Computer PANORÁMA

Computer Panoráma
XIII. évfolyam 13. különszám, 2002. október
Ára: 695 Ft

ADATBIZTONSÁG

Vírusvédelem felsőfokon

KÜLÖNSZÁM

CD-melléklettel

Hackereknek zárva
Tűzfalak mindenkinek

Kártyatrükkök
Bankkártyák és hamisítók

Hamis a baba
Elektronikus aláírás

Reszkessetek vírusok!
VirusBuster

Desktop biztonság
Windows XP & Office XP

Mobil biztonság
Java 2ME

Vírusok nagyító alatt
Antivírus tesztlabor

Plug and Protect
Symantec készülékek

Csak nyíltan, őszintén
Sun Liberty Alliance

A CD-lemezen:
Best Possible Privacy
Levéltitkosító (teljes verzió)
Tűzfalak
Antivírusok
Állománykódolók

Moduláris adatvédelem

Titkosított távközlés
Óriás titkosító kulcsok

Integrált biztonság

Szigorúan őrzött szerverközpont

Ismerkedjen meg az információvédelem újdonságaival!

02013
9 770865 524027

...azon rágódtam

megtettem-e mindent, hogy az adataim biztonságban legyenek?

Ma már

nyugodt vagyok, mert tudom, hogy a legsúlyosabb üzemzavar esetén is a nap bármely szakában elérhetem őket és segítenek a problémám megoldásában.

a magyar oktatás és állami szféra hivatalos beszállítója

22 platformon 7 keresőmotort kínálunk egy rendszerben,

közvetlen szakmai támogatást a gyártótól ***egy kézből***

VirusBuster
www.virusbuster.hu

1116 Budapest,
Vegyész utca 17-25.
Tel: 382-7000
Fax: 382-7007
mail@virusbuster.hu

ELMÉLET

TECHNOLÓGIA

SZOFTVER

HARDVER

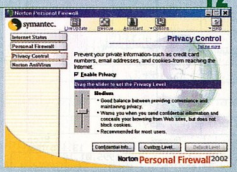
SZOLGÁLTATÁS

BANTECHNIKA

KÖRKÉP

MOBIL

TŰZFALAK 12



A világhálóra kapcsolódó számítógépünk szabad prédája a rosszindulatú behatolóknak, különösen ha naphosszat a neten lógunk. Szerencsére az úgynevezett tűzfalprogramokkal hatékonyan megvédhetjük adatainkat. Cikkünkben az otthoni felhasználóknak szánt tűzfalak közül mutatunk be néhányat.

BANKKÁRTYÁK 42

A hitelkártyák és a különböző mágnescsíkos kártyák, illetve chipkártyák pénzt helyettesítő eszközök, ezért hamisításukra épp olyan nagy a kísértés, ha ugyan nem nagyobb, mint a pénz esetében. A bankok Magyarországon is számolnak a kártyacsalás kockázatával, együttműködésük következtében azonban ez a kockázat még elviselhető.

IMPRESSZUM

ADATBIZTONSÁG
A Computer Panoráma különszáma
XIII. évfolyam 13. különszám, 2002. október

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.

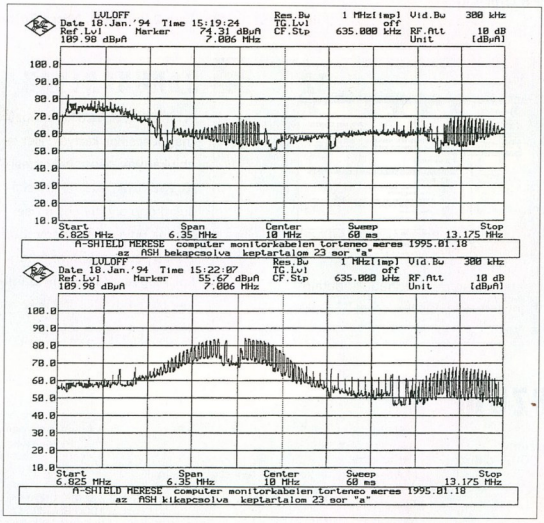
Az Adatbiztonság különszámot készítette:
Levilágítás: HVG Press Kft.
Nyomtatás: Szegedi Kossuth Nyomda Kft.
6723 Szeged, Makkosházi krt. 1.
Felelős vezető: Gera Imre ügyvezető igazgató

ISSN 0865-5243

Stratégiai titkok őrzése – költséghatékonyan

A legtöbben nem is sejtik, milyen furfangos módszerekkel próbálják egyesek megkaparintani a számítógépeken tárolt bizalmas adatokat. Az egyik ilyen eljárás a számítógépek „lehallgatása". Az árulkodó sugárzás megfékezésére eszelték ki a szakemberek az aktív lehallgatásvédelmet.

A számítógépek elektromágneses kisugárzásán alapuló lehallgatásról az első, szakfolyóiratban közölt elemzés *(Computers & Security 4/1985)* nem váltott ki pánikot az üzleti és a polgári életben annak ellenére, hogy a szerző, *Wim van Eck* kristálytisztán bemutatta, milyen egyszerűen és olcsó eszközökkel tulajdonítható el ily módon az információ. Akkoriban a számítógépek elterjedtsége, az információ közvetlen gazdasági ereje meg sem közelítette a mai szintet. A biztonságot a hozzáférés és a továbbítás során alkalmazott védelemmel általában megoldottnak tekintették. Ugyanakkor a katonai és stratégiai területeken már régóta a jelentőségének megfelelően kezelték az elektromágneses kisugárzás kockázatát és ennek hírszerzési alkalmasságát.



A monitorkábelen végzett mérések tanúsága szerint az aktív lehallgatásvédelem révén megfejthetetlenné válik a számítógép sugárzása

A közvéleményben – a COCOM-hagyományoknak megfelelően – erről a régóta stratégiai jelentőségű kérdésnek még a létezéséről sem alakult ki elképzelés, nem volt illendő beszélni róla. Így lehetett alacsony szinten tartani a lehallgatáshoz és a kivédéséhez szükséges eszközök és eljárások ismeretét. Ugyanezt segítette elő néhány tévhit intenzív terjesztése is – ami már más területeken is bevált. Ilyen tévhit volt például az, hogy a kisugárzott térből nagyon bonyolult feladat az adatokat rekonstruálni, ahhoz igen képzett személyzetre és nagyon fejlett érzékelő és dekódoló eszközökre van szükség. Az említett cikk ezeket a téveszméket már régen megcáfolta, és rávilágított a védelem lehetséges módszereire is.

Sugárzó adatok

Nézzük, mit tehetünk, helyesebben: mikor mit érdemes tennünk. Az első teendő az *önvizsgálat.* Milyen védelemre van szükségünk, mekkora kockázatot vállalhatunk? Vagyis van-e mérhető és nagy összegekben is kifejezhető veszélye annak, ha bizonyos adataink más kezébe „szivárognak"? Ha erre a kérdésre igen a válasz, akkor tovább léphetünk. Valóban teljes-e informatikai és távközlési rendszerünk védelme? Minden gazdaságilag, állami és üzleti szempontból stratégiailag fontos területen indokolt a kockázatok, valós veszélyek számbavétele.

Tegyük fel, hogy tökéletesen rejtjelezett formában tároljuk az adatainkat a számítógépben vagy valamilyen adathordozón, és ugyanígy küldjük el azokat publikus vagy bérelt távközlési csatornákon keresztül. De a képernyőn – legyen az hagyományos, LCD vagy plazma – csak a nyílt információval tudunk dolgozni. A kijelzőt meghajtó elektronika úgy működik, mint egy tévéadó: a képalkotáshoz szükséges jelek általában kiszivárognak, és elég erősek ahhoz, hogy jelentősebb távolságból felfogva is értékelhető információvá alakuljanak át. Mindehhez csak egy kissé módosított tévévevő, antenna és apró kiegészítő elektronika szükségeltetik.

Meg kell jegyeznünk itt, hogy természetesen készíthetők és készülnek is olyan számítógépek, amelyek nem bocsátanak

ki semmilyen mérhető, értékelhető sugárzást. Ezek azonban „zajos" társaiknál 8-15-ször drágábbak, és nem egykönnyen szerezhetők be.

Védett PC-k

A legnagyobb számban alkalmazott személyi számítógépek és laptopok eredeti konstrukciójukban igen kevéssé védettek a lehallgatás ellen. Ennek oka abban rejlik, hogy az eszközökön belül, alapműködésükből adódóan olyan frekvenciák használatosak, amelyek – vagy amelyek felharmonikusai – a rádiófrekvenciás tartományba esnek, ahol a jó terjedési viszonyoknak megfelelően a hagyományos vételtechnikával detektálhatók.

Igen cifra helyzet adódik, ha a modulációs tulajdonságokat is figyelembe vesszük. Az egyes hardverelemeket ugyanis nem rádiós eszközökbe szánták, így azután egyedi és eltéveszthetetlenül azonosítható eltéréseket mutat a kiszórt jelözön. A következmény az, hogy egy gépkupacból is minden további nélkül kiválasztható az érdekes tartalmú egyed, vagyis a lehallgatás – megfelelő eszközök birtokában – teljes mértékben szelektív lehet.

A jól ismert amerikai FCC szabályozás 15. szekciójában foglaltaknak megfelelő eszköz a kibocsátott szórt teljesítmény korlátozási feltételeinek tesz eleget, viszont a spektrum, ha gyengébben is, de jelen van. Úgy tekinthetjük ezt a feltételrendszert, mint egy egészségügyi szempontok alapján bevezetett környezetszennyezési korlátozást, amelynek azonban igen kevés köze van az informatikához.

Vegyük sorra, milyen forrásokból származnak gépünk rádiójelei. Az egyik legfontosabb ilyen forrás napjainkban a *hálózat*. Az *Etherneten* és más hálózati kábeleken továbbított jeleknek lehetnek rádiófrekvenciás tartományba eső felharmonikusai is. A *monitor* és annak vezérlése hasonlóan erős forrás. A gépen belül, az órafrekvencia növekedésével szintén megnő a lehallgatás szempontjából értékelhető jelek megjelenésének a veszélye. Ugyanígy a drótnélküli egér, illetve billentyűzet kommunikációja is lehallgatható. Az egér kábele, az elektromos és adathálózat (ha nem jól árnyékolt) továbbvezeti a gépben keletkező jeleket, kedvező feltételeket teremtve a jel vezetéken keresztüli kinyeréséhez, ha például „légi" úton nem menne a lehallgatás.

Aktív lehallgatásvédelem

Az érdekeltek néha nem túl gyorsan mozdulnak. Ilyen az ATM (azaz bankjegykiadó) automaták esete. Néhány évvel ezelőtt egy skandináv országban végzett felmérés szerint az ATM-ekben elhelyezett PC-k kétharmada rendesen sugárzott.

A védekezéshez háromféle – az alkalmazás teherbírásától és a kockázattól függő – módszer áll rendelkezésünkre.

A *TEMPEST* szobák fémötvözetű szendvicsszerkezetű falakból épített helységek, amelyek teljes mértékben védenek a lehallgatás és az elektromágneses lökéshullámmal való rombolás ellen is. A szobák az 1 MHz és 30 GHz közötti tartományban legalább 60 dB, többnyire 85-110 dB csillapítást jelentenek a szórt sugárzással szemben. Ergonómiailag nem kellemes bennük dolgozni, ráadásul a védelmi hatásuk nagyon könnyen lerombolható. Például elég egy szöget beverni a falba, és máris kiválóan sugárzó antennává változott a védett helyiség. Áruk miatt pedig csak különleges alkalmazásokban játszhatnak szerepet. Néhányszor 10 millió forint alatt nehezen úszható meg egy árnyékolt szoba megépítése.

A *sugárzásszegény* konstrukciójú gépek az átlagosnál 8-15-ször kerülnek többe. Alkalmazásuk elsősorban katonai területen kézenfekvő. „Tökéletes" védelem úgy érhető el velük, ha a sugárzásszegény konstrukciót a harmadik megoldással, az *aktív lehallgatásvédelemmel* kombinálják.

Az aktív lehallgatásvédelem szellemes és igazán költséghatékony megoldás. Egy detektor felfogja az adott PC által kibocsátott jeleket, azokat – a titkosításnál használt rejtjelezéshez hasonlóan – összekeverve fehér zajt bocsát ki, ezzel elfedi a jelek egy részét és csökkenti az azok rekonstruálásához szükséges vezérlőjelek kinyerésének lehetőségét. Antennaként az elektromos vezetéket használja, és igen kis kibocsátott teljesítménnyel dolgozik, amely nem befolyásolja a többi egység működését és az egészségügyi feltételeket is teljesíti.

A módszer hatékonyságát egy mérés eredményével szemléltetjük, amely a mérőszobában és a monitorkábelre csatlakoztatott igen érzékeny műszerrel történt. Ez a lehallgatás abszolút ideális esete: zavarmentes térben a szórt jelforrás közvetlen közelében érzékelve mérni. Látható, hogy a készülék bekapcsolásakor nincsenek értékelhető szikronjelek. Ennek a megoldásnak a legvonzóbb tulajdonsága a készülék ára, amely hozzávetőleg megegyezik egy jobb PC-ével. Nem véletlen, hogy a pénzügyi és üzleti életben egyre többen alkalmazzák az aktív lehallgatásvédelmet.

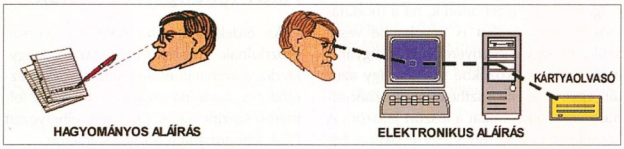
Hecks Ferenc
hecks@axelero.hu

Hamis a baba

Az elektronikus aláírásról szóló törvény jogi oldaláról közelíti meg említett problémakört, s minimális mértékben foglalkozik a biztonsági kérdésekkel. Sajnos a gyakorlatban számos olyan eszköz és eljárás létezik, amelyek súlyos biztonsági problémákat vetnek fel az elektronikus aláírás vonatkozásában.

Az elektronikus aláírási és hitelesítési folyamatot számos potenciális veszély fenyegeti. Cikkünkben a fő hangsúlyt a *használatra* helyezzük: megvizsgáljuk azoknak a hardver- és szoftverrendszereknek a biztonsági problémáit, amelyeket az elektronikus aláírás létrehozásában és ellenőrzésében használunk. Ugyanakkor *nem* foglalkozunk az olyan fenyegetésekkel, mint

- *a nyilvános kulcsú algoritmus okozta támadás:* megfelelően nagy számítási kapacitással a leggyakrabban használt *RSA* algoritmus is visszafejthető.
- *az ujjlenyomatot készítő Hash algoritmus okozta támadás:* megfelelően nagy számítási kapacitással olyan dokumentum generálható, amely létező ujjlenyomathoz tartozik.
- *az elektronikus aláírásról szóló törvény által megvalósított hitelesítési eljárás okozta támadás:* a törvény által megszabott eljárás garantálja, hogy a nyilvános kulcsú algoritmus titkos kulcsa valóban az aláírónak vélt személy birtokában van.



1. Papíralapú és elektronikus aláírás

Elektronikus vagy papíralapú aláírás

Az aláírás létrehozásakor két alapvető szempontot kell figyelembe venni: egyfelől az aláírónak pontosan tudnia kell, hogy mit ír alá, másfelől biztosnak kell lennie abban, hogy azt és csakis azt írja alá, amit szeretne. Nézzük, hogyan teljesülnek ezek a szempontok a papíralapú, illetve az elektronikus aláírás esetében.

Ha egy papír alapú szerződést szeretnénk ellátni az aláírásunkkal, pontosan tudjuk, hogy mit írunk alá. Csak el kell hinnünk a szemünknek, amit a papíron látunk. Ha viszont elektronikusan szeretnénk elhelyezni az aláírást a dokumentumon, akkor el kell hinnünk a szemünknek, hogy azt látjuk és értjük, ami a monitoron vagy nyomtatásban megjelenik. El kell hinnünk továbbá, hogy ami megjelent, annak pontosan az az értelme, amit a háttértár adott állományának bitsorozata jelképez. Végül el kell hinnünk, hogy az aláírás létrehozásával csak és kizárólag az általunk aláírni szándékozott állomány bitsorozatához képződik az aláírás. A szemének általában minden értelmes ember hisz, így a továbbiakban csak az utóbbi két problémával foglalkozunk.

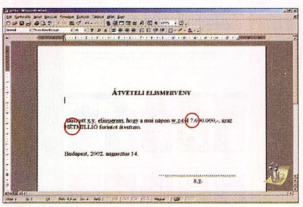
Az elektronikus aláírás folyamata

Az elektronikus aláírás létrehozása, illetve a létező elektronikus aláírás ellenőrzése/elfogadása a következő lépésekben történik:

1. Első lépésben a küldő eszközén előáll az aláírandó dokumentum.
2. Az aláírandó dokumentum bináris kódsorozatából elkészül a dokumentumra egyedileg jellemző ujjlenyomat. Ez az eljárás *Hash* algoritmusok segítségével valósítható meg, amelyek lényege az, hogy az ujjlenyomatból csak nagyon „nehezen" lehet előállítani az eredeti dokumentumot.
3. Az ujjlenyomatot valamely nyilvános kulcsú algoritmus kulcspárjának titkos részével titkosítjuk. Az így előálló kódsorozat a dokumentumhoz rendelt *digitális* vagy *elektronikus aláírás.*
4. A küldő ezt követően a dokumentumot és a hozzá rendelt digitális aláírást továbbítja.
5. A fogadó megkapja a dokumentumot és a digitális aláírást.
6. A dokumentumból ugyanazzal a Hash algoritmussal, amelyet a küldő is használ, előállítja a dokumentumhoz rendelt ujjlenyomatot.
7. Előállítja továbbá a digitális aláírásból a küldő nyilvános kulcsának felhasználásával a digitális aláíráshoz rendelt ujjlenyomatot.
8. Abban az esetben, ha a két ujjlenyomat megegyezik, a fogadó biztos lehet abban, hogy az elektronikus aláírás az ellenőrzéshez felhasznált nyilvános kulcs titkos párjával készült.

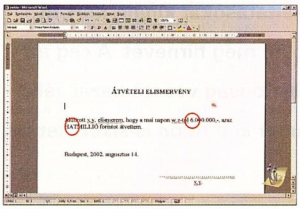
Bitsorozat megjelenítése

Alapvető elvárás a dokumentummal szemben, hogy az minden olyan információt tartalmazzon, amely a dokumentum értelmezéséhez, illetve megjelenítéséhez



2. Eredeti dokumentum

szükséges. Ha ugyanis bármilyen máshonnan vett információ is szükséges az értelmezéshez, befolyásolni lehet a dokumentum megjelenített képét. Tipikusan ilyen információ a karakterek képe. A dokumentum (készüljön az *Worddel* vagy *StarOffice*-szal) nem tartalmazza azokat a betűtípusokat, amelyek ahhoz szükségesek, hogy a dokumentum képét megjelenítsük. Így a betűtípusok változtatásával el-



3. A betűtípus módosítását követően megjelenített dokumentum

érhető, hogy ugyanannak a dokumentumnak a megjelenített képe más és más legyen. Sajnos ugyanez a helyzet az *ASCII* szövegállományokkal is. Jóllehet itt nincsenek betűtípusok, de a megjelenítéshez ismernünk kell a karakterek képét. Ez pedig a dokumentumon (a szöveg bitsorozatán) kívüli információ, amelyet az ASCII szabvány rögzít. Ahhoz tehát, hogy biztosítsuk a dokumentum és a megjelenített kép közti egyértelműséget elengedhetetlen, hogy *a dokumentum magában foglalja a karakterek bináris képét.*

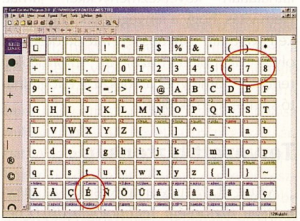
Felvetődik itt a kérdés, hogy milyen lehetőségei vannak egy támadónak, hogy kiaknázza ezt a biztonsági hézagot. Megteheti például, hogy egy kisalkalmazással felcseréli a betűk képét valamely betűtípusban. Számos letölthető freeware program létezik erre a célra az interneten. A betűk felcserélését elérheti egy saját készítésű kis programmal is. Ezt a kis programot akár bejuttathatja egy e-mail elküldésével is.

Megállapíthatjuk tehát, hogy a rosszindulatú támadó könnyedén megteheti azt (különösen akkor, ha a partnere nem ért az informatikai biztonsághoz), hogy a partner számítógépébe bejuttat valamilyen programot, amelyik azután gondoskodik arról, hogy az aláíró ne azt lássa a képernyőn, amit aláír. Megteheti azt is, hogy az aláírást követően (adott időpontban) teljesen kiirtja magát a laikus számítógépéről. Ezt követően a laikus felhasználó hiába próbálná bizonyítani az igazát, az elektronikus aláírás a törvény szerint a bíróság előtt bizonyító erejű.

Bitsorozat aláírása

Amennyiben pontosan tudjuk, hogy mit szeretnénk aláírni (vagy legalábbis elhisszük azt), elláthatjuk a dokumentumot elektronikus aláírásunkkal. Ahhoz, hogy ezt megtegyük, *aláírás-létrehozó eszközre* van szükségünk. Az aláírás-létrehozó eszköz mindenképpen tartalmaz szoftverelemeket, és tartalmazhat hardverelemeket is. Az eszköz arról gondoskodik, hogy minden szükséges feltétel meglegyen a gépben, ha úgy döntünk, hogy aláírunk egy dokumentumot. Manuálisan nem tudjuk ellenőrizni, hogy valóban azt a bizonyos bitsorozatot látjuk-e el aláírással, amelyet szeretnénk, és abban sem lehetünk bizonyosak, hogy más bitsorozathoz nem készül-e aláírás.

Tipikus támadási módszer a következő: a számítógépbe bejuttatott kis program figyel egy olyan interaktív tevékenységet, amelyet a felhasználónak kell megtennie azután, hogy az aláíráshoz szükséges valamennyi feltételt teljesítette (például behelyezte a chipkártyáját az olvasóba). Az esemény hatására érzékeli, hogy a felhasználói program milyen információkat küld aláírásra például a kártyaolvasónak. Ezt elküldi az olvasónak és megvárja a választ, de nem továbbítja a felhasználói programnak, hanem miután megkapta, elküld egy másik bitsorozatot az olvasónak aláírásra. Ha ez megtörtént, csak azután küldi vissza az elsőként megkapott aláírt választ a felhasználói programnak. Az egész természetesen olyan gyorsan történhet, hogy a felhasználó semmit sem vesz észre. Sőt! Még azt is megteheti a „bűnös kis program", hogy az e-mail vírusok többségéhez hasonlóan a saját SMTP rutinjával visszaküldi az aláírt bitsorozatot a támadónak. Így a



4. Eredeti betűtípus

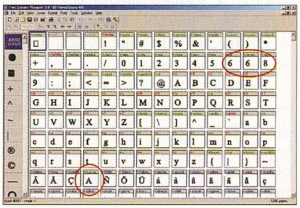
Egy dokumentum – két megjelenítés

A példa kedvéért egy dokumentumot készítettünk, majd írásvédett flopilemezre írtuk (2. ábra). Az eredeti betűtípust (4. ábra) egy kicsit módosítottuk: a „6"-os karakter képét a „7"-es karakter képére, míg az „A" karakter képét az „É" karakter képére másoltuk néhány kattintással (5. ábra). Ezt követően ismét megnyitottuk az írásvédett flopilemezre mentett dokumentumot (3. ábra). A megjelenített dokumentum már az új betűkkel jelent meg a képernyőn.

támadó akár távolról is képes arra, hogy a célpont felhasználóval aláírattassa az általa elkészített dokumentum ujjlenyomatát.

Konklúzió

Az elmondottakból kitűnik, hogy ha az aláírás-létrehozó eszköz egy más célra is használt PC, akkor ez hatalmas biztonsági kockázatot jelent. Semmi gondot nem jelent, ha egy zárt rendszerben célgépek csak meghatározott feladatot látnak el



5. Módosított betűtípus

(ilyenek például a bankautomaták). A fokozott biztonságú elektronikus aláírás a törvényi definíció alapján olyan elektronikus aláírás, amely többek között megfelel annak a kritériumnak, hogy „olyan eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll". Sajnos nehezen képzelhető el, hogy a mai PC-s operációs rendszerek – ideértve a *Linuxot* is – kizárólag az aláíró befolyása alatt állnának. Számos példát szolgáltatnak erre az operációs rendszerek biztonsági problémái, amelyeket az elmúlt másfél évtized vírusai ki is használtak.

Dr. Leitold Ferenc
Veszprog Kft.
fleitold@veszprog.hu

Moduláris adatvédelem

Az informatikai biztonsági szolgáltatásokat kínáló Kürt Rt. bravúros adatmentéseivel alapozta meg hírnevét. A cég az eltelt időszakban az információbiztonság vezető hazai vállalatává nőtte ki magát, amely immár külföldön is sikereket ért el egyedülálló megoldásaival.

A felhasználó rémálma: nem olvasható a merevlemez, odaveszett egy egész havi munka, mert a mai megbízható meghajtók korában nem gondoltunk tartalékmásolat-készítésre. Megfogadjuk, hogy ezentúl ötpercenként mentünk, csak történjen valami csoda. Aztán verejtékben úszva felébredünk, gyorsan bekapcsoljuk a számítógépünket, és megnyugvással tapasztaljuk, hogy ezúttal megúsztuk, mindez csupán egy rossz álom volt.

Sajnos azonban sokan vannak, akik nem csak álmukban csöppenek ilyen helyzetbe; velük próbál meg csodát tenni a *Kürt Rt.* (**www.kurt.hu**) csapata, amely 1989 óta foglalkozik adatmentéssel.

Bízzuk szakemberre

Miután bekövetkezett a baj, még tovább ronthatunk a helyzeten, ha megfelelő ismeretek hiányában magunk kíséreljük meg kijavítani a hibát, például egy sokat ígérő shareware programmal. Mivel az adatvesztésnek igen sokféle oka lehet, általános ellenszer nincsen, a leginkább eredményre vezető gyógymódot pedig csak szakember tudja megállapítani. A Kürtnél másolatot készítenek az adathordozóról, a mentési munkálatokat azon végzik, így további adatvesztést nem okozhatnak, mert bármikor vissza tudnak térni az alaphelyzethez.

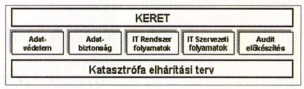
Mielőtt hozzálátnának az adatmentéshez, állapotfelmérést végeznek a hozzájuk eljuttatott adathordozón. Ennek során megállapítják, hogy van-e remény az adatok visszanyerésére, és a módszereikkel meg tudják-e valósítani azt. Az állapotfelmérés nagytisztaságú laboratóriumban történik, a legnagyobb körültekintés mellett, annak érdekében, hogy további károsodás ne történhessen.

Amennyiben lehetséges az adatmentés, és a felhasználó megrendeli azt, másolatot készítenek az adathordozóról. Erről nyerik vissza az adatállományokat, amelyeket azután egy másik adathordozón, többnyire CD-n juttatják el a megrendelőnek. Mi tagadás, megkérik az árát e nem mindennapi szolgáltatásnak, de hát ahogy mondani szokták, valamit valamiért. A szakvélemény ára például egy 8 gigabájtos merevlemez esetében, 3 napos határidővel 30 ezer forint, 24 órás határidőnél a sürgősségi felár 50 százalék (áfa nélküli árak). Egy hajlékonylemez vizsgálatáért 3 ezer forintot kérnek. Az adatmentés költségét a probléma súlyossága, az adathordozó kapacitása és a mentés sürgőssége határozza meg, az átlagár 260 ezer forint körül van. Nagy kapacitású eszköz, nem merevlemezes tároló vagy különösen bonyolult probléma esetén az ár ettől jelentős mértékben eltérhet – többnyire felfelé. Adatmentés megrendelésekor az előzetes vizsgálat árát beszámítják.

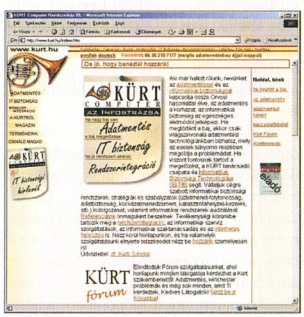
De nem csupán egy tárolóeszköz vagy más szoftver-, illetve hardverelem hibája okozhat hatalmas károkat egy informatikai rendszerben. Manapság, amikor a mindennapi életet behálózza az informatika, és az egész világ egy gigantikus méretű számítógép-hálózatra csatlakozik, sokféle veszélynek vannak kitéve adataink. Egy vírus vagy egy illetéktelen behatolás teljesen megbéníthatja a nagymértékben az informatikai rendszerükre utalt vállalatok és kormányhivatalok életét. És ott vannak a mára hatalmasra duzzadt adatbázisok: a bennük tárolt információk illetéktelen kezekbe kerülése vagy megsemmisülése beláthatatlan következményekkel járhat. Nem vitás, hogy a fenyegetések ellen tenni kell valamit: biztonsági intézkedésekkel olyan állapotba hozni az informatikai rendszert, amelynél a kockázat elfogadható szintre mérséklődik.

Tervezett biztonság

A Kürt Rt. válasza a kihívásokra az *Informatikai Biztonsági Technológia (IBiT)* nevű, moduláris felépítésű adatvédelmi rendszer. Ez a kockázatelemzést tartalmazó megoldáscsomag adatvédelmi és adatbiztonsági szempontból, dokumentált módon szabályozza a vállalat teljes informatikai tevékenységét. Szabályzatrendszerének kidolgozásánál figyelembe vették az általánosan elfogadott nemzetközi szabványokat. Az IBiT rögzíti a felső vezetés elkötelezettségét, tisztázza a felelősségi köröket, minimalizálja az emberi mulasztásból eredő károkat, és biztosítja a munkatársak folyamatos képzését. Bevezetése csökkenti a



Az Informatikai Biztonsági Technológia elméleti felépítése. Forrás: Kürt Rt.



A Kürt neve régóta összeforrt az információbiztonsággal

karbantartások költségét, a rendszerkiesések számát és idejét, továbbá javítja a rendelkezésre állási időt.

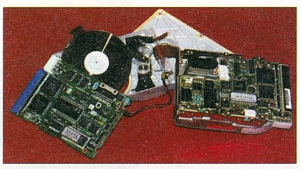
Az IBit felépítését a mellékelt ábrán láthatjuk. Az adatvédelmi modulok között találjuk az adatintegritást biztosító megoldásokat, a mentési rendszert és a vírusellenes védelmet. Az információkhoz való illetéktelen hozzáférést akadályozzák meg az adatbiztonsági modulok. Ide tartoznak a fizikai biztonságtechnikai megoldások, a titkosítási funkciók, a behatolást megakadályozó szolgáltatások és a rendszerhez való hozzáférést szabályozó megoldások. Az *IT rendszer folyamatok* és az *IT szervezeti folyamatok* csoportba sorolt modulok nem tartoznak a biztonsági szolgáltatások közé, ha telepítésre kerülnek, ezek biztosítják a teljes informatikai rendszer átfogó szabályozását.

Az *Audit előkészítés* moduljai teszik lehetővé a független informatikai auditok elkészítését. A kockázatelemzés során meghatározzák azt a biztonsági szintet, amely alatt érdemes megszüntetni a kockázatokat. A biztonsági szint feletti kockázatok bekövetkezését nevezzük *katasztrófának*, ennek a szabályozott kezelését biztosítja a *katasztrófa elhárítási terv*, amely minimalizálja a károkat és csökkenti a helyreállítás idejét. A keret az IBit moduljainak működéséhez szükséges váz, amely attól függően változik, hogy milyen funkciókat rendelnek meg.

Az IBit-hez *dokumentumrendszer* készül, amely iránymutatást ad a megrendelő cég informatikai rendszerének és informatikai szervezetének továbbfejlesztéséhez és szabályozásához. A dokumentumrendszer felülvizsgálatát meghatározott időközönként külső szakértő bevonásával kell elvégezni.

Veszélytelen próba

Komoly segítséget nyújt a rendszergazdáknak a Kürt Rt. *szimulátora*, amelyben kockázatmentesen tesztelhetik cégük informatikai rendszerét. Megvizsgálhatják például, hogy megfelelően működik-e a vírusellenes védelmük, mennyire ellenálló a hálózatuk a külső támadásokkal szemben, vagy új szoftverek üzembe állítása milyen nem várt következményekkel járhat. A szimulátorban tetszőleges PC-alapú hálózati környezet állítható össze és tesztelhető úgy, hogy nem kerülnek veszélybe az eredeti rendszerben található erőforrások, információk.



A merevlemez szétszerelését érdemes gyakorlott szakemberekre bízni

Néhány szó a kockázatelemzésről

Hazánkban is egyre nő a cégek és szervezetek informatikai függősége, ami előtérbe helyezi a biztonságos informatikai rendszerek megteremtésének a kérdését. Ennek egyik legfontosabb területe az *informatikai kockázatelemzés*. A kockázati tényezők teljes kiküszöbölése drága, és a tényezők sokrétűsége miatt nem mindig lehetséges. Olyan megoldásra van tehát szükség, amely a kockázati tényezők azonosításával, hatásuk felmérésével adja meg az elfogadható költségű megoldást. A különböző szervezeteknek saját biztonságuk érdekében tisztában kell lenniük informatikai rendszereik gyenge pontjaival, kockázataival, valamint azzal, hogy miként és milyen biztonsági intézkedésekkel tudják mérsékelni ezeket.

A kockázat annak a veszélye, hogy egy esemény vagy intézkedés hátrányosan befolyásolja a szervezet lehetőségeit üzleti céljainak és stratégiáinak megvalósítása során. A kockázatkezelés célja olyan optimális kockázatkezelési szint meghatározása, mely szinten a felmért és kezelt kockázati tényezők az üzleti folyamatokat csak az előre meghatározott mértékben befolyásolják.

Informatikai kockázatkezelésről akkor beszélhetünk, ha egy cég tudatos erőfeszítéseket tesz az informatikai rendszerét, infrastruktúráját és az ezt üzemeltető szervezetet fenyegető kockázatok rendszeres azonosítására és értékelésére, valamint az ehhez kapcsolódó kockázatcsökkentő intézkedések kidolgozására és megvalósítására.

A megvalósítás módja és mélysége szerint két kockázatelemzési módszer – a *kvalitatív* (minőségi) és a *kvantitatív* (mennyiségi) – ismeretes. A kvalitatív technika nem valószínűségeket, biztonsági mérőszámokat ad, hanem kockázati szinteket állapít meg, és ezzel viszonylag durva mérést tesz lehetővé. A kvantitatív elemzés lényegesen finomabb felbontású, számszerűsíti a kockázati valószínűségeket, és az észlelt adatokat a modellezési technikák alkalmazásával statisztikailag elemzi.

A megvalósítandó védelmi intézkedések meghatározásához, rangsorolásához és ütemezéséhez részletes és számszerűsített kiindulási információkra van szükség. Ezek az információk jelentik az alapját a *költséghatékonyság-elemzéseknek*, amelyek segítségével a felső vezetés számára indokolható egy-egy tervezett informatikai biztonsági beruházás vagy fejlesztés szükségessége. A sokkal használhatóbb eredményt adó kvantitatív elemzés bonyolultabb, több időt és ráfordítást igényel. A döntéshozóknak azonban minden olyan esetben, amikor ez lehetséges, a kvantitatív kockázatelemzés megvalósítására kell törekedniük, még akkor is, ha a rövid távú gazdaságossági szempontok ennek az ellenkezőjét sugallják. Míg Nyugat-Európában és Észak-Amerikában fokozatosan előtérbe kerül a kvantitatív módszer, addig Magyarországon még a kvalitatív elemzés az elterjedtebb. Hazánkban még nagyon kevés az olyan, megfelelő szakértelemmel felvértezett szakértő, aki képes eredményesen végrehajtani egy kvantitatív elemzést. Ez pedig oda vezethet, hogy a sikertelen próbálkozásokból tévesen arra következtetnek a döntéshozók, hogy a kvantitatív módszernek nincs értelme és nem is valósítható meg.

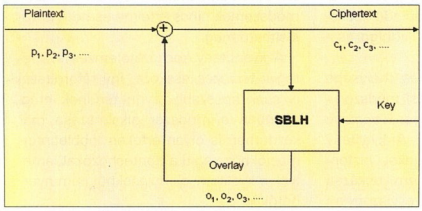
A kvantitatív kockázatelemzés a stratégiai tervezés eszköze, így ráfordításai is csak hosszabb távon térülnek meg. Azonban e módszer alkalmazása már kezdetben is olyan értékes többletinformációkhoz segíti a döntéshozókat, amelyek a kvalitatív elemzésekből nem nyerhetők ki.

A Kürt Rt. egyébként eddigi legnagyobb volumenű adatmentési esetét oldotta meg nemrég, amikor egy több mint *1 terabájt* (1000 gigabájt) összkapacitású német RAID rendszer adatait állította helyre. Ekkora tárolóeszköz hozzávetőleg 500 millió A4-es oldalnyi szöveget képes tárolni, s ha a lapokat egymásra tennénk, a Mount Everestnél háromszor magasabb papírtornyot kapnánk. Ekkora hely 5 és fél millió digitális fotó tárolására is elegendő. **M.Cs.**

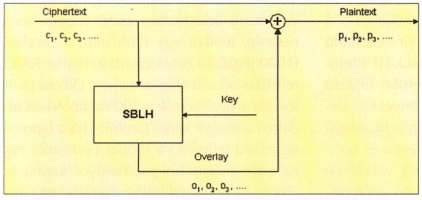
Óriás titkosító kulcsok

A távközlés titkosítására különleges eszközöket fejlesztettek ki az idők folyamán. A svéd Business Security cég az úgynevezett óriás rejtjelező kulcsokkal oldja meg az adatok titkosítását. Alábbi cikkünkben a cég termékei közül mutatunk be néhányat.

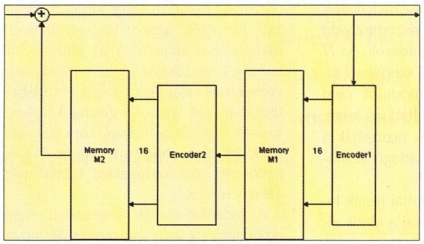
A távközlés titkosításában különleges szerepet töltenek be az *óriás rejtjelező kulcsokkal* dolgozó hardvereszközök, amelyek alkalmazásával jelentősen csökkenthető a kulcsmenedzsment költség- és komplexitásigénye. Írásunkban az egyik ilyen, itthon is széles körben ismert és elterjedt megoldást – a svéd *Business Security AB* portfoliójának főbb elemeit – mutatjuk be. A szabotázs-védett konstrukciójú család tagjai valamennyien a gyártó cég saját, szabadalmazott, *SBLH* algoritmus- és kulcskezelő rendszerén alapulnak. Az algoritmus konkrét megvalósítása történhet a vevő óhaja szerint, amint ez például nem ritka a katonai célú exportnál. A Business Security termékei a mai



1. Az SBLH kódolás sémája



2. Az SBLH dekódoló sémája



3. Az SBLH algoritmus felépítése

kor technológiai színvonalán és a távközlés új eljárásaihoz illeszkedve, a hagyományosan kiváló svéd ergonómiával valósítják meg az információvédelmet.

SBLH algoritmus

Az SBLH algoritmus úgy definiálható, mint egy szimmetrikus, bitfolyamos algoritmus, amely a titkosított információ *visszacsatolásával* dolgozik, a titkosított blokk hossza egy bit. A visszacsatolás biztosítja az önszinkronizálási képességet, az egy bites csomaghossz pedig azt, hogy gyakorlatilag nincs olyan távközlési technológia, amelynek a sebessége kezelhetetlen lenne az SBLH algoritmus számára.

Az *1. ábrán* a kódoló, a *2. ábrán* pedig a dekódoló folyamat sémája szemlélteti, hogy az alapot az *XOR* függvény adja. Az SBLH struktúrája teljesen egyedi, egyszerű és mégis erőteljes. A *3. ábrán* látható, két memóriatömböt és két dekódert tartalmazó blokkvázlat igen sok algoritmusnál alkalmazható a minél nagyobb hatékonyság elérésére.

A kulcsméret, a hibaterjedés és az önszinkronizáció létrejötte – utóbbi csak a visszacsatolást alkalmazó eljárások sajátja – a dekóderek *mélységével* (méretével) befolyásolható. Ez is jól mutatja a cégnek azt a korai felismerését, hogy nem a távközlést kell a titkosítási eljáráshoz igazítani, hanem a távközlési szabványoknak mindenben eleget tevő megoldást kell alkalmazni a védelemre.

A jelenlegi megoldások 256 bites valódi véletlenszám kulcsból indulnak ki, amelyet a szintén hardverben megvalósított expanziós algoritmus tölt M1 és M2-be. Az így előállított aktív kulcs a jelenlegi megoldásoknál hozzávetőleg 131 ezer bit. Az expanzió egyedi tulajdonságot ad az SBLH algoritmusnak: *a kulcshossz független az algoritmustól.* A teljes struktúra pedig szinte kínálja magát a nagy integráltsági fokú félvezető integrált áramköri megoldásra. A kiinduló 256 bites kulcs sokadmagával könnyen tárolható SmartCardon, ami néhány esetben, például a fax-, a hang- és néhány adatátviteli titkosító vagy azok egyes üzemmódjai esetében a végpontot kezelő személyhez is rendelheti a biztonságot.

A kulcsmenedzsment SmartCardos megoldásával *a készülékek előre programozott kivitelben is telepíthetők.* Ilyenkor a biz-

4.

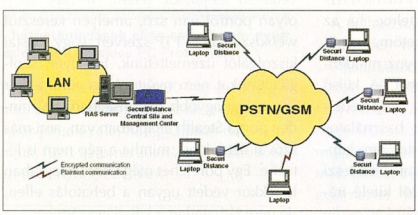
tonsági referens központi helyen őrzi a kulcsokat. Amikor a távközlési rendszer felkínálja a hálózati kulcsmenedzsment lehetőségét, mint például az ISDN esetében, akkor is van lehetőség közvetlen programozásra egy számítógép segítségével (a központi helyen). Mivel ebben az esetben nem haladnak kulcsinformációk a kommunikációs csatornán, ez utóbbi jelenti a teljes biztonság magasabb szintjét. Az algoritmusból következik az is, hogy nincs olyan alkalmazás, amelyet sebességi igénye miatt nem lehet titkosítani vele, mivel a memóriaszerkezetek a mindenkori digitális félvezető-technológiák leggyorsabb részei. (Arról persze lehet szó, hogy a költségek miatt nem érdemes megcsinálni.)

Az SBLH algoritmus erős. A rá épülő készülékek úgy válnak egyenszilárdságú biztonságot célzó megoldássá, hogy integrálják a fizikai és az elektromágneses támadás elleni védelmet magában az eszközben és a kulcselosztás területén is.

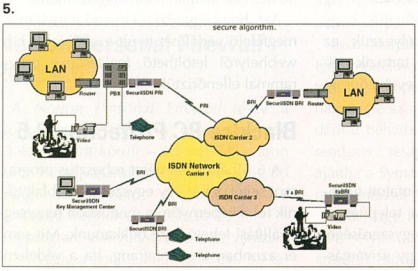
Az elmondottak után kézenfekvő, hogy egyedi, a vevő igényének, algoritmusának stb. megfelelő úgynevezett *custom* (azaz testreszabott) változat is szállítható. A következőkben néhány eszközt mutatunk be röviden.

SecuriDistance

A hordozható PC-k kétféle védelmet igényelnek, hogy sem a bennük tárolt információhoz, sem a távközlési csatornán elküldötthöz illetéktelenül ne férhessen hozzá senki. Erről gondoskodik a *SecuriDistance*. Az eszköznek két felhasználási területe van: két partner, illetve több személy és cégük/intézményük hálózata közötti kommunikáció. Az előbbi nem kíván magyarázatot, utóbbira példa a rendszergazda távoli beavatkozása (védetten) az általa felügyelt hálózatba, vagy az utazó diplomaták, üzletemberek kommunikációja cégük központi (mail) szerverével. Az eszköz bármilyen tárcsázós kapcsolatnál alkalmazható, így a GSM, az analóg és az ISDN vonalak esetében is. A személyhez kötött kódkulcsot ebben az esetben SmartCard tárolja (kép és alkalmazás: *4.* és *5. ábra).*

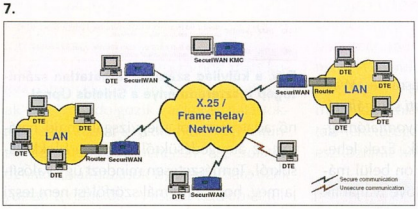


5.



6.

7.



8.

SecuriISDN

Az eszközkínálat lefedi a teljes ISDN palettát, az irodaházak közötti nagy sávszélességű vagy csatornaszámú védett kapcsolattól a videokonferencián át az asztali készülékpáron zajló beszélgetések egyedi védelméig. Biztonsági szempontból lényeges tudnivaló, hogy a készülékek egyedileg és helyileg, PC-vel és a hálózatra csatlakozó *Kulcs Menedzsment Központ* segítségével távolról is irányíthatók. A SecuriISDN valamennyi ISDN rendszerrel kompatibilis (kép és alkalmazás: *6.* és *7. ábra).*

SecuriWAN

A helyi hálózatok nyilvános vagy bérelt vonali összekapcsolása esetén védi az átviendő információt. Az eszközök *2 Mbps* sebességig dolgoznak, és X.25, valamint Frame Relay protokollok szerinti interfésszel látták el őket. Helyi vagy távoli kulcselosztás itt is lehetséges. Mint ismeretes, az előbb említett protokollok az internetes világ térhódításával elveszítették amúgy is gyenge védelmüket, mivel mióta kifejlesztették az illesztőszoftvereket, a világhálóról is meg lehet szólítani a végpontokat. Ez indokolja, hogy érdemi védelmet léptessünk életbe (kép és alkalmazás: *8. és 9. ábra).*

A teljesség kedvéért megemlítjük még a cég korábbról ismert eszközeit is, amelyek a világ sok országában, így itthon is állami, katonai és vállalati referenciák sokaságát vonultatják fel. A *SecuriFax* fax-titkosítók, a *SecuriVoice* hang-titkosító intelligens megoldása és az adatátvitel *SecuriCrypto V.24A, V.24S, V35/36, X.21, X.28, X.25, G703/704* protokollú, úgynevezett fekete dobozos védelmének eszközei SmartCardos kulcselosztással dolgoznak.

9.

Mindhárom eszközcsalád a SBLH algoritmus használatával kínál hatékony titkosítást.

Hecks Ferenc
hecks@axelero.hu

Tűzfalak mindenkinek

A világhálóra kapcsolódó számítógépünk szabad prédája a rosszindulatú behatolóknak, különösen ha naphosszat lógunk a neten. Szerencsére az úgynevezett tűzfalprogramokkal hatékonyan megvédhetjük adatainkat. Cikkünkben az otthoni felhasználóknak szánt tűzfalak közül mutatunk be néhányat.

Az esélyt a behatolásra *a Windowsba épített hálózati szolgáltatások, az állomány- és nyomtatómegosztás biztonsági lyukai* adják. Ezek lehetővé teszik, hogy egy hálózaton belül mások számára is hozzáférhetővé váljanak erőforrásaink. Amikor azonban az internetre kapcsolódunk, olyanok is bekukkanthatnak merevlemezünk tartalmába, akiknek ezt semmi szín alatt nem óhajtjuk megengedni.

Szkennelőprogramokkal mihaszna emberek állandóan vizslatják a netet olyan számítógépek után kutatva, amelyek nem alkalmaznak védelmet a behatolással szemben. Akik már telepítettek tűzfalat, tapasztalhatták, hogy szörfölés közben milyen sokszor éri támadás gépüket, a program ugyanis minden kísérletet jelez. Minél több időt töltünk a neten, annál nagyobb a valószínűsége, hogy ránk találnak, és ha nem védjük magunkat egy tűzfallal, nem is fogjuk soha megtudni, hogy valaki kutakodott a gépünkön.

Persze nem csupán kívülről fenyegeti veszély a gépünket: egy trójai program vagy valami más rosszindulatú alkalmazás megkérdezésünk nélkül szolgáltathat információkat megbízója számára. A jó tűzfal ezt is megakadályozza.

Hogyan működik?

A tűzfal beépül a számítógép és az internet közé, teljesen elszigetelve őket egymástól. Minden egyes bejövő és kimenő adatcsomagot megvizsgál, majd határoz az átengedésükről, illetve a blokkolásukról. Természetesen mindezt úgy valósítja meg, hogy a normál szörfölést nem teszi lehetetlenné folytonos akadékoskodással, a jogosulatlan behatolásra ugyanakkor mindig figyelmeztet. Arra is kapható, hogy meghatározott IP-címekről teljesen blokkolja az adatforgalmat, illetve csak egy adott webkiszolgálóval engedélyezze a kapcsolat létesítését.

Port	Service	Status	Security Implications
21	FTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
110	POP3	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
113	IDENT	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
135	RPC	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
139	Net BIOS	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
143	IMAP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
443	HTTPS	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

Egy, a külvilág számára láthatatlan számítógép teszteredménye a Shields Upnál

Magától értetődően bármely tűzfal használatának csak akkor van értelme, ha az minden biztonsági lyukat betöm, vagyis mindkét irányban megakadályoz mindenféle jogosulatlan adatforgalmat. A külső behatolásokkal szemben úgy nyújt védelmet, hogy a kapcsolódásra használatos portokat – és így magát az internetre kapcsolt számítógépet is – láthatatlanná teszi a külvilág számára. A belülről kifelé irányuló adatátviteli próbálkozásokat pedig jelzi számunkra, és mi eldönthetjük, hogy mely programoknak engedélyezzük az adatforgalmazást (ezek közé tartozik például a webböngészőnk és a levelezőprogramunk).

Vizsgálati módszer

Az összeállításunkban bemutatott tűzfalak esetében nem csupán a telepítés, a konfigurálás és a használat egyszerűségét vizsgáltuk, hanem azt is, hogy szivárgásmentes védelmet nyújtanak-e. Ehhez a *Shields Up* nevű webhelyet (**www.grc.com**) vettük igénybe, amely biztonsági szempontból átfogóan teszteli gépünket. Még a tűzfal telepítése előtt érdemes ide ellátogatni, hogy lássuk, milyen nyitott behatolási lehetőségeket kínál gépünk. A Shields Up *Test My Shields* gombjára kattintva először is kiderül, hogy sikerül-e kapcsolatba lépni a számítógépünkkel. Amennyiben a *Your Internet port 139 does not appear to exist!* és az *Unable to connect with NetBIOS to your computer* válaszokat kapjuk, nincs okunk az aggodalomra.

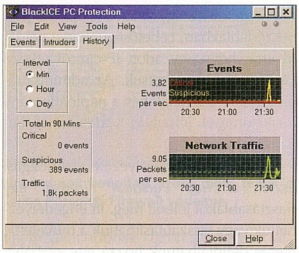
Ezek után a *Probe My Ports* gombbal vizsgáljuk meg az internetre való kapcsolódáshoz használatos portok állapotát. Válaszként egy lista tűnik fel a képernyőn, a *Status* oszlopban olvashatjuk a vizsgálat eredményét. Ha egy port mellett a *Stealth* szó áll, a port nem észlelhető a külvilág számára, vagyis itt nem lehet betörni a rendszerbe. Az *Open* állapotban lévő port védtelen bejáratot jelent, hacsak nem olyan portról van szó, amelyen keresztül webkiszolgálót, FTP-szervert vagy postai kiszolgálót üzemeltetünk. Ha ilyen szolgáltatásokat nem nyújtunk, gépünk akkor van a legnagyobb biztonságban, ha minden portja Stealth állapotban van, ami más szóval azt jelenti, mintha a gép nem is létezne. Egy port lehet még *Close* állapotban is, ekkor védett ugyan a behatolás ellen, de nem láthatatlan a külvilág számára.

Azt, hogy egy tűzfal kimenő irányban is megfelelő védelmet nyújt-e, a Shields Up webhelyről letölthető *leaktest.exe* programmal ellenőriztük.

BlackIce PC Protection 3.5

A 6 Mbájtos fájlméret robusztus programot sejtet, s bár egy egyszerű kis ablak tűnik fel a képernyőn, a menükben rengeteg beállítási lehetőségre bukkanunk. Mit sem ér azonban a sok cafrang, ha a védelem

komoly hiányosságokat mutat. Négy biztonsági szint közül választhatunk, de a tesztelés során még a legmagasabb szint beállításával sem tudtuk elérni, hogy gépünk teljesen láthatatlan legyen a külvilág számára. Telepítéskor a *BlackIce* alkalmazásvédelem címén összegyűjti a merevlemezünkön található valamennyi programállományt, aminek az eredménye egy kilométeres lista. A listán szereplő programoknál egyenként kell megtiltani, hogy kapcsolatba lépjenek az internettel. Ha ezt nem tesszük meg, a telepítéskor már a gépünkön lévő valamennyi program háborítatlanul küldözgethet adatokat a külvilág felé. Így természetesen a kimenő oldali védelem tesztelésére használt leaktest.exe gond nélkül áthatolt a tűzfalon. A súgó tanulmányozásakor kiderült, hogy a BlackIce külön utasítás hiányában csupán a telepítése után rendszerbe kerülő vagy megváltozó programokat blokkolja. Amikor azonban ilyennel próbálkoztunk, a védelem akkor sem működött.



A hátbatámadások ellen sajnos nem nyújt védelmet a BlackIce PC Protection

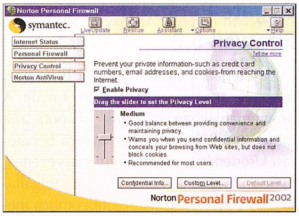
A letölthető program 30 napig használható, utána fizetni kell érte, de a legjobban akkor járunk vele, ha egyáltalán nem telepítjük, mert az ismeretlen alkalmazások ellen nem nyújt védelmet.

Internetcím: www.iss.net

Norton Personal Firewall 2002 4.0

A *Norton Personal Firewall* része a *Norton Internet Security* csomagnak, de 13 ezer forint körüli – áfa nélküli – áron külön is megvásárolható. A 16 Mbájtos, 30 napig használható próbaváltozat a *Symantec* webhelyéről tölthető le.

A program első futtatásakor egy varázsló vezet végig a konfigurálás lépésein. Mi tagadás, a beállítás némi odafigyelést és szakértelmet igényel, nem mennek olyan egyszerűen a dolgok, mint a *ZoneAlarmnál* vagy a *Tiny Personal Firewallnál*. A konfiguráló varázsló később is használható a beállítások megváltoztatására, ha nem akarjuk a menürendszert igénybe venni. A Norton Personal Firewall átvizsgálja a merevlemezünket olyan programok után kutatva, amelyeket internetezésre alkalmasnak tart. Nem dolgozik valami jó hatásfokkal, mert a kapott terjedelmes listán feltűnnek az internettel nehezen kapcsolatba hozható alkalmazások is, szerencsére ezek gyorsan törölhetők. A listára később is felvehetünk programokat, és szabályozhatjuk internet-elérésük módját. Amikor egy új program először próbálja elérni a netet, a Norton megkérdezi, hogy engedélyezzük-e az adatátvitelt. Ha kívánjuk, a válaszunkat elmenti, és emlékezni fog rá, valahányszor a jövőben ez a program online műveletbe kezd.



Tetszetős külső mögött profi szolgáltatásokat kínál a Norton Personal Firewall

A felhasználói felület jól áttekinthető, könnyedén megtalálhatók rajta a kívánt szolgáltatások. Háromféle biztonsági szint közül választhatunk egy tolókával, alaphelyzetben a legtöbb felhasználó számára megfelelő közepes védelem működik. Ez megakadályozza, hogy ismeretlen programok adatot küldjenek az internetre, és figyelmeztet, ha személyes információkat (név, cím, hitelkártya-szám) akarunk elküldeni.

Beállíthatjuk azt is, hogy a program milyen mértékben informáljon minket a biztonsággal kapcsolatos eseményekről (itt is háromféle szint közül választhatunk), például a behatolási kísérletekről. A védelmi rendszer tesztelésére saját weboldalát ajánlja a Symantec, ahová egy hivatkozásra kattintással juthatunk el.

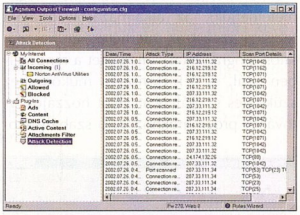
URL vagy IP-cím alapján lehetőségünk van olyan számítógépek megadására, amelyek korlátlanul hozzáférhetnek PC-nkhez. Ha ezekkel lépünk kapcsolatba, a tűzfal kiiktatja magát. Hasonlóképpen létrehozhatunk egy listát olyan gépekről, amelyekkel semmilyen körülmények között nem akarunk kommunikálni. Ide azokat a gépeket érdemes felvenni, amelyek korábban támadást intéztek ellenünk.

A biztonsági teszteket kiváló eredménnyel abszolválta a Norton Personal Firewall, védelmét nem sikerült feltörni.

Internetcím: www.symantec.hu

Outpost Firewall 1.0

A program különlegességét az adja, hogy bedolgozók (plug-inok) készíthetők hozzá, így bárki kiterjesztheti képességeit. Szolgáltatásai egy részét (így például a levélmelléklet-szűrést és a hirdetésblokkolást) már most is bedolgozók valósítják meg. A Windows Intézőjére emlékeztető barátságos programfelületen könnyen megtalálhatók a szolgáltatások és a beállítási lehetőségek, akár a menüket, akár az eszköztárat használjuk. Szinte nem is kell változtatni a biztonsági konfiguráción: az alapbeállítások a legtöbb felhasználó számára úgy jók, ahogy vannak. Figyelemre méltók a testre szabási lehetőségek is: tág határok között változtatható, hogy a program milyen információkat jelenítsen meg az adatátvitelről, a behatolási kísérletekről, az átengedett és a blokkolt adatcsomagokról, a meglátogatott webhelyekről.



Otthonosan mozoghatunk az Outpost Intéző-szerű felületén

Többnyelvű program lévén telepítéskor az angol mellett más nyelveket is felkínál. A magyar egyelőre nincs a lehetőségek között, ami azért különös, mert a gyártó webhelyéről egy pdf formátumú, magyar nyelvű dokumentáció is letölthető, amelynek a képernyő-illusztrációi magyar nyelvűek.

Ötféle biztonsági szint közül választhatunk, az internetezésre használt programok pedig három kategóriába sorolhatók

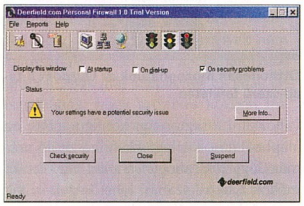
(megbízhatók, blokkoltak és szabály alapján szűrtek). A tesztelés során teljes védelmet nyújtó, 2,7 Mbájtos letöltési méretű Outpost használata ingyenes.

Internetcím: www.agnitum.com

Personal Firewall 1.0

Egyszerű felépítésű program, szolgáltatásai közvetlenül elérhetők az eszköztárról. Tesztjeink bizonysága szerint alapbeállításai megbízható védelmet nyújtanak mindkét irányban. A szokásos három biztonsági szinthez – a teljes blokkoláshoz, a szabály alapú normál üzemmódhoz és a mindennemű adatforgalom átengedéséhez – egy-egy közlekedési jelzőlámpa tartozik, így pofonegyszerű az átkapcsolás közöttük. Külön biztonsági beállításokat alkalmazhatunk az otthoni, az irodai és a mobil használatra, e profilok közül ugyancsak ikonokra való kattintással választhatunk.

Telepítés után az 1,4 Mbájtos *Personal Firewall* biztonsági ellenőrzést hajt végre a gépünkön (ezt később bármikor megismételhetjük), az alkalmazások listájára felveszi azokat az internetezésre használatos programokat, amelyeket a rendszerben talál, és a biztonságos működéshez szükséges szabályokat alkot hozzájuk. A további programokhoz való szabályalkotás azonban eléggé macerás, és csak tapasztaltabb felhasználóknak ajánlott. Más személyi tűzfalaknál első futtatásukkor a programok egyszerűen felvehetők a listára és gond nélkül alkotható hozzájuk szabály.



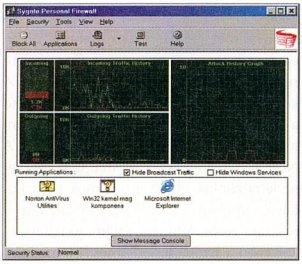
Egérkattintásokkal vezérelhető a Personal Firewall

30 napos kipróbálás után 30 dollárt kell fizetni a Personal Firewallért. A ZoneAlarm és a Tiny Personal Firewall ingyenes, és egyszerűbben konfigurálható.

Internetcím: www.deerfield.com

Sygate Personal Firewall 5.0

Hasonlóan a többi személyi tűzfalhoz, telepítése után azonnali védelmet nyújt. A programablakban grafikus állapotjelzők mutatják a hálózati forgalmat és a behatolási kísérleteket. A menük jól szervezettek, gyorsan megtalálhatók bennük a szolgáltatások. A tálcán lévő ikon jobbgombos menüjében ugyancsak elérhetők a legfontosabb lehetőségek.



Naplózásban verhetetlen a Sygate Personal Firewall

Háromféle biztonsági szintet kínál az otthoni használatra ingyenes *Sygate Personal Firewall*: a teljes blokkolást, a mindennemű forgalom átengedését és a normál üzemmódot. Amikor egy program először használja az internetet, felkerül az alkalmazások listájára. Itt aztán számos körülményre kiterjedő szabályt alkothatunk arra vonatkozólag, hogy mit tehet meg a későbbiekben. Így például ütemezhetjük futását, vagy korlátozhatjuk használatát bizonyos IP-címekre.

Az eszköztáron található *Test* gomb a *Sygate* webhelyének tesztoldalára röpít minket, ahol gépünk minden lehetséges portját vizsgáló, több órán keresztül tartó próbáknak vethetjük alá védelmi rendszerünket.

A program naplózási szolgáltatásai egyedülállóak. Részletesen regisztrálja a behatolási kísérleteket, az adatforgalmat és a konfiguráció változásait. Az adatokat többféle bontásban jeleníthetjük meg: az utolsó egy, két vagy három nap, az utolsó egy vagy két hét, vagy pedig az eltelt hónap szerint.

A konfiguráló párbeszédablak jól áttekinthető, bosszantó viszont, hogy egyes szolgáltatások érvénytelenítve vannak, ezeket csak a 40 dollárért megvásárolható *Pro* változatban használhatjuk. A legtöbb felhasználónak azonban nincs is szüksége ezekre, és a 4,6 Mbájtos letöltési méretű ingyenes verzió – mint a tesztelés során kiderült – is tökéletesen megvédi a gépünket a támadásoktól.

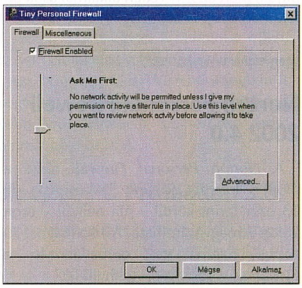
Internetcím: www.sygate.com

Tiny Personal Firewall 2.0.15

A *WinRoute Pro* biztonsági technológiára épülő program felhasználói felülete ennél egyszerűbb már nem is lehetne. Az adminisztrációs ablakot a tálcán lévő ikonra való kettős kattintással jeleníthetjük meg. Három biztonsági szint közül választhatunk, ezek: a teljes blokkolás, az engedélykérés minden adatmozgáshoz és az engedélykérés nélküli működés. Az utolsó esetben minden olyan hálózati aktivitás engedélyezett, amely nem ütközik az általunk korábban meghatározott szabályokba. Akár összetett szabályokat is egyszerűen hozhatunk létre egy világos felépítésű párbeszédablakban. Lehetőségünk van például arra, hogy egy adott IP-címről érkező kéréseket visszautasítsuk. Az adminisztrációs ablak használatát és a naplóállomány megtekintését jelszavas védelemmel láthatjuk el.

Amikor nem engedélyezett adatmozgást észlel, a *Tiny Personal Firewall* egy riasztásablakot jelenít meg. Itt engedélyezhetjük vagy visszautasíthatjuk a műveletet, illetve definiálhatunk hozzá egy szabályt, amely meghatározza, hogy a jövőben miként viselkedjen a szóban forgó program.

Az élő kapcsolatok nyomon követésére szolgál az állapotablak, amelyet úgy hívhatunk elő, hogy a jobb egérgombbal a



Tiny Personal Firewall: puritán felület, hatékony védelem

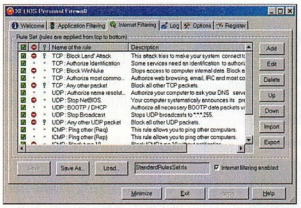
program ikonjára kattintunk, majd a menüben a *Firewall Status Window* lehetőséget választjuk.

Ami a biztonságot illeti, az 1,4 Mbájtos Tiny Personal Firewall szivárgásmentes védelmet nyújt mindkét irányban. Otthoni felhasználók számára ingyenes.

Internetcím: www.tinysoftware.com

Xelios Personal Firewall 2.02

A mindössze fél megabájtos letöltési méretű program felhasználói felülete egy többlapos párbeszédablak. A *főlapon* láthatjuk, hogy milyen IP-címen csatlakozunk az internetre, és folyamatosan figyelemmel kísérhetjük a beérkező és kimenő adatcsomagok számát, illetve azt, hogy ezek közül hányat blokkolt a program. Az *Options* lapon állíthatjuk be a működési



Hiába a sok beépített szűrő, nem teljes a Xelios Personal Firewall védelme

jellemzőket, többek között a jelszavas védelmet. Az *Internet Filtering* lapon találjuk az alapértelmezésbeli adatszűrő szabályokat, és itt hozhatunk létre újabbakat.

A biztonsági tesztelés két port esetében *Close* állapotot jelzett, ami azt jelenti, hogy a *Xelios Personal Firewall* megakadályozza az ezeken keresztüli behatolást, a gépünket viszont nem teszi láthatatlanná a külvilág számára. Valószínűleg olyan adatszűrő szabály is létrehozható, amely orvosolja a problémát, ez azonban egy személyi tűzfal használójától nem várható el. Ennél is nagyobb hiányossága a programnak, hogy az adatot küldő alkalmazások ellenőrzését csak akkor végzi el, ha bejelöljük az *Application Filtering* ablak *Application Filtering Enabled* lehetőségét. Vagyis amíg erre nem jövünk rá, bármelyik program bármit zavartalanul átküldhet a tűzfalon. Ezután már szigorúan őrködik adataink felett, és a listára felvett programok futási jellemzőit egyszerű egérkattintásokkal módosíthatjuk.

A Xelios Personal Firewallért a 30 napos kipróbálási időszak letelte után 32 dollár regisztrációs díjat kell fizetni. Emiatt, továbbá figyelembe véve hiányosságait, jobban járunk az ingyenes programok valamelyikével.

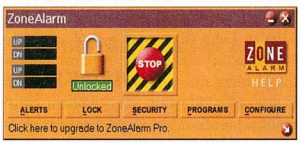
Internetcím: www.xelios.com

ZoneAlarm 2.6.362

A közel 3 Mbájtos állomány telepítése gyerekjáték, a művelet végén egy hétlépéses, lényegre törő oktatóprogram ismertet meg minket a *ZoneAlarm* használatával. A telepítés után azonnal a legmagasabb szintű védelmet nyújtja (ez az alapbeállítás), a jól áttekinthető konfiguráló ablak a tálcán helyet kapó ikonra való kétszeri kattintással jeleníthető meg.

A *Configure* gombbal előhívható beállítólapon írhatjuk elő, hogy a program rendszerindításkor automatikusan elinduljon-e vagy sem (célszerű az előbbi lehetőséget választani, így gépünk mindig védelem alatt áll majd). Az *Alerts* lapon tekinthetjük meg a legutóbbi riasztásokat, és itt adhatjuk meg, hogy a program naplóállományba mentse-e a riasztásokat, valamint azt, hogy behatolási kísérlet esetén jelenjen-e meg üzenet a képernyőn. A *Security* ablakban tekinthetjük meg a biztonsági beállítások szintjét, és engedélyezhetjük az e-mail mellékletek vizsgálatát.

A *Lock* lap szolgál a blokkolási beállítások megadására. Előírhatjuk itt, hogy a program bizonyos idő eltelte után vagy a



Egyszerű kezelhetőséggel és tökéletes biztonsággal büszkélkedhet a ZoneAlarm

képernyőkímélő elindulásakor blokkolja az internetforgalmat. Beállíthatunk teljes vagy a részleges blokkolást, az utóbbi esetben azok a programok férhetnek hozzá a nethez, amelyeknél a *Programs* ablakban engedélyeztük a *Pass Lock* lehetőséget. A Programs ablakban tekinthetjük meg az internet-elérésre használt programok listáját is, amelybe akkor kerül be egy program, amikor a ZoneAlarm telepítése után először futtatjuk. Egy program engedéllyel vagy engedély nélkül csatlakozhat az internetre, az előbbi esetben minden futtatáskor megerősítést kér a ZoneAlarm.

Az internet teljes blokkolása a lakatot ábrázoló ikonra való kattintással is elvégezhető, az internet-elérés azonnali leállítása vészhelyzetben pedig a *Stop* feliratú gombra kattintással tehető meg. A ZoneAlarm részletes súgója nem csupán a program használatát és az alkalmazott technológiát ismerteti, hanem bevezeti az olvasót az internet titkaiba is.

A tesztelés során a ZoneAlarm teljes védelmet nyújtott mind a bejövő, mind a kimenő próbálkozásokkal szemben. Otthoni használatra a program ingyenes, egyébként 20 dollár a regisztrációs díja.

Internetcím: www.zonealarm.com

Értékelés

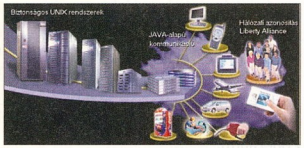
Egy otthoni használatra szánt személyi tűzfaltól azt várjuk el, hogy minél kevesebbe kerüljön, különösebb állítgatás nélkül, már alaphelyzetben teljes védelmet nyújtson, és az internetet használó alkalmazások konfigurálása egyszerű legyen.

Az otthoni felhasználók számára ingyenes ZoneAlarm telepítése után azonnal áthatolhatatlan pajzsot képez gépünk köré, és ha mégis szükséges valamit beállítanunk, azt egyszerűen megtehetjük a jól áttekinthető felhasználói felületen. Ugyancsak teljes védelmet nyújt és ingyenes a puritán felületű Tiny Personal Firewall, a naplózásban kiemelkedő Sygate Personal Firewall és a Windows Intézőre hasonlító Outpost.

A Norton Personal Firewall 2002 a neves fejlesztőtől megszokott kiváló minőséget nyújtja, akinek azonban nincs szüksége a többletszolgáltatásokra, csupán megbízható védelemre vágyik, jobban jár a ZoneAlarmmal vagy a többi ingyenes tűzfal valamelyikével.

A hiányos védelmű BlackIce PC Protection, valamint a nem túl egyszerűen konfigurálható Personal Firewall és Xelios Personal Firewall nem érik meg a regisztrációs költséget, ingyen sokkal jobb tűzfalakhoz juthatunk.

Mészáros Csaba



Csak nyíltan, őszintén

A tavaly szeptemberi New York-i események óta a vállalatok világszerte nagy hangsúlyt fektetnek a biztonságra. Ennek következtében érezhetően megnőtt az igény a nyílt rendszerek – például a UNIX – iránt. A biztonságos kommunikáció megteremtésében fontos szerepet játszhat a Sun Liberty Alliance nevű személyazonosítási megoldása is.

A *UNIX* úgynevezett nyílt kulcsokat tartalmaz, ami azt jelenti, hogy a rendszer bármely részét működtető programrészletek *(szkriptek)* bárki számára hozzáférhetők. A UNIX-programban nincs fekete doboz, az egyes folyamatok teljes mértékben áttekinthetők, a logikus szintrendszerben egy helyről állítható be minden paraméter, ellentétben például a Windows-zal, amelyben az egyes funkciók egészen más helyekről állíthatók be.

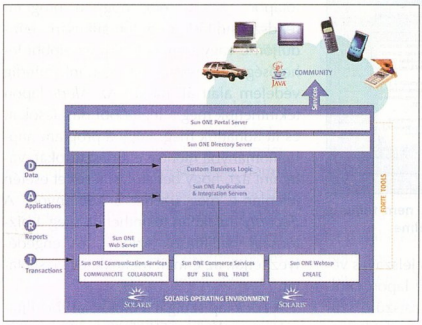
A UNIX biztonsági alapelvei indulásától a mai napig mit sem változtak, működési elve a jogosultságok rendszerén alapul, amelyet úgy alakítottak ki, hogy abban gyakorlatilag nem lehet kárt tenni. Természetesen a szoftver „agyához", a *roothoz* – különféle beállítási hibák vagy emberi mulasztás miatt – elméletileg hozzáférhetnek rosszindulatú behatolók, de ennek az esélye minimális.

A UNIX esetében ezenkívül a javítási idő és költség is jóval kedvezőbb lehet, mint más rendszereknél. Fontos megemlíteni még, hogy a UNIX a vírusokkal szemben is nagyobb biztonságot kínál, mint más operációs rendszerek.

Biztonság a virtuális térben

Az internet és az internet-alapú alkalmazások elterjedése miatt a vállalatközi adatforgalom jelentős része internetes platformon zajlik. Az informatika fejlődésével az adatok nemcsak a jogos felhasználók számára válnak egyre értékesebbé, hanem a konkurencia, a *hackerek* vagy más illegális behatolók számára is. Természetesen vannak olyan intézmények, amelyeknél az adatvédelem már most is nagy hangsúlyt kap; ilyenek a kormányzati, a nemzetbiztonsági és katonai szervek, a pénzügyi szervezetek – ezeknél azonban a védekezés elsősorban azon alapul, hogy rendszereik nem kapcsolódnak nyilvánosan elérhető hálózatokhoz.

A kommunikációs eszközök fejlődésével a cég számára nélkülözhetetlen adatok – közvetve vagy közvetlenül – többféle módon is rendelkezésre állnak, ezért ennek a folyamatnak az eredményeként a vállalati belső biztonsági gyűrűk erősítése is elengedhetetlenné vált. A hazai vállalatok jó része már most is használ alapvető biztonsági előírásokat, s a jövőbeni informatikai beruházások egyre nagyobb része is olyan fejlesztésekre irányulhat, amelyekben fokozott szerepet kap a biztonság.



A Sun ONE szoftverstratégiája

Internetes biztonságpolitika

Ugyancsak egyre határozottabban jelentkezik az az igény is, hogy a 2001. évben tapasztalt számítógépes kórokozók *(Code Red, Nimda* és *Goner)* gyors és igen széleskörű elterjedését minél hatékonyabban ki tudja küszöbölni a cég számítógépes rendszere. Egyes becslések szerint csak a Code Red vírus mintegy 2 milliárd dolláros kárt okozott világszerte.

A hálózatokon terjedő PC-s kórokozók 2000-ben mintegy háromszor annyi fertőzést okoztak, mint 1995-ben és 1996-ban együttesen. Ennek megfelelően a szakembereknek fokozott figyelmet kell fordítaniuk az internetes biztonságpolitikára, amely nem csak az eddig alkalmazott webszerver platformjukkal kapcsolatos álláspontjuk átértékelését jelenti, hanem egy átfogó, a megelőzésre, az észlelésre és a beavatkozásra is kiterjedő szemlélet kialakítását is. A nem megfelelő védelemre hivatkozva a hazai cégek egyelőre nem óhajtják internetes alapokra helyezni azokat az adatbázisokat, valamint alkalmazásokat, amelyekben valóban jelentős károkat okozhatnak a jogosulatlan hozzáférők vagy rosszindulatú behatolók. A hosszútávú megoldás azonban nem az adatbázisokhoz való hozzáférés akadályozásában, hanem – ezzel ellentétben – azok teljeskörű rendelkezésre bocsátásában rejlik, természetesen a megfelelő védelemmel együtt.

Java, a csodafegyver

Biztonsági szempontból a világszerte igen elterjedt PC-alapú szoftverkörnyezet igen sebezhetővé válik az internetes alkalmazások futtatása esetén. A *Java* technológia – a *Sun Microsystems* internetes programozási környezete és nyelve – jelenleg az egyik legelterjedtebb, valóban platformfüggetlen és biztonságos internetes programozási nyelv. A Java azáltal, hogy biztonságot nyújt az egész hálózaton, az olyan alkalmazások esetében is ideális, amelyek emeltszintű biztonságot követel-

Bejelentkezés a légitársaság honlapjára

nek meg, mint például az *elektronikus kereskedelem* vagy az *internetes banki* szolgáltatások. A Java programozási nyelv „Írd meg egyszer, és futtasd bárhol" tulajdonságának köszönhetően az alkalmazások ugyanabban a környezetben fejleszthetők, majd tetszőleges platformon futtathatók, időt és pénzt takarítva meg a cégek és intézmények számára. A program kicsi, futtatása egyáltalán nem lassítja le a processzort. A Java születésétől kezdve biztonságos, s úgynevezett *virtuális gépként* működik az őt futtató programkörnyezetben. Ez azt jelenti, hogy ha egyszer a program elindul, akkor onnan már nem lehet kilépni, vagyis kódja csak korlátok között futtatható.

Biztonság elérhető áron

Becslések szerint a világon jelenleg több mint hárommillió programozó szakember használja a Javát, mintegy 7 millió weboldal építésében. Az alkalmazásszerverek több mint 90 százalékában, továbbá sok millió vezeték nélküli kommunikációs eszközben – PDA-kban, mobiltelefonokban, valamint egyéb banki vagy kereskedelmi felhasználási területeken – használják folyamatosan a Java programnyelven íródott fejlesztéseket, alkalmazásokat, kihasználva a technológia gazdag lehetőségeit és platformok közötti, többféle eszközt támogató képességét.

A Sun Microsystems a kis- és közepes, valamint a nagyvállalatok számára is testreszabott biztonsági megoldásokat kínál. A vállalat ugyan túlnyomórészt hardveres termékeket értékesít, mégis mérnökeinek kétharmada szoftveres irányultságú szakember. Ez is azt mutatja, hogy a jövőben igen nagy szerepet szánnak a technológia elterjesztésének.

Ennek első lépése a Sun-Netscape összefogás volt, majd ezután 2001. februárjában létrejött a *Sun ONE (Open Network Environment)* nevet viselő tetszőleges internet-alapú szoftverkörnyezet, amely nem alkalmazás, hanem egy infrastruktúra-szintű szoftvermegoldás. Nyílt rendszerként bármely szoftverkörnyezettel kompatibilis, s magát a programstratégiát akár alkotórészeivel együtt is cserélni lehet.

A biztonságos technológia ma már nem csak a nagyobb cégek számára elérhető. A Sun ONE-t a kis- és közepes vállalatok számára is ajánlja a Sun. A *Sun Fire v1.0* elnevezésű egyprocesszoros szervert több ezer dollár értékű, nagyfokú biztonságot garantáló szoftverekkel kínálják. A mindössze 4000 dollár értékű csomag magában foglalja a hardvert, a *Sun Solaris* operációs rendszert, azonkívül egy webszervert, egy apache webszervert, egy ASP szervert, amellyel Microsoftos ASP alkalmazások is futtathatók, valamint egy directory szervert, amellyel akárhány felhasználó konfigurálható. A határ a processzor kapacitása.

Személyazonosítás az interneten

A mindennapi internetező nap mint nap szemben találja magát azzal a problémával, hogy a különböző weboldalakon újból és újból meg kell adnia a személyes adatait, úgy hogy közben már nem is tudja, hány szerveren találhatók meg azok. Igen nagy tehát az igény egy olyan integrált szolgáltatásra, ahol a felhasználóknak csak egyszer kell megadniuk adataikat, azokat a befogadó rendszer biztonságosan tárolja, és bármikor a felhasználó vagy szolgáltatója számára elérhetővé teszi, amennyiben a tranzakciókhoz szükség van rájuk.

A Liberty története

2001. szeptember: Bejelentik a Liberty Alliance megalakulását.

2002. február: Már 38 résztvevője van a szervezetnek. Bejelentik, hogy hamarosan megjelenik a szabvány első specifikációja.

2002. május: Alapítványok, non-profit szervezetek csatlakozása.

2002. július: Megjelenik az első specifikáció. A résztvevő tagok száma 65-re emelkedik.

A mai napig két nagy szolgáltatás szeretné elfogadtatni a világgal a maga azonosítási szabványait. Az egyik a Sun új, úgynevezett *Liberty Alliance* megoldása, a másik a már jól ismert *Passport* a *Microsofttól*. A Passport zárt, központi rendszerével szemben, ahol a felhasználók adatait csak és kizárólag a Microsoft tárolja, a Liberty Alliance esetében nyílt vagy elosztott rendszerről beszélhetünk, vagyis olyanról, ahol a felhasználók engedélyével az egyes tranzakciók összekapcsolhatók. Lássunk egy példát.

Hogyan is működik a Liberty?

Kiss úr üzleti útjára interneten rendeli meg a repülőjegyét és bérelt autóját az Egyesült Államokba, frankfurti átszállással. Kiss úr Ferihegyen minden gond nélkül felszáll Frankfurt felé. A baj ott kezdődik, hogy átszálláskor üzemzavar miatt két órával később indul tovább, ezért két órával később érkezik meg a tengerentúlra. Az előre lefoglalt bérelt autót a késés miatt nem tartották fenn számára, és a cégével

A program felajánlja az autókölcsönző szolgáltatás igénybevételét

kapcsolatban álló autókölcsönző nem tudott másik autóval szolgálni. Kiss úr a késés miatt fontos üzleti tárgyalásról maradt le. Ha Kiss úr a Liberty Alliance-t használta volna, a légitársaság rendszere értesítette volna az autókölcsönző cég rendszerét arról, hogy Kiss úr késni fog, és fenntartották volna számára az autóját.

A Liberty Alliance lényege éppen ebben rejlik: az elosztott rendszer elemei nyílt felületen kommunikálnak egymással. Ha a felhasználó úgy dönt, hogy két szolgáltatást össze kíván kapcsolni – esetünkben a repülőjegy-foglalást és az autókölcsönzést

Bejelentkezés az autókölcsönző céghez

–, a két – különben teljesen különálló – rendszer egy rendszerként kezd működni. Az azonosítás rendkívül biztonságos, hisz valójában a felhasználó engedélyével ajánlja fel az általa megadott és engedélyezett adatokat egy kiválasztott szolgáltatón keresztül több szolgáltatónak. A rendszer alapja a Sun Microsystems már működő directory szoftvere, amelyet belső azonosításra – például számlázásra, beléptetőkártyára vagy felhasználó-azonosításra – használnak. A jövő a több vállalat hasonló rendszereinek összekapcsolásában rejlik.

Változások az e-commerce-ben

A szoftvergyártók gőzerővel dolgoznak a Liberty Alliance megoldás termékeikbe való beépítésén. A közelmúltban mutatták be a projekt első specifikációját, amely a webes azonosítás alapjait fektette le. Ez azt jelenti tehát, hogy Kiss úrnak csak egyetlen egyszer kell bejelentkeznie, a többit a rendszer már automatikusan intézi, mint ahogyan azt az iménti példa is mutatja: ha egyszer Kiss úr kéri, hogy repülőjegye mellé bérautót is foglaljanak számára, s ne kelljen ezt külön elintéznie az autókölcsönző cég honlapján, egy bejelentkezés után, sokkal egyszerűbben és gyorsabban, a repülőjegy-foglalás után, külön kijelentkezés nélkül választhatja ki a kívánt autót. A rendszer továbbá leegyszerűsíti a tájékozódást, mégpedig oly módon, hogy a rendelkezésre álló azonosítási adatok alapján csak és kizárólag azokat az információkat jeleníti meg a képernyőn, amelyek a felhasználó számára relevánsak, továbbá a felhasználónak kijelentkeznie is csak egyetlen egyszer kell.

A most bemutatott szoftver lehetővé teszi a vezeték nélküli eszközökön is az azonosítási műveletek végrehajtását, így Kiss úr útközben mobiltelefonja és hordozható érintőképernyős számítógépe segítségével könnyűszerrel ellenőrizheti foglalásai státuszát. Maga a Sun is bejelentette, hogy integrálja a Sun ONE-ba a Liberty-t. A Sun is – mint a szövetség többi résztvevője – arra törekszik, hogy egységes internetes szabványokat használjon bárhol a világon, és a szabványokat ne használja profitszerzésre. Míg a most bemutatott *1.0*-s verzió bejelentkezési azonosítókra és a hozzájuk kapcsolódó jelszavakra, valamint a rendszerben részt vevő szolgáltatók bevonására kínál megoldást, a következő verzió – melynek megjelenése a szakemberek szerint hamarosan, 2003 elején várható – már más típusú információk cseréjére is lehetőséget nyújt majd. Többek között támogatni fogja a hitelkártyás fizetést, továbbá a telefonszámok, címek vagy más típusú adatok használatát is.

Passport kontra Liberty

A Liberty Alliance tavaly szeptemberi elindítását sokan a Microsoft Passport elleni nyílt támadásnak vélték. A Microsoft akkori nyilatkozataiban nem adott esélyt az új szabvány elterjedésének. A helyzet azóta megváltozott. A Sun Microsystems már csak inkább afféle tanácsadóként segíti a rendszer elterjedését. A Liberty elterjedését egyébként olyan nagyágyúk segítik, mint az *America Online*, az *EarthLink*, a *United Airlines*, az *American Airlines*, a *General Motors*, továbbá a *Vodafone*, a *Nokia* és a *France Telecom*, illetve a *Bank of America*, a *Visa*, a *Fidelity Investments*, az *American Express* és a *Citigroup*.

A két nagy szabvány olyannyira közelít egymáshoz, hogy maga a Passport is – amely jelenleg a Microsoft saját, egyedi technológiájára épül – 2003-ra várhatóan csatlakozik más azonosítási szabványokhoz, így a Liberty-hez is. A Microsoft továbbá bejelentette, hogy a Passport nyitottabb verzióját is 2003-ban tervezi bemutatni. A *Gartner* szerint a Passport jelenleg 14 millió regisztrált felhasználót tudhat maga mögött, amelyhez képest a Liberty vadonatúj technológiáját igénybevevő felhasználók száma igen csekély. Elemzők szerint azonban a Liberty-t használók tábora a közeljövőben jelentősen növekedni fog.

Míg a Passport sokkal több kisfelhasználót sorakoztatott fel maga mögött, a Liberty a nagyfelhasználók körében érhet el látványos eredményeket. A Liberty rendszere hasznos szerepet játszik majd a résztvevők közötti adatforgalom jelentős egyszerűsödésében és költséghatékonyságában. A cégek között, valamint a cégek és fogyasztóik között az egyszerűsödő adatkezelés miatt gyorsabban zajlanak

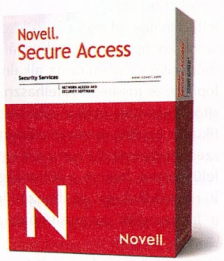
Az adatok automatikusan átkerülnek az autókölcsönzőhöz

majd az internetes üzleti tranzakciók, de az egyszerű fogyasztónak sem kell ki tudja hány helyen megadnia az adatait. A szabvány elterjedésével várhatóan jelentős áttörés következik be a tranzakciókat lebonyolító internetes piacokon, körülbelül úgy, mint ahogyan a készpénzfelvevő automaták az egyik pillanatról a másikra elfogadták a bankok bármelyike által kibocsátott kártyát. De hasonló változás várható a vezeték nélküli eszközök területén is. Az új szabványt tartalmazó új szoftverek ez év végén kerülnek a boltokba.

Kemény László

Integrált biztonság

Az informatikai biztonság és a megbízhatóság egymástól szinte elválaszthatatlan fogalmak. A Novell Secure Access integrált megoldáscsomag a személyazonosság egységes felügyeletét, s ezáltal az ügyfelek bizalmának növekedését kínálja a vállalkozásoknak.



A Novell Secure Access a biztonságos hozzáférés ideális eszköze a vállalatok számára

A bizalom minden üzleti kapcsolat alapja. A mai világban az elektronikus felületek egyre több helyen felváltják a személyes emberi kapcsolatokat. Ahogy egyre inkább a webes alkalmazások válnak a vásárlókkal és a partnerekkel való kapcsolattartás eszközeivé, a cégeknek is ugyanolyan szintű bizalmat és megbízhatóságot kell elérniük a webes felületeken keresztül is, mint amilyeneket a személyes kapcsolatok biztosítanak. A hatékony szolgáltatások érdekében tárgyalni kell a partnerekkel és a gyártókkal, az alkalmazottaknak pedig biztosítani kell a munkájuk végzéséhez szükséges erőforrásokat; meg kell osztani a cég hálózati erőforrásait, ugyanakkor védeni kell ezeket az erőforrásokat a jogosulatlan használat és a behatolók ellen. Átfogó biztonsági megoldásra van tehát szükség, amely egyszerre kínál egyszerű hozzáférést a hálózathoz, ugyanakkor megfelelő módon védi az IT rendszereket.

A *Novell Secure Access* biztonsági megoldáscsomag a Novell hozzáférési és biztonsági termékeinek új, integrált csomagja, amellyel *egyszerűsíthető, biztonságossá tehető és felgyorsítható a jogosultság kezelése* a különböző alkalmazások, platformok, adatbázisok és hálózati erőforrások között. A mai szokásos hozzáférési és biztonsági megoldások gyakran külön tárolják a személyazonossági adatokat és a biztonsági irányelveket. Ha viszont többszörösen, termékenként külön kell tárolni a személyazonossági adatokat és a biztonsági irányelveket, az nemcsak megnöveli a sérülékenységet és a felügyeleti/támogatási költségeket, hanem rontja a végfelhasználók hatékonyságát is. Ráadásul ezek a megoldások általában nem foglalják magukban az összes felhasználót, akivel egy szervezet kapcsolatba kerül.

A hálózatnak egyformán konzisztens hozzáférés-vezérlésre és biztonságra van szüksége, akár a vásárlókról, akár a partnerekről, akár pedig az alkalmazottakról van szó. A Novell Secure Access biztonsági megoldáscsomag segít a magas szintű biztonság kialakításában, csökkenti a felügyeleti és támogatási költségeket, valamint felhasználóbarát rendszert kínál a végfelhasználók számára. A Novell Secure Access *ideális biztonsági megoldáscsomag a különböző vegyes hálózatokhoz:* képes egységesíteni a Novell-termékek, valamint a nem Novell-alkalmazások, adatbázisok, platformok és más hálózati erőforrások jogosultság-kezelését.

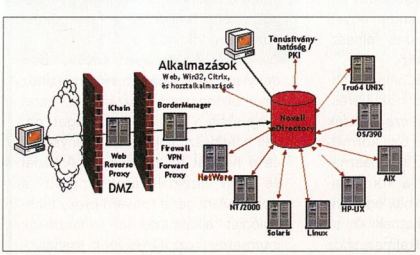
A sérülékenységek megszüntetése

A Novell biztonsági csomagja megszünteti a több azonosítóval és jelszóval rendelkező felhasználókkal, illetve a hálózaton elszaporodott „lejárt" felhasználói profilokkal együtt járó általános kockázatokat. A Novell Secure Access használatával a felhasználók biztonságosan hozzáférhetnek a hálózathoz az asztali PC-kről, a noteszgépekről, a mobiltelefonokról és a PDA-król egyaránt. A termék méretezhető is: *képes akár felhasználói profilok millióival is megbirkózni,* részletes adatokat tárolva minden egyes felhasználó szerepéről és kapcsolatairól a cégen belül és kívül egyaránt. Ez a személyazonosság-információ használható a felhasználók hitelesítésére, és ez alapján adható vagy tagadható meg a hozzáférés a hálózati erőforrásokhoz.

A Secure Access *többféle hitelesítési módszert is támogat,* így például az egyszerű és összetett *jelszavak,* a digitális *tanúsítványok,* a *token*-alapú technológiák (intelligens kártyák és tokenek), valamint a *biometriai* eszközök (retina- vagy ujjlenyomat-leolvasók) használatát.

Kisebb felügyeleti költségek

A Novell Secure Access a hálózat-felügyelet egyszerűsítésével *csökkenti a felügyeleti költségeket.* Sok más biztonsági megoldás esetében a rendszergazdáknak maguknak kell különféle megkerülő módszereket kidolgozniuk a különféle biztonsági infrastruktúrák békés egymás mellett élésének megoldására – a Novell Secure Access azonban rögtön *többféle platformot és alkalmazást támogat.* Ez egyszerűsíti a felügyeletet,



A Secure Access a legkülönfélébb platformokkal és alkalmazásokkal működik együtt

és lehetővé teszi a meglévő technológiai befektetések kiaknázását. A Novell Secure Access használata esetén nem kell kidobni a meglévő informatikai értékeket, és nem kell külön szoftvert telepíteni a kliensekre, mivel a heterogén rendszerek is könnyedén felügyelhetők ugyanazzal az eszközzel.

A termék a legtöbb platformmal és alkalmazással együttműködik (NetWare, Windows NT/2000/XP, Solaris, UNIX, Free BSD, Open MVS, OS/390, AS/400, Linux, illetve Windows-, web- és host-alkalmazások, Citrix/Terminal Server), ezenkívül javítja a hálózat teljesítményét is: a titkosítás terhét leveszi az alkalmazásszerverről, és a weblapok elérését gyorsító cache-funkcionalitást is kínál.

Azonosítók felügyelete

A Novell biztonsági megoldáscsomagjával *a felhasználói azonosítók tetszés szerinti helyről felügyelhetők.* A hálózat bármely pontjáról elláthatók az alapvető felügyeleti feladatok: a jelszavak kezelése, a felhasználók felvétele és törlése, a felhasználói konfigurációk és hozzáférési jogok módosítása, valamint az alkalmazások telepítése és frissítése. A felhasználói azonosító módosítása után a változások automatikusan tovább szinkronizálódnak az összes rendszerre. Ez nemcsak egyszerűsíti a felügyeletet, hanem a biztonságot is növeli. Ha például egy alkalmazott kilép, akkor a felhasználói azonosítóinak a központi törlése által azonnal meg lesz tiltva számára az összes hálózati erőforrás elérése. Ez megerősíti a hálózatnak a jogosulatlan hozzáféréstől való védelmét, valamint arról is gondoskodik, hogy ne maradjon egyetlen „hátsóajtó" se nyitva a hálózaton.

Biztonsági irányelvek

A Secure Access használatával mind a hozzáférés-vezérlés, mind a biztonsági irányelvek a felhasználó személyazonosságára alapozhatók. Megoldható például, hogy a marketing- és értékesítési osztály alkalmazottai más alkalmazásokat, adatokat és hálózati erőforrásokat érjenek el, mint a személyzeti osztály alkalmazottai. Megoldható továbbá, hogy a felsővezetés olyan adatokhoz is hozzáférjen, amelyek el vannak zárva az ügyfélkapcsolati alkalmazottak elől. A Novell Secure Accesszel *kifinomult módon szabályozhatók a hozzáférési jogosultságok:* ha kell, akár egyes fájlonként, sőt egyes attribútumonként (pl. e-mail cím) is kiosztható vagy megtagadható a hozzáférési jog. Ezenfelül a Novell Secure Access *tűzfallal védi a bejövő és kimenő adatokat,* hatékony védőgátat építve ki a belső hálózat és az internet között, hogy a rosszindulatú tartalom ne jöhessen be.

A *címtár-integráció* révén a Novell Secure Access segítségével a jogosult felhasználók elérhetik a számukra engedélyezett információt és erőforrásokat. További védelmet nyújt a *forward-proxy* technológia, amely képes korlátozni az alkalmazottak internet-hozzáférését. A proxy-technológiával a hálózat a belső fenyegetések ellen is védhető, hiszen az alkalmazottak kizárólag azokat a hálózati erőforrásokat érhetik el, amelyekhez kifejezetten jogokat kaptak.

Felhasználóbarát környezet

A csomag a végfelhasználók életét is megkönnyíti: lehetővé teszi számukra, hogy *egyetlen felhasználói névvel és jelszóval elérjék a hálózati erőforrásokat.* A felhasználóknak többé nem kell jelszavak sokaságát megjegyezniük, vagy egész nap különféle alkalmazásokba be- és kijelentkezniük. Egyszer kell csak bejelentkezniük, és máris elérik a számukra engedélyezett valamennyi hálózati adatbázist és alkalmazást. **J.R.**

A csomag tartalma

A *Novell Secure Access* csomag az alábbi biztonsági és hozzáférés-vezérlési termékeket tartalmazza:

- *Novell eDirectory:* A személyazonosság, irányelvek és hozzáférések kezelésének alapjaként a címtár minden átfogó biztonsági megoldás eleme. Az eDirectory használatával a cégek átvehetik, tárolhatják, szervezhetik és kihasználhatják azokat a személyazonossági információkat, melyek a hozzáférési jogok alkalmazottakhoz, ügyfelekhez és partnerekhez rendeléséhez szükségesek.
- *NDS Authentication Services (NDS-AS):* Az NDS Authentication Services biztonságos hozzáférést kínál a platformokhoz. Az NDS-AS kezeli a felhasználók létrehozását, törlését, módosítását, a jelszavak szinkronizálását és átirányítását a vállalati platformok – többek között a NetWare, a Windows 2000, a Solaris, a Linux és az OS/390 – között. Ez az integráció szükségtelenné teszi a különböző felhasználók létrehozását minden egyes platformon, mert az összes felhasználó egységesen kezelhető.
- *Novell iChain:* A Novell iChain feladata a biztonságos webes hozzáférés. Az iChain használatával a szervezetek biztonságossá tehetik webes környezetüket, szabályozhatják a felhasználói hozzáférést ezekhez a környezetekhez, és a felhasználóknak egypontos beléptetést biztosíthatnak szinte az összes webalapú alkalmazáshoz és tartalomhoz.
- *Novell Modulra Authentication Service (NMAS):* Az NMAS használatával a vállalatok többféle hitelesítési módszert tarthatnak fenn, beleértve a jelszavas, smart-kártyás, tokenes, biometriai és digitális tanúsítvány módszereket és akár ezek kombinációit is. Ezeknek a fejlett hitelesítési módszereknek a támogatása megerősíti az olyan hálózati adatok biztonságát, amelyek túl érzékenyek az egyszerű jelszavas védelem alkalmazásához.
- *Novell SecureLogin:* A Novell SecureLogin az alkalmazásokhoz való biztonságos hozzáférésről gondoskodik. Ezzel a termékkel a felhasználók egyetlen belépéssel elérhetik szinte valamennyi vállalati alkalmazást. A SecureLogin használatakor a felhasználóknak nem kell fejben tartaniuk a jelszavak és azonosítók tucatjait. Miután egyszer beléptek a hálózat valamelyik számítógépére, a SecureLogin automatikusan biztosítja a jogosultságot az általuk igényelt alkalmazásokhoz és adatokhoz.
- *Novell BorderManager:* A Novell BorderManager a vállalat erőforrásaihoz kínál biztonságos hozzáférést, ezzel megerősíti a vállalati biztonságot, növeli a felhasználók termelékenységét és a hálózat teljesítményét. A tűzfal és VPN szolgáltatások mellett a BorderManager a forward-proxy technológiát alkalmazza a felhasználók internetes hozzáféréseinek szabályozására, felgyorsítására és figyelésére.

Biztonság egy kézből

A Computer Associates (CA) október elején, a Data Security Day 2002 rendezvényen mutatta be legújabb biztonságtechnikai megoldását. Az eTrust Security Command Center egységes azonosítás-, hozzáférés- és fenyegetettség-kezelést kínál.

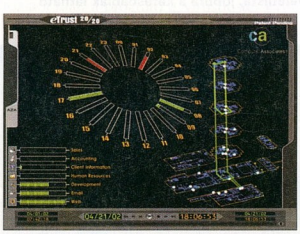
Az *eTrust Security Command Center (SCC)* tulajdonképpen a már korábban is létező CA eTrust megoldások, valamint az ezekhez kapcsolódó technológiák ötvözete. Újdonság viszont, hogy az eTrust Security Command Center segítségével a vállalat valamennyi biztonsági műveletét egyetlen vezérlőpultról vagy portálról irányíthatjuk.

A rendszer legnagyobb előnye, hogy a vállalatoknál működő biztonsági megoldásokat – beléptető, azonosító, ellenőrző rendszereket – egységes mederbe tereli, így a technológiában vagy az eljárásokban lévő „hézagok" nem teszik sebezhetővé a cég védelmét. Az integrált megoldás lényegesen kevesebb felügyeletet, adminisztrációt igényel, ráadásul így a rendszer automatizálása is könnyebben megoldható.

Az integráció növeli a hatékonyságot, ami már azért is lényeges, mert a cégek rendszereit egyre több támadás éri, a napvilágra került esetek 64 százaléka pedig anyagi veszteséggel jár. Mivel mind több cég kapcsolódik a világhálóra, a támadók gyakran éppen innen próbálnak hozzáférni a vállalatok rendszereihez. A támadások 70 százaléka ma már az internet felől érkezik, de a webes tartalmak elleni támadások száma is megduplázódott az elmúlt évben.

Bárhogy fejlődjön is a technika, a legnagyobb veszélyt a mai napig a saját munkatársak, partnerek jelentik. Ezért fontos, hogy a beléptetőrendszer, a telefonok, illetve a számítógépek használatához szükséges azonosító rendszerek, a gépek internetes forgalmának és a belső hálózathoz történő hozzáféréseknek a naplózása integrálva legyen. Így a biztonsági felelős ellenőrizheti, hogy ki, milyen alkalmazásokhoz, mikor fért hozzá, milyen telefonokat használt, illetve hogy mely helyiségekben tartózkodott. Legalább ilyen fontos a külső, hálózaton keresztül történő behatolások – például a vírusok és a hackerek – elleni védelem, amelyet szintén a Security Command Center ellenőriz, így valóban elmondhatjuk, hogy cégünk biztonságáról egyetlen rendszer gondoskodik.

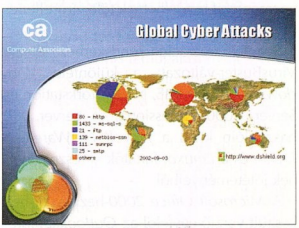
Mindez természetesen csak megfelelő jogosultsági hierarchia esetén hatékony, ám a rendszerrel a jogosultságok személyre szabhatók, így mindenki csak a munkájához szükséges alkalmazásokhoz, rendszerekhez és dokumentumokhoz férhet hozzá. A biztonsági felelős természetesen hálózaton keresztül menedzselheti a rendszert. Mivel csak a biztonsági felelős férhet hozzá a teljes rendszerhez, illetve mivel a központon keresztül minden szükséges információt megkap, valóban felelősséggel végezheti a munkáját.



A CA eTrust kezelőfelülete

Az *eTrust Identity Management* azonosítás-kezelés a felhasználók kiszolgálásáról gondoskodik, beleértve a biztonságos és egyszerűen kezelhető bejelentkezésüket az üzleti alkalmazásokba, összhangban a vállalatnál betöltött szerepükkel.

Az *eTrust Access Management* hozzáférés-kezelés a vállalati erőforrások megelőző módszerű, szabályokra alapozott védelmét, az üzletvitel szempontjából fontos rendszerek magas rendelkezésre állását biztosítja.



A hackertámadások megoszlása típus szerint

Az *eTrust Threat Management* fenyegetettség-kezelés védelmet nyújt a belső és külső fenyegetések ellen, mint amilyenek például a rosszindulatú programok és a szolgáltatás visszautasítását kiváltó támadások.

Az eTrust Security Command Center segítségével a rendszergazdák egyetlen vezérlési pontról felügyelhetik ezt a három szakterületet. Az eTrust Security Command Center valamennyi vállalati szintű biztonságtechnikai funkció integrált, portál jellegű menedzselését és megjelenítését látja el. Ezen felül nyílt csatlakozófelületeket is szolgáltat, amelyeken keresztül harmadik fél biztonságtechnikai termékeit, például behatolás-észlelő rendszereket, tűzfalakat és hálózati berendezéseket lehet illeszteni a CA termékéhez. Az integrálást a *CA Smart* megoldás-minősítő program segíti, így az adott feladatra legalkalmasabb megoldást választhatjuk, függetlenül a gyártótól.

Mint minden, a vállalat működését alapjaiban befolyásoló rendszer, az eTrust megoldások üzembe állítása is felbolygatja a cég életét, ám hogy ez minél kisebb megrázkódtatást jelentsen, a CA olyan cégekkel működik együtt, mint az *Ernst & Young*, az *EDS*, a *Fujitsu Siemens Computers*, az *SAFlink*, a *Gemplus* és az *SAP*.

Fülöp Norbert

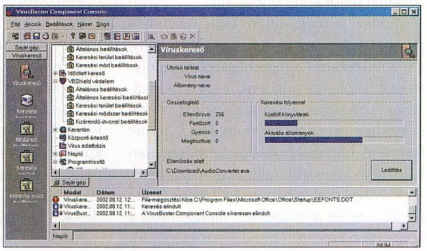
Reszkessetek kártevők!

A vírusok meg-megújuló támadásai miatt a felhasználók egyetlen percig nem érezhetik magukat tökéletes biztonságban. Hacsak nem gondoskodnak időben megfelelő vírusvédelemről. A magyar fejlesztésű VirusBuster termékcsalád teljes körű, 24 órás támogatást és számos platformra kiterjedő, központilag irányítható védelmet kínál a felhasználóknak.

Ha valaki netán még nem tudná, a félelmetes *VirusBuster* név mögött egy magyar fejlesztésű vírusellenes programcsalád rejtőzik, az 1997-ben alakult azonos nevű cég terméke. A *VirusBuster Kft.* a *Sybari*, a *Sophos* és a *ClearSwift* vírusellenes szoftvereit is forgalmazza. A cég nyár közepén felkerült a Minisztерelnökség Közbeszerzési és Gazdasági Igazgatóságának szűkített listájára, így a közigazgatási intézmények jelentős kedvezménnyel rendelhetnek tőle vírusellenes megoldásokat.

Számos operációs rendszerhez létezik VirusBuster-változat: a különféle *Windowsok* (95, 98, ME, NT 4 Workstation és Server, 2000 Professional és Server, XP) használóin kívül a *Novell NetWare*-t, a *DOS*-t és a *Linuxot* futtatók is részesülhetnek jótéteményeiből.

A *Microsoft Office 2000*-hez és *XP*-hez készült verzió egyfelől az *Outlookkal* intézett levelezést óvja a fertőzéstől, másfelől az *Office*-programokba (Access, Excel, PowerPoint és Word) integrált állandó védelem révén különféle dokumentumainkat mentesíti a kártevőktől. Folyamatosan ellenőrzi a bejövő és kimenő levelekhez csatolt állományokat (beleértve a tömörítvényeket), továbbá értesítést küld a fertőzött levél küldőjének: nem árt, ha tud róla, hogy mit terjeszt. A dokumentumokban lévő makrók csak negatív eredményű vírusellenőrzés után futhatnak. Levelezésszűrő csomag kapható a NetWare alatt futó *GroupWise*-hoz és a *Unix-alapú SMTP*-hez is.

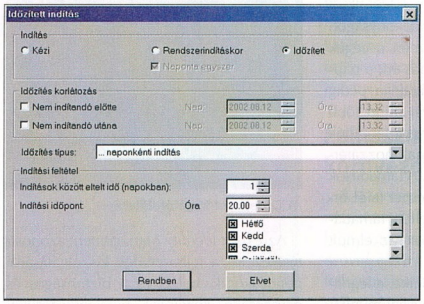


A VirusBuster jól áttekinthető programablaka víruskeresés közben. Bal szélen a Shortcut Bar, mellette jobbra a választólista, alul a műveletlista, jobbra a keresőablak látható

Windows NT-s és 2000-es hálózatokban használható eredményesen a *Windows Domain Securityre* épülő *VirusBuster Central Management Solution (CMS)*, amely lehetővé teszi a vírusellenes harc központi irányítását. Telepítési sablonjai által külön előírhatók a hálózatban található gépcsoportok védelmi jellemzői. A szoftver bizonyos időközönként megvizsgálja, hogy az egyes gépeken működő programoknál van-e újabb, és központilag elvégzi a frissítést. A hálózat kialakításától függően létrehozható többszintű irányítórendszer is. Automatikusan felismeri a hálózatra kötött gépeket, és hogy a hálózat terhelése ne nőjön számottevően, különböző időpontokban végzi el a frissítést.

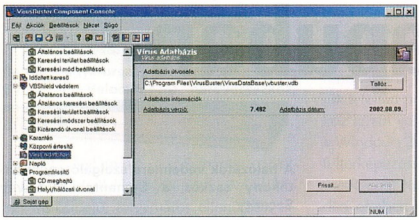
VirusBuster for Windows

Kipróbáltuk a VirusBuster család legtöbbek által használt tagját, a Windowsok alatt futó változatot. A problémamentes telepítés után a szokásos módon megjelenik az állandó védelmet biztosító *VBShield* pajzs ikonja a Windows tálcáján. Az ikon jobb egérgombos menüjéből közvetlenül elérhető a legfontosabb funkciók egy része, így például a víruskeresés, a program- és vírusadatállomány-frissítés, valamint a súgó. Elindítható innen a beállítások és mindennemű művelet elvégzésére használatos programablak is, a működési információk lehetőséggel pedig a pajzs addigi tevékenységéről kaphatunk képet.

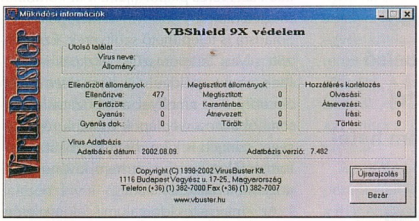


Az időzített víruskeresés megadására szolgáló ablak

A VirusBuster ablakának megjelenését többféleképpen konfigurálhatjuk. A windowsos programokat használóknak kicsit szokatlannak tűnhet a *Shortcut Bar*, ez a hierarchikus felépítésű ikonrendszer, amely afféle grafikus menüként működik. Ha azonban már hozzászoktunk, kiderül, hogy igen meggyorsítja a lehetőségek elérését. Ugyanezt a funkciót látja el az úgynevezett választólista, amely lényegében a Shortcut Bar szöveges megfelelője, kiegészítve egy, a keresési terület



Egy egérkattintással frissíthető a vírusadatbázis a készítésének időpontját mutató párbeszédablakból



Az állandó védelmet nyújtó VBShield pajzs működését leíró táblázat

megadására szolgáló könyvtárkezelővel. Egyszerre nem érdemes mind a választólistát, mind a Shortcut Bart használni. A programablak alján jeleníthetjük meg az elvégzett feladatokat mutató műveletlistát, míg az ablak nagy részét a választólistán vagy a Shortcut Baron megadott lehetőséghez tartozó párbeszédablak foglalja el. A műveletlistát, a választólistát és a Shortcut Bart a *Nézet* eszköztáron lévő ikonokkal jeleníthetjük meg, illetve tüntethetjük el. Az ablak tetején elhelyezkedő menü mindig a rendelkezésünkre áll, az eszköztárakat a Nézet menüben kapcsolhatjuk ki és be. A *Beállítások* menü tartalma helyzetérzékeny, attól függően változik, hogy a választólistán vagy a Shortcut Baron milyen lehetőséget jelöltünk ki.

Csakúgy mint a programablak egésze, a párbeszédablakok is jól áttekinthetők, a beállítási lehetőségek világosak. Ez részben annak köszönhető, hogy a magyar nyelvű kifejezések jól érthetők. Pofonegyszerű az állandó védelmet nyújtó pajzs működési jellemzőinek beállítása, valamint a kizárandó útvonalak és a víruskeresés célterületeül szolgáló meghajtók, illetve könyvtárak megadása. Aki mégsem értene valamit, igénybe veheti a minden részletre kiterjedő súgót, vagy tanulmányozhatja a VirusBuster webhelyéről letölthető, illusztrációkkal bőven ellátott, 47 oldalas, PDF formátumú felhasználói kézikönyvet. Bár a legtöbb felhasználónak nem kell változtatnia a víruskereső alapbeállításain, aki mégis módosítani akar valamit, alig ütközik nehézségekbe. Egy furcsaságot találtunk: ha cserélhető hordozójú meghajtót (például CD-ROM-olvasót) szeretnénk felvenni a kizárandó útvonalak listájára, ezt csak akkor engedi meg a program, ha a meghajtóban lemez is van. Alaphelyzetben a VirusBuster automatikusan vizsgálja a tömörítvényekben lévő állományokat is.

Automatikus frissítés

Mind a víruskereséshez, mind a programfrissítéshez (ez történhet CD-ről, hálózatról vagy FTP-kiszolgálóról) létrehozhatunk időzített feladatokat, amelyek az általunk megadott időpontban végrehajtják a kívánt műveletet. Így például előírhatjuk, hogy az ütemező minden este 8 órakor végezzen vírusellenőrzést a C meghajtón, és minden reggel 7-kor frissítse a vírusadatbázist. Az adatbázis frissítése manuálisan, gombnyomással is kezdeményezhető: ha újabb változatot talál a program a VirusBuster FTP-helyén, automatikusan letölti azt. A karanténba zárt (nem írható) vírusokat automatikusan ellenőrzi, és ha képes rá, írtja a vírusadatbázis frissítése után. Kérhető a vírusmentesített állományok visszaállítása is.

A programot ellátták beépített levelezőszolgáltatással, amelynek segítségével leveleket küldhetünk (például baj esetén a VirusBuster Kft. támogatási csoportjának), miután konfiguráltuk a levelező kliensünket. Az üzenettovábbító modul az előre definiált naplóbejegyzések (például vírust talált a program) bekövetkezése esetén üzenetet küld a megadott e-mail-címre.

Teljes körű támogatás

A VirusBuster Kft. az év minden napjára kiterjedő, 24 órás támogatást nyújt a vírusellenes csomag használóinak. Ha nem sikerül elhárítanunk a bajt, pár órán belül segítséget kaphatunk a cég szakembereitől. Képesek a vírusadat-állomány napi frissítésére, amivel a legmagasabb szintű biztonságra törekvők igényeit is maximálisan kielégítik.

A cég webhelyén **(www.virusbuster.hu)** hasznos információkhoz juthatunk a vírusokkal kapcsolatban. Magyar nyelvű tájékoztatókat olvashatunk a vírusfajták (boot, állomány, makró, szkript, féreg és trójai) jellemzőiről, az ábécé-rendbe szedett vírusadatbázisban az egyes vírusok leírását találjuk, és tanácsokat kapunk arra vonatkozólag, hogy mit kell tennünk adataink megvédése érdekében. Bekukkanthatunk a Magyarországon leginkább terjedő vírusok havi toplistáiba, a vírushírek archívumban pedig havi bontásban találjuk a legújabb kártevők felbukkanásáról szóló tudósításokat. Külön fejezetet szenteltek az e-mailben terjesztett hamis figyelmeztetéseknek *(hoaxoknak)*, amelyek nem fertőznek ugyan, viszont felesleges pánikot keltenek. Aki ismeretlen vírusba botlik, elektronikus vagy postai úton elküldheti azt a VirusBuster Kft. víruslaborjába, hozzájárulva ezzel az ellenszer mielőbbi megtalálásához.

A VirusBuster különféle változatainak próbaverzióit egy rövid regisztrációt követően a webhelyről is letölthetjük. A windowsos kiadás letöltési mérete 5,3, a friss vírusadatbázisé 1,5 Mbájt körül van. A 30 napos, teljes körű használatra jogosító regisztrációs kulcsot e-mailben kapjuk meg.

M. Cs.

Magyar nyelvű vírusleírások a VirusBuster webhelyén

Védelem a kapuban és mögötte

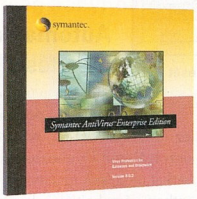
A hálózatok védelmére szolgáló egyik hatékony eszköz a Symantec Gateway Security

A vállalati hálózatokban is egyre jobban elterjednek az IP-alapú technikák. Ez egyben azt is jelenti, hogy a cég szervere hasonló eszközökkel védhető meg mind a belső – azaz cégen belüli –, mind pedig a külső rosszindulattól. A Symantec komplett eszközkészletet kínál a védelem hatékony megszervezésére.

Egyre több cég nyitja meg hálózatát a nagyvilág felé. A nagyvilág felé nyitott rendszerek esetében jelentős biztonsági feladattá vált a potenciális belépési pontok védelme.

Amennyiben nem egygépes, például otthoni „rendszerről" van szó, a belépési ponthoz odaültethetünk egy vagy több biztonsági őrt, akinek nincs más dolga, mint az itt folyó forgalom ellenőrzése. A kisebb hálózatok gazdáinak azonban megfelelőbb, ha „dobozos" termékkel, esetleg távolról felügyelt megoldással gondoskodhatnak a határőrizetről. Ezek azok a hardverelemként hálózatba csatlakoztatható *appliance* eszközök, amelyek közül néhányat hazánkban is bemutatott a *Symantec* 2002. júniusában, és amelyek részben az *Axent* egykori termékpalettájára alapozva, a *„Plug and Protect"* fejlesztési stratégia eredményeként kerültek a piacra.

A különböző méretű hálózatok védelmére szolgáló, hardveresen egy *Cobalton* futó terméksor tagjai a *Symantec Gateway Security,* a *Symantec Firewall/VPN Appliance,* valamint a *Symantec VelociRaptor.* Ezek legújabbjaiból aszerint választhatunk, hogy csak tűzfalat vagy ennél komplexebb megoldást akarunk-e telepíteni a rendszerünk védelmére. Operációs rendszerként egy Symantec által némileg testreszabott *Linux 2.2.x* kernel szolgál, amelyen a Symantec Gateway Security esetében vírusszűrés is működik.



A nagyvállalati vírusvédelemre fejlesztették ki a Symantec AntiVirus Enterprise Edition csomagot

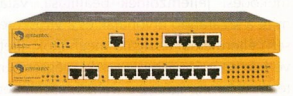
Ez a Symantec Gateway Security-val kapott *Carrier Class AV,* amelyben a korábban más Symantec-eszközöknél megismert *NAVEX* motor kap szerepet. A linuxos NAVEX motor már önmagában is figyelemre méltó, mivel a *Norton AntiVirusból* kiskereskedelmi, Linuxon használható termék nincs forgalomban. Így erre a platformra, otthoni használatra a Windows-os, illetve Macintosh gépekhez hasonlóan nem tudunk felszerelkezni a Symantec kínálatából.

A nagyobb rendszerek szoftveres felszereléséhez azonban már kapható linuxos termék, mivel a közelmúltban jelentették be a *Lotus Domino for Linuxra* szánt víruselhárító megoldást, a *Symantec AntiVirus 2.5 for Lotus Notes/Domino for Linuxot.* Ezzel a *Solaris,* az *AIX,* az *OS/400* és az *OS/390* után az említett csoportmunkaszoftver valamennyi platformján lehetőségünk van azonos termékkel megküzdeni a bináris kártevők ellen.

A Unix-rendszerek szoftveres biztonsági támogatása már nem annyira újdonság a Symantec termékeiben, mivel a nagyvállalatok szerveres platformjaira már korábban megjelentek a Windows mellett például a Solarisra is telepíthető szoftverek. Ezek között olyan tartalomszűrő eszközt is találunk, mint például a *Symantec Web Security 2.5,* amellyel a hálózatos forgalomból akár a weblapok és azok részegységei szintjén is kiszűrhetjük azokat az információkat, amelyeket nem kívánunk átengedni a hálózat határán.

Az internetes forgalom felügyeletére szélesebb körben alkalmazott szoftveralapú rendszerek a *tűzfalak.* Közülük a már említett Symantec Firewall/VPN Appliance külön hálózati hardverelem, de a tűzfal megvalósítására alkalmas megoldás külön telepíthető és „dobozos" szoftverként is beszerezhető. Ilyen a *Symantec Enterprise Firewall,* amely teljes eszközgyűjteményt kínál a Windows- és Solaris-alapú rendszereken megvalósított határvédelemre, mint ahogyan a Symantec Enterprise VPN lehetővé teszi a virtuális magánhálózat kialakítását. A nagyobb rendszerekben lényeges kérdés a nem kívánt forgalom kiszűrése és naplózása, de nem kevésbé lényeges a jogosult felhasználók azonosítása is. A Symantec eszközei a *Defender,* a *Radius,* a *Digital Certificates,* az *LDAP* és az *NT* doménalapú jogosítványvizsgálati szabványait egyaránt támogatják.

Természetesen a tűzfalakat a VPN-támogatáson kívül célszerű kiegészíteni a behatolási kísérletek szemmel követésével is. Amennyiben egy cégtől szeretnénk beszerezni a teljes vállalati rendszert, a korábbi komponenseket a *Symantec Intruder*



Az internetes forgalom felügyeletére szolgál a külön hardverelemként beszerezhető Symantec Firewall/VPN Appliance

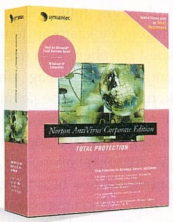
Immár Magyarországon is bemutatkozott a Symantec VelociRaptor hardvereszköz, amely a hálózatok biztonsága fölött őrködik

Alerttel, valamint a *Symantec NetProwlerrel* kell kiegészítenünk. Az előbbi egy valósidejű, folyamatos ellenőrzést kínál, amely kiegészül a teljes rendszerre érvényes biztonsági előírások érvényre juttatásával. Az utóbbi pedig a felhasználói tevékenységek folyamatos monitorozására alkalmas.

Mindkét feladat egyébként a központi kezelhetőséget feltételezi a rendszergazda számára. Ez a támogatás az IA esetében a rendszerszintű eseménykövetés mellett a rendszerszintű válaszok beállítását is jelenti, ami a jogosulatlan behatolások észlelésén kívül egyben jelentős korlátozás megvalósítását, a károk nagy részének megelőzését is lehetővé teszi. Platformként pedig a Windows NT mellett a legtöbb kereskedelmi Unix-verziót, valamint a Novell NetWare-t is támogatja.

Ahhoz pedig, hogy feltérképezzük a rendszerünk sérülékenységét, majd kezeljük a feltárt problémákat, szintén több eszköz közül választhatunk. A Unix, a Linux, a Windows 2000 és a NetWare rendszerek feltérképezésére például egyaránt a *NetRecont* használhatjuk. A kezelés minden esetben egy központi konzolról oldható meg. A teljes rendszer ISO 17799 alapú kezeléséhez pedig rendelkezésre áll a *Symantec Enterprise Security Manager*, amelynek alkalmazásmoduljai képesek az egyes kritikus alkalmazások és operációs rendszerek vállalati szintű figyelemmel kísérésére. A frissítésre pedig itt is rendelkezésünkre áll a *LiveUpdate* rendszer, amely az otthoni szoftverfrissítések alapjául is szolgál.

Az utóbbiak egyébként mintegy egygépes megfelelői a fentieknek, mint ahogyan a már említett Norton Antivirus is jó védelmet ad az otthoni eszközöknek, munkaállomásoknak, beleértve a levelekben terjedő kártevők elleni védelmet is. A tűzfalszolgáltatásokra pedig ott van a *Norton Internet Security*, amely különböző kiszerelésekben kapható, és amely valamelyest a tartalomszűrésben, illetve a személyes adataink védelmében is segít. A NIS dobozában egyébként szintén tartalmazza a Norton AntiVirust is, mely alapvető védelmi segédeszköz a *Norton SystemWorks* csomagban is megtalálható.



A Norton Antivirus Corporate Edition mindenfajta támadással szemben teljes védelmet kínál a vállalati hálózatok számára

Simay Endre István

Szigorúan őrzött szerverközpont

Néhány éve még nem sokan hallottak az úgynevezett kolokációs szolgáltatásokról. A szerverközpontok biztonságos elhelyezése komoly invesztíciót igényel, ezt a feladatot jobb egy erre szakosodott cégre bízni. Ilyen vállalkozás például a Dataplex, amely „bombabiztos" védelmet kínál mindenfajta informatikai infrastruktúra számára.

A robusztus, futurisztikus épület fehéren, titokzatosan terül el Budapest szívében, nem messze a Keleti pályaudvartól. Látszólag elhagyatott a környék, nincs nagy ki-be járkálás. Az idelátogatót azonban udvarias, ám annál szigorúbb őrség fogadja: a gépjárműveket átvizsgálják, tükrökkel ellenőrzik az alvázat, majd robbanásbiztos betonpillérek között engedik útjára. Vajon mit őriznek itt ennyire? Az itt tevékenykedő *Dataplex Kft.* talán a gazdaság legnagyobb értékeinek, az *információs rendszereknek* biztosít oltalmat.

A hazai viszonylatban még kuriózumnak számító, úgynevezett *kolokációs* szolgáltatás valójában igen egyszerű: a Dataplex adatközpontjában a cégek elhelyezhetik szervereiket, és biztonságos, megbízható infrastruktúrájú környezetben, a legkorszerűbb IT eszközökkel alakíthatják ki fontos központi üzleti rendszereiket (ERP, HRM, CRM stb.).

Az IT infrastruktúra azonban csupán az alap, amelyre a különböző emelt szintű szolgáltatások épülnek. Mint azt *Felsmann Balázstól*, a cég ügyvezető igazgatójától megtudtuk, a február óta a *Béres Befektetési Rt.* többségi tulajdonában álló Dataplex az elmúlt öt hónapban több szolgáltatást vezetett be, mint azelőtt összesen, a korábbi tulajdonos idejében. A Dataplex egyébként az egyetlen távközlési szolgáltatóktól független hazai kolokációs központ. *Kabay Panna*, a cég értékesítési menedzsere kalauzol végig a modern „erődítményben". Tartsanak velünk.

Fehér erődítmény a város szívében

Mint a filmekben

A szigorú, reptérihez hasonló beléptetés után megtudjuk, hogy a legnagyobb hazai adatközpontban járunk. A 8800 négyzetméteres alapterület jól felosztható: egyetlen rack-szekrénytől kezdve akár 1000 négyzetméteres, az adott céghez rendelt, elkülönített területet is ki lehet bérelni.

Megkétszerezett, biztonságos alállomásokon keresztül érkezik a városi hálózatról az áram, de az épületnek saját, önálló áramellátása is van: áramszünet idejére dízelgenerátorok is bevethetők, ezen felül szünetmentes áramforrások (UPS-ek) is gondoskodnak a maximálisan mintegy 8 MW-os teljesítmény folyamatos meglétéről. Az akkumulátorok végeláthatatlan sora meggyőzi a látogatót: a kisvárosnyi áramot fogyasztó létesítmény nem szenved energiahiányban.

Füstérzékelők, klímaberendezések, biztonsági kamerák mindenhol, rezgés-, ajtónyitás- és mozgásérzékelők, biometrikus azonosítók, mágneskártyás beléptetők – és ez csak néhány a védelmül szolgáló berendezésekből.

A biztonságos szerverekből szélessávú kapcsolaton keresztül jönnek-mennek az adatok: a Dataplexhez gyakorlatilag valamennyi jelentős hazai távközlési szolgáltató kiépített üvegszál-optikás csatlakozást, s ez azt jelenti, hogy tulajdonképpen korlátlan sávszélességgel lehet csatlakozni a világhálóhoz. A költségek miatt sem kell aggódni, a szabad választás a távközlési szolgáltatók között egyben a legkedvezőbb tarifák kiharcolásának lehetőségét is jelenti.

Az alapszolgáltatások között szerepel a

Kislexikon

Kolokáció: Az USA-ból indult ötletet már több magyarországi szolgáltató is megvalósította. A kolokációs központok tulajdonképpen helyet biztosítanak egy cég vagy vállalkozás, hivatal vagy akár magánszemély infokommunikációs eszközeinek, általában szervereinek. A biztonságos (fizikailag és szoftveresen őrzött) épületben elhelyezett kiszolgálókhoz a független kolokációs központokban több távközlési szolgáltató is kiépíti a szélessávú telekommunikációs kapcsolatot. A kolokációs központok másik fajtája szorosan kapcsolódik egy-egy távközlési szolgáltatóhoz, és a helybiztosítás tulajdonképpen egy plusz szolgáltatás az ügyfeleknek.

HRM: Human Resources Management, humánerőforrás- menedzsment; adatbázisába a cégek dolgozóinak személyes adatai, oktatása, képzése, a munkaerőszám-növelési, illetve csökkentési stratégiák kidolgozásának adatai kerülhetnek.

CRM: Customer Relationship Management, ügyfélelégedettség-menedzselés; a szolgáltató cégek egyik legfontosabb értéke az elégedett – és ezért visszatérő, hűséges ügyfél. Az ő megtartásuk érdekében kidolgozott stratégiai adatok, adatbányászati eredmények, adatbázisok képezik a CRM adatbázisának alapját.

ERP: Enterprise Resource Planning, vállalati erőforrás-tervezés; minden nélkülözhetetlen adatot tartalmaz, amely egy vállalat működéséhez szükséges (készlet-, eszköz-, anyagnyilvántartás, vevők, beszerzési és eladási információk stb.)

Szigorú beléptetési rendszer állja útját az autósoknak

terület biztosítása, a megfelelő tartalékokkal kialakított áramellátás, a légkondicionálás, a hatékony tűzészlelés és -oltás, illetve a folyamatos biztonsági és műszaki szolgálat. Ezekre épülnek a Dataplex *értéknövelt szolgáltatásai:* az üzemeltetési lehetőségek, az adattárolók elhelyezése, megőrzése és cseréje, az üzletmenet folytonossági szolgáltatás, illetve a tárterület bérleti szolgáltatás.

Az ügyfelek számára nagy előny, hogy a vállalkozásuk növekedésével roppant rugalmasan bővíthetik a bérelt területet, vagy változtathatják az igénybevett szolgáltatásokat.

Az ügyfelek skálája roppant széles: a távközlési, illetve internet-szolgáltatóktól (ISP-ktől) a legkülönbözőbb vállalkozásokig terjed. Az utóbbi időben egyre több nagyvállalat és multinacionális cég kerít sort például úgynevezett szerverkonszolidációra, azaz helyezi egységes hardver- és szoftveralapokra az országban esetleg elszórtan elhelyezkedő egységei eltérő informatikai rendszereit.

Diszkek vészhelyzetben

A Dataplex adatközpontjában – ez minden szerverhotelben alapszolgáltatás – 24 órás mérnöki felügyelet és folyamatos ügyféltámogatási rendszer gondoskodik a percre sem szünetelő üzemeltetésről, illetve az esetleges hibák gyors kijavításáról. Az itt elhelyezett szerverek felől tehát nyugodt lehet a vállalat vezetője, amit az utóbbi hónapok-évek néhány sajnálatos eseménye is bizonyít.

Prágában például az augusztusi árvíz miatt szerverparkokat kellett leállítani, a WTC-tragédia idején cégek komplett adatbázis-állományai semmisültek meg, de sajnos nem kell ilyen messzire mennünk hasonló esetekért: tavaly télen Budapesten kiégett egy optikai cikkekkel kereskedő cég irodája, s a lángok martaléka lett a fontos adatokat tároló winchester is.

Itt lép színre az úgynevezett *üzletmenet folytonossági szolgáltatás (Business Continuity, BC),* amellyel elsősorban azok a cégek élhetnek, amelyeknek az adatvesztés egyben tetemes haszonkiesést is jelenthet (például bankok, pénzintézetek, biztosítók, multik stb.).

A szolgáltatás különböző szinteken valósulhat meg: egyszerűen az ügyfél kérésére összeállított konfigurációjú gépeket és irodai felszerelést biztosítanak, vagy akár az online kapcsolat segítségével folyamatosan tükrözik a vállalati rendszereket, és vész esetén azok pontos mása várja a munkatársakat a központban.

Világelső adatkicserélő

A február óta a Dataplexnél működő, Magyarország első kereskedelmi *Internet Exchange* központjában az internet- szolgáltatók gyorsan, hatékonyan, az úgynevezett *peering* szolgáltatás keretében tudják kicserélni adataikat. A *PAIX. net Inc.* Európában elsőként itt honosította meg *Layer 2* kapcsolástechnikai infrastruktúráját, internet-kapcsolati lehetőségeit és a cég peering szolgáltatásait.

A *„Peering by PAIX"* ötlet arra épült, hogy regionálisan nem létezett megbízható kereskedelmi internet-kicserélő központ, bár erre komoly igény mutatkozott, elsősorban a távközlési, illetve internet-szolgáltatók részéről. A szolgáltatás lényege az, hogy a nagyobb felhasználók egy portot vásárolnak az eszközön, és helyben kicserélhetik egymást között az adatokat. A másodpercenként akár 1 gigabit sebességű Ethernet port által biztosított sávszélességgel és átviteli kapacitással kereskedhetnek is az ide csatlakozó ISP-k. Ez nemcsak gyorsítja az internetezést, ami ma már alapkövetelmény, de a szabályozásnak köszönhetően kizárt a kalózkodás, a vírusterjesztés, illetve a spam levelek küldése és fogadása is. Ráadásul a kapcsolat megbízhatóvá

Ezekben a cellákban helyezik el az eszközöket

Dataplex történelem

A *CityReach* befektetési csoport építette és adta át 2000 decemberében a világ legkorszerűbb technológiai felszereltségével bíró budapesti szerverhotelt. Az azóta csődbe ment cégtől a *Béres Csoporthoz* tartozó *Dataplex Kft.* idén januárban stratégiai befektetésként vásárolta meg annak eszközeit, és vette át személyi állományát. Idén júliusban 359 millió forintos tőkeemeléssel hosszú távra biztosította a Dataplex megbízható működtetését és piacvezető szerepének megőrzését.

válik, hisz a helyi internet-kicserélő központ leállása esetén nem kell leterhelni a kimenő nemzetközi sávszélességeket a helyi internetes adatforgalommal.

Ez a budapesti cég akár a közép-

Az oltógáz nem tesz kárt a merevlemezekben

kelet–európai régió adatkicserélő központjává is válhat a Dataplex kapacitását és kihasználtságát figyelembe véve.

Mégis, kinek az üzlete?

Felsmann Balázs, a Dataplex ügyvezetője szerint idén év végére éri el a cég a költségek megtérülését, és jövőre már 650 millió forintos éves bevétel mellett tisztes haszonra is számítanak.

A partnereikkel a tárgyalások megkezdése és a szerződéskötések között meglehetősen hosszú idő telik el, de a kezdeti nehézségek után partnerszámuk szépen emelkedik.

A nemrégiben történt 359 milliós tőkeemelés, az ügyvezető személye (F. B. a Béres Befektetési Rt. igazgatótanácsának is tagja) mind azt bizonyítják, hogy a Béres komoly stratégiai befektetésként kezeli a Dataplexet, s ez mind a dolgozók, mind az ügyfelek számára megnyugtató hátteret jelenthet.

F. Fülöp Hajnalka

Észrevétlen biztonság

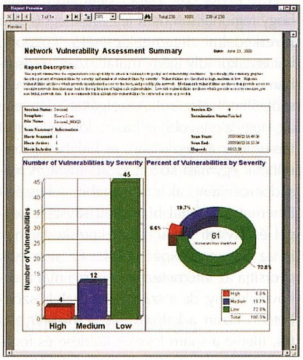
A biztonsági szoftverek vezető fejlesztőjeként ismert ISS termékeit forgalmazó Noreg Kft. teljes körű információvédelmi szolgáltatást, tanácsadást és oktatást kínál ügyfeleinek.

A *Noreg Információvédelmi Kft.* **(www.noreg.hu)** 1998-ban alakult, fő tevékenysége a sérülékenység-vizsgáló és behatolás-észlelő szoftverek területén piacvezető *Internet Security Systems (ISS*, **www.iss.net**) termékeinek forgalmazása, telepítése, valamint a felhasználók oktatása volt. 1999 októberétől a cég a *Montana Rt.* leányvállalataként működik. 2001 májusában a Montana teljes információvédelmi részlege a Noreghez került át, s ennek köszönhetően ma már mindenre kiterjedő információvédelmi szolgáltatásokat tudnak nyújtani. Tevékenységeiket két üzletágba szervezték. Az *IT biztonságtechnikai* üzletághoz az ISS termékeire épülő szolgáltatások mellett a biztonságos hálózati kommunikáció, a hozzáférés-védelem, a vírus- és tartalomszűrés, a rejtjelezés, az elektronikusaláírás-hitelesítés területei és az ezekhez kapcsolódó oktatás tartozik, míg a *tanácsadói* üzletág információbiztonsági auditálással, biztonsági stratégiák, szabályzatok kidolgozásával és tanácsadással foglalkozik. Az év elejétől a Noreg az ISS hivatalos oktatóközpontjaként működik, ahol a partnercég előírásai szerint folyik az oktatás, és hivatalos képesítés szerezhető.

Tervszerű megelőzés

Az ISS termékeire épülő szolgáltatások alapvetően két részre bonthatók: a sérülékenység-vizsgálatra és a behatolás-észlelésre. A sérülékenység-vizsgálat során a *SAFEsuite* biztonságmenedzselő platformhoz tartozó szoftverekkel térképezik fel az informatikai rendszer gyenge pontjait. A programok egy veszélyforrás-adatbázis alapján dolgoznak, amelyet az ISS mintegy 100-fős *X-force* **(xforce.iss.net)** gárdája rendszeresen bővít a folyamatosan nyilvánosságra kerülő programhibákkal, sérülékenységi pontokkal, hacker módszerekkel.

Az *Internet Scanner* afféle jóindulatú hackerként kívülről teszi próbára a vizsgált rendszert. Szondázza a kommunikációs szolgáltatásokat, az operációs rendszereket, a kulcsfontosságú alkalmazásokat és a routereket, olyan sérülékenységek után kutatva, amelyek támadások célpontjai lehetnek.



Az Internet Scanner részletes jelentései jól áttekinthető formában közlik a rendszer vizsgálata során szerzett információkat

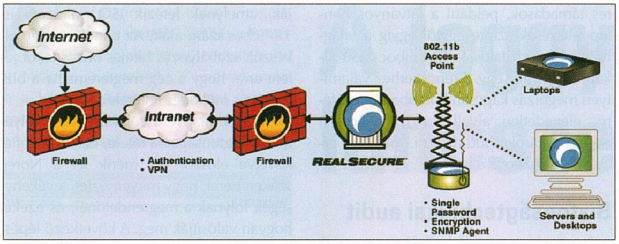
Belső vizsgálatokra használatos a *System Scanner*, amelynek ügynökeit a Unix vagy Windows NT hálózat gazdagépeire telepítik. Ez áttekinti a jogosultságokat, a jelszóbeállításokat, és tanácsokat ad arra vonatkozólag, hogy milyen javítások szükségesek, illetve milyen szigorításokat kell életbe léptetni.

Oracle, Microsoft SQL és Sybase adatbázisok jogosultságkezelésének, hitelességének és sértetlenségének biztonsági elemzését végzi a *Database Scanner*. Azonosítja és jelenti a biztonsági politikától való eltéréseket és a veszélyforrásokat. Részletes beszámolót készít, amelynek alapján helyesen konfigurálhatók és biztonságosabbá tehetők az adatbázis-kiszolgálók.

A *vezeték nélküli hálózatok* sérülékenységének vizsgálata új színfolt az ISS palettáján. A vállalatoknál mostanság divatba jövő vezeték nélküli kapcsolódás rendkívül elegáns és kényelmes megoldást kínál a hálózatépítésre. Nincs szükség kábelezésre, a felhasználó leül az íróasztalához, bekapcsolja a gépét, és az épületben elhelyezett adó-vevőn keresztül automatikusan rákapcsolódik a hálózatra. Ahogy azonban lenni szokott, a gyártók elsősorban a technológia működőképességének biztosítására törekszenek, és a biztonsági kérdésekkel nem sokat törődnek. Hiába van egy cégnek többmilliós értékű tűzfala, ha ezt egy vezeték nélküli porton keresztül meg lehet kerülni, az egész nem ér semmit. Az ISS válasza erre az új kihívásra a *Wireless Scanner*, amely a vezetékes hálózatoknál használt szkennerekhez hasonlóan teszteli a hálózat sérülékenységét.

Folyamatos őrzés

A különféle szkennerek pillanatfelvételt készítenek a rendszer állapotáról, amelyet kiindulási pontként lehet használni. A mai informatikai rendszerek azonban állandó figyelést igényelnek, hiszen nap mint nap fény derül valamilyen programhibára, sérülékenységre vagy új hacker-technológiára. A *RealSecure* behatolás-észlelő



Vezeték nélküli hálózatok sérülékenységét vizsgálja a Wireless Scanner

szenzorok veszély esetén automatikusan beavatkoznak, és megakadályozzák, hogy a támadó kárt okozhasson. Támadáskor többféle dolgot tehetnek: például riasztha tnak, megszakíthatják a kapcsolatot, átkonfigurálhatják a tűzfalat, vagy kitilthatják a támadót a rendszerből.

Tűzfalak előtt, mögött, behívó eszközöknél telepítve hálózati szegmensek teljes forgalmának figyelésére szolgál a *Network Sensor*. Egy adott gazdagép bejövő és kimenő forgalmát vizslatja a gazdagépre telepített *Server Sensor*. A szenzorok központi vezérlését, konfigurálását, beszámolók készítését és riasztások kiadását végzi a *Workgroup Manager*.

Annak érdekében, hogy a behatolás-védelem ne terhelje le túlságosan a kiszolgálókat és a hálózatot, célszerű a figyelést azokra a különféle okokból – például nem jelent még meg a javítás, vagy a sérülékenység befoltozása zavarokat okozna a működésben – nem megszüntethető sérülékeny pontokra irányítani, amelyeket a sérülékenység-vizsgálat felfedett. Nincs értelme ugyanis olyan támadások kivédésére felkészülni, amelyekről biztosan tudjuk, hogy semmi esélyük a behatolásra.

Másfelől azonban a sérülékeny-vizsgálat során rengeteg információ keletkezik, kiderülhet például, hogy az egyik szerveren száz sérülékenység található, egy másikon pedig csak kettő. Első látásra úgy tűnik, hogy minden védelmet a lényegesen sérülékenyebb kiszolgálóra kell összpontosítani. Ha viszont a behatolás-detektálás azt állapítja meg, hogy a száz sérülékenységet soha nem támadja senki, a másik kettőnél viszont állandóan próbálkoznak, akkor egészen máshogy fest a helyzet. Ezért olyan eszközök kellenek a biztonsági menedzserek kezébe, amelyek segítenek kihámozni az érdemi információt a keletkező adathalmazból.

Az ISS két megoldást kínál ezen a területen. A nagyvállalatok számára készült *SafeSuit Decisions* a különböző forrásból származó sérülékenységi, tűzfal- és behatolásvédelmi információkat adatbázisba gyűjti, amelynek alapján korrelációs jelentések készíthetők. Ezek megmutatják azokat a gyenge pontokat, amelyekre a védelmet összpontosítani kell. Hasonló szolgáltatásokat kínál a kisebb cégek számára az olcsóbb *Site Protector* rendszer, amelynek hatásköre egyelőre csupán az ISS termékeire, azon belül is az *Internet Scannerre* és a behatolás-észlelő szenzorokra terjed ki.

Desktop védelem

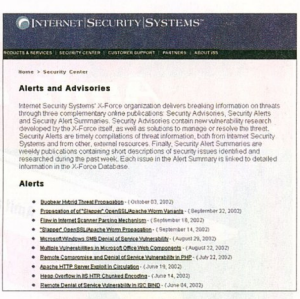
A kiszolgálók és a teljes hálózat védelme megoldott a Network Sensor és a Server Sensor révén, de mi a helyzet az egyre több értékes információt tároló munkaállomásokkal? Egy vezető beosztású alkalmazott otthoni gépén vagy notebookján éppolyan fontos információk találhatók, mint a szigorúan védett szervereken. Amikor aztán az illető védtelen vagy csupán egy egyszerű személyi tűzfallal védett gépével rácsatlakozik az internetre, könnyű prédájává válhat a hackereknek. És ha feltört gépével egy egyébként igen biztonságos virtuális magánhálózaton keresztül lép be a munkahelyi hálózatba, a behatoló ellenőrzése alá vonhatja a teljes hálózatot is.

A teljes körű védelem kialakítása érdekében az ISS tavaly megvásárolta az asztali gépekre szánt *BlackIce* személyi behatolás-védelmi és tűzfalmegoldást fejlesztő *Network Ice* céget. A vállalati környezetekben való alkalmazhatóság érdekében kiegészítette a programot központi vezérelhetőséggel, és jelenleg folyik ennek az illesztése a meglévő behatolás-észlelő szenzorok központi vezérléséhez. A *Desktop Protection* névre keresztelt termék központilag vezérelhető, konfigurálható és frissíthető, a program a begyűjtött információkat a központba továbbítja, míg veszély esetén önállóan tud beavatkozni, akkor is, ha éppen nincs kapcsolatban a központi vezérléssel, a felhasználó közreműködése nélkül.

A személyi tűzfalaknál és behatolás-detektáló programoknál gondot jelent, hogy a többnyire hozzá nem értő felhasználónak kell beállítani és kezelni őket. Ez vállalati környezetben nem biztonságos, és nem is lehet elvárni a munkatársaktól, ezért van szükség a központi felügyeletre. Magyarországon is terjed a távmunka, így a desktop védelem egyre nagyobb érdeklődésre tarthat számot a cégek körében.

Kettőzött páncélzat

Összefoglalásképpen tekintsük át, hogyan történik az ISS eszközeivel egy vállalat biztonsági rendszerének a javítása. Két fő tevékenységet különböztethetünk meg. Az egyik egy folyamatosan zajló *tervszerű megelőző munka*, amelynek során feltérképezik és kijavítják a sérülékenységeket.



A legfrissebb riasztások a hecker-ellenes kommandó, az X-Force webhelyén

Amikor egy cégnél először történik sérülékenység-vizsgálat, rengeteg hiányosságra derül fény, amelyeket mind ki kell javítani. Ez az úgynevezett rendszererősítési *(hardening)* folyamat, amely egy idő után eljut arra a szintre, amikor a szkennerek már nem találnak csak egy-két alacsony vagy közepes prioritású sérülékenységet, amellyel együtt lehet élni. A következőkben a feladat a szinten tartás, amely további rendszeres ellenőrzést igényel. Ennek az egyik oka az, hogy változik az környezet, például újabb gépek, szoftverek kerülnek a hálózatba, aminek eredményeképpen újabb biztonsági rések jelenhetnek meg. A

másik ok az, hogy állandóan újabb sérülékenységekkel bővül a szkennerek adatbázisa az ISS X-force csapata jóvoltából. A szinten tartás jóval kevesebb munkával jár, mint a hardening.

Párhuzamosan működik a másik fő tevékenység, a *valós idejű behatolás-detektálás*, amely folyamatosan figyeli, hogy mi történik az adott környezetben, milyen módon sértik meg a biztonsági politikát. Minden támadást feljegyez, nem csak azokat, amelyek a sérülékenységek ellen irányulnak. Veszély esetén automatikusan beavatkozik, és különféle módszerekkel megakadályozza a károkozást. Természetesen száz százalékos biztonság nem létezik, a megrendelőnek kell eldöntenie, hogy adatainak biztonsága milyen szintű beruházásokat ér meg neki.

Érdemes megemlíteni, hogy a statisztikák szerint a sikeres támadások mintegy 70 százaléka belülről jön. Nem az internet jelenti tehát a legnagyobb veszélyt egy informatikai rendszerre, annak ellenére, hogy a legnagyobb publicitást kapó sikeres támadások, például a látványos honlap-feltörések szinte egytől egyig a világhálóval kapcsolatosak. Egy elbocsátott alkalmazott vagy egy, a rendszerhez valamilyen megbízás kapcsán korábban hozzáférő, elégedetlen alvállalkozó lényegesen nagyobb károkat tud okozni, mint egy érzelmileg közömbös hacker.

Biztonságtechnikai audit

Minden technikai megoldás akkor működik a leghatékonyabban, ha mögötte egy szabályozott környezet található. Ennek kialakítása egy cégnél úgy kezdődik, hogy megvizsgálják, milyen információk birtokában vannak, ezeknek mi az értéke, megóvásuk érdekében indokolt-e pénzt költeni védelmi megoldásra, és ha igen, a védelem milyen szintű legyen. A Noreg tanácsadói üzletága ehhez nyújt hathatós segítséget azzal, hogy kockázati szempontból megvizsgálja a megrendelő informatikai rendszerét. A vizsgálathoz a *BS 7799*-es nemzetközi szabványt használják, amelynek létezik ISO változata is, *17799*-es szám alatt. Az ennek alapján elkészült szabályozás hiteles biztosítékot jelent arra, hogy a cég megteremtette a biztonságos működés feltételeit.

A cégek alapvető célja az üzleti folyamatok biztonságossá tétele, ezt a filozófiát követve először azt mérik fel a Noreg szakemberei, hogy milyen üzleti tevékenységek folynak a megrendelőnél, és ezeket hogyan valósítják meg. A következő lépésben azt határozzák meg, hogy milyen kockázatokkal járnak ezek az üzleti folyamatok, és megoldást adnak a kockázatok minimalizálására, amelyet egy információvédelmi kézikönyv rögzít.

A végső döntés a megrendelő kezében van. Határozhat úgy, hogy a biztonsági szabályzatok kidolgozása és betartatása megfelelő védelmet nyújt adatai számára, kérhet bizonyos időközönkénti sérülékenység-vizsgálatot a rendszerben lévő támadható pontok kiszűrésére, és választhatja a legmagasabb szintű védelmet nyújtó behatolás-detektálást. **M.Cs.**

A leggyengébb láncszem

A nemzetközi biztonságtechnikai piacon elvétve már alkalmazott informatikai biztonsági vizsgálatot végzett az egyik hazai nagybanknál a telnet Magyarország Rt. informatikai biztonság divíziója. A technikai információkkal megtámogatott adatvédelmi szakemberek ezúttal nem a megszokott informatikai úton, hanem a „leggyengébb láncszem" – az ember – hibáinak kihasználásával szimuláltak hacker-támadást.

A *Social Engineering* típusú vizsgálat során a szakértők – színészek, médiában gyakorlatot szerzett kommunikációs szakemberek – elsősorban arra a kérdésre keresik a választ, hogy a „megtámadott" cég munkatársaival folytatott beszélgetések során mennyi érzékeny

A telnet ügyfelei a szolgáltatások gazdag választékából meríthetnek

műszaki információhoz juthat hozzá az esetleg rossz szándékú támadó. Ezután már technikai jellegű vizsgálatok során derítik ki a magas műszaki felkészültségű munkatársak, hogy a megszerzett információ segítségével milyen technikai mélységekig sérülhet az ügyfél számítógépes rendszere.

Az első ilyen vizsgálat átütő sikert hozott. Az „áldozat", egy közelebbről meg nem nevezett hazai nagybankunk szakemberei a következtetések levonásával úgy tudták nagymértékben megnövelni a biztonságot, hogy az eddig felderítetlen terület kockázatait pontosan felmérve, felesleges költségek nélkül a leghatékonyabb védelmi struktúrát alakíthatták ki.

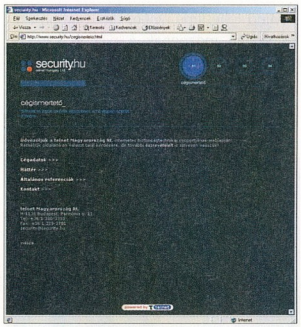
Amerikában és az évszázados banki hagyományokkal (is) büszkélkedő nyugati demokráciákban komoly múltja van ennek a fajta tevékenységnek. Az e módszert alkalmazó sikeres hackerek közül a legismertebb talán *Kevin Mitnick*, akit több állam számítógépes rendszereibe való behatolásért ítéltek el 1995-ben. Módszerének az a lényege, hogy az emberi hiszékenység és bizalom kihasználásával, valamint a megszerzett informatikai ismeretek birtokában súlyos anyagi kárt lehet okozni a profitorientált vállalatoknak és a kormányzati intézményeknek is.

A *telnet Magyarország Rt.* meglévő partnerei már az előzetes információk alapján is élénken érdeklődtek a szolgáltatás iránt, így a cég már a bevezetést követő hetekben is számos hasonló vizsgálat elvégzésére kapott megbízást.

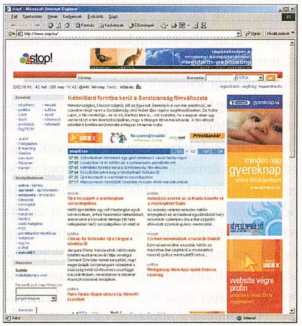
Kövesi Orsolya

telnet Magyarország Rt.

Az 1996-ban alapított *telnet Magyarország Rt.* egyike a legnagyobb hazai internetes társaságoknak. Tevékenységei közé tartozik az internet hozzáférés-szolgáltatás, a tartalom- és website-fejlesztés és kezelés, továbbá a hálózati biztonságtechnika, elsősorban a közepes és nagyvállalatok, illetve internetes cégek számára. A telnet Magyarország Rt. tulajdonában van a *stop!*, az egyik legnépszerűbb hazai általános portál. Főbb ügyfelei közé tartozik a *CIB Bank*, a *Colliers*, a *Concorde Direct*, a *Danubius Rádió*, az *EMI Music*, a *GlaxoSmithKline*, a *HBW Express*, a *HypoVereinsBank*, az *IBM Magyarország*, a *Klubrádió*, a *Pannon GSM*, a *Portfolio.hu*, a *Roxy Rádió*, a *Sun Microsystems* és a *Well*.



A Security.hu nem más, mint a telnet informatikai biztonság divíziója



A Stop! ma is a leglátogattottabb portálok egyike

Emberközpontú védelem

Nem múlik el nap, hogy ne hallanánk hacker-támadásokról. A vállalatokat érzékenyen érinti, ha bizalmas adataik elvesznek vagy kitudódnak. A kis és közepes cégeknek a hazai fejlesztésű PingWINet HSS biztonsági rendszer nyújt hatékony védelmet az illetéktelen behatolók ellen.

A vállalatok adatállományát fenyegető *hackerek* egy része nem okoz különösebb kárt: a rendszer feltörése után elkönyvelik a sikert, majd tájékoztatják a rendszergazdát a felfedezett hibáról. Többnyire találomra választják ki a célrendszert, és egyedül dolgoznak.

A másik csoportba tartozó hackerek annál kártékonyabbak: adatokat töltenek le a feltört rendszerről, lecserélik a weboldalakat, és hátsó bejáratokat alakítanak ki, hogy a későbbiekben vissza tudjanak térni akkor is, ha kijavították a rendszer hibáit. Sok esetben a feltört rendszereket átjárónak használják egy nagyobb betörés fedezésére. Általában csoportosan hajtják végre akcióikat, előzetes felmérés alapján választják ki a célrendszert, és nagy nyilvánosság előtt hirdetik önmagukat.

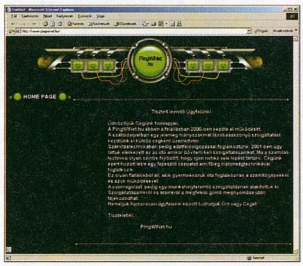
Tudásszintjük alapján ugyancsak osztályozhatjuk a hackereket. Az úgynevezett *script kiddyk* a mások által megtalált és nyilvánosság elé tárt hibákat használják ki. Átvizsgálják a célrendszert, és ha a rendszergazda nem tud a hibáról vagy nem javította ki azt, megpróbálnak bejutni a rendszerbe. Általában nem ismerik jól a célrendszert, így elég sok nyomot hagynak maguk után, és előfordulhat az is, hogy akaratlanul rendszerösszeomlást idéznek elő. Sok időt töltenek a feltört a rendszerben az illegális jogosultságokkal, és többször visszatérnek.

Az elit osztályba tartozó hackerek magas szinten ismerik az alapvető programozási nyelveket (Assembler, C, Delphi) és az operációs rendszereket. Hibák után kutatnak az új rendszerekben, programokban, és a felfedezett hibákat többnyire ők publikálják a különböző biztonsági fórumokon. A célrendszert saját tudásuknak megfelelően választják ki előzetes tanulmányozás alapján. Legtöbbször a saját maguk által felfedezett hibákat kihasználva törik fel a rendszert, és szinte teljesen nyomtalanok maradnak. Megkeresik a számukra fontos információt, letöltik, majd távoznak. Mivel felsőfokon értenek a célrendszer operációs rendszeréhez, véletlenül sem okoznak összeomlást.

Mindkét hackertípus komoly veszélyt jelent. Ha a rendszergazda biztonsági szempontból naprakészen karbantartja a rábízott rendszert, akkor a script kiddyk nem okozhatnak gondot. Az elit osztályba tartozókkal alapvetően más a helyzet, mivel ők mindent megtesznek annak érdekében, hogy bejussanak, és igen rövid idő alatt sikerrel is járnak. Náluk a lebukás veszélye minimális, nem úgy mint a script kiddyk esetében.

Védekezési eszközök

Mind teljesítményben, mind árban széles skálán mozognak a piacon kapható biztonsági megoldások. Legtöbbször operációsrendszer-függőek, leggyakrabban Windows NT-hez és 2000-hez készülnek. Sok cég foglalkozik úgynevezett *biztonságtechnikai audittal*, amely az ügyfél rendszerének átvizsgálását jelenti. Megpróbálják megkeresni a rendszerben lévő hibákat, réseket, és kijavítják őket. A biztonságtechnikai audit történhet úgy is, hogy a rendszergazda letölt egy auditáló programot, amely ismeri a már felfedezett hibák nagy részét, majd e szoftver segítségével átvizsgálja a hálózatát.



A PingWINet saját biztonsági rendszerét ajánlja a kis és közepes vállalatoknak

Miután a megrendelő előzetes tájékozódás után kiválasztotta a neki megfelelő biztonságtechnikai megoldást, saját rendszergazdájára bízza a telepítést, hangolást. Amennyiben kaptak vagy vásároltak terméktelepítési segítséget, akkor legfeljebb 30 napig segítenek a telepítő személyzetnek, a későbbiekben a rendszergazda gondozza, frissíti a rendszert.

A biztonságtechnikai megoldások legnagyobb hibája, hogy ezek a szoftverek bárki számára elérhetők, így a hackerek számára is, akik megpróbálnak hibát találni bennük, és azt kihasználva bejutni azokba a rendszerekbe, amelyekben ezt a szoftvert használják.

A másik nagy probléma az, hogy a szoftvereket sok esetben nem biztonsági szakember gondozza, hanem egy erre a célra betanított rendszergazda. Ráadásul a cégnél dolgozó munkatársak nagy része tudja, hogy milyen biztonsági szoftvert használnak, ami ugyancsak támadási felületet jelenthet. Előfordulhat az is, hogy a rendszer biztonságát szinte a teljes használhatatlanságig fokozzák, vagyis a legtöbb kényelmi szolgáltatást, valamint az internet elérését szűrik, korlátozzák, tiltják.

Biztonsági audit

A *PingWINet* **(www.pingwinet.hu)** szakemberei csak az audit kisebbik részét végzik az erre a célra kifejlesztett hibakereső szoftverrel. A vizsgálat nagyobbik része teljesen emberközpontú, ennek köszönhetően jóval nagyobb az esély arra, hogy a

rendszerben megbúvó hibákat felfedezzék. A vizsgálatot az elit hackerosztály tudásával felvértezett szakemberek végzik, akik bizonyítottan jártasabbak ezen a téren, mint egy szoftver, amely közel sem tudja követni egy hacker gondolatmenetét.

Első körben a rendszer hardver-összeállítását vizsgálják, a vizsgálat kiterjed a kiemelt funkciókat ellátó eszközökre, a hubokra, switchekre, routerekre és kiszolgálógépekre. A hardvereszközöket azért szükséges átvizsgálni, mivel a legtöbb egység (kivéve a számítógép hardverelemeit) távolról menedzselhető, így jogosulatlan irányítás alá vonható. A kiszolgálógép esetében arra keresnek választ, hogy annak teljesítménye elegendő-e a rábízott feladatok elvégzésére. A következő lépcsőben a rendszert az interneten keresztül kívülről vizsgálják meg. Megnézik, hogy a kívülről elérhető szolgáltatások biztonságosak-e. A megrendelő hozzájárulásával, kívánsága szerint az ő jelenlétében megpróbálják manipulálni, feltörni a publikus szolgáltatásokat, anélkül, hogy a rendszert megbénítanák, megrongálnák vagy működésében akadályoznák. Minden sikeres és sikertelen próbálkozásról pontos dokumentáció készül, amelyet kizárólag a megrendelő láthat.

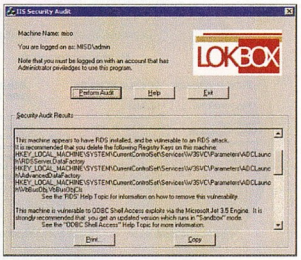
Mindezek után következik a belső rendszer vizsgálata. Ha egy olyan rendszerről (például egy webkiszolgálóról) van szó, amelyet folyamatosan használnak, a vizsgálatot végző szakemberek normál felhasználói jogosultsággal megpróbálják belülről manipulálni a rendszert és annak elemeit, amiről szintén pontos dokumentáció készül.

A vizsgálatok befejezése után konzultáció zajlik az ügyféllel a tapasztaltakról a hibák kijavítása érdekében. Valamennyi beavatkozás kizárólag az ügyfél hozzájárulásával történhet, és ha sikerül feltörni a rendszert, a helyben tárolt adatokba nem néznek bele, és nem törlik a naplóállományokat. A talált hibát kihasználó programot vagy annak forráskódját nem adják át az ügyfélnek, és törlik azt. Erre azért van szükség, hogy az esetleg még nem publikált hibáról harmadik fél ne szerezhessen tudomást, és ne használhassa máshol ártó szándékkal.

Linux- és UNIX-alapú szoftveraudit

Kevésbé közismert, hogy egy szoftver is lehet támadási felület, de ez ellen is lehet védekezni. Egyre inkább terjed a Linux, a UNIX, s egyre több cég ír programokat ezekre az operációs rendszerekre. Ha a programozás során nem tanúsítanak kellő figyelmet, előfordulhat, hogy egy program segítségével valaki kívülről vagy helyben illegális hozzáférést tud megvalósítani. Ennek elkerülése érdekében a PingWINet szakemberei vállalják az új programok biztonságtechnikai felülvizsgálatát. A vizsgálathoz nincs szükség a forráskódra.

Különböző technikákkal megpróbálják a programot a megszokott működéstől eltéríteni, és illegális jogosultságokkal megemelni a normál felhasználó szintjét. Mindezt a PingWINet saját fejlesztésű programokkal végzi. Siker esetén pontos dokumentáció készül, és elvi javaslatot tesznek a hiba kijavítására. A talált hibát nem hozzák nyilvánosságra, továbbá a hibát kihasználó programot és annak forráskódját nem adják át az ügyfélnek.



Az IIS Security Audit a Windows 2000 Server konfigurációkban deríti fel azokat a biztonsági réseket, ahol a hackerek a Microsoft Internet Information Server (IIS) segítségével tudnak behatolni a rendszerbe

HSS biztonsági rendszer

A PingWINet hat éve foglalkozik e nagyrészt saját fejlesztésű rendszer kidolgozásával és gondozásával. A HSS-t felszereléknek valamennyi fontosabb kényelmi szolgáltatással, és nincs észrevehető korlátozás a rendszer védelme érdekében. Nem kell lemondani az alapvető internetes szolgatatásokról, mint például egy proxyt használó védelmi rendszerben, hacsak nem az az ügyfél kifejezett kérése, hogy korlátozzanak bizonyos funkciókat.

A szoftver nem kerül kereskedelmi forgalomba, a telepítést a PingWINet szakemberei végzik, csakúgy mint a rendszer gondozását. Harmadik fél a HSS-t nem telepítheti, abba betekintést nem nyerhet, és nem is adminisztrálhatja azt.

A HSS rendszer Linuxra épülő, ügyfél-kiszolgáló alapú megoldás. Az ügyfélgép (lehet több is) az az egység, amely fizikailag a megrendelőnél helyezkedik el, annak hálózata előtt, mint egy tűzfal. Ehhez a számítógéphez csatlakozik a megrendelő belső hálózata, valamint ez a gép látja el az alapvető routolási és egyéb szolgáltatásokat. Lokális védelmi rendszerébe csupán a már felfedezett hibákat táplálták be, az ezek mentén történő próbálkozásokat naplózza és 100 százalékos biztonsággal elhárítja. Emellett folyamatosan adatokat gyűjt a rendszer állapotáról, valamint az élő kapcsolatokról, folyamatokról.

Az ügyfélgépek által összegyűjtött adatok valós időben, erős titkosítással, az interneten keresztül bekerülnek a HSS központi gépeibe. Minden egyes ügyféloldal mögötti rendszer életét és szokásait rögzítik, és bármikor, bármilyen eltérés azonnal észrevehető az adatok elemzése közben. A központi gépeknél a PingWINet munkatársai figyelik a rendszert a nap 24 órájában, aminek eredményeképpen a behatolás lehetősége minimális, és probléma esetén azonnal megkezdődik az elhárítás, így a támadónak nem marad esélye a rendszer feltérképezésére. Az automatizálás csak a minimális szükségesség határáig terjed, a vezérlés nagyrészt emberi.

Az ügyfél igényeit a lehető legrövidebb időn belül teljesítik. Korlátlan számú és bármilyen operációs rendszerű belső számítógép csatlakozhat az ügyféloldali HSS rendszerhez, mivel itt csak az ügyfélhardver feltételei szabnak határt. Kérésre belső szervereket is üzemeltethet a megrendelő, amelyeket kívülről is el lehet érni megfelelő kritériumok alapján. A legfrissebb fejlesztéseket és frissítéseket automatikusan felteszik az ügyféloldalra.

A HSS rendszerbe beépítettek egy levelezési szervert, amely vírusszűrést is végez, mivel manapság a rendszerek megbénulásának 90 százalékáért a levélben terjedő vírusok a felelősek. A vírusok elleni védelem tehát szerves része minden ügyfélgépnek, erre a célra a *McAfee* cég mindenkori legfrissebb termékét használják.

Igény esetén lehetőség van virtuális magánhálózat kialakítására, amelynek révén a megrendelő munkatársai úgy dolgozhatnak a világ bármely pontján az internet segítségével, mintha az irodában a tűzfal mögött ülnének. **-ba**

Cégre szabott védelem

Hogyan épül fel egy korszerű információbiztonsági rendszer? Milyen elemekből áll, mi minden ellen véd meg, és mi a legnagyobb veszély? Az informatikai biztonsági megoldásokat a Synergon Informatikai Rt. tanácsadási részlegének vezető szakértője, Kondákor Tibor segítségével mutatjuk be.

A legtöbb üzleti szervezet erőforrásainak jelentős részét az informatikai hálózat teszi ki. Az adatok sérülése, elvesztése, módosítása, vagy akár a rendszer lebénítása egyaránt bekövetkezhet külső támadás vagy belső felhasználói mulasztás, esetleg hardverhiba miatt. Éppen ezért a rendszer védelmére lehetőleg *komplex* megoldást kell alkalmazni. Az értékes vállalati információállományt többszörösen védik, mégpedig logikai, fizikai és adminisztratív úton.

A védelmi stratégia első lépésében a fejlesztők csapata a megbízó háza táján néz körül. E sajátos módszerrel, az üzleti partnerről nyert információk birtokában készít egy fenyegetettség- és kockázatelemzést, amelyben részletesen leírják, milyen veszélyek fenyegetik a megrendelő rendszerét, és mennyi az esélye, hogy azok bekövetkeznek. Ezt összevetik a várható veszteséggel, és azzal, hogy a vállalat mekkora kockázatot képes még elviselni. Ebből a szemléletből ered a *Synergon* megoldásainak egyedisége: mindig az adott megrendelő üzletvitelének megfelelően „testre szabott" intézkedéseket dolgoznak ki.

Az összegyűlt adatok alapján dolgozzák ki az információbiztonsági stratégiát az elkövetkezendő 2-3 évre.

Ekkor következik a megrendelő menedzsment és a fejlesztők közös megbeszélése, amelyen végül kialakítják a megvalósítandó informatikai biztonsági rendszert, a már említett hármas felépítés szerint.

A Synergon biztonsági koncepciója háromféle védelmi intézkedést foglal magában

Synergon Rt.

A *Synergon Informatikai Rt.* – az egyik vezető hazai megoldásszállító vállalkozás – 2001-ben 21,1 milliárd forintot meghaladó árbevételt ért el, saját tőkéje pedig mindegy 7,8 milliárd forint. A társaság részvényeit 1999 májusa óta jegyzik a budapesti értéktőzsdén és a londoni SEAQ elektronikus tőzsdén is. A Synergon piacvezető, multinacionális partnereinek termékeire és támogatására, illetve saját hozzáértésére alapozva alakítja ki információbiztonsági megoldásait. Kiemelt partnerei közé tartozik a *Cisco,* az *RSA Security,* a *Chekpoint,* de a *Nokia* is. Főbb referenciái között szerepel az *Állami Számvevőszék,* a *Budapest Bank Rt.,* a *Raiffeisen Bank,* a *Paksi Atomerőmű Rt.,* valamint a szaúd-arábiai értéktőzsde.

Ember a gép előtt

Az adminisztratív biztonsági intézkedések magukban foglalják a biztonsági követelmények dokumentálását, a jogosultságok, felelősségek, a kötelezően elvégzendő és a tiltott tevékenységek meghatározását. Kiemelt jelentőséget kapnak a nem várt események kezelését célzó üzletmenet–folytonossági tervek *(BCP: Business Continuity Plain).* Itt esik szó a biztonsági intézkedések emberi oldaláról, vagyis a felhasználók tevékenységéből adódó hibák, tévedések, illetve tisztességtelen munkavállalók által okozott kárról, amely a veszteségek 80%-át adja!

Ennek az úgynevezett *humán tűzfalnak* döntő jelentősége van az üzleti biztonság növelése szempontjából. Eszközei: a felhasználók feladatainak szétválasztása, a dolgozók motiválása, oktatása, ellenőrzése stb. Egy vállalat esetében megoldható például, hogy az ügyfélszolgálatokon dolgozó alkalmazottak más adatokat és hálózati erőforrásokat érjenek el, mint például a személyzeti osztály alkalmazottai vagy a marketing- és értékesítési osztály felhasználói. Ugyanakkor a felső vezetés olyan adatokhoz is hozzáférhet, amelyek el vannak zárva a többi alkalmazott elől.

Állj, ki vagy?

A logikai védelmi intézkedések a tárolt adatok bizalmas kezeléséről, sértetlenségének megőrzéséről és folyamatos rendelkezésre állásáról gondoskodnak. Ezek lehetnek vírusvédelmi eszközök, tűzfalak, behatolás–érzékelő rendszerek, autentikációs rendszerek, publikus kulcsú infrastruktúra a digitális aláírás és titkosítás megvalósítására, tartalomszűrés, virtuális magánhálózat a bizalmas kommunikációhoz (pl. vidéki kirendeltségek, illetve multina-

cionális leányvállalatok között), valamint mentési rendszerek.

Az adminisztratív és logikai védelmi intézkedések szorosan összekapcsolódnak a fizikai védelem alkalmazásával, amelynek a feladata az eszközök biztonságos, folyamatos őrzése, szünetmentes tápegységekkel, tűzvédelmi berendezésekkel, megfigyelő rendszerekkel és biztonsági (fegyveres) őrökkel a rongálás, lopás és egyéb erőszakos beavatkozások ellen.

A legnagyobb veszély

A legnagyobb hiba lenne azonban azt hinni, hogy az iménti biztonsági intézkedések kiépítése után a megrendelő, illetve a szolgáltató nyugodtan hátradőlhet a karosszékében, mondván hogy „a gép forog, az alkotó pihen".

A kiépített védelmi rendszer szakadatlan felülvizsgálata mellett a rendszer üzemeltetőinek és a felhasználóknak a folyamatos oktatása és a felmerülő hibák azonnali, szakszerű megoldása is a biztonsági megoldást szállító partner feladata.

A védelmi intézkedések teljes körű dokumentációját a vállalat egyedi információbiztonsági szabályzatában rögzítik.

Természetesen a fejlesztők a későbbiekben is teljes körű technikai-üzemeltetési készenléti hátteret biztosítanak.

F.F.H.

Informatikai biztonsági kislexikon

(Forrás: Synergon „Informatikai biztonság" c. kiadványa)

Tűzfal: A tűzfal a különböző hálózatok közötti kommunikáció ellenőrzését megvalósító szoftvereszköz, amely a külső (internet-) kapcsolattal rendelkező hálózatok biztonságára ügyel. Egy korszerű hálózati tűzfal elképzelhetetlen adatvédelmi politika, vagyis az információvédelmet érintő szabályrendszer nélkül.

A tűzfalak a kommunikáció szabályozásán kívül egyéb szolgáltatásokat is nyújtanak, például titkosítást, a virtuális magánhálózat *(VPN: Virtual Private Network)* kialakítását, felhasználó–azonosítást, a tartalomszűrés támogatását vagy sávszélesség-szabályozást.

A tűzfalakban alkalmazott technikák alapján megkülönböztethetünk csomagszűrés- és proxy-alapú technikákat.

Authentikációs rendszerek: A hozzáférés-védelem a felhasználó egyértelmű és hiteles azonosítására épül. A legelterjedtebb megoldás erre a felhasználónév-jelszó páros alkalmazása, amelynek azonban számos támadható tulajdonsága is van (továbbadható, kitalálható, lehallgatható stb.).

Ezek megelőzésére alkalmazzák az úgynevezett erős authentikációs rendszereket, amelyek a jelszón kívül valamilyen fizikai eszközhöz kötik a felhasználók hiteles azonosítását.

Ezek lehetnek speciális leolvasót nem igénylő úgynevezett *token* kártyák, valamint *chippel* ellátott intelligens kártyák (smart card), vagy *biometrikus* azonosítóeszközök, amelyek az azonosítandó személy valamely egyedi testi jellegzetességét (ujjlenyomatát, hangját, arcát, szivárványhártyáját stb.) vizsgálják.

Komplex PKI rendszerek: A titkosítás, a digitális hitelesítés és azonosítás alapja gyakorlatilag a *PKI (Public Key Infrastructure* – nyilvános kulcsú infrastruktúra), amelyet az elektronikus aláírás megbízható alkalmazása érdekében fejlesztettek ki.

Ennek központi alkotóeleme a *CA (Certificate Authority* –hitelesítő hatóság). E köré csoportosulnak a különböző feladatokat megvalósító rendszerek, melyekkel röviden összefoglalva a következő funkciók valósíthatók meg:

- VPN – titkosított kommunikáció nyilvános hálózaton keresztül megvalósított magánhálózattal
- Digitális aláírás – ezzel egy üzenet feladója vagy akár egy nyilvános hálózatról letölthető adatállomány tulajdonosa is hitelesíthető
- Biztonságos levelezés
- Erős authentikáció (a jelszón kívül valamilyen fizikai eszközhöz is kötik a felhasználók hiteles azonosítását)
- Állomány titkosítás
- Biztonságos web-elérés
- Hozzáférés minden kiszolgálóhoz egyszeri bejelentkezéssel (Single Sign On)

Behatolás–érzékelés: Az informatikai rendszerek elleni támadások kivédésre kifejlesztett aktív védelmi eszközök közé tartozik az úgynevezett behatolás-érzékelő rendszer *(Intrusion Detection System - IDS).*

Az egyik rendszertípus egy adott hálózathoz csatlakozva a hálózaton áthaladó forgalmat vizsgálja, valós időben, az összes csomópont védelmét egyszerre szolgálva, ismert támadási minták után kutatva. Találat esetén többféle reagálásra ad módot, a riasztástól a rendszer automatikus átkonfigurálásán át a veszélyes kapcsolat megszakításáig.

A másik típus egy adott számítógép operációsrendszerének naplófájljait vizsgálja betörésre utaló jelek után kutatva. Ennél a megoldásnál minden egyes csomópont saját IDS klienst igényel.

Biztonsági teszt: Egy rendszer védelmének kiépítése előtt és után biztonsági tesztek alkalmazásával derítik ki a rendszer védelmi hiányosságait és a meglévő intézkedések eszközök hatékonyságát.

Ehhez a vizsgálathoz úgynevezett *szkennerprogramokat* használnak. Ezek a szoftverek egy adott hálózati szegmens feltérképezése után különféle betörési kísérleteknek vetik alá a megtalált csomópontokat, az eredményt rögzítik, megjelölik a támadható rendszereket, és esetleg javaslatot is tesznek a védelmi hiányosságok megszüntetésére.

Az úgynevezett *penetration test* során a vizsgálandó rendszer ellen élethű körülmények között – kiemelt hozzáférés és előzetes ismeretek nélkül – kísérelnek meg támadást, ugyanúgy, ahogyan egy hacker vagy cracker is támadna, ebben az esetben azonban egy ellenőrzött és dokumentált folyamatról van szó.

Tartalomszűrés: A szoftveres ellenőrzéssel *(IAC: Internet Access Control)* többféle módon is meg lehet akadályozni a vállalati rendszer felhasználóit bizonyos internetes tartalmak elérésében. Például a konkrét internetcím (URL) alapján már előre ki lehet szűrni az olyan site-okat, amelyek nem az adott munkához tartoznak.

A több milliónyi tiltott URL címét listák tartalmazzák, amelyeket a tartalomszűréssel foglalkozó cégek állítanak össze, a megrendelők igénye szerint (ilyen például a *Surf Control* cég). A felhasználóknak egy adott cégen belül is biztosíthatnak különféle hozzáférési jogokat.

Lehetőség van konkrét fájltípusok szűrésére is, így például a zenei (mp3, wma, waw) vagy videóállományokat a rendszer nem engedi át. Itt is létezik kiskapu: megoldható a korlátozás úgy is, hogy csak bizonyos oldalakról tölthető le az adott fájltípus.

Biztos, ami Cisco

Magyarország legfejlettebb IT biztonsági rendszerét építette ki az elmúlt hetekben a Synergon Informatikai Rt. az egyik nagy magyar kereskedelmi bank megbízásából. A fejlesztés egyben a legnagyobb Cisco-eszközökből kialakított, egybefüggő rendszer hazánkban. A mintegy 1500 felhasználós informatikai rendszer csaknem 100 millió forintba került, és a Cisco SAFE módszertan alapján készült.

Magyarországon elsősorban pénzintézetek alkalmazzák a SAFE-et

A *Cisco SAFE* az egyik legkorszerűbb biztonsági megoldás a vállalatok számára. Az általánosan elfogadott meghatározás szerint egy olyan átfogó hálózatbiztonsági keretrendszerről van szó, amely a vállalatok számára lehetővé teszi, hogy biztonságos módon használhassák az internetes alkalmazásokat. A legtöbb vállalkozás multimédiás alkalmazásai védelmét várja el a rendszertől. A SAFE számukra ideális eszköz, hiszen integrált megoldást jelent a hang-, adat- és videóátviteli, valamint *VPN* hálózatokhoz.

A hálózat telepítése előtt kihagyhatatlan lépés a vállalati biztonsági irányelvek kialakítása, és az ezeknek megfelelő konfigurációs szabályok meghatározása. Hogy ez könnyebb legyen, kifejlesztettek egy színes, grafikus felületű tervező és megjelenítő alkalmazást, a *CSPM*-et *(Cisco Secure Policy Manager)*. Ez voltaképpen egy Windows alatt futó program, amellyel jól átláthatóan jeleníthető meg a hálózat topológiája, a hálózati és a VPN-forgalom adatai, az IDS beállításai és jelentései. Ennek a programnak a része a *CiscoView*, amellyel egy pontból, az eszköz grafikus képét mutatva konfigurálhatók a Cisco-eszközök.

Ne feledjük: a rendszer állandó készenlétet és folyamatos fejlesztést igényel

Csomagszűrés elvén működő tűzfal

A csomagszűrés elve szerint a tűzfalfunkciót ellátó eszköz (router vagy számítógép) a rajta áthaladó információt meghatározott ismérvek alapján ellenőrzi, és csak akkor továbbítja a címzettnek, ha megfelelőnek találja. Meg lehet határozni, hogy milyen protokollon keresztül lehet kapcsolatot teremteni a védett hálózattal, illetve melyek a csomagokkal megcímezhető kapuk (portok). Az internet elterjedt protokollja a *TCP/IP*. Ennek használatakor a különböző szolgáltatások (ftp, http, mail stb.) mindig ugyanazon a kapukon érhetők el, így azután egyszerűen a port tiltásával, illetve engedélyezésével a szolgáltatás igénybevételét is szabályozni lehet. A tűzfal programozásakor elő lehet írni, hogy bizonyos eseményekre hogyan reagáljon a rendszer (figyelmeztetést küldjön a rendszergazdának, vagy naplófájlba jegyezze az eseményt, esetleg szakítsa meg a kapcsolatot stb.).

A csomagszűrés hátrányai: a routerek nem alkalmasak részletes naplófájlok rögzítésére, és ez a technológia az alkalmazói programok szintjén nem nyújt védelmet.

Véd a SAFE

A SAFE hálózat használata a természetesen a bejelentkezéssel kezdődik. Az azonosítás kétféle módszert kezelhet: a hagyományos névvel és jelszóval történő bejelentkezést és az egyszer használatos *(one-time)* jelszóval való bejelentkezést, amelyhez értelemszerűen külső szervert is igénybe kell venni.

A PKI-val (Public Key Infrastructure) való bejelentkezést a Cisco stratégiai szövetségesei révén biztosítja.

A támadások és a jogosulatlan hozzáférések nagyobb része a hálózaton belülről érkezik, ezért ma már elterjedtek a belső tűzfalak is. Elhelyezésük az adott hálózati környezettől függ. A Cisco *PIX*-alapú tűzfalai az úgynevezett állapottartó csomagszűrés elvén működnek, Intel-alapúak, és PIX operációs rendszert, valamint tűzfalszoftvert futtatnak.

A szoftvert a gyorsmemóriából lehet előhívni, ráadásul a tűzfalaknak nincs mozgó alkatrészük (kivéve persze a hűtőventilátort), éppen ezért kiemelkedően jó a megbízhatóságuk.

A hálózati biztonság cél és nem állapot

A vállalatok sokszor igénylik vidéki kirendeltségeik vagy külföldi anyacégükkel folytatott kommunikációjuk biztonságossá tételét. Ezt támogatja az *IPSec* alapú *VPN*, amely az útválasztókba (routerekbe) és a tűzfalakba beépített modul segítségével, vagy az önálló VPN koncentrátorral egyaránt megvalósítható. Az elektronikus levelezés hozzáférési jogosultságainak korrekt rögzítése alapkövetelmény a vállalat biztonságtechnikai rendszerében. A Cisco SAFE módszertana erre is kiterjed.

Forgalmi ellenőrzés

Az elkészült rendszer folyamatos felügyeletét jó házőrző módjára a behatolásérzékelő (IDS) eszközök biztosítják: választható, hogy a hálózati forgalmat vagy a kiszolgálók terhelését figyelő modul kerüljön-e beépítésre. A hálózati forgalmat figyelő modul egy olyan hardverelem, amely 500 megabit/másodperc sebességgel figyeli a csomagokat, Intel-alapú Solaris operációs rendszerre épülő programjának megfelelően. Illetéktelen behatolási kísérlet esetén az IDS aktívan beavatkozik, valamint ezzel egy időben riasztást is küld. A kiszolgálókon működő IDS olyan program, amely a hálózati alkalmazásokat figyeli, és az ott észlelt hiba esetén riaszt. A hálózati forgalom figyelését használják a rendszergazdák, illetve a fejlesztők az elkészült hálózat tesztelésához és hangolásához, hiszen az informatikai biztonsági rendszerek – legyenek bármilyen korszerűek – soha sincsenek teljesen készen.

(-)

Virtuális levélbomba

Egy magyarországi nagyvállalatnál hatalmas problémák okozott egy úgynevezett virtuális levélbomba. Az történt ugyanis, hogy a rossz szándékú belső munkatárs a szakszervezeti vezető nevében egy elektronikus körlevelet küldött a vállalat minden dolgozójának, egy olyan időszakban, amikor a tervezett létszámcsökkentések és leépítések miatt amúgy is feszült volt a hangulat. Ebben a levélben burkoltan sztrájkra szólította fel a dolgozókat, arra hivatkozva, hogy a menedzsment nem törődik velük, ne tűrjék ezt. Természetesen óriási botrány lett, a vétlen szakszervezeti vezető ellen azonnali eljárást kezdeményeztek. Komoly átvilágításokat végeztek a biztonsági rendszerben, felülvizsgálták a biztonsági policy-kat és a hozzáférési jogosultságokat is. Bár a számítástechnikai rendszer nem igazolta a vétlen aktivistát, neki egy másik, off-line adattal sikerült bizonyítania igazát és egyben a levelezési rendszer óriási hibáját. A valódi vétkest nem sikerült nyakon csípni, azonban az óriási erőfeszítéssel és a hatalmas költséggel lefolytatott „nyomozás" után nem fordulhatott elő többet ilyen bűntény. A vészhelyzet elkerülhető lett volna egy korábbi, szakértők által végzett átvilágítással.

Tűzfal és web gyorsítótár

A Microsoft Internet Security and Acceleration Server 2000 egy bővíthető, nagyteljesítményű tűzfal és web gyorsítótár kiszolgáló, amely a Windows 2000 operációs rendszer biztonsági beállításait, menedzsment képességeit és címtárát kihasználva valósítja meg az internet-elérés házirend-alapú szabályozását, gyorsítását és menedzselését.

Az internet a kapcsolattartás új lehetőségeit kínálja a vállalkozásoknak, egyben különféle kockázatokat is magában hordoz, például a biztonság, a teljesítmény és a menedzselhetőség terén. A gondokra a *Microsoft Internet Security and Acceleration Server 2000 (ISA Server)* jelenti a megoldást. A termék egy többrétegű, nagyteljesítményű tűzfal, amely segít megvédeni a hálózat erőforrásait a vírusoktól, kalózoktól és az illetéktelen felhasználóktól. Web gyorsítótára pedig lehetővé teszi a sávszélesség takarékos kihasználását, ráadásul gyorsabb webelérést kínál azáltal, hogy a kérések egy részét a leterhelt internet helyett a helyi gyorsítótárból szolgálja ki. Az ISA Server egységes menedzsment konzolja egyszerűsíti a biztonság és a hozzáférések kezelését.

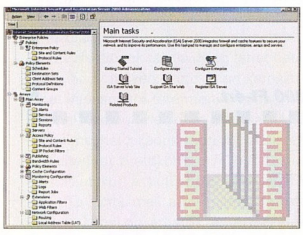
Az ISA Server célja a termék eljuttatása a bétatesztelőkhöz és a vásárlókhoz, akik így a gyakorlatban tesztelhetik a terméket, tesztrendszereket építhetnek, és visszajelzéseket adhatnak a Microsoft fejlesztő és tesztelő csoportjának.

Előnyök

Az ISA Server a *.NET* kiszolgálócsalád egyik kulcseleme, amely számos előnyt kínál elsősorban a gyors és jól menedzselhető internet-kapcsolatot igénylő nagyvállalatoknak. Nézzük, melyek is ezek az előnyök.

Elsőként a *magas szintű biztonságot nyújtó többrétegű tűzfalat* említhetjük, amely megakadályozza a hálózatok jogosulatlan elérését, védi a web- és levelezőkiszolgálókat a külső támadásoktól, valamint folyamatosan ellenőrzi a bejövő és kimenő forgalmat.

Egy további előny a *nagyteljesítményű web gyorsítótár segítségével megvalósított gyors internet-elérés*. A kérések egy részének a helyi gyorsítótárból való kiszolgálásával jelentősen csökkenthető a hálózati forgalom, s ezen keresztül a kommunikációs költségek. A gyorsítótár szétosztja a webkiszolgálók és az elektronikus kereskedelmi alkalmazások tartalmát, így az a vásárlókhoz gyorsan és költséghatékonyan jut el.

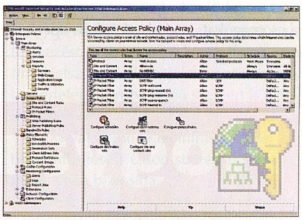


Az ISA Server felhasználói felülete

Az ISA Server *integrált eszközei gondoskodnak a jó rendszerfelügyeletről*. Ez magában foglalja a hozzáférések központi szabályozását a cég házirendjének biztosítása és kikényszerítése érdekében, az internet-használat korlátozását a jóváhagyott alkalmazásokra és weboldalakra, a sávszélesség üzleti szempontok szerinti elosztását a felhasználók között, valamint a jelentés-készítést az internet-használatról.

Az ISA Server tűzfal és web gyorsítótár összetevői a vállalat igényeitől és hálózatának felépítésétől függően külön gépekre vagy egyetlen gépre is telepíthetők. A szoftver ugyanakkor jó bővíthetőséget és testreszabhatóságot kínál a kiterjedt SDK és API készlet jóvoltából, amelynek segítségével az ISA Server funkcionalitása kiterjeszthető a felügyelet, a vírusszűrés, a tartalomszűrés stb. területén.

A vállalatok számára a *könnyű üzembehelyezhetőség* is jelentős előnynek számít. Az ISA Serverrel csak a tűzfal- és a gyorsítótár-kiszolgálók beállítására van szükség, így egyszerűsödik a kiszolgálók közzététele, a tűzfal és a gyorsítótár beállítása. Az ISA Server biztonságos címfordítási *(Secure Network Address Translation – SecureNAT)* képességének köszönhetően a rendszergazdáknak nem kell további szoftvert telepíteni az ügyfélgépekre vagy a közzétett kiszolgálókra a tűzfal vagy a gyorsítótár használatához. Az ISA Server láthatatlan az ügyfélgépek és más kiszolgálók számára, így csökkenthető a rendszerfelügyelet összetettsége és annak költségei.



Az ISA Server menedzsment konzolja

Alkalmazások

Az ISA Server háromféle üzemmódban működhet: tűzfalként, gyorsítótárként és integrált tűzfal-gyorsítótárként ugyanazon a gépen. Tűzfalként az internet és a belső gépek közti biztonságos átjáróként működik. Az ISA Server észrevétlen a kommunikációban résztvevők számára mindaddig, amíg olyan szolgáltatást vagy webhelyet próbálnak elérni, amelynek tiltott a használata. A biztonsági házirendek beállításával a rendszergazdák megelőzhetik a hálózat illetéktelen használatát, a veszélyes dolgok hálózatra kerülését, és letilthatják a kifelé irányuló forgalmat.

Az ISA Serverrel a belső hálózat bizton-

ságának veszélyeztetése nélkül oldható meg a szolgáltatások interneten való közzététele. Beállíthatók a web- és a kiszolgáló-közzététel szabályai, ezektől függ, hogy mely kérések továbbítódnak az ISA Server mögött található kiszolgálók felé. Az ISA Server mögött például egy *Microsoft Exchange* kiszolgáló is elhelyezhető; az Exchange Serverre bejövő leveleket az ISA Server (amely az ügyfelek számára levelező kiszolgálónak látszik) elfogja, megszűri, majd továbbítja az Exchange Servernek.

Gyorsítótárként telepítve az ISA Server a belső ügyfelek internet-eléréséről gondoskodik. Növeli az ügyfél böngészőjének teljesítményét, csökkenti a válaszidőt, és csökkenti az internet-kapcsolat sávszélességének használatát.

A gyorsítótár a külső ügyfeleket is kiszolgálhatja, hozzáférést biztosítva számukra a vállalati információkhoz. A bejövő webkérésekre az ISA Server webkiszolgálóként reagál, az ügyfél kéréseit pedig a saját gyorsítótárából szolgálja ki, és csak azokat a kéréseket továbbítja a webkiszolgáló felé, amelyeket nem tud innen kiszolgálni.

Az integrált tűzfal és gyorsítótár a biztonságos és gyors internet-kapcsolat megteremtésében segít. (-)

Ajtók és zárak

Válaszol Vityi Péter, a Microsoft Magyarország ügyvezető igazgatója

A legtöbb szoftvercég – így a *Microsoft* is – egyre többet törődik az információbiztonsággal. A cég biztonsági stratégiájáról *Vityi Pétert*, a *Microsoft Magyarország* ügyvezető igazgatóját kérdeztük.

- Miért foglalkozik most aktívabban a Microsoft az információbiztonsággal?

- A Microsoft mindig is fontosnak tartotta a biztonság témakörét, hiszen ez a probléma az egész IT iparágat érinti, ebben pedig a Microsoftnak – vezető szerepe folytán – feladatai és megoldásai is vannak. Régebben egyszerűbb volt az „élet": a felhasználók zárt terminálok előtt dolgoztak, az adatbevitel főképpen billentyűzeten keresztül történt, így elsősorban fizikai védelemre volt csak szükség. Később már különböző adathordozókon is lehetett információt cserélni, ekkor jelentek meg a vírusok. A különböző külső-belső hálózatok és az internet elterjedésével tovább nőtt a veszély, és teljesen megváltoztak az ezzel kapcsolatos feladatok.

- Mi a különbség az internet adatvédelmi és biztonsági kérdései között?

- Nehéz szétválasztani a kettőt, hiszen szervesen kapcsolódnak egymáshoz. A biztonság sérelmére elkövetett cselekmények az adatok sérelméhez is vezethetnek. A biztonság azt a kérdéskört öleli fel, hogy mennyire vannak védve az ember adatai a jogosulatlan vagy nem várt hozzáféréssel szemben, míg az adatvédelem inkább arra vonatkozik, hogy a külső adatkezelők hogyan férhetnek hozzá a személyes adatokhoz, és mit kezdhetnek azokkal. Az adatvédelem szubjektív dolog, mivel nagyrészt szokásfüggő: egyesek kevésbé aggódnak személyes adataik kezelésével kapcsolatban, míg mások még azt sem túrik könnyen, ha valaki megtudja az IP-címüket.

- Mikor érezhetjük magunkat biztonságban?

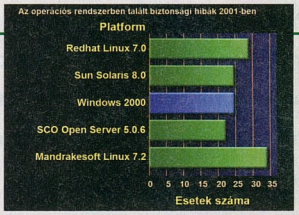
Véleményünk szerint három fontos terület határozza meg, mennyire érezhetjük magunkat biztonságban az információtechnológiában. Egyfelől szükség van egy bizonyos technológiai színvonalra. Természetesen a Microsoft minden tőle telhetőt megtesz a megfelelő alapinfrastruktúra megteremtésére; itt vannak például a Windows rendszerek vagy az Office alkalmazások, amelyek ugyan nem kifejezetten biztonsági célokat szolgálnak, ám olyan képességeik vannak, amelyek fokozzák a védelmünket. Ezen felül a Microsoftnak vannak olyan termékei is, amelyek kifejezetten a biztonságos információkezelést teszik lehetővé, mint például az *ISA 2000 Server (Internet Security and Acceleration Server).*

Ugyanakkor szükség van arra is, hogy a vállalatok pontosan szabályozzák, mit kell tenniük a biztonság érdekében, például akkor, ha mégis vírus került a rendszerbe. Ennek hiányában hálózatuk sokkal sebezhetőbbé válik. A harmadik fontos szereplő pedig maga az ember. Vagyis az a körülmény, hogy a felhasználók milyen oktatásban részesültek, pontosan ismerik-e a lehetőségeiket, és a vállalat milyen mértékben von be külső szakértőket a potenciális veszélyek kiszűrésére.

- Milyen megoldásokkal segíti a biztonságot a Microsoft?

- A biztonságot tekintve három összetevőből áll vállalatunk stratégiája. Az első az, hogy a biztonság elsőrendű prioritásként szerepel mindegyik termékünk elkészítésekor. A második, hogy hozzájuttassuk ügyfeleinket minél több biztonsággal kapcsolatos információhoz. Harmadsorban pedig megoldásokat keresünk a biztonsági alapelvek, az állami szabályozás, az infrastruktúra-védelem és az ezekhez hasonló, tágabb kérdéskör problémáira.

Hamarosan elindítunk egy új webhelyet, amely kizárólag a biztonság témakörével foglalkozik **(www.microsoft.com/hun/biztonsag)**, és igyekszik választ adni az egyéni és vállalati felhasználók online adatvédelemmel kapcsolatos leggyakoribb kérdéseire. A webhely ismerteti az adatvédelem és a biztonság növelését segítő szoftvereszközök különböző változatait. A Microsoft új webhelye olyan konkrét információkkal szolgál a felhasználóknak, amelyeket a gyakorlatban is alkalmazhatnak, és amelyek révén biztonságérzetre tehetnek szert.



Forrás: John McCormick, TechRepublic, 2001. szeptember 24, a Security Focus Bugtraq adatai alapján

Biztonsági szempontból az a webhely fő üzenete, hogy az interneten kockázat nélkül lehet ténykedni, amennyiben az ember megtesz bizonyos egyszerű óvintézkedéseket. Összevethetők a különféle vélemények, illetve összehasonlíthatók a különböző termékek, így a világhálón elérhető információk széles köre révén mindenki mérlegelheti, hogy pontosan mire is van szüksége.

Végül, de nem utolsósorban kiemelném a Microsoft Magyarország rendszermérnökei által vezetett nagysikerű *Technet* szemináriumainkat, amelyen meghívott vállalati ügyfeleink rendszergazdái, üzemeltetési szakemberei naprakész ismereteket szerezhetnek a Microsoft biztonságtechnológiai stratégiájáról, valamint többek között arról is, hogyan tehetők biztonságossá a vállalati rendszerek, hálózatok. **V.P.**

Desktop biztonság

A Microsoft Office 97 és a Microsoft Windows 98 piacra kerülése óta jelentős mértékben megnőtt a számítógépes hálózatokat érő fenyegetések száma. Az Office XP Professional és a Windows XP Professional megjelenésével a Microsoft a korábbinál sokkal kiterjedtebb eszköztárat bocsát a vállalatok rendelkezésére informatikai erőforrásaik védelmére.

Egyre több vállalkozás használ információs rendszereket, s akár végzetes következményekkel is járhat, ha a védelem megsérül. A vállalatokat érő támadások eredménye a szolgáltatásmegtagadástól a bizalmas információk megsérüléséig vagy elvesztéséig terjedhet. A kiszolgálókon és a felhasználók munkaállomásain tehát mindent meg kell tenni az integritás fenntartása és az adatok védelme érdekében.

A *Microsoft Office 97* és a *Microsoft Windows 98* bevezetése óta a Microsoft a kor jellemző fenyegetéseit és biztonsági kockázatait figyelembe véve folyamatosan fejleszti termékeit. A *Microsoft Windows XP Home Edition* és a *Microsoft Windows XP Professional*, illetve a *Microsoft Office XP Professional* is számos új biztonsági szolgáltatást nyújt, amelyek révén a rendszergazdák hatékonyan védekezhetnek napjaink jellemző támadásai ellen. A Windows XP és az Office XP egyaránt a szolgáltatások széles választékát állítják hadrendbe a vállalat védelme érdekében. Az XP környezet finombeállításával a rendszergazdák a vállalat biztonsági házirendjének és gyakorlatának megfelelő felhasználói és hozzáférési jogokról gondoskodhatnak. Az XP környezet magasabb fokon támogatja a központi felügyeletet és a biztonsági funkciók kezelését is, a telepítőeszközöktől kezdve egészen az *Active Directory* szolgáltatásig.

Windows XP

A Windows XP ellenőrzi és kezeli az adat be- és kiviteli műveleteket, illetve a helyben tárolt adatok védelméről is gondoskodik. Ezenkívül további funkciókat is tartalmaz a konfiguráció kezelésére és a felhasználói jogok ellenőrzésére. Vegyük sorra most a Windows XP fontosabb biztonsági szolgáltatásait.

A Windows XP *titkosított fájlrendszere (EFS)* segítségével a felhasználók titkosított könyvtárstruktúrában helyezhetik el érzékeny állományaikat. A csak megfelelő jogokkal rendelkező felhasználók számára elérhető fájlokat az alkalmazások automatikusan titkosítják és fejtik vissza. A titkosított fájlok és mappák a többi fájlhoz és mappához hasonlóan használhatók, mivel a felhasználó számára a titkosítás folyamata átlátszó.

A hálózaton keresztül továbbított adatok titkosítására az *Internet Protocol Security (IPsec)* és a *PPTP* titkosítást kell használni. Az EFS a titkosított fájlok visszaállítására is képes. A hitelesített rendszergazdák akkor is hozzáférhetnek a titkosított tartalomhoz, ha az eredeti felhasználói azonosítók megsérültek.

A felhasználói, illetve számítógépes környezet beállításainak kezelésére használhatjuk a *házirendeket*, amelyek segítségével – adott funkciókat szükség szerint ki- és bekapcsolva – a rendszergazdák egységesen és egyszerűen kezelhetnek nagy számú asztali számítógépet. A *csoportházirend* beépülő modul segítségével a csoportházirend-beállítások központilag, az Active Directory szolgáltatás segítségével adhatók meg. Az adatvesztések megelőzése, illetve az adatok visszaállítása is a Windows XP alapszolgáltatásai közé tartozik. A *biztonsági mentés* alkalmazásával a felhasználók beépített és eltávolítható adathordozóra egyaránt lementhetik állományaikat és mappáikat.

A Microsoft Office szolgáltatásai

Biztonsági szolgáltatás	Office 97	Office 2000	Office XP
Dokumentum digitális aláírása	–	–	Az Office XP-ben megjelent újdonság
Adatvédelem		Támogatva	Támogatva
Adat-visszaállítás	Az Office 97-ben megjelent újdonság Automatikus mentés	Automatikus mentés	Az Office XP-ben megjelent újdonság Automatikus visszaállítás
Makróvédelem	Megnyitáskor rákérdezés a makrók használatára	Magas, közepes és alacsony biztonsági szintű felügyelet és kódaláírás	Magas, közepes és alacsony biztonsági szintű felügyelet és kódaláírás
Biztonsági sablonok és eszközök	A telepítőeszközök az Office Resource Kit részeként szerezhetők be	A telepítőeszközök az Office Resource Kit részeként szerezhetők be	Továbbfejlesztett telepítőeszközök és központi felügyeleti szolgáltatások
Outlook biztonsági szolgáltatásai	Minimális	1. és 2. szintű csatolt fájlok	Sokkal jobb és rugalmasabb
Dokumentumvédelem	Csak olvasható, Ellenőrzésre és Jelszavas védelem	További verziók és Titkosítás	Újabb közzétételi lehetőségek Továbbfejlesztett titkosítás

A Microsoft Windows szolgáltatásai

Biztonsági szolgáltatás	Windows 98	Windows 2000	Windows XP
Vezeték nélküli hálózatok támogatása	–	–	A Windows XP-ben megjelent újdonság
Internetes tűzfal	–	Az ISA Server révén elérhető	A Windows XP-ben megjelent újdonság
Biztonságos hálózat (IPSec)	–	Alapszolgáltatás	Alapszolgáltatás
Felhasználói szintű biztonság megosztott fájlokhoz és mappákhoz	–	Alapszolgáltatás	Alapszolgáltatás
Titkosított fájlrendszer	–	Alapszolgáltatás	Alapszolgáltatás
Nyilvános kulcsú infrastruktúra	–	Alapszolgáltatás	Alapszolgáltatás
Csoportházirend-objektumok	–	Alapszolgáltatás	Alapszolgáltatás
Naplózás	–	Alapszolgáltatás	Alapszolgáltatás
Intelligens kártyák támogatása	Külső gyártó termékével elérhető	Alapszolgáltatás	Alapszolgáltatás

A Windows XP a *kapcsolat nélküli fájlok szinkronizálásáról* is gondoskodik. Amikor a számítógép újra hálózati kapcsolatot létesít, az esetleges módosításokat automatikusan szinkronizálja a kiszolgálóval, az ideiglenes helyi fájlokat pedig törli.

A Windows XP támogatja a nyilvános kulcsú *tanúsítványokat* és a nyilvános kulcsú infrastruktúrát *(Public Key Infrastructure, PKI)*. A megszokott felhasználónév–jelszó párosításnál erősebb biztonságot igénylő vállalatok számára a Windows XP beépített *intelligenskártya-támogatást* is nyújt. A Windows XP-t ugyanakkor kiterjedt *naplózási* képességekkel is ellátták, amelyek segítségével megfigyelhetők és felismerhetők a számítógépes környezetben előálló, nem kívánt vagy váratlan események.

A *vezeték nélküli hálózatok beépített támogatásával* a Windows XP egyszerű módszert kínál a hordozható eszközök, köztük PDA-k, mobiltelefonok és további számítógépek hálózatba kötésére.

Office XP

Az Office XP a Windows XP biztonsági szolgáltatásaira épít.

A *digitális aláírás* az adatok módosítása ellen kínál védelmet, egyúttal biztosítja a dokumentum hitelességét. A *kódaláírás* hasonló a digitális aláírásokhoz, ám az ilyen aláírást futtatható programkódon vagy makrón lehet elhelyezni.

Az Office XP alkalmazások mindegyike számos hozzáférés-vezérlési lehetőséget, valamint a különböző alkalmazásfunkciókat letiltó vagy engedélyező tulajdonságlapot és telepítősablont is tartalmaz.

Az Office XP-ben jelentősen javult a *makrók* kezelése és futtatásuk biztonsága. A legtöbb Office XP alkalmazás képes arra, hogy a makróbiztonságot az „alacsonytól" a „magasig" terjedő széles skálán határozza meg.

A Word, az Excel, az Access és a PowerPoint különféle szolgáltatásokkal segítik a dokumentumok védelmét a meghatalmazás nélküli hozzáférésektől és módosításoktól. Ezek a funkciók az operációs rendszer EFS szolgáltatásával és megosztási szintű engedélykezelésével párhuzamosan is használhatók. A dokumentumok elérését a felhasználók fájl szintű védelemmel szabályozhatják. A szerző emellett jelszóval is védheti a dokumentumot módosítás vagy megnyitás ellen.

A Microsoft Word további védelmi és változáskövetési funkciókat is tartalmaz, így az ellenőrzési ciklusban részt vevő dokumentumokat a szerkesztők és a lektorok úgy módosíthatják és láthatják el megjegyzésekkel, hogy eközben az eredeti változatot is megőrizhetik. A Word lehetővé teszi azt is, hogy a dokumentumnak csak adott részeit védjük a módosításoktól. Az Excel hasonlóan teszi lehetővé bizonyos cellatartományok védelmét, az Access pedig különféle módszerekkel ellenőrzi az adatbázis objektumainak (pl. táblák, lekérdezések, űrlapok stb.) elérését.

A Microsoft Office XP két lényeges fejlesztéssel támogatja a bizalmas jellegű *adatok védelmét*. A felhasználók az általuk megadott jelszót kulcsként használva *titkosíthatják* a fájlokat, amelyeket így azonosítatlan személy nem olvashat el. Az Office alkalmazások ugyanakkor képesek a kiegészítő információk (pl. a dokumentum tulajdonságai, címe, szerzőjének neve stb.) eltávolítására is, így a közzétett dokumentumokkal nem továbbítódnak a felhasználóval kapcsolatos adatok. Számos fenyegető tényezőt sikerült kiküszöbölni az *Outlook 2002* fejlesztése során is. Alapértelmezett beállításként az Outlook 2002 sokkal szigorúbban kezeli bizonyos típusú csatolt fájlok fogadását és küldését, illetve a címlista elérését. A rendszergazdák a vállalati követelményeknek megfelelően szabhatják testre a biztonsági beállításokat.

Az Outlook 2002 biztonsági modellje támogatja az *S/MIME v3* szabványt, amellyel a felhasználók biztonságosan levelezhetnek más S/MIME e-mail ügyfélprogramok felhasználóival a szervezeten belül vagy az interneten keresztül. A digitális aláírási és titkosítási lehetőséggel az Outlook 2002 minden segítséget megad a felhasználó adatainak védelméhez akár tárolás, akár továbbítás közben.

Az Outlook 2002 biztonsági funkciói között szerepel még a *biztonsági címkék* és az *aláírt nyugták* használata, amelyekkel biztonságosabbá tehető az elektronikus levelezés, és testreszabhatók a biztonsági szolgáltatások.

Valamennyi Office XP alkalmazás úgy is beállítható, hogy a telepített *COM bővítményeket* automatikusan megbízhatóként kezelje. Ekkor az alkalmazások aláírásuk ellenőrzése nélkül automatikusan betöltenek minden, a megbízható mappákban található COM bővítményt, alkalmazás-specifikus bővítményt és sablont.

Értékes szolgáltatás még az új *Automatikus visszaállítás* funkció, amelyet az Office XP összes alkalmazása támogat. Ha valamilyen Office XP alkalmazás végzetes hibával találkozik, amely megakadályozza további futását, az Automatikus visszaállítás szolgáltatás megpróbálja ellenőrzött módon lezárni a programot, s elmenteni a dokumentum éppen szerkesztett változatát, illetve a lemezen tárolt ideiglenes változatokat is.

Internet Explorer 6.0

Az *Internet Explorer 6.0* újdonsága a magasabb szintű adatvédelem, illetve további fejlesztéseket tartalmaz a *Windows XP Microsoft Authenticode* biztonságos kódhozzáférésében. A Microsoft Outlookhoz hasonlóan az Internet Explorer is támogatja a biztonsági zónákat és szinteket, amelyekkel a felhasználó pontosan, zónánként szabályozhatja az adatok és vezérlők letöltését és futtatását.

Kártyák a neten és a zsebben

A hitelkártyák és a különböző mágnescsíkos kártyák, illetve chipkártyák pénzt helyettesítő eszközök, ezért hamisításukra épp olyan nagy a kísértés, ha ugyan nem nagyobb, mint a pénz esetében. Ugyanakkor azt is el kell ismernünk, hogy a legtöbb kártya hamisítása nem igazán nehéz feladat. A bankok Magyarországon is számolnak a kártyacsalás kockázatával, együttműködésük következtében azonban ez a kockázat még elviselhető.

Érdemes megnézni azokat a módszereket, amelyekkel megkopasztható az ügyfél és a bankja, hogy amennyire csak lehetséges, védekezni tudjunk ellenük. A legfontosabb: van néhány aranyszabály, amelyet be kell tartanunk, ha plasztikkártyát használunk, ezek egyben a mindennapi túlélés szabályai is.

A kártyahasználat szabályai

1 SOHA ne írjuk fel a kártya titkos azonosító kódját. A PIN-t telefonon se mondjuk be soha, a bank ilyet nem kér, legfeljebb a nevében bejelentkező csalók. Ha a bank nevében kérik a kódot, az mindenképpen beugratás. A banki telefonos tranzakciók során más PIN kódot használunk, amelyet a bankkal való megállapodásunk rögzít. A bankok megint más kódot alkalmaznak az internetes home banking szolgáltatásaikra.

2 A PIN kódot, ha a bank rendszere engedi, a kézhezvétel után azonnal változtassuk meg olyanra, amelyet könnyen meg tudunk jegyezni. A legtöbb bank ezt ingyen vagy minimális díjért megengedi. Ezzel elkerüljük a PIN felírásának biztonságot alaposan rontó műveletét. Ha megváltoztattuk a PIN kódot, akkor nyugodtan a kártya mellett hagyhatjuk az eredeti – immár nem érvényes – cetlit a PIN kóddal. Ezzel elősegítjük, hogy néhány rossz próbálkozás után az automata elnyelje a kártyát.

3 A tranzakciókról kapott nyugtát sohase hagyjuk a helyszínen. A rajta szereplő adatokkal visszaélhetnek! A legtöbb esetben rajta van a teljes kártyaszám vagy annak nagy része, amellyel például visszaélhetnek az interneten. Jobbfajta banki automatáknál kérhető, hogy ne adjon bizonylatot. Vásárláskor ez sajnos kötelező.

Az OTP többféle bankkártyát kínál ügyfeleinek

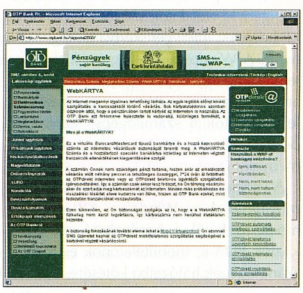
4 Amennyiben lehetséges, kérjünk a tranzakciókról rádiótelefonos automatikus értesítést. Így a klónozásos csalásokat idejében el tudjuk kapni.

5 A kártyalehúzáskor ne engedjük, hogy elvigyék a kártyát a szemünk elől. Kísérjük végig a kártya útját, mert ezzel meg tudjuk akadályozni a másolatok készítését.

6 A hó végi kimutatásokat és a bizonylatokat vessük össze. Ezzel felfedezhető a duplázásos csalások nagy része.

7 Több kártyánk legyen, különböző pénzintézeteknél. Mindig azt használjuk, amelyik hitel- és limitfeltételei a vásárláskor a legoptimálisabbak. Ezzel elkerülhetjük, hogy pénz nélkül maradjunk. Ezeket a kártyákat sohase tartsuk egyetlen helyen.

8 Bármilyen visszaélés gyanúja esetén tiltsuk le a kártyát. Ezzel a klónok is használhatatlanná válnak! Olcsóbb kifizetni a tiltást, mint futni a számlánkon tartott pénz után.



A virtuális bankkártyára jó példa az OTP webkártyája

Ennyi jó tanács után nézzük, miféle furfangokkal tudják kifosztani az ügyeskedők a pénztárcánkat és a bankot egyaránt. Ehhez tudnunk kell, hogy a kártyahasználat során kétféle fizetési módszert alkalmazunk.

Az egyik a *card present* típusú fizetés, ahol a kártya fizikailag is jelen van a fizetés során. A kártyák egy részén erre szolgál a *CV kód* is az aláírássávon. A másik a *card not present* típusú fizetés. Ilyenkor a kártya nincsen jelen, a kártyaadatok megadásával kezdeményezünk fizetést. Az ilyen típusú fizetésekkel követik el a visszaélések nagy részét. Most pedig tekintsük át a kártyahamisítások legfőbb fajtáit.

Kamulálás

A módszer lényege, hogy egy nem létező, de hihető kártya adatait hozzuk létre. A számítástechnika alvilágában megtalálható számtalan programcsomag segítségével minden további nélkül létrehozhatunk ilyen kártyaszámokat. Mégpedig vagy a saját kártyaszámunk extrapolálásával vagy pedig teljesen új számok generálásával.

A kártyaszám felépítése teljesen publikus. Az első számcsoport adja a kártyafajtát és a bankot, a következők a típusés a sorszámot, amelyeket a végén egy ellenőrzőszám követ. Egyes kártyatípusoknál létezik még egy card present ellenőrzőkód is a kártya hátoldalán, amely a kártyaszámot követi, de ennek itt nincs jelentősége.

Ha ezeket a generált számokat és a melléjük költött, de hihető adatokat a neten kisösszegű fizetésekhez használják fel – általában 5 dollár vagy 10 német márka alatt – akkor a rendszer az autorizálást csak negatív lista alapján végzi el, azaz azt nézi, szerepel-e a kártya a letiltottak között. A meglopott cég csak akkor kap észbe, amikor a banktól le akarja hívni az összeget.

A ConCorde Direct értékpapír-forgalmazó a Raiffeisen Bankkal közösen kínál ügyfeleinek teljes körűen felhasználható Eurocard-MasterCard bankkártyát

A bankok ilyenkor általában fizetnek, a kisösszegű kár jelenleg éppen a kezelhető kockázat körébe tartozik. Lebukás esetén viszont a „díja" ugyanaz, mintha egy ezerforintost hamisítottunk volna. Vannak ugyanis olyan bankkal összefonódott szervezetek is, amelyek a kisösszegű kifizetéseket is autorizálják. Ez pedig lebukási kockázattal jár.

Ha az adatokat mágnescsíkra írják, egykét helyen még kisösszegű online tranzakciót is kezdeményezhetnek a kártyával, hiszen a társbanki autorizálás is pénzbe kerül, és a bankok a kezelhető kockázat mértékéig ezt inkább magukra vállalják.

A jelenség tömegessé válását egy idióta – de ma is egyre gyakrabban alkalmazott – amerikai jogszabály idézte elő, amelynek nyomán az internetes szexoldalak, mégha ingyenesek is, hitelkártyaszámot kérnek a nagykorúság igazolására, egyes szolgáltatók pedig szolgáltatásaik ingyenes kipróbálását a hitelkártyaszám megadásához kötik. Ez az egyetlen eset, amikor kamulált kártyaszámot KELL a saját érdekünkben használni. Ezek a rendszerek – ellenőrizhetetlenségük, adatkezelésük miatt – a kártyaszám-lenyúlások leggyakoribb forrásai. Vagy pedig ne nézzük a széplányokat ilyen helyeken.

A tanulság egyértelmű: a plasztiklap fizetésre való és nem másra. Aki másra használja, az jogosulatlan adatkezelést követ el, és elősegíti a hamisítási üzletág felvirágzását. A kamulálás esetében a veszteség azt a bankot terheli, amelynek a kártyáját kamulálták, illetve ha nem fizet a bank, akkor a szolgáltatót.

A további csalástípusok már a kártyabirtokos számlájára mennek, éppen ezért a kispénzű emberek számára igencsak veszélyesek. A csalók ügyesek, és általában a számlákat, sőt a hitelkeretet is teljesen lefosztják. Ilyenkor egyetlen lehetőség marad: a bankkal való hosszadalmas egyezkedés, a rendőrségre járás, de még akkor sem lehetünk biztosak abban, hogy hozzájutunk-e a pénzünkhöz, vagy pedig a bank nyilvánít bennünket nem kívánatos személynek. A bankok nem szeretik a problémás ügyfeleket.

„Liftes csalás"

Az internetes kereskedelemben jelent meg a legújabb trükk, amelynek a károsultja a bank és az internetes kereskedőház. Az egyre terjedő módszer szülőatyáit a közelmúltban küldték hűvösre Oroszországban, de a módszert mégis sokan alkalmazzák.

A módszert mindig valamelyik internetes áruházzal szemben vetik be. A csaló ilyenkor bankszámlát nyit, mondjuk Ukrajnában, majd utána honlapot indít a neten. A honlapján egy az egyben hirdeti a kiszemelt internetes áruház kiszemelt termékeit. Fizetni átutalással kell, mondjuk a megadott ukrajnai vagy akár kajmán-szigeteki bankszámlára, esetleg le is tudja hívni a pénzt a hitelkártyáról. Mivel a megrendelés is valahol a világban megbúvó barátunkhoz fut be, ő ilyenkor folytatja a mókát. Máskor a pénzt fogja el, és nem fárad további ténykedéssel, mondjuk az áru vagy a szolgáltatás értékesítésével. Csupáncsak hamis linkeket helyez el a világban, amelyek beterelik hozzá a gyanútlan felhasználót. A pénzt megkapta, de nem jó a nyűgös vevő. Ezért a vevő adataival, annak nevében immár más áruházakban is megrendeli az árukat és szolgáltatásokat, neki szóló szállítási címmel. Vagy az egész adatbázisát egyszerűen eladja más csalóknak.

A másik módszernél lopott hitelkártyával fizet a jó helyett, amelyről ő inkasszált az eredeti áru hirdetőjénél. Ilyenkor az áru

Az Inter-Európa Bank tiniknek szánt bankkártyája belföldön és külföldön egyaránt használható

megjön, csak a pénz nem a szolgáltatónál köt ki. Így a csalónak megmarad a teljes összeg tisztán, az áruház, a hitelkártya társaság és a hitelkártya igazi birtokosa pedig elvitatkozhat az összeg jogosságán. Az amerikai tapasztalatok szerint az árut természetesen nem adják vissza azok, akik megrendelték, hiszen fizettek érte. A szállítási cím, meg a bankszámla közötti távolság senkinek sem tűnik fel, hiszen a jelenlegi adó- és vámrendszerek még sok esetben a nyugati polgárokat is ügyeskedésre kényszerítik.

A kártya klónozása

A klón annyit jelent, hogy az egy példányban létező kártyát valamiféleképpen megtöbbszörözik, s az eredeti kártya és a klónja az eset felderítéséig egyszerre létezik az időben. És természetesen amíg le nem bukik a számlaegyenlegek egyeztetésével, más is fizet a mi kártyánkkal.

A klónozásnak több alaptípusa ismert.

Ikresítés

Az ikresített kártya *pontosan* azonos az eredetivel. A kártyát ilyenkor még egyszer lehúzzák, majd a lehúzott kép mellé a mágnescsíkot is lemásolják. Utána következik a legnehezebb dolog, a kártya tökéletes másolatának az előállítása. Ehhez általában

több lopott, lejárt, de a hamisítandóval megegyező kártyát használnak. A legmacerásabb hamisítás ez, mert ezredmilliméteres pontossággal, darabokból állítják össze az új kártyát, amely a megtévesztésig hasonlít az eredetire. Természetesen a fényképes kártyák erre alkalmatlanok.

A Fujitsu POS terminálját a gyorséttermekben használják

Az ikresített kártyát pontosan úgy használják, mint az eredetit, és az az előnye is megvan, hogy a hátlapon az aláírást a hamisító kicserélheti a sajátjára. A kártyatársaságok ezért helyeznek el az utóbbi négyöt évben biztonsági jegyeket az aláírássávon is. A módszert elsősorban a jó kézműves kultúrájú országokban használják, de Törökországban, Olaszországban is előfordul. Előnye, hogy a beváltáshoz nem kell beavatni a kereskedőt is.

Stemplizés

A beavatott szám-összeszedő még egyszer lehúzza a papír slipet a beváltás során. Ez kerül át a kártyahamisítókhoz. Ők ennek alapján a bélyegzőkészítéshez hasonló eljárással elkészítik a kártya dombornyomású részét. Utána ezek a stemplik elkerülnek a beavatott kereskedőkhöz, akik erről hagyományos papírslipes-gyalus módszerrel lehúzzák a banki papír slipet, és benyújtják a fizetési igényt. Amikor megjön az általában egyszerre nagyobb tömegben benyújtott levonatokért járó pénz, a vállalkozás eltűnik.

Duplázás

Ekkor a csaló kereskedő vagy legalább kétszer húzza le a papír slipet, majd a második garnitúrát is benyújtja, vagy pedig az elektronikus kártyaolvasó POS-t manipulálják. Ebben az esetben a POS akár a PIN kóddal együtt is tárolhatja a korábbi tranzakciókat, amelyeket újra el lehet küldeni más összeggel. Ez a fajta manipuláció, ha ügyesen csinálják, eléggé nehezen leplezhető le, csak a terhelések pontos nyilvántartása segíthet. Ilyenkor általában viszonylag kis összegekkel és többször próbálkoznak.

A fejlettebb megoldásnál ezek az adatok kinyerhetők a manipulált POS memóriájából, és akár a világ másik pontján is újra felhasználhatók.

Felírás

Magyarországon ez a módszer igen divatos volt egyes helyeken, mára azonban jelentősen visszaszorult. Évekkel ezelőtt az M1 akkor még kapukkal ellátott fizetős szakaszán ilyen típusú visszaéléseket leplezett le a rendőrség. Itt annyi történik, hogy a kártyát még egyszer lehúzzák a hivataloson kívül. Erre egy apró, tenyérben nagyon jól elrejthető eszközt alkalmaznak, amely párszáz mágneskártya mágnescsíkjának tartalmát tudja megőrizni a memóriájában. A felírók általában fejpénzt kapnak a lehúzott kártyák után.

Az így megszerzett adatok nem tartalmazzák a PIN kódot, ami azt jelenti, hogy áruvásárlás céljára használhatók fel. A világban a bűnszövetkezeteknek számos beavatott partnerük van. Ezek a felírt mágneskártya sávot adatvonalon keresztül megkapják, majd újra kiírják egy akármilyen plasztiklapocskára.

A technológia nem bonyolult, alig száz euróból, kereskedelmi eszközökből összerakható. Az ügyfél nevében a hamisítványnyal olyan kereskedőknél vagy pénztárosoknál eszközölnek vásárlásokat, akik nem akarják észrevenni, hogy nem hitelkártyát húznak le hitelkártyaként. A kapott árut azután újra értékesítik, így jutnak a pénzükhöz.

Kártyaszám adatbázis lopás

Az internetes kereskedelemben van egy rossz szokás: a cégek adatbázisokban tárolják az ügyfeleik kártyaszámát. Ha ehhez az adatbázishoz valaki hozzáfér, olyan adatsort szerezhet meg, amely az elektronikus kereskedelemben, pontosabban a card not present típusú fizetéseknél használható fel.

Az InterCard POS terminálja analóg vagy ISDN vonalon egyaránt működtethető

A dolog még súlyosabb, ha a cégnél nem is a neten lévő, de különben jól védett adatbázist lopja el egy illojális alkalmazott, amire szintén van példa bőven. A leleplezés itt is csak a kártyás tranzakciók követésével lehetséges.

Összefoglalva megállapíthatjuk, hogy a kártyahamisítások és manipulálások köre igen széles. A jó rendszer, a lojális alkalmazottak csak csökkenteni tudják a veszélyt. Ugyanakkor fenyegető az a jelenség is, amelyet itthon lehet tapasztalni, hogy egyes kereskedőhelyek a fizetéskor kérik a PIN kódot, amely így könnyen „lesasolható". A gépek manipulálási lehetőségeitől eltekintve a boltokban nincsenek meg a PIN beadásának korrekt feltételei.

Íme egy tipikus vendéglői POS terminál (a RestaurantPlus cég terméke)

A jövő valamivel nagyobb biztonságot ígér. De ez a biztonsági többlet az életet is megnehezíti. Ilyen például a chipes bankkártya, amelynek használata a leolvasóktól és az ezekkel ellátott számítógépektől függ. A megfelelő intelligens eszközök jópár primitív trükköt ellehetetlenítenek ugyan, de a card not present típusú fizetéseknél továbbra is fennáll a csalás lehetősége. A klónozás nehezebbé válik, de ha a rádiótelefon kártyát is klónozni lehet, akkor semmi sem lehetetlen.

A bankok a hamisítás ellen egy újabb módszerrel is védekeznek. Ez a *felhasználói profil követése*. Azaz igyekeznek kiszűrni az olyan típusú tranzakciókat, amelyek szokatlanok. Ilyenkor – a normálisabb banknál – rövidesen csörög a telefon, és így kérnek megerősítést. A kevésbé normális banknál az ügyfélnek kell kinyomoznia, vajon miért nem működik a kártyája, mondjuk Szingapúrban.

Kis János

Kislexikon

- *Autorizáció:* A kártya meglétének, érvényességének és fedezetének ellenőrzése a kártyakibocsátó bank, illetve a kártyaszervezet elektronikus rendszerében. Eredménye egy engedélykód, amelyre a rendszer később, a folyamat során végig hivatkozik. Amennyiben az autorizációs folyamat negatív, a fizetés nem teljesíthető.
- *Bankkártya:* Olyan plasztiklap, amely csak a számla tulajdonjogát igazolja, és arról legfeljebb pénz felvételére jogosít a bank automatájából. Általában valamely egyéb szolgáltatás logójával is kombinálják. Ilyen esetben elektronikus tranzakcióban debitkártyaként használható fel *(Maestro)*, vagy bankautomatából pénz felvételére jogosító funkciója van *(Cirrus)*.
- *CP, azaz Card Present típusú fizetés:* A kártyának fizikailag jelen kell lennie a fizetéskor. Ilyen, amikor boltban a kártya lehúzásával fizetünk, vagy pénzt veszünk fel az automatából. Az eladóhelyek általában erre a módra kötnek szerződést.
- *CNP, azaz Card Not Present típusú fizetés:* Minden internetes tranzakció eddig ilyen volt. Azaz a kártyának nem kellett fizikailag jelen lennie az internetes fizetéskor, csak ellenőrző adatainak, újabban beleértve a CV kódot is. A chipkártya, amennyiben a számítógéphez olvasó is csatlakozik, lehetővé teszi a CP típusú fizetést.
- *CV, azaz card validate vagy card present kód:* A bankkártya hátoldalán, az aláíráscsíkon egy számcsoporttal több van, mint a kártyán. Ez a CV kód, amelyet eredetileg annak ellenőrzésére találtak ki, hogy a kártya fizikailag is jelen van-e fizetéskor. Most egyes elektronikus fizetési rendszerek kérik, bár az ajánlások szerint ez nem lenne szabályos.
- *Chipkártya:* Most terjedő fokozott biztonságú bankkártya, amelyen az azonosításhoz szükséges adatokat egy szabványos mikroprocesszor chip tartalmazza. Magyarországon csak a *K & H Bank* bocsát ki ilyet. Általában ezek a kártyák is rendelkeznek mágnescsíkkal a hagyományos rendszerekkel való kompatibilitás miatt. Hátrányuk, hogy cserélni kell a teljes fogadó infrastruktúrát, a számítógépeket pedig kártyaolvasóval és programmal kell ellátni. A mikrofizetésekre használt elektronikus pénztárca is chipkártyán alapul.
- *Debitkártya:* Csak a számlán lévő pénz értékéig költhet a kártya tulajdonosa. A legtöbb klasszikus kártya ilyen.
- *Elektronikus bankkártya:* Olyan NEM dombornyomású mágnescsíkkal ellátott kártya, amely kizárólag POS-nél használható fel. Használata a kártya fizikai jelenlétét feltételezi, a bankok általában internetes fizetésre nem engedélyezik.
- *Home banking:* Interneten vagy a bank által adott programmal, megfelelő kódolással a számla kezelése és esetleges tranzakciók kezdeményezése az otthoni vagy munkahelyi számítógépről.
- *Kártya használója, azaz cardholder:* Az a személy, akinek nevére szól a kártya.
- *Kártyaszám:* Adott szabály szerint képzett szám, amely a kártyát azonosítja. Részei: bank és kártyatípus azonosító, amely általában az első négy szám, az utolsó szám a modulo összeadással képzett ellenőrzőkód. Ebből egyes kibocsátók még összeállítják a CV kódot, amely csak az aláírás csíkon, a kártyaszám utáni számcsoportként található. Nemzetközi egyezmények alapján MINDEN kártyaszerű kibocsátásnak, amennyiben sorszámot visel, rendelkeznie kell ezzel a számozási rendszerrel akkor is, ha az nem bankkártya, hanem mondjuk ügyfélszolgálati azonosítókártya, húségkártya stb. Ez egyben lehetőséget ad a banki rendszerekben az egységes kezelésre is.
- *Kártya tulajdonosa:* A mindenkori kibocsátó bank, illetve kártyaszervezet. Ezért a talált kártyákat és sok esetben a lejártakat is nekik kell visszajuttatni, ahol ellenőrzött körülmények között megsemmisítik őket. A kártya használója nem tulajdonos.
- *Klónozás:* Lenyúlt adatok alapján egy másik kártya előállítása, így a kártyából két érvényes példány létezik a letiltásig.
- *Letiltás:* A lopott, elveszett vagy fedezet nélküli kártyákat a kibocsátó bank letiltja. Ilyenkor az autorizációs folyamat negatív eredményt ad, a fizetés nem teljesíthető. A letiltásért a kártya használójának kell fizetnie, cserébe új kártyát kap, ha megfelel a feltételeknek. A kárviselést a bank és a közte lévő szerződés szabályozza, esetleges viszontbiztosításokkal.
- *Hitelkártya:* A számla tulajdonosa adott hitelkeretig folyamatosan költhet. A valódi hitelkártyák jellemzője, hogy nem igényelnek számlán tartott pénzt, a hitelt adott határidőig részben vagy egészében kell visszafizetni.
- *Internet bankkártya:* Kizárólag internetes fizetésre találták ki, először Magyarországon kezdték használni. Általában fizikai valójában nem is létezik, csak egy szintaktikailag a kártyaszámnak megfelelő számsor, amely mögött egy elkülönített számla húzódik. Van olyan bank, ahol a számlaszám egy tranzakcióra szól. Másutt a szám állandó, csak össze van kötve az elkülönített számlával, ahova éppen annyit tesznek át a felhasználók, amennyi az adott tranzakcióhoz kell.
- *Lenyúlás:* Más hitelkártya számának megszerzése trójai programmal vagy egy fizető tranzakciós szerver feltörésével. Tipikus internetes bűncselekmény. A tulajdonos számlája ezután fiktív vásárlásokkal megcsapolható.
- *Mikrofizetés:* A kisösszegű díjak kifizetésének eszköze, általában 5 euróig. A mikrofizetéseknél nem minden tranzakció esetén van banki autorizáció, hanem a nap során egyszer vagy többször a fizetéseket összegyűjtve. Eszköze lehet a számláról adott címletű adatcsomagokkal feltöltött elektronikus pénztárca, vagy az emelt díjú SMS, ahol a díjat a telefonszolgáltató szedi be.
- *PIN:* Personal Identification Number, azaz titkos kód, amelyet meg kell adni egyes tranzakciók alkalmával vagy pénzfelvételkor a bankautomatából. A bankok nem vállalnak lopás esetén felelősséget, ha a számot a kártya mellett tároljuk, és azzal együtt kerül a tolvaj birtokába.
- *POS:* Point of Sale, elektronikus elfogadópont vagy bankterminál.
- *Sasolás:* A PIN kód ellopása azzal, hogy megfigyelik a kéz mozgását a boltokban, vagy a rosszul telepített banki automatáknál. Utána már a zsebtolvajnak az adott PIN-hez tartozó kártyát kell csak ellopnia.
- *Slip:* A hagyományos lefogadás eszköze, az a többpéldányos papír, amelyre egy gyaluszerű eszközzel lehúzzák a kártya adatait hagyományos fizetéskor. Erre értelemszerűen csak a dombornyomásos kártyák alkalmasak.

Hazai IT-biztonság

Minden ötödik megkérdezett magyarországi céget ért már közvetlen anyagi kár az IT-biztonsági hiányosságok miatt, az elmúlt két évben. Ennek ellenére az adatbiztonság kérdését a vállalatvezetők csak közepes fontosságúnak tekintik, állapítja meg a BellResearch tanulmánya.

Az informatikai szakemberek közül sokan ma is vitatják, hogy magas szintű védelmet csak információbiztonságra szakosodott külső cég nyújthat-e, illetőleg a márkás eszközök magasabb szintű védelmet biztosítanak-e, mint a noname termékek.

Fenyegetett világ

Az Egyesült Államokat tavaly szeptemberben ért terrortámadás tovább fokozta a civilizált világ már korábban is meglévő félelmeit: a gyűlölet a rombolás olyan módszereit képes létrehozni, amelyek ellen majdhogynem lehetetlen a tökéletes védekezés. De nem csupán eltérített utasszállító gépekkel, bombákkal vagy lépfene baktériumokkal lehet komoly csapást mérni valamely közösségre. A fejlett országok védelmi, kommunikációs és pénzügyi rendszere ma már olyan mértékben informatikai alapokon nyugszik, hogy a számítógépes terrorizmus hasonló méretű károkat tud okozni, mint a fizikai erőszak.

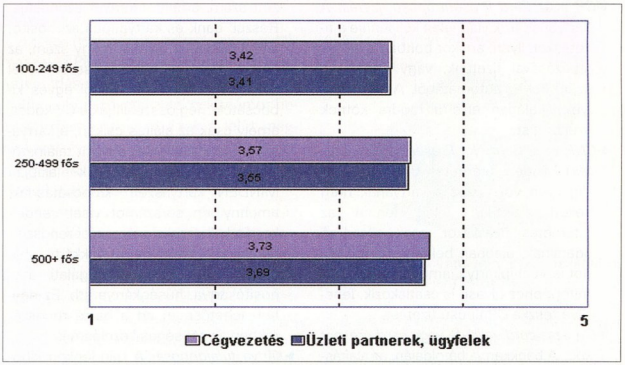
A vállalatoknál felhalmozott, egyre növekvő mennyiségű ügyfél-információ illetéktelen kezekbe kerülése a bizalom elvesztését, végső soron a cég fennmaradását veszélyezteti. Az internet elterjedése az utóbbi években tovább növelte a biztonsági kockázatokat. Ha egy cégnek nincs védelmi stratégiája a webhelyére vagy hálózatába behatoló hackerek ellen, nem tud gyorsan és megfelelően reagálni a támadásra. A legnagyobb problémát az okozza, hogy a biztonságra a szükségesnél kevesebb pénzt fordítanak, mert az informatikai rendszereket pénznyelőknek tekintik, amelyek nem termelnek profitot. *A behatolási lehetőségek felfedése és megszüntetése drága mulatság, de elengedhetetlenül szükséges a kockázat csökkentése és így a veszteségek elkerülése érdekében.*

Naponta hallani hacker-akciókról, szolgáltatásbénító támadásokról, de sok cégnél még mindig úgy gondolják, ez mások problémája, velük ilyesmi nem fordulhat elő, mert megvásárolták a szükséges védelmi eszközöket. Ez azonban még nem minden: a rendszergazdának tudnia kell kezelni ezeket az eszközöket, a munkatársaknak pedig meg kell érteniük, hogy miért van szükség a biztonsági előírásokra.

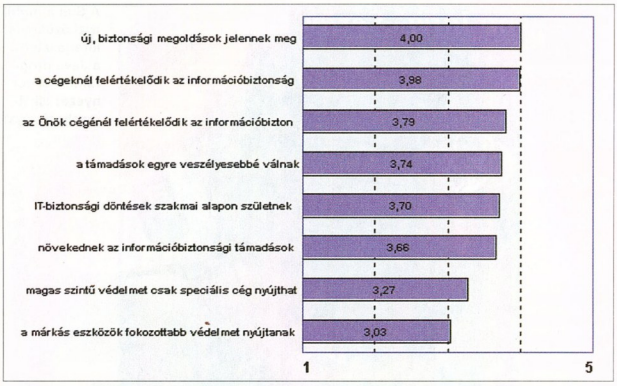
A sikeres támadások nagy része olyan hálózatok, számítógépek ellen irányul, amelyeket felszereltek tűzfallal és más védelemmel. Hogy miért lehetett akkor mégis eredményes a támadás? Mert *a rendszergazdák nem vették a fáradságot, hogy betömjék a biztonsági lyukakat,* így a behatolás nem valami zseni bravúros manővere volt, hanem egyszerű mulasztás következménye. Hiába telepítünk mégoly hatékony tűzfalat is, ha nemtörődömségből vagy hozzáértés híján rosszul konfiguráljuk.

Hasonlóképpen lényeges *a munkatársak megfelelő tájékoztatása.* Az e-mail mellékletek kiterjesztéséből könnyedén megállapítható, hogy egy programot (azaz egy potenciális vírust) vagy csak egy közönséges képet küldtek-e nekünk, aki azonban nincs tisztában a számítógép-kezelés és a biztonsági veszélyek alapjaival, egy rossz mozdulattal pillanatok alatt megfertőzheti gépét.

Mint az elmondottakból is kitűnik, a megfelelő védelem kialakítása több tényezőtől függ: *a vállalatvezetésnek fel kell ismernie a veszély jelentőségét, és elegendő pénzt kell szánnia a biztonsági eszközökre,* a kellő szakismerettel rendelkező rendszergazdákra és a munkatársak biztonságtechnikai képzésére. Szükséges továbbá egy *vállalati biztonságpolitika* kialakítása és annak szigorú betartatása. A *BellResearch* piackutató cég *IT-biztonság iránti attitűd és biztonságtechnikai megol-*



Milyen fontosságú kérdésként kezeli az Önök cégvezetése az IT-biztonságot? Mennyire fontos üzleti partnereik, ügyfeleik számára az Önök cégének IT-biztonsága (az adatok védelme és a rendszerek zavartalan működése)? (1: egyáltalán nem fontos, 5: nagyon fontos; 414 válaszadó).
Forrás: BellResearch 2002



Az információbiztonsághoz fűződő attitűd és védelem megítélése (1: egyáltalán nem ért egyet, 5: teljes mértékben egyetért; 414 válaszadó)
Forrás: BellResearch 2002

dások című tanulmánya, amelyből az alábbiakban közlünk részleteket, az IT-biztonság jelenlegi magyarországi állapotáról ad képet.

Honi helyzet

Az elmúlt két évben a magyarországi cégek közel 20 százalékát érte valamilyen közvetlen anyagi kár különféle információbiztonsági problémák miatt, azonban az IT vezetők megítélése szerint az informatikai adatbiztonságot mind a cég vezetése, mind az üzleti partnerek csak közepes prioritású feladatként kezelik. A BellResearch telefonos felmérése során megkérdezett több mint 400 cég informatikai szakemberei az ötfokú skálán *jellemzően 3 és 4 közötti pontszámokat adtak az IT-biztonság általuk megítélt fontosságára saját cégüknél.* Az IT-biztonság iránti elkötelezettség a cégmérettel egyenes arányban növekszik: az 500 főnél többet foglalkoztató vállalatok esetében mind a vállalatvezetés, mind az üzleti partnerek határozottan fontosabbnak ítélték a kérdést.

A BellResearch tanulmánya alapján egyértelműen kimutatható az a tendencia, hogy a vállalatoknál új, egyre kiforrottabb biztonsági megoldások jelennek meg (4,01) és *a cégeknél általában felértékelődik az információbiztonság* (3,99). Ezzel szemben ellentmondásos annak a megítélése, hogy magas szintű védelmet csak információbiztonságra szakosodott külső cég nyújthat-e (3,28), illetve a neves gyártók eszközei hatékonyabb védelmet biztosítanak-e, mint a noname termékek (3,04). Külső szakértőkre az 500 főnél többet foglalkozató vállalatok szorulnak legkevésbé (3,12-es részátlag, szemben a 3,28-as főátlaggal), amelynek oka a BellResearch elemzői szerint elsősorban abban keresendő, hogy *a nagyobb cégeknél házon belül nagyobb arányban foglalkoztatnak információbiztonságra szakosodott munkatársakat.* E vállalatok 36 százaléka alkalmaz saját biztonsági szakembereket, míg a 100-249 fős vállalatoknak csupán a 22 százalékáról, a 250-499 fős cégeknek pedig csak a 27 százalékáról mondható el ugyanez.

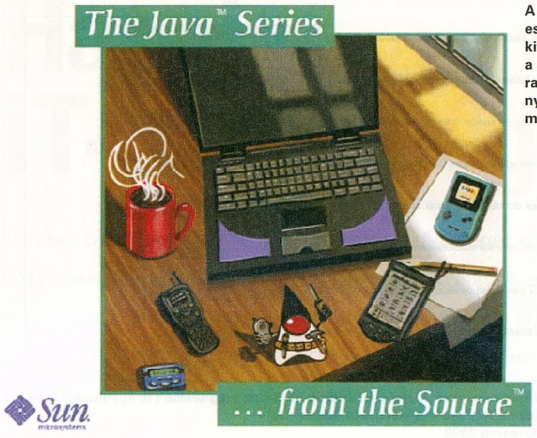
Kutatási módszer

A biztonsági kérdések világszintű felértékelődése ellenére mindeddig nem született olyan elemzés Magyarországon, amely a hazai cégek felkészültségét, információbiztonsági tudatosságát, a vállalatvezetés hozzáállását és értékrendjét vizsgálta volna, nem is szólva a biztonsági termékek és szolgáltatások iránti igény számszerűsítéséről. Ezt a hiányt pótolja a BellResearch tanulmánya, amely a vállalatok informatikai biztonsághoz fűződő hozzáállásán, megoldásaik fejlettségén, külső tanácsadói szolgáltatások iránti igényén és IT-biztonsági megoldásokba való beruházási hajlandóságukon keresztül mutatja be a keresleti piac érettségét és fejlődési potenciálját – kvantitatív, statisztikailag megbízható adatokra alapozva.

A kutatás célcsoportját a 100 főnél több munkatársat alkalmazó, internet-hozzáféréssel és legalább 20 számítógéppel rendelkező közép- és nagyvállalatok alkották. A megkérdezett 414 vállalat közül 196-ben 100-249, 111-ben 250-499, 105-ben pedig 500-nál több alkalmazottat foglalkoztatnak. A cégek tevékenység és regionális ágazat szerint reprezentálják a célcsoportot. Az adatgyűjtés telefonos interjúval történt a BellResearch call centerében, 2001. október 29. és november 16. között; az interjúk átlagos hossza hozzávetőlegesen 20 perc volt. Az interjúalanyok a cégeken belül az informatikai (biztonságtechnikai) kérdésekben döntéshozatali jogkörrel rendelkező vállalati vezetők voltak.

A BellResearch **(www.bellresearch.com)** magyar szakmai befektetők tulajdonában lévő, független piackutató és tanácsadó cég, amelyet a telekommunikáció, az informatika és az internetgazdaság területén vezető szerepet betöltő vállalatok marketinginformációs igényeinek kielégítésére hoztak létre. **M. Cs.**

A vállalatok és magánszemélyek egyre több bizalmas adatot tárolnak a számítógépeiken, ezért egyre nagyobb hangsúlyt kap az informatikai biztonság. Az asztali gépek, notebookok, PDA-k után a mobiltelefonokat is elérte az internet, így azok adatvédelme is fontos szempont ma már.



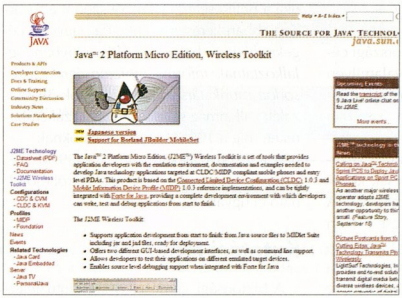
A Sun a mobil eszközökre is kiterjesztette a Java programozási környezet alkalmazhatóságát

JAVAsolt biztonság

Az internet és az internet-alapú alkalmazások elterjedése miatt a vállalati folyamatok egyre jelentősebb része zajlik internetes felületen, és így azok fokozottan ki vannak téve a különféle támadásoknak. Az informatika fejlődésével az adatok nemcsak a jogos felhasználók számára válnak egyre értékesebbé, hanem a konkurencia, a hackerek és más illegális behatolók számára is.

Természetesen vannak olyan intézmények, amelyeknél az adatvédelem hagyományosan már most is nagy hangsúlyt kap – ilyenek a kormányzati, a nemzetbiztonsági és katonai szervek, a pénzügyi szervezetek – ezeknél azonban a védekezés elsősorban azon alapul, hogy rendszereik nem kapcsolódnak a nyilvánosan elérhető hálózatokhoz. S mivel jelenleg a vírusok jelentős részét PC-s környezetre írják, azok elsősorban ilyen környezetben jelentenek veszélyt, Javás környezetben sokkal kevésbé.

Ugyancsak napról-napra nő az igény, hogy a tavaly tapasztalt számítógépes kórokozók (*Code Red, Nimda és Goner*) gyors és igen széleskörű elterjedését egyre hatékonyabban ki tudja küszöbölni a cég számítógépes rendszere. Egyes becslések szerint csak a Code Red vírus mintegy *2 milliárd dolláros kárt* okozott a világ informatikai rendszereiben. A hálózaton terjedő számítógépes kórokozók 2000-ben mintegy háromszor annyi fertőzést okoztak, mint 1995-ben és 96-ban együttesen. Ennek megfelelően a vállalatoknak fokozott figyelmet kell fordítaniuk az internetes biztonságpolitikára.



A J2ME Wireless Toolkit segítségével a mobiltelefonokra és PDA-kra fejleszthetünk alkalmazásokat

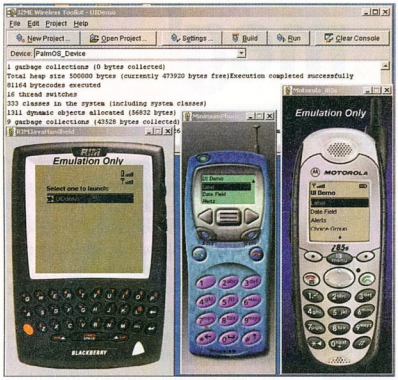
Új fejezet a biztonságban

A *Java* technológia, a *Sun Microsystems* internetes programozási környezete és nyelve jelenleg az egyik legelterjedtebb, valóban platformfüggetlen és biztonságos internetes programozási nyelv. A Java azáltal, hogy biztonságot nyújt az egész hálózaton, ideális az olyan alkalmazások esetében is, amelyek emeltszintű biztonságot követelnek meg, mint amilyen például az *elektronikus kereskedelem* vagy az *internetes banki szolgáltatások*. A Java programozási nyelv *„írd meg egyszer, és futtasd bárhol”* tulajdonságának köszönhetően az alkalmazások egyetlen környezetben fejleszthetők, majd tetszőleges platformon futtathatók, időt és pénzt takarítva meg minden cég, intézmény számára.

Becslések szerint jelenleg a világon mintegy *7 millió weboldal használja a Java programnyelvet*, és további sok millió vezeték nélküli kommunikációs eszközben használják fel folyamatosan a Java programnyelven írt fejlesztéseket, alkalmazásokat.

Java a mobilokban

A mobilkészülék-gyártók, a mobilszolgáltatók, valamint az érvényes tendencia szerint a mobilkészülékek piacán már



A Wireless Toolkit különféle mobiltelefonok emulációját is tartalmazza

nem az új előfizetők toborzása, hanem *a meglévő készülékek cseréje és a hozzáadott értékű szolgáltatások* növelik a bevételeket. 2002-től kezdődően az értéknövelt, azaz új alkalmazásokat és szolgáltatásokat nyújtó készülékek fogják kitenni a piac egyre nagyobb hányadát. Ennek alapvető eszköze a Java környezet alkalmazása.

A Java által kínált nyílt környezet lehetővé teszi, hogy a *külső fejlesztésű alkalmazásokat folyamatosan letölthessük a mobiltelefonra*, újabb és újabb alkalmazásokat telepíthessünk a mobilkészülék teljes élettartama során, nemcsak a kezdeti vásárláskor.

A mobilszolgáltatók számára az alkalmazás-letöltés várhatóan emeli majd a forgalmat, valamint új bevételi lehetőségeket nyit: díj megfizetése ellenében új szolgáltatásokat vezethetnek be, vagy rendelkezésre bocsáthatnak letölthető tartalmakat, például játékokat.

A *Sun Microsystems* nemrégiben jelentette be az iparág első kezdeményezését arra nézve, hogy a webes szolgáltatások szabványai *mobil és kisméretű kliensberendezésekre, például mobiltelefonokra, PDA-kra, set-top készülékekre, autós rendszerekre és otthoni internetes eszközökre* is eljussanak. Az új szolgáltatás a *Java 2 Platform, Micro Edition-re* építve segít a műszaki architektúra egyesítésében, a háttérszerverektől egészen a kis készülékekig. Elemzői becslések szerint *2006 végére több mint egymilliárd Java-alapú kézi készülék lesz forgalomban.*

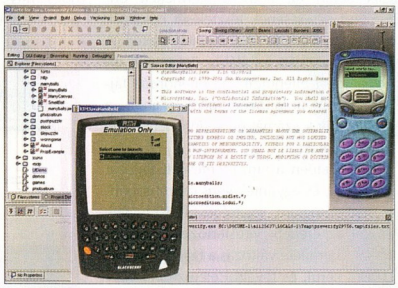
A Java 2 Platform, Micro Edition (J2ME) a Java platformnak az a része, amely a mobil, kézi eszközök, úgymint mobiltelefonok, személyes digitális asszisztensek és személyhívók, autóba épített rendszerek és smartcardok egyre szélesebb körének az igényeit célozza meg.

Az iparág olyan óriásai használják és terjesztik a Java platformot, mint az *IBM*, az *Oracle*, az *SAP*, a *Sony*, a *Motorola*, a *Nokia*, a *HP*, az *Ericsson*, a *Philips* vagy a *Matsushita*. Más világcégek, mint a *Palm*, a *BEA* vagy a *Cisco* aktívan közreműködnek a Java terjesztésében.

Az első fecskék

A Java technológiákban rejlő ígéretes lehetőségekre építve a *Sun Microsystems Inc*, a *Nextel Communications, Inc.* és a *Motorola, Inc.* bevezette az első Java technológiával működtetett telefonokat és szolgáltatásokat.

A *Motorola i85s* és *i50sx* készülékek Java technológiát tartalmaznak, amely lehetővé teszi a személyre szabott és interaktív szolgáltatások bevezetését. Az új Motorola telefonok kezdeti szolgáltatásai között szerepelnek például a specializált üzleti számológépek vagy a költségjelentés-készítő szoftver. A most rendelkezésre álló szolgáltatásokon kívül még számos további alkalmazás fejlesztése is folyamatban van.



A demók segítségével ellenőrizhetjük, hogyan fest majd a Java alkalmazás a mobilon

A *Sony Ericsson* is a Java technológiára vonatkozó licencszerződést írt alá a Sun Microsystems-szel, mivel a játékok és a szórakoztató szolgáltatások a Sony Ericsson termékstratégiájának alapvető részét képezik. A Java kulcsfontosságú része a multimédiás kommunikációs alkalmazások fejlesztésének.

Gy.L.

A Java előnyei

A Java technológiák számos előnyt kínálnak a vezeték nélküli szolgáltatások támogatása terén:

- Az alkalmazások betöltése igény szerint történik. *A felhasználó dönthet úgy is, hogy igény szerint tölti le az alkalmazásokat ahelyett, hogy az eszköz gyártója által előre telepített alkalmazásokkal feltöltött készüléket vásárolna.* Ez segít megőrizni a felhasználó vezeték nélküli eszközzel kapcsolatos befektetésének értékét, és lehetővé teszi a szolgáltató számára, hogy javítsa és bővítse szolgáltatás-kínálatát.
- A Java technológiákhoz olyan könyvtárak tartoznak, amelyek az alkalmazásfejlesztő számára lehetővé teszik a *gazdagabb, intuitívabb grafikus felhasználói felületek kialakítását.* Ezáltal a szolgáltatók személyre szabott és vonzó alkalmazásokat és szolgáltatásokat kínálhatnak, miközben azok használatát is megkönnyítik.
- A Java technológia lehetővé teszi *a hálózati sávszélesség intelligensebb kihasználását* (például *GPRS*), mivel az alkalmazások letöltődnek a készülékekre és ott kerülnek felhasználásra. A hálózatra csak akkor kell felkapcsolódni, ha adatokra van szükség a szerverről.
- A Java technológia a vezeték nélküli eszközökön teljesen új fejlesztői platformot hoz létre, amely *többféle készüléktípust és rendszerek közötti platformokat fog át.* A hálózati infrastruktúrában a Java platform robusztus végpontok közötti megoldást képvisel, amely lehetővé teszi a fejlesztők számára, hogy ugyanazokat az eszközöket és ismereteket használják új szolgáltatások fejlesztésében és bevezetésében.

Valaki mondja meg!

Özönlenek a vírusok, és mostanáig egész Magyarországon nem létezett olyan tesztlabor, amely naprakész és hiteles információt adhatott volna a vírusokról és a vírusellenes szoftverekről. Áprilisban a veszprémi Veszprog Kft. elindította a gyártóktól és forgalmazóktól független víruslaborját.

A *Dr. Leitold Ferenc* által vezetett *Veszprog Kft.* 1997 februárjában alakult. Kizárólag magyarországi magánszemélyekből álló társaságról van szó, amely főként szoftverfejlesztéssel, valamint szoftverek, szoftverrendszerek minőségbiztosításával foglalkozik.

A Veszprog szakemberei a *CheckVir* projekt keretében még 2000-ben kezdték el az antivírus tesztelési problémák megoldását segítő automatikus, illetve félautomatikus eljárásokat fejleszteni.

2002. márciusában hirdették meg, s áprilisban indították el a Magyarországon újdonságnak számító tesztsorozatukat, amely az antivírus termékek korábban példátlan mélységű vizsgálatát ígéri.

A havonta ismétlődő vizsgálatokat az alábbi platformokon végzik a tesztlaborban: MS-DOS 6.22, Windows 95/98/ME, Windows NT Workstation és Server, Windows 2000 Server és Professional, Novell Netware 5.0, 5.5 és 6.0, valamint Linux.

A tesztelésre korszerű, P IV/2000 processzoros, 512 Mbájt memóriával, CD-vel, merevlemezzel, hálózati adapterrel ellátott számítógépeket használnak, amelyek szigorúan zárt rendszert alkotnak. A vizsgálatokhoz felhasznált vírusok tenyésztését (egy-egy tesztre több százezer vírust kell előkészíteni vírusonként több ezres darabszámban!) egy speciális, saját fejlesztésű és szigorúan ellenőrzött, naplózott, így valóban reprodukálható és hiteles – *Debian Linux* alapú – rendszerben végzik.

A CheckVir projekt alapvető célja, hogy az antivírus fejlesztőktől függetlenül teszteljen antivírus szoftvereket és megoldásokat, egyaránt segítve a felhasználókat és az antivírus fejlesztő cégeket. A rendszeres

A víruslabor gépei napi 24 órában dolgoznak

antivírus teszteket a megadott alapelvek alapján, a 2002 évi tesztelési tervekben meghatározott ütemterv szerint végzik. Az aktuális hónap tesztjeinek lezárását követően a tesztelések havi eredményei 2002. április 30-tól mind megtalálhatók a **www.checkvir.hu** weboldalon.

Az előzetes tesztek fő célja a vírusirtási lehetőségek tesztelése és elemzése volt. Az antivírus termékek keresési lehetőségeinek ellenőrzése a naplófájlok elemzésével egyszerűen megoldható. Az előzetes teszt során az antivírus termékek on-demand keresésének tesztelését célozzák meg a víruskeresés és eltávolítás esetén. A naplófájl alapján az alábbi összesített információkat ellenőrzik: az ellenőrzött fájlok számát, a fertőzött fájlok számát, a gyanús fájlok számát és a vírusmentesített fájlok számát.

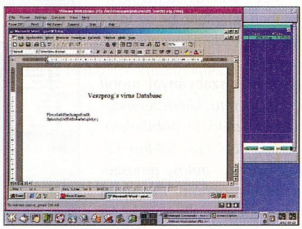
Ezt követően a vírusmentesített fájlokat ellenőrzik, és egy intelligens összehasonlító segédprogram segítségével összevetik azokat az eredeti, vírusfertőzés előtti fájlokkal. Bármiféle változás a fájlokban naplózásra kerül, és további elemzések, vizsgálatok tárgya lesz.

A tényleges tesztek a következőkre terjednek ki: vírusfelismerés, vírusirtás, hibakezelés, helyreállítás, problémás esetek. Az egyes antivírus szoftvereket a tesztelendő vírusok kisebb (kb. 700 ezer – 1 millió fertőzött állomány) csoportjával ellenőrzik. A teszteléssel kapcsolatban az egyik legfontosabb elvárás, hogy minden tesztpont reprodukálható legyen. Akkor és csak akkor jeleznek egy problémát vagy hibát, ha azt egzakt módon meghatározható lépések sorozatával ismételten elő lehet idézni.

Tesztjeikben határozottan megkülönböztetik a *problémát* és a *hibát*. A probléma azt jelenti, hogy egy új szolgáltatást, lehetőséget kellene kialakítani a tesztelt termékben (például az antivírus szoftver nem talál meg egy konkrét vírust vagy nem tudja azt eltávolítani), a hiba pedig azt jelenti, hogy a tesztelt antivírus szoftver nem megfelelően viselkedik (például azt jelzi a felhasználónak, hogy egy bizonyos vírust eltávolított, de a megtisztított programot nem lehet elindítani). Az alkalmazott tesztelési eljárások legfőbb célja, hogy radikálisan csökkentsék az antivírus termékek hibáinak és problémáinak számát.

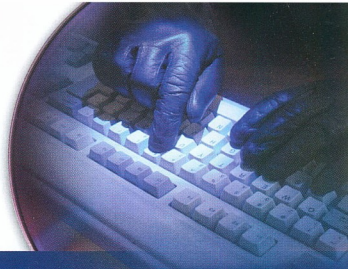
A teszteket a CheckVir laborba hivatalosan beküldött (általában 10-15) programcsomaggal végzik, a teszteredményeket a beküldők megkapják, s így javíthatnak termékeik esetlegesen felfedezett hiányosságain. Az eredmények publikusak, azaz nem csupán a programok beküldői, de bárki letöltheti ingyen és bármentve azokat, s felhasználhatja annak eldöntésére, hogy milyen irányban fejleszti számítógépeit, informatikai rendszerét.

dr. Nagy Gábor



A tenyésztő rendszer Debian Linux alatt működik

Hacker kézikönyv



Feltörés és védelem

Figyelnek bennünket. Kifürkészik legféltettebb titkainkat. Igen, ők a hackerek. Belegondolt már, hogy mihez is kezdhet egy hacker az Ön bizalmas vagy éppen személyes adataival? Tulajdonképpen mennyire is biztonságos az Ön PC-je? Ezt csak egy hacker tudhatja...
(...de Önt nem érheti váratlanul, ha elolvassa könyvünket.)

A Hacker kézikönyv talán befolyásolni fogja a biztonságérzetét és a magatartását is. Bepillantást nyerhet ugyanis a színfalak mögé, gondolkodásmódokat és stratégiákat ismerhet meg. Olyanokat, amelyek talán kamaszosak, ettől azonban nem kevésbé veszélyesek. És azt is meg fogja tudni, hogy a legveszélyesebb dolgok nem igényelnek különösebb tudást – egy makrovírust valójában mindenki meg tud írni.

Az előzmény

A *Hacker kézikönyv* szerzője éveken át tevékenykedett ezen a területen, és jól ismeri a dolgok menetét. Egy német nagybankba történt látványos betörés tette ismertté a nevét, amelynek során másfélmillió ügyféladatot kémleltek ki. „Egy pár számlát leüríthettünk és leléphettünk volna", – mondta a team egyik tagja. Ehelyett nyilvánosságra hozták a támadást, és ezáltal új jelentőséget nyert az online banki szolgáltatás témája.

Élesben tesztelve!

A számítógépek és a hálózatok megtámadásának itt bemutatott módjai a gyakorlatban többszörösen kipróbáltak. Ebből a könyvből sokat meg fog tudni résekről és lyukakról, sőt, a végén még akár egy makrovírust is tud majd írni. A szerző és a szerkesztők, akik hónapokon keresztül foglalkoztak a könyvvel, már egy új képernyőkímélőt sem töltenek le, és persze ismeretlen feladók csatolt fájljait sem nyitják meg.

A könyv

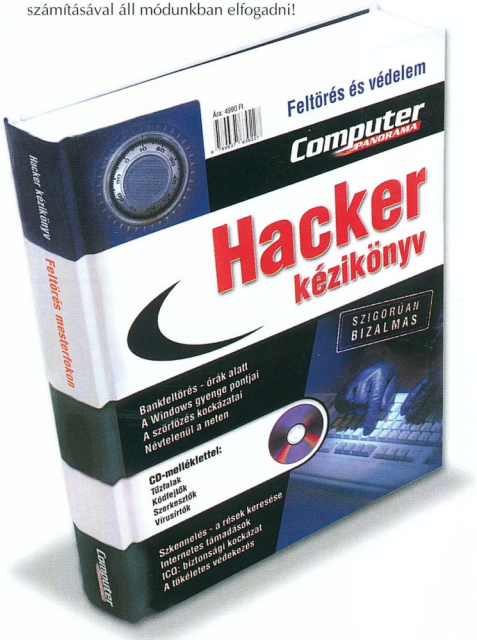
Ez a könyv helyenként olvasható krimiként, de semmi esetre sem regény. Esetenként technikai alapismeretekkel és programkódokkal fog szembesülni – mindkettőnek megvan a maga értelme. Ha eddig nem is érdeklődött a TCP/IP iránt, akkor is tudnia kell, milyen támadási lehetőségeket kínál ez a protokoll. A programkódok nem az Ön elrettentésére szolgálnak, hanem többnyire kommentárként. Egy vírust, mint amilyen az ILOVEYOU, a szeme láttára boncol fel alkotórészeire, és magyaráz el a szerző. Ez jelentősen megkönnyíti a kockázatok felmérését.

CD-melléklettel

Könyvünk persze arról gondoskodik, hogy Ön egy pillanatra se maradjon védelem nélkül. Éppen ezért a CD-mellékleten remek vírusirtó programokat, tűzfalakat, bináris szerkesztőket kínálunk.

Nincs postaköltség!

Önnek nem kell sem posta-, sem csomagolási költséget fizetnie! Így nem kell könyvesboltokba mennie, ezzel időt, benzint és parkolási költséget takarít meg. A könyv ára mindössze 4990 Ft, amelyet az újságban található csekkel fizethet be. Ez az ajánlatunk korlátozott ideig, az **december 31**-ig befizetett megrendelésekre érvényes! Utána a megrendeléseket csak postai díj felszámításával áll módunkban elfogadni!



Computer Panoráma Kiadói Kft. • 1091 Budapest, Üllői út 25. • Tel.: 456-6964
E-mail: terjesztes@cpanorama.hu • Web: www.computerpanorama.hu

LG

OPTIKAI TÁROLÓK

World No.1

2001/7 Computer Panorama
I. helyezett

AZ LG OPTIKAI MEGHAJTÓK NEMZETKÖZI DÍJAI

LG Electronics Magyar Kft.
www.lge.co.hu

Computer Hoy | Calidad
Feb. 01 Spain
CED-80808

Chip | Performance Winner
Nov. 01 Germany
CED-80808

Computer easy | EMPFEHLUNG
Oct. 01 Germany
CED-80808

PC Plus | Performance Award
Aug. 01 UK
CED-80808

PC QUEST | Editor's Choice
Jun. 50 India
CED-80808

Computer Partner | Component for reference PC
May. 01 Germany
CED-80808

Computer Bild | Test Winner
May. 01 Germany
CED-80808

PC WORLD KOMPUTER | Our Best Purchase
Apr. 00 Poland
CED-80808

Computer Channel | Best Performance
Mar. 01 Germany
CED-80808

PC Direkt | EMPFEHLUNG
Jan. 01 Germany
CED-80428

PC Praxis | Fast rezzider
Jul. 00 Germany
CED-80808

Chip | Tip Econo
Jan. 01 Poland
DRD-81208

PC Go | EMPFEHLUNG
DRD-81208

PC Praxis | Price Tip
Jul. 00 Germany
DRD-80808

PC Magazine | Editor's Choice
Jun. 00 UK
DRD-80808

PCWelt | Test Winner
May. 00 Germany
DRD-80808

Enter | Editor's Choice
Mar. 00 Poland
DRD-80808

PC format | Gold Award
Mar. 00 South Africa
DRD-80808

PC SHOPPING | EMPFEHLUNG
Jan. 00 Germany
DRD-80808

Computer Channel | Test Winner
Feb. 00 Germany
CED-84908