrastruktúra-támogató partnerei – az IBM és a UPS – szolgáltatásaira is.

Microsoft: Védett Wi-Fi

A *Microsoft* bejelentette, hogy ingyenesen letölthető a *Microsoft Windows XP* frissítése, amely Védett Wi-Fi hozzáférést *(Wi-Fi Protected Access, WPA)* tesz lehetővé. Ez a *Wi-Fi Alliance* új, szabványos biztonsági megoldása a vezeték nélküli hálózatokhoz. Az új megoldás a vezetékessel egyenértékű adatvédelmi *(Wired Equivalent Privacy, WEP)* szabványt váltja fel, s robusztusabb adattitkosítási és hálózati hitelesítési módszereket biztosít annál. Ennek eredményeképpen a korábbinál magasabb szintű védettséget érhetnek el, akik a Windows XP vezeték nélküli szolgáltatásait használják.

A Védett Wi-Fi hozzáférés két fronton veszi fel a küzdelmet a veszélyekkel: az adattitkosítás és a felhasználó-hitelesítés terén. A Védett Wi-Fi hozzáférés megoldást nyújt a vezetékes hálózat korábbi kriptográfiai gyengeségeire, és új metódussal, automatikusan generálja és továbbítja a titkosítási kulcsokat. Ezentúl az adatok a legutolsó bitig egyedi titkosítási kulccsal lesznek titkosítva, s ennek köszönhetően nagymértékben javul a biztonság. A megoldás az adatok integritását is ellenőrzi, vagyis a támadók nem tudják módosítani a kommunikáció során továbbított adatcsomagokat. A Védett Wi-Fi hozzáférés a vállalati szintű felhasználó-hitelesítés terén is előrelépést ér el: a hálózat minden felhasználóját hitelesíti, de az idegen hálózatokról csatlakozókat távol tartja.

Biztosított biztosító

Közel fél éves projekt keretében, az *ICON* segítségével az *Argosz Biztosító* új kommunikációs és adatbiztonsági rendszert alakított ki. A projekt során olyan komplex feladatok együttes megoldására került sor, mint az átállás *Microsoft Windows 2000* alapú rendszerre, a Lotus alapú egységes munkakörnyezet kialakítása és a biztonságos internet kapcsolat létesítése.

Kormányzati biztonság a Microsofttól

A nemzeti kormányok és főbb szervezeteik sokkal komolyabb biztonsági fenyegetésekkel néznek szembe, mint a technológia más felhasználói. Ezt felismerve a *Microsoft* nemrég bejelentette a *Kormányzati Biztonsági Programot (Government Security Program, GSP)*, azt a globális kezdeményezést, amely kontrollált hozzáférést kínál a *Microsoft Windows* forráskódhoz és egyéb műszaki információkhoz. Oroszország és a NATO már aláírta a GSP megállapodást a Microsofttal, és a cég több mint 20 országgal tárgyal azok részvételi szándékáról. A GSP programban való részvétel felfedése mindegyik aláíró ország saját hatáskörébe tartozik, ám ahol szükséges, a Microsoft biztosítja a titkosságot.

A Kormányzati Biztonsági Programot a kormányok speciális biztonsági követelményeire szabták. A GSP díjtalan kezdeményezés, amely képessé teszi a program résztvevőit arra, hogy egy kódellenőrző eszközzel ellenőrizzék a Windows forráskódot, és alávessék bizonyos engedélyezési korlátozásoknak. A forráselérésen túlmenően a GPS biztosítja a Windows platform műszaki információinak felfedését is, ami segíti a kormányokat abban, hogy erős biztonsági technológiákkal ellátott számítástechnikai infrastruktúrát építhessenek és telepíthessenek. A program a Microsoft biztonsági szakemberei és a program résztvevői közötti élénkebb kommunikációt és együttműködést is elősegíti, lehetőséget nyújtva a Microsoft redmondi fejlesztő létesítményeinek meglátogatására és a Windows forráskód fejlesztési, tesztelési és telepítési folyamatok különböző aspektusainak áttekintésére.

A Microsoft 2001-ben indította el a *Megosztott Forrás Kezdeményezést (Shared Source Initiative)*, abból a célból, hogy a Windows forráskódot átláthatóbbá tegye bizalmas partnerei és ügyfelei számára. A cég 2002-ben jelentette be a *Megbízható Számítástechnika (Trustworthy Computing)* kezdeményezését, a Windows fejlesztési munkájának középpontjába állítva a biztonságot.

A Kormányzati Biztonsági Program a *Közös Kritériumok (Common Criteria, CC)* tanúsítványra is támaszkodik. A Windows 2000 tavaly októberben megkapta a CC tanúsítványt – mely egy globálisan elfogadott, független szabvány az információ-technológiai termékek biztonsági jellemzőinek és képességeinek kiértékelésére –, arra való tekintettel, hogy az *Információ-Technológiai Biztonsági Kiértékelés Közös Kritériumai (Common Criteria for Information Technology Security Evaluation, CCITSE)* definíciója szerint átfogóbb reális forgatókönyv készletet produkált, mint bármelyik más operációs rendszer.

Új RSA partner

Az e-biztonsággal foglalkozó *RSA Security* a *DNS Hungária Kft.*-t választotta első disztribútorául Magyarországon. A DNS Hungária viszonteladói az RSA Security termékeit és szolgáltatásait a hálózatok kiépítésében használják majd. A DNS Hungária Kft. RSA termékeket, professzionális szolgáltatásokat értékesít és támogatást nyújt Magyarországon, valamint marketing és egyéb eszközökkel is hozzájárul az RSA termékek és szolgáltatások hatékony terjesztéséhez.

SAP a belbiztonságért

Az *SAP* újonnan bemutatott *SAP Security Resource Management* átfogó biztonsági-erőforrás-kezelő megoldása a belbiztonság speciális folyamatait támogatja – a határőrség munkáját, a rendkívüli készültség megteremtését és a rendkívüli helyzetek kezelését, az ellenintézkedések foganatosítását, az információelemzést és a külső koordinációt. Az SAP Security Resource Management révén a kormányhivatalok olyan technológiai platformra tehetnek szert, amely javítja együttműködési készségüket és kritikus fontosságú folyamataik kezelésének hatékonyságát. A belbiztonsági szervek emberi erőforrásait, folyamatait és technológiáit biztonságosan integráló új megoldás lehetővé teszi, hogy valamennyi érintett személy és szervezet közösen dolgozzon a biztonsági lépések lehető legeredményesebb végrehajtásán.

Az SAP Security Resource Management az SAP *e-government* technológiájára épül. A kormányzati szféra vezető nemzetközi megoldásszállítójaként ismert SAP az elmúlt 30 évben az állami és magánszektor 18 800 szereplőjét segítette hozzá globális működése sikeres integrálásához. A vállalat új, nyílt platformú megoldása zökkenőmentes kommunikációt biztosít a belbiztonság szempontjából fontos minisztériumok, kormányszervek és magáncégek között.

Műszaki hátterét tekintve az SAP Security Resource Management a heterogén informatikai környezetek együttműködését támogató *SAP NetWeaver* integrációs és alkalmazásplatformra épül. Az SAP NetWeaver egyben technikai alapot biztosít az XML és webszolgáltatások nyújtásához, valamint a strukturált, illetve strukturálatlan adatok és a kategóriájukban páratlan üzleti információs és tudásmenedzselési képességek összekapcsolásához. Az SAP Security Resource Management testre szabott eszközeivel kiegészülő új technológia a vezeték nélküli alkalmazások, a szimuláció és a kapacitásmodellezés támogatásával gondoskodik a különféle hivatalok és szervezetek kritikus folyamatainak tökéletes integrálásáról. A biztonságos környezet megteremtése érdekében az SAP ágazatvezető technológiája megbízható hitelesítést, automatikus „single sign-on" belépést, szerepalapú jogosultságszerzést, központi felhasználó-kezelést, titkosított információcserét, PKI-támogatást, valamint digitális aláírással és biometriai azonosítással védett dokumentum-továbbítást kínál.

Symantec szűrő Dominóra

A *Symantec* bejelentette a *Symantec AntiVirus/Filtering for Dominót*, amely vírusok elleni védelmet, egyúttal szűrést is kínál a *Lotus Notes/Domino* adatbázisokon.

A Symantec AntiVirus/Filtering for Domino a Solaris-on, AIX-en, iSeries-en, Linuxon és Windows NT/2000-en futó Lotus/Domino adatbázisokat védi a rosszindulatú tartalomtól és az ártalmas programoktól.

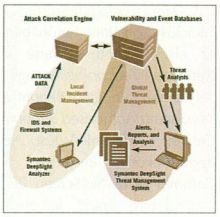
A termék már a *Lotus Notes/Domino 6.0*-t is támogatja, így a legfrissebb Notes-ra áttérő cégek megbízható védelméről is gondoskodik. Tovább javult a Symantec szabadalmaztatott *Dynamic Document Review*-ját használó, a nemkívánatos tartalmat szabályok alapján szűrő képesség.

Symantec riasztórendszer

A *Symantec* új riasztórendszerrel rukkolt ki: a *Symantec DeepSight Threat Management System 4.0* kellő időben ad átfogó, „madártávlati" áttekintést a cégeknek a világ internetes támadásairól. Gyors elemzései és ellenintézkedései védenek a rosszindulatú fenyegetések ellen. A termék a Symantec több mint 180 országban tevékenykedő 19 ezernél több partnerénél található tűzfalakról és behatolás-érzékelő rendszerekről (IDS) származó adatok alapján megjelenésüktől fogva nyomon követi a veszélyeket.

A DeepSight Threat Management System már órákkal gyors elterjedése előtt felfedezte a *Slammer* férget. A Symantec DeepSight Threat Management System ezt követően időben riasztott ahhoz, hogy a rendszergazdák az általa ajánlott eljárásokkal még azelőtt védekezhessenek, mielőtt a számítástechnikai környezetük veszélybe került volna.

A tűzfalak szolgáltatta adatoknak a 4.0 változatban megvalósított integrációja révén a Symantec DeepSight Threat Management System most már a korábban nem észlelt, széles



A DeepSight Threat Management System rendszerarchitektúrája

körben elterjedt támadásokat is érzékeli. Ezzel a fenyegető veszélyekről szóló korai riasztás a világon bárhol található jóformán valamennyi technikai platformon azokra a gyanús, azonosítatlan tevékenységekre is kiterjed, amelyek bizonyos portokat és eszközöket érintenek.

A Symantec elemzői a begyűjtött adatokból bonyolult eljárásokkal és adatbányászattal határozzák meg a támadást jellemző mintázatot. A sebezhető pontok és a támadások terén rendelkezésükre álló adatok elemzésével idejében tudnak széles körű riasztást küldeni az ügyfeleknek, hogy azok a támadás megelőzésére összpontosíthassanak.

Sikeres évet zárt a Noreg

Eredményes évet zárt a magyarországi információvédelmi piacon immár négy éve meghatározó szerepet betöltő *Noreg Információvédelmi Kft.* A *Montana Rt.* leányvállalata a 2002-es évet 370 millió forint árbevétellel zárta, ami az előző évhez képes 15%-os növekedést jelent. Míg 2001-ben a Noreg adózás előtti eredménye 12 millió forint volt, 2002-ben ez az összeg elérte a 35 millió forintot. A bevétel több mint 50%-a szolgáltatásból származó tevékenységekből tevődött össze.

A gazdasági, pénzügyi eredményeken kívül említésre méltó még, hogy a tavalyi év során a Noreg megszerezte az *ISO 9001/2000* minősítést, sikeresek a Noreg *ATC* tanfolyamok *(ISS Authorized Training Center)*, ezenkívül *Adatbiztonság Technológia és Jog* címmel rendezvénysorozatot indítottak. Az év során sikeresen zárult a Noreg több nagy projektje (Giro Rt. – PKI projekt, országgyűlési, valamint önkormányzati választások informatikai védelme, információvédelmi rendszerek kiépítése további hazai nagybankokban, vezető ipari vállalatoknál).

azaz small.

Egy kisvállalkozásnak sem nagy vállalkozás a számítógépes vírusvédelem megoldása.

azaz medium.

Középvállalat, nagy fejlesztések, merész célok. És a számítógépes vírusvédelemre gondolt már?

azaz large.

Egy nagyvállalat nem elégedhet meg félmegoldásokkal. Komplex számítógépes vírusvédelmi megoldások egy kézből.

azaz VirusBuster. Testreszabott megoldás minden méretben.

- **Teljes körű számítógépes vírusvédelem**
- Értéknövelt szolgáltatások
- Saját fejlesztésű programok, magyar nyelvű háttértámogatással
- Sybari Software piacvezető levelezésvédelmi megoldásainak forgalmazója

1116 Budapest, Vegyész u. 17-25.
Tel: (1) 382-7000 Fax: (1) 382-7007
www.virusbuster.hu
sales@virusbuster.hu

VirusBuster
www.virusbuster.hu

Azt kérik Öntől, hogy többet teljesítsen. Rövidebb idő alatt. A Microsoft® Windows® Server 2003 segítségével Ön ezeknek az egymással ellentmondó igényeknek is meg tud felelni. Hiszen kevesebb idő és pénz ráfordításával, zökkenőmentesebben használhat és készíthet hatékony informatikai megoldásokat.
További információk a www.microsoft.com/hun oldalon.

Microsoft® Windows Server 2003