# 2001. MÁRCIUS



## EDITOR



### Communicare necesse est

**Mindenki úgy építgeti a maga kis országának imázsát, ahogyan tudja.**

**Kelenhegyi Péter főszerkesztő**

kelenhegyi@byte.hu

Állítólag az internet mindent megváltoztat. Kihat kulturálódási igényeinkre, vásárlási szokásainkra s főleg az üzleti életre. Megváltoztatja a világról alkotott képünket és rákényszerít arra is, hogy újrarajzoljuk a világnak mutatott arculatunkat. Csakhogy a tőzsdei bizonytalanságok, egy sor dotcom cég likviditási gondja, sőt csődje nyomán sokan hallani sem akarnak többé az e-business forradalomról. Pedig „utólag tisztán látható: az új internetes cégek többsége eleve halálra volt ítélve, hiszen csak vázlatos üzleti tervvel és életképtelen bevételi modellel vágott bele a vállalkozásba, így amint a pénzforgalom, a nyereségesség örök gazdasági törvényei jelentkeztek, nem volt esélyük a túlélésre".

E gondolatok abban a felmérésben olvashatók, amelyet a KPMG készített az ügyfélkörébe tartozó magyar vállalatok e-felkészültségéről. Ha hinni lehet a válaszoknak, a hazai üzleti szféra szereplői – de legalábbis a vegyipari és gyógyszergyártó cégek, a pénzügyi szektor vállalatai, valamint az informatikai, kommunikációs és szórakoztató ipar cégei – többségükben felkészültek az e-businessre. Átgondolták e-üzleti stratégiájukat, saját technológiai infrastruktúrájukat megfelelőnek tartják az elektronikus üzleti fejlesztésekhez, talán csak a szervezetüket nem sikerült még kellőképpen az újgazdaság igényeihez igazítaniuk, s a felkészültebbek sem rendelkeznek részletes, dokumentált stratégiával.

S bár a cégek felső vezetői általában tisztában vannak az átalakulás szükségességével, az e-gazdaságot jellemző új vállalati kultúra még nem honosodott meg; az e-stratégia, a vezetés ez irányú lépései nem jelennek meg a vállalaton belüli kommunikációban.

Communicare necesse est – olvasom a római szállóige kifordítását egy olyan weboldalon, amelyhez az országimázs szó begépelésével vezet az út a Miniszterelnöki Hivataltól. Vajon milyen arcot mutat magáról az ország egésze a világhálón? A MeH.hu címen keresve százszázalékos a találat: Országimázs = Hajrá, magyarok! Innen küldhetünk üzenetet a sidneyi olimpia magyar résztvevőinek.

Aki azonban nem a kormányzati negyedben keresi az országimázst, hanem az Alta Vista keresőjével, pillanatok alatt rálelhet a *www.kancellaria.gov.hu*

*/hivatal/felepites/orszagimazs/orszag-imazs.htm* oldalra. Jóllehet a legendás augusztusi tűzijátékról egy szó sem esik, megtudhatjuk például azt, hogyan vélekedtek múlt ősszel Magyarország EU-csatlakozásáról a megkérdezett külhoni és belföldi polgárok. Az egyre szűkszavúbb grafikonokon végighaladva pedig a tizenhatodiknál megtalálható a válasz arra a kérdésre is, megteszik-e az ország vezetői azt, ami az uniós tagsághoz szükséges.

Communicare necesse est.

Nos, ennyi bevezető után elárulhatjuk: mi sem maradtunk tétlenek. Elkészült az az országos médiaanalízis, amely magában foglalja a BYTE Magyarország olvasótáborának elemzését. Mielőtt szó érné a ház elejét, szögezzük le: nemcsak a divat vitt rá bennünket, hogy „országimázst" készíttessünk, s főleg nem tűzijátékos látványosságokat akartunk látni és mutatni.

Persze jó érzés, hogy belső tükrünk eddig sem mutatott torzképet. Jó tudni, hogy hónapról hónapra legalább hatszor annyian veszik kézbe lapunkat, mint ahányan előfizetői címlistánkon szerepelnek. És fontos visszajelzés számunkra a többi adat is: a fővárosiak és Budapest környékiek, illetve vidékiek egészséges (33–17–50 százalékos) megoszlása, a kimagaslóan nagy vásárlóerővel bírók aránya, az országos átlagot jócskán felülmúló iskolázottság, az internet-hozzáférés, a műveltség és a nyelvtudás, egyszóval az, hogy a szakmai elitnek, elsősorban művelt, több nyelvet beszélő, megtakarított pénzüket befektetni kész férfiaknak írunk.

A Szonda Ipsos és a Gfk Hungária Nemzeti Média Analízise csak a címében hangzatos, a tartalom, az eredmény mentes minden pompától; mindössze egy hosszú Excel számoszlop, amelyet jól értelmezve tovább építhetjük imá-zsunkat. Értelmezni persze sokféleképpen lehet a mégoly független szakértőktől származó adatokat is. Mivel azonban „csupán" a magunk érdekéről van szó (és nem a következő választásokig kell ellavíroznunk valahogy, hanem a következő számunk olvasóit kell újra meg újra megszólítanunk), szeretnénk elkerülni az országimázs-exportálók szokásos csapdáit.

Mert – legyen bármily botrányos kis ország a miénk – a politizálástól sem mentes szaksajtó mégsem afféle kormányzati portál, amelyen belépve vegytiszta optimizmus lengi körül a látogatót, de nem is amolyan zugfórum, ahol bárki sárral dobálhatja a másikat.



## HÍREK



## E-GAZDASÁG

**IMV**

Információs társadalom

Az Európai Bizottságnak a kutatást és fejlesztést, valamint a technológia terjesztését célzó projektjeit tartalmazó ötös számú, az Információs Társadalom Technológiai Programja (IST) nevű keretprogram állt az IMV 2001 előadásainak középpontjában. Az első napon brit, finn, német, olasz és cseh előadók ismertették a kutatóhelyeiken, egyetemeken, kutatóintézetekben, gyártóhelyeken elért eredményeket. A példák a gyakorlatban mutatták a képfelismerő technológia alkalmazását többek között fűrészüzemben, a precíziós eszközök vékonyréteg-bevonatának kialakításában, a papírgyártásban, a humánsebészetben. Az előadások tematikája kapcsolódott az Európai Unió 1997–2000. évre szóló kiemelkedő kezdeményezéséhez, a HPCNTTN hálózathoz (High Performance Computing and Networking, Technology Transfer Nodes). A Műegyetemen rendezett technológiai konferencia második napján az Európai Bizottság képviselője ismertette az Információs Társadalom Technológiái programot, valamint a szervezet új (6. sz.) felhívását. A Trial elnevezésű projektek az ipari és szolgáltató ágazatban a felhasználóknak és beszállítóknak segítenek a vezető technológiák átvételében és alkalmazásában. A Best Practice projektek a felhasználókat segítik az iparban és a szolgáltatásban bevett gyakorlati, eljárásbeli és működéssel kapcsolatos témák, megoldások és technológia megismerésében. *www .cordis.lu/ist.*

**EHT**

Közigazgatási egyeztetés

Februárban elkészült az egységes hírközlési törvény újabb, tizedik tervezete, amely az illetékes minisztérium reményei szerint legkésőbb március közepéig a parlament elé kerülhet – hangzott el a Figyelő fórum megnyitó előadásában. *Stumpf István* miniszter szerint a mostani verzió számos ponton eltér az eddigiektől, számos újdonságot tartalmaz, így valószínűleg a reakciók is megoszlanak majd. Ezért a minisztérium munkabizottságot állított fel, amelynek feladata, hogy a reakciókat megszűrje, és a szabályozók, a törvényszöveg kidolgozóinak egyértelmű megfogalmazásokat adjon. Ez a munkabizottság februártól – a MEH miniszterének vezetésével – hetente ülésezik. Szintén készül az elektronikus aláírás törvénytervezete és az elektronikus közbeszerzésről szóló törvény, amelynek alapján a jövő évtől megnyílik az elektronikus közbeszerzés lehetősége. Az információs társadalom civil programjaira idén 2,3 milliárd forintot különít el a kormány, az ezzel kapcsolatos pályázatok beadási határideje 2001. január 31-én járt le – közölte a miniszter a Montana Rt. és a Sun Microsystems Magyarország támogatásával megrendezett Figyelő fórumon. További információ: *www.kancellaria.gov .hu/tevekenyseg/.*

**ICL Hungary**

Netbanki kérdőjelek

Banki szakembereknek rendezett szemináriumot februárban az ICL magyarországi képviselete. A résztvevők a fiókhálózat fejlesztésének szükségességét megkérdőjelező internetes banki szolgáltatásokról folytathattak véleménycserét. *Braun Péter,* az OTP Bank vezérigazgató-helyettese a bankvilág változásairól, kihívásairól szóló előadásában hangsúlyozta, hogy a bankoknál is az ügyfélkapcsolat-menedzsment elektronikus eszközeié (a CRM-é) és az adatbányászaté a jövő, ám a bankok esetében a korszerű megoldások bevezetése óvatosabban zajlik: egy ma nyilvánosságra kerülő technológiai újdonság mintegy hét-nyolc év múlva lehet jól használható banki alkalmazás építőeleme. Mindenképp a megbízható, mobil ügyfélkiszolgálás és a 7×24 órás szolgáltatás bevezetése várható a jövőben, de a kockázatok (központosított online adattárak, nyitott bankok, internet stb.) is növekednek. Az ICL előadói szerint a CRM a pénzügyi szektorban is a vállalati stratégia fontos eleme, azonban a fókuszeltolódásokkal itt is számolni kell: stratégiai szinten a régi, termékközpontú helyett az ügyfélközpontú megközelítés felé, a megvalósítás szintjén az ügyféligények teljes megértése felé s a támogató eszközök területén a technológiai igény helyett az emberi tényezők felé kell fordítani a figyelmet. A szemináriumon szó volt még a döntéstámogatásról, az elektronikus banki szolgáltatások elvárt biztonságáról, a magas szintű rendelkezésre állásról, a banki befektetési információszolgáltatásról, a mobilkapcsolatok térhódításáról és az intelligens kártyák bevezetéséről. *www.icl.hu.*

**Cisco Systems**

Hálózati egyetem

Február 14-én rendezték meg a Cisco hazai értékesítési partnereinek a Cisco University újabb előadás-sorozatát, amelynek fő témái az ügyfél igényeinek felderítése, a hálózat feltérképezése, megtervezése, a LAN/WAN hálózatok tervezése, a címzés és a névhasználat, az útválasztó protokollok, a Cisco IOS operációs rendszer, a hálózatmenedzsment, a prototípus és a pilot készítése voltak.

Tartalomszállító szolgáltatók

A múlt hónapban a Cisco Systems Magyarország szűk körű bemutatón ismertette a Content Delivery Networks (CDN) műszaki, technológiai koncepcióját, valamint a Cisco CDN-ek fő komponenseit. Az előadó szerint a Cisco hazai gold partnerei, az LNX és a Synergon már felkészültek az internet- és tartalomszolgáltatók CDN-igényeinek kielégítésére. Információ: *www.cisco.hu.*

**eBolt**

Áruházi hitel

Az 1999 júniusa óta működő eBolt internetes áruház árbevétele tavaly megközelítette a százmillió forintot, látogatóinak száma havonta 40 ezer körül van – hangzott el az eredményeket összegző februári sajtótájékoztatón. Az elsősorban műszaki cikkeket forgalmazó cég nemrégiben internetes áruhitel-akciót indított a Credigen Rt.-vel együttműködésben. A hiteligényléshez elegendő az online adatlapot kitölteni, amelyet a Credigen Rt. hitelbírálat után hagy jóvá. A procedúra munkanapokon és munkaidőben maximum egy órát vesz igénybe. A részletfizetés lehetőségével egyelőre csak a Budapesten és környékén élők élhetnek, de a tervek szerint hamarosan az ország más területein lakóknak is elérhető lesz a szolgáltatás. Az áruház, amelynek keretrendszerét a német Hybris cég elektronikus áruházi rendszerének licencére alapozva az Areco Systems Kft. fejlesztette, a főbejáraton kívül elérhető a BYTE Magyarország, az MTI, az Origo, a Prim Online és a Windows.hu oldalakról is. További információ: eBolt Kft. Tel.: 464-7550. *www.ebolt.hu.*

**The Argonauts**

Az aranygyapjú nyomában

Többhavi jelenlét és egy sor projekt után lépett a sajtónyilvánosság elé a német származású webfejlesztő cég, az argonauták magyarországi csapata. Mint *Török Tamás* ügyvezető hangsúlyozta, szolgáltatásaikkal elsősorban a Magyarországon tevékenykedő multinacionális vállalatokra koncentrálnak. A jelenleg hat munkatársat és külső

szakembereket foglalkoztató leányvállalat olyan ügyfelek hazai projektjeiben vett részt, mint a Nokia Magyarország, a Grey, a British American Tobacco, az Alfa Romeo, a Lancia, a Fiat és a MasterFoods. A website-specialisták e-fogyasztói szolgáltatási palettáját *Hansjörg Zimmermann,* a német cég egyik alapító tulajdonosa a következőkkel jellemezte: stratégiakészítés, márka- és arculatkialakítás, projektmenedzselés, koncepció kialakítása, anyagok írása, tervezése, mobilszolgáltatás, felületprogramozás, háttér-integráció, márkakommunikáció, a fogyasztók megszerzése és megtartása. További információ: *www.argonauts.hu.*

**CityReach**

Budapest után Dublin

A CityReach International (CRI) Dublinban nyitotta meg legújabb európai létesítményét. A CRI az üzleti internethez szükséges infrastruktúra és szolgáltatások pán-európai szállítója. A több mint 11 ezer négyzetméteres központ a CRI-hálózat legnagyobb létesítményei közé tartozik és az írországi rendszerintegrátorok (SI-k), alkalmazásszolgáltatók (ASP-k) és web hoster cégek új generációja számára teremti meg a lehetőséget, hogy az e-businessben érdekelt vállalati ügyfeleinek a legmagasabb színvonalú szolgáltatásokat kínálhassák. A központok abba a láncba illeszkednek, amellyel a CRI egy egész Európát felölelő menedzseltinfrastruktúra-platformot kíván létrehozni. Ez a lánc az év végére több mint 16 magas színvonalú, biztonságos központot foglal magában, közülük nyolc máris működik. A vállalat az első olyan pán-európai vállalkozás, amelyik elnyerte a Cisco Alkalmazás Infrastruktúra Szolgáltató (AIP) minősítést. Információ: *www.city-reach.com.*

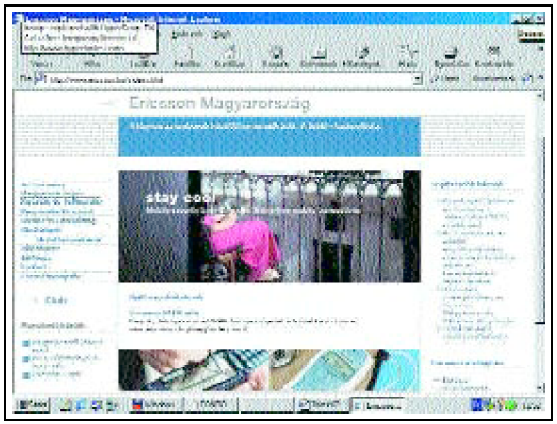


## TÁVKÖZLÉS

**Ericsson**

Címszerepben az oktatás

Kezdetben elsősorban a cég dolgozóinak továbbképzését szolgálta az Ericsson Magyarország Oktatási Központja, amely alig egy évvel a hazai képviselet megalakulása után, 1991-ben nyílt meg. Tíz évvel később, idén február 1-jén a központ csatlakozott az Ericsson Competence Solutions nevű nemzetközi szervezetéhez. A távoktatási és hagyományos módszerekkel folytatott képzés tematikája a GPRS-től a WCDMA és UMTS alapú megoldásokig terjed.




**Működő GPRS**

Az Ericsson Magyarország Kft. és a Westel Mobil Rt. február közepétől előbb Budapesten, majd az ország hetvenszázaléknyi területén elérhetővé tette a GPRS általános csomagkapcsolt rádiós átvitelt – jelentették be abból az alkalomból, hogy a két cég vezérigazgatói aláírták a különféle mobiltelefon-hálózati berendezések, know-how-k, szoftverek szállítására vonatkozó idei, közel 15 milliárd forintos keretmegállapodást. A GPRS-szolgáltatásnál a bázisállomásonként rendelkezésre álló nyolc időrésből beállítás, illetve beszédfoglaltság szerint kettőt–négyet adatátvitelre használnak. Az adatátviteli időrésekben adatcsomagok mozognak vegyesen, és a bázisállomás körzetében lévő bekapcsolt mobil készülékek maguk válogatják ki közülük a nekik szólókat. Sebessége miatt a GPRS vonzó lehet az adatátviteli szolgáltatásokat igénylő előfizetőknek, így ugrásszerű javulást hozhat a WAP megítélésében. Információ: *www.ericsson.hu.*

**BME**

IPv6

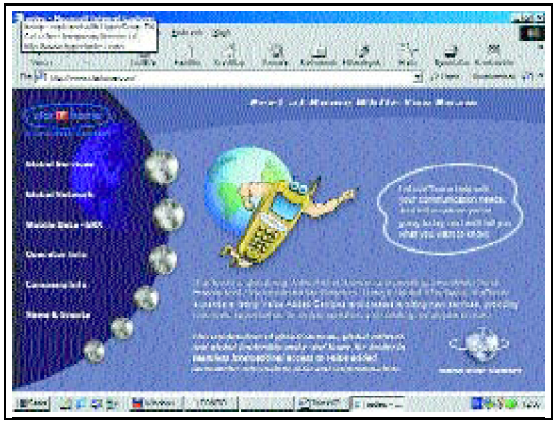
Az Internet Protocol 6-os verziójáról tartott szakmai nap a 4-es verzióval kapcsolatos gondok (szűk címtartomány, biztonsági problémák, elérési és hozzáférési hiányosságok, QoS-garanciák hiánya stb.) ismertetésével kezdődött. Ezekre az új címzési struktúra, az autokonfiguráció és újrakonfiguráció, az IPsec-adatbiztonság, az egyszerűsített fejlécstruktúra, a szolgáltatásminőség támogatása és az IPv4-kompatibilitás adja meg a választ. Az IPv4-ről nem lehet átállni egyik napról a másikra – mondták az előadók –, ezért a két verzió sokáig fennmaradhat egymás mellett. A hazai kísérletek a BME, a KFKI, a Matáv-PKI és a KFKI égisze alatt folynak. Összeköttetés jelenleg Budapest, Szekszárd, Szeged és Miskolc között van. A Nokia előadója szerint az áttérést a gazdaság fogja szabályozni, ütemét a mobilszolgáltatás igénye diktálja majd. A hozzáférési hálózatokban az IP-kommunikáció IP-alapokra helyezése a mobil IP-t támogatja, de a lokális IP-mobilitás (amikor a felhasználó mozgás közben használja a rendszert) megoldása még nehézségekbe ütközik. Bővebb információ: *http:// lists.kfki.hu/mailman/listinfo/ipv6* és *http://tipster6.ik.bme.hu*.

**Star*home**

Hazai kód külföldön

Rövid kódokat használó külföldi utazók ezentúl Romániából is ugyanúgy érhetik el hangpostafiókjukat, mint otthon. A Star*home és a Vodafone csoporthoz tartozó Connex román mobiltelefon-szolgáltatató közös Home Short Code (honi rövid kódú) szolgáltatásával a Connex hálózatot választó külföldiek romániai tartózkodásuk alatt ugyanazokat a kódokat használhatják például a hangposta, ügyfélszolgálat stb. elérésére, mint otthon. Ugyanez vonatkozik a Connex előfizetőire, ha olyan országba utaznak, ahol Star*home

hálózat működik. A Star*home szolgáltatása saját globális IP-hálózatán és IntelliGate platformján alapul. Mivel mind a GSM, mind a nem GSM hálózatokhoz kapcsolódik, segítségével a mobilhálózat-üzemeltetők globalizálhatják értéknövelő szolgáltatásaikat ügyfeleik számára. *www .starhome.com.*



**GTS**

Vezetőcsere és szerkezetátalakítás

*Duncan Lewis* személyében új elnök-vezérigazgató került a Global Telesystems, Inc. (GTS) távközlési vállalat élére. Lewis fogja felügyelni a Global Telesystems napi működését, előtérbe helyezve az Ebone (Broadband Services) fejlesztését, ami a vállalati szerkezetátalakítási program megvalósítását követően a cég legfőbb tevékenységi területe lesz. Bővebb információ: GTS Hungary. Tel.: 452-4715.

**Chello**

Magyaros hangzás

Teljes lett a Chello Broadband Hungary menedzsmentje – jelentette be *Hivatal Péter,* a szélessávú internetszolgáltató magyarországi vállalatának új ügyvezetője. A megbízott vezetői gárda kizárólag magyar szakemberekből áll, akiknek feladata a hazai piac meghódítása lesz. A United Pan-Europe Communications (UPC) érdekeltségébe tartozó cég célja, hogy 2001 végéig vezető pozíciót érjen el működési területén. Ennek érdekében az eddigieknél kedvezőbb feltételekkel kínál állandó, nagysebességű szolgáltatást, amiért fix havidíjat kell fizetni. További információ: Chello Broadband Hungary. *www.chello.hu.*

**Vodafone**

Vitamax City

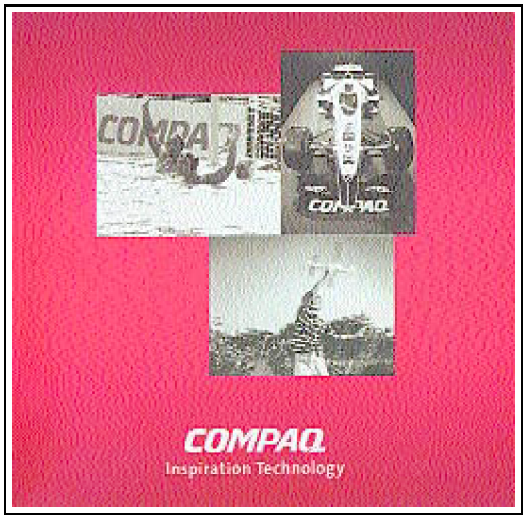
Új tarifacsomaggal bővült a Vodafone kínálata. A Vitamax City feltöltőkártyás csomaggal az ügyfelek rendkívül kedvező percdíjakkal telefonálhatnak bármely mobilhálózatba a már saját lefedettséggel rendelkező területeken. A szolgáltatást leginkább a nagyobb városok és megyeszékhelyek lakóinak ajánlják. További információ: *www.vodafone.hu.*

# INFORMATIKA

**Compaq**

Akadémiai mérleg

Az MTA épületében tartotta 2000. évi eredményéről szóló beszámolóját a Compaq Computer Magyarország Kft. *Beck György* vezérigazgató elmondta: vállalata 30 százalékos növekedés után 40 milliárd forintos összbevétellel zárta a 2000-es pénzügyi évet. Ebből több mint 70 százalékot tettek ki a nem PC jellegű bevételek (nagyvállalati technológiák, szolgáltatások, rendszer-integráció). Ugyanakkor közel negyvenezer eladott géppel a Compaq a hazai PC-piac körülbelül 20 százalékát mondhatja a magáénak. A cég tavaly jelentős beruházásokat és fejlesztéseket kezdett Magyarországon. A februárban megnyitott BDG e-Infrastruktúra Szakértői központ 95 ország internetes projektjeit koordinálja. A nyitás óta több tucat, köztük számos „egzotikus" projekt került a szakértőkhöz. A Compaq nevéhez fűződik az első hazai elektronikus piactér, a Marketline.hu és a kormányzat támogatását élvező CsaládiNet PC program is. Beck György értékelése szerint a dátumváltás utáni esztendő a vártnál mérsékeltebb fellendülést eredményezett; a gazdaság erősödése, a tavaly elhalasztott beruházások megvalósításának szükségessége, az internet rohamos terjedése azonban az informatikai piac felfutását vetíti előre. További információ: Compaq Computer Magyarország Kft. Tel: 458-5466.




*laszlo.mezriczky@compaq.com.*

**Microsoft**

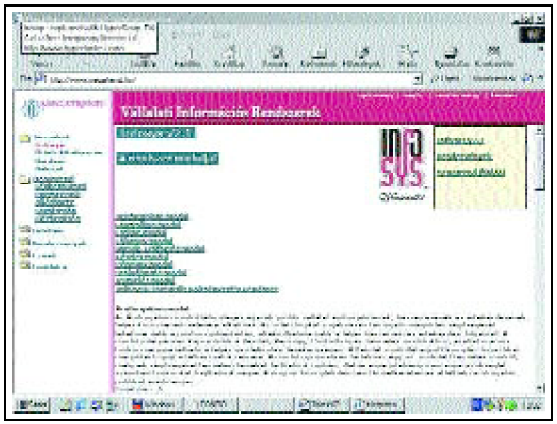
Szoftvervédelem

Technikai megoldásokkal is igyekszik korlátozni termékeinek illegális használatát a Microsoft. Az Office és a Windows újabb változatai nem másolható telepítőkészletekkel kerülnek forgalomba. A rendszer alapja, hogy az alkalmazás használatához aktiválni kell majd a szoftvert az ahhoz kapott, valamint a gép hardverkonfigurációja alapján számított kód segítségével. Az aktiváláshoz szükséges kód a Microsoft helyi képviseletétől telefonon és interneten szerezhető be. A Microsoft rövidesen teljes termékpalettáját hasonló védelemmel kívánja ellátni; egyes termékeknél ötven rendszerindítás, másoknál harmincnapos korlát lesz az aktiválás határa. Minthogy a cég tervei szerint a nagyfelhasználók vállalati szintű aktiválókulcsot kapnak, a kódolásos védelem elsősorban a Microsoft termékek azon magánfelhasználóit hozza nehéz helyzetbe, akik időről időre átalakítják, bővítik otthoni számítógépüket. Információ: *www .microsoft.hu.*


**Megatrend**

Az Infosys a szoftverbörzén

Ismételten Budapest adott otthont a hagyományos számviteliszoftver-seregszemlének február elején. Ennek keretében tartott sajtótájékoztatót az Infosys szoftverrendszert gondozó Megatrend. A cég tavaly számottevően növelte működési hatékonyságát és megőrizte 1,3 milliárd forintos árbevételét – többek között az Infosys rendszerek értékesítésével. Tizenöt új projektet sikerült megszervezni, és folyamatos maradt a rendszer-támogatási tevékenység. Mint a rendezvényen elhangzott, folytatódik a kutatás-fejlesztés, amelynek eredményeként az Infosys jelenlegi 2.1-es verziója továbbfejlesztett munkafolyamat-kezelővel (ISWF) és eseménykezelővel (ISES) bővült. Információ: *www.megatrend.hu.*




**Debis IT Services Dataware**

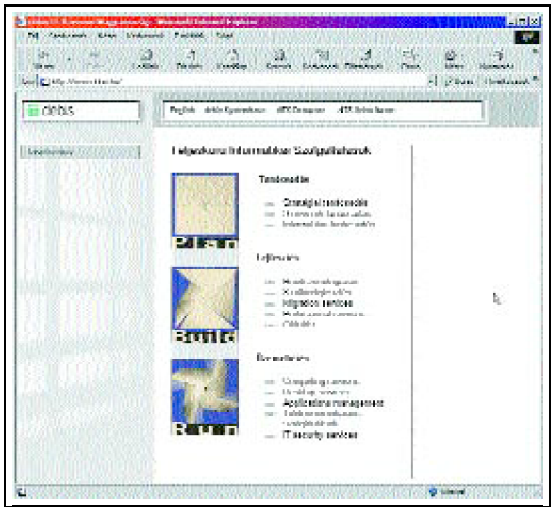
Adatvilág

Elsősorban a pénzügyi, a kormányzati és a távközlési szektor szereplőinek szánja új termékét a Debis Dataware. A fejlett adatminőség-biztosítási rendszerrel és adattisztítási funkciókkal jellemzett Adatvilág olyan komplex adatelemző rendszert ad a felhasználó kezébe, amellyel az adatokból üzletileg hasznosítható információ nyerhető ki. A csomag elemei közül az Adattárház az a közeg, amely az információkat egy CRM megoldás számára rendszerbe foglalja. A többi elem az informá-ciók használhatóvá tételére szolgál. A cég 2001-ben ötmilliárd forint árbevétel mellett 700 millió forintot meghaladó nyereséggel számol, nem kis szerepet szánva az Adatvilág csomag sikerének. További információ: Debis IT Services Dataware Kft. Tel.: 467-1100.

**Debis IT Services Unisoftware**

Kedvezmények a Postán

Befejeződött az áttérés a Magyar Posta Rt.-nél az SAP integrált vállalatirányítási rendszer 4.6 B verziójára. Az immár egyvállalatos modellel – a korábbi, többvállalatos modellel szemben – lehetővé válik az ügyfelek forgalmának országos összesítése, s ezzel nagyobb kedvezményekhez juthat a mintegy 8-10 ezer partnervállalat. A Posta a forgalom arányában nyújt kedvezményt üzletfeleinek, a korábbi SAP rendszer azonban csupán igazgatóságonként tette lehetővé az adatok összesítését. Az évek során az egykori SAP verzió, de a postai struktúra felett is eljárt az idő, így a Magyar Posta Rt. vezetése a rendszer cseréje mellett döntött. A vállalati folyamatokat feltérképező BPR (Business Process Reengineering), illetve az erre épülő, az SAP változat bevezetését célzó projektet a Debis IT Services Unisoftware Kft. nyerte el. Az átállás az értékesítési, a számviteli, a pénzügyi, a kontrolling, a logisztikai, valamint az emberi erőforrás modult érintette, elindultak az eszközgazdálkodási funkciók és az első havi zárás is hiba nélkül zajlott. Az informatikai rendszer korszerűsítésével a Magyar Posta Rt. a világ nagy postáival szemben versenyképes, az információs társadalomban is korszerű szervezetté válik. Információ: *www .debis.hu.*



**Hermes SoftLab**

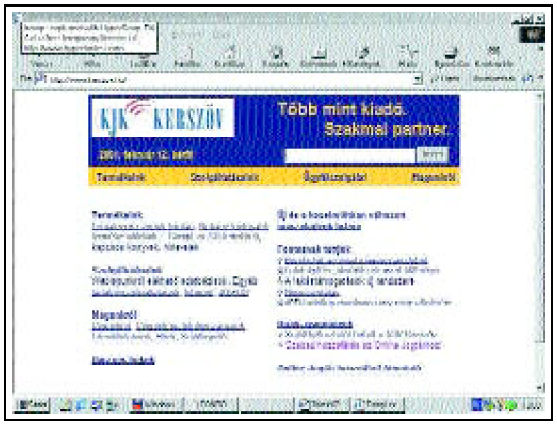
Szlovén fejlesztőcég

Budapesten is megnyitotta irodáját a Hermes SoftLab. A szlovén érdekeltségű szoftverfejlesztő cég irodákat tart fenn Stuttgartban, Bécsben, Szarajevóban, valamint a Szilícium-völgyben. A vállalat 2000-ben 32 millió euró bevétellel zárta az évet, termékeit főként az Egyesült Államokban és az EU piacain értékesítette. Információ: Magma Kommunikációs Kft. Tel.: 312-2282.

**KJK-Kerszöv**

Online jogtár

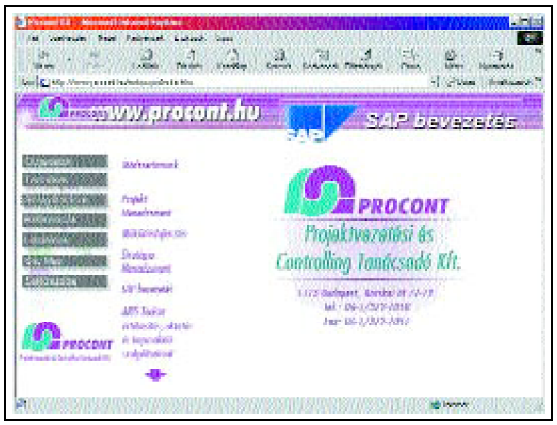
A havi megjelenésű CD-változat előfizetői január végétől bármikor letölthetik a KJK-Kerszöv központi számítógépéről az utolsó CD lezárása óta megváltozott vagy új jogszabályokat, valamint a szakközlönyökben megjelenő pályázati felhívásokat, személyi híreket – hangzott el azon a sajtótájékoztatón, amelyen két új terméket is bemutattak: az Adó CD-t és az Önkormányzat CD-t. A KJK-Kerszöv a jövőben három pillérre építi stratégiáját: jogi, adóügyi és üzleti kiadványokra, internetes és online termékekre, továbbá az eddiginél nagyobb hangsúlyt fektet szoftverekre és alkalmazásokra. Információ: *www.kerszov.hu.*




**Procont–KPMG–Synergon**

PakSAP

Alig három hónap alatt állították „éles” üzembe a Paksi Atomerőmű Rt. új vállalatirányítási rendszerének első moduljait. Ezzel a Procont Projektvezetési és Controlling Tanácsadó Kft. fővállalkozásában, a Procont, a KPMG Hungária Kft. és a Synergon Informatikai Rt. munkatársaiból álló szakértői csapat egy átfogó átalakítási folyamat első mérföldkövéhez érkezett. Január első napjaitól működnek az új SAP rendszer pénzügyi (FI), kontrolling (CO), eszköz- (FI-AA) és anyaggazdálkodás-, valamint beszerzés- (MM) moduljainak alapfunkciói. A kilencven nap arra is elegendő volt, hogy funk-cionális, üzemi, integrációs és go-nogo teszteket végezzenek el, hogy biztosak legyenek a hibamentes eredményben. Az SAP bevezetése a Paksi Atomerőműben elsősorban a szervezeti, gazdálkodási és műszaki területeket érinti. A cél az, hogy a változások után a jobban átlátható, hatékonyan működő erőmű könnyebben megfeleljen a vele szemben támasztott követelményeknek, beilleszkedjen az MVM informatikai rendszerébe. Az SAP karbantartási (PM) modul bevezetésével közvetve tovább javítható a műszaki berendezések megbízhatósága is. Információ: *www.procont.hu.*



**Scala**

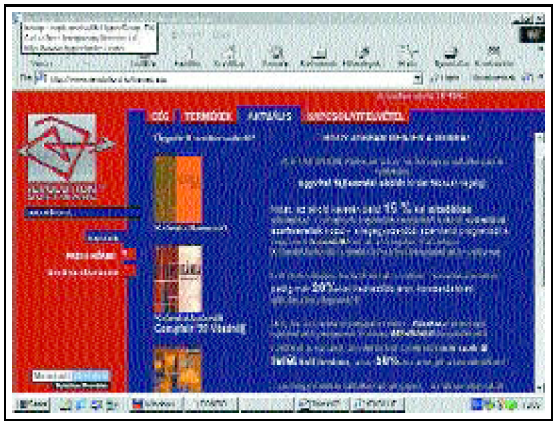
Újraskálázzák

Március 5-én várhatóan 17 millió dollár negyedéves bevételről, éves szinten pedig 71 millió dollár forgalomról számolhat be a Scala. Az átszervezési és költségcsökkentési program indítása óta a cég évente világszerte mintegy 30 százalékkal csökkentette dolgozóinak létszámát, működési költségeit pedig körülbelül 12-15 millió dollárral mérsékelte. Ezenközben négymillió dollár értékben kötött szerződéseket például az Ericssonnal, az ITT Flygttel, az Alarmcommal és az Atlas Copcóval. Ezek jelentős része tartalmazza az iScala internetes szolgáltatásait és az elektronikus vállalatirányítási megoldásokhoz szükséges programokat. Információ: Scala ECE Hungary Kft. Tel.: 452-7567. *www.scalaworld.com, www.scala.hu.*

**Revolution Software**

Ügyviteli hirdetések

Szinte napról napra bővül az internetes oldalak hirdetőinek köre – legutóbb a Revolution Software indított kampányt az ügyviteli szoftverek használati kultúrájának terjesztéséért. A cég 15–50 százalék engedményt ad induló, a számítástechnikától még idegenkedő vállalkozásoknak, hogy kipróbálhassák a gépi számlázás, a számítógépes ügyvitel előnyeit. További információ: NetAktív. Tel.: 320-6986. E-mail: *medit@netaktiv.hu.*



**2001. MÁRCIUS / HÍREK / HTE-hír**

## HTE-hír

**Vezetőválasztás és szakosztálygyűlés**

Ez év januárjában tartotta vezetőválasztással egybekötött rendezvényét a Hírközlési és Informatikai Tudományos Egyesület (HTE) Számítástechnikai Szakosztálya, a European

Organization for Quality Magyar Nemzeti Bizottság (EOQ MNB) Informatikai Szakbizottsága és az Information Systems Audit and Control Association (ISACA) Magyar Fejezete. A három szervezet együttműködéseként kialakult egyesület vezetőjének *Szenes Katalin* informatikai és biztonságtechnikai auditort kérték fel. Szenes Katalin (Certified Information Systems Auditor, CISA) korábban is részt vett a HTE, illetve más szervezetek tevékenységében, közreműködött a digitális aláírásról szóló törvényt előkészítő KHVM bizottság munkájában, több felsőoktatási intézmény tantárgyainak felépítésében.

Az egyesületet alkotó szervezetek mellett több multinacionális cég szerepel a résztvevők között, így a szakosztálygyűlések alkalmas fórumok az informatikai szakemberek véleménycseréjére is.

A januári találkozón *dr. Kornai Gábor,* az AAM Vezetői Informatikai Tanácsadó Kft. ügyvezetője a Gartner Group magyarországi képviseletének vezetője a magyar vállalatok és az elektronikus üzlet kapcsolatának kérdéskörét feszegette. Az összejövetel másik előadója, *Szekfű Balázs,* a Carnation Internet Consulting Rt. elnöke speciális témával, a virtuális közösségek kialakulásával és a bennük rejlő üzleti lehetőségek kiaknázásával foglalkozott.

Információ: dr. Szenes Katalin, *szenes@novserv.obuda.kando.hu.*

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



## NJSZT-hírek

**„e" nélkül nem megy…**

A Neumann János Számítógéptudományi Társaság, az NJSZT IEEE CS Budapest Center és az IEEE Hungary Section közös rendezvénye. Helyszíne: INFO 2001, Budapesti Vásárközpont. Időpontja: 2001. május 8. Program: Megnyitó: *dr. Arató Péter* egyetemi tanár, az NJSZT alelnöke és *dr. Péceli Gábor* egyetemi tanár, az IEEE Hungary Section alelnöke. *Az e-business alkalmazásához szükséges információtechnológiai követelmények.* Előadó: *dr. Pataricza András* (BME MIRT, IK). *A „mobil elektronikus pénztárcák" biztonsága.* Előadó: *Hornák Zoltán* (BME MIRT). *A digitális aláírás hazai bevezetésének megoldandó feladatai.* Résztvevők: *dr. Loványi István* (BME IIT), *dr. Nagy Ákos* (BME IIT), *dr. Nemetz Tibor* (MTA Matematikai Kutató Intézet), *ifj. Stark Gáspár* (KFKI-Classys), *Vadász Pál* (Montana Rt.). Moderátor: *dr. Bakonyi Péter,* az NJSZT elnöke. A 2000– 2001. évi Országos Informatikai Tanulmányi Versenyek ünnepélyes eredményhirdetése. Információ, jelentkezés: hpg@njszt.hu.

**ECDL-hírek**

Új vizsgapéldatár

Már megvásárolható a Kossuth Kiadó gondozásában megjelent új vizsgapéldatár: március 1-jétől már csak ebből kerülnek ki a vizsgakérdések.

**Hatodikok vagyunk**

2001 januárjában az ECDL-vizsgázók száma Európa-szerte meghaladta az egymilliót, és a tagországok éves előrejelzése szerint ez a szám hamarosan a többszörösére emelkedik. Az ECDL-esek számát az országok lélekszámához viszonyítva Magyarország a 6. helyen áll Svédország, Dánia, Írország, Norvégia és Ausztria után. Svédországban

a lakosság 3,13 százaléka, Dániában 2,23 százaléka vizsgázott, hazánkban ugyanez az arány pillanatnyilag 0,18 százalék.

**Intézményi szinten**

Az ECDL államigazgatásban betöltött szerepének további erősödését jelenti, hogy a Miniszterelnöki Hivatal önálló vizsgaközpontot hozott létre dolgozói képzésére és vizsgáztatására, és egyre több minisztérium, illetve más állami intézmény kapcsolódik be a „mozgalomba". Ezzel egy időben egyre növekszik a bizonyítvány nemzetközi állami és magánszektorbeli elfogadottsága is. 2001. január 26-i ülésén az Akkreditációs Bizottság újabb hat intézményt jogosított fel ECDL-vizsgák tartására. Jelenleg összesen 157 intézményben lehet vizsgázni, ezek közül hét határainkon túl működik.

*A rovatot gondozza: Szedlmayer Bea. További információ: NJSZT Titkársága (1054 Báthori u. 16.). Tel.: 332-9390, fax: 331-8140. E-mail: titkarsag@njszt.hu.*



## Távközlési hírcsokor

– Megkezdte a NICAM sztereoadások kísérleti sugárzását erre alkalmas vidéki adóin az **Antenna Hungária** Rt. Az adást NICAM-dekóderes készülékekkel lehet fogni. A teszt január 22-én ért véget.

– A négy helyi koncessziós távközlési társaságban érdekelt **Hungarian Telephone and Cable Corporation** (HTCC) felvásárolta a magyarországi leányvállalataiban lévő kisebbségi részesedéseket. A HTCC valamennyi értékpapírt készpénzért vette meg. A cég eddigi magyarországi befektetései meghaladják a 250 millió dollárt.

– A **Nokia** és a Pannon GSM Távközlési Rt. ismét meghosszabbította a GSM berendezésekkel kapcsolatos hosszú távú keretmegállapodását, s több mint 50 millió dolláros szerződést kötött újabb eszközök szállítására. A két cég közleménye szerint így a Nokia továbbra is a Pannon GSM hálózatának legjelentősebb beszállítója marad. A Pannon GSM előfizetőinek száma a múlt év végén elérte az 1,217 milliót.

– *Straub Elek,* a **Matáv** elnök-vezérigazgatója Skopjéban aláírta a macedón kormánnyal a MakTel nemzeti távközlési társaság részvényeinek 51 százalékának megvételéről szóló megállapodást. A Matáv által vezetett konzorcium összesen 343,3 millió eurót fizetett ki a macedón kormánynak.

– A **Westel Mobil Távközlési Rt.** WAP-os útvonalajánló szolgáltatást indított.

– A **Fotexnet Kft.** és a Westel Mobil Távközlési Rt. januári közös sajtótájékoztatóján bejelentették, hogy a múlt év decemberében indult Ingyenlotto.hu játékot SMS-Ingyenlottó néven kiterjesztik a Westel Mobil Távközlési Rt. előfizetői körére.

– Sajtótájékoztató keretében mutatták be a **Vivendi Telecom Hungary** távközlési szolgáltató újonnan kialakított budaörsi szolgáltatásfelügyeleti központját (SMC), videokapcsolat útján pedig a veszprémi híváskezelő (call center) alapú tudakozóját. A központ mintegy 500 millió forintos beruházással készült el. A veszprémi tudakozó szolgálat, amelynek megteremtése 200 millió forintot emésztett fel, a Vivendi valamennyi primer körzetét kiszolgálja.

– Január 18-tól folyamatosan vezeti be új stratégiáját, új megjelenését, reklámkampányát a **Matáv,** amely a vezetékes telefont használóknak készült új díjcsomagstruktúráját is meghirdette. A stratégiaváltás lényege: az erőforrások jelentős részét a fő célokra koncentrálva ezután négy fő területre (internet, mobiltelefónia, adatátvitel, „földrajzi" bővülés) fokuszál a társaság. Az új Matáv új logóval és szlogennel, új akusztikus logóval, három új reklámfilmmel, valamint megújult honlappal jelentkezett. A Matáv öt bevezetendő

vezetékes tarifacsomagját is ismertette.

– A **Vivendi Telecom Hungary** február 1-jétől átlagosan 2,4 százalékkal emelte távközlési tarifáit, ezen belül a lakossági tarifák 5,9 százalékkal, a kormány által várt infláció mértéke alatt nőttek.

– Infokommunikáció a harmadik évezred hajnalán címmel január 18-án rendezte nyolcadik konferenciáját a **Távközlési Érdekegyeztető Fórum** (TÉF). A konferencia első meghívott előadója *Dessewffy Anna,* az Informatikai Kormánybiztosság szabályozási főcsoportfőnöke, az EHT-vel kapcsolatos jelenlegi munkák személyes irányítója volt, aki az EHT szerepéről és a szakmai fejlődésre gyakorolt hatásáról szólt. Szerinte nem a készülő új hírközlési törvény hajtja végre a liberalizációt a hazai hírközlés terén, hanem jelentősége abban áll, hogy „kezelni fogja azt a helyzetet, ami a liberalizáció egyébként is megtörténő bekövetkezése esetén fenn fog állni".

– Elkészült és a **Hírközlési Főfelügyelet** (HÍF) honlapján elérhető a Hírközlési piac az ezredfordulón című, a magyarországi helyzetet bemutató tanulmány. Az anyag sok grafikonnal, ábrával szemléletes módon ad áttekintést a hazai hírközlés szereplőiről, eredményeiről.

– Idén a távközlési tarifák átlagosan legfeljebb 6 százalékkal növekedhetnek – közölte *Sík Zoltán* informatikai kormánybiztos egy január végén tartott sajtótájékoztatón. A Matáv szolgáltatási területén éves átlagban a lakossági havi előfizetési díjak átlagosan 19,9 százalékkal nőnek majd, ám azoknak, akik a kisfogyasztói csomagot választják, csak 6 százalékkal kell nagyobb havi előfizetési díjat fizetniük, mint tavaly. A szolgáltatók 15-20 százalékos díjkedvezményt adnak az internetezőknek, és a legtöbb szolgáltatási területen a kapcsolási díj is megszűnik internetes bejelentkezéskor – jelentette ki a kormánybiztos. Nyártól ugyanakkor valószínűleg megszűnik az eddigi 150 forintos kedvezmény, vagyis nem lesz „plafonja" a kedvezményes időszakban az internetezésért felszámított díjnak.

– Digitális mobil gyorsjelentés 2000. december címmel újabb adatokat tett közzé a hazai mobiltelefon-használatról és a -szolgáltatókról a **Hírközlési Főfelügyelet** Piaci Monitoring Igazgatósága. Ezek szerint a múlt év utolsó hónapjában kiugróan, 11,1 százalékkal nőtt az előző hónaphoz képest a digitális mobiltelefon-előfizetők száma az országban. Ebben a hónapban került a Vodafone először 6 százalék fölé az aktív előfizetők száma szerinti piaci részesedést illetően (Westel Mobil 53,30, Pannon GSM 40,56, Vodafone 6,14 százalék). A száz lakosra jutó GSM-előfizetők száma 2000 decemberében elérte a harmincat.

– A tavaly decemberben az Egyesült Államok hírközlési piacát felügyelő szabályozási hatósággal, az FCC-vel aláírt megállapodás alapján 2001. január második felében a **HÍF** vezetői az amerikai hatóság illetékeseivel és tanácsadóival folytattak munkamegbeszélést az USA-ban. A két hatóság idei tervei között a HÍF–FCC együttműködés regionális bővítése és közös rendezvények megtartása is szerepel.

– A BRFK XIV. ker. Kapitányságon a múlt évben lefolytatott **Tetrapol** professzionális mobilrádió-hálózat bemutató (pilot) rendszerének kísérleti működtetése Tetrapol Pilot 2001 néven idén tovább folytatódik – jelentették be az érdekeltek a Tetrapol nemzetközi helyzetét értékelő budapesti sajtótájékoztatón.

– Három új WAP-szolgáltatást indított a **Pannon GSM:** az e-mail küldését lehetővé tévő Pannon W@P E-mailt, az utazóknak az eligazodásban segítő Pannon W@P Navigátort és a bioritmusunkat elkészítő funkciót.

– Tíz toronyból álló rendszert építene ki a **Hírközlési Főfelügyelet** a frekvenciák engedély nélküli vagy szabálytalan használatának kiszűrésére.

– A **Nokia Hungary Kft.** februári sajtótájékoztatóján bemutatkozott *Heikki Vappula,* a cég új ügyvezető igazgatója. A kft. a múlt évben mintegy 63 milliárd forint nettó árbevételt ért el.

– A 25-ös primer körzet utolsó analóg távbeszélőközpontját váltotta ki korszerű digitális központtal Sárbogárdon a Vivendi Telecom Hungary csoporthoz tartozó **V.fon** cég. A körzetben a 45 ezer ügyfél mostantól – a régi analóg központ egyidejű kiiktatásával – a legkorszerűbb technikára épülő szolgáltatásokat veheti igénybe.

– Odaítélték a Nonprofit Információs és Oktató Központ, valamint a Soros Alapítvány által az adakozó magánszemélyek és vállalatok elismerésére alapított Civil Díjakat. A vállalati kategória kitüntetettje és ezzel Az Év Vállalati Adományozója a 2000. évben kifejtett támogatási tevékenysége révén a **Siemens Rt.** lett.

– *Stumpf István* kancelláriaminiszter februárban készült aláírni az adatátviteli célokat szolgáló, 3,5 gigaherzes frekvencia árverését engedélyező dokumentumot.

– Februártól Zuglóban és Újpesten is elindítani tervezi szélessávú internetszolgáltatását a **UPC.**

– Bejelentették, hogy a Németkábel Vagyonkezelő Rt. tulajdonában lévő, győri székhelyű **Kábeltelevízió Szolgáltató Kft.** magába olvasztja a mosonmagyaróvári Kábeltévé Kft.-t.

**Kovács Attila**

**2001. MÁRCIUS / HÍREK / Könyvszemle**

## Könyvszemle

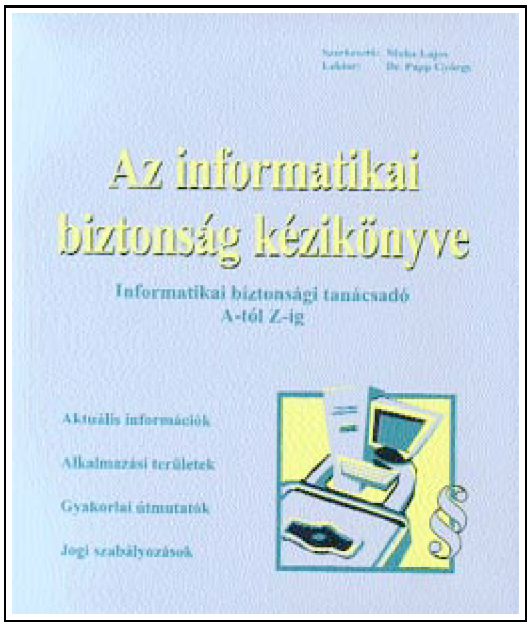

**Új és megújuló információs rendszerek**

**Kiadó: BME Információmenedzsment Tanszék**

**Ára: 2000 Ft**

Az Alma Mater sorozat első kötete napjaink rohamosan fejlődő informatikai iparágának fő fejlődési irányzatait ismerteti. Külön fejezet foglalkozik többek között az elektronikus

kereskedelemmel, a digitális pénz jelenével és jövőjével, a kiskereskedelmi adatok elemzésével, a népszámlálás informatikai hátterével, a high-tech és internetes inkubátorházakkal, az adatkezelési bizalom megteremtésének kérdéseivel és a kutatási célú személyi információs rendszerek fejlesztésével. Az egyetemi jegyzet formátumban tördelt kiadvány elsősorban a szakembereknek kínál hasznos információkat, a minden egyes fejezet végén megtalálható irodalomjegyzék pedig elősegíti a témákban való mélyebb elmélyülést.




**Az informatikai biztonság kézikönyve**

**Informatikai biztonsági tanácsadó A-tól Z-ig**

**Kiadó: Verlag Dashöfer Szakkiadó Kft. & T. Bt.**

**Ára: 14 490 Ft (áfa nélkül)**

Amióta egyáltalán létezik informatika, a számítógépek által kezelt adatok megóvása mindig is fontos feladat volt. Különös jelentőséget kap azonban a kérdés manapság, amikor egyre nagyobb tömegű kritikus adat gyűlik össze az interneten a külvilággal kapcsolatba kerülő cégeknél, állami intézményeknél, amelyek elvesztése, illetéktelen kezekbe kerülése jóvátehetetlen károkat okozhat. Az évente 3-4 alkalommal frissített, iratrendezős kiadvány részletesen szól az informatikai biztonság fogalmairól és követelményeiről, az informatikai biztonsági politikáról, a védelem megvalósításáról, valamint napjaink biztonsági problémáiról. A kötetet részletes irodalomjegyzék zárja.


**Kék oldalak**

**Országos mobiltelefonkönyv és szakmai névsor, a hazai e-mailek és internetes honlapok jegyzéke**

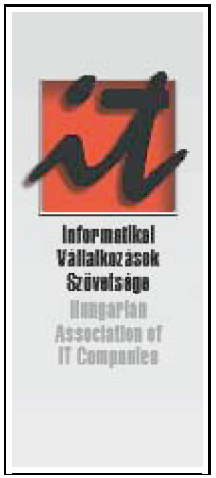
**Kiadó: Greger-Delacroix Kiadói Kft.**

**Ára: 3600 Ft**

Kétségtelenül hiánypótló mű, azonban kézbevételekor az emberben jogosan felmerül a kérdés, vajon nem lenne-e célszerűbb inkább a folyamatosan frissíthető interneten közzétenni. A közel 750 oldalas kiadvány első 379 oldala tartalmazza a mobilszámokat, ezután több mint 110 oldalnyi hirdetés következik, végül 350 oldalon szemezgethetünk a webcímek között. Az e-mail címek jegyzékének nyoma sincs; lehet, hogy a hirdetések némelyikén feltűnő e-mail címekre gondoltak a szerkesztők. A kötet postahivatalokban, benzinkutaknál és a kiadóban vásárolható meg.

**2001. MÁRCIUS / HÍREK / IVSZ-hírek**

## IVSZ-hírek




**Az Év Informatikai Menedzsere 2000 díj**

Az Informatikai Vállalkozások Szövetsége 2001. február 1-jén ünnepélyes keretek között kiosztotta a 2000. év legjobb informatikai vezetőinek Az Év Informatikai Menedzsere 2000 díjat. Idén három kategóriában díjazták az arra pályázó informatikusokat. Az Év informatikai menedzsere kategóriában *Keresztesi János,* a Sun Microsystems Magyarország Kft. ügyvezető igazgatója kapta meg a vándordíjat (a vezetői kvalitásokat szimbolizáló karmesterpálcát), valamint az oklevelet, míg *Nemes Dániel,* a Telnet Magyarország Rt. ügyvezető igazgatója és *Kenyeres Judit,* az ICL Hungary Kft. projektvezetője az Év fiatal informatikai menedzsere, illetve az Év informatikai projektvezetője – 2000 kategóriában nyerte el az elismerést. A harmincöt beérkezett pályázat alapján a díjakat a BYTE Magyarország, a CW Számítástechnika, az Infopen Magazin, a Telecomputer, az Új Alaplap és a VGA Monitor, valamint a Világgazdaság című lap szerkesztőinek szavazatai alapján ítélték oda a kitüntetetteknek.

**Dokumentumkezelési szakcsoport alakult**

Napjainkban a reprográfia, az információtechnológia és a konzultációs tevékenység közötti határok mindinkább kezdenek összemosódni. Ezt felismerve az IVSZ szakcsoportot alakított, amely célul tűzte ki a dokumentumkezelési eljárások széles körű megismertetését; olyan közös termék létrehozását, amit önmagában egy cég sem tudna megvalósítani; a jogi-törvényhozási környezettel való kapcsolattartást; és annak elfogadtatását a piaccal, hogy a dokumentumkezelési eljárások pénzbe kerülnek. Az ülésen 2001-re a szakcsoport vezetőjévé *Lakatos Istvánt* választották.

**2001. MÁRCIUS / KÖRNYEZET Távközlési infrastruktúra**

## KÖRNYEZET
## Távközlési infrastruktúra

# Lehetne együtt?

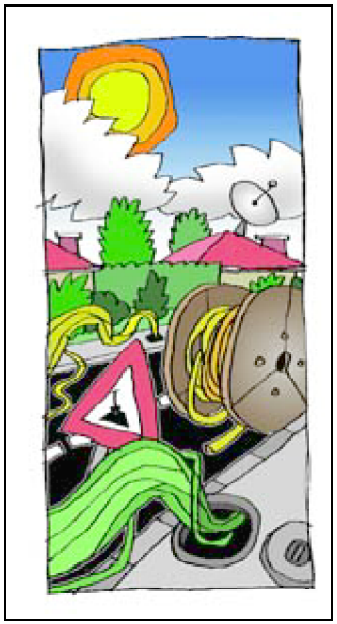
**A MEISZ legutóbbi konferenciáján folytatódott a vita arról, valójában kinek kell a hálózat.**

**Szerző: Varga Miklós**

A lapunk tavaly októberi számában megjelent írás nyomán (*Kinek kell a hálózat?,* BYTE Magyarország, 2000. október, 30. oldal) alapvetően azt próbálta tisztázni a Magyar Elektronikai és Infokommunikációs Szövetség (MEISZ), hogy az információs társadalom nélkülözhetetlen eszközeként vagy az önkormányzatoknak jellemzően károkat okozó, s ezért kártalanításra okot adó létesítményeknek tekinthetők-e a távközlési alépítmények. A szövetség ezért meghívta a Miniszterelnöki Hivatal Informatikai Kormánybiztossága, a Gazdasági Minisztérium, a Hírközlési Főfelügyelet, a Fővárosi Önkormányzat, a kerületi önkormányzatok, az érintett tudományok s természetesen a távközlési vállalatok képviselőit. A fő téma a hírhedt kábeladó volt. Többen fölvetették: hogyan lehet ellentét a közcélúság és a közterület fogalmai között? És ha nincs, miért köti az önkormányzat súlyos összegek befizetéséhez a hálózat tulajdonjogának bejegyzését? Szó volt még a távközlési beruházások jogi hátteréről és gyakorlatáról, a lakosság- és környezetbarát, olcsó, jó megoldások lehetőségeiről is.

**Félkerek kerekasztal**

A meghívottak széles köréből sajnos csak „félkör” lett, mert távol maradtak a főváros vezetői és a kerületek első emberei, valamint a hálózatépítés engedélyezéséhez hozzászólni tudó, a párbeszédben részt venni akaró önkormányzati szakemberek. Senki sem érvelt a főváros közgyűlésének 48/2000. közgyűlési határozata mellett. Nem akadt, aki megmagyarázza, hogy az önkormányzati források pótlásán kívül mi indokolja a hálózatok építési költsé-geit kétszeresen, sőt olykor ötszörösen meghaladó kártalanítás igényét. Nem volt, aki türelmet kér, amiért hetekig, hónapokig, olykor esetleg másfél évig késik a tulajdonosi hozzájárulás. Hiányzott a körből, aki az önkormányzatok szempontjából is ésszerű javaslatot ad a kölcsönösen tervezhető, konstruktív együttműködés módszereire.



A domináns távközlési szolgáltató háttérbe szorított versenytársai egyébként a MEISZ fórumát megelőzően tiltakoztak a Fővárosi Közigazgatási Hivatalnál és az Alkotmánybíróságnál a Fővárosi Közgyűlés jogsértő határozata ellen. Az Alkotmánybíróság január végéig nem nyilatkozott. A közigazgatási hivatal a hónap közepén jogsértőnek ítélte a közgyűlés döntését, a fő-város vagyonkezelői ügyosztálya pedig – igaz, korábbi keltezéssel – a hónap második felében is sürgette a kártalanítással kapcsolatos űrlapok kitöltését az egyik új szolgáltatónál.

**Kábeladó**

Ma még nem tudni, sikerül-e elérni, hogy Budapesten ne terhelje övezetenként 4800, 6400, illetve 9600 forint kábeladó a közcélú vezetékek egy-egy folyóméterét, 4000-5000, illetve 6000 forintos kiadás az aknákat és egyéb létesítményeket s mindennek két-háromszorosa a nem közcélú távközlési szolgáltatásra szánt vezetékeket és létesítményeket.

Kérdés, mikorra normalizálódik a közgyűlés határozata előtt lelassult engedélyezési folyamat, nem fékez-e útfenntartóként, aki tulajdonosként már megadta az engedélyt, mennyi pecsétet kell, illetve kellett szereznie, akinek időközben lejártak az egyéb engedélyei, tartható-e az ütemterv az évszakonként változó időjárás és forgalom közepette, mennyire szólnak közbe a környéken zajló egyéb beruházások, lesz-e éppen szabad műszaki ellenőri kapacitás, s még sorolhatnánk tovább.

Az is kérdés, nem kapnak-e kedvet más települések önkormányzatai, hogy kártalanításnak nevezett sarccal pótolják egyéb bevételeik hiányát. A törvényeknek ezért egyértelműen el kellene fogadtatniuk az önkormányzatokkal, hogy a XXI. század infrastruktúrájába ugyanúgy beletartozik a távközlési kábel, mint a víz, a gáz és a villany. Továbbá garantálniuk kellene az adófizető lakosoknak és vállalkozóknak, hogy az önkormányzat nem drágíthatja, nem lassíthatja az elektronikus üzletvitelre, a távmunkára, a távoktatásra vonatkozó terveik megvalósítását.

Természetesen a másik félnek is be kell tartania a játékszabályokat. Nem lett volna rossz, ha az önkormányzatok képviselői elmondják, milyen tipikus hibákkal találkoztak s milyen magatartást várnak a távközlési cégektől. Így is kiderült például, hogy a telefonközpontok korszerűsítése óta 4,5 tonnányi kihasználatlan réz „dögkábel” foglalja a helyet

a járdák alatt, illegális kábelek kerültek a földbe az Infoparkban, s a járdák közepe alá, a házfalak mentén és a zöldsávnál egyaránt fektettek kábeleket Zuglóban. Nyilván bőven akad példa a járdák koordinálatlan, ismételt felbontására is.

**Közös árok**

Persze az önkormányzatok, valamint az informatikai és távközlési hálózatépítő cégek együttműködésének jó példái mellett sem mehetünk el. A Fővárosi Önkormányzat felhívására nyolc szolgáltató használta ki közműépítésre az Alkotás utca rekonstrukcióját, s így jó ideig nem kell felbontani a mintegy 2500 méternyi járdát. A II. kerületi Önkormányzat kezdeményezésére öt cég 1600 méter hosszan közösen építette hálózatát a Hűvösvölgyi úton. A VI. kerületi Önkormányzat is elérte négy cégnél, hogy együtt fektessék kábeleiket a Podmaniczky út 1100 méteres szakaszán. Három-három szolgáltató közös megállapodással működött együtt a Közraktár utca (1200 méter), illetve a VIII. kerületi Ciprus utca, Asztalos utca és Salgótarjáni utca (2500 méter) kábelfektetéseiben.

A Seltel Távközlési Kft. tanulmánya szerint számos pozitív hatása lehet az önkormányzatok és a beruházók együttműködésének. A beruházók megoszthatják egymás közt az árokásás és a helyreállítás költségeit, emellett az önkormányzattal együtt gondoskodhatnak a talajszerkezet javításáról, új dísznövényzet telepítéséről, a burkolt felületek részleges, illetve teljes felújításáról, a járdaszegélyek letöréséről – hogy könnyebben közlekedjenek a babakocsikat toló kismamák és a rokkantak –, a jelzőlámpák esetleges áthelyezéséről és újak építéséről, a nem funkcionáló műtárgyak, alépítmények, dögkábelek eltávolításáról, új parkolóórák elhelyezéséről. Ezzel együtt a por, a piszok, a zaj is kisebb lenne.

**Alépítményminták**

Svédországban a városi hatóságok új utak építésekor állítólag eleve elhelyezik a közművezetékek befogadására szánt alépítményeket, s ezeket – nyilván mindkét félnek méltányos összegért – igénybe vehetik az egymással versengő szolgáltatók. A hirdetésekben természetesen ez a telek, a ház, a lakás értékét növelő elemként, s nem értékcsökkentő tényezőként jelenik meg.

Nálunk is vannak elképzelések a távközlési és informatikai közművek hálózatainak rekonstrukciójára, gyűrű alakban elhelyezkedő gerinchálózatokra s a háztömbök nagyobb csoportjait körülfutó, rövid csatlakozásokat igénylő racionális hálózati szakaszokra. Van új kábelfektetési technológia és nagy teljesítményű gép, ami olyan gyorsan vágja a keskeny nútot az optikai kábeleknek, hogy a gyalogosok előtt ér át a zöld jelzésen. Egy év múlva pedig – állítólag – lesz olyan hússzor húsz centiméter keresztmetszetű alépítmény is, amelyben száz (!) mikrokábel kaphat helyet.

Rengeteg minden van, lesz, lehet, illetve lehetne. Csupán az igazi nagy verseny hiányzik a távközlési és informatikai infrastruktúrák tulajdonosai között. A meglévő hálózat birtokosai módjával keresik a fogyasztók kegyeit, míg versenytársaiknak bármelyik magyar városban a reális költségek többszörösét kell kifizetniük a hálózatépítéssel okozott „kárért”, s hónapokig várnak az építési engedélyekre. A fogyasztók pedig az infokommunikáció költségeiben fizetik meg a kábeladót.

Varga Miklós a BYTE Magyarország munkatársa.

E-mail: **vargam@mail.matav.hu.**

2001. MÁRCIUS / TECHNOLógia Cisco OPT / Csomagkapcsolt telefon

# Csomagkapcsolt telefon

**A távközlés fejlődési lendülete töretlen. Az iparág szereplői közül a Cisco is aktivizálta magát ígéretes technológiai megoldásával.**

Szerző: Vargha Márton

A forrásban lévő távközlés számtalan alternatívát kínál a telefonközpontoktól kezdve az átviteli megoldásokon keresztül egészen az előfizetői készülékekig (az átalakulást kiszolgá a Siemens SURPASS rendszereit mutattuk be). Ebben a cikkben a Cisco szemszögéből írjuk le, milyen lesz a vezetékes telefónia az új évezred első néhány évtizedében.

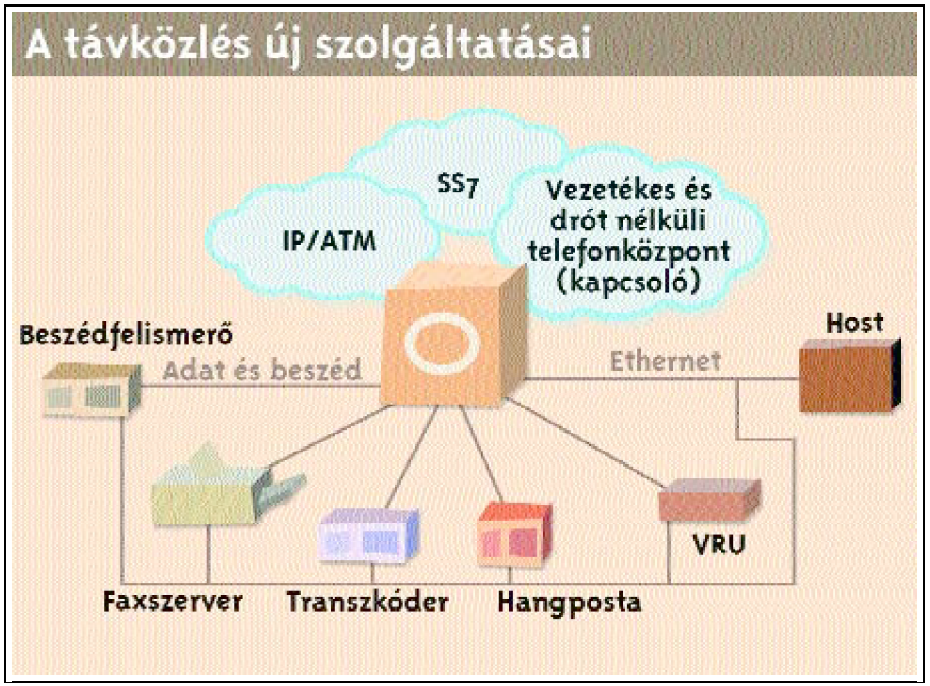
**Verseny az előfizetőkért**

Az Amerikából indult, és lassan az egész világon bekövetkező távközlési liberalizálás révén kialakuló versenyben – különösen a cégek tőzsdei megítélésében tavaly ősszel bel legjövedelmezőbb legyen a beszéd- és adatátvitel? Miként tudnák integrálni a szolgáltatásokat, megtartani az előfizetőket és újakat szerezni?

A Cisco válasza ezekre a kérdésekre és a csomagkapcsolt beszédátvitel kihívására az Open Packet Telephony (OPT), aminek már a nevében jelzik, hogy koncepciójuk alap sokszínűséghez vezet. A telefontársaságok és vállalkozások új, sosemvolt szolgáltatásokkal különböztethetik meg magukat egymástól, miközben technikai szempontból súrlódásmente

**Digitális telefónia**

Egyre több házban jelennek meg a vezetékes szolgáltató átalakító dobozai: az épületig üvegszálon megy a beszélgetés és a hang, ott bontják szét a jelet a hagyományos analóg digitális beszédátvitel most, az internettel együtt jelenik meg. Ugyanis a központok közötti távolsági kapcsolatok digitálisak, ott már régóta használják a kapacitáskihasználás r rendben összekeverve továbbítják a beszélgetések részleteit. Olyan ez, mint a körkapcsolásos mérkőzések közvetítése a rádióban, azzal a különbséggel, hogy olyan gyorsan fut k időosztással tartanak kapcsolatot a GSM hálózatban a bázisállomások és a telefonok is; ott egy másodpercben nyolc időszelet van, tehát egy cellán belül egy időben nyolc beszé Kbps sebességű csatorna fér el. Ekkora adatsebességre van ugyanis szükség ahhoz, hogy a beszélgetések minősége ugyanolyan jó legyen, mint az analóg vonalon. Az ISDN-nél két 6




**Vonal- és csomagkapcsolt hívások**

A digitális telefóniában a hívó és a hívott közötti kapcsolat létrejöttekor egy 64 Kbps sebességű digitális csatorna, vonal nyílik meg, ezért hívják ezt vonalkapcsolt szolgáltatásna szolgáltatás. Tehát a két fél kap egy időszeletet, és addig az övék, amíg le nem teszik a kagylót. Értékes tizedmásodpercek mennek el a hallgatások, csöndes szuszogások közvetíté akkor is a miénk, és fizethetjük érte a percdíjat.

Csomagkapcsolt átvitelnél nem egyenletesen, időosztással keverik össze és választják szét a hálózatban a telefonbeszélgetéseket, hanem úgy, hogy minden adatcsomagba beler közvetíti a rendszer.

Ennélfogva a csomagkapcsolt hálózatban – amikor egy nagyobb kapacitású adatátviteli vonalra ráteszik a kisebb (telefonhálózatban a 64 Kbps sebességű előfizetői) vonalak fo adatcsomag sincs, a helyet elfoglalhatják mások. Így már általában nem 32, hanem annál jóval több csatorna fér el ugyanazon a sávszélességen, és azok sávszélessége is változó lehet

Ám egy beszélgetés lebonyolításához, egy előfizetői szolgáltatás végrehajtásához nem elég az információtartalom – adat vagy beszéd – továbbítása, „díszkíséretre" is szükség va nemzetközi telefóniában a Signaling System 7 (SS7) jelzésrendszer, melynek feldolgozását, továbbítását, kezelését beágyazták a telefonközpontokba. Ha egy telefontársaság ú választani a jelzést a beszédről, majd fel kell dolgozni és intézkedni a teljesítéséről.

**A Cisco OPT működése**

Ebben a feladatban elsősorban két szabványra épít a Cisco OPT: a H.323-ra és az MGCP-re (Media Gateway Control Protocol).

A csomagkapcsolt hálózatban az információáramlás hektikus volta miatt kiegészítő információkat kell ráaggatni a jelre – ez az adatcsomag fejrészébe kerül –, a hálózat akt feladategyüttest a Cisco OPT három rétegre osztott távbeszélő-infrastruktúrára bízza, amelyek szabványos nyílt protokollok szerint működnek együtt:

• szolgáltatáskezelő réteg

• híváskontroll réteg

• kapcsolatréteg

A modell elválasztja a híváskontrollt a kapcsolattól (a TDM-ben ezek kötelezően együtt vannak). A csomagkapcsolt hálózatban a kapcsolatrétegben zajlik a tartalom (a beszéd) átv híváskontroll rétegből. A két szint között a H.323 és az MGCP protokoll vezényli az információáramlást. Az IP vagy ATM adatcsomagokat mozgató kapcsolatrétegben jön beszédkódolás és -tömörítés. A hang megbízható minőségéért két eszköz felel. Az integrált Cisco beszédkapuk feladata, hogy a digitális hangmintákat kódolják úgy, hogy a le érkezzenek meg a célállomásra az adott beszélgetéshez tartozó adatcsomagok.

Ehhez az adatcsomag-továbbító technikához tartozik a WFQ (Weighted Fair Queuing, súlyozott elfogulatlan sorba állítás) és a Resource Reservation Protocol, az erőforrást lefo adatforgalom rugalmas irányítása révén – a csomagkapcsolt gerinchálózaton minden kapcsolat megkapja a biztonságos lebonyolításhoz szükséges sávszélességet. (Egy e-mailn szaggatott a kép, netán előbb hullik le az elítélt feje, aztán sújt le a bárd. Ennek megelőzésére szolgál a QoS.)

Ahhoz, hogy érthető beszédhangot lehessen előállítani a hívott félnél, az adatcsomagok beérkezésének egyenetlensége miatt szükség van átmeneti tárolásra, ami zökkenőket okc elhallgatunk, a másik oldalról mindig kis zökkenővel lendül be a beszélőpartner hangja.


A Cisco OPT adatcsomag-továbbítási megoldásai évekkel ezelőtt – teszteredményekkel bizonyítottan – jóval az elviselhetőség határán belül tartották ezeket a kényelmetlenségeket. M

A Cisco OPT híváskontroll rétegében történik a TDM jelzésrendszerben érkező információ fogadása, lefordítása, valamint a kapcsolatról gondoskodó parancsok eljuttatása az akt tartják fenn a vonalat a beszélgetés ideje alatt. Hívás beérkeztekor a jelzést a médiakapu közvetlenül a VSC-nek továbbítja, mintegy leválasztja arról a vonalról, amelyen a kapcsol fél között, nincs előrelátás. Nem így az OPT-ben. A VSC két külön végponttal dolgozik: a kezdeményezővel és a célponttal, és egyszerre tartja rajta „a szemét” mind a kettőn. Í forgalmat, majd a beérkező jelentések alapján döntéseket hozva gondoskodik arról, hogy minden rendben menjen.

A híváskontroll réteg nem improvizál, de nincs is beleégetve, hogy mikor mit kell tennie. Inkább közvetítőként fogható fel: minden helyzetben a szolgáltatásrétegtől kapott infc

telefontársaság API-k és szabványos protokollok segítségével tudja kikényszeríteni a hálózatból. Az OPT tehát felfogható alkalmazásplatformként, ami a beérkező igényhez
berendezései már számos kifinomult szolgáltatással dicsekedhetnek. Ilyen például a hangos levélküldés, a parancshívás (amikor nem kell tárcsázni, csak bemondani, kit keresünk), va
Az OPT telefonhálózathoz a Cisco által kínált berendezések közötti adatforgalom bonyolítható IP és ATM hálózaton egyaránt, míg az előfizetői kapcsolat lehet analóg, xDSL, ISDN
Vargha Márton az Infopen munkatársa. E-mail: **vamaa@infopen.hu.**



## A hagyományos vonalkapcsolt telefonhálózat hátrányai

| | |
|---|---|
| **Kicsi a csatorna sávszélessége** | A telefonálásra szabott, 64 Kbps sebességű vonalon nem lehet mozgóképet közvetíteni, a nagyobb állományok átvitele nagyon lassú |
| Sok az üresjárat | Minden kapcsolat folyamatosan lefoglalja a csatorna teljes sávszélességét |
| A telefonközpontok a 64 Kbps-os csatornák kapcsolására valók | Minden központban be kell építeni azokat a költséges berendezéseket, amelyek szétbontják, majd az iránytól függően újra összecsomagolják a csatornákat |
| Zárt, rugalmatlan jelzésrendszer | Minden továbbítási információt a telefonközpontm kezel, a szolgáltatáskészlet erősen gyártófüggő. Lassító tényező, hogy az új szolgáltatások kialakítása nem a telefontársaság, hanem a telefongyár kezében van |



## A Cisco OPT alaptulajdonságai

- Együttműködik a meglévő telefonhálózattal
- A nagy telefonközpont választékában minden berendezés kezeli az univerzális elérést és a jelzéstovábbítást
- Egyetlen, integrált hálózatban kínál hatékony működést
- A szolgáltatásfejlesztés fölötti ellenőrzés a szolgáltató hatáskörébe kerül
- Segítségével több cég működhet együtt az új szolgáltatások fejlesztésében

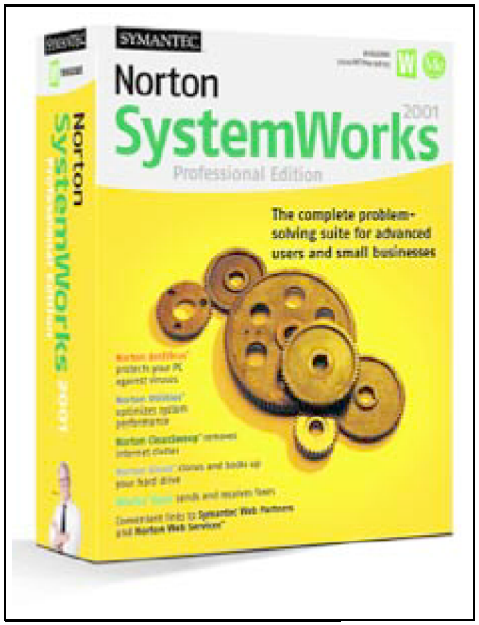
• Gyorsul a szolgáltatásbevezetés
• Kiterjeszti a szolgáltatók piacát
• A hagyományos telefonnál megszokott hangminőséget produkálja
• A párhuzamosítással megszünteti a felesleges redundanciát a funkcionalitásban

**2001. MÁRCIUS / MÉRLEG Symantec Norton Systemworks 2001**

## MÉRLEG
## Symantec Norton Systemworks 2001

**2001. MÁRCIUS / MÉRLEG Symantec Norton Systemworks 2001 / Tisztogatás CleanSweeppel**

## Tisztogatás CleanSweeppel




Egyetlen rossz pontot kapott

Symantec Norton  Systemsworks 2001

Forgalmazó:

Sved Informatikai Rt.

1143 Budapest,

Francia út 38/B

Tel.: 469-9051

Nettó ár: 24 500 Ft

Négy fő csoportba oszthatók a CleanSweepben rejlő alkalmazások: a tisztogató, azaz Cleanup programok, az internetprogramok, a varázslókként megjelenő menedzsmenteszközök, végül a magasiskolát képviselő bejegyzésszerkesztők csoportjába.

A tisztogatást végző alkalmazások közül a SmartSweep figyeli a különböző programok telepítését, azokról jegyzőkönyvet készít, amelyek alapján utóbb nyom nélkül kiirthatók mind a merevlemezről, mind a registryből úgy, hogy írmagjuk sem marad. Ezt a nemes feladatot egyébként az Uninstall Wizard fogja végrehajtani, amely ezernél több programot önállóan is felismer és eltávolít a SmartSweep információi nélkül. Ez volt az egyetlen rossz pont, amit a CleanSweep nálam szerzett: a SmartSweep monitor néha elvesztette a fonalat, és a telepítés második részét végző program ténykedését egyes alkalmazásoknál már nem kísérte figyelemmel.

A Fast & Safe Cleanup eltávolít minden olyan adatállományt a gépről, amit büntetlenül lehet: internet cache fájlokat, ideiglenes állományokat és a Lomtár tartalmát.

A Restore Wizard képes helyreállítani a korábban elmentett alkalmazást – erről bővebben az Archive és a Backup Wizardnál szólunk.

Az internetes eszközök közül az első az Internet Uninstall, amely plug-inek és ActiveX vezérlők eltávolítására szolgál. A SmartSweephez hasonlóan az InternetSweep nevű alkalmazás figyeli azok települését, hogy utóbb nyom nélkül lehessen törölni őket. Az Internet Cache Cleanup – mint a neve is utal rá – a cache könyvtárak tartalmát veszi kezelés alá, míg a Cookie Cleanup ugyanezt teszi a süti állományokkal. A Plug-In Cleanup és az ActiveX Cleanup feladata pedig azoknak a plug-in, illetve ActiveX vezérlőknek az eltávolítása, amelyek valahogy elkerülték az InternetSweep figyelmét.

Ami a menedzsmenteszközöket illeti, az Archive Wizard és a Backup Wizard működése nagyon hasonló. Mindkettő másolatot készít egy alkalmazásról, annak minden hozzávalójával, beleértve még a könyvtárbejegyzéseket is, de az Archive Wizard ki is törli, míg a Backup csak a másolatot készíti el. Az így készült archívum a Restore Wizarddal állítható helyre. A Move Wizard azonos gépen másik könyvtárba, másik merevlemezre költözteti az alkalmazást, a Transport Wizard alkalmazás pedig gépek közötti mozgatására alkalmas: újratelepítés nélkül lehet másik gépre átköltöztetni az alkalmazást!

A haladóknak szóló segédprogramok közül a legelső a Registry Sweep, amely kigyomlálja az érvénytelen bejegyzéseket és újraszervezi a registry adatbázist. A Duplicate File Finder azonos nevű és méretű vagy megadott kritérium szerinti állományokat keres, segítve ezzel a feledékenyebb felhasználók munkáját. A Redundant DLL Finder .DLL és .VBX kiterjesztésű fájlokat keres, amelyeket kevésbé intelligensen megírt telepítőprogramok hajlamosak több példányban a gépre másolni – így azonban elejét vehetjük a helypazarlásnak, hiszen több program bízvást használhatja ugyanazt a példányt belőlük.

Az Unused File Type Finderrel magunk definiálhatunk olyan állományokat, amelyek a CleanSweep söprögetése alkalmával halálukat lelik mint szükségtelenek. Az Orphan Finder dolga, hogy megtaláljon olyan állományokat, amelyek valaha egy alkalmazáshoz tartoztak, de azóta az alkalmazást eltávolítottuk (persze nem a CleanSweeppel), ezek pedig magukra maradtak. Használható továbbá arra is, hogy parancsikonokat visszacsatoljunk eredeti gazdájukhoz, ha azt valamiért elvesztették volna.

A Norton Safe megőrzi értékes fájljainkat: amit eldobunk, és megfelel előzetesen beállított feltételeinknek, az a Lomtár helyett itt landol, és a Safety Sweep megmenekíti őket a CleanSweeppel végzett tisztogatás elől.

Noha a témakör részletesebb kifejtést is megérdemelne, hely hiányában itt kell véget vetnem a CleanSweepről szóló történetnek.

*Tóth Endre számítástechnikai szakértő. E-mail:* ***xorn@matavnet.hu.***

**ÉRTÉKELÉS**

| | |
|---|---|
| Technológia | **** |
| Megvalósítás | ***** |
| ÁR/Teljesítmény | **** |

# Ericsson R380s

**2001. MÁRCIUS / MÉRLEG Ericsson R380s / Kihajtható kényelem**

## Kihajtható kényelem

**Az Ericsson hosszas mérlegelés után belépett a kommunikátor kategóriájú telefonkészülékek gyártóinak sorába.**

**Szerző: Kis János**


Strapabíró, nagy tudású és kellemesen kezelhető

Ericsson R380s

Westel Mobil Távközlési Rt.

www.westel.hu

Nettó ár: 180 000 Ft

Az Ericsson R380s típusú készülék a kommunikátor irányzat képviselője, amely kifogástalanul fordított magyar menürendszerrel most került a hazai boltokba. A telefon tudásában és méretében is jelentősen eltér a klasszikus etalontól. Bár a fejlesztők a konkurens Nokia és a Psion billentyűs rendszereit vették alapul, és ennek megfelelően igyekeztek beleépíteni minél több funkciót, a legfontosabb cél mégis a kis méret és a menedzserkalkulátori feladatok integrálása volt.

Innen ered néhány zavaró hiányossága is. Nem tud például faxolni és csak a WAP-ot képes megjeleníteni, a HTML oldalakat nem. Ha ezen hiányosságaitól eltekintünk, egy igen strapabíró, nagy tudású és kellemesen kezelhető személyi asszisztenst kapunk társul. Az R380s telefon az EPOC/ PALM OS alapján készült, amely az Ericsson utolsó ilyen zárt rendszerű gépe. Ez azt jelenti, hogy hiába szabványos az EPOC operációs rendszer, azt a felhasználó nem tudja megváltoztatni, esetleg új programokkal bővíteni. Ugyanakkor a szabványos EPOC számos olyan új lehetőséget ad, amely megkönnyíti a hibrid eszköz használatát.

A gép az infraporton keresztül képes a saját adatai, azaz névjegyek átküldésére bármelyik újabb típusú, WAP-os Ericsson készülékre. Ugyancsak akadálytalan az infrakapcsolat az EPOC-ot használó marokkomputerekkel és a PALM család tagjaival. Itt nemcsak névjegyet, hanem határidőnapló-bejegyzést vagy szövegállományt is küldhetünk, fogadhatunk. Programok áttölthetők más gépből, de készülékünk azt szövegként értelmezi, így nem telepíti.

Az Ericsson üdvösképének két üzemmódja van. Az egyik, amikor az előlap csukott. Ekkor hagyományos WAP telefonként használhatjuk, s a funkciógombjai is az Ericsson típuscsaládnál megszokott módon viselkednek.

Ha kinyitjuk a készüléket az előlap lehajtásával, akkor megpillanthatjuk az alaptrükköt. Behajtott állapotban a billentyűk az érintőképernyő adott pontjához érve közlik az akaratunkat az eszközzel. Így még a „szokásos” koszolódási hiba sem fordulhat elő. Viszont a nyomógombok becsukott állapotban kissé keményen működnek, határozott erőkifejtést igényelnek.

Az előlapot kinyitva telefonunk automatikusan átvált a marokgépeknél már jól ismert üzemmódba, ekkor ugyanis érintőképernyővel dolgozhatunk. A kijelző kontrasztos, de hátsó megvilágítása ilyenkor nincs. Ha elegendő a beeső fény, akkor kiválóan lehet vele dolgozni.

A szöveg beírására két út közül választhatunk. Az egyik a gyors pötyögtetésre is alkalmas érintőképernyőn feltűnő billentyűzet. Ezen némi gyakorlás után a hölgyek kihegyezett körmeikkel, az erősebb nem képviselői pedig a mellékelt pálcikával tehetnek próbát. Mazochistáknak viszont ott a kézírás-felismerés. Ugyanis ez nem egy kézírás-felismerő, nekünk kell megtanulnunk egyfajta gyorsírást, amivel szintén szép sebességet lehet elérni a szöveg bevitelében. A beírt szöveg az-után átvihető infraporton keresztül egy másik Palmra vagy adatkábellel akár egy PC-re.

A telefonhoz mellékelik a Windows 95/98/NT/2000 platformokon futó Lotus Organizer programot. Amennyiben teljes Lotus Smart Suite van a számítógépünkön, és az Organizer, valamint a szinkron programok telepítését is elvégeztük, a rendszer az egész komplex alkalmazással képes együtt dolgozni.

Talán a közgazdászok hiányolják, hogy a telefonban nincs számolótábla, csak kalkulátor. Viszont van nagyon sokoldalú határidőnaplója. A gép webes képességekkel dicsekedhet, s ha a szolgáltató lehetővé teszi, POP3 levelezésre is használható. Az elektronikus leveleket elküldhetjük az E-mail-to-SMS szolgáltatás vagy – ha a szolgáltatónak van ilyen – az SMTP szerver segítségével.

A készülék egyébként robusztus felépítésű; véletlenül többször is leejtettük, mégis kibírta. Olyan menedzsereknek ajánljuk, akiknek fontos a sok cím és telefonszám, valamint a határidők áttekinthető és rendezett tárolása, ugyanakkor nem ragaszkodnak a mobilkommunikáció teljes tárházához. A kis méret és tömeg mellett az Ericsson R380s határozott erőssége a megbízható működés.

Kis János szabadúszó informatikai szakújságíró.

E-mail: **johannes@mail.datanet.hu.**

**ÉRTÉKELÉS**

| | |
|---|---|
| Technológia | ***** |
| Megvalósítás | **** |

| | |
|---|---|
| Technológia | ***** |
| Megvalósítás | **** |
| ÁR/Teljesítmény | *** |


A készülék tesztelését a  Westel Mobil Távközlési Rt. támogatta.

**2001. MÁRCIUS / MÉRLEG Philips Magic 2 Classic 6 in 1**

# MÉRLEG
# Philips Magic 2 Classic 6 in 1

**2001. MÁRCIUS / MÉRLEG Philips Magic 2 Classic 6 in 1 / Hatot egy csapásra**

## Hatot egy csapásra

**A múlt és a jelen ötvözése egy készülékben.**

**Szerző: Hanácsek István**

Irodai mindenes kompromisszumokkal

**Philips BE Hungary Ltd.**

1119 Budapest,

Fehérvári út 84/a

Tel.: 382-1700

Bruttó ár: 89 990 Ft

Festékkendő ára: 6990 Ft

A nyolcvanas évek elterjedt adatátviteli eszköze volt a telex, ám a faxkészülék megjelenése szinte egyik pillanatról a másikra véget vetett karrier-jének. Most hasonló helyzet előtt állunk: az internet, illetve az e-mail terjedésével lassan bealkonyul a hagyományos faxoknak. A gyártók is érzik ezt, sorra dobják piacra kombinált berendezéseiket, amelyek több feladat ellátására is képesek. Az öszvér berendezések szinte kivétel nélkül a számítógép perifériájaként is használhatók.

A Philips magyarországi képviseletétől olyan eszközt kaptunk, amely meglehetősen kilóg a sorból. A *Magic 2 Classic 6 in 1* faxkészülék a múlt és a jelen technikájának furcsa keveréke. A Philips mérnökei rájöttek, hogy egy ilyen szerkezet minden különösebb átalakítás nélkül is alkalmas a beolvasott dokumentáció másolására és szkennelésére. Mivel a berendezés távbeszélővonalon keresztül működik, telefonként is alkalmazható. Ehhez már csak egy kicsit kell hozzátenni, és akkor üzenetrögzítő is lehet.

Eddig semmi különös nincs ebben, hisz tucatszám léteznek ilyesfajta eszközök. Csakhogy a Philips fejlesztői nem álltak meg itt. Az első meglepetés a nyomtatási mód. A szöveget vagy képet normál papíron, a régóta ismert festékkendős módszerrel jeleníti meg. A másik furcsaság a kivehető szkenner. Ezzel a megoldással az egyébként áthúzó rendszerű szkennert könyvek, vastagabb brosúrák beolvasására is használhatjuk. Az ötlet némiképp a kézi szkennerek virágkorára emlékeztet. Praktikussága mellett komoly hátránya ennek a megoldásnak, hogy a beolvasott kép minősége kézügyességfüggő.

A Philips Magic 2 beépített digitális üzenetrögzítője akár harmincpercnyi hanganyag tárolására képes, fax része szintén komoly kapacitással rendelkezik. Papírhiány esetén ötvenoldalnyi anyag fér el a memóriájában, amit később kinyomtathatunk. Az adatátviteli sebessége viszont mindössze 9600 baud, ellenben a faxokat egy beállított időpontban is

elküldhetjük (körfax). Érdekes szolgáltatás, hogy az intelligens faxkapcsoló segítségével a beszélgetések átkapcsolhatók külső készülékre, például vezeték nélküli telefonra. A telefonmodul is korszerű. A számos alapfunkció (telefonkönyv, kihan-gosítás stb.) mellett tízféle csengőhangból választhatjuk ki a számunkra legmegfelelőbb dallamot.

Ez a modell nem illeszthető közvetlenül számítógéphez, igaz, az említett faxkapcsolóval – külső modemen keresztül – a dokumentumokat átküldhetjük PC-re.

Mit tud még a Philips Magic 2 Classic? Másolóként egyszerre ötven kópiát készíthetünk kétféle (finom- és fénykép-) felbontásban. Természetesen a technológiából adódóan ne várjunk csodát a kapott másolat minőségétől! A másolásnál és a szkennelésnél beállítható nagyítás és kicsinyítés. A telefonkönyv kapacitása figyelemre méltó, hiszen 200 név és telefonszám fér el benne; ebből tízet gyorstárcsázásra is kijelölhetünk.

A világ legkisebb multifunkciós készüléke címre esélyes Magic 2 elsősorban a kis hellyel és számítógéppel nem rendelkezőknek ajánlható.

Hanácsek István a HiCo Számítástechnika cégvezetője.

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

**ÉRTÉKELÉS**

| | |
|---|---|
| Technológia | *** |
| Megvalósítás | *** |
| ÁR/Teljesítmény | *** |

**2001. MÁRCIUS / MÉRLEG Philips Magic 2 Classic 6 in 1 / FÓKUSZ**

## FÓKUSZ

**Kendőzetlenül**

A kilencvenes évek elején a nyomtatótechnológiák jellegzetes megoldásainak egyike volt a festékkendő. A nyomtatandó lap teljes felületét befedő kendővel gyorsabb nyomtatást lehetett elérni, ám számos hátrányos tulajdonsága miatt mégsem terjedt el. A kendő együtt mozgott a papírral, és azok csak a nyomat helyén érintkeztek. Ha csak a lap tetején és az alján volt szöveg, akkor is egy egész oldalnyi festékkendő fogyott el, ugyanis ezeket – szemben a festékszalagokkal – egyszer lehetett használni. Az igencsak pazarló és költséges prin-telés biztonsági szempontból sem volt tökéletes: az elhasznált festékkendő – az indigóhoz hasonlóan – megőrizte a kinyomtatott dokumentum tükörképét.

FOTÓ: **SZEPESI TIBOR**

**2001. MÁRCIUS / MÉRLEG Pulsar CL és CL+**

# MÉRLEG
# Pulsar CL és CL+

**2001. MÁRCIUS / MÉRLEG Pulsar CL és CL+ / Káros feszültségek nélkül**

## Káros feszültségek nélkül

**Érthetetlen módon az emberek nehezen szánják rá magukat, hogy drága berendezéseik mellé megfelelő biztonságot nyújtó eszközöket vásároljanak.**

**Szerző: Hanácsek István**


A Pulsar CL elosztók olcsó, ám hasznos készülékek

**FOTÓ: SZEPESI TIBOR**

**MGE UPS SYSTEMS**
**Hungary Kft.**
**1119 Budapest, Fehérvári út 83.**

**Tel.: 204-3033**

**Pulsar CL**

**Nettó ár: 5500 Ft**

**Pulsar CL+**

**Nettó ár: 8000 Ft**

A gyakorlati tapasztalat azt mutatja, hogy számos felhasználó áldoz jelentős összeget, hogy a „leg-leg” számítógépet tudhassa a magáénak, azonban ha a rendszer biztonságáról esik szó, már minden drága, ami nem ingyenes. Ezen érdemes egy kissé elgondolkodni. Egy sereg példa akadt már arra, hogy egy egészen egyszerűnek tűnő, hétköznapi eset komoly, több tízezer forintos kárt okozott a gépben. Ehhez elegendő egy váratlan, mindössze egyetlen pillanatig tartó áramkimaradás. Az ilyenkor fellépő áramlökés akár az alaplapot is tönkreteheti. És akkor még nem említettem a villámcsapást, ami a kábelen keresztül – legyen az bármilyen – káros feszültséget indukálhat a gépünkben. Az ilyen és ehhez hasonló károk megfelelő, aránylag alacsony áron beszerezhető eszközökkel elkerülhetők.

A közelmúltban a Pulsar CL és CL+ túlfeszültség-védelemmel ellátott tápelosztókat tesztelhettük a gyártó, az MGE (Merlin Gerin) jóvoltából. Mindkettő a 220 voltos hálózatot osztja szét öt csatlakozóhelyre. Az elosztó jellegzetessége, hogy a bejövő feszültséget elektronika figyeli, és kiszűri az esetleges áramlökéseket. Végső esetben biztosíték is védi az elosztóhoz kapcsolt berendezéseket. A CL+ változat mindössze annyival nyújt többet, hogy az alján két darab (be/ki) RJ 11-es telefoncsatlakozót is elhelyeztek. Ha a telefonvonalra ezeken keresztül kapcsolunk bármilyen telefonkészüléket, faxot, modemet, ez az eszköz is védett lesz például a villámcsapás okozta károk ellen.

A Pulsar CL-t úgy alakították ki, hogy bármilyen formájú konnektorcsatlakozó, de még a közvetlenül konnektorba dugható tápegységek is kényelmesen elférjenek egymás mellett. Az elosztó oldalán található billenőkapcsolóval a biztonság tovább fokozható, hiszen a rá kapcsolt és használaton kívüli berendezések megbízható áramtalanítása egyetlen mozdulattal elintézhető. A Pulsar tetejére két kis lámpát tettek a tervezők. A zöld a bekapcsolt állapotot, a narancsszínű a túlfeszültség-védelem működését jelzi. Az elosztó alján és oldalán egy-egy kábelvezető csatorna van, így valamelyest rendezhetjük azt a kábelerdőt, ami a számítástechnika kellemetlen velejárója. Szintén az alján rejtőzik egy két csavarfejnek kialakított rés, ezekkel akár a falra is fölerősíthetjük az elosztót.

Mindkét készülék alkalmas a legfeljebb 230 voltos, 50-60 Hz-es hálózat kényelmes megosztására. A legnagyobb terhelhetőség viszont csak 10 A lehet. Ez azt jelenti, hogy a Pulsarhoz nem ajánlatos egyszerre több, ráadásul nagy fogyasztású háztartási gépet csatlakoztatni, viszont remekül használható a számítástechnikai eszközökhöz és a szórakoztató elektronikához. Az elosztó 1,8 méteres, PC szabványú kábellel kerül forgalomba.

Hanácsek István a HiCo Számítástechnika cégvezetője.

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

**ÉRTÉKELÉS**

| | |
|---|---|
| Technológia | **** |
| Megvalósítás | ***** |
| ÁR/Teljesítmény | ***** |

**2001. MÁRCIUS / MÉRLEG Pulsar CL és CL+ / FÓKUSZ**

## FÓKUSZ

**TÁPZAVAROK**

**Feszültségemelkedés:** a normálisnál 10 százalékkal magasabb feszültség.

**Nagyfeszültségű tüske:** a feszültség hirtelen, rövid időre 6000 V fölé emelkedik.

**Kapcsolási tranziens:** a feszültség 10–100 mikroszekundum alatt 20 000 V-ra emelkedik.

**Feszültségletörés:** a feszültség a normális 80-85 százaléka.

**Frekvenciaingadozás:** olyankor lép fel, ha a tápellátást szükségáramforrásról kapjuk.

**Feszültségcsökkenés:** túlterhelt hálózat folyamatosan alacsony feszültségi állapota.

**Áramszünet:** legalább két perióduson át tartó nulla feszültség.

**Vonali zaj:** rádiófrekvencia és elektromágneses interferencia.

**Harmonikus torzítás:** a nemlineáris fogyasztók (például kapcsoló üzemű tápegységek, fordulatszabályozós motorok, faxkészülékek, fénymásolók) okozzák.

**2001. MÁRCIUS / DR. WATSON Fóti Marcell rovata**

## DR. WATSON
### Fóti Marcell rovata

**2001. MÁRCIUS / DR. WATSON Fóti Marcell rovata / Technokrimi II. rész**

## Technokrimi II. rész

**Amíg a világ világ, a bankokat ki fogják rabolni, az operációs rendszereket pedig meg fogják erőszakolni.**

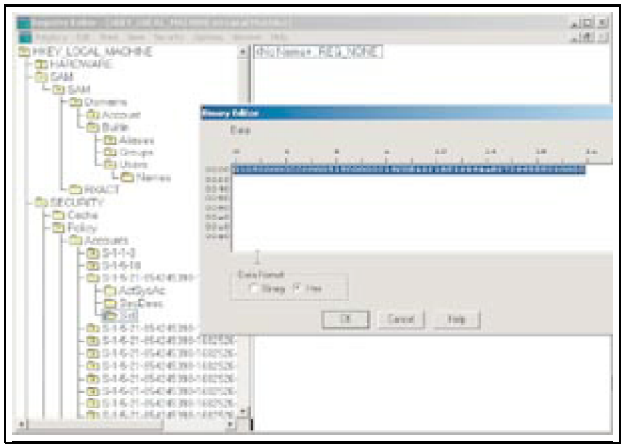
FOTÓ: SEBESTYÉN JENŐ

Hát sokféleképpen fogalmazhatnám át a múltkori számban megjelent krimi első részének fogadtatását, de szó, mi szó, nem jött be. Viszont örömmel tapasztaltam, hogy igen sokan olvassák Dr. Watson cikkeit, hisz csak a „jéghegy csúcsa” mond véleményt, ad visszajelzést a szerzőnek a mű fogadtatásáról, s ha ekkora a csúcs, jó nagy lehet az a jéghegy. A „nem áll jól neked a hazudozástól” a „végre valaki a sajtót is lelepleziig” mindenféle hatást sikerült kiváltanom pamfletemmel. Mindenesetre a békesség érdekében a biztonsággal kapcsolatos cikksorozatomat mostantól szereplők nélkül folytatom, nyitva hagyva az égető kérdést: vajon az előző részben tényleg igazat írtam-e vagy mégsem?

**A hackerek álma**

A kérdés tehát az: vajon hogyan képzelhető el, hogy valaki idegen a rendszergazda nevében (szándékosan nem nevét és jelszavát írtam, hisz nem feltétlenül kellenek ezek az adatok a rendszergazdává váláshoz) tesz-vesz a hálózatban, s ezzel gyakorlatilag nevetségessé teszi a rendszernapló bejegyzéseit? Mivel még számos vállalatnál nem tértek át az elődeinél lényegesen megbízhatóbb Windows 2000 használatára, könnyű dolga lehet a botcsinálta hackernek is. A rendszergazdává válásnak elképesztően széles palettája alakult ki a történelem folyamán, ezek közül ismerkedünk meg néhánnyal. Néhány trükk persze azonnal elavult a Windows 2000 megjelenésével, ám ravasz gondolkodással – csökkenő számban ugyan, de – újak és újak fedezhetők fel.

Tulajdonképpen minden behatoló célja a rendszergazdai jogosultság megszerzése, annak birtokában ugyanis bárki bármit tehet egy adott rendszerrel – még azt is, amit nem!



1. ábra. Rövid keresgélés után az „olvashatatlan” SID-ekbe is belepillanthatunk

Lássuk először azt a trükköt, ami rávilágít a hacker gondolkodásmódjára: közismert tények megfelelő csoportosításával és más nézőpontból történő szemlélésével egészen érdekes megoldásokra tudjuk rávenni a rendszert és a rendszergazdit. A Windows NT alapértelmezett NTFS jogosultsági „rendszere” enyhén szólva lyukacsos, kitárulkozó: Everyone – Full Control. Ennek birtokában gyakorlatilag bárki, aki a rendszerhez hozzáfér – Everyone esetén az anonim felhasználók is – azt csinál az NTFS-en, amit nem szégyell. Töröl, átnevez, mozgat stb. Most képzeljük el, hogy gyalogos, sima felhasználók vagyunk egy rendszerben, és erről a mélypontról szeretnénk kimozdulni a rendszergazda segítsége nélkül. Mi lenne, ha a WINNT\Profiles\All Users mappában elhelyeznénk egy olyan batch fájlt, amelynek a tartalma a következő:

*NET LOCALGROUP Administrators XY /add*

Ez az XY nevű felhasználót az Administrators csoport tagjává teszi. Ezután ez a fájl minden felhasználó bejelentkezésekor le fog futni. Ha Pityi Palkó-erősségű felhasználóval jelentkezünk be, csak egy furcsa felvillanást látunk, amíg a CMD.EXE jogosultság híján reménytelenül küzd a feladattal. De ha rendszergazda lép be, akkor… nos, XY rendszergazdává válik.

Ez az egyszerű trükk sokféleképpen variálható. Egy másik megoldással még csak ki sem kell várnunk, hogy arra járjon egy rendszergazda, a „felkonvertálás” vagy „lovaggá ütés” megtörténhet külső beavatkozás nélkül. Ehhez azt kell tudnunk, hogy az operációs rendszer részei a SYSTEM felhasználó nevében futnak, azaz mindent megtehetnek. A SYSTEM futtatja a WinLogon processzt, amely unalmas óráiban a logon.scr képernyővédővel próbálja elejét venni annak, hogy a Ctrl+Alt+ Del ablakocska örökre beégjen a képernyőbe. Nos, az NTFS alapjogosultságai segítségével a logon.scr két egérmozdulattal lecserélhető akármire, aminek logon.scr a neve.

*REN logon.scr akarmi.qqq*

COPY cmd.exe logon.scr

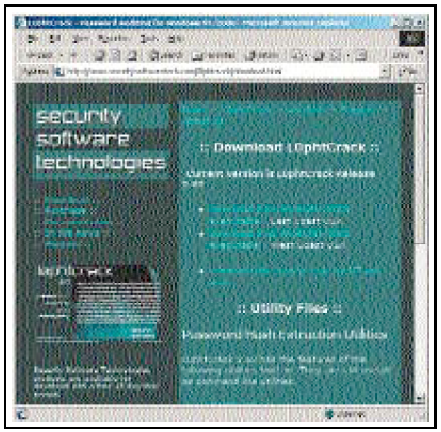
Ezután jelentkezzünk ki, és várjuk meg, amíg a WinLogon elunja a bejelentkezésre várást, és belekezd a képernyővédő futtatásába: egy frankó, erős parancssorhoz jutunk, amelyben izomerőből fut minden! Az innen indított Regedt32.EXE például simán írja és olvassa a regisztrációs adatbázis SAM részét, amit még az Administrator is csak akkor tehet meg, ha jogot ad magának!

Hát nézzünk körül a SAM-ban!

**„Titkosított” jelszavak**

A SAM a régi, öreg Windows NT biztonsági adatbázisa, de ugyanezzel futnak a nem tartományvezérlő Windows 2000 gépek is – Pro és Server. Ebben tanyáznak a felhasználói fiókok és a jelszavak. Jobban mondva a közhiedelemmel ellentétben a jelszavak nincsenek itt, hanem sehol sincsenek; az NT nem a jelszavakat, hanem az azokból képzett úgynevezett hasheket tárolja – egyébként valóban a SAM-ban.

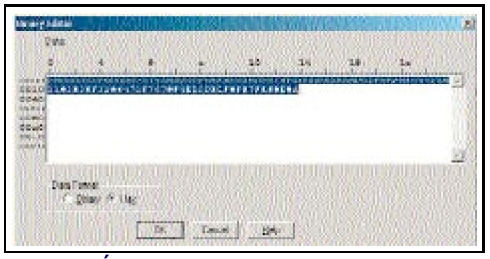
Érdekes, Redmond hogy dugdossa előlünk a SID-eket! Aki bátortalan vagy figyelmetlen, bizony nem kattint kettőt a REG_NONE típusú változón, és így sohasem botlik bele a SID-ekbe. A jelszó-hashek még jobban el vannak dugva. Tekintve hogy itt a jelszavak még csak nem is visszafordítható titkosítással tárolódnak, azt hihetnénk, a világon senki nem képes ezeket elolvasni. A Microsoft is pusztán elméleti lehetőségként tekintett e „jogsértésre” mindaddig, amíg a LOphtCrack társaság a gyakorlatba át nem ültette ezt 1992-ben. Különös, hogy ez a hackerbanda hogyan szelídült meg az idők folyamán a pénz szagától. Míg régebben eszközüket úgy dicsérték mint nélkülözhetetlen hackerszerszámot, manapság kormányzati és egyéb köröknek ajánlják mint pótolhatatlan biztonságnövelő terméket (2. ábra).



2. ábra. A LOphtCrack átállt a jó oldalra

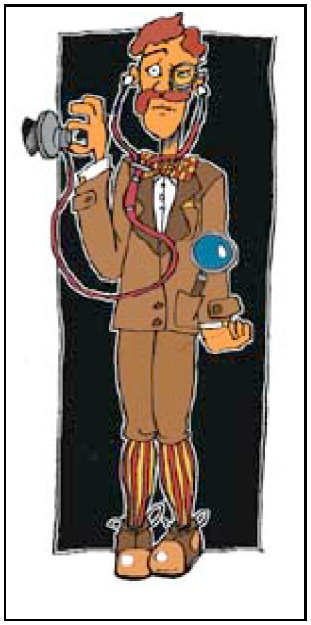
**Van megoldás!?**

S hogy mit tehetünk ennyi gonoszság láttán? Lemondunk a Windows 95, 98 és NT használatáról minden olyan környezetben, ahol a biztonság valamit is számít, és roppant sürgősen áttérünk Windows 2000-re – amíg lehet. Tartománykörnyezetben ugyanis a SAM-ok gyakorlatilag (enyhe csúsztatással) üresek, a jelszó-hashek az Active Directoryban tárolódnak, ami ellen egyelőre nincs orvosság. 2001 második felétől pedig jön a Windows 2000 utódja, a Whistler, s lehet, hogy minden megváltozik – bár a kompatibilitási igény nagy úr. De addig is, amíg tehetjük, éljünk vissza jogainkkal! (Íme egy jelszó-hash a SAM-ból a 3. ábrán.)



3. ábra. Így fest egy jelszó-hash

Van-e olyan trükk, ami esetleg a Windows 2000-nél is lehetővé teszi a rendszergazdává válást? Van. De olyan is akad, ami a büszke Linuxot szégyeníti meg. Amíg a világ világ, a bankokat ki fogják rabolni, az operációs rendszereket pedig meg fogják erőszakolni. Sokan ismerik az Administratorrá válás ama fortélyát, hogy idegen operációs rendszerrel bejelentkezve letöröljük a SAM-ot. Ekkor az NT a bootoláskor készít magának egyet, egy vadiújat, benne adminnal, üres jelszóval. Nos igen. A halott indián a legjobb indián, a leállított operációs rendszer nyilván nem védi a gépet. Éppen ezért adhatunk igazat a Microsoft Security oldalakon olvasható tízparancsolat első tételének: Az a gép, amelyikhez idegenek hozzáférhetnek operációs rendszer indítása céljából, az a gép nem a miénk többé. S aki habzó szájjal azt fröcsögi, hogy e szabály alól mentes bármelyik másik operációs rendszer (OS/2, MacOS, BeOS, Linux stb.), annak nem ajánlom, hogy odaengedjen engem bootlemezzel a gépe közelébe… :)



**GRAFIKA: BUTTINGER GERGELY**

És mi a helyzet a hálózattal? Kell-e nekem egyáltalán a rendszergazda jelszava ahhoz, hogy fájlokat lopkodjak? A hálózaton az NT4-gyel bezárólag az adatforgalom

titkosítatlanul zajlik. Elég (lehet) egy Network Monitor és némi türelem ahhoz, hogy kivárjuk, míg a hálózaton áthalad az orrunk előtt a FONTOS.XLS, és mi szépen elkapjuk. A LOphtCrack pedig a hálózaton átvonuló NTLM hashek elkapásában és visszafejtésében nyújt pótolhatatlan segítséget.

Hát, kedves hook, ez a válaszom arra a kérdésre, hogyan lehetséges az, hogy az eseménynapló szerint te loptad el a műsortervet. A következő alkalomtól a megelőzésre, a védekezésre adok tippeket, gyakorlati segítséget. Megnézzük a bejelentkezés biztonságosabbá tételének lépéseit, a titkosított hálózati forgalom megvalósítását, a titkosított fájlrendszert, a jogosultsági rendszer értelmes használatát – röviden mindazt, ami ahhoz hiányzik, hogy nyugodtan aludhassunk.

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

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

**2001. MÁRCIUS / FÓKUSZ Adatbiztonság**



**2001. MÁRCIUS / FÓKUSZ Adatbiztonság / Kisebb a narancsnál**

# Kisebb a narancsnál

**A személyes információk védelmére magyar kódolóeszköz született.**

**Szerzők: Landy Kornél és Sziklay Péter**

Általános tapasztalat, hogy még az anyagigényesnek tartott iparágakban (nehézipar, építőipar) is igen kevés azok aránya, akik közvetlenül kapcsolatba kerülnek a felhasznált matériával, az alapanyaggal, a félkész és késztermékkel. A legtöbben inkább csak az ezekről szóló, illetve a munkaszervezéssel, a megrendelőkkel, a szállítókkal, a dolgozókkal, a bérezésekkel, a pénzügyekkel és az üzleti tervekkel kapcsolatos információkkal dolgoznak. A modern vállalkozások tevékenységének hatásfokát, sikerességét, megbízhatóságát tehát az információfeldolgozás milyensége határozza meg.

Az információs forradalom eufóriájában azonban hajlamosak vagyunk megfeledkezni bizonyos alapvető adatbiztonsági, hitelességi igényekről. Az írásos, papír alapú információcsere és -tárolás egyeduralma alatt például a postai szolgáltatásoknál, a bíróságokon, a hivatalok hiteles okiratkezelésénél igyekeztek létrehozni – saját körükön belül – az adott formához illeszkedő adatbiztonsági eljárásokat. Ezzel szemben a digitális adatfeldolgozás automatikusan semmilyen manipuláció elleni védelmet nem tartalmaz. (Ráadásul az adatbankba betörő tolvaj nem hagy ujjlenyomatot, azonosításra alkalmas szövet-, haj- vagy egyéb maradványt.)

Természetesen információink védelme és hitelessége éppúgy fontos a tárolt adatoknál, mint az illetéktelenek kizárása. A jogosulatlan hozzáférés kizárása a digitális adattárolás

esetében szinte lehetetlen, hiszen fizikai szinten (vonallehallgatás, háttértár-kiolvasás) a hozzáértő rosszindulat „meg tudja nézni a biteket”. Az illetéktelen hozzáférés nem, de az illetéktelen felhasználás, illetve az illetéktelen manipulálás a rejtjelezett adatokkal megakadályozható, ha a rejtjelezés-visszafejtés, valamint az ehhez tartozó kulcsok és eljárások kellően védettek.

**Rejtjelezés**

A rejtjelezés nem más, mint adatokon végzett manipuláció, amely az eredeti tartalmat lehetőség szerint (a visszafejtéshez szükséges ismeretek hiányában) semennyire nem tükröző kimenetet ad. A rejtjelezettekből az eredeti adatokat csak bizonyos ismeretek birtokában lehet könnyen visszaállítani, míg nélkülük a visszaállítás csaknem reménytelen, a próbálkozások száma és időtartama csillagászati nagyságrendű.

Szimmetrikus rejtjelezéskor a rejtjelező és a visszafejtő ugyanazt a kulcsot használja, e kulcs birtokában rejtjelezett üzenet előállítására és visszafejtésére is képes. Aszimmetrikusnál a rejtjelezés kulcsa más, mint a visszafejtésre alkalmas párja, sőt az egyikből a másik nem is számítható (RSA algoritmus).


**Üzenethitelesítő kód**

Sokszor nem is az a legfontosabb, hogy védjük az üzenetet, illetve annak tartalmát az illetéktelen szemek elől, inkább a dokumentum változatlanságának garantálása a cél. Ezért olyan tömörített kivonat (lenyomat) előállítása vált szükségessé, amely az eredeti dokumentum bármelyik bitjének megváltozására megváltozik, de visszafelé már nem követhető, hogy egy adott bitcsere hatása hogyan „kompenzálható”. Jó védelmi hatású, ha a kivonat (MAC, üzenethitelesítő kód) előállítása tartalmaz változó elemet (kulcs). Az üzenet hitelesítése természetesen a kapott üzeneten végigfuttatott eljárással és az üzenettel „utazó” kontrollkód összevetésével történik. Azért, hogy a küldött kódot ne lehessen az üzenettel együtt manipulálni, kiválóan használható a nyilvános kulcsú rejtjelezés. A MAC-ot (és még néhány, a keletkezés körülményére vonatkozó információt, például az időpontot, az adatállomány nevét, sőt a MAC kulcsát is) a titkos kulcsféllel rejtjelezve elérhető, hogy az üzenet fogadója a változatlan MAC-ot kapja meg (digitálisaláírás-, illetve digitálispecsét-képzés).

**Transzformáció**

Bármily meglepő, de az adatbiztonság terén jól használható olyan „rejtjelezés” is, amikor a rejtjelezett adattömegből nem lehet visszaalakítani a kiindulási állapotot. Itt pontosan ez a cél! Annak érdekében, hogy csak a jogosult személyek férjenek hozzá a védett információkhoz, illetve használhassák a rendszer szolgáltatásait, általában szükség van

valamiféle azonosítókód tárolására.

Ahhoz azonban, hogy még a rosszindulatú hozzáértő se tudja a tárolt kódokból a beadandó jelszót megállapítani, a kódokat a jelszavakból transzformációval kell meghatározni.

A tartalmi változatlanságot a MAC többféle eljárással elvégzett meghatározása és nyilvános kulcsú csomagolása (digitális pecsét) garantálja. Ha ebben a készítés dátuma is szerepel, a forrás azonossága mellett a készítés időpontja is hitelesen ellenőrizhető (időpecsét). Ha a pecsét vételoldali ellenőrzése után a vevő fél szintén elkészíti a saját pecsétjét a kapott információról, s ezt visszaküldi a feladónak, az adott tartalmú üzenet vételét is egyértelműen nyugtázta.

**Biztonsági problémák**

A védelmi rendszer akkor egyenszilárdságú, ha a védelem bármely pontjának áttörése ugyanannyi munkát (időt, pénzt) igényel. Hiába erős a matematikai algoritmus, ha a használt kulcsok védtelenek, könnyen ellophatók vagy a rendszer használatához (personal access) elegendő egy begépelt jelszó.

Ezért alapvető biztonsági kérdés, a felek hogyan juttatják el egymáshoz az aktuális rejtjelkulcsot. Az adatgyűjtésen alapuló feltörés ellen véd, ha a kulcsokat véletlengenerátorral állítják elő. (A legjobb az úgynevezett fizikai véletlengenerátorok alkalmazása, amikor valamilyen véletlenszerű elektronikus zaj digitalizálása szolgáltatja a valóban független számértékeket.) Ilyenkor az ak-tuális kulcsot csak védetten szabad vonalra engedni. Ez megoldható például úgy, hogy a rejtjelezést véletlen kulccsal végezzük valamely ismert rejtjelező eljárás szerint, a kulcsot pedig nyilvános kulcsú eljárással duplán „csomagolva” küldjük el a fogadónak (a saját rejtett és a cím nyilvános kulcsfelével rejtjelezve).

Szimmetrikus rejtjelezés esetén természetesen külön kulcs kell, amelynek a rendszeren belüli szétosztása nem egyszerű. Ilyenkor a hálózaton belül kriptográfiai hálózatot kell létrehozni, továbbá az e rendszer számára használatos kulcsok generálására, szétosztására felkészített Kulcsgondozó Központot is üzemeltetni kell, ami legalább olyan összetett probléma, mint maga a rejtjelezés.

*Shannon* szerint a törhetetlen rejtjelezés receptje, ha az üzenettel megegyező hosszúságú fizikai, véletlen bitsorozatot alkalmazunk. Ezzel a sorozattal EXOR művelet segítségével rejtjelezzük az üzenet bitjeit. A véletlen bitsorozatot (kulcsot) abszolút biztos csatornán kell eljuttatni a vevőhöz. Ezután a rejtjelezett üzenet bármilyen csatornán eljuttatható a vevőhöz, aki a kapott üzenetből a kulccsal végzett EXOR művelettel vissza tudja állítani az információt.

Ahhoz, hogy a hálózatba szervezett felhasználók az abszolút biztos csatornát az egymás közötti információcsere védelmére is fel tudják használni, célszerű pont–pont közötti kulcsokat is használni. Hogyan valósítható meg a kulcsok ilyen előállítása, szétosztása? Lehetséges megoldás, ha az N résztvevős kriptográfiai rendszer meghatározásakor fizikai véletlengenerátor segítségével hozunk létre egy N×N-es szimmetrikus mátrixot. Minden rejtjelező eszköz megkapja a mátrix egy sorát (az i-edik eszközbe az i-edik sort, a j-edik eszközbe a j-edik sort). Ha a mátrix alapfeltöltése fizikai véletlen számokkal történt, ez az elem e két helyen kívül sehol máshol nem fordul elő és nem is kikövetkeztethető. Ezek után ha az i-edik eszköz a benne tárolt mátrixsor j-edik elemét használja rejtjelkulcsként, biztos lehet, hogy üzenetét csak a j-edik eszköz lesz képes megérteni – természetesen ha tudja, hogy neki pedig az i-edik elemet kell elővennie.

**Jogosultság-ellenőrzés**

Minthogy a rejtjelezést információfeldolgozó gépek végzik, külön feladat bebizonyítani a jogosultságunkat a gépeknek. Olyan eljárásra van szükség, ami hitelt érdemlően és lehetőség szerint hamisíthatatlanul képes a személyt azonosítani. A szakirodalom három módszert (vö. *A biztonság kilenc pontja,* BYTE Magyarország, 2001. február) ismertet: a fizikai birtoklást (nálunk van a kulcs), a logikai birtoklást (tudjuk a jelszót) és a biometriai paraméteren alapuló azonosítást (egyezik az ujjlenyomatunk). E három eljárásból legalább kettő egyidejű alkalmazása szükséges a megbízható hozzáférés-engedélyezéshez.

**Egyenszilárdság**

Százmilliónyi személyi számítógép szolgálja világszerte az információfeldolgozás, -szolgáltatás, -fogadás igényeit, s ezek egyre nagyobb része kerül egymással kapcsolatba a világhálón. A mögöttük lévő hatalmas embertömegben óhatatlanul akadnak rosszindulatúak is. A hozzáértő rosszindulat számára mindaz nyílt, ami szoftveresen felfedhető. Az

egyenszilárdsághoz hardverkiegészítés szükséges. Milyen információkat, műveleteket kell extra hardverre bízni?

• Az effektív rejtjelkulcs nem jelenhet meg a PC memóriájában.

• A rejtjelezés folyamata ne legyen a PC felől megfigyelhető.

• A kulcsok generálására valódi (fizikai) véletlengenerátort kell használni.

• Lehetőség szerint saját időalapot és nem felejtő memóriában tárolt naplót is tartalmazzon.

• A personal access, illetve a személyes jogosultságok és kulcsok fogadására csak biztonsági csatornát szabad használni.

• A személyhez kötött hozzáférések és jogosultságok eldöntése nem történhet a PC-ben.

Az utolsó pont azt jelenti, hogy a személyhez kötött hozzáférések és jogosultságok nem a PC-ben lévő programok futtatását engedélyezik, hanem az extra hardver belső működésének beállítását eredményezik, és a használhatóságot szabják meg („hajlandó-e" rejtjelezni vagy digitális aláírást képezni az extra hardver).

Személyes adatbiztonság céljára nem elegendő például a PC-n futtatott szoftver, egyéni rejtjelező gépre van szükség. E megfontolások alapján készült az ITEA Kft.-nél az angol Personal Privacy kifejezés alapján PePynek nevezett személyes biztonsági eszköz. A gyufásdoboznyi hardver centronics felületre (nyomtatókimenetre) csatlakoztatható, és alkalmas csak a tulajdonosára jellemző módon 128 bites kulcsú szimmetrikus, valamint digitális aláíráshoz a nyilvános kulcsú rejtjelezést védetten futtatni.

Landy Kornél az ITEA Kft. műszaki igazgatója, Sziklay Péter pedig az ITEA Kft. főmérnöke.

E-mail: **mail@itea.hu.**

**HOL TALÁLHATÓ?**

**Információtechnika és Elektronikus Adatvédelem Kft. (ITEA)**

1026 Budapest, Hidász u. 2/b

Tel.: 200-2638

**2001. MÁRCIUS / FÓKUSZ Adatbiztonság / PePy csak egy van**

## PePy csak egy van

Minden PePynél egy gyártási szám egyetlenegyszer fordul elő. Az egyedi kulcstáblázatok garantálják, hogy több mint négymilliárd PePy közül csak ketten képesek ugyanazt a kulcsot előállítani, reprodukálni, így e hatalmas rejtjelező hálózat tagjaiként bármelyik két eszköz alkalmas mások által megfejthetetlen (úgynevezett viszonylatfüggő) rejtjelezés és visszafejtés elvégzésére. Az eszköz belső fizikai véletlengenerátora segítségével állítja elő saját kulcsait. Felhasználói parancsra generálja a nyilvános kulcsú rejtjelezés kulcshármasát is, amelyből a rejtett kulcsfél csak az adott PePy belsejében fordul elő, onnan ki nem olvasható. Lehetőség van egymástól független rejtjelezési csoportok létrehozására (belső fizikai véletlengenerátor segítségével előállított egyedi kulcselem szétosztásával), amelynek tagjai így képesek csak a csoport számára értelmezhetően védeni adataikat. Egy PePy összesen 128 különböző csoporthoz tartozó kulcsot tárolhat.

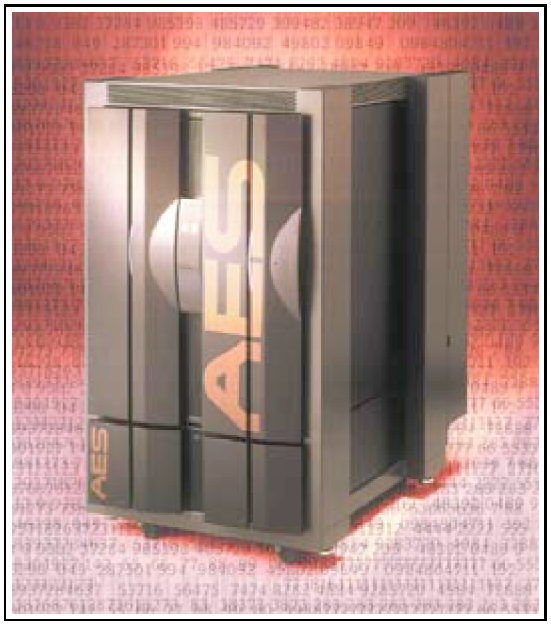
Az eszköz saját időalapja garantálja, hogy a kriptográfiai ellenőrző összeget tartalmazó digitális pecsét egyben hiteles időpecsét is. A nem felejtő memóriában tárolt hamisíthatatlan eseménynapló segítségével bármikor ellenőrizhető a megelőző több mint 2000 esemény bekövetkezésük sorrendjében, annak pontos idejével együtt.

**2001. MÁRCIUS / FÓKUSZ Adatbiztonság / Belga titkosítók Amerikában**

# Belga titkosítók Amerikában

**Hamarosan belga fejlesztésű titkosítási szabvány lép a kiszolgált DES helyébe.**

**Szerzők: Nemetz Tibor és Papp Pál**




Míg az ingó és ingatlan vagyon, a szellemi tulajdon védelmét egy sor törvény, hivatal, hatóság segíti évszázados múlttal, a digitális tulajdon ma még nem jól definiált fogalom. A szellemi tulajdon megjelenési formája viszont egyre inkább digitális. A digitális tulajdon kialakulóban lévő fogalma azonban nem pusztán megjelenési formát takar. Egy előszerződés, egy szándéknyilatkozat maga is jelentős értéket képviselhet, de nem tartozik e három tulajdoni kategória egyikébe sem.

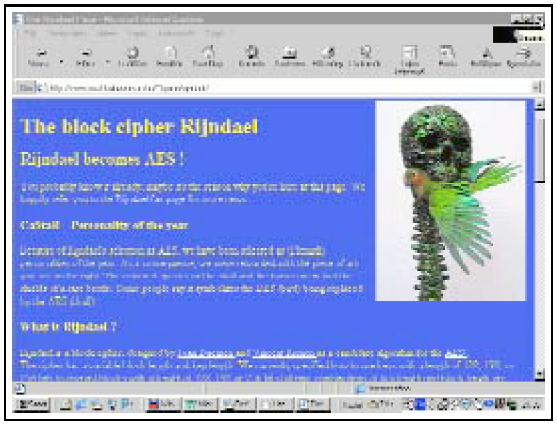
A digitális tulajdon fogalma előbb-utóbb jogilag is elfogadható meghatározást kap; itt és most számunkra ez kevésbé lényeges. Fontosabb az a megjelenési forma, amely megengedi, hogy a digitális tulajdon védelmére biztonságos módszereket alkalmazhassunk. Ezért megkísérlünk operatív meghatározást adni, amely a megjelenési formára

összpontosít. Digitális dokumentumnak nevezzük azt a véges karaktersorozatot, amelynek karakterei meghatározott (előre adott) halmaz elemei. A halmazt az információelméletből kölcsönzött ábécé szóval jelöljük. Ez a meghatározás elegendően általános: az ábécé lehet bináris, állhat bájtokból, nyomtatható karakterekből, írógépekkel leírható jelekből. Ennek megfelelően a digitális tulajdon magában foglalhat értelmes szövegeket, szabadalmakat, (digitalizált) képeket, zeneműveket. A digitális tulajdon védelme legalább olyan fontos, mint más értékeinké. El szeretnénk kerülni, hogy illetéktelenek tekintsenek bele ezekbe a digitális formában megjelenő tulajdonokba és azokban változásokat hozhassanak létre. E feladat megoldására szolgálnak a kriptográfia módszerei.

**Hírszerzők és diplomaták**

A kriptográfiát hagyományosan a diplomáciában, az elhárításban, a hadügyben alkalmazták. A klasszikus alkalmazások két fél üzenetváltásainak titkosságát garantálták. A két fél előre megállapodott egy transzformációban (rejtjelezésben), amelyet a küldendő üzenetre (nyílt szövegre) alkalmaztak, és amely egy összevisszaságnak tűnő (rejtjeles) szöveget eredményezett. A transzformációt a lehető legnagyobb titokban tartották. Ez a titkosítás gondoskodott arról, hogy illetéktelen ne olvashassa el az üzenetet. Ennek a Julius Caesar kora óta ismert módszernek a szépséghibája, hogy az ellenség mindig megtalálta a transzformáció megszerzésének módját.

Olyan megoldásra volt szükség, amely megnehezítette a kódfeltörők életét. Ennek megfelelően nem egy, hanem rengeteg transzformációban állapodtak meg. Ezek a transzformációk az információelméletben használt kódok voltak. A kódokat paraméterezték (mondjuk, sorszámozták), és egy-egy üzenetváltáshoz a felhasználandó kód paraméterében állapodtak meg. Ezt a paramétert az üzenet kulcsának nevezik. A kulcsnak az ellenség számára a legnagyobb bizonytalanságot kellett megjelenítenie, ezért azt az összes lehetséges paraméterérték közül egyenletes eloszlással választják ki. A kiválasztott kulcsot a legszigorúbb módon titokban kell tartani.




Az 1970-es évek elejére egyre többen ismerték fel a rejtjelezésnek a polgári életben betöltendő fontos szerepét. Szükség volt erre két vállalkozás egymással folytatott levelezésében, de a privát dokumentumok archiválásában (akár egy hatóság előli elrejtésében) is. Az üzleti siker szaga töltötte be a levegőt. Elkezdődött olyan kódrendszerek tervezése, elemzése, amelyek a kódhalmaz ismeretében, de a kulcs ismerete nélkül a kor számítástechnikai szintjén nem tűntek megfejthetőnek. Az első biztató eredmények az IBM-hez kötődtek, ahol *Feistel* vezette a kriptográfiai kutatásokat. Kezdetben a kormányok határozottan felléptek a polgári alkalmazások ellen, ám hamarosan be kellett látniuk, hogy a tiltás pusztán szélmalomharc.

Ezért a fejlett országok inkább besegítettek megbízható rejtjelezési algoritmusok előállításába, sőt nemzeti szab-

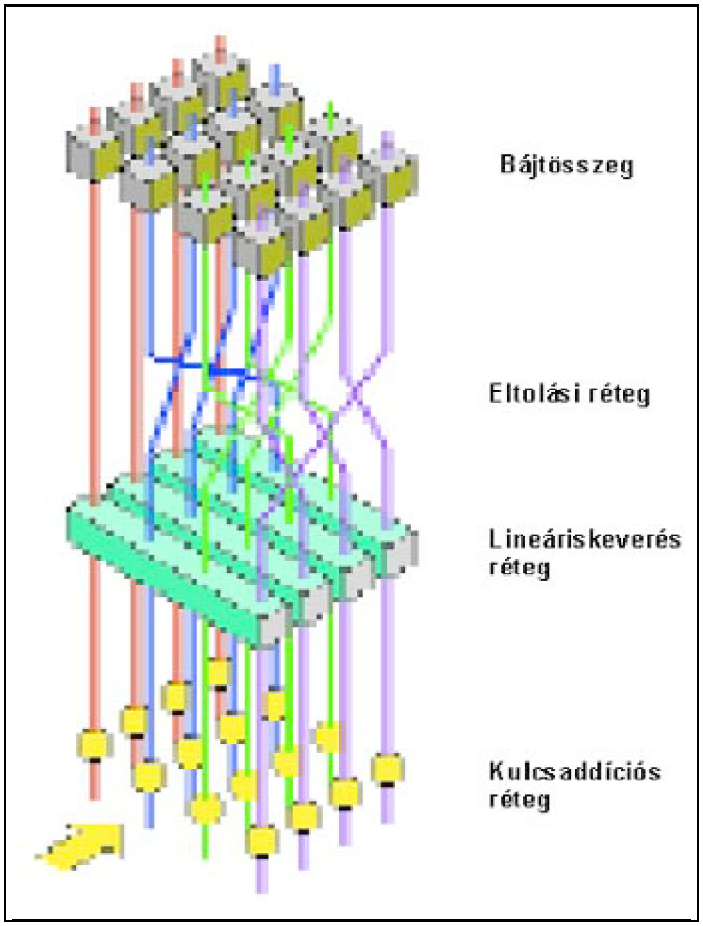
vány elfogadását szorgalmazták. Ebben a folyamatban az Egyesült Államok játszotta a vezető szerepet.

**Data Encryption Standard**

1976 decemberében a National Bureau of Standards bejelentett egy új nemzeti adatfeldolgozási szabványt (FIPS No. 46), amelyben a Data Encryption Standard (DES) rejtjelező algoritmust szabványosították. (Leírása megtalálható az Egyesült Államok szabványgyűjteményében.)

A DES Feistel elképzeléseit továbbfejlesztő blokkos rejtjelezést valósít meg bináris bemeneteli ábécével. A blokkméret 64 bit, ami a 8 bájtos ábécé mellett is blokkos rejtjelezés marad. A nyílt üzeneteket először 64 bites blokkokra bontja (ha az utolsó blokk csonka, akkor azt kiegészíti). Ezeket ugyanazzal a kóddal képezi le szintén 64 bites rejtjeles blokkokba, amelyeket egymás után írva a rejtjeles üzenetekbe a megválasztható kódok száma 256, tehát a kulcsméret nagysága 56 bit.

A blokkon belül a kimenet minden bitje függ a bemenet minden bitjétől. Ezt a „lavinahatást” úgy biztosítja, hogy egyetlen függvényt iteráltan alkalmaz. Az eredeti nyílt szöveg blokkra bontása és az alkalmazott kód kimenetele közbülső rejtjeles blokkot eredményez, amely egyúttal a következő iterációs lépés bemenetele lesz. Az egyetlen iterá-ciós lépésben végrehajtandó műveletek részblokkok közti permutációt, azokon belül helyettesítést alkalmaznak, amiket gyorsan lehetett az akkori technikai szintnek megfelelően végrehajtani. Ez különösen a hardverimplementáció miatt volt rendkívül fontos, hiszen akkor még a fejlesztők sem álmodtak a 64 bites lapkákról.




A szabvány tartalmazta azt a kikötést is, hogy csak hardverimplementált változata használható az Egyesült Államokon belül, és az USA kormányzata megtiltotta a hardveres megoldás vagy 56 bites szoftvermegoldás exportját, viszont elkészült a 40 bites kulcsot használó verzió is, amelynek külföldi használatát előszeretettel engedélyezték. Magát az algoritmust ötévenként biztonsági vizsgálatnak vetették alá. Ez utoljára 1994-ben történt meg, amikor 1998-at jelölték meg a felhasználhatóság utolsó határának. Ennek ellenére kissé módosított változatban ma is általánosan használják. Minthogy a DES algoritmusa korán nyilvánosságra került, bárki készíthetett rá programot. A DES fontos elemként szerepel a nyilvános kulcsú alkalmazásokban. Legutóbbi változatai hazánkban is általánosan elterjedtek.

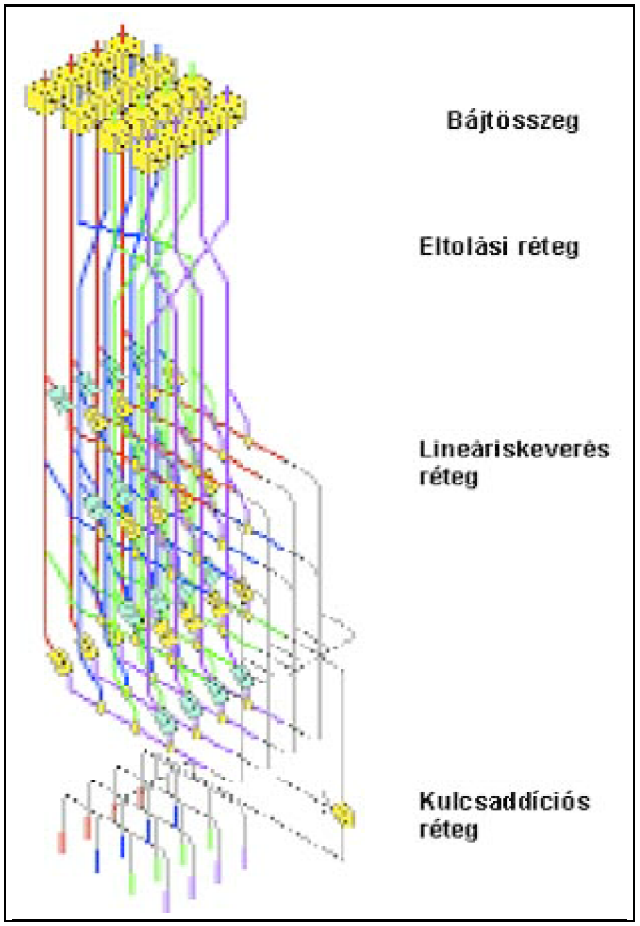
A DES megfejthetőségére utaló publikációk sorát *Martin Hellman* egy 1977-ben tartott előadása nyitotta meg, aki – megfelelő hardverrel – a teljes kipróbálást is kivitelezhetőnek tartotta. Hellman a célgép megépítésének idejét két évre becsülte. Ettől kezdve terjedtek el azok az elképzelések, amelyek szerint az Egyesült Államok rejtjelfejtői meg tudják fejteni a DES-szel rejtjelezett dokumentumokat, ami az alkalmazókat óvatosságra intette. A DES-re *Biham* és *Shamir* munkássága mérte az első súlyos csapást, akik 1993-ban egy újonnan kifejlesztett módszer, a Differential Cryptanalysis segítségével adtak meg fejtési eljárást. 1994-ben *Matsui* egy más típusú, úgynevezett

lineáris kriptanalízis módszert dolgozott ki, amely már tulajdonképpen kivitelezett fejtésről számolt be.

Javításként először a fejtést gyakorlatilag kivitelezhetetlennek beállító eljárást, a DES kétszeres alkalmazását javasolták. Ehhez az üzenetet kétszer kellett egymás után rejtjelezni két, egymástól függetlenül választott kulccsal, ami a kulcs méretét 108 bit hosszúságúvá növelte. Ezzel kapcsolatban Hellman és *Merkle* már 1992-ben nyilvánvalóvá tette, hogy ha a simple DES fejthető, akkor a „Középen találkozunk" elnevezésű módszer igaz a double DES fejtésére is.

A DES jelenlegi legfejlettebb változata a triple DES, azaz a 3-DES. Ez vagy kettő, vagy három 58 bites kulccsal dolgozik. Az üzenetet először az első kulccsal rejtjelezik normál DES módban, majd a második kulccsal a megoldó algoritmust alkalmazzák. Az így nyert közbülső szövegre alkalmazzák ismét az első, háromkulcsos rendszerben a harmadik kulcsot. Ismeretes, hogy több helyen építettek olyan célgépet, amellyel a double DES-t fejteni lehet. Sokan tudni vélik, hogy az Egyesült Államok biztonsági köreiben használnak olyan gépet, amellyel a triple DES is fejthető, bár erről tényleges információ nem áll a nyilvánosság rendelkezésére.

Az exporttilalom miatt számos konkrét processzormegvalósítás van a piacon, és a pénzügyi szféra több nemzetközi szabványában található 3-DES elem. A triple-DES chipek vásárlóinak ajánlatos erősen kritikus szemmel megvizsgálniuk az alkalmazni kívánt megoldást. Az internetről letölthető szoftver alkalmazása a leghatározottabban kerülendő. Mivel az algoritmus publikus, így jogtisztán programozható. Programozás során az időfaktort számos matematikai trükk tudja csökkenteni.




**A XXI. század algoritmusa**

Az elkészült néhány célgéppel szerzett tapasztalatok állítólag azt mutatták, hogy a DES kulcstér teljes kipróbálásához néhány óra elegendő. Közben kimutattak néhány algoritmikus gyengeséget is a DES szerkezetében. Mindezek következtében a National Institute of Standards and Technology (NIST) a DES utódjának kifejlesztésére vonatkozó döntést hozott. Az új algoritmus az Advanced Encryption Standard (AES) nevet kapta.

A NIST döntése alapján az AES algoritmust nyilvános pályázat során választották ki. Ehhez több mint három évvel ezelőtt, 1997 szeptemberében közzétették azon elvárások listáját, amelyeknek az AES algoritmusnak meg kell felelnie. Ugyanakkor deklarálták, hogy a benyújtott rejtjelezési algoritmusok nyilvánosak, szabadon felhasználhatók lesznek. A kiírás szerinti elvárások:

• legyen blokkos algoritmus 128 bites blokkmérettel;

• a 128, 196 és 256 bites kulcsméret egyaránt megválasztható legyen;

• az algoritmus legyen nyilvános, jogdíj nélkül használható;

• álljon ellen valamennyi ismert rejtjelfejtési módszernek;

• legyen világos, logikus szerkezetű, áttekinthető;

• mind a kódolás, mind a dekódolás gyors legyen;

• kevés memóriát foglaljon el;

• többféle processzoron is hatékonyan implementálható legyen.

Az ezeknek az elvárásoknak megfelelő rejtjelezési algoritmus várhatóan hosszú távra, akár 20-25 évre megoldja a polgári életben keletkező adatok biztonságos védelmét. A követelmények erőssége miatt kérdéses, maga az állam képes lesz-e arra, hogy a kulcsok megszerzése nélkül hozzájusson a közlemények információtartalmához.

A beérkezett pályaművek közül tizenöt felelt meg a formai elvárásoknak. A benyújtott algoritmusok mögött komoly multinacionális cégek sorakoznak fel (IBM, Microsoft, RSA Laboratories, Deutsche Telekom AG, Nippon Telegraph and Telephone Corporation, Centre National pour la Recherche Scientifique stb.). Ezek elemzése a legszélesebb nyilvánosság bevonásával folyt. Maguk a szerzők és más kriptográfusok is elemezték az algoritmusokat, s több, kifejezetten e témának szentelt konferenciát is tartottak.

A NIST 1999. március 22–23. között Rómában rendezte meg a második szakértői konferenciát a tizenöt pályamű értékelésére. E tanácskozás megrendezésének célja az volt, hogy az elhangzott értékelések segítséget nyújtsanak annak az öt algoritmusnak a kiválasztásához, amelyek továbbra is versenyben maradnak.

Az öt kiválasztott ábécésorrendben:

• Mars algoritmus. Szerzői: az IBM több mint tízfős csapata (USA).

• RC6 algoritmus. Szerzői: *Ron Rivest* és csapata (RSA Laboratories, USA).

• Rijndael algoritmus. Szerzői: *Daemen, Rijmen* kriptográfusok (Belgium).

• Serpent algoritmus. Szerzői: *Anderson, Biham, Knudsen* (nemzetközi csapat).

• Twofish algoritmus. Szerzői: *Bruce Schneier* és csapata (USA).

Az IBM csapatát olyan, a DES előkészítésében is jelentős szerepet játszó kriptográfusok alkották, mint Ron Rivest (aki az RSA-ban az R betű), Biham, aki a DES differenciálanalízis megfejtési módszerének egyik kidolgozója és Schneier, aki két évvel ezelőtt a DAK konferencián nagy érdeklődéssel fogadott előadást tartott.

Az algoritmusok elemzése rendkívül nagy erőket kötött le. A viszonylag rövid, kétéves vizsgálati idő ellenére állítható, hogy a DES után ez az öt a világ legmélyebben elemzett algoritmusa. A győztes algoritmust 2000. október 2-án jelentették be. A versenyt a Rijndael algoritmus nyerte. Szerkezete nem hagyományos, nem követi a DES Feistel-struktúráját. Ez is számos iterációs lépésben valósul meg. Minden iteráció három rétegből áll, ezek szerepe különböző.

• Lineáriskeverés réteg;

• nemlineáris réteg;

• kulcsaddíciós réteg.

Az algoritmus több érdekes technikát alkalmaz (például bájt szintű operációk a 256 elemű véges test fölött).

Érdekességként megemlítjük, hogy a szerzők több nyilvános előadásban tippelték meg a győztest, bejelentve, hogy a rejtjelezés programját a nyilvánosságra hozás napján piacra

fogják dobni. Bár optimalizált programjaik elkészültek, nem találtak piacot. A Rijndael algoritmus egyszerű, világos, bármely programozási nyelven gyorsan programozható. Az internetről számos változat tölthető le, jóllehet ezt a megoldást senkinek nem ajánljuk.

A győztes kihirdetése nem jelenti azt, hogy automatikusan ez lesz az új amerikai szabvány. Át kell mennie egy sor formalizmuson, ami akár egy teljes évet igénybe vehet. A nyilvános kulcsú infrastruktúrában várhatóan folyamatosan bevezetik mint opcionális elemet, de igazi alkalmazása csak az április–június között várható szabványba iktatás után várható. Nem kell tehát a 3-DES-t használóknak kétségbeesett sebességgel lecserélniük algoritmusukat. A nyilvános kulcsú kriptográfia kulcscseremód-szereivel két levelező fél kicserélheti az AES kulcsát, így az AES rejtjelezési algoritmus előzetes egyeztetés nélkül is használható titkos üzenetváltásra.

*Nemetz Tibor adatbiztonsági szakértő, a matematikatudomány doktora* ***(nemetz @dbassoc.hu),*** *Papp Pál matematikus, informatikai biztonsági szakértő (papp@cryptor.hu).*

**HOL TALÁLHATÓ?**

Az AES-jelöltekről bővebb leírás található a *www.nist.gov/aes* címen.

A NIST címe: *www.ta.nist.gov.*

**Joan Daemen és csapata:** *joan.daemen@protonworld.com.*

Vincent Rijmen: *vincent.rijmen@esat.kuleuven.ac.be.*

A DES és a triple DES leírása: *http://csrc.nist.gov/fips/fips46-3.pdf.*



## Meddig él egy titkosítás?

Egyelőre senki nem merne fogadásokat kötni arra, meddig tölti majd be kijelölt szerepét az AES. Az azonban biztosnak tűnik, hogy ez idő alatt nemigen fogják feltörni. A kilencvenes években készült speciális DES kulcstörő gépekkel néhány óra alatt sikerült megállapítani, milyen kulccsal kódolták az üzenetet. Feltételezve, hogy létezne olyan berendezés, amellyel a DES kulcsot egy másodperc alatt fel lehetne törni (azaz képes volna 255 kulcsot kipróbálni másodpercenként), ugyanennek a gépnek mintegy 149 ezermilliárd (149 trillió) évre volna szüksége a 128 bites AES kulcs feltöréséhez. Összehasonlításul: a világegyetem becsült életkora kevesebb mint húszmilliárd év.



## A kályhától az auditig

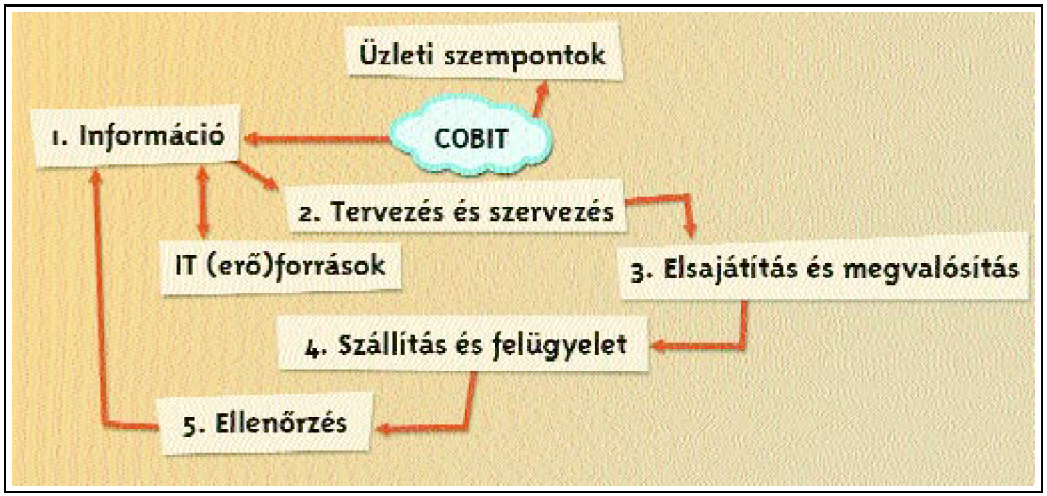
**Egyre nagyobb pénz forog a vírusirtók, tűzfalak és egyéb, jó PR-körítésű termékek piacán, a hazai cégek mégsem léptek nagyot a védelemben.**

**Szerző: Kincses Zoltán**

Amikor új dolgozó lép be a céghez, az Informatikai Biztonsági Szabályzat alapján ismerheti meg informatikai mozgásterét, amikor pedig visszaélést követ el, ennek alapján felelősségre lehet vonni, hiszen aláírta: betartja a szabályzatot az abban foglalt megszegéseket követő felelősségre vonással és ezek következményeivel együtt. Amennyiben a kockázatfelmérésben szereplő kedvezőtlen esemény fordul elő, amely érinti a vállalat informatikai működését, a szabályzat „Katasztrófaterv" részében leírtak alapján lehet egységesen cselekedni. Katasztrófatervet nyugodt körülmények között kell írni, hogy szükséghelyzetben lévő, fásult emberek is tudjanak dolgozni belőle, így a kár végösszegében a pánik része lesz a legkisebb.

Persze a szabályzatot nem elég egyszer megírni, majd hátradőlni, mint ahogyan az egyszer megvásárolt vírusölő sem fog örökké megvédeni, és a telepítés után magára hagyott tűzfal sem jelent mást, mint hamis biztonságot. A legnagyobb biztonsági probléma a hamis biztonságérzet, hiszen ebben az állapotban a figyelem is lankad, így a támadó könnyebben kihasználhatja a hibákat. Hiba pedig minden rendszerben van, nincs tökéletes biztonság. Ezt – Gödel idevonatkozó tételéből kiindulva – lehet tudományos módszerekkel bizonyítani, de talán az is elegendő, ha szemügyre vesszük a biztonsági réseket felfedő levelezőlisták napi adagjait.

A biztonság tudatos kockázatvállalás. A tudatosság azon alapszik, hogy a leírt szabályzat kitér-e minden részletre, és nem hagy rést, amit ne szabályozott volna akár a kezdetektől, akár a működés során tapasztaltak alapján a szabályzat felülvizsgálatakor. Itt kell megemlíteni az ISO 9002 minőségbiztosítás jelentőségét, amely többek között a dokumentumkezeléshez ad megfelelő keretet és fegyelmet.




A cég folyamatábrája és a COBIT szerepe

**ILLUSZTRÁCIÓ: BUTTINGER GERGELY**

A kockázatvállalás annak felmérése, milyen veszélyforrások mekkora károkat okozhatnak, és ennek megfelelően mely intézkedésekkel minimalizálható ez a kockázat. Lehet az irodai számítógép távol-keleti sorozattermék és elviselhető az operációs rendszer kék halál néven ismert tulajdonsága (a szín állítható a registryben). Ám az már mindenkiben kétségeket ébreszt, ha egy bankkártya-tranzakciókat százmilliós értékekben feldolgozó cég csak *közel* százszázalékos biztonságot szavatoló rendszerrel dolgozik.

**Keretrendszerek**

Mielőtt a szabályzat(ok) elkészítésébe fognánk, át kell tekinteni, milyen módszerrel lehet a céget úgy feltérképezni, hogy az egyes konkrét feladatokat a keretrendszerbe illeszthessük. Miután mindennek megvan a helye, kezdődhet a szabályzatlista, majd a szabályzatok elkészítése.

Két, szélesebb körben ismert keretrendszer, az ISACA nevű szervezet *(www .isaca.org)* által kezelt CISA (Certified Information Systems Auditor) minősítést adó COBIT (Common Objectives for Information and Related Technology), illetve az ISC$^2$ *(www.isc2.org)* által kezelt CISSP (Certified Information Systems Security Professionals) és SSCP (Systems Security Certified Practitioner) címeket adó tanok közül választhatunk. Az előbbi szélesebb elméleti alapon, míg az utóbbi mélyebb gyakorlati úton közelíti meg az informatikai biztonságot és az auditálást. Mindkét szervezet vizsga keretében méri föl a jelentkezőket, akik a későbbiek során is minden évben megküzdenek a vizsgán megszerzett minősítés megtartásáért. A megadott címeken rengeteg információ érhető el, így most csak rövid minta keretében ismerjük meg a COBIT logikáját, amelyet minden cég alkalmazhat magára.

**COBIT**

A háromdimenziós modell a következőképp állítja fel keretrendszerét: *X tengely* – IT eljárások: tartományok – eljárások – tevékenységek; *Y tengely* – IT források: emberek – alkalmazói rendszerek – technológia – lehetőségek – adat; *Z tengely* – Információkövetelmények: minőség – megbízhatóság – biztonság. Ezek alapján az IT erőforrások és az üzleti szempontok szerinti kör (lásd az ábrán) járható be a cég működési felépítésében. A számozott lépések a tartományok, ezeken belül vannak az eljárások, amelyek a konkrét tevékenységek által fedik le az adott területet. Az IT (erő)források elemei: humán erőforrás, alkalmazási rendszerelemek, technológia, lehetőségek/tartalékok, adatok. Terjedelmi korlátok miatt itt nem soroljuk fel az egyes elemeknél figyelembe veendő tényezőket.

**Információ**

Az információ garantálja a feldolgozás hatékonyságát, és minél kevesebb olyan elem legyen benne, amely az entrópiát növeli – például az információ értékét „hígítják” a nullával feltöltött sorok ott, ahol ráadásul ez nem is muszáj.

A feldolgozáshoz szükséges információ legyen teljes, és ne hiányozzon olyan eleme, amely a feldolgozást vagy annak eredményét befolyásolja – például számadatok oszlop- és sornevek nélkül.

Az információ nem kerülhet illetéktelen kezébe – például nem olvasta el kívülálló személy.

Az elemek nem lehetnek sérültek – például az információt senki nem módosította egyetlen részében sem.

A megfelelő információ legyen elérhető – például hiába kaptam egy fájlt, ha jelszavas tömörítéssel látták el és a jelszó nem ismert.

A feldolgozáshoz és a cél eléréséhez legyen megfelelő az információ – például egy digitális aláírás ellenőrzéséhez az aláíró nyilvános kulcsával kell rendelkezni.

Az információban meg lehet bízni akár tartalmát, akár jótállóját vagy éppen forrását tekintve – például a forrás elismert (nem bulvárlap írta, hanem egy hírszolgálat adta ki), az aláíró személye megbízható, az információ tartalma nem ad okot komolyabb kételkedésre.

**Tervezés és szervezés**

Meg kell határozni a cég rövid (egyéves) és/vagy hosszabb távú (hároméves) informatikai stratégiai tervét. Ez tartalmazza az üzleti terv teljesítéséhez szükséges informatikai stratégiát, de kitérhet a részletekre is – főként a rövidebb távú tervben (például milyen hardver- és szoftvereszközök vásárlása szerepel a megindokolt beszerzések listáján).

Az IT architektúra az üzleti célokat kielégítő optimális összetételű legyen – ideértve például az adatszerkezeteket is.

Figyelembe véve a technológiai fejlődést annak alapján kell kialakítani az alkalmazott infrastruktúrát.

Az informatikai szervezetek egyes részlegeinek feladatait és felelősségét szervezzük meg, lehetőleg átfedés- és résmentesen.

Az informatikai igényeket és az anyagi lehetőségeket közelítsük egymáshoz.

Fontos, hogy az alkalmazottak ismerjék a cég céljait és azt az irányt, amelyet követve el akarják érni e célokat.

Az informatikai eljárásokhoz nélkülözhetetlen a legmegfelelőbb személyek kiválasztása, képzése, ellenőrzése (beszámoló, vizsga).

Garantálni kell a jogi, a szabályzati (szabványos) és a szerződéses követelményeknek való megfelelést.

Szavatolni kell az informatikai rendszer teljesítményét és választ kell adni az informatikai szolgáltatások ellátását veszélyeztető tényezőkre.

Az egyes terveket a megfelelő módon idő- és költségkeretben kell tartani, de figyelembe veendő például a felhasználók bevonása, a minőségbiztosítás vagy éppen a felelősségek meghatározása az egyes részfeladatoknál.

A minőségbiztosítás szabványainak és rendszereinek tervezésén kívül azokat alkalmazni és fenntartani is kell.

**Elsajátítás és megvalósítás**

A megoldások azonosítása az alternatív lehetőségek vizsgálatán alapul, és figyelembe veszi többek között az olyan paramétereket, mint a költséghatékony biztonság, a felhasználók követelményei vagy az informatikai elvárások meghatározása.

Alkalmazói szoftverek beszerzésénél és fenntartásánál minden kompatibilitási, teszt- és felhasználói követelményt figyelembe kell venni.

A technológiai architektúrák beszerzése és fenntartása történjen az üzleti alkalmazások kiszolgálásának megfelelően.

Informatikai eljárások fejlesztésénél és fenntartásánál garantálnunk kell a bevezetett alkalmazások és technológiai megoldások szakszerű felhasználását.

Rendszerek telepítésekor és felruházásakor ellenőrizni kell, hogy a megoldás megfelel-e a szándéknak.

Csökkentsük a minimálisra a megszakítás, a jogosulatlan módosítás vagy a hiba előfordulásának valószínűségét.

**Szállítás és felügyelet**

Érthetően, egységesen fogalmazzuk meg a mennyiségi és a minőségi paramétereket.

Harmadik fél szolgáltatásainak menedzselésénél a szerepek és a felelősségek érthetően meghatározottak, az elvárások folyamatosan kielégíthetőek.

Teljesítmény és képesség menedzselésénél garantáljuk a szükséges mértéket.

Az informatikai rendszer szolgáltatásainál garantáljuk a folyamatosságot, kiesés esetén a lehető legrövidebb időn belül álljunk vissza a legkisebb üzleti hatással.

Gondoskodjunk az információk védelméről a jogosulatlan felhasználás, a felfedés, a módosítás, a sérülés vagy az elvesztés ellen.

Elengedhetetlen a szolgáltatások megfelelő árpolitikájának kialakítása.

A felhasználók oktatásával és képzésével elérhetjük a felhasználók hatékony, tudatos és felelős munkáját.

Tartsunk fenn vevőszolgálatot és tanácsadást a felmerülő problémák mielőbbi megoldására.

Fizikailag tartsuk nyilván az informatikai rendszert (hely, darab stb.).

Problémák és balesetek esetén a mielőbbi megoldáson kívül az újbóli előfordulás elleni intézkedések meghozatala is idetartozik.

Garantáljuk az adat teljességét, pontosságát és érvényességét a bevitel, a frissítés és a tárolás ideje alatt.

Alakítsunk ki olyan fizikai környezetet, amely megvédi az emberi és rendszererőforrásokat a kézi és természeti kockázatoktól.

A fontos informatikai támogatási feladatokat a kellő rendszerességgel és rendezettséggel hajtsuk végre.

**Ellenőrzés**

Fordítsunk figyelmet annak vizsgálatára, hogy az alkalmazott rendszer teljesítménye megfelelő-e.

Gondoskodjunk arról, hogy az informatikai eljárásokkal szemben állított belső kontrollok teljesítménye mindig megfelelő legyen.

Erősítsük a bizalmat és a megbízhatóságot a cég/szervezet, a vevők és a külső (harmadik) partnerek között.

Gondoskodjunk független auditról a bizalmi szintek és a legjobb gyakorlati tanácsokból származó előnyök növelésére.

És a kör bezárultával új kör veszi kezdetét… Egyre több auditor rendelkezik CISA minősítéssel, így az audit esetén már az is előnyt jelent, ha a COBIT alapján épülnek fel a szükséges dokumentációk és a működési szemléletek. A drága auditot nem kérő cégeknek sem árt ilyen rendszer alapján felmérni a vállalatot és folyamataikat. Amikor a felmérés és a szabályzatok kialakítása már megtörtént, jöhet a megfelelő termékek és eszközök keresése. Ahogy a biztonságtechnika egyik legnevesebb szakembere, *Bruce Schneier (www.conterpane.com)* havi hírlevelében írta: „A biztonság nem termék, hanem eljárás.”

Kincses Zoltán az ELTE TTK doktorandusz hallgatója. E-mail: **secureco@telnet.hu.**

**2001. MÁRCIUS / FÓKUSZ Adatbiztonság / Láthatatlan tüskék**

# Láthatatlan tüskék

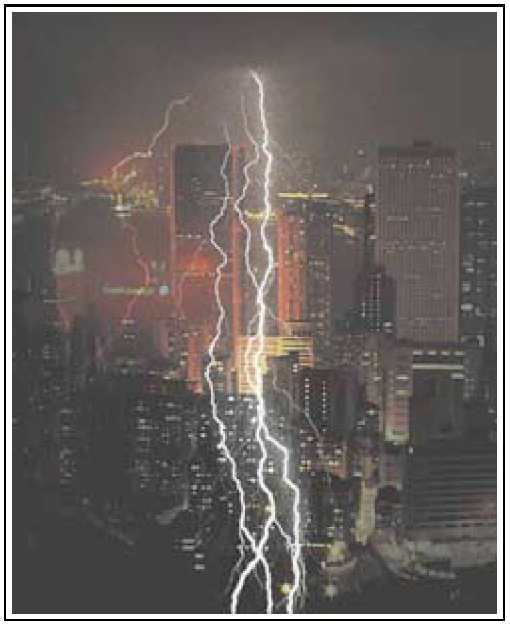
**A feszültségvédelem a számítógépek és hálózati rendszerek iztonságának első védelmi vonala.**

**Szerző: Kelenhegyi Péter**

Állítólag kétféle számítógépes hálózat létezik: az egyik, amelyik meghibásodott már és veszített el adatokat feszültségproblémák miatt, a másik, amelyik csak fog. A Contingency Planning Research szerint a tápellátási zavarok és feszültségtüskék okozzák az adatvesztések 45,3 százalékát és az ezzel összefüggő hardverhibákat az újraindításhoz szükséges és állási idővel együtt. Ma már minden felelősségteljes rendszergazda készít biztonsági másolatot a fontos adatokról, azt azonban még mindig sokan figyelmen kívül hagyják, hogy tápellátás nélkül nem működnek a számítógépek; hiába van mentés, az adatok mégsem érhetők el.

A pillanatnyi feszültségingadozás is jelentős károkat okozhat. Egy, az IBM által készített tanulmány szerint egy átlagos számítógép havonta több mint 120-szor van kitéve feszültségingadozásnak, amelyek hatása a billentyűzet lefagyásától kezdve az alacsony hardverteljesítményen át egészen a berendezések súlyos károsodásáig és visszaállíthatatlan, sérült állományok keletkezéséig terjedhet.

A fogyasztói energiahálózat nem gondoskodik az érzékeny számítógépek által megkövetelt, káros ingadozásoktól mentes feszültségről, miközben végső soron a vásárló a felelős saját eszközeinek biztonságos és hibátlan működéséért. A Gallup intézet felmérése szerint a megkérdezett vállalatok több mint fele óránkénti 5000 dollárra vagy annál is többre becsüli a gépek leállásából származó károkat.



Hálózati környezetben a – sokszor más-más telephelyen található – berendezések áramellátási zavarainak káros hatása az egész rendszerre kiterjedhet. A hálózati gerinc egyetlen kritikus elemét érintő feszültségesés vagy feszültségtüske észrevétlenül megrongálja az érzékeny alkatrészt, és nemcsak a hálózati forgalmat szakítja meg, de a hiba megkeresése ráadásul értékes időt rabolhat el a rendszergazdától.

A kritikus rendszerek folyamatos, jó minőségű tápellátását nyújtó szünetmentes tápegységek feladata a poten-ciálisan ártalmas elektromos zajok, feszültséghullámok és tüskék kiszűrése, mielőtt azok kárt tehetnének a csatlakoztatott berendezésekben. Használatuk nemcsak a nagyszámítógépek, hanem a kiszolgálók, hálózati perifériák (tárolóeszközök, szalagos egységek, hubok, kapcsolók, útválasztók) és sok PC-s munkaállomás mellett is elengedhetetlenné vált. Jellemzőik:

• egyszerű, automatikus („plug-and-play”) telepítés;

• az üzem közben cserélhető akkumulátorok minimalizálják a szerelési igényt és maximalizálják a működési időt;

• a tápellátás-felügyeleti szoftver probléma esetén figyelmezteti a felhasználókat vagy automatikusan menti a használatban lévő adatokat;

• a moduláris kiépítéssel megoldható a tápellátás-kapacitás szükség szerinti növelése.

**Hálózati tápellátás**

A tápellátási problémák káros hatásai bármilyen fajta hálózatot érinthetnek. A feszültségvédelmi stratégia kialakításakor azonban a hálózat mérete az elsődleges szempont.

**Kis munkacsoportok.** A kisvállalkozásoknál és több telephelyes vállalatoknál a hálózatok általában húsznál kevesebb, egyenrangú (peer-to-peer) csomópontból állnak, nem tartoznak hozzájuk sem dedikált kiszolgálók, sem összetett felügyeleti rendszerek. Ezeknél az egyes számítógépeken tárolt adatok értéke és az állási időből eredő veszteségek felhasználókra vetített összege alapján határozhatók meg a feszültségvédelmi igények.

A tápellátási igények meghatározásakor figyelembe kell venni, mekkora veszteséget okoz a közösen használt perifériák elérhetetlenségéből vagy meghibásodásából fakadó termeléskiesés. Egy alapszintű asztali UPS mindössze 5-10 százalékkal növeli egy új PC beszerzési árát, ugyanakkor megduplázhatja annak rendelkezésre állási idejét. A kevésbé kritikus eszközök érzékeny hardverelemeit jó minőségű, feszültségingadozás ellen védő csatlakozó (surge suppressor) ennél is gazdaságosabban meg tudja védeni a veszélyes feszültséghullámoktól és -tüskéktől – az áramkimaradástól, a feszültségeséstől és a túlfeszültségtől azonban nem.

**Kisméretű, kiszolgálóra épülő helyi hálózatok.** A 250-nél kevesebb csomópontból álló, kisméretű helyi hálózatok (LAN-ok) sokféle vállalati igényt elégítenek ki: betölthetik egy kisvállalat teljes hálózatának vagy akár a nagyvállalati környezet egyik távoli telephelyi hálózatának szerepét. Ezek a hálózatok nemcsak a kiszolgálótól és a fontos adatok tárolását és a felügyeletet végző munkaállomásoktól függnek, hanem a hálózaton keresztüli információáramlást garantáló tárolóeszközöktől és huboktól is. Ha ezek közül bármelyik meghibásodik vagy leáll, a felhasználók sem elérni, sem a szerverre menteni nem tudják az adataikat, ami végső soron adatvesztést, vagy ami még rosszabb, sérült állományokat és adatbázisokat eredményez.

Az akkumulátoros háttér biztosítása és a túlfeszültség elleni védelem mellett az ilyen hálózatokhoz tervezett UPS-ek további biztonsági funkciókat nyújtanak. Ahol több száz felhasználó termelékenysége forog kockán, ott hatékony feszültségszabályozási megoldásról, többféle működés közben végrehajtható funkcióról, valamint a rendszer távoli ellenőrzését és irányítását kínáló tápellátás-felügyeletről kell gondoskodni. A felügyeleti szoftvernek képesnek kell lennie arra, hogy a feszültségproblémákról személyhívón értesítse a rendszergazdát, illetve hogy hosszabb áramszünet esetén automatikusan és biztonságosan leállítsa a számítógépeket.

**Közepes méretű helyi hálózatok.** A 250–1000 csomópontból álló LAN-ok felügyeleti rendszere összetettebb, gyakorta különféle operációs rendszereket futtató kiszolgálókat tartalmaznak, amelyekhez bonyolult tárolórendszerek – például redundáns lemezalrendszerek (RAID-ok) – csatlakoznak. A különböző hálózati zónák közötti kommunikációról a hubok és a kapcsolók mellett útválasztók és hidak gondoskodnak. A felhasználók munkája itt is a kiszolgálók – bármelyik szerverre jelentkeznek is be –, a hozzájuk

csatlakoztatott tárolóeszközök a munkaállomást a kiszolgálóval összekötő hálózati eszköz zökkenőmentes működésétől függ.

Az ekkora hálózatok védelmét ellátó UPS-ektől a rendszergazdák gyakran elvárják, hogy azokat a könyebb telepítés érdekében keretbe lehessen szerelni. Emellett biztosnak kell lenniük abban, hogy a tápellátás-felügyeleti szoftver több kiszolgálóval és az általuk futtatott bármelyik operációs rendszerrel képes kommunikálni. A webes felügyeleti eszközök szintén egyre hasznosabbnak bizonyulnak a platformfüggetlen ellenőrzés és jelentéskészítés elősegítése terén.

**Vállalati hálózatok.** Valójában nincsenek méretbeli korlátjai a vállalati hálózatoknak, de általában úgy definiálják azokat, hogy egy adatközpont működésének részét képező vállalati szervereket és nagygépeket tartalmaznak. Emellett többnyire SNMP útján folyik a hálózati elemek adminisztrálása, és összetett hálózati felügyeleti rendszereket tartalmaz.

A vállalati hálózatok feszültségvédelme bizonyos értelemben egyszerűbben megoldható, hiszen itt a kritikus adatok legnagyobb részét egyetlen helyen, például egy adatközpontban tárolják, ahol nagy UPS-ek védik a processzorokat, a tárolóeszközöket, a legfontosabb perifériákat vagy az egész helyiséget. Ahogy egyre több lesz az ügyfél–kiszolgáló típusú alkalmazás, a vállalati kommunikációt elősegítő hálózati és telekommunikációs eszközök feszültségvédelméről is gondoskodni kell. A kiegészítő funkciók segítségével meghatározható, az eszközök hány százalékos rendelkezésre állására van szükség.

A nagyvállalatok feszültségvédelmét ellátó UPS-ek e képességeken kívül a következő, kifejezetten nagyvállalati igényeket kielégítő tulajdonságokkal rendelkeznek:

• redundáns, a hibalehetőséget kiküszöbölő funkciók;

• a felhasználó által egyszerűen cserélhető moduláris alkatrészek (például akkumulátorok) csökkentik a szerelési időt;

• a rendszer növekvő igényeinek megfelelően növelhető akkumulátoros védelmi idő.

Ilyen nagy hálózatok esetén általában a felügyeleti igények is összetettebbek, ezért hát olyan szünetmentes tápegységet kell választani, amelynek szoftvere együtt tud működni a vállalat felügyeleti alkalmazásaival.

**Hogyan válasszunk?**

A rossz feszültségviszonyok az informatikai és távközlési eszközökben egyaránt kárt okozhatnak, s bár a problémák többsége – így a feszültséghullámok és -esések – észrevétlen marad, mégis gyorsítja a készülék elhasználódását. Az UPS kiválasztásakor több szempontot kell figyelembe venni.

• **Áthidalási idő hossza.** Az áramkimaradások általában nem tartanak tovább néhány percnél, mégis minden helyzetet egyedileg kell értékelni. A hálózati rendszergazdának általában legalább 5-10 perc akkumulátoros áthidalásra van szüksége ahhoz, hogy kézzel vagy tápellátás-felügyeleti szoftverrel automatikusan leállíthassa a rendszert. Más elektronikus berendezések esetén mások az igények, attól függően, hogy a felhasználók szempontjából mennyire fontos folyamatos működésük.

• **A tápellátás távoli ellenőrzése és irányítása.** A tápellátás-felügyeleti szoftver beépített biztonsági funkciói segítségével távolról is megtehetjük ezt, akár egy kiszolgálón vagy egy PC-n, akár a weben keresztül.

• **Védendő eszközök összesítése.** Minden olyan eszközt vegyünk számba, amely létfontosságú adatokat tárol vagy kritikus műveleteket hajt végre, beleértve az összes biztonsági berendezést, a monitorokat és az alapvető információt hordozó hálózati hardvert.

• **Kategorizálás.** A nagyobb UPS-gyártók aszerint kategorizálják UPS-eiket, hogy azokat milyen számítógépes eszköz – asztali, hálózati, vállalati – védelmére tervezték. Nagyobb hálózatok vagy összetettebb konfigurációk esetén meg kell határoznunk azok összes tápellátásigényét.

• **Teljesítmény.** Minden elektronikus eszköz virtuális címkéjéről leolvasható annak bemenetifeszültség- és tápigénye voltamperben (VA), amperben (A) vagy wattban (W). Mivel az UPS-eket általában VA-ben rangsoroljuk, szorozzuk össze a feszültségértéket az amperekkel, hogy megkapjuk a voltamper értékét. Ha csak a wattszám van megadva, szorozzuk meg 1,4-del.

• **Összesítés.** Adjuk össze eszközeink voltamperigényét. Olyan UPS-t válasszunk, amelynek VA-kapacitása legalább akkora, mint a teljes rendszer igénye. Ha a jövőben növelni kívánjuk rendszerünket, érdemes lehet már most nagyobb kapacitású UPS-t beszerezni.

Végül – ha az összes kritikus eszköz egy helyen található – érdemes őket egyetlen nagyobb UPS-hez csatlakoztatni. Amennyiben az eszközök különböző helyeken vannak, általában gazdaságosabb néhány kisebb UPS-t beszerezni.

Kelenhegyi Péter a BYTE Magyarország főszerkesztője.

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

**HOL TALÁLHATÓ?**

BPS Kft.

ww.bps.hu

Interware Kft.

ww.interware.hu

Traco Rt.

ww.traco.hu

MGE UPS Systems Hungary Kft.

Tel.: 204-3033

**2001. MÁRCIUS / FÓKUSZ Adatbiztonság / Pannon-védelem**

## Pannon-védelem

Eleinte főként a vidéki területi képviseletek védelmére használt UPS-eket a Pannon GSM. Ezek az irodák rendszerint a városközpontokban, régi épületekben kaptak helyet, amelyekben elavult, megbízhatatlan az elektromos hálózat. A környező fogyasztóktól származó elektromos zavarokat rosszul tűrték az erre érzékeny átviteltechnikai berendezések, ezért a cégnek mindenképpen fejlett funkciókkal rendelkező (szinuszos bemenetű, online rendszerű), ám viszonylag kis teljesítményű UPS-ekre volt szüksége. A mobilszolgáltatónál különleges UPS-eket igényelnek a 48 voltos áramról működő GSM távközlési eszközök. A GSM rendszert felügyelő informatika és a cég működéséről gondoskodó szerverrendszerek, a munkaállomások és az irodai eszközök viszont már hagyományos szünetmentes tápegységekről működnek.

mikor a vállalat központja új épületbe költözött, szükségessé vált a szerverterem UPS-ének lecserélése is. „Nagy hangsúlyt fektettünk az elektronikai jellemzőkre, a zavarérzékenységre, az átkapcsolási időkre, a tranziensekre, arra, hogy mennyire bírja a nemlineáris terhelést – fejtegette Szigeti György, a Pannon GSM rendszermérnöke, aki szerint a távközlési szektor erős versenyhelyzete is arra kényszeríti a céget, hogy minden lehetséges eszközzel védekezzen az üzemszünet ellen.

A mobilpiac azonban olyan gyorsan növekszik, hogy nehéz előre becsülni az igényeket. Az előfizetők számának emelkedésével párhuzamosan nő a vállalatnál működő

informatikai rendszerek száma és teljesítménye, így folyamatosan ehhez kell igazítani az UPS-ek teljesítményét is. Először egy darab APC Silcon DP340 készüléket vásárolt a cég a gépterembe, majd egy második üzembe állításával redundánssá tették a rendszert. Az igények növekedésével lecserélték azokat két (majd három), szintén sorba kapcsolt DP380E-re, a felszabadult berendezéseket pedig az épület (munkaállomások, nyomtatók, faxok) védelmére használták fel. Ez év elején viszont már kétszer három darab DP380E látja el a géptermek védelmét, két DP360E az egyik épületet, az eredeti DP340-ek pedig egy új, kisebb épületet szolgálnak ki.

**K. P.**

**2001. MÁRCIUS / FÓKUSZ Adatbiztonság / ISP városnyi energiával**

## ISP városnyi energiával

Redundáns üzemű, 2×300 kVA-es szünetmentes tápegységet telepített az RTL Klub székházában az MGE UPS Systems. A Galaxy típusú, felharmonikus szűrésű áramforrások több mint 94 százalékos hatékonysággal működnek. Szintén az MGE rendszereit alkalmazta magyarországi központjában a City-Reach International: 16×400 kVA teljesítmény, A+B redundáns felépítés, 15 perces független üzem, az épületfelügyeleti rendszerrel és a generátorokkal való együttműködés jellemzi a 3+1 paralel konfigurációt. Összehasonlításul: 6,4 MVA egy 30 000 lakosú város teljes lakossági energiaellátását is fedezné.

**2001. MÁRCIUS / FÓKUSZ Adatbiztonság / Powerware az Interware-nél**

## Powerware az Interware-nél

Fennakadásoktól mentes internetszolgáltatás nélkül az internetezőkért folyó versenyben minden ISP kudarcra van ítélve. Az Interware Kft., amely 1997 végén kezdte teljes körű internetszolgáltatását Budapesten, mára több ezer előfizetővel és országos hálózattal rendelkezik. A cég a kapcsolt és bérelt vonali szolgáltatáson kívül – a komplexebb megoldásokat igénylő vállalkozások részére – ASP és kolokációs szolgáltatásokat fejlesztett ki, amelyek egyre fontosabb szerepet töltenek be kínálatában. Ezek folyamatos működését szolgálja a Budapest Internet Exchange-dzsel egy épületben található adatközpont, amelyben az ország összes jelentős távközlési szolgáltatója optikai hálózattal van jelen, illetve a cég Victor Hugo utcai központjába telepített 2×250 kVA kapacitású, redundáns, háromfázisú, kettős konverziójú tápegység. Mint Benyó Zoltán műszaki igazgató elmondta, az Interware teljes körűen redundáns kiépítést, kettős tápellátást, tökéletes és állandó kimenő elektromos paraméterek mellett is gazdaságos működést választott, miután korábbi tápellátási rendszerét minden szempontból kinőtte. Az erősáramú rendszer és a gépterem korszerűsítését magában foglaló projekt generálkivitelezője a Traco Rt. volt, a Powerware tápegységeket a BPS Kft. munkatársai állították üzembe. A szünetmentes táprendszer az internetszolgáltatáshoz szükséges szervereket és hálózati eszközöket, valamint az ügyfelek szervereit védi. A teljes rendszert a Powerware Powervision monitoring szoftvere felügyeli, az informatikai hálózatot pedig az Onlinet shut-down szoftvere menedzseli. A tápellátási rendszer egy további, 1×250 kVA-es készülékkel bővítést is lehetővé tesz.

# FÓKUSZ
# Adatvédelem



## Rizikó vagy kényelem?

**Az internetes tranzakciók biztonságával foglalkozó cikkek többsége csak riogatja az embereket.**

**Szerző: Világhy Tamás**

Nemegyszer éreztem úgy a biztonságtechnikával, kriptográfiával, digitális aláírással foglalkozó cikkeket olvasva, hogy a szerzőknek egyetlen célt sikerült elérniük: eltanácsolni az internetezőket hitelkártyaszámuk megadásától, mert annak birtokában könnyedén kifoszthatják őket, és amúgy sem biztos, hogy megkapják az árut.

Az internet első szakaszában, amikor a weblapok szerepe lényegében csak a marketing- és információszolgáltatás, a biztonságtechnika kevés figyelmet kap. Azt a tényt, hogy valamely cég a Busz utca 15-ös számú házban található, és reggel 9-től délután 5-ig tart nyitva, valóban nem kell védeni. Az ilyen információ „csak” egy célt szolgál: hogy a Busz utcai vállalkozás versenytársainál több potenciális vevőt, beszállítót találjon. Mennyivel egyszerűbb volna beüvegeztetni a betört ablakot, megjavíttatni az elromlott hangszórót, ha elég volna beadni az „üveges” vagy „hangszórójavítás” kulcsszót valamelyik hazai portálon, mint napokig kérdezősködni, kutakodni környékbeli mesterember után.

A rizikó vagy kényelem címbéli dilemmája akkor kezdődik, amikor túl akarunk lépni az információszolgáltatáson. Az internetgazdaság második szakaszában ugyanis már

tranzakciókra is sor kerül a weben, legyen az termék- vagy szolgáltatásárusítás, netán önkiszolgálás. Nem beszélve arról, hogy nemcsak webes, hanem például WAP-os vagy hívóközpontos ügyfélcsatornák is léteznek. Ezeknél ugyanis az ügyfél (a vevő és a beszállító egyaránt) elveszti névtelenségét, adatokat szolgáltat magáról, amelyeket a partner dolga megvédeni és tisztességes célokra használni. Minthogy vi-szont az üzletet fejleszteni kell, a vevő pedig kényelemre, jobb kiszolgálásra vágyik, az eladón múlik, sikerül-e biztonsági garanciákkal meggyőznie a vevőt arról, hogy nála nem kell félni, kicsi a rizikó. Ekkor és csakis ekkor jöhetnek létre új üzletek, és a vevő is jobban érzi magát, mert este 9-kor még el tudja intézni pénz- és cégügyeit.

Tehát a kérdés az: előbb jönnek-e a biztonsági garanciák és utána a kényelmes üzlet, vagy előbb a kényelmes üzlet és ez hozza maga után a biztonsági kívánalmakat? A hazai internetes vásárlások számát és értékét nézve úgy tűnik, a magyar vásárlók már döntöttek. Mégis jó volna, ha a médiák riogatás helyett a kényelmet, a kiszolgálást, az elérhetőséget, esetleg az alacsonyabb árakat vagy az új árusítási formákat is említenék.

Sok szó esik a kriptográfiáról, ami fontos, hiszen ki tudja, hányan látják azt az információt, amit a hagyományos gazdaságban szerződésbe foglal az eladó és a vevő, és senki másnak nem köti az orrára.

Visszatérő téma a digitális aláírás, ami szintén fontos, hiszen ki tudja, ki ül az internetes drót két végén (autentikáció), és ki tudja, nem fogjuk-e letagadni azt a bizonyos vásárlást (non-repudiation), ha közben meggondoljuk magunkat? Mindezekre megoldást nyújtanak a hagyományos gazdaságban a hiteles papírok, igazolványok és tintás aláírások, a digitális aláírás pedig itthon még várat magára.

„Kedvenc" bankom digitális aláírás nélkül is szolgáltat, és habár nem vagyok mindig megelégedve a szolgáltatás sebességével, a nyitva tartás nekem sokat számít. Nemrégiben azonban szöget ütött a fejembe, vajon a tengerentúlon miért működik az internetes kereskedelem digitális aláírás nélkül is, bár ott van már törvény, jóllehet nem régóta. Valószínűleg azért, mert – mind a vevők, mind az eladók – üzletet látnak benne. Felhasználói azonosítóval és jelszóval, digitális aláírás nélkül.

Vajon előbb kell-e megtanulnunk kezelni és használni a digitális igazolványunkat, utána vásárolunk, vagy előbb megtanulunk együtt élni a kényelemmel, és később tanuljuk meg használni a digitális aláírást? Elképzelem, amint Kovács úr 26 év után (nem megveszi második autóját) megkapja digitális igazolványát hajlékonylemezen vagy chipkártyán. Vajon tudni fogja-e, hogyan kell kezelni? Vajon a hackerek nem tudják-e lelopni a számítógépéről? Vajon a PIN-kódot nem fogja-e felírni egy kis cetlire, és betenni a chipkártya mellé a tárcájába? Vajon vesz-e kártyaolvasót a PC-jéhez, vagy megvárja, amíg a bank ingyen adja azt, s vajon a bank már húszezredik ügyfelének ingyen kártyaolvasót ad majd, vagy megvárja, míg tízszer annyi lesz? Vajon lesz-e így kétszázezer ügyfele?

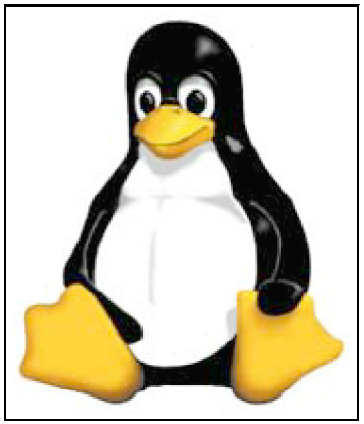
Addig is, míg mindezekre megszületik a válasz, a gazdaság megy előre; az üzletemberek és a vevők eldöntik, megéri-e jobban kiszolgálni a vevőt és a vevő is eldönti, mi éri meg neki jobban: a rizikó vagy a kényelem. Én a kényelemre szavazok, a vevőkiszolgálásra, a jobb szolgáltatásokra, arra a szabadságra, hogy megkapjam azt a terméket vagy szolgáltatást, amire és amikor szükségem van. Hogy van benne kockázat? Persze hogy van. Ezért nélkülözhetetlen a biztonságtechnika folyamatos bevezetése, a macska-egér harc mindennapi alkalmazása és tanítása. Riogatással ugyanis nem megyünk semmire, csak lemaradunk.

*Világhy Tamás az IBM Magyarországi Kft. e-business szolgáltatási vezetője.*

E-mail: **tamas.vilaghy@hu.ibm.com.**

# Sun és Linux: szeret, nem szeret…

**A Linux számára a következő meghódítandó területet  a vállalkozások jelentik.**



Az IBM-től a HP-n és a Dellen át a Computer Associatesig már minden érintett letette a garast a Linux mellett, csupán egy nyitott kérdés maradt: a Sun Microsytems.

Megfigyelők szerint a kiszolgálópiacon meghatározó szerepet játszó Sun viszonya nem egyértelmű a Linuxhoz. Igaz, hogy elkötelezte magát a GNOME grafikus felhasználói felület kezelése mellett, a nagyközönség számára közreadta a StarOffice kódot és webhelyéről Linux-disztribúciókat tölthetnek le UltraSPARC-hoz az érdeklődők, ám saját gépeihez mindmáig nem tette hozzáférhetővé a Linuxot.

Most azonban, amikor az új Linux 2.4-es mag jóvoltából az operációs rendszer többprocesszoros feldolgozási képességei megerősödnek, a Sunnak színt kell vallania.

A január végi LinuxWorld Expón a Sun megpróbált minden kétséget eloszlatni a Linuxszal kapcsolatban. „Linux iránti elkötelezettségünk szilárd és mély – jelentette ki *Herb Hinstorff,* a Sun Linux programirodájának vezetője. – A probléma az, hogy a Linux súlypontja az Intel platformokon van, nekünk pedig nincs ilyen platformunk.”

A Sun a GNOME Foundation egyik alapítója, és hozzáférhetővé teszi a GNOME 2.0 grafikus felületet, amint a KDE-t felváltja a Solaris felület. A Sun ezenkívül létrehozta az

OpenOffice .org-ot, amelynek több ezer közreműködője van. A Sun szóvivője szerint erre a kódra épül majd a StarOffice 6.

Megfigyelők mégis azt állítják, hogy a Sun támogatása kevésbé erőteljes, mint más cégeké. A Sun nyílt rendszerekre vonatkozó elképzeléseiben nyilvánvalóan szerepet játszik a Linux, vélik az elemzők, azonban a Sun aranytojást tojó tyúkja a Solaris, emiatt a Linux mostohább elbírálásban részesül.

Más nehézsúlyú csúcstechnológiai cégektől eltérően a Sun nem tagja az Open Source Development Laboratorynek, amely azon dolgozik, hogy a Linux alkalmazásokat a csúcsszintű többprocesszoros rendszerekre alkalmazza. A Sun képviselője szerint azért, mert nem hívták őket; ha érkezne ilyen felkérés, megfontolnák a dolgot. A 2.4-es mag révén a Linuxot négy- és nyolcprocesszoros gépeken is hatékonyan lehet majd futtatni, ami komoly előrelépés, bár a különféle Unix-változatok, így például a HP-UX, a Solaris és az AIX még mindig több processzort támogatnak.

Az IDC rendszerszoftver-elemzője, *Al Gillen* azzal magyarázza a Sun habozását, hogy a cég többet veszíthet a Linuxon, mint más Unix-fejlesztők. Az IBM és a HP – mindkettőnek van saját Unix-változata – teljesen elkötelezték magukat a Linux mellett, mivel nyilvánvalóan úgy vélik, hogy még mindig kifizetődőbb, ha ők vesznek el saját maguktól üzleteket, mint ha mások teszik ugyanezt.

Ha megnézzük a Linux-piacot, azt látjuk, hogy a pingvines rendszert 93-97 százalékban Intel gépeken telepítették, és a maradék 3-6 százalék is egyenlően oszlik meg a RISC architektúrák között. Nem csoda, ha ez a tény kissé lelohasztja a Sun lelkesedését. A Unix-piacon viszont a HP-val és az IBM-mel ellentétben oroszlánrészt birtokol a cég, itt tehát a vesztenivalója is jóval több.

A Sun azonban újabban felismerte, hogy kétértelmű Linux-politikája káros, és rájött, hogy ha a közvéleményt meg akarja győzni elkötelezettségéről, aktivizálódnia kell. Linuxszal kapcsolatos döntését nyilván befolyásolja az a tény is, hogy a Microsoft nem szíveli különösebben ezt a platformot. Úgyhogy a legtöbb elemző szerint nem kétséges, hogy előbb-utóbb keblére öleli a Linuxot.

A januári bemutatón sokat vitatkoztak arról, hogy a Linux miként tagozódhatna be jobban a nagyvállalati környezetekbe. Még a nyílt kód legszenvedélyesebb hívei is elismerik, hogy a fejlesztési folyamatban néhány dolgot meg kell változtatni, ha a Linux és a nyílt forráskód teret nyer a nagyvállalatoknál. Ahogy a HP egyik nyíltforráskód-stratégája nyilatkozta: itt nem lehet ugyanazt a játékot eljátszani, mint az Apache-nál, amelyet annak idején a hívek anélkül alkalmaztak és futtattak saját vállalataiknál, hogy a szoftver rendesen le lett volna tesztelve.

A Linux fejlődése szempontjából további fontos kérdés az együttműködés más operációs rendszerekkel, a Unixszal és a többiekkel. Ennek megoldási módjairól a szakemberek vélekedése szerint még sokat fogunk hallani a jövőben. Természetes ugyanis, hogy a cseperedő Linux keresi a helyét a nagyvállalati környezetekben. De ahhoz, hogy meg is találja, meg kell tanulnia együttműködnie azokkal a rendszerekkel, amelyek már ott vannak.

*Forrás: TechWeb News*

**2001. MÁRCIUS / NEMZETKÖZI HÍREK / Tovább hullanak a dotcomok**

## Tovább hullanak a dotcomok

Rosszul kezdődött az új év a dotcom cégek számára. Az internetes szektorban az első hónapban csúcsokat döntött az elbocsátások száma: a Challenger Gray & Christmas piackutató cég adatai szerint 12 828 állás szűnt meg, 23 százalékkal több, mint tavaly decemberben. Az 1999 decembere óta megszűnt munkahelyek száma ezzel 54 453-ra

emelkedett.

A leépítési hullám elérte az infrastrukturális szegmenst, vagyis azokat a cégeket, amelyek technikailag felépítik és karbantartják az internetet. 1999 decembere óta 108 cég, a vállalatok 18 százaléka szűnt meg.

Most már a második vonal, a dotcomokat kiszolgáló cégek is szenvednek – véli a Challenger Gray & Christmas elnöke, *John Challenger,* aki szerint a csődhullámot csupán azok az internetes vállalkozások élhetik túl, amelyek bevételei nem kizárólag az internettől függenek.

Kategóriák szerinti bontásban vizsgálva a statisztikákat a gyászos listát a technológiai cégek vezetik 3132 megszűnt álláshellyel, utánuk a fogyasztói szolgáltatások következnek 2732, majd pedig a professzionális szolgáltatások 2652 leépítéssel.

A januárt az óriások is megszenvedték. Az AOL Time Warner 2025 álláshelyet szüntetett meg, az Excite@home 250 dolgozótól vált meg, a professzionális szolgáltatásokat nyújtó MarchFirst 550 embert bocsátott el, a Lucent Technologies pedig bejelentette, hogy belső átszervezések miatt tízezer főtől kénytelen megválni.

*Forrás: Information Week*

**2001. MÁRCIUS / NEMZETKÖZI HÍREK / Árat csökkent az Apple**

## Árat csökkent az Apple

A rendkívül erőteljes – helyenként 1000 dollárt is elérő – árcsökkentés a csúcsszintű asztali rendszereket és noteszgépeket érinti. A leárazás célja, hogy a viszonteladók megszabadulhassanak felhalmozódott árukészleteiktől.

Kétévi virágzás után rossz idők köszöntöttek az Apple-re. A PC Data piackutató cég elemzése szerint az Apple kiskereskedelmi eladásai december első három hetében 40 százalékkal csökkentek, míg a teljes PC-piacon mindössze 24 százalékos volt a visszaesés. Az Apple decemberben bejelentette, hogy a forgalom apadása a negyedik negyedévben 225-250 millió dollár tiszta veszteséget okozott a cégnek. Az Apple történetében ez volt az első veszteséges negyedév azóta, hogy 1997 szeptemberében *Jobs* visszatért a kapitányi hídra.

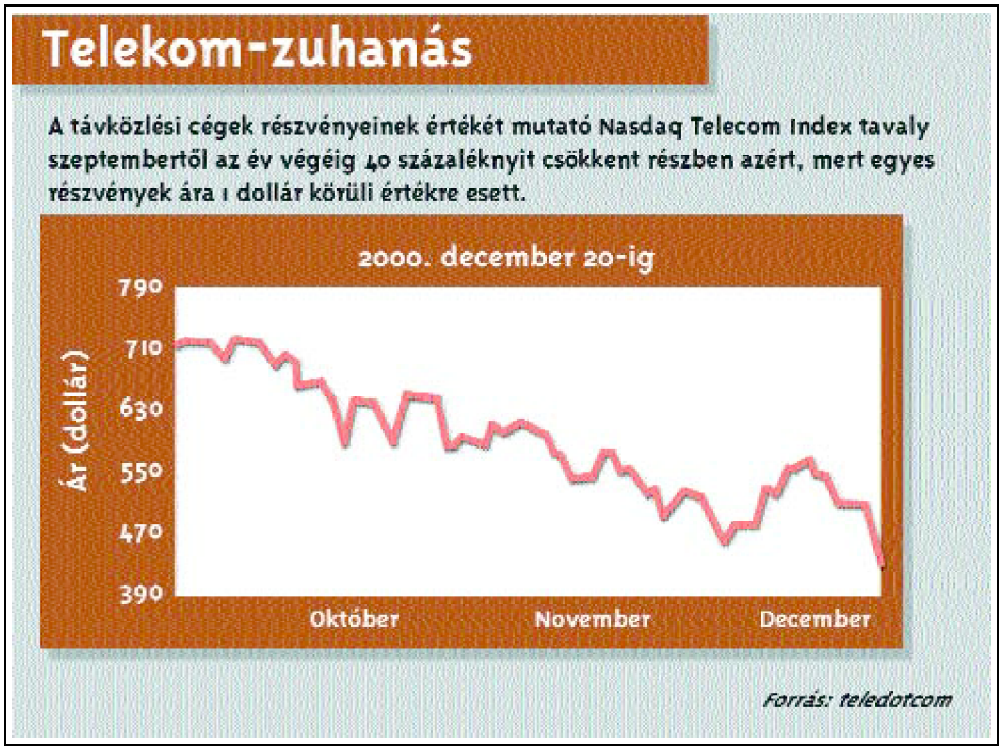
*Matt Sargent,* az ARS piackutató cég elemzője az Apple bajainak egyik fő okát a hosszú termékfejlesztési ciklusban látja, amely miatt a vállalat kilenc hónapos gépeket szállít

akkor, amikor a PC-k forgalma amúgy is esik. Az Apple termékek kiskereskedelmi raktárkészlete értékben a november végi 11,5 hetesről egy hónap alatt 8-9 hetesre apadt. Az Apple a maga tempójában halad, véli a szakértő. Hatalmas csinnadrattával piacra dobja az újdonságokat, aztán hosszú ideig nem nyúl hozzájuk, nem cseréli le őket.

*Forrás: Information Week*

**2001. MÁRCIUS / NEMZETKÖZI HÍREK / TELEKOM-ZUHANÁS**

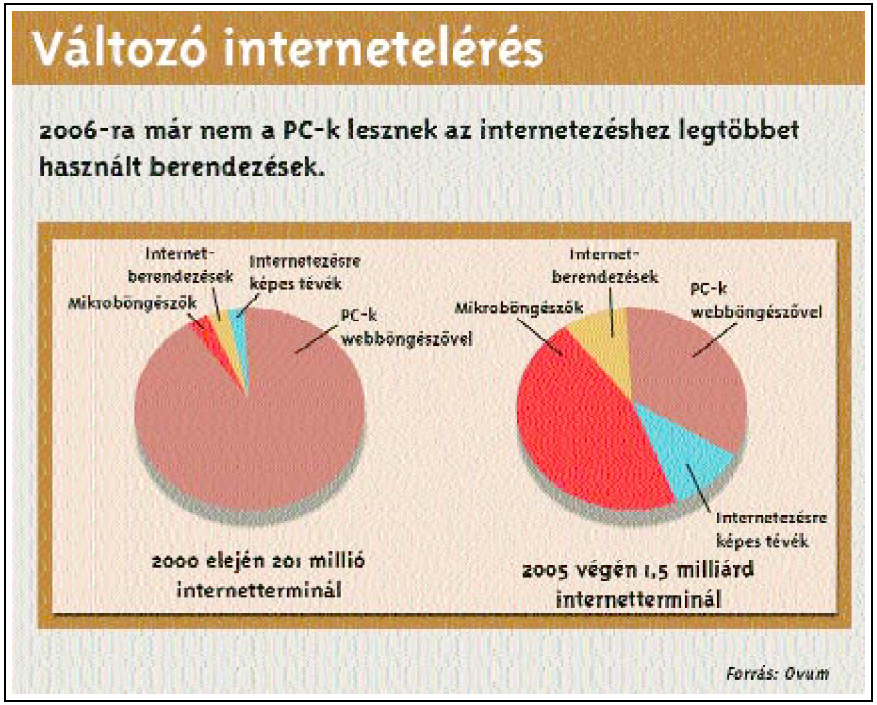
## TELEKOM-ZUHANÁS




A távközlési cégek részvényeinek értékét mutató Nasdaq Telecom Index tavaly szeptembertől az év végéig 40 százaléknyit csökkent részben azért, mert egyes részvények ára 1 dollár körüli értékre esett.

**2001. MÁRCIUS / NEMZETKÖZI HÍREK / VÁLTOZÓ INTERNETELÉRÉS**

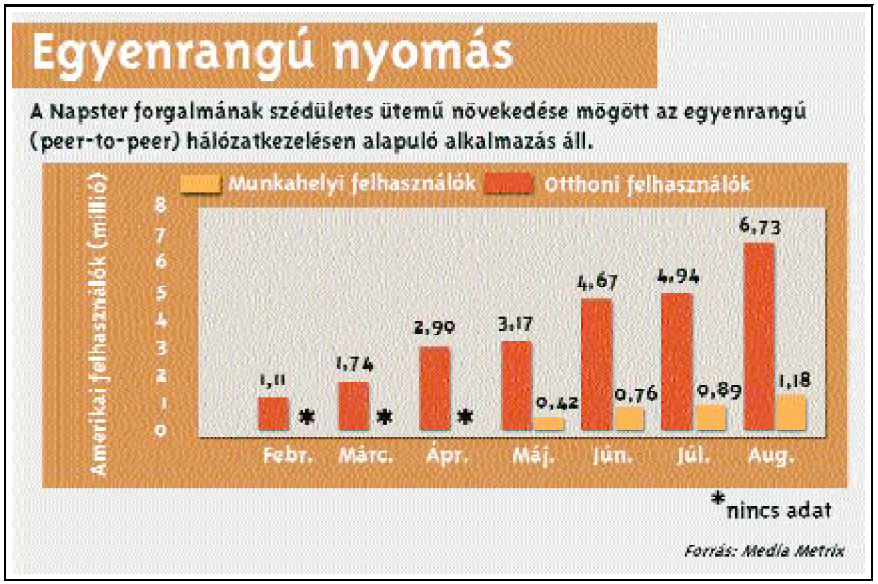
# VÁLTOZÓ INTERNETELÉRÉS




2006-ra már nem a PC-k lesznek az internetezéshez legtöbbet használt berendezések.

**2001. MÁRCIUS / NEMZETKÖZI HÍREK / EGYENRANGÚ NYOMÁS**

# EGYENRANGÚ NYOMÁS




A Napster forgalmának szédületes ütemű növekedése mögött az egyenrangú (peer-to-peer) hálózatkezelésen alapuló alkalmazás áll.

**2001. MÁRCIUS / NEMZETKÖZI HÍREK / Vírusok a levegőben**

# Vírusok a levegőben

**Ahogy a mobiltelefonok és a személyi digitális asszisztensek egyre többet tudnak, mind jobban vonzzák a kétes hírnévre törekvő számítógépkalózokat is.**

**Szerző: Andrew Dornan**

**ILLUSZTRÁCIÓ: BUTTINGER GERGELY**

Azt képzeljük, hogy a nagyobb számítási teljesítmény és az egyre könnyebbé váló kommunikáció csakis jó dolog lehet? Gondoljuk ezt végig még egyszer! Legalábbis ha hiszünk egyes gyártóknak, rövidesen a vírusok újabb járványával nézhetünk szembe.

Mindennek rögtön két oka is van: először is, Moore törvénye szerint rövidesen a mobiltelefonok, elektronikus határidőnaplók és digitális karórák is elérik azt a szintet, amikor szoftvert lehet futtatni rajtuk. Másrészt, a különféle eszközök Bluetooth vagy más hálózati kapcsolat általi összekötése megnyitja az utat az önreprodukáló programok terjedése előtt. Egy fertőzött berendezés a közelében lévő továbbiaknak a fény sebességével lesz képes továbbjuttatni vírusait.

A vállalati rendszergazdák számára azonban ennél is riasztóbb, hogy ezen az úton amúgy biztonságos rendszereik is támadásoknak lesznek kitéve. A mobil készülékek jellemzően a munkatársak birtokában vannak, így a vállalati informatikusoknak nem sok hatalmuk van fölöttük, és mivel az átlagos felhasználónak készülnek, biztonsági jellemzőiktől amúgy sem várhatunk sokat. Ahogy *Cary Nachenberg,* a Symantec Antivirus Research Center *(www.sarc.com)* kutatója fogalmaz: „A kockázat óriási. Mi próbáljuk felvenni a kapcsolatot a készülékgyártókkal, de nem nagyon hallgatnak ránk.”

További híreink is vannak, rossz és jó egyaránt: a vírusok már megkezdték támadásukat a kéziszámítógépek ellen; eddigi kedvenc célpontjaik a népszerű PalmOS-t futtató készülékek voltak. A vírusirtók viszont ugrásra készen várják, hogy újabb programjaikat eladhassák nekünk. Sőt ennél is jobb hír, hogy jelenleg még nincs szükségünk ezekre a szoftverekre.

„A vaklárma ma még gyakoribb, mint a valódi vírus” – véli *Graham Cluley,* a vírusölőket forgalmazó Sophos *(www .sophos.com)* vezető technológus-tanácsadója. Ahogy megemlítette, egyetlen Palm-vírust sem a nagyvilágból gyűjtöttek be, a hírverésre áhító programozók maguk juttatták el azokat a vírusirtó cégekhez. „Sok hűhó semmiért, több a sajtóközlemény, mint a fertőzött felhasználó.”

A szakértők egymásnak ellentmondó véleménye folytán rendszergazdaként magunk leszünk kénytelenek megérteni a vírusok működését. Először is fel kell mérnünk, milyen új platformokat vagyunk készek befogadni a hálózatba: mindenfajtát, amit a munkatársaink használni szeretnének, vagy lehorgonyzunk egy konkrét rendszer mellett? Alighanem túl korai lenne a végleges döntés, de a lehetőségeket számításba kell vennünk. Az is lehet, hogy kollégáink már most is kísérleteznek Palm készülékek vagy WAP mobiltelefonok használatával, pedig hivatalosan még meg sem teremtettük ennek a lehetőségét.

Második lépésként mérjük fel a veszély nagyságát. Térképezzük fel a kiválasztott platform gyenge pontjait és válasszunk védekezési stratégiát. A megelőzés mindig kifizetődőbb, mint a károk elhárítása, ám ebben is többféle választási lehetőség áll előttünk. Egyes vírusölők a PC-n vagy a szerveren futnak, így az ügyfelek adminisztrációja egyszerűsödik, másokat viszont egyedileg kell telepíteni, ily módon viszont az ügyfelek akkor is védelem alatt állnak, ha nem kapcsolódnak a nagy hálózatra.

Jobb, ha szkeptikusak vagyunk, de cinikusak azért ne legyünk. A vírusirtóknak érdekükben áll minden megtörtént esetet felfújni, így tehát a legtöbb vírustámadásról szóló hír puszta reklám. A Sophos becslése szerint a bejelentett vírusok 99,7 százaléka soha nem fertőzött meg senkit a vírusirtó szakemberek tesztgépein kívül. Persze, azért a fennmaradó 0,3 százalék is elég bajt tudna okozni.

**Az érintettek**

Bár eljöhet az az idő, amikor a kenyérpirítónkat is megtámadja egy vírus, elsőként mégis inkább az úgynevezett mobil eszközöknél, a telefonoknál és a személyi digitális asszisztenseknél (PDA-knál) kell ilyenre számítanunk. Az elsőt már senkinek sem kell bemutatni, a második kategóriájába tartozik a rendkívül karcsú Palm V-től a Microsoft Jupiter osztályú, noteszgép méretű – a számítási teljesítmény rovására inkább hosszabb akkumulátoros üzemidőt kínáló – gépeiig mindenféle eszköz. A vírusok elleni küzdelem szemszögéből a noteszgépek nem számítanak ilyen mobil eszköznek, hiszen pontosan ugyanazok a vírusok fenyegetik őket, mint asztali társaikat, tehát a szükséges védekezés is ugyanabból áll. A mai PDA-k már meglehetősen sokat tudnak, grafikus felhasználói felület, irodai alkalmazáscsomagok, kézírás-felismerés található szolgáltatásaik között; processzoraik legalább az Intel 80386 teljesítményének felelnek meg, számos programot tudnak betölteni és futtatni – a vírusveszély tehát nem üres fenyegetés.

Mindezek ellenére a veszélyekre utaló hírek elsősorban a vírusirtók köreiből származnak, akiknek eddig nem nagyon állt érdekükben erre a kis piacra dolgozni. „Már évek óta lehetne vírust írni ezekre a készülékekre – érvel Cluley –, de senki nem vacakolt vele egészen 2000-ig.” Nem volt érdemes, hiszen csak kevesen használtak ilyen eszközöket. „Ha egy vírusíró hírnévre akar szert tenni, akkor a legnagyobb és leginkább homogén platformon támad: ez pedig a Windows.”

A mobil készülékek világa azonban egyáltalán nem ilyen egységes. A PDA-k piacán nincs a Microsoft és az Intel PC-piaci erőfölényéhez hasonló helyzet: három szoftvercég is harcol azért, hogy az övé legyen a legjobb operációs rendszer, kettő közülük ráadásul többféle processzoron is fut. A különféle környezetekhez át kell írni a programokat, így a vírusok terjedése sokkal nehézkesebb.

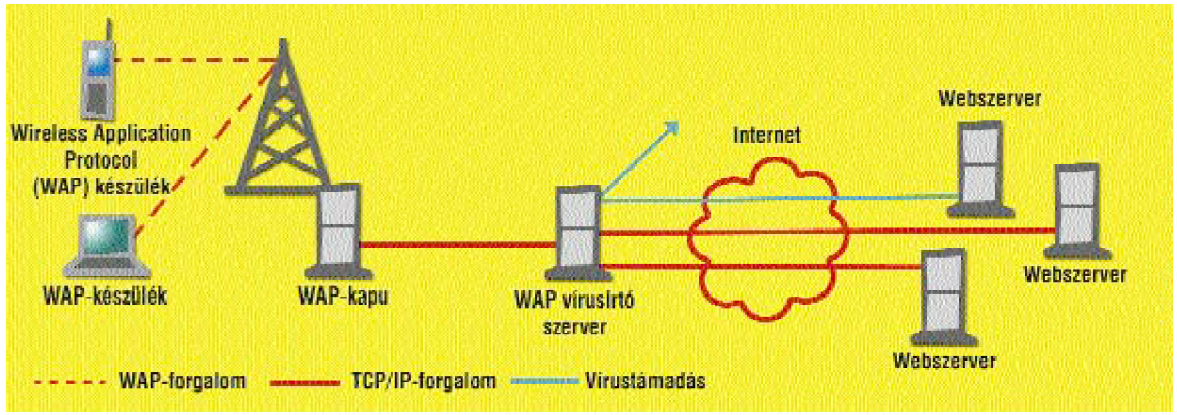
A legnépszerűbb a 3Com-ból kivált Palm Computing *(www.palm.com)* PalmOS rendszere. Elterjedtségének és a közös processzornak, a Motorola Dragonballnak köszönhetően igazi vírusok még csak ezen a rendszeren okoztak kárt. Ugyanez az operációs rendszer megjelenik híresebb cégek (IBM, Sony, Qualcomm) számítógépein is.

A Microsoft már három éve igyekszik elkeseredett harcban megtörni a Palm dominanciáját, sikertelenül: a Windows CE messze lemaradva, a harmadik helyen áll. A második helyen a PDA-t eredetileg kitaláló angol Psion található (a Palm előtt ez a cég volt a piacvezető). EPOC operációs rendszerük elsősorban a menedzserkalkulátorszerű, QWERTY billentyűzetből és rácsukható kijelzőből álló berendezésekre jellemző.

Ugyanez az operációs rendszer áll a Psion és a vezető telefongyártó cégek által 1998 júniusában létrehozott Symbian *(www.symbian.com)* közös vállalat középpontjában is. Már akkor felismerték, hogy a telefonok és a PDA-k egyre inkább magukba olvasztják egymás szolgáltatásait, és előre látták, hogy a telefonoknak is szükségük lesz valamilyen operációs rendszerre. A szövetséget a Nokia, az Ericsson és a Motorola nem titkoltan azzal a céllal hívta életre, hogy a kezdeményezés ne kerüljön ki a kezükből és megmenekülhessenek a Microsoft vagy a 3Com dominanciájától. El akarják kerülni, hogy a Windows követelményeinek megfelelő számítógépeket összeszerelő üzemekké váljanak.

**Szelektív memória**

A PDA-k operációs rendszerét és a vezeték nélküli távközlési terminált egyesítő okos telefonokat a szakértők különösen sebezhetőnek tartják. „A víruskészítők a Palmra és a Windows CE-re nem sok figyelmet fordítottak, mert használatuk az infravörös porton és a gazdagéppel történő együttműködésen alapul” – érvel Cluley. Ha viszont ehhez egy mobiltelefon is csatlakozik, akkor rögtön új távlatok nyílnak meg: a vírusok a hálón keresztül vagy akár más telefonok közvetlen felhívásával terjedhetnek.




**A vírusirtó a WAP-kapu előtt foglal helyet, így minden vírust megállít a telefonrendszerbe kerülés előtt**

Asztali számítógépek sokasága csatlakozik az internetre évek óta, és persze nagy részük nem vált még semmilyen támadás áldozatává. Érdemes tehát ennyire tartanunk a veszélytől? A Symantec szerint például igen. Nachenberg álláspontja az, hogy a mobil készülékek alapvetően kiszolgáltatottabbak, mint az asztali gépek, mert processzoraik jóval kevésbé biztonságosak. A Pentiumban és változataiban (sőt, a 80286-os óta mindegyik Intel processzorban) van memóriavédelem, a telefonok processzoraiban azonban nincs, így az egyes alkalmazások nem tudnak saját, más programok számára elérhetetlen memóriaterületet kapni. Ámbár az is lehet, hogy a memóriavédelem inkább elméleti, mintsem gyakorlati gond, elvégre a Windows asztali vál-tozataiban sem volt ilyen a 95/ 98 és az ME előtt. Ezen operációs rendszerek magja még mindig a régi processzorokhoz írt DOS-ra épül.

A szkript- és makróvírusok megjelenése folytán a memóriavédelem még kevésbé lesz fontos, mert ezek magasabb szinten működnek és nem szorulnak közvetlen memória-hozzáférésre. A legutóbbi ijedelmet a Windows 98 óta minden asztali Windowsban megtalálható Microsoft Visual Basic Scripting (VBS) nyelven írt .vbs vírus okozta. A makróvírusok is gyakoriak; ezek olyan szolgáltatásokkal élnek vissza, amelyeket bizonyos alkalmazások (például a Word és az Excel) visszatérő feladatainak automatizálásához hoztak létre. Ilyen vírusokat könnyebb írni, mint hagyományosakat, ráadásul könnyebben átjutnak az eltérő operációs rendszerek közötti határon.

A Windows CE-be épített Pocket Word és Pocket Excel még nem kezeli a makrókat, de előbb-utóbb alighanem fogja, hiszen az asztali gépek programjaival mindenben kompatibilis alkalmazások a PDA-k népszerűségének növeléséhez is jól jönnek. „Ma még a vezeték nélküli elektronikus levelezés alig több, mint egyszerű üzenetek továbbítása, de amint a csatolt fájlok ide is eljutnak, a vírusok szintén beindulnak” – jósolja Nachenberg.

**Méregkeverék**

A telefonok és a PDA-k tehát szkriptnyelvekkel bővülnek, és ez a vírusszerzőknek nagyon csábító perspektíva. A Sun Microsystems tavaly nyáron jelentette be népszerű nyelvének mobil készülékekhez szánt Java2 Micro Edition (J2ME) változatát. Ez a nyelv is képes platformfüggetlen – operációs rendszertől és processzortól nem függő – alkalmazások (appletek) írására. A Java appletjei egy virtuális gépen futnak – népszerű nevén a homokozóban –, ahonnan nem képesek helyi fájlok kezelésére, kommunikációs kapcsolatok vezérlésére vagy a rendszer más részeinek megtámadására. Habár ez véd a vírusok ellen, egyúttal azt is megakadályozza, hogy az applet sok hasznos feladatot elvégezhessen, ezért a Java megengedi, hogy az alkalmazás nagyobb jogokat kérjen magának. Ehhez azonban a felhasználó hozzájárulása is szükséges, így a Java az odafigyelő felhasználó kezében biztonságosnak tekinthető.

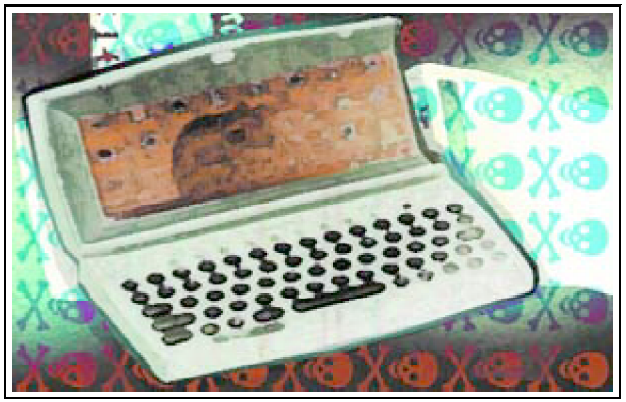
Csakhogy a felhasználók oroszlánrésze korántsem ilyen figyelmes. Szinte mindegyik e-mail vírus arra alapoz, hogy a felhasználó kinyit egy csatoltan küldött fájlt, és ez a legkevésbé sem akadályozta meg a terjedésüket. Tavaly a végzetesnek bizonyult „szerelmes levél” is azt használta ki, hogy az internetezők – nem tudván, hogy programot indítanak el – gyanútlanul megnyitották a csatolt vbs fájlokat. Két évvel korábban még az így kapott exe programokat is vidáman elindították, magukra szabadítva az ártalmatlan, de bosszantó Happy99-et. Szigorúan véve egyik program sem vírus, hanem féreg: a féreg saját magát sokszorosítja, a vírus viszont más programokban próbál elbújni; káros hatásuk azonban gyakorlatilag ugyanaz.

A Javánál nagyobb veszélyt jelent a Wscript, a WAP beépített szkriptnyelve, amely szinte mindegyik újabb – még a nem kifejezetten okos – telefonban megtalálható, akárcsak a Palm és a Symbian legújabb termékeiben. Ma már több mobiltelefon van a világon, mint PC, ráadásul az elemzők szerint négy éven belül a mobil válik az internetelérés alapvető eszközévé. A WAP rövidesen elterjedtebb lesz, mint a Windows, így a vírusban utazóknak új, csábító területet jelenthet.

További problémát okoz, hogy a Wscript kevésbé biztonságos a Javánál: a WAP szkriptjei közvetlenül hozzáférhetnek a telefon szolgáltatásaihoz. Egy vírus tehát végigolvashatja a telefonban tárolt számokat, sorban felhívhatja mindegyiket és elküldheti saját másolatát. A japán NTT DoCoMo hálózatban telefonálók már tapasztalhattak is valami hasonlót: amint készüléküket számítógépükhöz kapcsolták, a PC-n lévő vírus hamis hívást kezdeményezett a rendőrséghez.

A vírusirtók megegyeznek abban, hogy a védekezés legjobb módja a mobil hálózat és az internet közötti kicserélő pontot jelentő WAP-kapura telepített ellenszoftver lenne (lásd az ábrát). Ezek a kapuk a telefontársaság vagy az internetszolgáltató kezelésében vannak, bár egyes nagyobb vállalatok is használnak hasonlót (elsősorban biztonsági

megfontolásokból, mert a titkosítás is ebben a készülékben történik, így a bizalmas adatokat nem kell a kezükből kiadniuk).



A WAP-kapuk egyik feladata éppen a Wscript appletek gépi kóddá fordítása, tehát meg lehetne akadályozni, hogy bármilyen vírus átjusson rajtuk. De ha a vírus egyszer már keresztüljutott akár csak egyetlen kapun, ahol nem futott vírusellenes szoftver, telefonról telefonra már közvetlenül is terjedhet. Jelenlegi eszközeinkkel ezt meg sem lehetne akadályozni. Az egyes telefonokhoz még senki sem írt vírusirtó programot, bár van remény arra, hogy a telefongyártók előbb-utóbb a készülékekbe építenek be ilyen szolgáltatást.

**Félrevert telefoncsengők**

Tavaly júniusban a sajtó izgatottan számolt be egy Timofonica nevű telefonvírus megjelenéséről. Bár a beszámolónak volt igazságalapja, a vírus végül is nem a telefonokat támadta meg: közönséges .vbs vírus volt, és a Windows 98-as és 2000-es rendszereken sem kárt okozott, hanem politikai üzenete volt. A vírus megjelenítette szöveg azzal vádolta a spanyol Telefonica társaságot, hogy törvénytelen üzletekben vesz részt. Ugyanilyen szövegű üzenetet SMS-ként is igyekezett elküldeni más telefonokra, így a legrosszabb, ami a telefonfelhasználókat érte, egy rövid, kéretlen SMS-üzenet volt.

„Ma még a telefonokat nem fenyegezti közvetlen veszély” – érvel Nachenberg; a készülékek tudása ehhez még egyszerűen nem elegendő. A WAP egyetlen kilobájtban korlátozza a fájlok méretét, ez éppen csak elég egy hosszabb bekezdéshez. „De pár éven belül lesznek vírusok által veszélyeztetett telefonjaink is.”

A vírusirtó cégek már most árusítanak olyan szoftvereket, amelyek – állításuk szerint – a jövőbeni támadások ellen is védik a mobil készülékeket (lásd táblázatunkat az 51. oldalon). Legtöbbjük nem a PDA-n, hanem az asztali gépen fut, mivel a szoftverek is általában ugyanezen az úton kerülnek a hordozható gépbe. A két berendezés összekapcsolásakor a vírusirtó végignézi a PDA memóriáját, és minden gyanús elemet eltávolít.

Ezek a PC-n futó programok tehát nem használják a mobil berendezések amúgy is szűkös memóriáját és egyéb erőforrásait, de nem is nyújthatnak tökéletes védelmet, hiszen a felhasználók két PDA között vagy modemről is letölthetnek programokat, a vezeték nélküli hálózat pedig még inkább megkönnyíti majd ugyanezt. Akadnak tehát olyan gyártók is – bár jóval kevesebben –, amelyek a PDA-n futó vírusirtókat forgalmaznak.

Az első ilyen szoftvert 1998-ban az Iris Software készítette a Windows CE számára. Egy év múlva azonban leálltak vele, és új tulajdonosuk nem árusítja, sőt, nem is foglalkozik a termékkel. Lehet, hogy az ismétlődéstől tartanak, de mások sem léptek még a nyomukba. Használt kópiákat még fellelhetünk itt-ott, de ez egy vírusirtónál nem sokat ér, hiszen rendszeres frissítés nélkül hatástalan, a régi csomagok inkább csak a hamis biztonság illúziójába ringatják használóikat.

A Windows CE-t egyébként eddig megkímélték a vírusok; alighanem azért, mert nem különösebben népszerű. Az EPOC-ról ez már korántsem mondható el, ámbár az eddigiek csupán ártalmatlan viccek voltak. A legijesztőbbnek a Fake tűnt, amely animált ablakban közölte a felhasználókkal, hogy formázza a lemezüket. Persze a PDA-kban nincs is lemez…

A ma beszerezhető PC alapú víruskeresők megtalálják mindegyik ilyen tréfacsinálót, az F-Secure pedig egy, az EPOC-on futó programot is készített. Amint ez az operációs rendszer WAP-ot és Bluetootht ismerő mobiltelefonokba kerül, mások is nyilván követik a példájukat.

**Vírusőrségben**

A PalmOS-hez három cégtől lehet vírusirtót venni, ez tűnhet tehát a legjobban körülbástyázott platformnak, de azért nem árt óvatosnak lennünk ítéletünkkel: a Trend Micro cég – amely egyébként nem érdekelt a Palm-programokban – véleménye szerint nem fognak a szoftveresek túl sok energiát pazarolni a fejlesztésre, mert nem éri meg. Amiként a vállalat alelnöke, *David Thompson* fogalmaz: „A PalmOS programok zöme shareware, és a felhasználók nem túlságosan szeretnek pénzért venni programot.” Valóban, a Palmhoz kínált három vírusirtó is szabadon tölthető le az internetről, és szokás szerint nincs is hozzájuk technikai támogatás.

Ez az ingyenprogramokra alapozó szemlélet vezetett egyébként az első, valóban kártékony program, a Liberty Crack megjelenéséhez is. Alkotói álruhába öltöztették: a Nintendo GameBoyát emuláló Liberty shareware játék törésének álcázta magát, de Tetris helyett orosz rulettet játszhatott vele a gyanútlan felhasználó, és a program nemritkán minden adatát és programját kitörölte. Tehát nem vírus volt, hanem – ahogy a programozók nevezik – trójai faló: azzal vette rá a felhasználókat a futtatására, hogy valamilyen kívánatos programnak tüntette föl magát.

Az első igazi vírusra 2000 szeptemberéig kellett várni: a Phage a Liberty Crackhez hasonló pusztítást végzett, de az infravörös porton keresztül más gépeket is megfertőzött. Sokat és sokszor beszámoltak róla, rengeteg ijesztő hír kapott szárnyra, de ahogy Cluley mondja: „Egyetlen felhasználóról sem tudunk, nemcsak mi, a többi vírusellenes cég

sem, aki ténylegesen megkapta volna.”

**Farkast kiáltani**

A Symantec-féle AntiVirus Research Center figyelemmel kísér minden vírust, veszélyességüket egytől ötig terjedő skálán értékelve. Ötöst kap a legveszélyesebb (például a hírhedt Melissa és más, egész hálózatokat romba dönteni képes) vírus. Ezen a skálán az eddig írt összes mobil vírus csak egyes fokozatot kapott: előfordulásuk ritka és jórészt ártalmatlanok.

Az igazságot ritkán hallani ki az alapzajból. A vírusirtók nyilván érdekeltek abban, hogy mindenféle új veszedelemmel riogassanak bennünket, akár igazi a veszély, akár nem. „Ez önmagában is riasztó – figyelmeztet Cluley. – Ha az emberek páni félelemben szaladgálnak összevissza, nem fognak hinni nekünk akkor, amikor az igazi veszély eljön.”

*Andrew Dornan **(adornan@cmp.com)** a Network Magazine szerkesztője, a The Essential Guide to Wireless Communications Applications (Prentice Hall) szerzője.*

*Forrás: Network Magazine, a CMP Media, Inc kiadványa.*

**Fertőzést gyógyító programok**

| Gyártó | PalmOS | Windows CE | Symbian EPOC | WAP |
|---|---|---|---|---|
| F-Secure, www.f-secure.com | natív és PC | — | natív | kapuban |
| Sophos, www.sophos.com | PC | — | — | kapuban |
| McAfee, www.mcafee.com | natív és PC | PC | PC | — |
| Symantec, www.sarc.com | natív és PC | — | — | — |
| Trend Micro, www.trend.com | — | — | — | kapuban |
| Panda Software, www.pandasoftware.com | PC | PC | PC | — |

## TOVÁBBI INFORMÁCIÓ

Az átveréseket és a túlzó riasztásokat leplezi le a *www.vmyths.com,* szkeptikusan elemezve a vírusveszélyt, 1996-ig visszamenőleg ismertetve a beszámolókat, a piramisleveleket és egyéb állítólagos vírusokat.

A Symantec AntiVirus Research Centerének *(www.sarc.com)* kikötőjében az összes ismert vírus részletes leírását megtalálhatjuk.

Az F-Secure (korábban Datafellows) Globális Palm Vírusinformációs Központja a *www .f-secure.com/palm* címen található; a PalmOSen futó ingyenes vírusirtó is innen tölthető le.

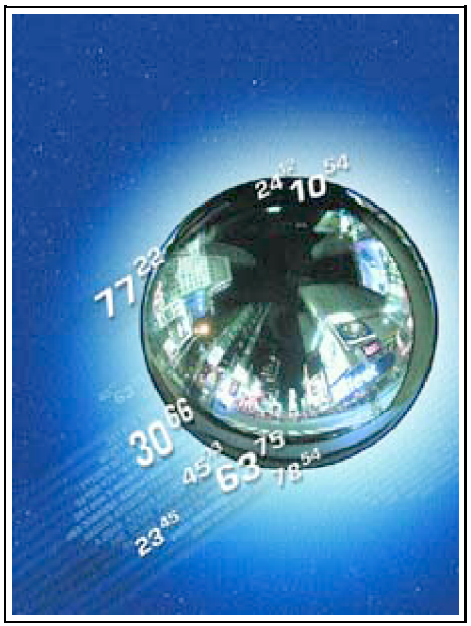
A Stiller Research *(www.stiller.com)* ismerteti, miként hozzuk ki a legtöbbet a vírusirtó programokból.

Az IBM is fenntart egy vírusokról és történetükről szóló anyagot a *www.av.ibm.com* címen. Mivel a vírusellenes iparban nem érdekeltek, véleményük alighanem pártatlan.

# Letámadott szolgáltatók

**A hackerek fürgék és mindig készek az ütközetre, ezért a PC-k és szerverek védelmi rendszerének kialakítása megéri a fáradságot.**

**Szerző: William Betts**



Akármi is áll a webhelyek és a vállalati hálózatok ellen intézett támadások mögött, nem valószínű, hogy a rosszakarók egyhamar felhagynának vele. A leginkább a webszerv bombázza a kiszemelt célpontot, azt remélve, hogy az kifogy az erőforrásaiból.

Az elosztott DoS (Distributed DoS) támadás esetén a támadó nem egyedül indít rohamot, hanem számos idegen számítógépre eljuttatja ügynökét – vagyis a támadást megvalósító prc

Jelen cikkünkben e két támadási módszer részleteit, a sebezhető pontokat és a védekezés lehetőségeit ismertetjük.

**Támadási módok**

A következőkben néhány népszerű támadási módozatot veszünk szemügyre.

**Lepattanó FTP.** Az FTP a dokumentumok és az adatok anonim, külön jogosultság nélküli átvitelére szolgál. A lepattanó FTP segítségével lehet bejutni az alkalmazásokhoz kötőd a nevét és a jelszavát, majd letölti a kívánt adatokat. A csalárd kapcsolat során viszont a behatoló feltölt egy állományt az FTP szerverre, majd ezt továbbküldeti egy hálózatoı processzorát.

Ennek elkerülésére frissítsük fel a szerverek FTP démonát. A tűzfalak szintén segíthetnek a tartalom és a parancsok kiszűrésében. Egyes tűzfalak bizonyos kiterjesztésű állományoka

**Halálos ping/elárasztásos ping.** A támadó IP pingcsomagokkal bombázza az áldozat gépét; ehhez csak egy egyszerű, parancssorból meghívható programra van szüksége. Az á útválasztók és a nyomtatók között is van támadható (részleteket a *flowserv .teco.uni-karlsruhe.de/Ping/* címen olvashatnak). A nyomtatók és útválasztók javítókészleteit globális l jutni, ha túl méretes csomagot küld és parancssorból kiadható utasítással darabolja fel. Amint a tűzfal mögé jutott, rögtön meg is indíthatja a támadást.

**Törptámadás.** A pingtámadás egy változata közbenső hálózat felhasználásával: a pingkéréseket nem közvetlenül a támadott gépnek küldik, hanem egy broadcast címre, de az üzenet

Megoldás lehet, ha szerverünket nem engedjük broadcastként használni. Az útválasztók beállításai között is le kell tiltani, hogy más hálózatoktól IP alapú broadcastkéréseket foga fogadunk el olyan csomagokat, amelyek nem a saját hálózatunkból származnak. Ezt a kellő hatékonyság érdekében a hálózat mindegyik útválasztóján el kell végeznünk, nem csak a h

Ha a megcélzott áldozat a saját hálózatunkon belül található, az útválasztók konfigurálása nem lesz elegendő ellenszer: az operációs rendszert kell szigorúbbra formálni, hogy ellenáll

Egyes operációs rendszereket javítókészlettel meg lehet reparálni (a részletekről a gyártótól érdeklődhetünk). Kezdjük ezt a webszervereknél, mivel ezek a leggyakoribb célpontok. Ma

**SYN elárasztás.** Ez a támadás a célgépet arra kényszeríti, hogy megállás nélkül válaszüzeneteket küldjön egy nem létező számítógépnek. A küldött csomagok arra kérik a kérelmeket elégítsen ki.

A szabályos TCP kapcsolat kezdetekor a célállomás SYN (szinkronizáció kezdete) csomagot kap a küldő géptől, erre pedig SYN ACK (szinkronizáció visszaigazolása) választ l TCP háromlépéses kézfogásának.

A SYN ACK-ot elküldött és az erre érkező ACK-ra váró célgép egy listában tárolja a felépítésre váró kapcsolatokat. Mivel az ACK általában néhány ezredmásodpercen belül köv gép erre küldi vissza SYN ACK csomagját, és az ACK-ra várva felveszi a címet a listájába. A nem létező géptől azonban hiába várja az ACK beérkezését, ezért a cím a listábaı listát, így a valódi kérelmek kiszolgálása nem történhet meg.

A Windows NT alapbeállítása szerint például a SYN ACK elküldése ötször történik meg, minden egyes alkalommal megkétszerezve a várakozási időt, így több mint három perc telik

A várakozási idő csökkentése vagy a lista méretének növelése segít a támadás kivédésében, ám hasznos lehet a rendszer frissítése is. A mai operációs rendszerek már nem érzékenyek

**IP-tördelés.** Az eredeti szándékok szerint az eldugult adatátviteli csatornákat segítendő az IP-csomagokat kisebb méretű csomagokká lehet széttördelni. Ha a támadó nagyon ki tartalmát a fogadó fél újra összeállítja, ezzel túlcsordulnak a pufferei és a számítógép – a szoftverek jellemzőitől függően – leáll, újraindul, de az is lehet, hogy semmi baja nem történ

Egy másik változat szerint az összeállított csomag egy másik csomag közepén kezdődik. Ahogy az operációs rendszer feldolgozza ezeket az érvénytelen csomagokat, elhasználhatja n

**ARP gyorsítótár megmérgezése.** Az Ethernet hálózat adatátvitele az egyes csatolókártyákhoz rendelt MAC-címen alapul. Ahhoz, hogy a megfelelő számítógép jusson hozzá az szerveren futó Address Resolution Protocol (ARP). Ha az általa használt táblázatba hamis adatok kerülnek, a behatoló bármelyik hálózati gép helyébe léphet.

A védekezés legjobb módja intelligens átkapcsoló (switch) vagy hub használata. Unix rendszereken célszerű kikapcsolni a kernel promiscuous módját. Különféle szoftvereszközök – i

**IP-sorozatok előrejelzése.** Miután a támadó létrehozta a kapcsolatot, megszerezheti az IP-csomagok sorozatszámát. Ezzel a számmal felfegyverkezve átveheti a vezérlést, és a támad

A legtöbb operációs rendszer ma már véletlenszerűen osztja ki a sorszámokat, így nem lehet őket előre megtippelni.

**TCP-kapupásztázás.** Támadások előkészítésére szolgál, ha a kalóz automa-tikusan végigpásztáz egy IP-porttartományt, hogy élő kapcsolatra bukkanjon. A védekezéshez nem kell m

**A DNS gyorsítótár megmérgezése.** A DNS névszerver szolgáltatja a domainnevek és IP-címek egymáshoz rendeléséhez szükséges információt. A hatékonyság növelésére a DNS akkor a létező hálózati kapcsolatokat új útra lehet terelni vagy egyes webhelyek elérését le lehet tiltani.

A SANS Institute *(www.sans.org)* szerint a leggyakrabban a Berkeley Internet Name Daemon- (BIND-) féle implementációt támadják, ennek több Unix és Linux rendszer is h függőben lévő kéréseket, így az illetéktelen címeket könnyebben kiszűrik.

**SNMP támadás.** A legtöbb hálózati eszköz alapértelmezésként kezeli az SNMP-t. E támadási móddal átrendezhetők a hálózati hivatkozások, megfigyelhető és máshová irányítható á

A legjobb védekezés, ha áttérünk az SNMP3-ra, amely már titkosítja a jelszavakat és az üzeneteket. Mivel ez a szolgáltatás gyakorlatilag minden egyes berendezésben, útválas eszközöket, amelyekkel globális hálózatokon keresztül lehet teríteni a frissítéshez szükséges anyagokat.

Ellenőrizzük, hogy a vállalati tűzfalra lehetséges-e SNMP3 proxyt telepíteni. Bár ez nem végleges megoldás, a frissítés közben is nyújt valamiféle védelmet.

**UDP elárasztás.** A támadás során a behatoló két gyanútlan rendszert köt össze, összekapcsolva az egyik rendszer UDP-jét (ennek tesztszolgáltatása, hogy minden beérkezett karaktert). A két gép között haszontalan adatok folyamatos áramlása indul meg.

A támadás elhárításához többrétegű megközelítés szükséges. Először is távolítsunk el minden szükségtelen UDP szolgáltatást a rendszerről, majd blokkoljuk a tűzfalon az UDP porto

**Sebezhetőség**

A behatolók arra számítanak, hogy a vállalatok jó része nem tesz meg mindent sebezhetőségének csökkentéséért, és ezen feltételezésükben a legtöbbször nem is csalatkoznak. A SAN

**BIND (Berkeley Internet Name Daemon).** A BIND sebezhetőségén alapuló támadások kivédéséhez célszerű letiltani a BIND démonokat mindazon gépeken, amelyek nem felj meg kell vizsgálni, nem hagyatkoznak-e a DNS-től jövő információkra. A BIND-nek javított változatai is léteznek; a legújabbak jobban ellenállnak a támadásoknak.

**Sebezhető CGI programok.** A Common Gateway Interface (CGI) programok adatgyűjtési és interaktív lehetőségeket kínálnak a webszervereknek. Telepítéskor a legtöbb sze szkriptek felülvizsgálata.

**RPC kihasználása.** A távoli eljáráshívások (Remote Procedure Calls, RPC-k) segítségével az egyik számítógép végrehajthatja a másikon futó programot – ez a szolgáltatás a gyengeségek kihasználása állt.

Ha lehetséges, kapcsoljuk ki vagy távolítsuk el ezeket a szolgáltatásokat az interneten is elérhető rendszerünkről, vagy ha ez nem járható út, telepítsük a gyártó legújabb programvált

**RDS biztonsági lyuk a Microsoft IIS-ben.** A Microsoft Internet Information Serverében (IIS) található, távoli parancsokat adminisztrátori jogosultságokkal futtató Remote Dat komponense – az IIS 3.0-s vagy 4.0-s változatát futtató rendszeren jogosulatlan felhasználónak is megengedi, hogy privilegizált feladatokat (például shell parancsok futtatását) végez

A lehetőség letiltásához a konfiguráción kell változtatni; részleteit a *www .microsoft.com/technet/security/bulletin /ms99-025.asp* címen találják meg.

**Sendmail.** A Sendmail puffertúlcsordulási hibája Unix és Linux rendszereken lehetővé teszi a visszaélést a *root* felhasználó jogaival. Elkerüléséhez a legújabb változat vagy javí vagy átjátszók.

**Sadmind és Mountd.** A Sadmind a Solaris operációs rendszer távoli adminisztrációját szolgálja, és nemritkán megengedi a távoli felhasználóknak, hogy *root* privilégiumokkal fu Sadmind alapállapotban bekapcsolva található; esetleg kapcsoljuk ki addig, amíg a megfelelő frissítéseket be nem szereztük.

A Mountd a Network File System (NFS) szervereken futva szolgálja ki a Unix gépek NFS-re irányuló kéréseit. Puffertúlcsordulási hiba okozza, hogy külső támadók adminisztrátori

**Globális állománymegosztás.** Segítségével hálózaton keresztül megoszthatjuk állományainkat, de ha nem végezzük gondosan, támadásoknak tesszük ki magunkat Unix, Wind megosztást. A windowsos rendszereken feltétlenül erős jelszavas védelmet állítsunk be, az NT-ben blokkoljuk a NetBIOS szerverhez bejövő kapcsolatokat az útválasztó vagy a host s

**Felhasználói azonosítók.** Ha a támadó hozzájut a felhasználói azonosítókhoz, bármiféle rendszeren komoly pusztítást végezhet. Távolítsunk el minden *guest* és *demo* belépési Töröljünk minden egyes jelszó nélkül is használható azonosítót.

**IMAP és POP.** Ha az alkalmazottak a külvilághoz kapcsolódnak, hogy leve-leiket elküldhessék, erre leginkább az IMAP (Internet Message Access Protocol) és POP (Post Off levelezést, akadályozzuk meg a tűzfallal, hogy .dos, .pif, .vbs, .exe, .js, .jse, .bat, .com, .wsh, .wsc, .cmd, .vbe, .wsf, .sct, .shs és .hta kiterjesztésű állományok mellékletként beérkezh

**SNMP.** Erősen ajánlható az áttérés az SNMP3-ra, mivel hitelesítése és a hozzáférések kezelése sokkal fejlettebb. Mivel az áttérés időbe telik, először győződjünk meg arról, hogy a v

Végezetül soha ne feledjük, hogy a hálózatot emberek használják; ha nincsenek tisztában az információvédelem jelentőségével, hozzáállásuk és közreműködésük nélkül a világ legbizt

William Betts **(wbetts@levi.com)** a kaliforniai Levi Strauss cég biztonságtechnikai szakértője.

*Forrás: Network Magazine, a CMP Media, Inc. kiadványa.*

**Operációs rendszerek sebezhetősége**

| Operációs rendszer/ támadási mód | FTP | Ping | SYN | Törp | IP-tördelés | UDP elárasztás |
|---|---|---|---|---|---|---|
| Windows 95 | 1 | 2 | 1 | 1 | 3 | 1 |
| Windows NT 4.0 | 2 | 2 | 1 | 1 | 3 | 1 |
| Sun Solaris | 2 | 3 | 1 | 3 | 2 | 1 |
| Digital Unix | 2 | 3 | 4 | 3 | 4 | 1 |

| Operációs rendszer/ támadási mód | FTP | Ping | SYN | Törp | IP-tördelés | UDP elárasztás |
|---|---|---|---|---|---|---|
| AIX 4.2 | 2 | 3 | 3 | 3 | 2 | l |
| SCO | 4 | 3 | l | l | 3 | l |
| OpenServer Linux | 2 | 3 | l | l | 3 | l |
| FreeBSD | 2 | 3 | 4 | 3 | 2 | l |

l = sebezhető 2 = nem sebezhető

3 = sebezhető, de megvalósítható a védelem 4 = nem ismert

**HOL TALÁLHATÓ?**

A Center for Education and Research in Information Assurance and Security *(www.cerias.purdue.edu)* a veszélyekről és a használható javítókészletekről ad felvilágosítást.

A CERT Coordination Center széles körű információkkal rendelkezik a biztonsági veszélyekről, a javítókészletekről és hasonlókról a *www.cert.org* címen.

Az International Computer Security Association webhelyén *(www.icsa.net)* hivatkozások, tűzfalakról szóló dokumentációk és ingyenesen letölthető szoftvereszközök találhatók.

Az Information Systems Security Association a *www.issa.org* címen tananyagokra, szoftvereszközökre, javítókészletekre, vírusirtókra mutató hivatkozásokat tart fenn.

A SANS Institute biztonsági résekről szóló információkat, oktatási segédanyagokat, operációs rendszerek biztonságosabbá formálásához szükséges tippeket kínál a *www.sans .org* címen

A Security Focus szoftvereszközöket és a biztonsági hiányosságok technikai hátteréről szóló leírásokat kínál a *www.securityfocus .com* címen a Bugtraq fejezetben.

*Dave Dittrich* (Washington Egyetem) tanulmánya a hálókalózok által használt DdoS programokról a *www.washington.edu/People /dad/* címről tölthető le.

A Technotronic.com DoS támadásokkal foglalkozó tudnivalóit a *www.technolotronic.com /denial.html* címen találhatjuk meg.

**2001. MÁRCIUS / CÍMLAPSZTORI / Újabb biztonsági rés**

## Újabb biztonsági rés

Az internet talán legfontosabb szoftvercsomagjának hibája megbéníthatja minden olyan cég munkáját, amelyik webhelyet tart fenn – adta hírül az Egyesült Államok védelmi minisztériuma által támogatott CERT koordinációs központ.

A rosszindulatú behatolók az újonnan felfedezett hiba révén ellenőrizni tudják a tartománynévrendszert (DNS-t), amely a webhelyek címét a felhasználó által könnyen megjegyezhető nevekből (például www.byte.hu) a számítógép által feldolgozható számsorozatokká alakítja át. Aki hatalmába keríti ezeket az eszközöket, könnyedén kicserélheti

vagy átszervezheti a numerikus IP-címeket – állítják a pittsburghi Carnegie Mellon Egyetemen működő CERT szakemberei.

Egy ilyenfajta csere következményei szinte felmérhetetlenek: a webhozzáférések, az elektronikus levelezés, az állományátvitelek, egyszóval a teljes internetforgalom a behatolók által megválasztott címre irányítható át.

A hackerek bárkit elvághatnak az internettől, megakadályozhatják hozzáférését a világhálóhoz és őt magát is elérhetetlenné tehetik. A világhálón majd mindegyik hely egy vagy több névkiszolgálót használ, és a CERT becslése szerint e kiszolgálók nyolcvan százaléka sebezhető.

A CERT felszólítja a rendszer- és hálózati adminisztrátorokat, hogy BIND-jüket (Berkeley Internet Name Domain; a DNS szerverekben legelterjedtebben használt szoftver) haladéktalanul fejlesszék tovább arra a változatra, amely feltehetőleg védett a támadásokkal szemben. A BIND 4-es és 8-as változatában is találtak olyan hibákat, amelyeket kihasználva a számítógépes kalózok önkényes akciókat hajthatnak végre.

A továbbfejlesztésre vonatkozó technikai információk és tanácsok a *www.cert.org/advisories/CA-2001-02.html* címen olvas-hatók. A BIND szerzője, az Internet Software Consortium a *www.isc.org* címen már elhelyezte a szoftver új változatait.

A sebezhető részt a Network Associates egyik részlege, a PGP Security találta meg a szoftverben. A PGP Security szerint a hiba szinte minden olyan internetes kommunikációt veszélyeztet, amely tartománynéven alapul, és érinti az összes céget, amelyik webhelyet tart fenn vagy elektronikus postán keresztül kommunikál. A CERT internetes biztonsági elemzője szerint azonban eddig még nem tapasztalták, hogy bárki is visszaélt volna a frissen felfedezett hiba kínálta lehetőségekkel.

A tájékoztatón nem esett szó a Microsoft webszolgáltatásával kapcsolatos problémákról, amelyeket a hivatalos megfogalmazás szerint DoS támadások okoztak (lásd másik keretesünket – *A szerk.*)

*Forrás: TechWeb News*

**2001. MÁRCIUS / CÍMLAPSZTORI / Kalózkézre került MS routerek**

## Kalózkézre került MS routerek

Nem sokkal a cég üzleti szoftvereinek megbízhatóságáról szóló, kétszázmillió dolláros reklámkampány beindulása után előbb egy router konfigurációs hibája, majd egy támadási sorozat bénította meg órákra a Microsoft weboldalait és a Hotmail szolgáltatást január végén. Az első kétórás DoS támadás után újabb szoftvertúlterhelés fullasztotta le a rendszert. A Microsoft hálózatát felügyelő San Mateó-i Keynote Systems technológiai igazgatója elmondta: a kalózakció – amelyről az FBI-nak is jelentést tettek – annyiban különbözött a korábbiaktól, hogy nem a szervereket, hanem az azokat körülvevő infrastruktúrát célozta.

A szerverleállásokat és hackertámadásokat követően a Microsoft az Akamai Technologiest bízta meg weboldalai védelmével. Az Akamai négy biztonsági szervert állít üzembe, ily módon küszöbölve ki a szerverek túlterhelésével indított támadásokat. A szoftvergyártó elismerte, hogy a hálózatba kötött négy központi szervert egyetlen szolgáltatásmegtagadási támadással meg lehetett bénítani.

Tavaly decemberi 54 milliós látogatottságával a Microsoft.com a világ harmadik legforgalmasabb portálja az AOL és a Yahoo! mögött. Problémák esetére mind az AOL, mind a Yahoo! rendelkezik különböző hálózatokon elhelyezett tartalék szerverekkel, a Microsoftnál azonban minden szerver egyetlen központi szerveren keresztül tartotta a

kapcsolatot a külvilággal.



**LABOR**
**Szoftver**



# Tűzfal a lakásban

**Hatékony személyi tűzfal hiányában az otthoni és kis irodai gépek kiszolgáltatottak az internetről érkező támadásokkal szemben.**

**Szerző: Curtis E. Dalton**

Az internet kalózai már régóta rengeteg galibát okoznak a vállalati hálózatokban, de az otthoni felhasználókat és a távdolgozókat csak most kezdik hasonlóképpen bosszanta nagyvállalatok lehetőségeihez mérhető biztonsági csapat, méregdrága eszközökkel. Márpedig megfelelő háttér hiányában ezek az otthoni gépek és a kisvállalati hálózatok nagyon is v

Ismerkedjünk meg tehát a személyi tűzfalakkal. Ezek az egyszerű, olcsó rendszerek védelmet ígérnek, de vajon mennyit képesek ebből megvalósítani? Valóban elegendő lehet gyorsan

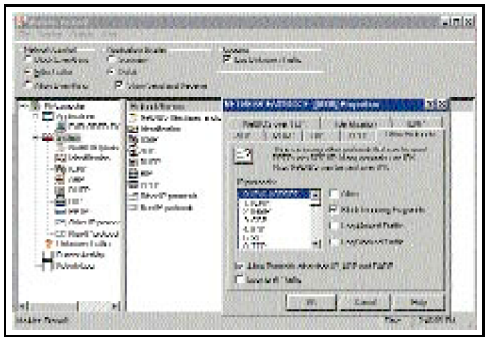
**Személyi védelem**

A személyi tűzfalakat egyetlen asztali gép internetes csatlakozás közbeni védelmére tervezték. Ennek érdekében folyamatosan figyelik a befelé és a kifelé haladó forgalmat, engec felhasználó maga határozhatja meg. Vállalati környezetben egy központi kiszolgáló egységes biztonsági beállításokat kényszeríthet minden egyes tűzfalra.

A személyi tűzfalaknak meg kell oldaniuk a behatolások és a próbálkozások földerítését is, amelynek során értesíteniük kell a felhasználót a folyamatban lévő támadás jellegéről nem elegendőek. A tűzfalaknak megbízható módon kell kapcsolatba lépniük a távoli számítógépekkel: noha az otthoni felhasználásban még nem terjedt el, a virtuális magánhálózatok

A személyi tűzfalaknak háromféle változata létezik: önálló, hardveres és ügynök alapú.

A leggyakoribbnak számító önálló tűzfalak a gépre egyszerűen telepíthető programként futnak Windows 95/ 98/NT, esetleg 2000 alatt. Csak egyetlen készülék védelmére alkalm formájában az internetcsatlakozást védik. Használatukhoz további szoftverre nem, de DSL-csatlakozásra vagy kábelmodemre szükség van. E tűzfalak némelyike akár több száz külső fél kezelheti.



A McAfee Firewall forgalomszűrő szolgáltatása megakadályozza a trójai falovak behatolását

Az ügynök alapú tűzfalak is programok, ám az önálló szoftveres változatokkal ellentétben központi biztonsági szerverről kapják beállításaikat, így velük a vállalati hálózat távoli rész

A legtöbb szolgáltatást olcsó – sőt ingyenes – termékekben is megtalálhatjuk. Ennek ellenére ne a költségek alapján válasszunk tűzfalat magunknak!

Az ismertetett tűzfalakat kipróbálandó, mindegyiket az általa kezelt legfrissebb operációs rendszerre telepítettük, az önálló berendezéseket pedig egy kis helyi hálózatra. letapogatásával, DoS támadásokkal teszteltük a tűzfalak biztonsági szintjét, naplózási és felderítő képességeit.

**McAfee Personal Firewall**

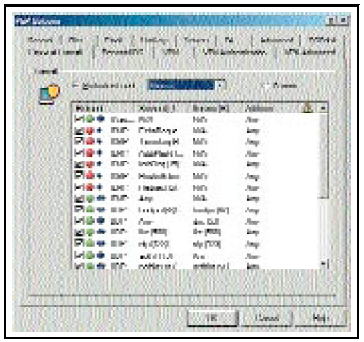
A korábban Signal 9 Solutions ConSeal Private Desktop néven ismert program tiszteletre méltó szolgáltatási listát kínál. A beállítások megváltoztatásához jelszót köthetünk ki, faló programoktól nem is védhetnénk meg magunkat. Miután sikeresen landoltak gépünkön, ezek a programok a számítógép beállításait, jelszavait, webhasználatunkkal kapcsol szükséges. A kémprogramok zöme nem okoz közvetlen kárt, de a legutóbbi szoftverletöltésekről, a meglátogatott weboldalakról és a gépünkön található programokról infor tekinthetők rosszindulatúaknak.

A trójai faló programok jelszavakat vagy kiválasztott állományokat juttathatnak vissza a feladónak. Egyik legutóbbi képviselőjük, a BackDoor-G a számítógépünk fölötti teljes re felvehetjük a harcot az ilyen behatolók ellen.

A program három előre beállított biztonsági szintet ismer: mindent blokkol, mindent megenged vagy szűri a forgalmat. Az első nem sokat ér, ezzel az erővel akár ki is léphetünk megadhatjuk, milyen protokollokat és csatlakozókat kívánunk engedélyezni és melyeket letiltani. Ezek meghatározása persze nem minden felhasználó számára egyszerű feladat. azonban elesünk a finomhangolás lehetőségétől. Amint megfelelőnek találjuk a beállításokat, a tűzfal által készített jegyzőkönyvek elemzésével folytathatjuk a testre szabást.

A szűrő üzem alapbeállításai nem térnek ki egy-két közepes és kis veszélyt jelentő támadási lehetőségre. Nem jelzik például, ha a támadó próbaképp a csatlakozóinkat vizsgálgatja, tá

A program telepítése kicsit nehézkes. Amikor újraindítjuk a gépet, először a readme állományt kell elolvasnunk. Ez leírja a kötelező, kézzel még elvégzendő lépéseket, majd – l biztonsági szintje nem rossz, ráfér azonban még egy kis javítás, továbbfejlesztés.



Többféle biztonsági szintet állíthatunk be  a PGP-ben

**Norton Internet Security 2000**

A webről érkező reklámokat, süti (cookie) állományokat, a böngésző verziójára vonatkozó információkat, JavaScript- és ActiveX-tartalmakat képes blokkolni, továbbá alkalmas nem. Ha azonban egy véletlenül átcsúszott reklámot a tűzfal szemétládájába dobunk, legközelebb már nem engedi át.

A program beállításai: biztonsági, bizalmas, szülői felügyelet és reklámtiltás. A biztonsági kategória szabályokon alapul, de interaktív tanulásra is képes – ez kevés versenytársán ezt meg is jegyzi magának. Mivel ez mindkét irányú forgalomra vonatkozik, a legelső alkalommal mindig végig kell haladnunk ezeken a lépéseken, e nélkül ugyanis az Outlook legnagyobb biztonság mellett is így maradnak.

A bizalmas beállításnál a böngészők jellemzőit és a sütiket különféle szinteken blokkolhatjuk: mind bejövő, mind kimenő forgalmukat megakadályozhatjuk. A program kiválóan naplo

Az automatikus konfigurálás kellemes, ám ellenünk fordulhat, ha tényleges támadásban lesz részünk. Csatlakozóletapogatás vagy DoS támadás során a tűzfal egészen addig új sz kell beállítanunk a szűrési feltételeket.

A Norton programja ugyancsak megvéd minket a vírusoktól, beleértve jó néhány trójai faló programot is. Ha egyetlen, mindent magában foglaló tűzfalmegoldásra vágyunk, ez a szof

**BlackICE Defender**

A felhasználók körében a Network ICE programja örvend a legjobb hírnévnek. Telepítése és beállítása egyszerű, négy beépített biztonsági szintje – nemtörődöm, óvatos, ideges és legszigorúbb szint, az ideges és a paranoiás is védtelenül hagyja az Internet Control Message Protocol (ICMP) és a Traceroute támadási pontokat – alighanem csak azért, ho fragmentált csatlakozóletapogatásokat is, és a felhasználó riasztásának különféle módozatai közül választhatunk. IP-cím és  a gazdagép neve alapján kitilthatunk egyes támadókat igyekszik kideríteni, időnként viszont egyes jóhiszemű hálózati tevékenységet is támadásnak minősít. A felhasználó azonban gyorsan megtanulhatja, miként válassza szét a hamis és a

A különféle csatolókhoz ezzel szemben nem rendelhetünk eltérő kívánalmakat: az otthoni helyi hálózatunkra nem adhatunk meg másfajta biztonsági jellemzőket, mint az interne nem védekezhetünk vele, de még csak észre sem vesszük, hogy ilyen támadás áldozatai lettünk – és legalább tucatnyi ilyen, vírusellenőrzők által nem azonosított trójai faló progr számára a személyi tűzfalak piacán.

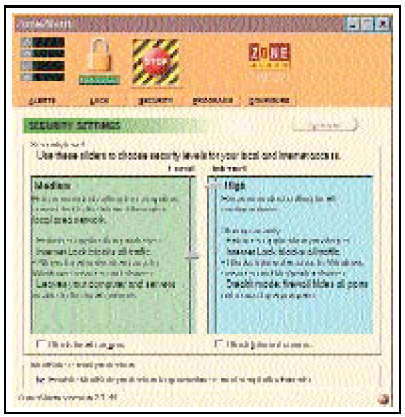
**Pretty Good Privacy**

A Network Associates programjának közelmúltban bemutatott legújabb változata igazán imponáló szolgáltatáslistát kínál. A korábbi verziókból ismert lehetőségek – állományrer bekerült a programcsomagba. Számtalan előre beállított biztonsági szintje tovább finomítható jól áttekinthető felhasználói felülete segítségével. Alapbeállítása azonban semmi védelm

A program megkülönbözteti a kiszolgáló- és az ügyfélgépeket. Ha szerveralkalmazásokat futtatunk számítógépünkön, a beépített biztonsági beállítások igencsak jól jöhetnek. A
egyes támadásokról hangos, látható vagy elektronikus levélben elküldött értesítést kérhetünk. Az alapbeállítás szerint a támadók azonnal behatolóknak minősülnek, és a program min

A legszigorúbb fokozat viszont már egyetlen lyukat sem hagyott betömetlenül, az összes ismert támadási kísérletnek szilárdan ellenállt. Ugyanakkor nem azonosította az e
elvégezhesse a megfelelő elemzéseket, és mivel a program a bemenő adatok zömét sikeresen blokkolja, ez az elemzés nem lehetett sikeres.

A PGP-vel nem zárhatjuk ki teljesen a kémprogramokat, ehhez az kellene, hogy az általuk használt csatlakozókat és protokollokat előre ismerjük. Mivel azonban a rosszindulatú p
biztonsági szabályokat, egyes rosszindulatú programok átcsúszhatnak rajta.



Internetezéskor hatékonyan védi meg gépünket az otthoni használatra ingyenes ZoneAlarm

További kellemetlenség, hogy ha már gondosan beállítottuk komplex biztonsági szabályainkat, a program nem engedi meg, hogy mindezt mentsük. Amint visszaváltunk – akárcsa
hogy a védelem teljes egészében a PGPnet komponensre épül: ha ezt véletlenül letiltjuk, minden tűzfalas védelem megszűnik. Még további hátrány, hogy nem képes a támadó lenyom

Az említett hiányosságoktól eltekintve a PGP Desktop Security 7.0 biztonsági programok nagy tudású együttesét jelenti az otthoni felhasználóknak. A gazdagép védelme és a felhaszı

**ZoneAlarm**

Kényelmes használatának köszönhetően ez az egyértelmű nyertes. Telepítése és kezelése gyerekjáték, interaktív öntanuló modulja menet közben kérdezi meg a felhasználót, en
programok ellen a be- és kimenő forgalom szűrése véd. A vizsgált termékek közül egyedüliként nemcsak a kimeneti csatlakozókat azonosítja, de megadja azt is, melyik program prób

A levelező ügyfelek – például az Outlook – esetében kézzel kell megadnunk a távoli levelező kiszolgáló adatait. Ha kívánjuk, a program saját frissítései automatikusan letöltődne
ugyanakkor még ezen a szinten sem adott riasztást a csatlakozókat pásztázó és a DoS támadásokról.

Otthoni használatra a ZoneAlarm ingyenes. Ha csupán az internetkapcsolat idejére kívánunk védelmet, és nincs szükségünk más tűzfalak speciális szolgáltatásaira, ezzel a programm

**Titkos ügynökök**

Ha vállalati hálózathoz keresünk biztonsági megoldást, más programokon kell gondolkodnunk. Az ügynök alapú személyi tűzfal a távoli és helyi irodai hálózatok biztonsági beáll
eltéréssel: az ICEcap Manager központi kezelőszervertől kapja meg beállításait. A riasztások a helyi programhoz és ehhez a szerverhez egyaránt befuthatnak. A helyi rendszerek
Ennek érdekében a BlackICE Agent számos népszerű vir-tuális magánhálózati (VPN) ügyféllel együttműködik. Nem egy, a VPN-t széles körűen használó cég egyébként abban

megakadályozni abban, hogy szándékosan kiiktassák vagy megkerüljék a védelmet. Nem szerencsés, ha egy cég úgy véli, belülről semmiféle támadás nem érheti. A behatolók állományok titkosítása továbbra is az egyetlen járható út.

Szinte mindegyik jelenlegi VPN-megoldás lehetővé teszi, hogy a központi VPN kapuról adjuk meg az ügyfelek biztonsági beállításait. Azzal, hogy egyszerűen megtiltjuk az ügyfe –, az ügyfelek minden igényükkel a VPN kapuberendezést lesznek kénytelenek megkeresni, ahonnan a forgalom a megfelelő helyre továbbítódhat. A titkosításnak köszönhetően ha otthoni VPN-ek ugyanazt a védelmi szintet élvezhetik, mint a vállalat irodáiban lévő társaik. Az otthoni gépeket vírusellenőrző és állománytitkosító programokkal is el kell látni, n kulcs gondos megőrzése nélkül. Jó eszköz hozzá a Network Associates PGPdiskje (ez a PGP Desktop Security 7.0 csomag része): segítségével megfelelő biztonsággal titkosíthatjuk a

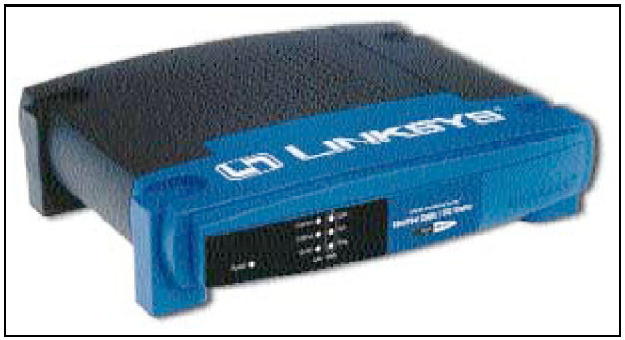
**LinkSys és társai**

A hardveres tűzfalak szintén kínálnak hasonló szolgáltatásokat. Vállalati környezetben, ahol központi helyről kell menedzselni a számos telepített személyi tűzfalat vagy kevé két-három, az internetre egyszerre kapcsolódó otthoni számítógép védelme a cél. Az áruk azonban elriasztja a kevésbé elszánt felhasználót.

A LinkSys-féle BEFSR11 és a SonicWall gyártmányú SOHO a két leggyakoribb ilyen tűzfal. Az egyszerű védelmen kívül mindkettő számos egyéb szolgáltatást kínál. A SOH felhasználók (RADIUS), DHCP kiszolgáló- és ügyfélszolgáltatások, webtartalom szűrése, VPN, digitális hitelesítés, központosított biztonsági szabályzatok, testre szabható tűzfalas

Mindezek közül talán a központosított szabályzat a legfontosabb. Elengedhetetlen, hogy egyetlen központi helyről a távol elhelyezett gépekre is letölthessük a biztonsági szab környezetben a SOHO tűzfal mind gazdaságossága, mind kezelhetősége szempontjából kiemelkedik. Mindemellett még takarékoskodni is segít, mert – az internetkapcsolatunk kellene telepítenünk, az ehhez tartozó külön IP-címekkel együtt.

A tűzfal a behatolásokat is észleli, a riasztása azonban e-mailen alapul: ha tehát a levelező kiszolgáló nem él, vagy éppen az esik DoS támadás áldozatául, a riasztás nem k figyelemmel kísérheti.



A kommunikációs csomagok szűrésével garantálja a védelmet a LinkSys hardveres tűzfala

A LinkSys tűzfala a versenytársáénál kevesebb szolgáltatással büszkélkedhet, de ára ezzel arányban áll. Hiányzik a VPN, a központosított szabálykezelés, a beépített vírusellenő amely a csomagok szűrése alapján nyújt védelmet. Ennek ellenére a LinkSys és az általa védett rendszerek nem bizonyultak érzékenyeknek a leggyakoribb DoS támadásokra és a tűzfalakkal; kevesebbet tud ugyan, mint a SOHO, de megfelelő – és főleg jutányosabb árú – alternatíva lehet.

**Egyéb bonyodalmak**

A távoli irodák tűzfalainak központi helyről való karbantartása éppen az a szolgáltatás, amire sok cég már nagyon várt, hiszen ezekben a külső irodákban általában nincs megfe

többféle csatolója van, és a megfelelő beépítés elengedhetetlen a megbízható működés szempontjából.

Amint megismerkedtünk az alapvető kérdésekkel, a bonyolultabb feladatok – a szabályzatok kialakítása, a felmerülő események kezelése – sem okozhatnak már gondot. Vajon által beküldött jelzéseket? Hogyan érkeznek be a jelzések? Titkosítatlan, közönséges internetforgalomban – amibe mások kívülről belepiszkálhatnak – vagy virtuális magánhálóz vagy a technikai személyzet azonnal értesítést kapjon a biztonságot érintő események bekövetkeztéről?

Csak néhány példát ragadtunk ki a technikai részleteken túlmenően fölmerülő logisztikai és eljárási kérdésekből. Akár távoli irodákat kell kiszolgálnunk, akár egyetlen otthoni gé a tűzfalak jó segítőtársaink lehetnek.

Curtis E. Dalton **(cdalton@greenwichtech.com)** a Greenwich Technology Partners tanácsadó cég főmérnöke.

*Forrás: Network Magazine, a CMP Media, Inc. kiadványa.*

**A VIZSGÁLT TERMÉKEK**

| Gyártó | Termék | Webhely |
|---|---|---|
| LinkSys | BEFSR11 | www.linksys.com |
| McAfee.com | McAfee Personal Firewall | www.mcafee.com |
| Network ICE | BlackICE Defender | www.netice.com |
| Network Associates | PGP 7.0 Personal Firewall | www.nai.com |
| Symantec | Norton Internet Security 2000 | www.symantec.com |
| SonicWall | SOHO Firewall | www.sonicwall.com |
| ZoneLabs | ZoneAlarm | www.zonelabs.com |



## ÚJDONSÁGOK

## HARDVER

**Compaq zenedoboz**

MP3 formátumú zenei fájlok lejátszására is képes digitális sztereó jukeboxot fejlesztett ki a Compaq. A készülék bizonyos szempontból inkább hifiberendezésként működik, semmint PC-perifériaként. A digitális jukebox, amely körülbelül akkora, mint egy hagyományos hifiberendezés, PC nélkül is használható. 20 GB-os merevlemeze mintegy 400 CD vagy 5000 MP3 formátumú zeneszám tárolására képes, ezenkívül tartalmaz egy 56 Kbps sebességű modemet az internetes rádióállomások hallgatásához. Televízióhoz csatlakoztatva interaktív zenei adatbázis megjelenítésére is képes, a PC-csatlakozás létrehozását pedig HomePNA hálózati funkció segíti. A felhasználó a menü alapján különféle módokon rendezheti el a dalokat, korlátlan számú lejátszási listát és stíluscsoportot hozhat létre. Az iPaq Music Center természetesen CD-lejátszót is tartalmaz, és megkönnyíti a CD-lemezek internetes beszerzését.

*www.compaq.hu*

**3com kamera**

Január közepétől Magyarországon is kapható a 3Com digitális kameracsaládjának új tagja, a Homeconnect PC Digital WebCam Lite. A Homeconnect család új tagja ideális megoldás mindazoknak, akik a videózáshoz nem igényelnek túl nagy rugalmasságot és mobilitást, de elérhető áron szeretnének webes kamerát vásárolni. Felhasználásával kényelmesen, otthonról lehet kapcsolatot tartani a távoli családtagokkal és barátokkal. Azoknak az otthonukban dolgozó szakembereknek is hasznos lehet, akiknek a hordozhatóság nem elsődleges szempont. Az USB csatolóval ellátott kamera teljes képet egy lépésben letapogató 1/4 hüvelykes VGA CCD képszenzora 640×480, 320×240, 160×120 és 176×144 képpontos felbontásra képes. Legnagyobb felbontásban a készülék tíz képet rögzíthet másodpercenként. A WebCam Lite-tal egy időben jelennek meg a termékcsalád már korábban kapható kamerájának szélesebb körű felhasználását elősegítő új tartozékok, a mobilitásról gondoskodó Travel Pak, a Laptop Clip és a három kiegészítő lencsét tartalmazó Digital Lens Pak.

*www.3com.com*

**ProLiant miniszerver**

A Compaq Észak-Amerikában kibővíti ProLiant DL kiszolgálócsaládját az új ProLiant DL320 egyprocesszoros szerverrel. Az új készülék tovább folytatja a kis helyigényre és internetes kiszolgálásra optimalizált ProLiant megoldások generációját. A DL320-at alapkiszerelésben egy Pentium III 800 MHz-es processzor hajtja 256 KB másodszintű gyorsítótárral; 128 MB 133 MHz-es memóriája 2 GB-ig bővíthető, és választhatóan SCSI Ultra Wide3 vagy ATA-100 csatolójú merevlemezt tartalmaz akár 40 GB méretben. A ProLiant DL320-szal a Compaq olyan költséghatékony, nagyon kis helyigényű kiszolgálót szállít, amely gyors kiépítésű, akár több ezer kiszolgáló esetén is könnyen kezelhető távfelügyeletet jelent és egyszerűsíti a bonyolult, sokkiszolgálós környezetet. A DL320 garantálja a ProLiant DL sorozatra jellemző intelligens kezelhetőséget és a kiemelkedően jó szervizelhetőséget, amelyet a bővülő lokális internetszolgáltatók és a dotcom cégek számára alakított ki a cég.

*www.compaq.com*

**700 MHz-es Cyrix**

A VIA Technologies január végén bejelentette a Cyrix III generációjának legújabb és leggyorsabb, immár 700 MHz sebességen működő processzorát. A leginkább árérzékeny területekre szánt, nagy teljesítményű processzor 0,18 mikronos gyártósoron készült, így megfelel a mai követelményeknek. A Socket 370-es foglalatú Cyrix III sorozat 128 KB elsőszintű gyorsítótárral rendelkezik, képes 100 és 133 MHz buszsebességre is processzorfüggően, és ismeri mind az Intel MMX, mind az AMD 3DNow! technológiáját. Ezzel az összeállítással a VIA nyíltan ringbe szállt a Celeron II és a Duron ellen a „value-PC” piacon. A processzor különlegessége, hogy a 0,18 mikronos gyártási technológia és a VIA saját megoldásai miatt energiafelvétele és hőkibocsátása egyaránt jelentősen csökkent a hasonló kategóriájú központi egységekhez képest. A processzorcsalád 500, 533, 550, 600, 650, 667 és 700 MHz-es sebességű változatai nagykereskedelmi tételekben már kaphatók.

*www.via.com*

**2001. MÁRCIUS / ÚJDONSÁGOK / SZOFTVER**

## SZOFTVER

**Távfelügyelet**

A Computer Associates távfelügyeleti megoldásának új verziójával, a Unicenter TNG Remote Control Option (RCO) 5.1-gyel az IT menedzserek elektronikus kioszkok és bankautomaták felügyeletét is elláthatják. A Unicenter TNG RCO 5.1 nem csupán a földrajzilag szétszórt berendezések kezelésével járó költségeket csökkenti, hanem a biztonságos kommunikációt és a távoli berendezések automatikus leltározását is megoldja.

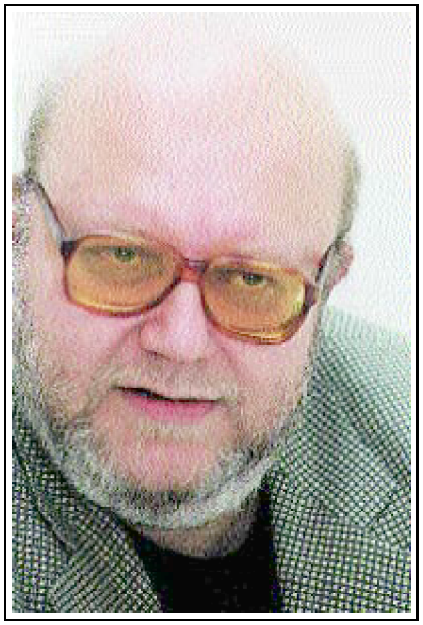
*www.ca.com*

**2001. MÁRCIUS / SZABAD SZEMMEL Kis János rovata**

## SZABAD SZEMMEL
### Kis János rovata

**2001. MÁRCIUS / SZABAD SZEMMEL Kis János rovata / A II. Cyber War első harcai**

## A II. Cyber War első harcai



FOTÓ: SEBESTYÉN JENŐ

Az új évezred beköszöntével kitört a korábban sokszor megjósolt II. Cyber War, amelyre az utókor talán az első szerzői jogi háború címkét fogja ragasztani. Mindenesetre tény, hogy megtörténtek az első ütésváltások. Áldozatok még nemigen vannak, bár számuk idővel rohamosan nőni fog. Minden oldalon dörögnek a fegyverek, a hátországi csendőrség pedig végzi alattomos munkáját, a deviánsok és a vélt árulók felderítését.

A háború nem sokkal 2001 fordulója körül egy meg nem határozható napon tört ki. Ekkor írta alá ugyanis több nagy számítógépgyártó cég azt a szabványajánlást, amelyről így számolt be a szakma internetes hírügynöksége:

„A vezető hardvergyártók olyan, másolás elleni eljáráson dolgoznak, amellyel a felhasználó számítógépében megakadályozhatnák a jogvédett tartalmak másolását. Az Intel, a Panasonic, a Toshiba és az IBM vezetésével készített CPRM technológia (Content Protection for Recordable Media, tartalomvédelem írható hordozókra) a merevlemezeken, a cserélhető háttértárakban és a CD-ROM-okban fogja megakadályozni az illegális másolást. A hagyományos MP3-as vagy más, házilag elmentett formátumok blokkolására nem alkalmas. A technológiát a hardverszabványokat alkotó National Committee for Information Technology Standards 2001 februárjában kívánja beépíteni saját tervezetébe, amelyet akár már a nyáron alkalmazhatnak a kereskedelmi termékeknél.”

E hír nem egyéb, mint a háború alapokmánya. Már réges-rég nem a felhasználó jobb kiszolgálása, hanem minél alaposabb megkopasztása a fő törekvés. Ami ellen az érintettek természetesen tiltakoznak, ez viszont újabb és újabb törvényszigorításokra és -módosításokra vezet a szent cél, a felhasználók megfélemlítése érdekében. Ez érthető, hisz az üzletben egyesek nagyon sok pénzt látnak. Az internetes tartalomban, a szoftverben pedig még annál is többet: az önmegsemmisítő árucikket, amely pótolni tudja a gazdaság keringésében a kiesett hadibeszerzési bevételeket.

A rendszer és kistestvérei már Magyarországon is üzemben vannak. Szinte egyszerre jelent meg a piacon két elektronikus könyvkiadó. Az egyik a Cyber War összes nehézfegyverét felvonultatta. Ott van például az Adobe E-book nevű disztribúciós szervere, amely olyan védelemmel látja el a megvásárolt elektronikus könyveket, hogy azok csakis a letöltő gépén olvashatók. Az természetesen nem zavarja hősünket, hogy ezzel megszegi a szerzői jogi törvényt, mely szerint a könyvekről vagy tartalmuk egy részéről magán-, tudományos vagy oktatási célra másolat készíthető. Egy másik társaság komolyan veszi a tisztességet és a felhasználó olvasáshoz való jogát. A tőlük vásárolt elektronikus könyvek nemcsak megfizethetők, de bármelyik gépen olvashatók is. Hiszen a tisztességre építve a védelem nélküli Adobe formátumot alkalmazzák.

Vihar egy pohár vízben – mondhatnánk. De sajnos nincs így. Most járt errefele két szoftver – hosszas utánajárás után sikerült megszereznem –, és látható, hogy az elektronikus hálón megjelent hírnek van némi valóságalapja. A Microsoft két programcsomagját volt alkalmam megtekinteni egy osztrák tesztelő cégnél, és elmondhatom – az időközben már sajtótájékoztatón is bejelentett – tényt: a Microsoft alapjában megváltoztatja licencelési politikáját. Az új szoftverek jellegzetessége, hogy géphez kötik magukat. A telepítési eljárás során kapunk egy kódot, amit közölni kell a Microsoft illetékes egységével, ahol adnak egy arra a gépre érvényes válaszkódot. Így csakis abban a konfigurációban, azon a gépen használhatjuk a szoftvert. Ugyancsak ilyen típusú licencekkel kezdi majd több cég alkalmazásait forgalmazni.

Megjegyezendő, hogy ennek halovány előkísérletéből annak idején Magyarországon majdnem az adatvédelmi biztosig húzódó botrány lett, és a Microsoft mostanáig csak szűk körben, a Windows 2000 terminálszervereinél alkalmazta ezt a megoldást.

Más vállalatoknál a „piszkos trükkök osztályain” újabb módszereken dolgoznak. A cél a tartalom megjelölése, géphez kötése, a felhasználó leszoktatása a számítástechnikáról. Használja az infoközművet, és fizessen. A gép egyesek szerint túl jól sikerült, ideje elfelejteni. De a Net rejtett gerillabázisain meghúzódóknak még valószínűleg lesz pár szavuk ehhez.

A Cyber War folytatódik. Pedig még csak a csapatok és a fegyverek felvonulásánál, a hírszerzők telepítésénél tartunk. A haditörvénykezés azonban már életbe lépett.

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

E-mail: **johannes@mail.datanet.hu.**

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