WWW.IT-SECURITY.HU

III. ÉVFOLYAM 7. SZÁM 2006. SZEPTEMBER 19.

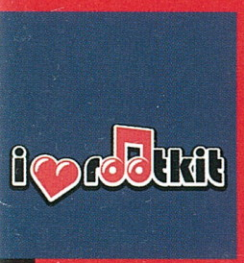
# IT-SECURITY

AZ INFORMATIKAI BIZTONSÁG LAPJA

IT-SECURITY SPECIAL

AZ INFORMATIKAI BIZTONSÁG NAPJA

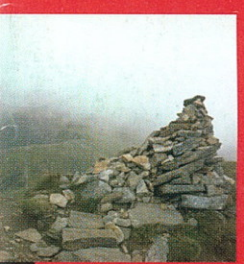
AZ IT-BUSINESS MELLÉKLETE




20. OLDAL

## Aki bújt, aki nem...

Nehéz védekezés



27. OLDAL

## Titkok a levegőben

Kulcsok és frekvenciák

30. OLDAL

## A törvény szava

E-számlák, feltételek, kötelmek

# Szigorúan ellenőrzött honlapok

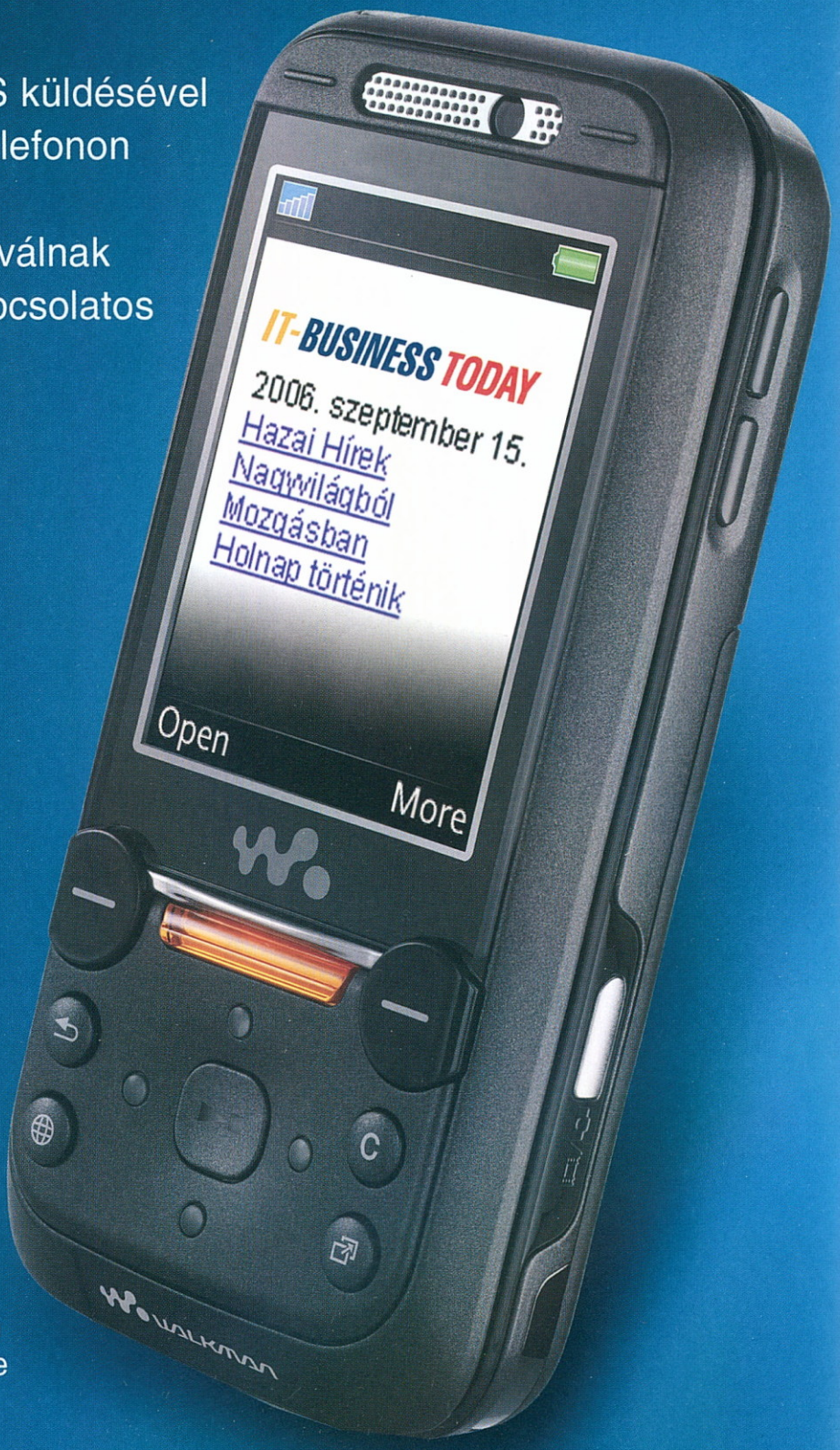
Monitorozás, szűrés, cenzúra, blokkolás

14. oldal

# IT-BUSINESS TODAY

# goes mobile ...

Az IT-BUSINESS TODAY SMS küldésével WAP rendszerben már mobiltelefonon is elérhető, így számítógép segítsége nélkül is elérhetővé válnak a legfontosabb ICT-piaccal kapcsolatos hírek, történések, események.




**Próbálja ki most!**

Küldje el az ITBTODAY szót SMS-ben a +36 30 285 5441 számra és kövesse az instrukciókat!

WAP cím: **wap.it-business.hu**

# TOLERANCIA

***Az internet olyan platform, ahol az üzleti élet és a magánszféra békésen megfér egymással.***

Statisztikák szerint a munkaidő közel fele magáncélú internetezéssel és a világhálóval kommunikáló alkalmazások használatának jegyében telik.

Érthető hát, ha a munkáltatók gyakran „bekeményítenek": letiltják az üzenőrendszerek használatát, P2P-alkalmazásokat, korlátozzák az interneten elérhető információk körét.

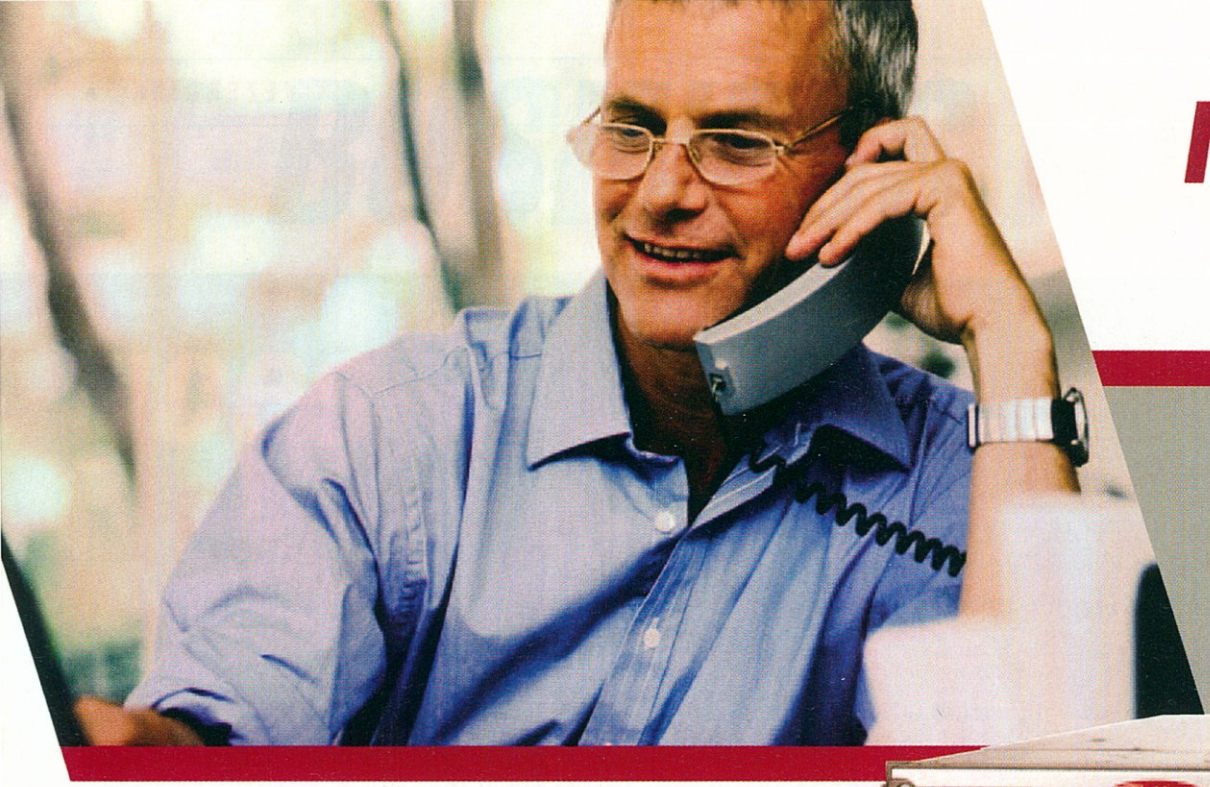
Ahhoz már hozzászoktunk, hogy a reggeli kávézgatás vagy az ebédet követő ejtőzés idején sok kolléga képernyőjén valamilyen internetes újság cikke villódzik. Újabban pedig az iwiw-es ismerősvadászat és üzengetés is a munkalyi relax kategórájába tartozó bocsánatos bűn. S ha valaki rákeres arra, hogy egy-egy nagyember mikor is járt utoljára fenn az iwiw-en, érdekes dolgokat tapasztal…

Mindezt a magam részéről gond nélkül tolerálom, nem látok benne semmi kivetnivalót, hisz a napunk nagy részét úgyis munkahelyi környezetünkben töltjük. Hát akkor az ilyen kedélyjavító dolgoktól nem kéne megfosztani a kollégákat! Az azonban már arcátlanság, amikor egyesek visszaélnek az internetkapcsolattal, s „megeszik" a sávszélességet. Nem hinném, hogy a munkahelyi közegben elfogadható, ha valaki zenéket, filmeket, programokat tölt le, (szerencse)játszik, felnőttoldalakat nézeget… Az ilyen típusú tartalmak monitorozása, szűrése, blokkolása, kizárása egy másodpercig sem fáj, s nem érzem, hogy alapvető emberi vagy alkotmányos jogaiban sérülne bárki, akinek ezek a webes tartalmak munkahelyi közegében nem érhetők el.

És hogy milyen technológiákkal válnak szigorúan ellenőrzöttekké a honlapok, megtudhatják e havi címlapos összeállításunkból.

Sziebig Andrea

**Sziebig Andrea**
*főszerkesztő*



McAfee®
Proven Security™

## A fenyegetés:

- 2005-ben a veszélyes támadások 85 százaléka az interneten vagy e-mailen keresztül terjedt
- A kémszoftverek száma és az általuk okozott károk költsége féktelenül nő
- Az e-mailek 75 százaléka spam
- A helytelen web-böngészés rontja a hatékonyságot
- Az adathalászat már nagyvállalati probléma, mert a dolgozók esetleges reagálása védtelenné teheti a hálózatot

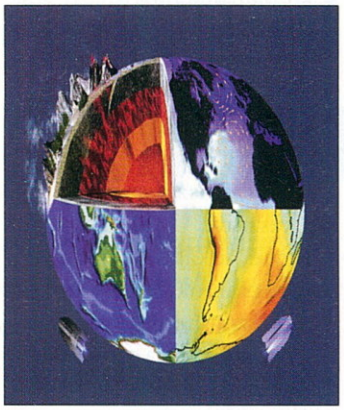
## A megoldás:

**A McAfee Secure Content Management (SCM) megoldások képesek megállítani a támadásokat, még mielőtt azok bejuthatnának a rendszerbe:**

- Antivírus modul (teljes körű védelem a web- és e-mail alapú támadások ellen)
- Anti-Spyware modul (egyedülálló kémprogram kereső, a Network World Magazin "legjobb az iparágban" díjának nyertese)
- Webszűrő modul : káros tartalmú honlapok böngészésének korlátozása egyedi és előre definiált szabályok kikényszerítésével akár felhasználók szintjén is
- Anti-Spam modul (védelem a spam és az adathalászati kísérletek ellen)
- A McAfee ePolicy Orchestrator segítségével az alkalmazások központilag kezelhetők, az asztali gépektől az átjárókig

A McAfee Képviseleti Iroda elérhetőségei: +36 30 9679 040 Arpad_Toth@McAfee.com
+36 20 9711 320 Tamas_Barna@McAfee.com
www.mcafee.hu

## TERMÉKHÍREK




6 A helyzet változatlan
6 Pénzmosás ellen
7 Neten futó programok
7 Hamis biztonság
7 Webnapló a férgekről
8 Hitelesítés pecséttel
8 Együtt könnyebb
9 Becsapós helyek
9 Kínálatbővítés
10 Laza azonosítás
10 Lapkafüggő vírus
11 Automatizált megfeleltetés
11 E-mailek borítékban


## MEGKÉRDEZTÜK


12 Talált, süllyedt!
*Papp Péter,* a Kancellár.hu ügyvezető igazgatója


## CÍMLAPON


# Szigorúan ellenőrzött honlapok

***Törvényességi és kulturális okok; politikai és vallási szempontok... Környezettől függően számos megfontolás miatt lehet szükség a netes forgalom monitorozására, szűrésére és blokkolására. Nem utolsósorban például azért is, mert sok esetben zsebre megy a játék. A nemkívánatos tartalmak súlyosan veszélyeztethetik a szervezetek rendszereinek biztonságát vagy a szellemi javaikat.***

14. oldal

## ESZKÖZTÁR


20 Aki bújt, aki nem...
A felhasználói szint kevés

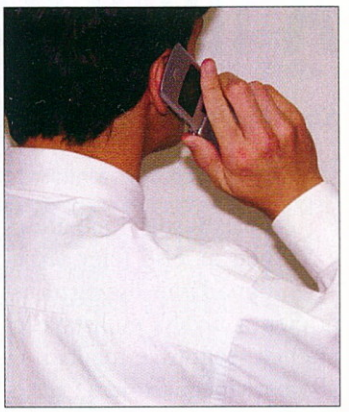
22 Elhanyagolt e-számlák
Az üzlet sava-borsa

24 Hibajelentés
Mozgalmas uborkaszezon


## IT-SECURITY SPECIAL AZ INFORMATIKAI BIZTONSÁG NAPJA


32 Fontos vélemények
33 Hálózaton az adatot
34 Kipipált kockázat
35 Megmondom, ki vagy!
36 Javuló biztonság
37 Az első lépés a legnehezebb


## KOMMUNIKÁCIÓ




26 Ellopott beszélgetések
Az IP-telefónia kockázatai

27 Titkok a levegőben
Bonyolult kulcsok, változó frekvenciák

28 Bluetooth: legendák és tények
Túldramatizált veszélyek

30 A törvény szava
E-számlák: feltételek és kötelmek


## MENEDZSMENT



39 Eseménynaptár
39 Oktatás, tanfolyamok
40 Az ITIL és a biztonság
Mit fed le?

41 Hálózatban az alvállalkozók
Könyvajánló

42 Mit olvas a szakértő?
Evangelizáció

# A helyzet változatlan

*Szemezgettünk a biztonsági cégek szokásos félévi jelentéseiből.*

A VirusBuster jelentésében az első félév vírustámadásait összegző lista élén a tavalyi év listavezetőjének számító, e-mailben és állománymegosztókon terjedő I-Worm.Zafi.B féregprogram végzett, amely a támadások 30 százalékáért felelős. A második helyre 28,5 százalékkal az online jelszavak begyűjtésére specializálódott HTML.Bayfraud trójai került, amely tavaly még csupán a 8. helyet foglalta el.

A fertőzések közel 60 százalékát okozó két programkártevő olyan hírhedt bűnözőket szorított háttérbe, mint a Lovegate.AL és a MyDoom.R férgek, amelyek 2006 első félévében a lista 8. és 11. helyére estek vissza, és az összes támadásnak csak alig másfél százalékáért okolhatók.

Az F-Secure értékelése szerint az év első fele látszólag csendes volt IT-biztonsági szempontból, ennek ellenére számos új programkártevő jelent meg. Januárban „ünnepelhettük" az első számítógépes vírus, a Brain 20. születésnapját, jelenleg pedig már több mint 185 ezer vírust tartanak nyilván. Míg kezdetben a vírusírók kedvtelésből terjesztették a rosszindulatú kódokat, manapság a legtöbb kártevőt haszonszerzési célból készítik.

www.virusbuster.com
www.f-secure.com

Egyre inkább terjednek a botprogramok, amelyek a fertőzött számítógépeket távolról irányíthatóvá alakítják, s ezt spamüzenetek és adathalászati célú levelek terjesztésére használják, olvashatjuk az F-Secure jelentésében.

**Tóth István**

## PÉLDÁS BÜNTETÉS

Három év börtönre ítéltek egy férfit az Egyesült Államokban, és 250 ezer dolláros kártérítés megfizetésére kötelezték, mert több tízezer számítógép ellen intézett támadást. Pechére a gépek egy részének az amerikai Védelmi Minisztérium adott otthont. *Christopher Maxwell* és két meg nem nevezett bűntársa az ellenőrzésük alá vont számítógépekből álló, nagyméretű bothálózattal adwareeket telepítettek más gépekre, és ezek révén több mint százezer dollárnyi haszonra tettek szert. Maxwell volt a második bothálózat-építő, akit elítéltek az Egyesült Államokban.

# Pénzmosás ellen

*Drogkereskedelem, fegyvercsempészet.*

A törvénytelen cselekedetekre utaló összegek nyomon követése és a pénzmosás felderítése a nyomozó hatóságok és a pénzintézetek közös feladata. Ma már a szabályozás is szükségessé teszi az informatikai eszközök használatát: az Európai Unióban januárban lép életbe az amerikai szabályozást követő Európai Pénzmosás Elleni Direktíva.

www.sas.com/hungary

Csakhogy a pénzmosás leleplezése korántsem olcsó: az Egyesült Királyságban eddig összesen 40 millió euró tisztára mosását leplezték le, ám a felderítés költségei ennek több mint tízszeresére rúgtak. A bankok mégsem nézhetik a megtérülés költségeit, hiszen a bizalom a legfőbb tőkéjük.

A gyanús ügyletek gyors, hatékony felderítésére a pénzintézetekben olyan üzletiintelligencia-megoldásokat vezetnek be, mint például a SAS Anti-Money Laundering szoftvere. A hatékonyság ebben az esetben azt jelenti, hogy a nyomozó hatóságok valóban csak a pénzmosást rejtő ügyleteknek eredjenek a nyomába; ha túl nagy volna a gyanúsnak ítélt tranzakciók száma, az hátráltatná a munkájukat.

*A leleplezés sem olcsó*

**Kelenhegyi Péter**

# Neten futó programok

***Az online alkalmazások gyors ütemű terjedése biztonsági problémákat vet fel.***

Sebezhető az internetre kapcsolódó számítógépünk, támadás érheti a mobiltelefonunkat, miért lennének abszolút biztonságosak az egyre népszerűbb online alkalmazások, amelyek piacán ádáz küzdelmet folytat a hagyományos szoftverek legnagyobb gyártója, a Microsoft és a keresőszolgáltatása révén internetes nagyágyúvá fejlődött Google?

És valóban, az aggodalmak jogosak: a SANS Institute legutóbb közzétett jelentésében több mint 60, a webes alkalmazásokban felfedezett új sérülékenységről számol be. Igaz, a két óriáscég alkalmazásai nem szerepelnek a listán, vagyis úgy tűnik, a webes fejlesztéseknél komolyan ügyelnek a biztonságra.

Egy másik, nem elhanyagolható biztonsági kérdés, hogy vajon rábízhatjuk-e bizalmas dokumentumainkat egy online alkalmazásra, nem élnek-e vissza a birtokukba jutott információkkal a szolgáltatók? A bizalom kialakulásához nyilvánvalóan idő kell, és lesznek majd olyan esetek, amikor illetéktelen kezekbe kerülnek adatok. De az is nyilvánvaló, hogy a rájuk bízott információkat mostohán kezelő vállalkozások gyorsan lehúzhatják majd a rolót, és csak a megbízhatóak maradnak a piacon.

**Tóth István**

www.sans.org

## HAMIS BIZTONSÁG

Egy kezdő nagy-britanniai vállalkozás olyan böngészőt fejlesztett ki, amely a szörfölési menet minden nyomát automatikusan eltünteti. Így nem lesz előzmények lista, továbbá nem tárolódnak cookie-k és a keresőmezőkben megadott kulcsszavak.

A Browzar névre hallgató, mindössze 264 kilobájtos programot még telepíteni sem kell, futtatásához elég, ha kattintunk kétszer az .exe állományon. Használatához olyan, legalább a Windows 98-as változatát futtató számítógép szükséges, amelyen telepítve van az Internet Explorer 5.5-ös vagy frissebb kiadása (tervezik maces és linuxos verzió elkészítését is). Amennyiben USB-memórián tároljuk, idegen gépeken is biztonságosan szörfölhetünk vele. A biztonsági szakértők vizsgálatai szerint a program kevesebbet nyújt, mint amennyit ígér, ráadásul meghamisítja az internetes keresések eredményeit, és kéretlen reklámokat is terjeszt. Kiderült még, hogy a Browzar nem önálló böngésző, hanem csak egy „átszabott takaró" az Internet Explorerhez.

# Webnapló a férgekről

***Nyilvános weblogot indított a biztonsági fenyegetésekről a Trend Micro.***

Néhány perccel az informatikai biztonságot fenyegető események, fertőzések megjelenése után már olvashatók a szakemberek megelőzéssel, javítással kapcsolatos jegyzetei a Malware Blogon. A portálon található naptárban piros szín jelöli azokat a napokat, amelyekhez vírusfenyegetés, újabb biztonsági rés felfedezése vagy éppenséggel frissítés megjelenése fűződik.

http://servicecenter.antivirus.com/malwareblog/diary/

A TrendLabs kutatóinak gyakorlati útmutatói a megjósolhatatlan fenyegetések elleni védekezésben segítenek az átlagos felhasználóknak és az informatikai biztonsággal foglalkozó szakértőknek.


*Piros napok a naptárban*

Például az adathalászokat segíthetnek leleplezni a hamis címre csábító levelek képei.

**Kelenhegyi Péter**

# Hitelesítés pecséttel

*Újabb módszereket kénytelenek bevetni a webes szolgáltatók a csalók ellen.*

Az adathalászok elleni védekezésül a bejelentkezést hitelesítő pecsét bevezetését tervezi a Yahoo, amely biztosítja majd az előfizetők számára, hogy valóban a népszerű webportált látogatják meg, nem pedig annak hamisítványát. A biztonsági szolgáltatást egyelőre csak az előfizetők véletlenszerűen kiválasztott csoportjának ajánlják majd; a pecsétet a későbbiekben fokozatosan terjesztik ki az egész közösségre.

Az előfizetők által elkészítendő pecsét minden egyes alkalommal megjelenik, amikor az előfizető felkeresi valamelyik Yahoo-szolgáltatás bejelentkező képernyőjét. A számítógéphez kötődik, így még a felhasználói azonosító és a jelszó begépelése előtt feltűnik a képernyőn.

www.yahoo.com

Tóth István

## MOBILVESZÉLYEK

Új csalási módszerre, a SMiShingre (phishing támadás sms-en keresztül) figyelmeztette a mobiltelefonok használóit a McAfee. A mobilozókat úgy próbálják meg lépre csalni a hackerek, hogy szöveges üzenetben egy webcímet küldenek nekik. Ha az emögött található weboldalt meglátogatják, készülékükre egy trójai töltődik le, amelynek révén a támadó átveheti az ellenőrzést a mobiljuk felett. Szakértők szerint az új típusú támadás kétségtelen jele annak, hogy a mobiltelefonok és más hordozható informatikai eszközök egyre inkább a csalók célpontjává válik.

# Együtt könnyebb

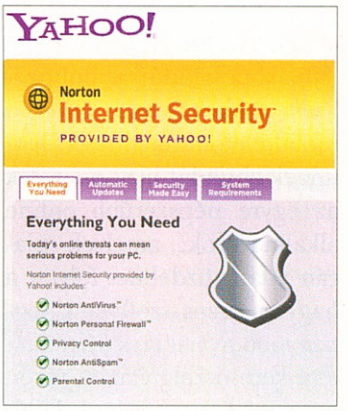
*Az internetes szolgáltatók és a biztonsági cégek összefogása hatékonyabbá teszi a védelmet – a tesztváltozat használatát vásárlás követheti.*

Ösztönző lehet egy portál látogatói számára, ha kedvenc webhelyükön számítógépük biztonságát növelő eszközökhöz juthatnak hozzá.

A Yahoo nemrégiben megegyezett a Symanteckel, hogy webportálján, valamint a Yahoo Mail levelezőszolgáltatás, a Yahoo Toolbar eszköztár és a Yahoo HotJobs álláskereső segítségével terjeszti a biztonsági cég Norton Internet Security csomagját és más szoftvereit. A látogatók letölthetik a tűzfalat, valamint a képprogram-, vírus- és spamellenes modult tartalmazó Norton Internet Security 30 napos tesztváltozatát, amit a próbaidő lejárta után 50 dollárért megvásárolhatnak.

www.yahoo.com
www.symantec.com

Az együttműködés keretében kínált további szolgáltatások között megtalálható a Yahoo Toolbarról indítható képprogram-keresés, a Norton Spyware Scan for Yahoo Toolbar, a biztonsági eszközökhöz gyors hozzáférést kínáló, közös márkajelzésű Symantec Yahoo Toolbar, valamint a Norton AntiVirust és a Norton Personal Firewallt bevető, internetes kapcsolaton keresztül futtatható Yahoo Online Protection.




*Ösztönző eszköz*

# Becsapós helyek

***Haszonszerzési céllal ismert cégek címeihez hasonló doménnevű webhelyeket létesítenek a hackerek.***

Két polgári pert indított az Egyesült Államokban a Microsoft négy magánszemély ellen, akik az általa használt doménnevekhez hasonlító webcímekkel követtek el csalásokat. Összesen 409 doménnevet jegyeztettek be, közöttük olyanokat, mint például freehotmail.net, windowshome.info és 1microsoft67.info.

Ezekre a címekre az óvatlan netezők elgépeléssel vagy keresőkön keresztül juthattak. A doménnevek bejegyeztetésével a négy férfi megsértette az 1999-ben elfogadott Anticybersquatting Consumer Act nevű törvényt, amely kifejezetten tiltja az ilyen tevékenységet. Az illegálisan létrehozott weboldalakon az elkövetők hirdetéseket helyeztek el, amiből bevételük származott.

www.windowsonecare.com

Ugyancsak a redmondi céggel kapcsolatos hír, hogy OneCare nevű, alacsony áron kínált biztonsági csomagjukkal az értékesítés első hónapjában 15 százalékos részesedést szereztek az amerikai kiskereskedelmi piacon, ami a második helyet jelentette számukra. A vírusellenes programot, automatikus tartalékmásolat-készítő modult, személyi tűzfalat és PC-karbantartó segédprogramokat tartalmazó terméket az Egyesült Államokban csupán 50 dollárért kínálják.

A siker leginkább a Symantecet érintette, amelynek piaci részesedése a májusi 69,9 százalékról júniusban 59,8 százalékra csökkent.

Egyébként a OneCare augusztus végén új szolgáltatással bővült: az egyelőre csak az Egyesült Államokból elérhető OneCare Family Safety a web szűrésével valósít meg szülői felügyeletet, a szörfölési menetekről pedig részletes jelentést készít.

**Tóth István**

## KÍNÁLATBŐVÍTÉS

Részvényenként 28, összesen 1,3 milliárd dollárért vásárolta meg az IBM a biztonsági szoftverek készítésével és tanácsadással foglalkozó Internet Security Systemset (ISS-t), amely a továbbiakban a Kék Óriás Global Technology Services nevű outsourcing-részlegét erősíti majd.

Az IBM illetékesei szerint az akvizícióval a cég tovább bővíti kínálatát a biztonsági technológiák és szolgáltatások növekvő piacán.

Az ISS termékei között megtalálható Proventia hálózatvédelmi és RealSecure kiszolgálóvédelmi szoftver jól kiegészíti az IBM-féle Tivoli infrastruktúra-kezelő és biztonsági termékcsaládjának tagjait, amelyek főként a végpontok biztonságára összpontosítanak. Arról egyelőre nem érkezett hír, hogy az IBM árusítani fogja-e külön termékekként az ISS szoftvereit és berendezéseit.

# Laza azonosítás

*Többnyire egyszerűbb módszerekkel érik el céljukat.*

A vállalati hálózatba bejelentkező felhasználók jogosultságának azonosítása minden más biztonsági intézkedésnél fontosabb – derül ki a BIOS-fejlesztő Phoenix Technologies által megrendelt kutatásból, amely az amerikai bíróságokon 1999 és 2006 között tárgyalt ügyek

www.phoenix.com

adatain alapul. A céges hálózatok elleni támadások több mint 80 százaléka elkerülhető lenne, ha nem csupán a felhasználót azonosítanák, hanem azt a számítógépet is, amellyel az illető be akar jelentkezni a hálózatba. Az ellopott vagy más módon megszerzett felhasználói azonosítókkal történt behatolások a vállalatoknak átlagosan sokkal több – 1,5 millió dolláros – kárt okoztak, mint a féreg- és vírustámadások, amelyek átlagosan 2400 dollárnál kevesebbe „kerültek".

Az azonosítókhoz jelszófeltörő programokkal és az alkalmazottakkal való összejátszással jutnak a bűnözők. Dolgukat megkönnyítik az olyan felelőtlen cselekedetek is, mint például az azonosítók megosztása más kollégákkal, ha ugyanis ezek később sértődötten távoznak a cégtől, a birtokukban lévő információkat hackereknek adhatják át, vagy maguk kísérlik meg a behatolást a hálózatba.

A tanulmány szerint a behatolók és a megtámadott cég viszonyát tekintve a támadók 60 százaléka semmilyen kapcsolatban nincs áldozatával, és csupán 36 százalékuk kerül ki a vállalat jelenlegi vagy volt alkalmazottai közül. Ez a megállapítás ellentmond más kutatásoknak, amelyek többsége szerint a belülről indított támadások száma lényegesen meghaladja a külső behatolásokét.

**Tóth István**

## LAPKAFÜGGŐ VÍRUS

Bizonyító hatású (proof of concept) vírust fedeztek fel a Symantec kutatói.

A két változatban létező, w32.bounds és w64.bounds elnevezésű férgek nem operációsrendszer-specifikusak, kifejezetten a 32, illetve 64 bites AMD processzorokra épülő rendszereket veszik célba.

Az első hírek utáni alapos vizsgálatok során kiderült, hogy a probléma az Itanium IA64 rendszerek kivételével az Intel alapú platformokat is érinti – hangzottak az első állásfoglalások.

# Automatizált megfeleltetés

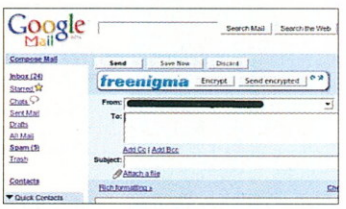
*A kockázatok elemzésével növelhető a védelem hatékonysága.*

Biztonsági termékválasztékának teljesebbé tétele érdekében két új terméket mutatott be a McAfee. A prioritáson alapuló sérülékenységkezelő Foundstone Enterprise 5.0, valamint a megfelelőség-ellenőrző és kockázatelemző Preventsys Compliance Auditor and Risk Analyzer használatával a vállalatok automatizálhatják a biztonsági megfelelőségekről szóló jelentéskészítést. A fejlesztő szerint a Foundstone Enterprise 5.0 segítségével rangsorolni lehet a legértékesebb üzleti tulajdonokat, ezt követően pedig meghatározhatók azok legkritikusabb biztonsági sérülékenységei, valamint az ezeket kihasználni képes fenyegetések.

www.mcafee.com

Az ilyen információk alapján a vállalatok a szükséges erőforrásokat a megfelelő területekhez tudják rendelni, és a program automatikus jelentéskészítő funkciójával csökkenthetik az informatikai működési költségeket.

A Preventsys Compliance Auditor a Foundstone adataiból, valamint a vállalati biztonsági elvekből és szabványokból állítja össze a megfelelőségi jelentést. Megvalósítja az irányelvek központosított ellenőrzését, így csökkenthetők a biztonsági megfelelőség kimutatásával összefüggő kiadások.




*Tulajdonrangsor*

## E-MAILEK BORÍTÉKBAN

Az internet végtelen útvesztőiben bolyongó elektronikus levelek a boríték nélküli levelezőlapokhoz hasonlíthatók: tartalmukat semmi sem védi az illetéktelen szemektől. Szerencsére van megoldás, az egyelőre igen kevesek által alkalmazott titkosítás.

Német fejlesztők most ingyenes titkosító plug-int készítettek webmailes alkalmazásokhoz.

A Firefoxhoz telepíthető Freenigma többek között a Yahoo Mailhez, a Gmailhez és a Hotmailhez használható, s igen egyszerűen kezelhető felhasználói felülettel szerelték fel. A szolgáltatás használatához a program webhelyén lehet regisztrálni. A titkosított levelek címzettjeinek ugyancsak regisztrálniuk kell magukat.

www.freenigma.com
www.mozilla.org

FOTÓ: IT-SECURITY

**Papp Péter,**
**Kancellár.hu**

# Talált, süllyedt!

***Sok cég szinte mindent megtesz azért, hogy weblapjára felhívja az internetezők figyelmét; ennek egyik legjobb módja, ha előkelő helyen szerepel a nagy keresők, elsősorban a Google találati listáján. A Google azonban sok olyasmit is tudhat rólunk, amit még csak nem is gyanítunk.***

***– Mi teszi veszélyessé a keresőket?***

– Az ilyen oldalak automatikus keresőrobotjai rendszeres időközönként – általában ötnaponta – „végigkúsznak" a teljes interneten, és a belsőleg fejlesztett algoritmusuk szerint tárolják a megtalált dokumentumokat. De itt nem is a módszer az igazán érdekes, hanem annak az eredménye: ami egyszer felkerült a nyilvános internetre – akár szándékosan, akár véletlenül –, az előbb-utóbb bekerül a keresők, így a Google adatbázisába.

*Gyakori, hogy semmit sem változtatnak a gyári beállításokon*

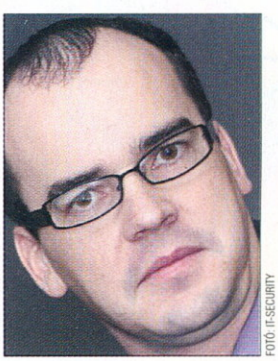
***– Miért pont a Google-ra kell a legtöbb figyelmet fordítani, hiszen azon kívül is vannak komoly keresők?***

– Ma vitathatatlanul a Google a legnépszerűbb kereső a világhálón, és nem véletlenül lett azzá. Komoly újítása volt a „page ranking" bevezetése, ami a talált oldalak relevanciájának sorrendjét határozza meg. A korábbi keresők azt az oldalt jelenítették meg elsőnek, amely a legtöbbször tartalmazta a keresett szót. A Google-nál viszont az lesz az első, amelyre a legtöbb oldal hivatkozik, ráadásul a hivatkozó oldalak is súlyozva vannak fontosság szempontjából.

A találati arányokat lehet legális és illegális módszerekkel is javítani; ez utóbbiak közé tartozik például, ha a háttér színével megegyező betűkkel, vagyis az olvasó számára láthatatlanul szerepelnek a szavak az oldalon. De a Google nagyon keményen fellép a csalók ellen, és előfordult, hogy a BMW német lapjait tette elérhetetlenné a keresőben meg nem engedett módszerek használata miatt.

***– Azt hihetnénk, hogy a vállalatok, szervezetek nagyjából tudják, hogy milyen anyagokat tesznek nyilvánosan elérhetővé.***

– Ez sem mindig van így. A modern rendszerek – legyenek azok komoly nyomtatószerverek, faxszerverek, nagyobb útválasztók – már mind kapcsolódnak az internetre. Ráadásul telepítésük is gyakran webes felületen keresztül zajlik, nagyon egyszerűen üzembe állíthatók. Az egyszerű telepítés sajnos azt is jelenti, hogy az esetek nagy részében semmit sem változtatnak a gyári beállításokon. Pedig rendkívül fontos lenne, hogy „keményítsenek" az eszközökön és biztonságosabbá tegyék őket, mert nagyon sok információt árulnak el magukról.



FOTÓ: IT-SECURITY

Ezeket az információkat a Google ugyanúgy felderíti és tárolja, mint mondjuk a hírportálok dokumentumait, ami ugye azt is jelenti, hogy egy alaposabb kereséssel ezekhez az információkhoz is hozzá lehet jutni.

***– Mennyire nehéz megtalálni ezeket az információkat?***

– Az átlagember csak úgy használja a Google-t, hogy beírja az ablakba a keresett szót, és elindítja a keresést, pedig a Google ennél sokkal többre képes. Közel kéttucatnyi kifejezéssel, operátorral lehet finomítani, pontosítani a keresést. A *hacker* szóra keresve a világ minden tájáról hoz találatokat, de ha azt írjuk be, hogy *hacker site:hu*, akkor csak a magyar (.hu végződésű) oldalakon talált eredményeket jeleníti meg, de ezt továbbvihetem úgy is, hogy *hacker site:kancellar.hu*, és akkor csak a Kancellár.hu weblapján keres. Ha azt írom be, hogy in*url:hacker*, akkor csak azokat az oldalakat jeleníti meg találatként, amelyeknek az URL-címében szerepel a hacker szó. De lehet használni az ÉS, VAGY és egyéb logikai operátorokat is. Mindezek le vannak írva a Google Súgójában (www.google.com/help/operators.html), tehát viszonylag egyszerűen elsajátítható az összetett keresés tudománya is.

***– Mi mindent lehet így felderíteni?***

– Néha egészen meglepő dolgokat; nekem már sikerült találnom például védtelen routert is. Az egyéni felhasználók között az egyik legelterjedtebb gyártmány a Linksys, nekem is ilyen van otthon. Ezeket böngészőn keresztül lehet menedzselni, azon keresztül lehet elvégezni minden beállítást. A saját routerem kezdőlapjára lépve kimásoltam egy hosszabb magyarázó szöveget, amelyet az egyik mező mellett találtam, és ezt illesztettem a keresőbe, idézőjelek közé, hogy a teljes kifejezésre rákeressen a Google.

Fel is jött egy találat, amelyre rákattintva máris bent találtam magam egy francia cég routerében. Itt gyakorlatilag láttam a cég belső hálózatának felépítését; ráadásul adminisztrátori jogosultságaim voltak, vagyis akár lekapcsolhattam volna a routert, átállíthattam volna a MAC-szűrőt, és így tovább. Ugyanezt el lehet játszani komoly nagyvállalati útválasztókkal is.

De ilyen módon csatlakozni lehet nyomtató- és faxkiszolgálókra például, azokon pedig látszik, hogy ki mit nyomtatott legutóbb, mit és kinek faxolt, honnan jött fax, és így tovább. Nem kell különösképpen ecsetelnem, hogy az ilyen információknak az avatatlan, pláne a rosszindulatú kezekbe kerülése mekkora kárt tud okozni bármelyik vállalatnak. Még nagyobb a potenciális veszély, ha a szabadon maradt kezelőfelületen keresztül valaki konfigurálni is tudja a rendszert.

Vagy egy másik nagy csoport a szünetmentes tápegységeké. Ezeket is böngészőn keresztül szokták konfigurálni, így rengeteg UPS kezelőfelülete érhető el a nyilvános interneten keresztül is. Magyarországon még nem terjedt el ugyan, de az intelligens épületek vezérlését is lehet webes felületen keresztül intézni, és ha ezt nem védik, akkor bárki le tudja például kapcsolni a villanyt az adott épületben, hogy az egyéb „csínyekről" ne is beszéljünk.

Egyre több a biztonsági kameraként működő webkamera, és ha ezeket „kint felejtik" a nyilvános interneten, akkor az általuk közvetített kép is hozzáférhetővé válik mások számára. Ezek a kamerák sokszor saját IP-címmel rendelkeznek, és bár talán sehonnan nem mutat rájuk hivatkozás, a címük alapján mégis megtalálhatók.

De lehet találni digitális fényképeket is. Minden fényképezőgép-márka meghatározott séma szerint nevezi el és rendezi mappákba a vele készített fotókat. Erre a könyvtárstruktúrára is rá lehet keresni a Google-ban, és máris találhatunk olyan fotókat is, amelyeket nem a nyilvánosságnak szántak.

Kipróbáltam azt is, hogy magyar weblapokon kerestem olyan pdf-állományokat, amelyek tartalmazzák a „szigorúan belső használatra" kifejezést. Meglepően

FOTO: IT-SECURITY

sok találat jött vissza. Ezek egy része csak publikus formanyomtatvány volt, de volt olyan intézmény, amely egy nyilvánvalóan belső használatra szánt dokumentumot kint felejtett a nyilvános hálózaton. Az URL nagyon összetett volt, vagyis egészen biztosan nem akarták, hogy más is lássa, de a weboldal mögött feltehetően egy olyan adatbázis áll, amiből elő lehetett varázsolni a dokumentumot. Ha pedig olyan Excel-állományokra keresünk rá, amelyek tartalmazzák az „Üzleti terv" kifejezést, akkor is számos találatot kapunk.

*Ne zökkenjünk ki a „normál paranoid" állapotunkból!*

***– De ha kiderül, hogy bizalmas anyag van kint, akkor a kérdéses weblapot vagy dokumentumot el is lehet távolítani, nem?***

– Az sem feltétlenül jelent megoldást, mert a kereső cache-ében még sokáig elérhető marad a kérdéses oldal. Arról nem is beszélve, hogy ami egyszer elterjed a világhálón, azt onnan nem lehet eltávolítani – gondoljunk csak a híresség botrányos képeire vagy videóira, amelyeket egymástól vesznek át a különböző webhelyek üzemeltetői.

***– Mindezek után mi lehet akkor a kárelhárítás módszere?***

– Ha észrevettük, hogy nemkívánatos anyagaink is elérhetőek az interneten, akkor lehet jelezni a Google-nak, hogy mely oldalakat, tartalmakat és milyen indokkal szeretnénk eltávolíttatni a keresőből. Ezt rendszerint el is fogadják, de az eljárás néhány napba is beletelhet.

***– Hogyan lehet elérni azt, hogy a bizalmas dokumentumok, oldalak fel se kerüljenek a Google oldalaira?***

– Az egyik legfontosabb dolog, hogy ne zökkenjünk ki a „normál paranoid" állapotunkból, és mindig nagyon ügyeljünk arra, hogy milyen anyagokat publikálunk a nyilvános webszerveren. Az a legjobb, ha a mindenki számára elérhető webhely különálló szerverre kerül, és arra csak azt tesszük fel, amit mindenkivel közölni akarunk.

Ezek után jöhet az ellenőrzés: meg kell nézni, hogy a Google mit tud rólunk. Erre szolgál az *info:* operátor: ennek használata esetén kiadja, hogy milyen információkat tárol a kettőspont után beírt weboldalról. De már kereskedelmi forgalomban is kaphatók olyan termékek, amelyek imitálják a Google keresőmotorjának működését, és így mutatják meg, hogy milyen információkat lehet kinyerni a nyilvános weboldalainkból. Tipikusan hozzáférhető információ szokott lenni a használt webszerver típusa és verziószáma; ezt is jobb eltitkolni, mert számos támadást könnyíthet meg, ha a hackerek tudomására jut ez az adat.

A gyökérkönyvtárban elhelyezhető egy robots.txt névre keresztelt szövegállomány is, amelyet a keresők értelmeznek. Meghatározott szintaxis szerint ebbe lehet felvenni azokat a mappákat (például a képeket tartalmazó könyvtárat), amelyeket ki akarunk zárni az indexelésből, és így a keresésből. No persze ezek után a robots.txt állományokban rá lehet keresni az erre a célra használt „Disallow:" szövegre is, hogy feltérképezzük, ki milyen könyvtárakat rejteget a fürkész szemek elől…

**Schopp Attila**

# Szigorúan ellenőrzött honlapok

***A világon a dolgozók tekintélyes hányada munkája során olyan folyamatos internetkapcsolattal rendelkezik, amelyet a munkáltató bocsát a rendelkezésére. Az internetelérést persze nemcsak a munkára lehet használni, hanem játékra és online szerencsejátékra; zenék, filmek programok letöltögetésére – „warezolásra"; saját ügyek intézésére és még sok olyan dologra, ami a vállalatnak nem jó.***

A legtöbb szervezetnél tisztában vannak azzal, hogy az alkalmazottak nemcsak élhetnek, de vissza is élhetnek az internetelléréssel, ezért keresik azokat az eszközöket, amelyekkel elejét vehetik a dolgozók tobzódásának. Az internetszűrő rendszerek vagy sok más elnevezés mellett webszűrőként, filterware-ként, illetve némi pejoratív felhanggal censorware-ként – és sok más néven – is emlegetett technológiák célja a tartalom és különösen a HTTP-protokollal letölthető, böngészhető webes tartalom szűrése bizonyos szempontok szerint. Ezek az eszközök döntik el, hogy a felügyelt gépen vagy hálózaton milyen internetes információ érhető el.

A szűrés motívuma környezettől függően igen sokféle lehet. Ugyanígy igen szerteágazóak lehetnek az okokkal összefüggésben a felügyelt tartalmak. Bár a tartalomszűrőknél nem az internetelérés teljes blokkolása az elsődleges cél, de adott esetben erre is alkalmasak.

## Ki, mit, miért és hol szűr?

A különféle szervezetek, intézetek, vállalatok mellett a családok és otthoni felhasználók, sőt az országok és kormányok is igen sokféle okból használhatnak internetszűrést (történetileg valójában az egyedi, háztartási rendszerek léteztek először).

A családok esetében leggyakrabban a gyermekek számára káros oldalakkal gyűlik meg a szülők baja. Ebben az értelemben az internetszűrés a szülői felügyelet kiterjesztése arra az időszakra, amikor a csemete egyedül barangol az interneten. A „parenteral control" célú eszközök feladata a pornográf, erőszakos tartalmakat hordozó vagy a gyermekek számára más módon káros honlapok megtekintésének korlátozása. Hasonló okból használnak webfiltereket az oktatási intézményekben és könyvtárakban.

Az országok vagy kormányzatok több okból is működtetnek szűrőrendszereket, így az elektronikus kereskedelem és törvényesség betartatásának okán adózási, szerzői jogvédelmi szempontok, illetve a gazdaság védelme és más jogi szempontok miatt vagy az ifjúság védelme érdekében szűrhetik a pornográf és erőszakos tartalmakat.

Kifejezetten a tartalomra koncentrálva szűrni szoktak

- kulturális okból – például pornográf oldalakat vagy online szerencsejátékokat;
- politikai okból – a disszidensek és a független sajtó esetleges „káros hatásainak" a kivédésére;
- biztonsági okból – a (cyber)terrorizmus, a hackerek, internetes csalók és más bűnözők jelentette kockázatok miatt.

Az imént már említett törvényességi, üzleti és biztonsági okok mellett vállalati környezetben a fő motívumok:

- a nemkívánatos tartalmak nézegetése a munkaidő rovására megy;
- az internetkapcsolattal való visszaélés csökkenti a drága sávszélességet;
- a kifelé irányuló forgalom szűrése a bizalmas információk védelme miatt.

Környezettől függetlenül általános indok még azoknak a webhelyeknek a szűrése, amelyek kifejezett biztonsági kockázatot jelentenek (például phishing), vagy technológiai értelemben veszélyes tartalmakat, kártevőket (vírusokat, spywareeket) terjesztenek.

A szűrőtechnológiák implementációja erősen környezet- és helyfüggő. Lokalizáció alapján a fentieknek megfelelően három kategóriáról beszélünk:

*Környezetfüggő tiltás*

- a lokális szűrőmegoldások a családok, intézmények számítógépeire vagy publikus terminálokra telepített szoftverek;
- a szervezeti szűrők a munkahelyek, intézmények, internetszolgáltatók hálózati szűrői;

*Megzabolázott felhasználók*

- a nemzeti szűrők azok az állami ellenőrzés alatt álló technológiák, amelyek a gerinchálózat forgalmát felügyelik.

## A tágabb értelemben vett probléma

Szélesebb aspektusban nemcsak a böngészőkkel megtekinthető oldalakkal lehetnek gondok, hanem bármelyik olyan alkalmazással, amelyik kommunikál a világhálóval. A sávszélességet tekintélyes mértékben csökkentheti – vagy bármilyen tartalmi okból nemkívánatos lehet – a levelezés, az üzenőrendszerek használata, a P2P-alkalmazások és számos más szoftver. Mint említettük, a kifelé menő forgalom is hordozhat nemkívánatos tartalmakat. A bizalmas vállalati adatok kiszivárgása az egész kérdéskört a komplex biztonsági probléma szintjére emeli.

Összegzésképpen elmondható, hogy a statisztikák szerint a vállalati közegben a http-protokollal összefüggő problémák a tartalombiztonság tárgykörébe tartozó eseteknek csak mintegy 20–30 százalékát teszik ki; a visszaélések többi 70–80 százalékáért más alkalmazások felelősek.

## Néhány további megfontolás

Az internetszűrőket több helyen és többféleképpen lehet működtetni. Vállalati környezetben gateway-megoldásokat alkalmaznak. Ezek vagy szerverre telepíthető szoftverek, vagy előre telepített szoftverrel rendelkező célhardverek. Közös jellemzőjük, hogy a szűrő szabályrendszer kialakítása és az eszközfelügyelet a vállalat kezében van, így azonnal tud reagálni egy új fenyegetés ellen, valamint a működés során keletkező auditinformációkat fel tudja dolgozni. Természetesen léteznek külső féltől (gyakran magától a szolgáltatótól) igénybe vehető szolgáltatások is.

Noha legtöbben egyetértenek abban, hogy a szűrőmegoldások hasznosak, arról már sok vita folyik, hogyan kell őket használni és persze az ezzel kapcsolatos szervezeteken belüli szabályokról vagy egy ország viszonylatában a törvényekről is megoszlanak a vélemények. A szűrőszabályok mögötti morális és politikai megfontolások propagandisztikus célokat is szolgálhatnak. A szolgáltatók vagy éppen a szűrőmegoldások szállítói a törvények vagy saját megfontolásaik alapján felállíthatnak olyan megkerülhetetlen és kikapcsolhatatlan szabályokat, amelyek sokak számára elfogadhatatlanok lehetnek. Néha nem egyszerűen csak elfogadhatatlanok, hanem alapvető emberi vagy alkotmányos jogokat sérthetnek.

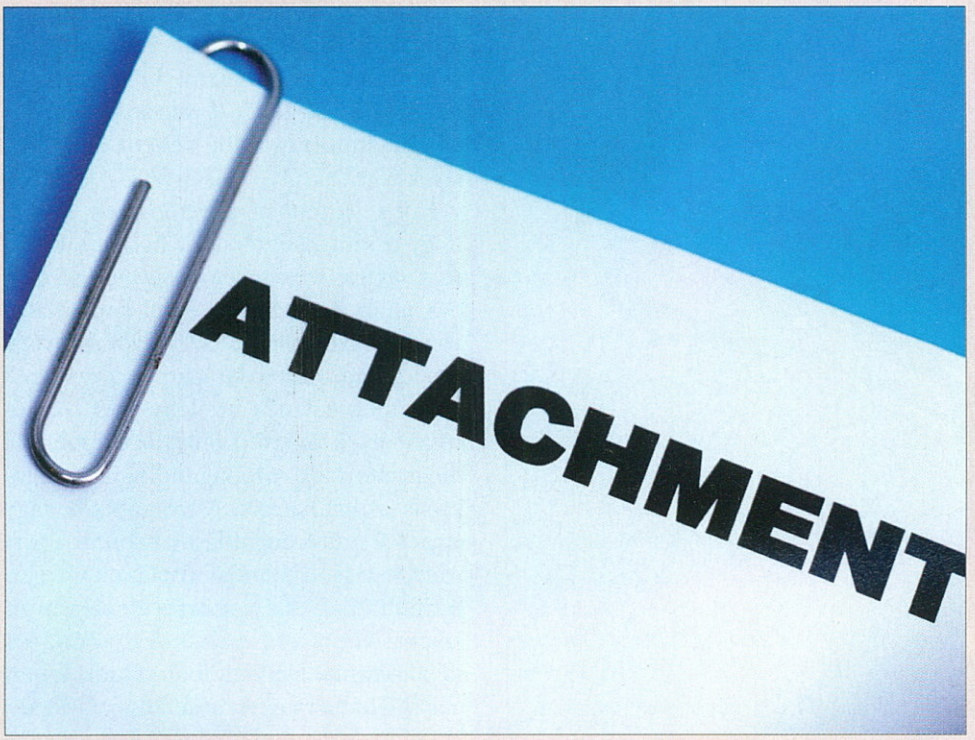
## Honlap- vagy URL-blokkolás

A webhelyeket blokkoló megoldások nem vizsgálják a webhelyről letöltött tartalmakat, ehelyett magának a webhelynek az elérését gátolják meg, innen az URL-blokkoló elnevezés. Minden oldallekérés átmegy egy ellenőrző ponton; ez lehet tűzfal, proxykiszolgáló vagy webes gyorstár-eszköz. A kérelem az adatcsomag fejléce alapján azonnal elbírálódik, és rögtön megszületik a verdikt a teljesíthetőségéről – persze közben az oldallekérés és a döntés naplózódik.

A blokkolórendszerek általában jókora, legalább 3–4 millió honlap adatait tartalmazó adatbázisokat használnak. Az adatbázis lehet inklúzós (megengedő, fehérlistás); ekkor a blokkolórendszer csak a tartalmazott URL-ek felkeresését en-

gedi meg. A gyakoribb exklúziós (kizáró, feketelistás) URL-blokkolók minden webhely felkeresését engedik, kivéve azokat, amelyek benne vannak az adatbázisban. Az URL-adatokat különböző szempontok szerint tekintélyes számú, akár 70–100 kategóriába (szerencsejáték, pornográfia, letöltőhely stb.) szokás szortírozni. Minden kategóriához hozzá lehet rendelni felhasználókat vagy felhasználói csoportokat.

A kérelmek lehetnek teljesíthetők vagy tilthatók, esetleg részlegesen tilthatók – időzítések, forgalmi kvóták vagy más szempontok alapján. A döntést támogató adatbázist a fejlett megoldásokban valamilyen rendszerességgel frissítik; az aktualizálás történhet kézzel vagy automatikusan.




*Védett állományok*

A blokkolómegoldásoknak vannak nyilvánvaló előnyeik és hátrányaik. A legnagyobb előny a teljesítmény, hiszen pillanatok alatt el lehet dönteni, hogy egy felhasználó vonatkozásában adott körülmények között egy oldallekérés teljesíthető-e, vagy elutasítandó.

## A blokkolás hátrányai

A becslések szerint hetente 3–5 millió közötti számú új honlap keletkezik. Vegyük hozzá azokat is, amelyeket valamiért átneveznek. Ezeknek az akkurátus követése egyszerűen lehetetlen. A hatalmas számok ellenére rendszeres adatbázis-aktualizálás mellett az URL-blokkolókkal el lehet érni a 90 százalékos pontosságot.

Igen nagy a hamis pozitív találatok száma, ami azt jelenti, hogy sok megfelelő vagy alapjában jó, de némi helytelen tartalmat is hordozó honlapra hivatkozó kérelem kerül elutasításra.

A hagyományos blokkolótechnológiák a HTTP alapú forgalomra koncentrálnak, így a levelező-, üzenő-, FTP- és más alkalmazások vidáman kikerülik őket, márpedig ez folyamatos biztonsági kockázatot jelent. Mint ahogy az is, hogy ezeknek a protokolloknak a kifelé irányuló forgalmára nincs korlátozás, pontosabban azt nem az URL-blokkoló, hanem a tűzfal felügyeli. Az újabb URL-blokkolók természetesen már más protokollokat is felügyelnek.

Az előző pontban leírt jelenség célzottan is kihasználható, azaz az alternatív protokollokba ágyazott HTTP-kérelmek alkalmas szervezeten kívüli szerver segítségével értelmezhetővé és kiszolgálhatóvá tehetők. Ehhez valójában a felsorolt protokollok sem szükségesek, hiszen az URL-szűrők az adatcsomag fejlécére koncentrálnak. A valódi lekérést HTTP-csomagba is bele lehet ágyazni, sőt valamilyen titkosítást is lehet használni.

A hamis negativitás (azaz teljesített helytelen oldalra vonatkozó kérelem) azt az álságos hitet plántálja a felhasználóba, hogy – mivel átment a rostán – a honlap jó és látogatható.

## Tartalommonitorozás és szűrés

A technológia kulcsjellemzője, hogy nem a forgalmi adatokra vagy az adatcsomag fejlécére koncentrál, hanem a kommunikáció tényleges tartalmára – „a tartalomra" –, ezért alkalmas a HTTP-forgalom, levelezés és levelek csatolmányai, üzenőrendszerek, Word, PowerPoint és bármilyen más alkalmazás kétirányú internetes kommunikációjának a felügyeletére.

A tartalomszűrés két területre koncentrál:

- az állománytípusok szűrésére és
- a szövegelemzésre.

Az állománytípusú szűrés a forgalomban utazó állományok jellemzőire (például fájl típusa, mérete) vonatkozó kritériumrendszer szerint engedi vagy blokkolja a forgalmat. Be lehet állítani például, hogy végrehajtható állományokat sem letölteni, sem e-mailben fogadni nem lehet, így olyan ártó szándékú prog-

## FOGALMAK

**AUP – Acceptable Use/Usage Policy.** Az elfogadható felhasználási szabályok gyűjteménye: az adott hálózat vagy rendszer használatára vonatkozó előírások.

**PICS – Platform for Internet Content Selection.** Az internetes tartalomválogató platform a W3C által készített specifikáció, amely metaadatokkal írja le az internetes honlapokat abból a célból, hogy azok elérhetősége ellenőrizhető legyen.

**RDF – Resource Description Framework.** Az erőforrás-leíró keretrendszer eredetileg a W3C XML alapú leírórendszere volt, később az információk modellezésére alkalmas általánosan használható módszerként terjedt el. Lényege, hogy a beszélt nyelvek alany–állítmány–információcsomag triászához hasonló struktúrában IT-eszközök által használható formában írja le az erőforrásokat, és mint ilyen, alkalmas az automata tudáskezelő rendszerekben való felhasználásra. Az RDF integrálja a PICS-rendszert, de annál általánosabb, ezért kézenfekvően nemcsak honlapok, hanem bármilyen információ kategorizálására alkalmas.

**UTM – Unified Threat Management.** Egységesített fenyegetéskezelő – általában olyan tűzfal alapú eszközt jelent, amely számos védelmi technológiát (vírus-, spam-, kémprogram-, behatolásellenes megoldások, URL-blokkolás és/vagy tartalomszűrés) egyesít egyetlen csomagban a hagyományos tűzfalfunkció mellett.

## KÉRDÉSEK ÉS VÁLASZOK A TARTALOMSZŰRÉSRŐL

**Kérdés:** a tartalomszűrés hatékony módszer-e a helytelen online tartalmak elérésére vonatkozó felhasználói aktivitás szűrésére vagy monitorozására?
**Válasz:** igen, sőt valójában ez a legpontosabb szűrőmódszer, mert nem az egész webhelyeket blokkolja, hanem csak az aktuálisan helytelen tartalmak azonosítására is alkalmas.

**Kérdés:** lehet-e a tartalomszűrő egy már telepített URL-blokkoló kiegészítője?
**Válasz:** igen; bizonyos vállalatok a hálózaton URL-blokkolást alkalmaznak, a munkaállomásokon pedig tartalomszűrőket az alkalmazások monitorozására – a kettő együtt növeli a biztonságot.

**Kérdés:** kiválthatja-e a tartalomszűrő az URL-szűrőt?
**Válasz:** igen, mert hatékonyabb és pontosabb megoldás.

**Kérdés:** lehet-e időzíteni a tartalomszűrés bizonyos vonatkozásait?
**Válasz:** természetesen elejét lehet venni a munkaidőben végzett internetes vásárlásoknak vagy bármilyen szezonális, nem munkával kapcsolatos tevékenységnek.

**Kérdés:** alkalmas-e a tartalomszűrés a felhasználók tevékenységéről szóló beszámolók készítésére?
**Válasz:** igen, sőt kliensmegoldásokkal képernyőfelvételek készítése révén a felhasználók nem megfelelő viselkedéséről bizonyítékokat is lehet gyűjteni.

ramok is kiszűrhetők, amelyeket egy vírusérzékelő rendszer még nem ismer.

A szövegelemző általában olyan könyvtárakat használnak, amelyeknek a szavaival, kifejezéseivel összehasonlítják az internetről érkező tartalmakat. Ha az elemzés egyezést talált, vagy a tartalom megsérti az AUP-t, akkor a tartalmat meg lehet változtatni – azaz „szalonképessé" lehet alakítani –, le lehet tiltani a megjelenítését vagy elküldését, kliensmegoldás használata esetén be lehet zárni az adott alkalmazást, naplózni lehet, értesítőt vagy riasztást lehet küldeni, illetve a felsoroltak bármilyen kombinációja alkalmazható.

Az explicit terminológiát és jó kontextusszabályokat használó könyvtárak lehetővé teszik a szervezetek számára, hogy csak a biztonsági házirenddel vagy a morális, politikai és más elvekkel ellentétes tartalomra koncentráljanak. A szexuális információkat tartalmazó dokumentumok például hordozhatnak pornográf vagy oktatási célú, esetleg tudományos tartalmat is. A megfelelő szótárak a szövegkörnyezet alapján képesek különbséget tenni például pornóipari termékek és, mondjuk, olyan szakdolgozatok között, amelyek szövege a „mell" szót tartalmazza.

Fontos hangsúlyozni a technológia kétirányúságát, hiszen jól összeállított szótárakkal monitorozhatók és kiszűrhetők a kifelé irányuló bizalmas információkat hordozó tartalmak.

Természetesen ezeknek a technológiáknak is vannak előnyeik és hátrányaik.

### Előnyök

A kliensmegoldások előnye, hogy bármilyen, internettel kommunikáló alkalmazás forgalma szűrhető. Az operációs rendszer szintjén is működtethetők olyan tartalomelemző szoftverágensek, amelyekkel bármilyen esemény tartalmi vonatkozásai felügyelhetők, akár az Explorerrel (az Intézővel) helyileg megnyitott állomány is.

*Magánügyek munkaidőben*

A módszer képes lefedni a szervezet rendszerének legnagyobb biztonsági résést, hiszen a statisztikák szerint a biztonsági incidensek 70–80 százaléka belülről generálódik. Az ilyen esetek jó részében tartalom-ellenőrzéssel megelőzhető a szellemi javak szándékos vagy véletlen közkinccsé tétele, illetve egyéb bizalmas információk kiszivárogtatása.

A technológia nemcsak az AUP érvényesítésében hasznos, hanem a segítségével kiszűrhetők és felelősségre vonhatók azok az alkalmazottak, akik a szabályok ellenében „munkálkodnak".

A tartalomszűrés keretei között kliensmegoldásokkal olyan tevékenységek is elvégezhetők (képernyő-pillanatfelvétel készítése; felhasználó, alkalmazás és más paraméterek rögzítése), amelyek egy esetleges későbbi törvényi vagy kriminalisztikai eljárás során hasznosak lehetnek. Természetesen ennek jogi vonatkozásai is vannak, amennyiben a dolgozót tájékoztatni kell az ilyen jellegű felügyeletről, és alá kell vele íratni a biztonsági házirendet.

Az információk felügyelete a felelősségre vonhatóság és a bizonyíthatóság miatt nagyszerűen használható a felhasználók biztonsági tudatosságának a javítására.

A jól beállított szűrőkkel és jó szótárakkal jelentősen csökkenthető a hamis po-

## STATISZTIKÁK

A megkérdezett vállalatok szerint a biztonsági incidensek 48 százalékáért az alkalmazottakat terheli a felelősség.

Az alkalmazottak 61 százaléka látogat meg munkaidőben nem a munkájával kapcsolatos honlapokat.

A vállalatok 90 százalékának az a legnagyobb problémája az ellenőrizetlen alkalmazotti internetelérással, hogy csökken a munka produktivitása.

A dolgozók munkaidőben internetezéssel töltött idejének 49 százaléka kapcsolódik a munkájukhoz. A fennmaradó 51 százalékot a gyakoriság sorrendjében az alábbi tevékenységekre fordítják:

- (1) privát üzleti ügyek intézése és internetes vásárlás;
- (2) személyes levelezés, csevegés;
- (3) „felnőtt oldalak" nézegetése;
- (4) internetes információk keresése más személyes okból;
- (5) zenék, filmek, programok letöltögetése.

Munkaidőben az internetes vásárló és aukciós helyek óránkénti forgalma többszöröse a munkaidőn kívüli forgalomnak.

A pornográf webhelyek forgalma 9 és 17 óra között 70 százalékkal magasabb, mint máskor, és ugyanez érvényes a hírportálokra is.

A cégvezetők 82 százaléka szerint szükség van az alkalmazottak internethasználatának monitorozására.

A munkaidőben üzenőrendszerekben töltött alkalmazotti idő folyamatosan nő; a becslések szerint jelenleg a világ dolgozó polgárai összegezve huszonötmilliárd percet töltenek havonta üzengetéssel és üzenetolvasással.

zitivitás, azaz kevés az olyan esetek száma, amikor megfelelő tartalmak helytelennek minősülnek.

A módszer differenciálni is képes, tehát nem kell egész internethelyeket blokkolni azért, mert vannak rajtuk helytelen tartalmak is. Tartalomszűréssel megoldható, hogy mondjuk egy szexuális információkat tartalmazó webhely pornográf oldalai fennakadjanak a rostán, de a felvilágosító célzatú dokumentumai ne.

A szövegelemzés alkalmas számos kórokozó, de főként a szkript alapú (a weblapokban vagy HTML formátumú levelekben szereplő rosszindulatú szöveges parancsállományok) támadások elleni védekezésre.

## AZ ICRA

Az Internet Content Rating Association, azaz az Internet-tartalom-osztályozó Szövetség egy nemzetközi nonprofit szervezet. A mögötte álló vállalatok között megtaláljuk az AOL-t, a British Telecomot, a Microsoftot és a Verizont, de az ICRA-t sok más szervezet és alapítvány mellett az EU Internetes Akcióterve is támogatja.

Az ICRA célja a következők elősegítése:

- a felhasználók találják meg a keresett információkat;
- megbízhassanak a találatokban (pontossági és biztonsági értelemben is);
- kiszűrhessék a nemkívánatos tartalmakat.

A szervezet olyan tartalomleíró rendszert használ, amelyben a készítők maguk látják el kategóriacímkékkel a saját szerzeményeiket. Ennek a struktúrának sarkalatos eleme, hogy maga az ICRA semmit sem osztályoz, nem is minősít, azaz a tartalmakról semmilyen formában sem mond ítéletet. A felhasználók kizárólag a tartalomszolgáltatók önosztályozása révén döntik el, hogy mi kell nekik és mi nem.

Maga a minősítés webes űrlapok segítségével történik. Az adatok megadása után egy RDF-állomány generálódik, majd tárolódik az adott tartalom elérési adataival. Ezután a felhasználók erre a célra kifejlesztett szűrői a rendszer adatbázisából el tudják dönteni, hogy az adott domén megjelenítése engedélyezett vagy blokkolandó. Maga az ICRA is gondoz egy ilyen tartalomszűrő szoftvert: az ICRAplus-t.

A tartalomleíró rendszer szótárát egy nemzetközi testület készítette. Szándékaik szerint ez annyira semleges, amennyire csak lehet. 2005-ben azért vizsgálták felül, hogy ne csupán a webes tartalmak leírására legyen alkalmas, hanem minden online terjedő információ osztályozására. A rendszerhez nemrégiben applikálták az Európai Unió által támogatott Quatro projektet, amely a tartalomcímkék mellett a minőségi és a bizalmi (megbízhatósági) paramétereket is kezeli. Az ICRA olyan szolgáltatás bevezetését is tervezi, amely képes lesz a kategorizálás pontosságának az ellenőrzésére, és amelyet külső szervezetek (például internetes keresők) is igénybe vehetnek majd a saját megoldásaikban.

### A technológia hátrányai

A tartalomelemzők szótárainak összeállítása is rendszeres karbantartást igényel, sőt néha speciális (nyelvészeti) szakismereteket is megkövetel.

A tartalmak nyelvfüggősége miatt a módszer kevésbé általánosítható és több lokalizációs terhet jelent a megvalósítása. A többnyelvű rendszerek kézenfekvő okból még ezt a helyzetet is bonyolítják.

Ha szoftverágensekkel nem valósítják meg a tartalomszűrést, nagy hálózat sok munkaállomása esetében munkaigényes lehet a telepítés – bár a „push" technológiákkal ez a probléma is megoldható. Természetesen az átjáró alapú megoldások üzemeltetése egyszerűbb.

A tartalomszűrés egyértelműen erőforrás- és teljesítményigényesebb, mint az URL-blokkolás. A titkosított tartalmak szűrése kiegészítő megoldásokat igényel.

### Gyorstipp

A nagy szervezetek a felhasználóikat minőségi szolgáltatással igyekeznek kielégíteni. A biztonsági incidensek, de főként az adatok helytelen kezelése vagy az ezzel kapcsolatos visszaélések a minőség ellenében dolgoznak. A hagyományos URL-blokkolás a mondottak miatt csak a probléma 20–30 százalékát fedi le: a HTTP-forgalmat. A nagyobb biztonság érdekében a szervezeteknek érdemes a meglévő URL-szűrő mellé vagy helyére tartalomszűrőt telepíteniük, mert az nemcsak a HTTP-forgalmat szűri/monitorozza.

A biztonság filozófiája egyszerű: monitorozz, szűrj, blokkolj részlegesen, vagy zárd ki teljesen. Ennek jegyében: ha van URL-blokkolód, azt cseréld le, vagy vegyél mellé tartalomszűrőt; ha még nincs, akkor egyből tartalomszűrőt vegyél!

A gyakorlatban mind a két technológiát használják.

A szűréssel két alapvető probléma lehet:

- túlszűrés, azaz amikor a helyes tartalom vagy honlap is blokkolódik;
- alulszűrés, amikor a helytelen tartalom átmegy a szűrőn.

### Listagondok

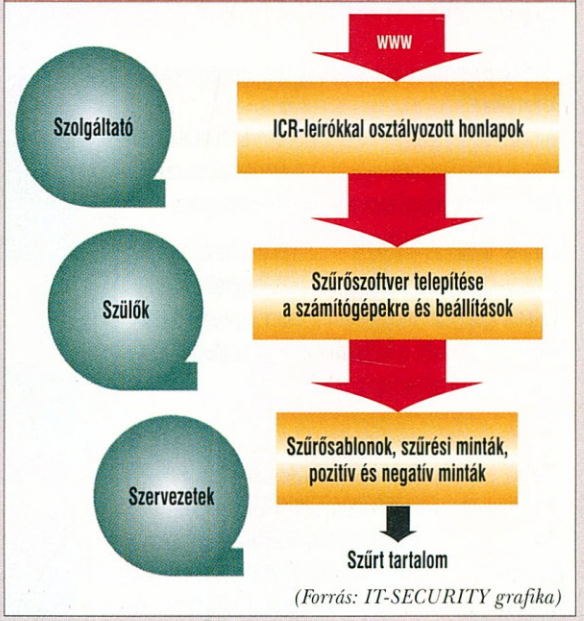
Ezek természetesen a rosszul osztályozott honlap-adatbázis vagy a helytelenül definiált szótár következményei. Az egyszerűség kedvéért a kettőt együttesen listának nevezve kijelenthető, hogy minden szűrőmegoldás kulcseleme a lista.

Léteznek publikusan letölthető vagy lekérdezhető (ezek általában a pornográfiára koncentrálnak), illetve kereskedelmi listák, valamint nemzeti szinten használt – titkos – listák.

A kereskedelmi listák a szűrők fejlesztőinek védett termékei, ezért azok sem nyilvánosak. Némelyik fejlesztő interneten lekérdezhető szűrőmegoldást is kínál, de a használt lista sem felhasználásra, sem pedig a jóságának az elemzése céljából nem érhető el.

A szervezetekben használt szűrők listái általában előre definiáltak, és jobb esetekben a rendszeradminisztrátorok manuálisan is hozzájuk férhetnek.

### AZ ICRA MŰKÖDÉSE




*(Forrás: IT-SECURITY grafika)*

### Szoftvertől a szolgáltatásig

A különböző technológiákat használó filterware-ek hosszú evolúciós utat jártak be a 90-es évek első URL-blokkolói óta. Az internetes technológiák fejlődésével nemcsak a titkosított információk vagy az üzenőrendszerek tartalomfelügyeleti kérdései kerültek előtérbe, hanem a fejlesztőknek követniük kellett a kockáza-

tok fejlődését is, ezért különféle védelmi (vírus- és kémprogram-ellenes, spamszűrő stb.) rendszerekkel kezdték felvértezni termékeiket.

A kezdeti, tisztán szoftveres internetszűrők után megjelentek az appliance-ek, de ma már léteznek menedzselt szolgáltatásként is.

A szoftveres szűrők kínálják a legnagyobb flexibilitást. A választható opciók nemcsak a választások szabadságát növelik, és a telepítést egyszerűsítik le, hanem a felhasználók teljes védelmi rendszerre fordított költségei is csökkennek. Másfelől a szoftverfrissítések menedzselésével lehetnek problémák, emellett nagy a sávszélesség-igényük. A kiszolgálókon futtatott szűrőszoftverek alkalmasak monitorozásra, és jól felügyelhetők, miközben lehetőséget kínálnak a különböző felhasználók és csoportok egyedi beállításainak a kezelésére.

Az internetszűrő appliance-ek gyorsan telepíthetők, olcsó az üzemeltetésük, megbízhatóak, és nagy a teljesítményük. A komponensek választhatósága azonban „beléjük van égetve".

A menedzselt szolgáltatások igénybevétele kíméli a sávszélességet, kiszámíthatók a költségvonzatok – amelyek azonban jelenleg elég tetemesek, emellett a standard tulajdonkészlet mellett nem nyújtanak sok választási lehetőséget.

## Gyors növekvés

Az előrejelzések szerint a 2004 és 2008 közötti időszakban a filterware-ek piacának forgalma 18 százalékkal nő; a 2006-os forgalom várhatóan meghaladja a 890 millió dollárt. A szegmensen belül a kisvállalkozások UTM-eszközeinek forgalma fejlődik a leggyorsabb ütemben az egyszerű kezelhetőség és a járulékos biztonsági előnyök miatt. Az elemzők szerint ezek „elég jók", de még jobbak az alkalmazásspecifikus appliance-ek.

Ismételten hangsúlyozzuk a kifelé irányuló forgalom tartalomfelügyeletének fontosságát. E helyen azért is, mert nemcsak a bizalmas adatok kiszivárogtatására utalunk, hanem arra is, hogy a beágyazott kérelmekkel megkerülhetők a védelmi rendszerek, másrészt a titkosított csatornák kommunikációjának a felügyeletére is szükség van. A jobb szűrők képesek „darabokra tépni" nemcsak az SSL-csomagokat, hanem más csomagolótechnológiákat, sőt egyre több alkalmazás egyedi titkosítását is visszafejtik. Így nemcsak a szűrőtechnológiák megkerülését célzó kódolt lekéréseket blokkolják, vagy a titkosított csatornákon érkező rosszindulatú ágensek ellen védenek, hanem kivédhető velük a zene-, film- és pornográf tartalmak letöltögetése és a bizalmas információk kiszivárogtatása is.

## Kockázatok és szellemi javak

Az SSL csak egy lehetőség, és még ennek a tartalomfelügyeletével is vannak etikai és jogi problémák. Nemcsak a filterwareek piaca fejlődik, hanem az egyedi titkosítást használó üzenőrendszerek, a VoIP és más „békés" technológiák mellett a kockázatok száma is nő. A DNS-mérgezés, a pharming és a webhely-átirányítás intő jelek arra, hogy a szűrők fejlesztőinek folyamatosan résen kell lenniük. A hagyományos URL-szűrők itt már édeskevés védelmet nyújtanának – itt értékelődik fel a tartalomszűrők szerepe.

Az intenetszűrésre szakosodott fejlesztők és a nagy IT-biztonsági cégek kínálatában sokféle és számos olyan tulajdonsággal felvértezett megoldás található, amelyekkel a különböző méretű szervezetek felhasználóit kordában lehet tartani. A választásnál a forgalom és méret mellett döntő szempont a szűrendő tartalmak jellege, a biztonsági házirend.

Tekintettel kell lenni azokra a kockázatokra, amelyek ellen járulékos védelemre van szükség és azokra a szellemi javakra is, amelyeket védeni akarunk.

**Kelemen László**

## FEJLESZTŐK ÉS SZŰRŐMEGOLDÁSAIK

8e6 Technologies – szerveres és kliensoldali szűrő- és beszámolókészítő alkalmazásokat fejlesztő cég.
BESS – olyan internetszűrő, amely integrálható a hálózatba; képes együttműködni a legismertebb tűzfalakkal, útválasztókkal, proxykkal és webes gyorstár-alkalmazással.
Blue Coat – webes biztonsági eszközöket, nagy szervezetekben használható, megfelelőségi kívánalmaknak is eleget tevő tartalomszűrőket fejlesztő vállalat.
Clearswift – a cég Mimesweeper termékei teljes értékű átjáró-, webes és levelezőszerver-tartalombiztonsági megoldások, amelyekhez számos további biztonsági modul illeszthető.
CyberPatrol – egyedi, Windowst használó számítógépekhez kínált szülői felügyeleti szoftver.
DansGuardian – nyílt kódú webszűrő megoldás, számos platformon fut; publikus blokkolólistákat használ.
Elron – integrált szerveres biztonsági termékeket fejlesztő vállalkozás.
eSafe – átjáró alapú integrált tartalombiztonsági megoldás.
eTrust SCM – integrált tartalombiztonsági rendszer URL-szűrővel és spamvédelemmel.
McAfee WebShield – appliance-család; a hardver mellett tartalmazza a McAfee vírus-, levelezés- és tartalomvédelmi megoldásait.
Sentian – szerverszoftver; a BESS-hez hasonlóan hálózatba integrálható, és képes más hálózati/hálózatbiztonsági eszközökkel együttműködni.
SmartFilter – proxykra, előinstallált gyorsítótárakra és tűzfalakra telepíthető szűrőszoftver.
Smooth Guardian – szerverrendszerekhez integrálható webes proxy- és szűrőmodul.
SquidGuard – a Squidhez kínált kombinált szűrő-, redirektor- és hozzáférés-vezérlő modul.
SurfControl – teljes szűrőmegoldás; a web-, email- és gyorsüzenő-forgalom szűrésére is alkalmas.
Symantec – a cég elképesztően széles skálán kínál szoftver alapú és appliance-szűrőket a háztartások és a különféle méretű szervezetek számára is; igen változatos a választható modulok, a járulékos képességek, illetve az integrált védelmi technológiák kínálata is.
Websense – számos szűrőmegoldást fejlesztő cég; a termékek közös jellemzője, hogy segítségükkel transzparensen monitorozható, naplózható és felügyelhető az internethasználat.
Earthlink, Yahoo!, AOL – csak néhány példa azokra a szolgáltatókra, amelyek publikusan elérhető online szűrőmegoldást kínálnak.
A Mac OS X 10.4-nél újabb változatai, illetve a Microsoft később megjelenő Windows Vistája az operációs rendszer szintjén tartalmazzák a szűrőmegoldást.
Csak felsorolásszerűen néhány további kombinált URL-blokkoló/tartalomszűrő szoftver: ContentProtect, CYBERsitter, NetNanny.
A Child Safe, Cyber Sentinel, Cyber Snoop és a FilterPark tisztán URL-blokkoló megoldások.
További fejlesztők és szűrők: AdIEFiltr, BajEye, Barracuda, BrightFilter, CipherTrust, Cisco, CSWEB, Cyber Sentinel, Filseclab (Internet Guardian Angel), FilterGate, i:Filter, Internet Watcher 2000, Interscan eManager, iProtectYou, IronPort, ISS, KidSplorer, KidsUnderground, LANguard, MessageLabs, MXtreme, Naomi, NetIQ, nXp, Panda, Postfix, Postini, SafeEyes, SaferSpace, Secure Computing, SmartFilter, Sonicwall, Spector, Trend Micro, Tumbleweed, X-Stop.

# Aki bújt, aki nem...

***Ebben a játékban a felhasználói szint már kevés.***

Sokat változtak a számítógépes fertőzések. A rosszindulatú programok készítői egyre nagyobb szakértelemre tettek szert, és a támadások is rafináltabbak lettek. A vírusíróknak nemcsak a tudásuk változott, hanem a céljaik is. A polgárpukkasztó erőfitogtatás helyét átvette az üzleti érdek. A mai kártevők nagy része már pénzszerzési célzattal készül. Az egykori állományfertőzők után a makróvírusok, férgek, szkriptvírusok, hátsóajtó-programok, trójaiak, reklámhordozók, kémprogramok evolúciós sora jól szemlélteti az elüzletiesedést.

## Ne érzékeljék!

A rootkitek régóta ismertek, de a kórokozók arzenáljának csak nemrég lettek „ghostware-ként" (szellemprogramként) is emlegetett tagjai. Valójában nem is a kártevők vonatkozásában kerültek igazán előtérbe, hanem a Sony tavalyi másolásvédelmi skandaluma miatt (IT-SECURITY, 2005. november, 24. oldal). Olyan álcázási technikákról van szó, amelyek elrejtenek valamilyen kódot, hogy a felhasználók – vagy más szoftverek – ne érzékeljék a jelenlétét.

Az IT-biztonság vonatkozásában sok kórokozót egyszerűen rootkitként emlegetnek, pedig ezek az ágensek tiszta formában nem léteznek. Legtöbbször más szoftverek részei, néha önálló kis programok, és céljuk, hogy egyfajta álca vagy gubó módjára elrejtsék a más kártevők létezésére utaló jeleket:

- magukat a rosszindulatú folyamatokat;
- állományokat (.exe, .com, .bat, .sys, .vbs stb.) és könyvtárakat;
- regisztrációs adatbázis-bejegyzéseket;
- szolgáltatásokat és eszközmeghajtókat;
- a használt portokat, kapcsolatokat és
- minden egyéb kódot vagy entitást, amely a fertőzéssel kapcsolatos.

http://www.securityfocus.com/infocus/1850
http://www.windowsecurity.com/articles/Hidden_Backdoors_Trojan_Horses_and_Rootkit_Tools_in_a_Windows_Environment.html
http://kareldjag.over-blog.com/5-archive-12-2005.html

Az álca miatt a rosszindulatú programok nemcsak az Intéző vagy a népszerű állománykezelők – mondjuk, a Total Commander – számára lesznek láthatatlanok, de például a Windows „mélyebbre látó" segédeszközei – Feladatkezelő vagy MSConfig – sem képesek érzékelni őket.

Nagyobb baj, hogy az álcázó programot és az általuk lopakodóvá tett kártevőket a hagyományos biztonsági szoftverek sem képesek érzékelni; a jócskán megfertőzött számítógépet makkegészségesnek nyilvánítják, és csupán a felhasználók veszik észre kisebb-nagyobb jelekből, hogy „valami nem stimmel".

## Álcázási szintek

A lopakod(tat)ó módszereket takaros kategóriákba lehet sorolni.

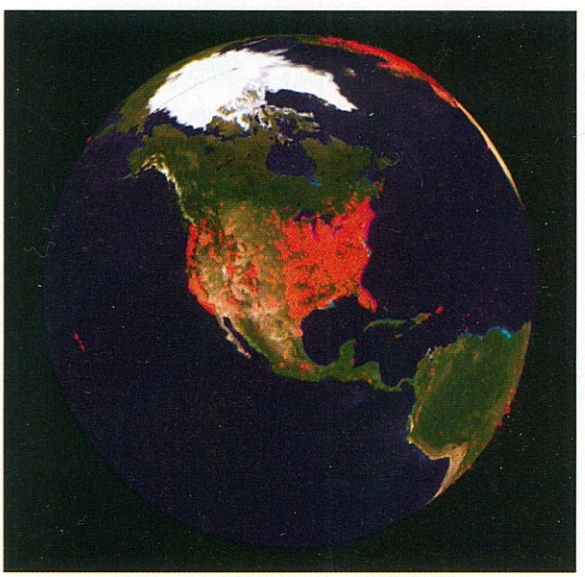
- A virtualizáló álcák a lehető legalacsonyabb szinten avatkoznak be. Úgy változtatják meg a rendszerindítás folyamatát, hogy ők töltődjenek be az eredeti operációs rendszer állományai helyett. A memóriában elvackoló ágens az eredeti rendszerállományokat klasszikus Virtuális Gépben futtatja. A parazita természetesen a vendégplatform minden alacsony szintű és hardverhívása felett átveszi az ellenőrzést.
- A rendszermag-szintű eszközök járulékos kódokat adnak hozzá a platformhoz, vagy lecserélik annak egyes részeit. Linux alatt ezt legtöbbször opcionálisan betölthető magmodulokkal (Loadable Kernel Modules), a Windows esetében többnyire eszközmeghajtó programokkal érik el. A biztonsági következmények mellett további kellemetlen mellékhatás lehet, hogy a rosszul megírt bújtató kód veszélyezteti a rendszer stabilitását.
- A könyvtármodulok szintjén beavatkozó élősdiek a rendszerhívások vagy rendszerfunkciók úgynevezett elkampózásával (hook), azaz eltérítésével vagy egyszerű átírásával valósítják meg a rejtőzködést.
- Az alkalmazásszintű álcázás esetén a felhasználói programok futtatható állományai cserélődnek le „trójaiasított" kódra, az alkalmazások viselkedését azonban kódbeültetéssel vagy a hívási mutatók táblázatainak átírásával is meg lehet változtatni.

## Felhasználói és rendszermag-mód

Gyakorlati szempontból az álcákat a működésükhöz használt jogosultsági szint szerint is csoportosíthatjuk. A ma legelterjedtebb AMD és Intel processzorok architektúráján négy ilyen szintet lehet(ne) használni. A Windows csak a 3. (felhasználói) és a 0. (rendszermag) szinteket alkalmazza. A lopakodók ezzel összefüggésben lehetnek:

- felhasználói módú álcák – ebben a csökkentett módban „csak" rendszerfunkciókat hívhatnak, de nincs ellenőrzési lehetőségük az egységmeghajtók és a memória felett;
- rendszermag-módban nincs semmilyen korlátozás, szabadon lehet garázdálkodni bármilyen fájlban – futtatható kódokban is – vagy a regisztrációs adatbázisban, a memóriában és a hardveren.

A lopakodás trükkje a 3. szintről a 0. szintre történő ugrás; természetesen a kódolásnál is ez jelenti az igazi kihívást. Ha már sikerült bejutni a rendszermagba, át lehet írni a szolgáltatásleíró táblát (SSDT), a megszakítások táblázatát



*A Sony DRM-rootkitjének elterjedtsége*

(IDT) és egy sor más mutatót; figyelni és manipulálni lehet a rendszermag adatforgalmát és a már említett módok (egységmeghajtó vagy opcionális magmodul) valamelyikével közvetlen rendszermag-objektumokat lehet elplántálni.

## Észlelési nehézségek

A legegyszerűbben és legbiztosabban úgy lehet megtalálni a rejtőzködő programokat, ha a rendszert tartalmazó adathordozót (merevlemezt) egy biztosan intakt másik számítógépen (vagy alternatív módon – USB, CD-ROM – betöltött rendszerrel) összehasonlítunk egy garantáltan fertőzésmentes rendszerrel vagy biztonsági másolattal. A gyakorlatban problematikus lehet a technikai kivitelezés, és gondot okozhat a referenciamásolat hiánya is. A helyzetet tovább bonyolítja, hogy az informatikai struktúrák nem statikusak; folyamatosan történnek olyan legitim rendszerváltozások, amelyek megnehezítik az összehasonlítást.

Az ideális érzékelőnek a potenciálisan fertőzött rendszerben kell megtalálnia az élősdieket. A feladat bonyolult, de a megoldás nem reménytelen – csak az a probléma, hogy az álcák írói is figyelnek, és folyamatosan megpróbálják kijátszani – néha egyszerűen leállítani – az érzékelő szoftvereket.

Rossz hír, hogy nincs tökéletes detektor, jó hír viszont, hogy nem létezik tökéletes rejtőzködés sem. A gyakorlatban nem szabad lecövekelni egyetlen érzékelőmegoldásnál, hanem többet is célszerű használni, emellett pedig feltétlenül követni kell a fejlesztők frissítéseit.

## Detektorok

A nagy biztonsági fejlesztők (McAfee, Symantec, Trend Micro stb.) különböző vírus- és kémprogram-ellenes megoldásai nem mellékesen képesek jó néhány lopakodó ágens szignatúra alapú vagy heurisztikus kiszűrésére. Számos önálló RootKit Detector is létezik, ezek nagy része adott lopakodókra specifikus.

Az általános megoldásra törekvő lehetőségekről készítőik néha elég szűkszavúan nyilatkoznak. Némelyikről csak annyit tesznek közzé, hogy „a rendszer

*Észlelési nehézségek*

mély átvizsgálását végzi". A megoldások működési módja persze nem mindig titkos:

- vannak programok, amelyek a felhasználói és a rendszermag-módok környezeteit hasonlítják össze, és a különbözőségeket jelentik;
- természetes veszély a fals pozitivitás, de az „NTFS alternate data streamekben" megbújó paraziták után kutakodó eszközök esetében még nagyobb lehet a hamis találatok száma;
- más programok a rendszerrutinok belépési pontjait ellenőrzik, de ezek a legitim változásokat is kijelzik.

Vannak még futó folyamatokat, rendszerindítást, aktív portokat figyelő lehetőségek, valamint olyan készletek, amelyek a leírtak kombinációit alkalmazzák.

### NÉHÁNY ÉRZÉKELŐ ÉS ELTÁVOLÍTÓ MEGOLDÁS:

Aries Sony Rootkit Remover (Lavasoft), Archon Scanner (X-Solve), AVG AntiRootkit (Grisoft), chkrootkit (Murilo & Jessen), DarkSpy (CardMagic), Blacklight (F-Secure), Gmer, Helios (e-Security), HiddenFinder (Wenpoint), HookExplorer (iDefense), IceSword (XFocus), Process Master (Backfaces), RootKit Hook Analyzer (Resplendence), Rootkit Hunter (Boelen), RootkitRevealer (Sysinternals), RootKitShark (Advances), RootKit Uncover (BitDefender), RootKit Unhooker (UG North), Rosszindulatú Szoftvereket Eltávolító Eszköz (Microsoft), Sophos Antirootkit (Sophos), System Virginity Verifier (Joanna Rutkowska), Unhackme (Greatis), Zeppoo

## Szanálási gondok

Általában elmondható, hogy a mai felderítőeszközök által adott eredmények értelmezése meghaladja a mindennapi felhasználók szintjét.

Különösen csínján kell bánni azokkal a programokkal, amelyek a bajok orvoslását is ígérik. Alapvetően két problémáról van szó: el kell távolítani a rejtőzködő komponenst és a bújtatott rosszindulatú programot. A helyzetet bonyolítja, hogy sok esetben maga az operációs platform változott meg, és a lopakodók kiirtása instabillá teszi a rendszert.

Legjobb megoldás a visszaállítás a biztosan egészséges biztonsági másolatból. Ez a biztonságra valamit is adó szervezeteknél nem jelenthet különösebb gondot – de amennyiben mégis, akkor marad az „adatmentés–formázás–újratelepítés–adatok vissza" vesződsége.

## Jobb megelőzni

Az álcázók begyűjtésének elkerülése hasonlít a más kórokozók prevenciójához, de van néhány speciális megfontolás:

- a bujkáló ágensek „szeretik" az adminisztrátori jogosultságú felhasználókat, hiszen így maguk is ilyen jogokat élvezhetnek; a lehető legalacsonyabb privilégiumok kiosztása segít;
- vannak olyan megelőző biztonsági eszközök, amelyek képesek monitorozni és blokkolni a rendszerhez hozzáférni akaró próbálkozásokat, védik a rendszerleíró adatbázist, elejét tudják venni a rejtett településeknek, a kódbeültetésnek, a globális mutatók átdefiniálásának stb.

Nemcsak ezért előzi meg nagy várakozás a Microsoft következő operációs rendszerét, de a Vista rendszerszinten tartalmaz egy sor olyan megoldást, amely az álcázóprogramoktól is véd – csak felsorolásszerűen néhány közülük: virtualizációs technológiák, az új adatfuttatás-védelmi mechanizmus, véletlen kódbelépési címek, kontrolláltabb rendszerhívások, megváltozott jogosultsági szintek és kezelésük, biztonságosabb böngészés, Windows Defender…

### PÉLDÁK MEGELŐZŐ ESZKÖZÖKRE

AntiHook (InfoProcess), AppDefend (Ghost), Cyberhawk (Novatix), DefenseWall (HIPS), Dynamic Security Agent (Privacyware), Exe LockDown (Horizon), GeSWall (Gentle), Neoava (Arman Nayyeri), ProcessGuard (DiamondCS), SocketShield (Exploit Prevention), ThreatMon (WenPoint), Windows Defender (Microsoft)

**Kelemen László**

# Elhanyagolt e-számlák

***A vállalkozások közötti kommunikációban ma már számtalan információ halad elektronikusan. Az egyik legfontosabb, az üzlet savát-borsát jelentő tétel – a számla – azonban ma még a legritkább esetben létezik kizárólag elektronikus formában.***

A papír alapú számla két vállalat között maga a megtestesült ellentmondás és pazarlás. A számlán lévő információk a kibocsátó cégnél bizonyos számítógépen, elektronikus formában állnak elő; a befogadónak pedig szinte biztosan, elektronikus formában van rá szüksége, hogy saját számítógépes rendszerébe bevigye a rajta szereplő információkat. Ehhez képest a kiállító papírra nyomtatja a számlát, azt fizikai valójában juttatja el a címzetthez, amelyik egy újabb munkafázis beiktatásával dolgozza fel az adatokat, hogy utána még a papír tárolásával és megőrzésével is bajlódnia kelljen.

Ennél sokkalta hatékonyabb megoldást kínál az elektronikus számla, amit már Magyarországon is több mint két éve ki lehet bocsátani: 2004 áprilisában jelent meg a 20/2004. számú pénzügyminisztériumi rendelet, amely tisztázta az ezzel kapcsolatos kérdéseket.

## Jogszabályi előírások

A rendelet egyik legfontosabb megállapítása, hogy e-számlát csak abban az esetben lehet kibocsátani, ha annak kiállításához a számla címzettje előzetesen hozzájárult. (Ez a hozzájárulás persze történhet úgy is, hogy miután a nagy szolgáltató az Általános Szerződési Feltételekben jelezte a vele kapcsolatba kerülőknek, hogy elektronikus számlát fog kiállítani, a befogadó a szolgáltatás további igénybe vételével, ráutaló magatartással adja hozzájárulását.)

Jogszabályhoz híven a PM-rendelet technológia- és így versenysemleges a számlák formátumát illetően. Lehetőség van elektronikus számlák kibocsátására a bizonyos iparágakban elterjedtnek nevezhető EDI (Electronic Data Interchange) rendszerben, de igazán nagy lehetőség a (legalább fokozott biztonságú) elektronikus aláírással és időbélyegzővel ellátott, rugalmasabban előállítható és befogadható e-számlában van – mondja *Nagy Zsolt*, a NetLock Kft. jogász PKI-tanácsadója. Bármelyik módszert is használják a vállalatok, bizonyos feltételeknek mindenképpen meg kell felelniük. Így a jogszabály előírásai szerint mind a kibocsátáskor, mind a megőrzés során biztosítani kell a számla

- eredetének hitelességét;
- sértetlenségét;
- értelmezhetőségét;
- jogosultak általi hozzáférhetőségét;
- valamint a jogosulatlan hozzáférés, módosítás, törlés és megsemmisítés elleni védelmét.

A hitelességet és a sértetlenséget jól tudja bizonyítani az elektronikus aláírás (hogy most csak erről, az EDI-nél egyszerűbben alkalmazható módszerről beszéljünk). Szükség van még a számla hitelesítéséhez időbélyegzőre is, amelyet egy erre szakosodott szolgáltató „nyom rá" a számlára (pontosabban csak annak „ujjlenyomatára"): ezzel lehet igazolni, hogy a számla az adott időpillanatban az adott tartalommal már létezett. Ahogyan elektronikus aláíráshoz szükséges tanúsítványból is van fokozott biztonságú és minősített szintű, az időbélyegzőből is létezik ez a két kategória. Az e-számla kibocsátásához azonban csupán fokozott időbélyeg kell, de a megőrzéshez már minősített.

## Formátumok bősége

A számla kibocsátása azonban csak az egyik fele a teljes számlázási folyamatnak; legalább ilyen súllyal esik latba a befogadás kérdése is. Az e-számlát megkapó szervezetnek ellenőriznie kell az aláírás hitelességét, és ha az aláírás nincs beágyazva magába a dokumentumba, akkor erre a célra külön alkalmazást kell üzembe állítani.

Az elektronikus számlákat ugyanúgy meg kell őrizni, mint papír alapú társaikat, és ehhez az alkalmazott kriptográfiai algoritmusok változása esetén minősített időbélyegzőt kell elhelyeztetni, vagyis a számlát felül kell pecsételtetni. Végül, de nem utolsósorban a beérkezett számlák feldolgozását a cégek szeretnék beilleszteni meglévő informatikai folyamataikba, ez viszont nagymértékben függ a számla formátumától.

Éppen a technológiai semlegesség jegyében a jogszabályok nem határozzák meg az elektronikus számla formátumát,


*Hitelesség és sértetlenség*

vagyis így elméletileg bármilyen állományformátum használható – magyarázza Nagy Zsolt. A gyakorlatban azonban több, egymásnak esetenként ellentmondó követelménynek is meg kell felelniük az e-számláknak. Így például jó, ha a számla ember és gép számára is könnyen értelmezhető (utóbbi az automatikus feldolgozást könnyíti meg); a hitelesítésnek egyszerűen ellenőrizhetőnek kell lennie; és nagymértékben segíti az elektronikus számlázás terjedését, ha a befogadó félnek ez nem jelent költségtöbbletet, nem kell speciális szakértelemmel rendelkeznie, esetleg külön programokat telepítenie. Sajnos olyan e-számlázási rendszer még nemigen van, amely mindezeknek a követelményeknek egyszerre eleget tud tenni – foglalja össze a jelenlegi piaci tapasztalatokat a NetLock szakértője.

A gyakorlatban kétféle formátum lát-

szik terjedni: az egyik a PDF, a másik az XML. Előbbi mellett szól, hogy strukturált, jól szerkeszthető állományként is létrehozható, amelyhez könnyen előállíthatók a megfelelő sablonok is, ráadásul az elektronikus aláírás és az időbélyeg magába a dokumentumba illeszthető. Így aztán a befogadói oldalon sem igényel szinte semmilyen beruházást: elegendő az ingyenesen letölthető Adobe Acrobat Reader, amellyel nem csupán maga a számla tekinthető meg, de annak hitelessége is ellenőrizhető.

A másik gyakorinak mondható formátum az XML. Ezt azért kedvelik nagyon sokan, mert igen rugalmasan bővíthető, nagyon sok mindent meg lehet benne valósítani, és az XML-támogatás révén számtalan szoftver automatikusan fel tudja dolgozni az ilyen típusú dokumentumokban tárolt adatokat.

## Feldolgozni is tudni kell

Egy teljes elektronikus számlázási rendszer kiépítése esetén azonban más problémákkal is szembe kell nézni. Három olyan kérdéskör is van, amelyeket nagyon gyakran elhanyagolnak, noha a későbbiekben alapvetően befolyásolhatják egy-egy projekt sikerét és az elektronikus számlázás jogszerűségét.

Az első a kontírozás, vagyis amikor bizonyos könyvelési információt rávezetnek a számlára. Papír alapú számlákra egyszerűen ráírják, de ugyanezt meg kell(ene) tudni valósítani az e-számlákkal is. Technikailag ez viszonylag könnyen megoldható: a kontírinformációkkal kiegészítik a meglévő számlát, majd újra hitelesítéssel látják el.

### AZ E-SZÁMLA ELŐNYEI

Az elektronikus számla sok tekintetben jobb, mint hagyományos, papír alapú társa. Így például az e-számla:

- olcsóbban bocsátható ki;
- olcsóbban és gyorsabban jut el a címzetthez;
- könnyebben archiválható;
- hatékonyabban, akár automatizáltan is feldolgozható a címzettnél.

A második fontos téma a konverzió kérdése. Számlát bármilyen formában lehet küldeni és tárolni, de azt nem lehet elvárni az adóhatóságtól, hogy mindezekre felkészüljön. Ezért az APEH közzétette, hogy milyen formátumokban fogadja el az ellenőrzésre bekért számlákat (ezek között szerepel egy XML-séma is). A jövőre is gondoló vállalatnak – akár kibocsátója, akár befogadója az e-számláknak – mindenképpen fel kell készülnie arra, hogy a tárolt számláit át tudja konvertálni a megkívánt formátumra.

A harmadik nagyon lényeges terület a számlák megőrzése – folytatja Nagy Zsolt. A jogszabályokban előírt megőrzési idő (8-10 év) mindenképpen több, mint általában az informatikai rendszerek (sőt, egyes technológiák) életciklusa.

## Kiszervezve

A fenti feladatok egy része elkerülhető, ha a vállalat nem maga intézi elektronikus számlázási folyamatait, hanem erre szakosodott szolgáltatók segítségét veszi igénybe. Ennek a teljes folyamata az úgynevezett elektronikus számlabemutatás és -fizetés, angol betűszóval EBPP (electronic bill presentment and payment).

Magyarországon összesen két ismert szolgáltató működik, amelyek egyelőre csak a tömeges számlakibocsátóknak kínálják szolgáltatásaikat. Az egyik a T-Systems kebelén belül működő Távszámla, amely a Magyar Telekom-csoport vállalatait szolgálja ki, a másik pedig az EBPP.hu, amelynek egyelőre a Fővárosi Vízművek az egyetlen ügyfele.

A magyar szolgáltatók még nem specializáltak, egyszerre állnak kapcsolatban a fogyasztóval és számlakibocsátóval, valamint az elektronikus fizetést lehetővé tévő banki szolgáltatóval.

Nagy Zsolt szerint az EBPP-piac bővülésének egyik akadálya, hogy egyelőre még drága az EBPP-szolgáltatókhoz való kapcsolódás. A számlakibocsátók részéről ez több tízmillió forintos beruházást is jelenthet, hiszen egyrészt informatikai fejlesztések is szükségesek az interfészek kialakításához, másrészt belső eljárásokat is módosítani kell. Emiatt számos cégnél reális alternatíva a saját számlázási rendszer kibővítése e-számlázási funkcionalitással, amit össze lehet kötni egyéb hitelesítési megoldások bevezetésével, amelyekkel például a call centerbe befutó hívások, a papíron kiküldött számlák kötelezően őrzendő elektronikus másodpéldányainak vagy bármilyen egyéb dokumentumoknak a hitelesítése is megoldható.

**Schopp Attila**

# Hibajelentés

*Folt a foltozott folt hátán.*

A sérülékenységek alapvető tulajdonságából – gombamód szaporodnak – és az előző lapszám óta eltelt hosszabb időből adódóan megnövelt táblázatunkban is csak az általunk legfontosabbaknak ítélt problémákról tudunk beszámolni.

A bejelentett szoftverhibák mellett az uborkaszezon ellenére számos olyan esemény is történt, amelyet érdemes külön is kiemelni.

## Huszárvágás 1.0

Kezdjük az Apple MacBookjainak hardveres problémájával. Az almás noteszgépek némelyik felhasználója arra panaszkodott, hogy elégtelen a hűtés. Kiderült, hogy az egyik sorozatban „gyárilag benne felejtettek" egy kis műanyag bigyót, és az blokkolta a hátsó hűtőventillátort.

A felsőkategóriás MacBook Pro-sorozattal még a pöcök eltávolítása után is akadtak melegedési gondok, ezért az Apple közzétett egy olyan firmware-frissítést, amely nemes egyszerűséggel állandóan bekapcsolva tartja a propellert. A felhasználók szerint a hűtés zaja még mindig elviselhetőbb, mint a hőtágulás miatti korábbi aggasztó recsegés-ropogás – meg a véletlenszerű időközökben bekövetkező rendszerleállások.

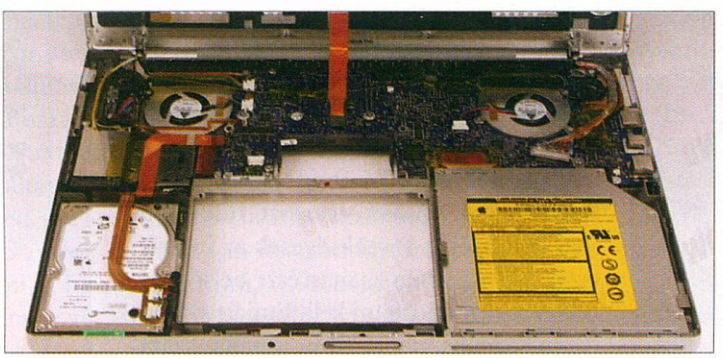
## Huszárvágás 2.0

Ugyancsak az Apple augusztus 7-én, hétfőn útjára bocsátotta Xeon processzorokkal felvértezett csúcsgépeit, a Mac Prókat. A cég világrekordot jelentő két nap után, az szerdán, már közzé is tette erőműveihez, pontosabban operációs rendszerükhöz az első javítócsomagot. Ez már önmagában is furcsa, de az még érdekesebb, hogy a csomag egy része – egészen pontosan öt javítás – a gépeken előre telepített Mac OS X 10.4.7-hez már augusztus elseje óta elérhető volt.

A közzétett nyilatkozat szerint a korábban felfedezett problémák javításait nem sikerült maradéktalanul tesztelni a Mac Pro gyártásáig, ezért ebben a biztonsági javítócsomagban tették közzé.

## Nem(csak) az, aminek látszik

*Brendan O'Connor* biztonsági szakértő érdekes demonstrációt tartott a Black Hat hacker-világtalálkozón. A Xerox WorkCenter multifunkciós hálózati nyomtatójának kezelésére szolgáló webes felület konfigurációs problémáit kihasználva ellenőrzése alá vonta az eszközt. Ezt követően sikeresen futtatott különféle programokat, nyomtatgatott ezt-azt, és természetesen jól megmonitorozta, hogy mások milyen dokumentumokat „eresztenek át" az irodai mindentudón.



O'Connor szerint ezután közölte, hogy a látszat ellenére ez egy „nyomtatódobozba bugyolált linuxos szerver", ezért sikeres behatolás esetén a támadó nemcsak azt nyomtat, amit akar, nemcsak monitorozhatja a szkennelt, faxolt, másolt, nyomtatott tartalmakat, hanem a készülék szerverfunkciói révén részlegesen a hálózatra is rálát – aminek további biztonsági következményei lehetnek.

A nyomtatók problémái nem új keletűek, és nemcsak a Xerox készülékeire érvényesek. Maga a Xerox egyébként közzétett februárban hasonló sérülékenységhez egy javítást, de O'Connor egy teljesen befoltozottnak vélt rendszer felett vette át sikeresen az uralmat. A szakember egyébként Xerox-párti, és a problémákkal kapcsolatos részleteket kizárólag a vállalat képviselőivel osztotta meg.

## A javítás javítása

Augusztus második keddjén menetrendszerűen jöttek a Microsoft szokásos biztonsági és egyéb javításai a Windows és Office rendszerekhez. Ezek közül az egyik, az MS06-042 biztonsági értesítőben hivatkozott csomag összesen nyolc sérülékenységet javított az Internet Explorer 5.01-es és 6-os (és 7-es béta-) változatain.

A dolog szépséghibája, hogy a frissítés után a böngésző SP1-gyel ellátott 6-os változata Windows XP SP1 és Windows 2000 alatt „lesérült" – azaz tömörített HTTP 1.1 protokollt használó honlapok meglátogatásakor puffertúlcsordulás miatt nemcsak „elszállt", hanem a leállás igen súlyos biztonsági rést is teremtett. A Microsoft ezért először a hónap közepén kibocsátott egy gyorsjavítást (ami csak a HTTP 1.1. protokollt tiltotta le), majd augusztus negyedik keddjét is foltozókeddnek nyilvánítva közzétette a végleges megoldást.

**Secunia:** *http://www.secunia.com*
Feliratkozás a legfrissebb sérülékenységeket naponta, részletesen leíró, IT-Security Today című hírlevelünkre: *http://www.it-business.hu/engine.aspx?page=hirlevel*

## Korai frissülések

A sok negatívum után zárásként egy kellemes hír. A Windows Vista meglehetősen rögös utat jár be, mire év végén vagy jövő év elején(?) elér a felhasználók gépeihez. Sokan üdvözlik, mások kritizálják a biztonsági tulajdonságait. Azt azonban a rosszakarói sem vethetik a Microsoft szemére, hogy ne gondoskodna a szoftverfrissítéseiről – ráadásul jó előre. Mindezidáig ugyanis a Vista az informatika történetének az első olyan operációs rendszere, amelynek bétaváltozataihoz azok első kiadásai óta folyamatosan jelennek meg biztonsági javítások.

Nemcsak a szerves részét képező Windows Defender szignatúraállományai frissülnek, hanem például a böngésző és maga a felépítmény is. Nem volt ez másképp augusztusban sem, amikor a hónap második keddjén érkezett egy frissítés a rendszermaghoz (MS06-051) és az ominózus javítócsomag (MS06-042) az Internet Explorerhez – ez utóbbi a Vista esetében nem okozott gondot.

**Kelemen László**

## FELFEDEZETT HIBÁK ÉS JAVÍTÁSAIK

| Szoftver/alkalmazás | Secunia-fokozat (1–5) | Secunia-azonosító | Leírás | Megoldási javaslat/további információ |
|---|---|---|---|---|
| **Microsoft termékek** | | | | |
| .Net keretrendszer 2.0 | 3 | 20999 | A keretrendszer sérülékenysége érzékeny információkhoz való hozzáférést tesz lehetővé. | *http://www.microsoft.com/technet/security/Bulletin/MS06-033.mspx* |
| Windows 2000, XP, 2003 | 3-4 | 20748, 20906, 21006, 21007, 21377, 21388, 21394, 21401, 21408, 21415, 21417 | Az operációs rendszerek változatos sérülékenységei távolról történő kódfuttatáshoz, jogosulatlan hozzáférés-szerzéshez, érzékeny információkhoz való hozzáféréshez és más kellemetlenségekhez vezethetnek. | *http://www.microsoft.com/technet/security/Bulletin/MS06-034.mspx és …035, 036, 040, 041, 043, 044, 045, 046, 047, 049, 050, 051….mspx* (a Secunia nem sorolt fel minden sérülékenységet) |
| Az Excel 2000-ben és azóta megjelent összes Windows és Mac OS X alatt futó változata | 4-5 | 20268, 20686 | A táblázatkezelőben felfedezett sérülékenységek tetszőleges kód távoli futtatásához vezethetnek, illetve más módon is veszélyeztetik a rendszert. | *http://www.microsoft.com/technet/security/Bulletin/MS06-037.mspx* |
| A PowerPoint 2000-ben és azóta megjelent összes Windows és Mac OS X alatt futó változata | 4-5 | 21040, 21061 | A bemutatókészítőben felfedezett két sérülékenység tetszőleges kód távoli futtatásához vezethet, de a felhasználók rendszerei más módon is veszélyeztethetők. | *http://www.microsoft.com/technet/security/Bulletin/MS06-048.mspx* |
| Az Office 2000-ben és azóta megjelent összes Windows és Mac OS X alatt futó változata | 4 | 21012, 21013 | Az irodai alkalmazáscsomag lényegében összes komponensét érintő sérülékenység tetszőleges kód távoli futtatásához vezethet. | *http://www.microsoft.com/technet/security/Bulletin/MS06-038.mspx és …039.mspx* |
| Internet Explorer 5.01 és 6.x (és 7 béta) | 4 | 21396, 21557 | A böngésző több (összesen nyolc) sebezhetősége elsősorban távolról történő kódfuttatást eredményezhet, de a felhasználók rendszerei más módon is veszélyeztethetők. | *http://www.microsoft.com/technet/security/Bulletin/MS06-042.mspx* |
| **Más operációs rendszerek** | | | | |
| Apple Macintosh OS X | 4 | 21253 | Az operációs rendszerben felfedezett összesen 19 (a legsúlyosabb „kritikusnak" minősített) sérülékenység változatos súlyos következményekhez vezethet. | *http://secunia.com/advisories/21253/ – http://www.security-protocols.com/sp-x32-advisory.php – http://www.security-protocols.com/sp-x33-advisory.php – http://docs.info.apple.com/article.html?artnum=304063* |
| Suse platform és levelezőszerver | 4 | 21459, 21467, 21498 | A Suse több platformjához és levelezőszerveréhez a fejlesztőgárda szorgalmasan, csaknem hetente tesz közzé biztonsági javításokat. | *http://secunia.com/advisories/21459/ http://secunia.com/advisories/21467/ http://secunia.com/advisories/21498/* |
| **Böngészők, levelezők** | | | | |
| A Mozilla Firefox 1.5.0.5 előtti, a Seamonkey 1.0.3 előtti és a Thunderbird 1.5.05 előtti változatai | 4 | 19873, 21228, 21229 | A Mozilla termékek több kritikus sérülékenysége miatt a fejlesztő biztonsági javításokat eszközölt, de a Secunia leírása óta nem biztonsági jellegű frissítések miatt a Firefox tovább frissült 1.5.0.6-ra, a Seamonkey pedig 2.0.4-re. | *http://secunia.com/advisories/19873/ http://secunia.com/advisories/21228/ http://secunia.com/advisories/21229/* |
| Safari 2.x | 4 | 21271 | Az „almás" böngésző KHTMLParser::popOneBlock() függvényének sebezhetősége tetszőleges kód futtatását teszi lehetővé. | Le kell tiltani a JavaScriptet. Lásd még: *http://browserfun.blogspot.com/2006/07/mobb-31-safari-khtmlparserpoponeblock.html* |
| **Multimédia** | | | | |
| Winamp 5.x | 4 | 20722 | A médialejátszó MIDI-moduljában felfedezett hiba puffertúlcsordulás és annak következményei miatt veszélyeztetheti a felhasználó rendszerét. | Át kell térni az 5.24-es változatra. Lásd még: *http://www.winamp.com/player/version_history.php#5.24* |
| Apple iTunes 4.x, 5.x, 6.x | 4 | 20891 | A szoftver AAC-állományok (például .M4A) lejátszásakor jelentkező aritmetikai túlcsordulási hibája a memória veszélyeztetése révén tetszőleges kód futtatásához vezethet. | Át kell térni a 6.0.5-ös változatra: *http://www.apple.com/itunes/download/*. Lásd még: *http://docs.info.apple.com/article.html?artnum=303952* |
| **Egyéb** | | | | |
| Cisco Unified CallManager 5.x | 4 | 21030 | A platform több sérülékenysége miatt DoS-helyzetet lehet teremteni, illetve más módon is veszélyeztethető a rendszer. | Át kell térni az 5.04-es változatra. Lásd még: *http://www.cisco.com/warp/public/707/cisco-sa-20060712-cucm.shtml* |
| Számos McAfee-alkalmazás | 4 | 21264 | A McAfee SecurityCenter puffer-túlcsordulási problémája több biztonsági terméket is érint. A sebezhetőség miatt tetszőleges kód futtatható az érintett rendszereken. | Frissíteni kell a SecurityCenter 6.0.23-as változatára: *http://us.mcafee.com/root/login.asp*. Lásd még: *http://ts.mcafeehelp.com/faq3.asp?docid=407052* |

*(Forrás: Secunia és a felsorolt termékek fejlesztőinek honlapjai)*

# Ellopott beszélgetések

***Az interneten folytatott hangforgalom ugyanolyan veszélyeknek van kitéve, mint a netes adatforgalom.***

Ha az ember egy IP alapú telefonhívás biztonságára, illetve lehallgathatóságára gondol, akaratlanul is egy hagyományos vezetékes, esetleg mobilkészülék jut az eszébe.

Csakhogy amíg ezeket az eszközöket tényleg „kihallgatjuk", addig egy internetes beszélgetés megszerzése inkább adatlopásnak minősül.

## Hagyományos módszerek

Egy klasszikus telefonbeszélgetés lehallgatásának alapvetően négy módja van. A legegyszerűbb, ha két készülék helyezkedik el a beszélgetés egyik végén. Ez egy átlagos, vezetékes telefon esetében nevele. Azonban mobiltelefonoknál – vezeték híján – ez a lehetőség sem áll fenn.

A harmadik módszer a telefonközpontban történő lehallgatás; a mostanában használt technológiák lehetővé teszik ezt. Előnye, hogy kényelmes, és mobilkészülékek esetén is alkalmazható. Problémát csak a központhoz való hozzáférés jelent, ezért mostanában a rendőrség eszköze ez a módszer.

Végül a negyedik megoldás a gerincvezetékek, mikrohullámú vagy műholdas jelek megcsapolása. Ebben az esetben rengeteg telefonbeszélgetés válik elérhetővé, ám nagyon nehéz egy konkrét személyt lehallgatni. Ezzel szemben ez a módszer alkalmas véletlenszerű vagy átfogó lehallgatásra, így leginkább a titkosszolgálatok és hírszerző szervezetek használják. A klasszikus telefonoknál a hívások biztonságát ezek a támadások fenyegetik.

*Veszélyeztetett VoIP-végpont*

## Új veszélyforrások

Egy IP-telefon működése alapvetően különbözik a hagyományos készülékétől. A hanganyag kódolt formában, kis adatcsomagokban, az interneten keresztül utazik, ezáltal ugyanazoknak a veszélyeknek van kitéve, mint bármilyen más netes adatfolyam. Az adatcsomagokat pedig az útjuk során bárhol el lehet kapni, és így a beszélgetést le lehet hallgatni.

Megtehetik ezt azoknak a számítógépeknek a tulajdonosai, amelyeken az adatok keresztülfutnak (például az internetszolgáltatók), és igazából bárki, aki képes ezekbe a gépekbe betörni. Egy kicsit hasonló a dolog a telefonközpontos lehallgatáshoz, azzal a nem elhanyagolható különbséggel, hogy többek képesek egy távoli számítógép fölött észrevétlenül átvenni az irányítást, mint egy központba bejutni.

hezen kivitelezhető észrevétlenül, de egy vezetéknélküli telefonnál elegendő ismerni a használt rádiófrekvenciát, és máris hozzáférhetővé válnak a hívások. Ez a módszer azonban nem működik mobilkészülékeknél.

A második lehetőség a rácsatlakozás a vezetékre, bárhol a hívás két végpontja között. Ez így természetesen azt jelenti, hogy nem kell a beszélgető felek közelébe kerülni, a lehallgató pedig könnyen észrevétlen maradhat. Régebben előszeretettel alkalmazta a módszert a rendőrség, mostanában inkább a bűnözők élnek

Az IP-telefon széles körű elterjedésének komoly akadálya lehet, hogy ilyen nagyfokú lehallgatásveszélynek van kitéve. Amíg ugyanis nincs megfelelően levédve a rendszer, addig a használata lehetőséget teremthet adatlopásra, ipari kémkedésre, akár bírók, politikusok zsarolására olyan szinten, amely a hagyományos telefonvonalak használatakor elképzelhetetlen.

## Hatékony módszer az adattitkosítás

Az ilyen fenyegetések ellen hatékony módszer az adatok titkosítása. Ha egy titkosító eljárással készült adatcsomagot elfognak, azt lehetetlen dekódolni a megfelelő kulcs nélkül, kulccsal jó esetben pedig csak a beszélgetés résztvevői rendelkeznek. Szerencsére léteznek ilyen eljárások: például a Skype saját, beépített titkosítást fejlesztett ki, vagy említhetjük az egyszerűen használható, nyílt forráskódú Zfone-t (*Phil Zimmermann*, a népszerű PGP e-mail-titkosító rendszer megalkotójának feljesztése).

Sajnálatos módon azonban a legkomolyabb fenyegetést a titkosítás sem védheti ki. Hiába utazhatnak ugyanis biztonságban az adatcsomagok, ha a két végponton már nem titkosított formában is meg lehet őket szerezni. Elég ugyanis egy vírust az egyik beszélgető fél gépére juttatni, hogy könnyen hozzáférhetővé váljon a társalgás. Ezenkívül egy képzett számítógépes bűnöző könnyen bejuthat bármely nem megfelelően védett rendszerbe.

A mindezekből levonható következtetés persze nem meglepő: biztonságos gépekre, biztonságos operációs rendszerekre és biztonságos adatcsatornára van szükség ahhoz, hogy az IP-telefon széles körben elterjedt, megbízható eszközként egyáltalán szóba jöhessen.

**Bajzik Dávid**

### ZFONE

A Phil Zimmerman által megalkotott eljárás hatékony titkosítást kínál az IP alapú telefonhívásokhoz. A technológia legfőbb erénye, hogy nem kell kulcsokat tárolni egy központi szerveren, azokat csak a beszélgetés résztvevői ismerik. A kódolás-dekódolás valós időben történik, de természetesen csak akkor, ha mindkét félnél telepítik a Zfone-t. A megfelelő védelmet emellett a minden hívásnál újragenerálódó kulcsok is biztosítják.

# Titkok a levegőben

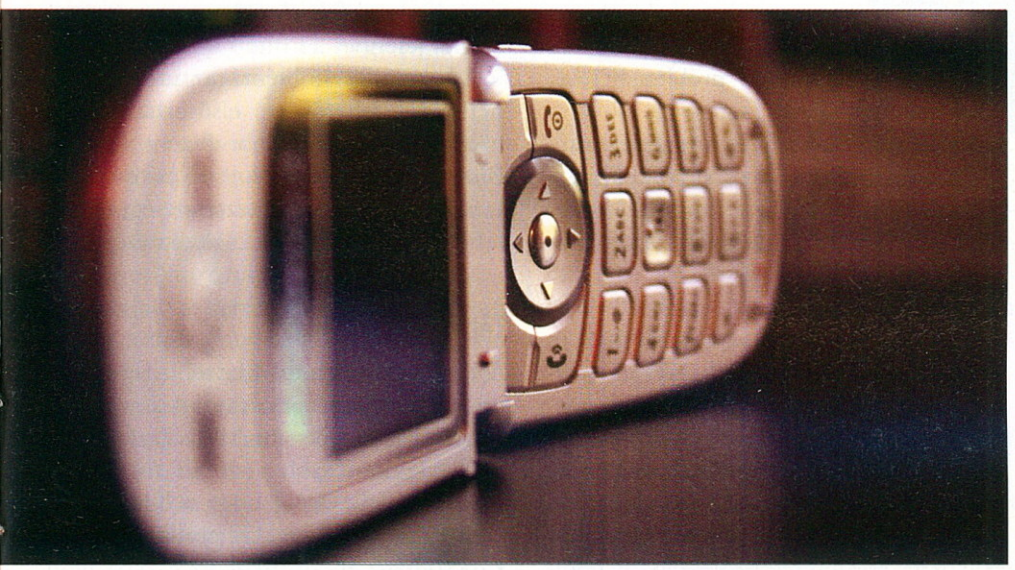
***Lehetetlen nincs ugyan, de felkészültség és komoly informatikai háttér kell egy mobilbeszélgetés lehallgatásához.***

A kárcsak a hagyományos és az IP alapú vezetékes telefóniában, a GSM világában is felmerül a beszélgetések lehallgatásának veszélye. A GSM-készülékek között digitalizált, összerendezett jelek utaznak, a jelfolyamot állandóan változó frekvenciákon továbbítják, mégpedig úgy, hogy minden keret különböző csatornát használ.

Ezek az eljárások már önmagukban valószínűtlenné teszik a lehallgatást, ám a GSM-szabvány egy magasabb szintű biztonságot is alkalmaz: a továbbítás előtt a rendszer titkosítja az adatokat.

## Hitelesítés minden híváskor

Talán minden másnál fontosabb, hogy a hálózat a hívás felépítése előtt hitelesítést végez. Leellenőrzi, hogy a SIM-kártya valóban az, aminek kiadja magát. A módszer lényege, hogy a SIM-kártya tartalmaz egy privát kulcsot, aminek a másolatát az AuC-ben (Authentication Centre) őrzik. Ez a kulcs sohasem kerül ki a rádiós hálózatba.



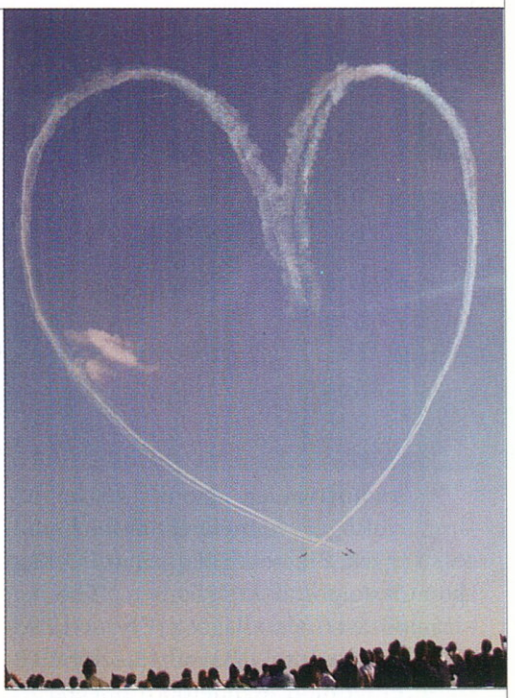
*Nehéz belehallgatni*

A hálózat minden hívás felépítése előtt hitelesíti a SIM-kártya azonosságát. Először egy véletlenszámot küld a készülékre, majd a mobilvégpont ezt a számot – egy titkosító algoritmust alkalmazva – egyesíti a SIM-kártya saját privát kulcsával. Az eredményt a mobilkészülék visszaküldi a hálózatba. Ezzel egy időben a hálózat ugyanazt a véletlenszámot elküldi az AuC-be. A hitelesítő központ – a SIM-kártya privát kulcsának másolatát használva – ugyanazt a feladatot végzi. Ha a két válasz megegyezik, akkor a SIM-kártya hitelesítése sikeres.

Ezt követően – ugyanazt a véletlenszámot, valamint a SIM-kártya privát kulcsát használva – mind a mobil, mind az AuC egy másik algoritmussal egy titkos kulcsot generál. Ezt a kulcsot nem küldik ki a rádiós hálózatba, de a mobil és a hálózat egyaránt ezt alkalmazza az adatcsomagok titkosításakor.

Mi következik mindebből? Az, hogy a GSM-hálózaton folytatott beszélgetések meglehetősen nagy biztonságban vannak. Ha valakinek sikerül elfognia az adatokat, hihetetlenül bonyolult feladat feltörni a titkosítást. Szakértők szerint teljesen valószínűtlen, hogy hatalmas számítógépes háttér nélkül ezt a feladatot bárki valós időben végrehajtaná.

Mivel a SIM-kártya soha nem fedi fel privát kulcsát, az is teljességgel valószínűtlen, hogy a jel megszerzésével lehessen klónozni a SIM-kártyát.



*Privát kulcs*

## Hosszadalmas kártyamásolás

Nem kizárt (bár rendkívül költséges és nehéz) a SIM-kártya másolása. Ha valaki fizikailag hozzáfér a SIM-kártyához, és rendkívül sok türelme van, akkor a következőt teheti: betáplál a SIM-kártyába 150 ezer különböző alapszámot, majd feljegyzi az azokra kapott válaszokat. Ezt követően megfordítja a folyamatot: a korábbi válaszokat táplálja be, és figyeli, hogy mit felel rájuk a SIM-kártya. Így megszerezhető a privát kulcs. E feladatot dedikált hardver és szoftver tudja csak elvégezni, sok-sok órás munkával.

Elméletileg ugyanez az eljárás a rádiós hálózaton keresztül is lefolytatható. Fel kellene állítani egy ál-bázisállomást (valamelyik bázisállomás utánzatát), amely kapcsolatba lépne a mobilkészülékkel, majd arra utasítaná a SIM-kártyát, hogy válaszoljon az elküldött alapszámokra.

Már csak azért is tűnik mindez valószínűtlennek, mert a mobiltelefon akkumulátora jóval a folyamat befejezése előtt lemerülne.

Végül, de nem utolsósorban említést érdemel a SIM-kártya adatainak a másolása. A ma használatos szoftverek csak a kártya telefonkönyvének adatait másolják át, nem pedig a biztonsági beállításokat vagy a SIM-kártya azonosságát.

**Mallász Judit**

# Bluetooth-biztonság: legendák és tények

***A vezetéknélküli adatátviteli mód nem olyan sebezhető, mint egyesek terjesztik, de kétségtelenül léteznek biztonsági kockázatai.***

A rádióátvitelen alapuló, kis hatótávolságú, vezetéknélküli technológia, a Bluetooth alapjait az Ericsson kutatói dolgozták ki 1994-ben. 1998-ben számos távközlési világcég (Ericsson, Nokia, Toshiba, Intel, IBM stb.) közreműködésével létrejött a Bluetooth Special Interest Group (SIG), amely máig ellátja a technológia gazdájának szerepét. A Bluetooth a kis teljesítményű sugárzásokra szabadon használható 2,4 gigahertzes sávon működik, hatótávolsága 10–100 méter, maximális adatátviteli sebessége 723 kilobit/másodperc. Egy pont egyszerre több ponttal állhat kapcsolatban, a rendszer számára definiált úgynevezett picohálózatot egyszerre nyolc egység használhatja.

*Zaklatások célpontja lehet*

Az első Bluetooth eszköz egy Ericsson headset volt, amelyet azóta mobiltelefonok, PDA-k, autó-kihangosítók és másfajta eszközök sokasága követett. A kényelmesen használható technológia mára hatalmas népszerűségre tett szert, a gyártók hetente több millió új eszközt szállítanak, és az IDC adatai szerint 2008-ra a Bluetooth-képes eszközök száma megközelíti az egymilliárdot.

Természetesen mint minden olyan vezetéknélküli technológiánál, ahol a küldő és fogadó között nem lehet jól körülhatárolni az adatátvitelt, a kommunikáció itt is védett csatornán valósul meg, hangsúlyosan vetődik fel ugyanakkor az adatbiztonság kérdése.

Egyes szakértők hajlamosak felnagyítani a Bluetooth ilyen irányú veszélyeit, de ha leszámítjuk is a szenzációhajhász túlzásokat, bizonyos biztonsági problémákkal mindenképp számolnunk kell.

## Jogosulatlan és sérelmes

A Bluetooth biztonsági problémái négy csoportba oszthatók:

- jogosulatlan hozzáférés a vezérléshez;
- jogosulatlan hozzáférés az adatokhoz;
- lehetőség a névtelen kommunikációra;
- beazonosítás, nyomkövetés, „kiszimatolás".

Lássuk a gondokat közelebbről! A jogosulatlan hozzáférés a vezérléshez (a szakirodalomban elterjedt nevén *bluebugging*) azt jelenti, hogy a szakértő hacker az eszköz tulajdonosának tudtán kívül részben vagy egészben hozzáfér az eszköz szolgáltatáskészletéhez, és lényegében azt csinál a berendezéssel, amit akar. Egy mobiltelefonról például nemzetközi hívásokat kezdeményezhet, vagy sms-t küldhet, és ezzel akár egy bombariadót is kiválthat, annak minden erkölcsi-anyagi felelősségét a tulajdonos nyakába zúdítva.

Vagy hogy egy másik alkalmazási területről hozzunk példát: az autó Bluetooth-kihangosítójának segítségével lehallgathatja az autóban zajló beszélgetést.

A jogosulatlan adathozzáférés (másnéven *bluesnarfing*) esetében a hacker az eszköz (jellemzően ismét csak mobiltelefon) tulajdonosának tudta nélkül garázdálkodhat a berendezésen tárolt címtárak, naptárak, képek, névjegykártyák stb. között: szabadon írhatja, olvashatja vagy le is töltheti őket.

A névtelen kommunikáció lehetősége nem kevesebbet jelent, mint hogy a hozzáértő felhasználó (aki akár egy bűnöző vagy terrorista is lehet) a Bluetooth-eszközök közötti kommunikáció első, az eszköz nevének továbbítására szolgáló részét rövid, maximum 248 karakteres üzenetek forgalmazására használhatja fel. Ez a technika módot ad a hatóságok által beazonosíthatatlan kommunikációra.

Végül a „kiszimatolás" *(sniffing)* azt jelenti, hogy viszonylag egyszerűen összebarkácsolható antennás összeállítások birtokában az aktív eszközök nagy (a normál Bluetooth-hatótávot többszörösen meghaladó) hatókörben betájolhatók és beazonosíthatók, így elvileg hackertámadások vagy egyszerű zaklatások *(bluejacking)* célpontjaivá válhatnak.

Több szkennelő eszköz felhasználásával olyan térfigyelő rendszer is kiépíthető, amely egy objektumon (például áruházon) belül vagy szabad téren módot ad az alanyok mozgásának pontos nyomkövetésére, ami feltétlenül a magánélet sérelmét jelenti.

A harmadik probléma (az anonim üzenetküldés lehetősége) elsősorban a hatóságokat érinti, a többi viszont minden Bluetooth-felhasználót. A fő kérdés: milyen mértékű a veszélyeztetettség, és mit tehetünk a kockázatok csökkentésére.

## Többszintű biztonság

A Bluetooth-technológia többszintű biztonsági rendszert alkalmaz. A kommunikációkat erős titkosítás védi. Eszközszinten a legfontosabb védelmi mechanizmus az a lehetőség, hogy a berendezés „rejtett", más néven „láthatatlan" módba kapcsolható át. Ilyenkor az eszköz nem jelenik meg más Bluetooth-eszközök keresési listáján, és külső megfigyelők számára érzékelhetetlenné válik, miközben azokkal a Bluetooth-eszközökkel, amelyekkel már korábban párosították, továbbra is zavartalanul használható.

Léteznek bizonyos technikák a rejtett módba kapcsolt eszközök felfedezésére, de ezek a címtartomány végigszkennelésén alapuló eljárások ma még túl hossza-


dalmasak ahhoz, hogy gyakorlati veszélyt jelentsenek.

A párosítás szintén a biztonságot szolgálja. A Bluetooth-eszközöket a kommunikáció megkezdése előtt egy többjegyű PIN-kód beírásával „be kell mutatni" egymásnak: a párosítás során a technológia a PIN-kódokból egy bonyolult algoritmussal olyan kulcsot generál, amelyet a továbbiakban a megbízható kapcsolat azonosítására használ.

Végül a szolgáltatások szintjén három előre definiált biztonsági szint létezik: szolgáltatások, amelyek hitelesítést és jogosultság-ellenőrzést igényelnek; szolgáltatások, amelyek csak hitelesítés után használhatók; és szolgáltatások, amelyek minden eszköz számára elérhetőek. A gyártó maga dönti el, hogy termékein melyik kategóriába teszi az egyes szolgáltatásokat.

Ideális esetben, ha mindig láthatatlan módba kapcsoljuk a Bluetooth-eszközt, amikor nem használjuk; ha élünk az eszköz nyújtotta biztonsági lehetőségekkel, és szigorúan csak megbízható eszközzel párosítjuk a berendezésünket; valamint ha az eszköz gyártója is kellő körültekintéssel jár el, és a Bluetooth szabvány gondos implementációjával megvédi a fontos szolgáltatásokat, ez a védelmi szisztéma rendkívül megbízható. A gyakorlatban azonban a hackerek több ponton is fogást találhatnak a rendszeren.

## Párosodási ösztön

Az első hibaforrás maga a felhasználó – pontosabban a felhasználói könnyelműség. Ennek szintjét jól jellemzi az a teszt, amelyet egy biztonsági szakember végzett nagy, dél-kelet-ázsiai bevásárlóközpontokban. Az eredmény elég megdöbbentő: a tesztelő úgy találta, hogy az aktív, látható Bluetooth-képes mobilok tíz százaléka minden fenntartás nélkül hajlandó volt összekapcsolódni az ő ismeretlen eszközével. Valószínűleg nem is sejtették, hogy ezáltal nemcsak ők fogadhatnak adatokat a másik féltől, de a saját rendszerükön lévő adatokat is tálcán kínálják az ismeretlen partnernek.

De ha a felhasználó az ilyenfajta csapdákat elővigyázatosan elkerüli is, és csak megbízható eszközökkel lép kapcsolatba, akkor sincs teljesen biztonságban. Ma már bizonyítottan léteznek olyan hackertechnikák, amelyekkel a támadó a megbízható felek között kikényszeríti a kapcsolati kulcs újragenerálását, a forgalmat elfogja, és a kapcsolati kulcsból megfelelő algoritmussal kiszámítja a felhasznált PIN-kódot, majd saját eszközét az egyik megbízható félnek álcázva hozzáfér a másik eszközhöz. A módszer sarokpontja a PIN-kód visszafejtése: ha a kód nem négyjegyű (általában ez az alapértelmezés), hanem hosszabb, az algoritmus működési ideje nagyságrendekkel nő, és az akció kivitelezhetetlenné válik.

A biztonsági kockázatot tehát a rövid PIN-kód jelenti: a felhasználó megfelelően erős PIN-kód választásával ezt a rést könnyen betömheti.

## Elővigyázatos használat

A harmadik hibaforrás a gyártó, illetve az a hanyagság, ahogy a Bluetooth-szabványt implementálja. Korábban több nagy márka (Nokia, Sony Ericsson stb.) mobiljáról kiderült, hogy a felhasználó tudtán kívül adatok szipkázhatók le róluk. A hibát az okozta, hogy fontos szolgáltatásokhoz a biztonságos használatot garantáló engedélyezési folyamat megkerülésével lehetett hozzáférni. Ez gyártói felelősség: a cégek az eszközök szoftverének frissítésével orvosolták a bajt, és az újabb modellek tervezésekor már körültekintőbben jártak el. Ilyenfajta, implementálási hibákból eredő biztonsági résekre bármikor újból fény derülhet: védelmet ellenük a szoftverek frissítése jelent.

Összességében tehát azt mondhatjuk, hogy a felhasználó egyáltalán nem kiszolgáltatott a támadásokkal szemben. Amennyiben eszközét lehetőség szerint mindig rejtett módba kapcsolja át, és csak akkor használja, amikor tényleg kell; körültekintően jár el a kapcsolatok engedélyezésénél; és kihasználja a készülék által nyújtott biztonsági lehetőségeket (például erős PIN-kódot választ), az illetéktelen hozzáférések és támadások, valamint magántitok-sértések veszélyét az elméleti lehetőségek birodalmába száműzheti.

Ez hatványozottan igaz az ugyancsak biztonsági kockázatot jelentő vírusokra. Mint köztudott, ma már léteznek olyan féregvírusok (például a Cabir), amelyek Bluetooth-kapcsolaton keresztül fertőzik meg az eszközöket. A fertőzéshez azonban szükség van arra, hogy a vírust tartalmazó elemet a felhasználó telepítse – ha ismeretlen forrásból érkező küldeményeknél ezt nem tesszük meg (ez amúgy is a hatékony vírusvédelem első és legfontosabb szabálya), a fertőzések ellen védve vagyunk.

**Tóth István**

# A törvény szava

***Az elektronikus számlázás szigorú jogi előírásokat támaszt a kibocsátókkal és vevőkkel szemben.***

Nem mondhatni, hogy egyszerű lenne teljesíteni az elektronikus számlákra vonatkozó követelményeket, amelyeket a 20/2004 számú pénzügyminiszteri rendelet ír elő. Az alábbiakban ismertetjük ennek fontosabb előírásait.

## Alapvető követelmények

Az elektronikus számláknak egyrészt meg kell felelniük a számukra kidolgozott követelményeknek, másrészt teljesíteniük kell a számlákra vonatkozó általános feltételeket.

Mindenekelőtt meg kell említeni, hogy elektronikus számlát kizárólag abban az esetben lehet kibocsátani, ha erről előzetesen megállapodtak a vevővel. A megállapodás nincs alakisághoz kötve, feltéve, hogy az elektronikus számlát elektronikus aláírással ellátott elektronikus adatként bocsátják ki. Ilyenkor a megállapodás történhet szóban és írásban egyaránt, sőt, ráutaló magatartással is megkötheto.

Ha azonban a számlázás elektronikus adatcsere (EDI) rendszerben történik, akkor a fent hivatkozott rendeletben meghatározott, előzetesen megkötött írásbeli szerződés alapján lehet csak számlát kibocsátani.

Kibocsátáskor és a számla őrzési időszaka alatt folyamatosan biztosítani kell a számla eredetének hitelességét, tartalmának teljességét, megváltoztathatatlanságát, sértetlenségét és olvashatóságát, a jogosultak általi hozzáférhetőségét, valamint a jogosulatlan hozzáférés, módosítás, törlés és megsemmisítés elleni védelmét. Mindezeket a követelményeket a rendelet előírása szerint fokozott biztonságú elektronikus aláírással és időbélyegzővel vagy EDI rendszerben végrehajtott továbbítással kell biztosítani. Az utóbbi esetben az adóalanyoknak a számlázásokról papír alapú összesítő dokumentumot kell készíteniük.

Az eredet hitelességén azt érti a rendelet, hogy technikai eszközök segítségével egyértelműen azonosítható legyen a számlát kibocsátó vállalkozó. Ami a tartalom sértetlenségét illeti, itt arról van szó, hogy a számla mindig egyezzen meg az eredetileg kibocsátottal, és semmilyen változtatást ne lehessen végrehajtani rajta. Az olvashatóság értelmezése: biztosítani kell, hogy a számla tartalmát az arra jogosultak az őrzési időszak alatt megismerhessék. Hasonlóképpen a hozzáférhetőség azt jelenti, hogy az illetékesek mindig hozzáférhessenek a számlához, az arra nem jogosultak pedig soha ne férhessenek hozzá, és ne tudják azt módosítani vagy törölni.

*A jogosulatlanok ne férhessenek hozzá!*

## Számlakiállítás

Kétféleképpen bocsátható ki elektronikus számla: elektronikus aláírással és időbélyegzővel ellátott elektronikus adat formájában vagy EDI rendszer alkalmazásával.

Az elektronikus iratok aláírásának rendjét a 2001. évi XXXV. törvény szabályozza, azaz: fokozott biztonságú aláírást vagy még ennél is szigorúbb követelményekkel rendelkező minősített e-szignót kell alkalmazni.

Az EDI rendszerben kiadott számlák technikai szempontból zárt rendszeren keresztül jutnak el a kibocsátótól a vevőig. Követelmény továbbá, hogy a felek előzetesen írásban megállapodjanak az EDI használatáról, és erre vonatkozóan a rendeletben megadott formájú szerződéssel rendelkezzenek.

Ugyancsak előírás, hogy az EDI rendszeren keresztül kibocsátott számlákhoz papír alapú összesítő dokumentumot kell készítenie havi rendszerességgel a számla kibocsátójának.

## Megőrzés

Az elektronikus számlát és (EDI rendszerben) az összesítő dokumentumot eredeti formájában kell megőrizni. Ez más szóval azt jelenti, hogy a papíron kiadott számlákat nem lehet kinyomtatva őrizni, ugyanis a szabályok szerint a számla kibocsátáskori formátuma igazolja az adófizetéssel összefüggő kötelezettségek és jogok meglétét. Fontos előírás az is, hogy az elektronikus számlákat csak az Európai Unió valamely tagállamának területén lehet megőrizni. Az adóhatóság felszólítására az adóalany három munkanapon belül köteles bemutatni az elektronikus számlát, továbbá az összesítő dokumentumot.

A számlák megőrzésére kötelezett adóalany a megőrzést végezheti saját maga, vagy megbízhat ezzel egy, a törvényi előírásoknak megfelelő archiválási szolgáltatót. Az előbbi esetben az adóalany köteles az elektronikus aláírással ellátott számlán egy arra feljogosított szolgáltatóval időbélyegzőt elhelyeztetni. Az utóbbi esetben a felek között megkötött szerződés alapján az archiválási szolgáltató szavatosságot vállal a számlák megőrzéséért.

Az alkalmazható elektronikus aláírás és időbélyegző mindenkori biztonságos algoritmusát az illetékes hatóság közleményben határozza meg.

Az elektronikus számlákat az adóhatóság .txt, formázott szöveget nem tartalmazó bármilyen nyomtatási állomány, valamint .xml formátumban fogadja el hajlékonylemezen vagy cd-n.

**Tóth István**

# IT-SECURITY SPECIAL

## Fontos vélemények

Az IT-biztonság Napjához közeledve egy 31 kérdésből álló kérdőívet állítottunk össze, és az átlagos fontosság sorrendjében áttekintjük, mi foglalkoztatja leginkább a szakterület (fő)szereplőit

32. OLDAL

## Hálózaton az adatot

A hálózati infrastruktúra biztonságának garantálása az alfája és ómegája az adatok védelmének – állítják a szakértők, de a leggyengébb láncszem még mindig az ember

33. OLDAL

## Kipipált kockázat

A vállalatok jó részénél szabályozott az informatikai biztonság, a kockázatkezelésre azonban még sok helyen nem fordítanak kellő figyelmet

34. OLDAL

## Az első lépés a legnehezebb

A biztonság felügyeletének és üzemeltetésének területén még sok a nyitott probléma. Érdemes-e foglalkozni vele? Ha igen, akkor hogyan? Mik az eszköz- és szervezeti vonatkozásai?

37. OLDAL


# Fegyelem, figyelem, finomhangolás

# Fontos vélemények

***Kérdések és válaszok az IT-biztonságról.***

Az IT-biztonság Napjához közeledve egy 31 kérdésből álló kérdőívet állítottunk össze. Megkértük az esemény részvevőit, hogy kitöltés közben fontosságuk szerint 1-től 5-ig osztályozzák a kérdéseket.

Terjedelmi okokból sajnos nem tudjuk közreadni az összes választ és a részletes statisztikát sem. Csak arra vállalkozhatunk, hogy az átlagos fontosság sorrendjében áttekintjük, mi foglalkoztatja leginkább a megkérdezetteket.

**Milyen a biztonsági incidensek kiindulási helyének (külső/belső) százalékos megoszlása? (Fontosság: 3,71)**

A válaszolók 20 és 50 százalék közötti külső, 50 és 80 százalék közötti belső kiindulási helyet adnak meg. A külső–belső arány átlagosan 35–65 százalék.

## NÉHÁNY TOVÁBBI KÉRDÉS

Kell-e lokális jelenlét, vagy jó megoldás a külföldi támogatás? (Fontosság: 3,7)

A közepes méretű hazai szervezetek hány százaléka készült fel katasztrófaelhárításra? (Fontosság: 3,66)

Egy közepes méretű hazai szervezet számára a jól összeválogatott „Best of Breed" vagy az integrált biztonsági megoldások a jobbak? (Fontosság: 3,6)

A Windows Vista megjelenése rontja vagy javítja a biztonsági fejlesztők piaci helyzetét? (Fontosság: 3,55)

**Mikorra válhat valósággá az, hogy minden biztonsági eszköz egy pontból felügyelhető legyen? (Fontosság: 3,72)**

*– A közös üzenetformátum kialakulásától függ.*

*– Talán nem is az egyetlen felügyeleti pont a leglényegesebb, hanem a legkisebb költségű felügyelet.*

*– Fontos, hogy a felügyeletet ellátó személyzetnek ne kelljen sok rendszert megtanulnia, mert sok a hibalehetőség.*

*– Technikailag most is lehetséges, de biztonsági – és ennek okán üzleti – szempontból nem minden esetben preferált.*

*– Soha, mert mindig jönnek újabb támadási technológiák, amelyek ellen új eszközök kellenek.*

*– Homogén rendszereknél többé-kevésbé megvalósítható; heterogén struktúrákban viszont utópia.*

*– Ilyen nem lesz, mivel ez egységes szabványt és felhasználást is feltételez MINDEN eszközre.*

*– Most is monitorozható, de a konfigurálás mindig külön történik majd.*

*– Amikor egy kézbe kerül az egész IT-biztonsági piac.*

*– Soha.*

**Egy közepes hazai cég információtechnológiai költségvetésének hány százalékát lenne célszerű IT-biztonságra fordítani? (Fontosság: 3,80)**

A válaszolók 8 és 30 százalék közötti értékeket adnak meg; az átlag 15 százalék. Néhány kommentár:

*– Nem a költségvetés arányában kell meghatározni, hanem a védendő értékek alapján.*

*– Attól is függ, hogy milyen eszközök vannak már meg.*

*– Ez sok mindentől függ: a cégprofiltól, a számítógépes munkahelyek számától. Egyszer valaki kiszámolta, hogy a cégek többsége jóval többet költ egy évben kávéra, mint informatikai biztonságra.*

**Melyik az a tudományos vívmány vagy új technológia, amelynek még nincs számottevő gyakorlati alkalmazása, de fontos szerepet tölt majd be az IT-biztonságban? (Fontosság: 3,83)**

*– A mesterséges intelligencia alkalmazása a biztonsági incidensek korrelálásában.*

*– A digitális páncélterem.*

*– Az IPv6.*

*– A viselkedés alapú védelmi megoldások.*

*– Az RFID-technológia, de az alkalmazása számos nem IT-biztonsági kérdést is felvet.*

*– A biometrikus azonosító eljárások.*

**A hazai cégek hány százalékánál elfogadható az IT-biztonsági helyzet? (Fontosság: 3,88)**

A becslések az 5–40 százalékos tartományban mozognak. Az átlagérték 15 százalék körül van.

**Hatékony technológia a behatolásvédelem? Érdemes alkalmazni? (Fontosság: 4,09)**

A válaszolók többsége szerint igen.

*– Nagy figyelmet és sok finomhangolást igényel.*

*– Mérhetően növeli a biztonsági szintet. Akkor érdemes használni, ha a kockázatelemzés indokolja.*

*– Igen, de nem szabad minden erőforrást a peremvédelemre összpontosítani. Belső hálózaton inkább hozzáférés-védelemről kell gondoskodni.*

*– Az integrált biztonsági megoldások fontos része.*

*– Feltétlenül. Csak ezzel csökkenthetők a sérülékenység alapú, célzott támadások.*

*– Általában nem. Csak a testre szabott megoldásoknak van értelmük.*

**A hazai cégek hány százalékánál történt az elmúlt évben az üzletmenetet komolyan befolyásoló biztonsági incidens? (Fontosság: 4,14)**

A válaszok 5 és 70 százalék között szóródnak. Az átlag nagyjából 30 százalék.

**Megoldódott-e a spam-helyzet? (Fontosság: 4,18)**

Általános vélemény, hogy nem.

*– A védekezési módszerek egyre összetettebbek, de sajnos mindig vannak új spam-megoldások.*

*– A spamet csírájában elfojtó technológiák ma még gyermekcipőben járnak.*

*– Sajnos nem lehet konkrét minta alapján védekezni.*

*– Nem beszélhetünk teljes győzelemről... A rabló–pandúr verseny még nem ért véget.*

*– Nem. Csak kezelhető.*

*– Sokat javult azoknál, akik megtanulták használni az antispam-technológiákat.*

**Egyre több multi van jelen a piacon. Hogyan érinti ez az ön szervezetét? (Fontosság: 4,36)**

*– Fontosabbak a költségek, mint a minőségi tudás, és ennek később negatív hatásai lehetnek.*

*– A kis és a nagy cégek megfelelő aránya a kívánatos. Egy multi stabilitása fontos háttér a kockázatokat kerülő IT-biztonsági piacon.*

*– Ez természetes. A lényeg, hogy a mennyiség ne menjen a minőség rovására.*

*– Pozitívan. A globális tapasztalat sokat segít a lokális védekezésben.*

*– Részmegoldásaikkal a core területet erősítik. Ha akarják, jók lehetnek, mert van erejük.*

*– Mint a piacon 6 éve jelenlevő multit, minket ez nem zavar...*

# Hálózaton az adatot

***A hálózati infrastruktúra biztonságának garantálása az alfája és ómegája az adatok védelmének – állítják a szakértők, de a leggyengébb láncszem még mindig az ember.***

***– Időnként hallani olyan véleményeket, hogy nem a számítógépes rendszereket, hanem az adatokat kell védeni. Hogyan vélekednek erről a kérdésről?***

**Hirsch Gábor, Cisco:** Szerintem az adatok és az infrastruktúra védelme nem választható el egymástól. Az adatokat nem csupán tárolni kell, hanem elérhetővé kell tenni különféle szolgáltatások számára, és ezeket a szolgáltatásokat az infrastruktúrán keresztül lehet igénybe venni. Különösen igaz lesz ez manapság, amikor egyre többféle adat és szolgáltatás kerül az IP-hálózatokra. Éppen azért kell védeni a hálózatot, hogy azon keresztül hozzáférhessünk az adatokhoz; ebből adódóan a hálózat védelme jóval összetettebb dolog, mint az adatvédelem.

**Illés Márton, Balabit:** A hálózat azért is nagyon jó hely az adatok megvédésére, mert használat közben az adatoknak át kell haladniuk a hálózaton, mint ahogyan a kívülről jövő támadásoknak is a hálózatot kell igénybe venniük. A védelem első vonalát ott kell kiépíteni, ahol hozzá lehet férni az adatokhoz.

***– Örök téma az is, hogy érdemes-e a védelmi funkciókat egyetlen eszközben ötvözni, vagy minden feladatra dedikált rendszert alkalmazni. Ezt önök hogyan látják?***

**Márton János, Computerlinks:** Jól látható tendencia, hogy kezd eltűnni a határ az egyes védelmi eszközök között. A hagyományos tűzfalakat ellátják behatolásdetektálási vagy vírusvédelmi képességekkel, és így tovább. Manapság már szinte minden gyártó a zászlajára tűzte az integrált védekezés, az úgynevezett Unified Threat Management (UTM) koncepcióját.

**Illés Márton:** Érzésem szerint az UTM-eszközök inkább csak a kis- és közepes vállalatok számára jelenthetnek jó megoldást, a nagyvállalatoknak inkább meg kell maradniuk a különálló eszközöknél. Ha azonban az UTM a központi felügyelet lehetőségét jelenti, vagyis hogy egyetlen helyről lehet kezelni a különféle védelmi eszközöket – legyenek azok egybeépítve vagy külön dobozokban –, akkor mindenképpen komoly lehetőségeket látok benne.

**Márton János:** Az UTM-eszközöket nagyvállalatok is használják. Meg tudom érteni ugyanakkor azokat is, akik nem minden gyártó esetében látnak garanciát arra, hogy az egybeépített eszközökben minden modul egyenértékűen a legmagasabb színvonalat képviseli.

**Csinos Tamás, DNS Hungária:** És akkor még nem beszéltünk arról a kérdésről, hogy mi számít Magyarországon közepes vagy nagyvállalatnak. Ugyanakkor én is azon a véleményen vagyok, hogy az UTM-eszközöknek a kisebb cégek körében is van létjogosultságuk, különösen amíg nem javul nagymértékben a biztonsági tudatosság.

***– Miért, hogyan áll Magyarországon az információbiztonsági tudatosság?***

**Soós Zoltán, DNS-Hungária:** A teljes védelmi rendszerben minden bizonnyal az ember a leggyengébb láncszem, minden információ rajtuk keresztül szerezhető meg a legkönnyebben. És ami a legfontosabb, ez ellen informatikai eszközökkel nem igazán lehet védekezni (bár az infrastruktúra, a jogosultsági rendszerek helyes kialakítása segíthet), hanem az emberek gondolkodásmódját kell megfelelőképpen átalakítani.

**Hirsch Gábor:** Ezen a téren is óriási különbségek vannak a nagyobb és kisebb vállalatok között. A nagy cégek 90 százalékánál már működik például tűzfal, de egyébként is sokkal összehangoltabbak a rendszereik. Minél kisebb egy cég, annál kevésbé valószínű, hogy gondot fordít az informatikai infrastruktúra védelmére.

Csinos Tamás, Hirsch Gábor, Illés Márton, Márton János, Soós Zoltán

**Márton János:** Pontosan emiatt lehet jelentőségük a kisebb cégek körében az UTM-rendszereknek (akár a távolból felügyelve is), hiszen ezekkel könnyebben megoldható a kisebb cégek védelme.

***– Hogyan állunk Magyarországon az IT-biztonsági távszolgáltatásokkal?***

**Hirsch Gábor:** Évek óta Magyarországon is elérhetők a menedzselt szolgáltatások, de ennek ellenére eléggé kicsi a piac – pontosan a tudatosság alacsony szintje miatt.

**Csinos Tamás:** Érdekes, hogy nálunk ezeket a szolgáltatásokat inkább azok a nagyvállalatok veszik igénybe, amelyek egyébként jó eséllyel tudnának kiállítani saját IT-biztonsági csapatot is. A közepes és kisebb méretű vállalkozások, amelyekre ezeket a szolgáltatásokat külföldön leginkább kitalálták, viszont nem kérnek belőle, több okból sem.

Egyrészt, a teljes körű szolgáltatások többnyire drágák, hiszen nagyobb cégek számára fejlesztették ki őket; másrészt félnek attól, hogy az adataik cégen kívülre kerülnek; harmadrészt egyelőre nem érzik annyira fontosnak a kérdést, hogy külön pénzt adjanak érte.

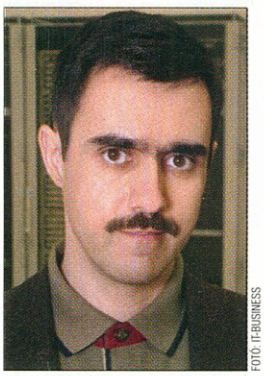
Ha akarnának, gyakorlatilag az összes internetszolgáltatótól lehet rendelni alapvető spamszűrést vagy tűzfalszolgáltatást; arról már nem beszélve, hogy a legegyszerűbb ADSL-routerben is komoly tűzfalszoftver működik, csak használják ki.

# Kipipált kockázat

***A vállalatok jó részénél szabályozott az informatikai biztonság, a kockázatkezelésre azonban nem fordítanak kellő figyelmet.***

***– Mennyire éreztetik hatásukat a különféle nemzetközi szabályozások Magyarországon?***

**Zsiday Béla, PSZÁF:** Ez leginkább az amerikai tulajdonú pénzügyi szervezeteknél tapasztalható, amelyek a Sarbanes–Oxley-törvény (SOX) alapján végzik tevékenységüket. Ennek alkalmazása terjedőben van a több európai országban jelen lévő pénzintézeteknél is, és keveredik az európai uniós előírásokkal. Ugyanakkor az ilyen cégekkel együttműködő hazai vállalkozásoknak is elemi érdekük igazodni a SOX követelményeihez.



FOTÓ: IT-BUSINESS

Fábián János

**Vécsi László, Abesse:** Természetesen a SOX hatálya nemcsak a pénzügyi szervezetekre terjed ki, hanem minden olyan cégre és ezek leányvállalataira, amelyek jelen vannak az amerikai tőzsdéken. A Sarbanes–Oxley 404-es szakasza vonatkozik az informatikára, amelynek előírásait más módszertanokkal is le lehetne fedni, az érintett cégek azonban egyszerűen csak ki akarják pipálni ezt a feladatot, nem alkalmazzák például a BS7799-et vagy az ISO 27001-et.

**Fábián János, Icon:** Az Európai Unió 8. direktíva módosításának 2007 tavaszán várható hatályba lépése előtt Magyarországon valóban a SOX tűnik a legnagyobb közvetlen hatású nemzetközi szabályozásnak. Ennek fő oka, hogy a hazai cégek közül a TOP 200 jelentős részét érinti. E cégek törvényi kötelezettségei egyrészt befolyásolják az általános hozzáállást, kezelési kultúrát a szabályozott területeken, másrészt méretüknél fogva továbbsugárzó hatásuk van a tanácsadói tevékenységre és a biztonsági piacra is.

***– Léteznek-e a pénzügyi szektorra vonatkozó előírásokhoz hasonló informatikai szabályozások más iparágakban is?***

**Vécsi László:** Szinte minden iparágra megvannak a szabályozások, ilyen többek között a HIPAA (Health Insurance Portability and Accountability Act) az egészségügyben vagy hazai példát említve az Állami Számvevőszék informatikai audit-előírásai. De minden olyan szervezetre vonatkoznak törvényi előírások, amelyek például adatkezeléssel foglalkoznak. Ezek közül kiemelkedik a telekommunikációs szektor, de érintettek a közművek és egyéb szolgáltatók is, illetve azok a cégek, amelyek hűségkártya-programokat folytatnak.

**Krasznay Csaba, BME:** A kormányzatnak is van rendeletszintű utasítása, amely előírja, hogy a közigazgatásban részt vevő egységeknek foglalkozniuk kell a kockázatkezeléssel.

**Fábián János:** A pénzügyi szektor messze a leginkább szabályozott nálunk. A szigorúsági sorrendben a következő a kormányzat. Ezeket a szektorokat külön szervezetek ellenőrzik, mint a PSZÁF vagy az ÁSZ. A többi szektorra vonatkozó előírások jórészt csak közvetve vezethetők le az általános jogszabályokból. Ellenőrzésük is inkább csak egy-egy kirívó eset kapcsán kerül szóba, pedig többek között a közműszolgáltatók és az egészségügyi intézmények is kezelnek érzékeny adatokat.

***– Érzékelik-e a hazai cégek, hogy a kockázatelemzés és -kezelés a biztonsági projektek kiindulópontja?***

**Vécsi László:** Minden módszertan, minden szabályozás azt követeli meg, hogy a kockázatelemzésből, majd később kockázatkezelésből kell kiindulni. A mi tapasztalataink azonban azt mutatják, hogy a cégek először részproblémákat kezdenek megoldani, olyasmiket, amelyeket sürgősnek ítélnek, és amelyekre jut pénz. Sokszor előfordul, hogy nem is tudják, milyen kockázatok merülhetnek fel a szervezeten belül, vagy hogy ezeket miként szokták mások kezelni.

**Zsiday Béla:** Az én megítélésem szerint a cégek nagy része láncépítés helyett karikákat gyárt, a nagy igyekezetben egyszerre lát neki mindennek, a kockázatfelmérésnek, a kockázatelemzésnek, és egyúttal keresi a megoldást is. Aki valamennyire is ért ehhez a szakmához, az jól tudja, hogy ez így nem megy. Nincs olyan dokumentált módszertan, amelyik megengedné, hogy az egymás után következő lépéseket egyszerre lépjük meg. Mindenekelőtt módszertant kell választaniuk, és azt végigkövetni, nem pedig az előírások egymás utáni kipipálásával kellene foglalkozniuk.

**Krasznay Csaba:** Tapasztalataim szerint ha a kockázatelemzés meg is történik, azt általában nem követi a kockázatkezelés.

**Zsiday Béla:** Ezt én is meg tudom erősíteni: tudok olyan cégről, amelyiknél a 2002-ben elvégzett kockázatelemzést nem követte felülvizsgálat, az akkori felmérés eredményét a mai napig elfogadják mint hiteles kockázatminősítést.

**Fábián János:** Kockázatkezelés terén a legtöbb cég egyszerűen arra törekszik, hogy ha jogszabály kötelezi rá, akkor pro forma kipipálhassa a feladatot. Élő, tudatosan irányított, tervezett kockázatmenedzsment-rendszer csak az olyan szervezeteknél alakult ki, ahol a törvényi kötelezettség mellett közvetlen üzleti kárt okozna a hiánya – vagyis a nagyobb pénzintézeteknél.

***– Saját maguk is fel tudnák mérni a cégek a kockázataikat?***

**Vécsi László:** A legtöbb cég nem rendelkezik az ehhez szükséges szakértelemmel. Én nem hiszek abban, hogy egy kinyomtatott módszertan alapján el lehetne végezni a felmérést. Támogatni azonban lehet ezt a törekvést.

**Krasznay Csaba:** Ez egy külön megtanulandó szakma, én egyetemi emberként úgy vélem, hogy a felsőoktatásban vagy posztgraduális szakokon nem képeznek olyan szakembereket, akik magas szinten tisztában lennének a kockázatelemzés módszertanával.

**Fábián János:** Valóban külön szakma a kockázatmenedzsment, ráadásul számos ága van. Az üzleti folyamatokból származó pénzügyi kockázatok kezelése más szakértelmet igényel, mint az informatikai működési, biztonsági kockázatoké. Tanácsadó cégek között is ritka, amelyik mindkettőhöz egyformán jól ért. ■

# Megmondom, ki vagy!

***Az azonosság- és hozzáférés-kezelő megoldások piaca egyelőre lassan gyarapszik, de a technológia előtt nagy jövő áll.***

***– Az azonosság- és hozzáféréskezelés (identity and access management) témaköre már több éve „benne van a levegőben". Mennyire időszerű ez a technológia, és hol járnak az adaptálásában a magyar vállalatok?***

**Bártfai Attila, HP:** Továbbra is megállják a helyüket azok az érvek, amelyek e rendszerek bevezetése mellett szólnak, sőt, inkább csak erősödtek azok a tényezők – a help deskre nehezedő nyomás, az elszámoltathatóság követelménye –, amelyek szükségszerűvé teszik a technológiát. Ugyanakkor az eltelt idő csak arra volt jó, hogy a felhasználók ismerkedni kezdjenek a technológiával; a pénzügyi és a távközlési szektoron kívül egyelőre viszonylag kevés projekt indult.

**Keleti Arthur, Icon:** Gyakran tapasztaljuk, hogy a cégeknél az azonosságkezelési rendszerek bevezetésének szervezeti előfeltételei is hiányoznak. Nincsenek definiálva a szerepkörök, nem tudják, hogy kinek mihez van jogosultsága, és éppen ezért félve nyúlnak a témához, nehogy kiderüljenek az eltitkolt hiányosságok. Sok helyen akár egy-két év is eltelhet, mire eljutnak egyáltalán odáig, hogy nekiállhatnak bevezetni egy informatikai rendszert – addig csupán a szervezeti átalakítás, a szerepkörök és jogosultságok tisztázása folyik, ez pedig egyáltalán nem informatikai feladat, ugyanakkor fontos első szakasza egy jogosultágkezelési projektnek.

**Gazsó Gábor, Bull:** Ugyanakkor arra is van lehetőség, hogy megfelelő szervezéssel a projekt informatikai részét az előkészítő tanácsadói munkával párhuzamosan megkezdjük. Ha a két szakaszt hermetikusan különválasztjuk, egy soha véget nem érő tanácsadói munka lesz a bevezetésből.

***– Az eddigi tapasztalatok szerint mik a projektek legnagyobb buktatói?***

**Bártfai Attila:** Egy azonosság- és jogosultságkezelési projektet a szokásosnál is jobban körbe kell bástyázni felsővezetői támogatással. Ráadásul olyan vezetőkkel is együtt kell működni – például a HR-főnökkel –, akikkel a „hagyományos" informatikai bevezetések során ritkán találkozik a szállító.

**Márton János, Computerlinks:** Nagyon fontos ezért mindenkivel személyre szabottan, a saját munkájához kapcsolódóan megértetni, hogy számára milyen előnyöket jelent a rendszer működtetése. A pénzügyi vezető a megtakarításra lehet érzékeny, az operáció vezetője számára pedig az lehet a haszon, ha az új munkatárs nem két hét, hanem egy délelőtt alatt megkaphatja minden jogosultságát, és munkába állhat.

**Gazsó Gábor:** Ez persze nem mindig könnyű. Az emberek hajlamosak rá, hogy azonnal fenyegetettnek érezzék magukat, ezért arról kell meggyőzni őket, hogy egy ilyen rendszer nem helyettesíti őket, hanem a munkájukat teszi könnyebbé.

**Keleti Arthur:** Az informatikai jellegű problémák között említhetném az olyan öröklött (legacy) alkalmazások meglétét, amelyeket nem készítettek fel arra, hogy a jogosultságokra vonatkozó információikat megosszák más alkalmazásokkal. Sok esetben ezek olyan egyedi vagy külföldi fejlesztésű rendszerek, amelyekhez senki sem nyúl szívesen, és emiatt igen nehéz, de nem lehetetlen velük az adatkapcsolat kialakítása. A jogosultságkezelési projektek integrációs fázisának pedig ez a legfontosabb része.

Bártfai Attila, Gazsó Gábor

***– Eddig inkább az azonosságkezelésről beszéltünk. Mi a helyzet a hozzáférés-kezelés terén Magyarországon?***

**Bártfai Attila:** Ez a technológia két megoldandó kérdés kapcsán szokott felmerülni: az egyik a webes hozzáférés-kezelés, a másik az egész vállalatra kiterjedő egyszeres bejelentkezés.

**Keleti Arthur:** Én, mint rendszerintegrátor, óva intenék mindenkit attól, hogy egyszerre vágjon bele az azonosság- és hozzáférés-kezelési projektbe. Az utóbbi valamilyen szinten egyébként majdnem minden vállalatnál megtalálható, hiszen az informatikai rendszerekhez való hozzáférést már eddig is biztosítani kellett.

**Márton János:** Ugyanakkor vannak olyan megoldások, ahol a két terület egészen jól összekapcsolható. Megoldható például, hogy más jogosultságai legyenek ugyanannak a felhasználónak, ha a vállalaton belülről vagy ha kívülről, VPN-en jelentkezik be a céges alkalmazásokba. Ennek óriási jelentősége lehet az adatvédelem szempontjából, hiszen így meg lehet akadályozni, hogy külső, nem biztonságos számítógépekre töltsék le a bizalmas információkat.

**Gazsó Gábor:** A cégek inkább a weben keresztül bejelentkező ügyfelek, mint a belső dolgozók számára könnyítik meg először a belépést. Pedig érdemes lenne figyelembe venni azt is, hogy egy belső projekt kevesebb kockázattal jár, megfelelő mennyiségű tapasztalatot nyújt, és a belső folyamatok egyszerűsítésén keresztül csökkenti a költségeket.

***– Mi lehet a technológiai fejlődés iránya a most tárgyalt területeken?***

**Keleti Arthur:** Érdekességként vetném fel, hogy vannak például olyan jövőbe mutató kezdeményezések, hogy ne az alkalmazásokban kelljen állítani a jogosultságokat, hanem ezeket az információkat maga az adatcsomag „cipelje magával". Vagyis az adat akármilyen rendszerbe is kerülne át, mindig ugyanazokkal a jogosultságokkal bírna.

**Márton János:** Ennek azért még messze lehet a gyakorlati megvalósítása, hiszen egy ilyen megoldás elképzelhetetlen a széles körű szabványosítás nélkül.

**Bártfai Attila:** Ezt a funkcionalitást a meglévő rendszerekbe nem nagyon lehetne beépíteni, ezért szerintem csak hosszabb távon lehet életképes. Addig viszont mindenképpen szükség lesz a hagyományos megoldásokra.

# Javuló biztonság

***Napjaink újszerű támadásai – amelyeket haszonszerzési céllal indítanak – mind összetettebb védekezési módszereket igényelnek.***

***– Melyek napjaink legveszélyesebb fenyegetései?***

**Szabó Gábor, Microsoft:** Régebben a viszonylag nagy informatikai tudással rendelkező hackerek próbáltak meg behatolni egy kiszemelt rendszerbe. A mostani támadások automatizáltak, több célpontjuk van, az elkövetők pedig kevésbé képzettek, és fő céljuk az anyagi haszonszerzés. Manapság a klasszikus vírustámadások – bár megvannak – kevésbé jelentenek veszélyt, ugyanakkor virágzik a cross site scripting, az adathalászat, a spamküldés, valamint a rejtőzködő rootkitek és a kémprogramok terjesztése. Ugyancsak a veszélyes újszerű fenyegetettségek közé tartozik a website defacement, ami azt jelenti, hogy lemásolják például egy bank weboldalát, hogy az ügyfeleket félrevezessék. Itt jegyzem meg: a mai támadások elleni védekezést megnehezíti, hogy azok a korábbiakkal ellentétben két olyan ajtón keresztül – a web és az e-mail – zajlanak, amelyeket nem lehet lezárni.

**Gyurik Csaba, VirusBuster:** Több szempontból közelíthetjük meg a fenyegetettségeket. Egyrészt vannak a cégek ellen, ismeretlenek által, informatikai módszerekkel végrehajtott külső támadások, másrészt beszélhetünk a vállalatoknál dolgozók által szándékosan vagy akaratlanul elkövetett károkozásról. Olykor valaki csak azért vállal munkát egy cégnél, hogy annak bizalmas adatait megbízójának kiszolgáltassa. Más esetekben a munkavállalók tudatlansága vezet információk kiszivárgásához.

**Szabó Gábor:** Nagyon nehéz elmagyarázni az átlagfelhasználóknak, hogy milyen veszélyek leselkednek rájuk például egy e-mail megnyitásakor. Az arc nélküli támadókat pedig nem lehet felelősségre vonni, mivel a legtöbb esetben olyan országokból indítják a támadást, ahol az efféle bűncselekményeket egyáltalán nem szankcionálják.

***– Milyen védekezési módszerekre van szükség?***

**Gyurik Csaba:** Alapszintű biztonságot kínál az alkalmazottak által elérhető webtartalmak szabályozása, ráadásul ez olcsón megoldható. Figyelmet kell fordítani továbbá a behatolás elleni védelemre, a vírus- és spamszűrésre, a szoftverfrissítésekre és hasonlókra. Igen fontos a vállalati hálózatba belépő felhasználók

FOTÓ: IT-BUSINESS

**Szabó Gábor, Gyurik Csaba**

megfelelő szintű azonosítása, annak biztosítása, hogy az egyes erőforrásokhoz csak az arra jogosult személyek férhessenek hozzá. Ha sorrendiséget kellene felállítani, akkor a vírus-, a spamszűrés, a tűzfal és az autentikáció, amivel először foglalkozni kell, majd a többi biztonsági rendszerre is figyelmet kell fordítani egy nagyvállalatnál.

**Szabó Gábor:** A régi módszer, miszerint mindenki mindenhez hozzáférhet, ma már nem alkalmazható. Meg kell határozni, hogy a felhasználók milyen weboldalakat és e-maileket nyithatnak meg, milyen programokat futtathatnak, mely hálózati szegmensekhez férhetnek hozzá. Külön kell vizsgálni a felhasználók és gépük jogosultságát, ha ugyanis valakinek fertőzött a számítógépe, az a felhasználói jogosultságával ne léphessen be a hálózatba. Hasonló szegmentációs folyamat zajlik az alkalmazások világában is: a biztonság fokozása érdekében megszabják, hogy egy alkalmazás milyen rendszererőforrásokhoz és memóriaterületekhez férhet hozzá. A rosszul megírt programok ugyanis komolyan veszélyeztetik a biztonságot.

***– A Windows Vista megjelenése mennyiben növeli a biztonságot?***

**Szabó Gábor:** A Windows Vista teljes architektúráját úgy fejlesztették, hogy illegálisan ne lehessen hozzáférni a rendszerhez, amelynek a magja és kritikus részei nagyon jól elszigeteltek. Amikor például valami be akar írni a rendszerkönyvtárba, de nincs rá jogosultsága, a rendszer egy virtuális könyvtárat emulál a számára. A programok szeparáltan és védetten futnak, a védelem többszintű, a BitLocker titkosítással pedig elérhetetlenné lehet tenni a kritikus adatokat. Beépített biztonsági szolgáltatások védik a felhasználókat – a tűzfal, a szülői felügyelet és a kémprogramok elleni védelem, vagy a phishing-szűrő, .

**Gyurik Csaba:** Régóta foglalkozunk a Windows Vistával, hiszen ezt az operációs rendszert a jövőben támogatnunk kell. A Windows Vista biztonsági újdonságai miatt nekünk is módosítanunk kell a védelmet. Az újdonságok az alacsony (kernelszintű) és a magasabb (felhasználói szintű) rétegeket, valamint az azok közötti kommunikációt is érintik. Ezeknek a biztonsági követelményeknek meg kell felelnie minden antivírus-terméknek.

**Szabó Gábor:** Az új operációs rendszerbe beágyazott védelmi megoldások egy új, rendszerszintű biztonsági zónát alkotnak. Előtérbe kerül továbbá a hozzáférés-kontroll, amelynek révén egy fertőzött gép vagy egy jogosulatlan felhasználó nem kapcsolódhat a hálózathoz, megelőzve ezzel egy esetleges incidenst. A Windows Vista tehát proaktív védelmet valósít meg, reaktív védelemmel kiegészítve.

# Az első lépés a legnehezebb

*A biztonság üzemeltetésének és felügyeletének területén még sok a nyitott probléma. Érdemes-e foglalkozni vele? Ha igen, akkor hogyan? Mik az eszközös és szervezeti vonatkozásai?*

*– Mitől függ, hogy érdemes-e a biztonság felügyeletével foglalkozni?*

**Keleti Arthur,** az **Icon** IT-biztonsági üzletágának igazgatója: Szerintem az egyik legfontosabb kérdés, hogy megéri-e. Érdemes-e a felhasználónak foglalkoznia vele? Ha igen, akkor vásároljon-e hozzá eszközöket, és tartson-e saját szakembergárdát, vagy bízza szolgáltatókra? Ha a távfelügyelet biztonsági vonatkozásait is nézzük, klasszikus kérdés, hogy mennyire kockázatos kiadni valakinek mondjuk a naplóállományokat.

Manapság az audit is szempont, hiszen volt már olyan ügyfelünk, aki auditálni akarta a távfelügyelet minden vonatkozását.

**Kőrös Zsolt** ügyvezető igazgató, **Noreg** Kft.: Én azzal kezdeném, hogy menynyire éri meg; ez nyilván a szervezet méretétől és a felügyeleti rendszertől függ. Logikusan úgy látszik, hogy minél kisebb egy cég, annál nagyobb a távfelügyelet létjogosultsága, de a kisebb vállalatoknak erre kevesebb erőforrás áll rendelkezésükre. A költségek mellett fontos szempont még, hogy a szolgáltatóknál a több szervezet rendszereire központilag felügyelő szakemberek sokkal több információhoz jutnak, mint a szervezet egyedi hálózatára figyelő saját csoport. Egy adott támadás érzékelésekor a szolgáltató felkészülhet az incidensre más rendszereknél, és természetesen azok működtetőit is időben értesíteni tudja.

FOTÓ: IT-BUSINESS

**Keleti Arthur, Konkoly Thege Szabolcs, Kőrös Zsolt**

**Konkoly Thege Szabolcs,** a **Symantec** Magyarország területi igazgatója: Szerintem is alapkérdés, hogy mennyi, milyen minőségű és komplexitású biztonsági információ keletkezik, és a szervezet képes-e a megfelelő válaszlépésekre. Egyké biztonsági alrendszer használatánál szerintem nem érdemes foglalkozni a problémával. Főleg akkor nem, ha úgy oldják meg, hogy a félállású rendszergazda a vírusvédő alrendszer naplóit havonta átlapozza. Több biztonsági megoldástól származó információ feldolgozása már érdekesebb feladat, nemcsak a mennyiség és a bonyolultság, hanem az összefüggések feltárása miatt is. Hogy ekkor a felügyelet házon belül vagy kívül történjen-e, nehéz megmondani. A szolgáltatások drágábbak ugyan, de a felhasználó több értéket kap a pénzéért.

*– Létezik-e valamilyen motiváció vagy szabály?*

**Kőrös Zsolt:** Kérdés, hogy effektív védelmet is kínáló lehetőségről vagy csak egy elemző, a későbbi döntéseket támogató megoldásról beszélünk-e. Véleményem szerint a valós idejű védelem megvalósításán a kisebb cégeknek is érdemes elgondolkozniuk. Náluk nem az a fontos, ami történt, hanem az, hogy legyen megoldva. Nagyobb szervezeteknél már az is izgalmas lehet, hogy mi vezetett az incidenshez.

**Keleti Arthur:** Azt hiszem, abban megegyezhetünk, hogy lokális vagy távfelügyelet igénybevételét előíró ökölszabályt nem tudunk felállítani. Tapasztalatom szerint valamilyen szintű felügyeletre mindenkinek szüksége van. Ha másért nem, hát azért, mert ezt a PSZÁF előírja.

**Konkoly Thege Szabolcs:** A szabályozók mellett ez a biztonsági kultúrával is összefügg. A köztudatban valóban az él, hogy az igazi védekezésnél az eseményre van reakció; rögtön működik a védelem is. Szép dolog a törvényi előírás, de nem biztos, hogy meg kell várni azt a pillanatot, amikor külső hatásra kerülünk lépéskényszerbe. Érdemes elgondolkozni a szabályozók miértjén, és nem helyes megvárni a saját károkból származó tapasztalatokat.

**Kőrös Zsolt:** Egyetértek. Amikor valakihez betörnek, akkor rájön, hogy kell egy riasztó. Utána arra is, hogy be kell kötni a rendőrségre. A szervezetek általában a károk miatt szembesülnek a biztonsággal mint folyamattal. Baj esetén azonnal kell egy gyors, tűzoltó jellegű megoldás, de ennek jobb lenne elébe menni, mert rendszerint drágább és kevésbé hatékony, mint egy jól megtervezett és üzemeltetett védelmi rendszer.

**Keleti Arthur:** Valószínűleg mindenkinek érdemes elindulnia az IT-biztonság szervezett üzemeltetésének irányába. Ha egy szervezet megteszi a kezdő lépéseket, akkor azon is elgondolkozik, hogy milyen eszközökre van szüksége, sőt előbbutóbb felmerül a kérdés, hogy maga oldja-e meg a feladatot, vagy szolgáltatóhoz forduljon. Az első lépések a legfontosabbak. Véleményem szerint a felügyeleti szerveknek és a szabályozóknak is az a céljuk, hogy tudatosságra neveljenek. Ha a tudatosság megvan, akkor az üzemeltetés és felügyelet kérdése már szinte magától tisztázódik.

## IBM–ISS EGYESÜLÉS

Az év egyik legnagyobb horderejű IT-biztonsági híre szerint az IBM bejelentette, hogy 1,3 milliárd dolláros ajánlatot tett az ISS-re – éppen a menedzselt biztonsági szolgáltatások iránti élénk érdeklődése miatt. A tervezett akvizíció a Noreget is érinti, mint az ISS patinás hazai nagykövetét. Kőrös Zsolt szerint az ISS-eszközök terméktámogatásával és fejlesztésével valószínűleg nem lesz probléma, hiszen információi szerint a rendszer és a kiépített partnercsatornák nem változnak, de a jövő még számos nyitott kérdést tartogat.

INFORMATIKAI BIZTONSÁG NAPJA

# Palace MOM Park Mozi
# 2006. szeptember 26.

## EGYEDÜLÁLLÓ ALKALOM, HOGY IDÉN ISMÉT KONZULTÁLJON A SZAKMA ÖSSZES KÉPVISELŐJÉVEL!

**Kiemelt meghívott előadóink között:**

**Marcus J. Ranum,** a proxy tűzfal megalkotója, világhírű biztonságtechnikai szakértő
**John K. Davies,** a Brit Kormányzat szakértője
**Guy Lifshitz**, az EU ipari rendszereit vezérlő hálózatok biztonsági szakértője

Többek között **"Küzdelem az újszerű fenyegetettségek ellen", "Hálózat és az infrastruktúra biztonsága"** témákról szakmai előadásokat hallgathat meg a támogatók szakértőitől.

**Részvételi szándékát kérjük, jelezze minél előbb weboldalunkon, ahol bővebb összefoglalót is talál a konferenciáról és az előadásokról! A támogatók jóvoltából a részvétel idén is *ingyenes*!**

## www.itbn.hu

**Várjuk érdeklődését az info@itbn.hu e-mail címen, valamint a /30/ 474-8975 info-vonalon!**

Az előadások látogatásával CPE pontok gyűjthetőek (ISACA, (ISC)$^2$).

ICON · Microsoft · McAfee · UK Trade & Investment · Brit Nagykövetség · EMC² where information lives · hp invent · RSA Security · Check Point Software Technologies Ltd. We Secure the Internet. · Cisco Systems · symantec. · NOREG · BULL Architect of an Open World · APC Legendary Reliability · VirusBuster · Trend Micro · CITRIX · CROSSBEAM Systems · BalaBit IT Security · Aladdin Securing the Global Village · CARISMA · utimaco safeware

Védnök: Műegyetem 1782 · BME IIT

Médiatámogatók: IT-Business · Magyar Hírlap · Computerworld · index · PROHARDVER!

## ESEMÉNYNAPTÁR

| Időpont | Megnevezés | Helyszín | Web | Részvételi díj | Leírás |
|---|---|---|---|---|---|
| Szeptember 27. | Az Informatikai Biztonság Napja | Palace MOM Park Mozi | *www.itbn.hu* | Ingyenes, előzetes regisztrációhoz kötött | A konferencián az informatikai biztonság legújabb kihívásairól és megoldásairól lesz szó, továbbá tájékoztatnak a legfrissebb technológiákról és veszélyekről. |
| Október 10–12. | Information Security Solutions Europe 2006 | Róma | *www.eema.org/static/isse/* | | Néhány kulcsfontosságú terület, amelyet a konferencián érintenek: azonosításkezelés, e-azonosítás, PKI, biometrikus azonosítás, megbízható számítástechnika, biztonsági szabványok, e-kormányzati és e-egészségügyi megoldások. |
| Október 10–13. | Security 2006 | Essen | *www.security-messe.de/index.php?content=00000000&lang=en* | 52 euró, napijegy 22 euró | Idén 17. alkalommal rendezik meg az esseni nemzetközi biztonsági kiállítást, amelyen negyven országból közel ezer kiállító vesz részt. |
| Október 19—21. | 1. Biztonság & Technika nemzetközi biztonságtechnikai szakvásár | Syma Rendezvényközpont | *www.securifocus.com/portal.php?pagename=esemenynaptar* | n. a. | A szakvásár az e+e 2006 nemzetközi ipari elektronikai és elektrotechnikai szakvásár társkiállításaként fogadja a látogatókat. |
| Október 25–26. | Alarm | Kielce Trade Fair Center, Lengyelország | *www.targikielce.pl/targi/index.php?language=_en&module=targi&targ_id=251* | n. a. | A hetedik alkalommal megrendezendő Video Surveillance Conference and Exhibition rendezvényen bemutatják a legújabb védelmi eszközöket és megoldásokat. |
| Október 25–28. | Security & Safety | Syma Rendezvényközpont | *www.securityinfo.hu/index.php?idx=18* | Ingyenes | Egyidejűleg három rendezvényt tartanak: a 17. Nemzetközi Biztonságtechnikai, Tűz- és Vagyonvédelmi, Bank- és Adatbiztonsági Kiállítást és Vásárt, a Pro-Filasec 4. Nemzetközi Tűz- és Munkabiztonsági Kiállítást és Vásárt, valamint a Guns' Expo 2. Nemzetközi Fegyver- és Lőszerkiállítást. |

**Szerkesztőségi ajánlat:** Az Informatikai Biztonság Napján a plenáris ülésen kívül 4 szekcióban lesznek előadások, a témák: Azonosítás és jogosultságkezelés; Küzdelem az újszerű fenyegetettségek ellen; Előírások és szabványok, kockázatok kezelése; Hálózat és az infrastruktúra biztonsága; Adatok integritásának, védelmének módszerei; Integrációs tapasztalatok az IT-biztonságban, ízelítő a legjobb gyakorlatokból.

## OKTATÁS, TANFOLYAMOK

| Tanfolyam címe | Leírás | Időpont | Időtartam | Részvételi díj | Webcím | Helyszín |
|---|---|---|---|---|---|---|
| Designing Security for Microsoft Networks | A tanfolyam bevezet az alapvető titkokba a hackelés, a titkosítás (kriptográfia), valamint a webes alkalmazások használatának és „rosszul" használatának témakörébe. Lehetőség nyílik a különböző algoritmusok alapos megismerésére, valamint átgondolt biztonsági stratégia kidolgozására és megvalósítására. Ismertetik a tipikus támadásokat – buffer overrun, sniffelés, backdoor, féreg és vírus, session hijacking, man-in-the-middle, social engineering stb. –, amelyek mögött valós fenyegetés bújik meg. Hogyan védekezzünk? Erről szól ez a tanfolyam. | Október 2. | 5 nap | 195 000 forint + áfa | *http://www.netacademia.net/course.aspx?id=2810/2830* | Budapest, Andrássy út 62. |
| A hálózati határvédelem elmélete és gyakorlata | A résztvevők a tanfolyam alatt megismerkedhetnek a mai határvédelmi technológiákkal mind elméleti síkon, mind pedig gyakorlati példákon keresztül. Bemutatják ezek működési elveit, előnyeit és hátrányait. A tanfolyam célja a tűzfalakkal megvalósítható határvédelmi funkciók áttekintése, a konfigurálás során előforduló tipikus hibák ismertetése, valamint a napi üzemeltetési feladatok ismertetése. | Október 4. | 3 nap | 59 000 forint + áfa | *www.dashofer.hu/?fejezet=15#kepzesnaptar* | A helyszínt a visszaigazolásban adják meg |
| Spam | Bemutatják a plágium legmodernebb változatát, karakterisztikáját és természetét, szó lesz arról, aki terjeszti a mételyt, és azokról, akik védekeznek ellene. Megvizsgálják, hogy a fertőzés hogyan kezdődik és jut el az áldozathoz; ismertetik azokat a technikai lépéseket, amelyekkel detektálni lehet a káros tevékenységet és csökkenteni hatásukat. S végül kitérnek a nemzetközi helyzetre és a jogi háttérre is. | Október 25. | 1 nap | 50 000 forint + áfa | *www.wsh.hu* | Budapest, Árbóc u. 6. |

# Az ITIL és a biztonság

***Az IT Service Management területén az utóbbi évek egyértelműen az ITIL elterjedését, de facto szabvánnyá válását, majd tényleges szabványként való megjelenését (BS 15000, ISO/IEC 20000) hozták.***

Az ITIL (IT Infrastructure Library) sikerének kulcsa, hogy elsősorban az üzleti szféra által közvetlenül „fogyasztható" folyamatokra koncentrál: a fókuszban természetesen az incidensek és a szolgáltatáskérések kezelése, a változás- és konfigurációkezelés áll, bizonyos háttérfolyamatok azonban az implementálás folyamán általában később vagy egyáltalán nem jelennek meg – említette *Hidvégi Zoltán*, a HP vezető tanácsadója.

Ugyanakkor a Sarbanes–Oxley-nak (SOX), a Basel II-nek és a sorra megjelenő nemzetközi és nemzeti iparági előírásoknak az IT-területre vetített értelmezése megmutatta, hogy a legmagasabb szintű kockázatok általában az informatikai biztonság területén jelennek meg. Ezért nem meglepő, hogy mostanában az ITIL, illetve az ITIL alapú BS 15000, ISO/IEC 20000 szabványok is kiemelten kezelik a hagyományosan elhanyagolt biztonságmenedzsment (Security Management) folyamatát.

Tegyük hozzá rögtön, hogy a menedzsment kifejezés már az ITIL eredeti meghatározása szerint is egyértelműen a vállalati biztonsági keretek kialakítására utal, és nem a technológiai rendszerek, megoldások kezelésére.

## Mit fed le az ITIL?

Felmerülhet azonban a kérdés – és fel is merül az informatikai biztonsággal foglalkozó szakemberekben és a vállalatok vezető IT-pozícióban levő döntéshozóiban –, hogy mennyiben elégítheti ki az ITIL alapú megközelítés egy adott vállalat teljes biztonsági követelményrendszerét. Másképpen fogalmazva: az ITIL-t követve le tudjuk-e fedni az informatikai biztonságot teljes terjedelmében, illetve teljes mélységében?

Nyilvánvaló, hogy célkitűzéseiben az ITIL biztosan „jó irány" az informatikai biztonság szempontjából. Akár az ITIL/BS 15000/ISO 20000 területét, akár az informatikai biztonság BS 7799/ISO 17799 /ISO 2700X szabványait tekintjük – de nyugodtan ide sorolhatjuk az IT-irányítás fő módszertanaként a CobiT-ot (Control Objectives for Information and related Technology) is –, lényegében mindegyik ugyanazt a fő célkitűzést hangsúlyozza: legyenek kontrolláltak az érintett folyamatok az üzlet által, legyenek dokumentáltak, mérhetőek, folyamatosan és rendszeresen ellenőrzöttek.

**AZ IT SERVICE MANAGEMENT FOLYAMATAI AZ ISO/IEC 20000 SZABVÁNY SZERINT**


*(Forrás: IT Service Management Forum)*

Az ITIL/BS 15000/ISO 20000 biztonságmenedzsment folyamatát közelebbről megvizsgálva azonban már nyilvánvaló, hogy az adott folyamat csak magas szinten fogalmaz meg követelményeket a vállalati biztonságmenedzsment keretrendszerére vonatkozóan – tette hozzá Hidvégi Zoltán –, és nem határozza meg sem a biztonsági rendszer részterületeit, sem pedig az egyes területek folyamatait és eljárásait.

Nagy előrelépés viszont a legújabban kiadott ISO 20000 szabványban az eredeti ITIL-biztonságmenedzsmenthez képest, hogy abban már explicit ajánlásként említik az ISO 17799-et (ma már ISO 2700X) mint az implementálás preferált keretrendszerét.

Fontos megjegyezni azt is, hogy az ITIL folyamatai több ponton is kapcsolódnak a kialakított vállalati biztonságmenedzsment eljárásaihoz, ezért a továbbiakban – a teljesség igénye nélkül – olyan példákat mutatunk be, amelyek az ITSM (ITIL)-folyamatok és az informatikai biztonság szerves kapcsolatát jelzik.

A legkézenfekvőbbnek talán az incidenskezelés biztonsággal való kapcsolata tűnik – mondja a HP vezető tanácsadója –, hiszen a köznapi értelemben is incidensnek tekintett hibabejelentéseknek szinte mindig van biztonsági vonzatuk: az érintett rendszerek adatainak rendelkezésre állása, sértetlensége vagy akár a bizalmassága is veszélyben kerülhet egy komolyabb hiba esetén.

Lényeges megemlíteni, hogy az utóbbi időben az informatikai biztonság önálló részterületeként, saját módszertani megközelítéssel jelent meg a biztonsági incidenskezelés (Security Incident Management – SIM). Ezért igen fontos, hogy az ITIL/ITSM-incidenskezelés (és -szolgáltatáskérés) folyamatában a lehető leghamarabb azonosítsák a biztonsági incidenseket, és azokat közvetlenül a specifikus (és általában igen gyors, hatékony) SIM-folyamatok kezeljék.

## Változáskezelés

Minden változás potenciális kockázatot jelent – az ITIL/ITSM-folyamatokra ez fokozottan igaz. Ezért biztonsági szempontból talán a változáskezelés folyamata tekinthető a legkritikusabbnak. Nagyon fontos tehát, hogy a döntési folyamatban a biztonsági kockázatok mérlegelése mind a szokványos, mind az egyedi változások meghatározásakor megtörténjen.

Itt ismételten hangsúlyozni kell, hogy a változáskezelési folyamat maga a keretet (a kockázatok mérlegelésének lépését) adja meg, de nem ad módszertani alapot a biztonsági kockázatok meghatározásához – ehhez az informatikai biztonság egy specifikus területének, a kockázatelemzésnek a módszertanához kell fordulnunk.

**Matula Zsolt**

IT Service Management Forum, nemzetközi szakmai szervezet – *www.itsmf.com*
Az ISO 2700X szabványról – *www.27000.org/* és *www.iso27001security.com/*
Oktatás, tréninganyagok – *www.itilsurvival.com/* és *www.itiltraining.com/*

# Hálózatban az alvállalkozók

*A technológiai fejlődés nem csupán a magánszférát alakítja át, de az egész gazdasági struktúránkat is.*

Mit is nyújt a gyors és olcsó kommunikáció? Első ránézésre kényelmet. Másodikra már észrevesszük, hogy a közhiedelemmel ellentétben közelebb hozza egymáshoz az embereket. Ma e-mailen, mobiltelefonon és a közösségépítő site-okon keresztül több száz emberrel, régi barátokkal, volt kollégákkal, távoli rokonokkal tarthatunk fenn napi kapcsolatot. Emlékszik még valaki arra, hogyan beszéltünk meg húsz éve egy közös mozit az unokatestvérünkkel, aki véletlenül a városban járt? Sehogy. A vezetékes telefon sem volt kellően elterjedt ehhez a szociális távkapcsolathoz.

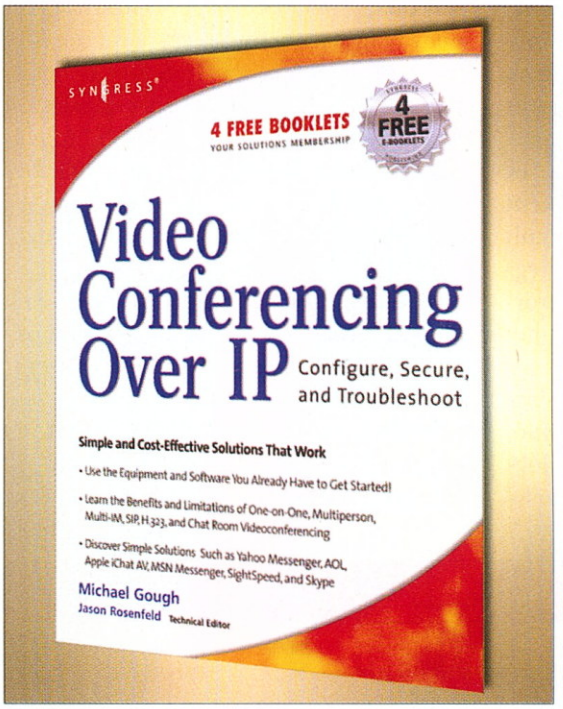
## Átalakul a gazdasági struktúra

Harmadik ránézés szükséges ahhoz, hogy rádöbbenjünk: a technológiai fejlődés nem csupán a magánszférát alakítja át, de az egész gazdasági struktúránkat is. Európának ebben a felében nehezebb ezt észrevenni, hiszen egyébként is egy nagy változás közepén járunk. Viszont érdemes felismerni, hogy az a nyugati kapitalista gazdaság, amihez felzárkózni próbálunk, szintén a változás és az útkeresés fázisában van.

Nehezen ismerjük fel a körülöttünk zajló eseményeket, mert közelről nézve nem látjuk az összefüggéseket. Pedig már több évtizede téma a globalizáció, amelynek elindulásához és kiteljesedéséhez „elég" volt a közlekedés, a telefon, a fax és a műholdas televízió.

Az internet, pontosabban az internet infrastruktúráját használó szolgáltatások ennél mélyebb és gyökeresebb változásokat hoznak majd a gazdaságba. Nem a piac méretét alakítják át, hanem magát a piacot. Az IP alapú telekommunikációs szolgáltatások ugyanis drasztikusan csökkentik a vállalatközi és a vállalaton belüli koordinációs költségeket. Míg a globalizáció lehetővé tette, hogy a cégméretek óriásira nőjenek, az internet lehetővé teszi, hogy a cégek kompetenciáik mentén felbomoljanak.

A jövő gazdaságában egy divatos sportszermárka egyetlen irodából fog állni. A terméktervezést, a marketinget, az értékesítést és a gyártást alvállalkozók összetett és többszintű hálózata végzi majd. Ez a hálózat pedig legalább olyan hatékonyan dolgozik majd együtt, mint egy múlt század végi mamutvállalat.




A világon három helyen gyártanak TFT-paneleket, talán féltucat gyárban cd-ket, és a világon eladott notebookok nyolcvan százalékát egy maroknyi délkelet-ázsiai üzem állítja elő.

A marketingtevékenységgel a cégek évek óta nem foglalkoznak; ezt már ma is specialisták végzik. Hamarosan már a termékeket is erre szakosodott kisméretű vállalatok, irodák tervezik majd. A jelenség elsőként az autógyártásban figyelhető meg, ahol a gyártásnak is már csak az utolsó, összeszerelő fázisa van a márkatulajdonos kezében. Az alkatrészeket és fő elemeket beszállítók készítik.

A jövőben tehát a vállalatok kiürülnek, és háromféle, kisméretű alaptípussá alakulnak át: a márkaneveket és szabadalmakat birtokló cégekre, a szakértelemmel rendelkező specialistákra és a tőkével rendelkező befektetőre.

## Megtanítani az eszközhasználatra

Hogy mindezt miért volt fontos megtudni, mielőtt rátérünk Michael Gough könyvének – Video Conferencing over IP: Configure, Secure, and Troubleshoot – a bemutatására? Ez a látszólag érdektelen kézikönyv nem céloz meg mást, mint megtanítani a vállalatokat arra, miként használják a túlnyomórészt már meglévő eszközeiket videotelefonálásra és videokonferenciára.

Ezzel a könyv tulajdonképpen azt tanítja meg a vállalatoknak, hogyan dolgozzanak együtt hatékonyan és rugalmasan alvállalkozóikkal, hogyan koordinálják kiterjedt irodahálózatukat, és azt, hogy miként irányítsák otthonról dolgozó alkalmazottaikat.

A szerző – a biztonsági szakemberekkel együtt – látja, hogy ez azért nem lesz ilyen egyszerű. Az IP alapú telefónia hemzseg az aluldefiniált szabványoktól és a kritikus biztonsági hibáktól. A cégeknek segítségre lesz szükségük a megfelelő technológia és eszköz kiválasztásában, valamint üzemeltetésében. A kötet ebben is úttörő szerepet játszik, hiszen a piacon elérhető talán legteljesebb biztonságtechnikai útmutatást nyújtja.

Míg a múltban a videokonferenciák luxusából csupán a legnagyobb vállalatok profitálhattak, manapság már minden eszköz a rendelkezésükre áll, csupán megfelelően kell őket használni. Semmi nem áll az útjukban, csak az információ hiánya. Michael Gough ezt a problémát is a könyv szellemében oldotta meg, hiszen műve mindenki számára könnyen és gyorsan elérhető e-book formában kapható.

**Sós Éva**

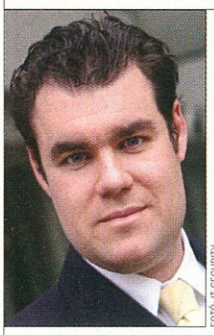
**KÖNYV-JELZŐ**

**Cím:** Video Conferencing over IP: Configure, Secure, and Troubleshoot
**Szerző:** Michael Gough
**Ár:** 49,95 dollár

IT-SECURITY

# Mit olvas a szakértő?

*Izgalmas információk a blogokban.*



FOTÓ: IT-SECURITY

**Szabó Gábor**

Lassan mindenkinek meg kell szoknia, hogy a Microsoft az információbiztonsággal kapcsolatos hírekben nemcsak termékeiben támadott cégként szerepel, hanem gyártóként, sőt igen aktív gyártóként is. A vállalat az elmúlt hónapokban számos új biztonsági megoldással lépett a piacra: ezek magyarországi bevezetése *Szabó Gábor* termékmenedzser egyik legfontosabb feladata.

Másik nagyon fontos feladata az IT-biztonság „evangelizációja": az érdeklődő, de nem eléggé tájékozott felhasználóknak igyekszik bemutatni az egyes veszélyforrások anatómiáját és a védekezési technológiák működését. Nem kell mindenkinek információbiztonsági szakemberré lennie, de az alapvető ismereteket minden felhasználónak el kellene sajátítania – vallja Szabó Gábor.

Ehhez a munkához elengedhetetlen a folyamatos tájékozottság. Híranyagban nem is lenne hiány, mert naponta sok száz cikk születik, amely akkor is hatalmas mennyiség, ha sok köztük az átfedés. Ezek áttekintésében segít az RSS hírolvasó (amit az új Internet Explorer már beépítve tartalmaz) – ez minden egyes figyelt hírforrás mellett megmutatja, hogy hány új hír került fel az oldalra.

A biztonsági értesítők és hírlevelek mellett rendszeres olvasója egyes blogoknak is, amelyek talán szubjektívebb szempontból, de a többi hírforrásnál nem csekélyebb szakmaisággal tájékoztatnak az információbiztonsági világ aktuális híreiről, eseményeiről. Szabó Gábor érdeklődési területéhez hozzátartozik még a mind népszerűbb VoIP és annak biztonsági aspektusai is.

**Schopp Attila**

## A LEGJOBB FORRÁSOK

| Hírforrás | URL | Jellemzők |
|---|---|---|
| **Biztonsági értesítők** | | |
| Microsoft Security Bulletin | http://www.microsoft.com/technet/security/current.aspx | A legfrissebb biztonsági értesítők (Microsoft) |
| Secunia | http://secunia.com/ | Új sérülékenységek és vírusok |
| CERT | http://www.cert.org/ | Új sérülékenységek és vírusok |
| SANS @RISK hírlevél | http://www.sans.org/newsletters/risk/ | Heti rendszerességgel megjelenő hírlevél |
| Anti-Phishing Working Group | http://www.antiphishing.org/ | Adathalászattal kapcsolatos információk |
| **VoIP-biztonság** | | |
| Voice over IP Security Alliance (VOIPSA) | http://voipsa.org/ | A VoIP-biztonsági szövetség oldala |
| **Blogok** | | |
| Bruce Schneier Blog | http://www.schneier.com/blog/ | Érdekes, nem csak IT-biztonsággal kapcsolatos írások |
| Microsoft Security Response Center Blog | http://blogs.technet.com/msrc/default.aspx | Háttérinformációk a biztonsági frissítésekhez |




**AZ INFORMATIKAI BIZTONSÁG LAPJA**

**SZERKESZTŐSÉG**
**Főszerkesztő**
Sziebig Andrea – *asziebig@vogelburda.hu*
**Felelős szerkesztő**
Kelemen László – *kelemen@hungary.com*
**Vezető szerkesztő**
Varga János – *jvarga@vogelburda.hu*
**Szerkesztőbizottság**
Bártfai Attila – *attila.bartfai@hp.com*
Konkoly Thege Szabolcs – *szabolcs_konkolythege@symantec.com*
Papp István – *pappi@albacomp.hu*
Papp Péter – *papp.peter@kancellar.hu*
Szabó Gábor– *gabors@microsoft.com*

**Munkatársak**
Bende Magdolna – *mbende@vogelburda.hu*
Kelenhegyi Péter – *pkelenhegyi@vogelburda.hu*
Mallász Judit – *jmallasz@vogelburda.hu*
Mészáros Csaba – *csmeszaros@vogelburda.hu*
Schopp Attila – *aschopp@vogelburda.hu*
Sós Éva – *pingvin@terminal.hu*

**Tervezőszerkesztők**
Bujdosó Anikó – *abujdoso@vogelburda.hu*
Papp Gyula – *gypapp@vogelburda.hu*

**Korrektor**
Viosz Károly – *kviosz@vogelburda.hu*

**Fotó**
Jekler Gábor – *gjekler@vogelburda.hu*

**Lapterv**
Kocsis Gábor – *emotion@axelero.hu*

**Grafika**
Szántói Krisztián – *estharang@index.hu*

**Online hírlevél**
Kelemen László – *kelemen@hungary.com*

**Szerkesztőség és kiadó címe:**
Vogel Burda Communications Kft.
1088 Budapest, Kéthly Anna tér 1.
Tel.: 888-3400, fax: 888-3499

**KIADÓ**
**Kiadja a Vogel Burda Communications Kft.**

**A kiadásért felel**
Carsten Gerlach ügyvezető igazgató
*cgerlach@vogelburda.hu*
Tel.: 888-3470, fax: 888-3499

**Lapigazgató:**
**Walitschek Csilla**
*cswalitschek@vogelburda.hu*
Tel.: 888-3450

**Médiareferensek:**
Harsányi Erika – *eharsanyi@vogelburda.hu*, tel.: 888-3452
Németh Krisztina – *knemeth@vogelburda.hu*, tel.: 888-3468
Rátóti Sarolta – *sratoti@vogelburda.hu*, tel.: 888-3453
Szendrey Szilvia – *szendrey@vogelburda.hu*, tel.: 888-3455
Fax: 888-3459

**Online-referens:**
Pái Attila – *apai@vogelburda.hu*, tel.: 888-3491

**Marketing:**
Gajdos Barna – *bgajdos@vogelburda.hu*, tel.: 888-3494

**Hirdetési koordinátor:** Szőke Erika
*eszoke@vogelburda.hu*
Tel.: 888-3411, fax: 888-3459





**Nemzetközi hirdetésfelvétel:**
Eric N. Wicha – *ewicha@vogelburda.com*
Vogel Burda Holding
Poccistrasse 11, D–80336 München
Tel.: +49 89 74642-326, fax: +49 89 74642-325
A hirdetések körültekintő gondozását kötelességünknek érezzük, de tartalmukért felelősséget nem vállalunk.

**TERJESZTÉS**
**Terjesztett példányszám:** 8000–10 000
**Terjesztési osztály:** 1426 Budapest, Pf. 300/39

**Ügyfélszolgálat és bolt:** Budapest VI., Teréz körút 47. (Nyugati pu.-nál) Hétfő–péntek: 9–20 óráig, szombat-vasárnap: 9–15 óráig

**Nyomda:** Origo Print Kft.
2040 Budaörs, Gyár u. 2.
Felelős vezető: Bánáti László ügyvezető igazgató

# IT-BUSINESS MEDICAL

EGÉSZSÉGÜGYI INFOKOMMUNIKÁCIÓ ÜZLETI ÉS EGÉSZSÉGÜGYI DÖNTÉSHOZÓKNAK

- egészségügyi szférában érdekelt informatikai döntéshozóknak és technológia szakembereknek
- az elmúlt 168 óra legfontosabb, az egészségügyi informatikát érintő hírek és események
- heti ingyenes elektronikus hírlevél

**Regisztráljon!**

www.it-business.hu/hirlevel

# ENNYIRE VESZÉLYES TEREP

## SYNERGON INFORMATIKAI BIZTONSÁGI MEGOLDÁSOK

VÍRUSOK, KÉRETLEN LEVELEK, HACKER-TÁMADÁSOK, ADATLOPÁSOK ÉS ILLETÉKTELEN INFORMÁCIÓSZERZÉSEK? A VÁLLALATOK INFORMATIKAI RENDSZEREI ELLEN ELKÖVETETT BŰNCSELEKMÉNYEK MÖGÖTT TÖBBNYIRE A HASZONSZERZÉS ÁLL.
A KÜLSŐ TÁMADÁSOKAT TALÁN MÁR KIVÉDTE, DE MI A HELYZET A VÁLLALATON BELÜLRŐL JÖVŐKKEL?

TUDJA BIZTONSÁGBAN BIZALMAS ADATAIT, ÉS TESZTELJE VÁLLALATA SÉRÜLÉKENYSÉGÉT!

SÉRÜLÉKENYSÉGI TESZT A
WWW.SYNERGON.HU/GO/SECURITY
OLDALUNKON!

SYNERGON