A FELHŐ BIZTONSÁGA

A felhőszolgáltatók állítják: az adatközpontjaik sokkal biztonságosabbak, mint egy vállalaton belüli szerver. Igaz ez?

» 14. oldal

AVATÁRVADÁSZAT

A kiberbűnözők olykor virtuális személyiség álarca mögé rejtőznek. Vajon meg lehet-e találni őket?

» 20. oldal

495 forint

SZÁMÍTÁSTECHNIKA
ICT-STRATÉGIA DÖNTÉSHOZÓKNAK • WWW.COMPUTERWORLD.HU
ALAPÍTVA 1969 • 2011. SZEPTEMBER 27. • XLII. ÉVFOLYAM 39. SZÁM
IDG Communications HUNGARY

COMPUTERWORLD

A biztonság rögös útjai

Az informatikai biztonság az elmúlt években minden korábbinál gyorsabban fejlődött, aminek eredményeként komplex IT-területté nőtte ki magát. Kezelése komoly erőforrásokat, szakértelmet és figyelmet követel.

Összeállításunk a 11–13. oldalon

9 770587 151006 11039

HUNGARIAN SOFTWARE TESTING FORUM

H.T.B. Hungarian Testing Board

SZÁMÍTÁSTECHNIKA COMPUTERWORLD

IDŐPONT: 2011. október 13–14.
HELYSZÍN: Budapest, Danubius Hotel Helia (1133 Budapest, Kárpát utca 62–64.)
A konferencia angol nyelvű, de megfelelő számú igény esetén tolmácsot biztosítunk.

KIKNEK SZÓL?

Szoftvertesztelőknek ➘ Tesztmenedzsereknek ➘ Tesztkoordinátoroknak ➘ Tesztelési vezetőknek ➘ Szoftvertervezőknek ➘ Szoftverfejlesztőknek ➘ Rendszertesztelőknek ➘ Tesztmérnököknek ➘ IT-igazgatóknak, -vezetőknek ➘ IT-projektvezetőknek ➘ IT-fejlesztési vezetőknek, menedzsereknek ➘ Informatikai szakembereknek

A TERVEZETT PROGRAM

2011. OKTÓBER 13. CSÜTÖRTÖK

- **Lloyd Roden:** A szoftvertesztelés jelentősége és kihívásai (keynote)
- **Esettanulmányok**
- **Rex Black:** A menedzselt szoftvertesztelés vállalati bevezetésének előnyei és szükségessége
- Moderált kerekasztal-beszélgetés

Este kötetlen beszélgetési lehetőség az előadókkal

2011. OKTÓBER 14. PÉNTEK

Párhuzamos workshopok

- **Lloyd Roden:** Becsléstechnikák a szoftvertesztelésben: hogyan is végezzük sikeresen? A sikeres tesztmenedzser eszköztára – amire feltétlenül szükség van, amit mindenképpen ismerni kell
- **Rex Black:** Rizikóalapú tesztelés eredményes alkalmazása a gyakorlatban

A részletes program a http://computerworld.hu/konferencia/55 weboldalon található.

PARTNEREINK

GOLD PARTNER

ERICSSON

mortoff

SILVER PARTNER

4DSoft

ALVICOM TESTCENTER

KIÁLLÍTÓ PARTNER

NewNet szoftverfejlesztés

Masterfield TRAINING

FRONTENDART

IT Services

Lufthansa Systems
IT that makes your life easier

Jelentkezni a konferencia@idg.hu e-mail címen lehet.
További információk:

Biró Ilona
Telefon: +36-1/577-4374
Fax: +36-1/266-4274
E-mail: ilbiro@idg.hu

Héjjas Ágnes
Telefon: +36-1/577-4314
Fax: +36-1/266-4274
E-mail: ahejjas@idg.hu

AKTUÁLIS

05 HYDE TECH CORNER

06 TÁMAD A LÁTHATATLAN ELLENSÉG
A Hacktivity konferencián *Szőr Péterrel*, a McAfee kutatójával beszélgettünk.

07 KIBERTÁMADÁSOK IS SÚJTJÁK JAPÁNT

08 GOOGLE-ERŐ: VESZÉLY VAGY LEHETŐSÉG?

09 ÁRULJÁK A TABLETEKET
A leleményes szakemberek közül többen úgy döntöttek, pénzt csinálnak *Steve Ballmerék* ajándékából, és az eBay-en árulni kezdték a különféle extrákkal felpöccentett mobileszközöket. A gépeket azért kapták a fejlesztők, hogy alkalmazásokat készítsenek a Windows 8 érintésérzékeny Metro platformjára.

09 AZ APPLE ELÉGEDETTÉ TESZ

10 FENYEGETI A GMAIL A MICROSOFTOT?
A Gartner piackutató szerint a Google e-mail szolgáltatása hamarosan komolyan meg fogja csapolni a redmondiak vállalati szférából származó bevételeit.

10 TESCO MOBILE JANUÁRTÓL

FÓKUSZ

11 A BIZTONSÁG RÖGÖS ÚTJAI
A védelem komplexitása olyan szintet ért el, amelynek kezelése izzasztó munkát követel. Sajnos jelenleg a kedvezőtlen tendenciák megfordulására egyelőre nincs remény, sőt!

ÜZLET

14 BIZTONSÁG A FELHŐBEN

16 PIACI ÁTLAGON FELÜL TELJESÍT A BI

17 NAGYOK NAGY BUKÁSAI
Csupa olyan eset, amiből a kisebbek is okulhatnak, de a legnagyobbak – a Google és a Microsoft – követték el őket.

TECHNOLÓGIA

18 BEHÁLÓZOTT KAMERÁK
A korszerű megfigyelőrendszerek kamerái ugyanúgy kapcsolódnak a hálózatra, mint a számítógépek.

20 AVATÁRVADÁSZAT

22 SZOFTVERVÉDELEM - MÁR AZ ALAPOKTÓL
Hogyan lehetnek még ellenállóbbak a jövő alkalmazásai? Ha figyelmet fordítanak a biztonságra.

ÁLLANDÓ ROVATAINK

04 VÉLEMÉNY
Fóti Marcell: Rendszerhiba az IT-biztonságban
A hekkerek 2011-ben elloptak mindent, ami nem volt lebetonozva. Vitték az RSA SecurID-tokenek kritikus kódját, a SONY ügyféladatbázisát, a PHP forráskódját, a McAfee reputációját, az Xbox market kuponalgoritmusát és még sorolhatnánk. Pedig már kezdtük azt hinni, a biztonsági réseket lassan befoltozzák mindenhol – de nem. A kérdés az, hogy miért nem, és meddig nem?

05 HÍRMOZAIK

07 ESEMÉNYEK
Mi várható a héten? Konferenciák, előadások, tapasztalatcserék

IMPRESSZUM COMPUTERWORLD-Számítástechnika
ICT-stratégia döntéshozóknak - alapítva 1969 - 2011. szeptember 27. - XLII. évfolyam 39. szám

Kiadja	IDG Hungary Kft. 1075 Budapest Madách I. út 13–14. A ép.
HU ISSN 0237-7837	Postacím: 1374 Budapest 5, Pf. 578 Internet: www.idg.hu
Bankszámlaszám	10300002-20328016-70073285
Felelős kiadó	Bíró István ügyvezető – ibiro@idg.hu
Műszaki vezető	Babinecz Mónika – mbabinecz@idg.hu
Nyomás és kötészet	D-Plus Kft. 1037 Budapest, Csillaghegyi út 19–21.
Ügyvezető igazgató	Németh László

SZERKESZTŐSÉG

Főszerkesztő	Dervenkár István – idervenkar@idg.hu
Vezető szerkesztő	Odrovics Szonja – szodrovics@idg.hu Szalay Dániel – dszalay@idg.hu
Olvasószerkesztő, korrektor	Sz. Erdős Judit – jerdos@idg.hu
Munkatársak	Dávid Imre – idavid@idg.hu Egri Imre – iegri@idg.hu Kis Endre – ekis@idg.hu Mallász Judit – jmallasz@idg.hu Szilágyi Szabolcs – szszilagyi@idg.hu Tóth Lívia – ltoth@idg.hu Vass Enikő – evass@idg.hu
Szerkesztőségi ügyelet	Cseresznye Anita – acseresznye@idg.hu Telefon: 577-4302, fax: 266-4343 Internet: www.computerworld.hu

Újságíróink szakmai képzésének hátterét a NetAcademia Oktatóközpont biztosítja. www.netacademia.net

TIPOGRÁFIA

Berényi István – iberenyi@idg.hu

HIRDETÉSFELVÉTEL

Hirdetési igazgató	Melovics Csaba – csmelovics@idg.hu Telefon: 577-4310, fax: 266-4274
Lapreferens	Rodriguez Nelsonné – irodriguez@idg.hu Telefon: 577-4311
Kereskedelmi asszisztens	Bohn Andrea – abohn@idg.hu Telefon: 577-4316, fax: 266-4274 e-mail: keriroda@idg.hu

TERJESZTÉS ÉS ÜGYFÉLSZOLGÁLAT

Terjesztési igazgató	Babinecz Mónika – mbabinecz@idg.hu Telefon: 577-4301, fax: 266-4343 MediaShop: mediashop.idg.hu e-mail cím: terjesztes@idg.hu

MARKETING

PR-munkatárs	Kovács Judit – jkovacs@idg.hu

JOGI KÖZLEMÉNYEK

Szerkesztőségünk a kéziratokat lehetőségei szerint gondozza, de nem vállalja azok visszaküldését, megőrzését.

A COMPUTERWORLD-ben megjelenő valamennyi cikket (eredetiben vagy fordításban), minden megjelent képet, táblázatot stb. szerzői jog védi. Bármilyen másodlagos terjesztésük, nyilvános vagy üzleti felhasználásuk kizárólag a kiadó előzetes engedélyével történhet. A hirdetéseket a kiadó a legnagyobb körültekintéssel kezeli, ám azok tartalmáért felelősséget nem vállal.

TERJESZTÉSI, ELŐFIZETÉSI, ÜGYFÉLSZOLGÁLATI INFORMÁCIÓK

A lapot a Lapker Rt., alternatív terjesztők és egyes számítástechnikai szaküzletek terjesztik. Előfizethető a kiadó terjesztési osztályán, az InterTicketnél (266-0000 9-20 óra között), a postai kézbesítőknél (06/80-444-4444; hirlapelofizetes@posta.hu, fax: 303-3440) Előfizetési díj egy évre 16 440 forint, fél évre 8220 forint, negyed évre 4110 forint.

Lapunkat a MATESZ auditálja

Olvasóink szokásait a Nemzeti Médiaanalízis méri fel.

A Computerworld az IVSZ hivatalos médiapartnere.

print-audit GfK Ipsos

A szerkesztőségi anyagok vírusellenőrzését a **NOD32 Antivirus** programmal végezzük, amelyet a szoftver magyarországi forgalmazója, a **Sicontact Kft.** biztosítja számunkra. eset

HP-vezércsere?
Meg nem erősített hírek szerint a HP lecserélné kevesebb mint egy éve kinevezett vezetőjét, *Leo Apothekert*.
» computerworld.hu/cikk/hpleo

100 éves az IBM
A nagyvállalat szakmai fórummal ünnepel New Yorkban. A 75 éves magyar leány is a jövő jegyében idézte fel az innováció évszázadát.
» computerworld.hu/cikk/100ibm

Mobil oprendszer lesz a Facebook?
Sikerének bebetonozása érdekében öt éven belül mobil operációs rendszerré kell válnia a Facebooknak – az ABI Research szerint.
» computerworld.hu/cikk/mopfb

Ingyenes Facebook-biztonság
Az F-Secure kiadta a Facebookon terjedő kártékony hivatkozások kiszűrésében és a profilok biztonságosabbá tételében segítő alkalmazást.
» computerworld.hu/cikk/secfb

WWW.COMPUTERWORLD.HU

Rendszerhiba az IT-biztonságban

Fóti Marcell
ügyvezető,
NetAcademia

A hekkerek 2011-ben elloptak mindent, ami nem volt lebetonozva. Vitték az RSA SecurID-tokenek kritikus kódját, a SONY ügyféladatbázisát, a PHP forráskódját, a McAfee reputációját, az Xbox market kuponalgoritmusát és még sorolhatnánk. Pedig már kezdtük azt hinni, a biztonsági réseket lassan befoltozzák mindenhol – de nem. A kérdés az, hogy miért nem, és meddig nem?

Milyen jövő elé néz a hekkerszakma? És meddig lesz ez így?

A szoftvertényező. Laikus szoftverfejlesztőként gyakran szembesülök azzal a problémával, hogy akárhogy is próbálom végiggondolni és letesztelni a kezem alól kikerülő szoftverek felhasználási eseteit, ez gyakorlatilag sohasem sikerül. Bevallom, az általam kibocsátott kód garantáltan bugos. Ha úgy gondolja a kedves olvasó, hogy ez csupán az én képességeimet minősíti, és egyébként irreleváns információ, téved. Manapság már senki nem tud hibátlan szoftvert fejleszteni, egész egyszerűen azért, mert senki nem látja át a szoftvereket a maguk teljességében. Nincs olyan ember, nincs olyan team és nincs olyan gépezet sem, amely kívülről és felülről a maga teljességében meg tudná vizsgálni mondjuk, egy böngészőprogram kódját, értve, értelmezve annak minden ágát és bogát, kiszűrve ezzel az összes hibalehetőséget. Merthogy nincs erre módszer.

A módszeres hibátlanság helyett módszeres próbálgatással igyekszünk úrrá lenni a káoszon, ezt hívjuk tesztelésnek: alfa-teszt, béta-teszt, penetration testing, fuzzing és egyebek. Nincs még egy olyan iparág, ahol trial-and-fail „módszertan" szerint alakítanák ki a termékek végső formáját. Az autóipari törésteszt hasonló eljárásnak tűnik, de ott a teszt nem arra való, hogy kiderítsék, a termék működőképes-e egyáltalán. A szoftveriparban azonban a teszt a minden. Ami nincs letesztelve, az sokszor nem is működik. Egyfelől ez jó dolog, mert rendkívül sok embernek ad munkát, másfelől a módszertelenség miatt eleve biztos, hogy minden szoftver bugos marad.

Most tételezzük fel, hogy egy végletekig becsületes gyártó 100%-os hibamentességig teszteli egyik alkalmazása következő verzióját. Sajnos azonban ezzel a pepecséléssel lemaradt az éppen zajló, immár sokadik paradigmaváltásról, a konkurencia gyorsabban dobja piacra a maga újdonságát, így a 100%-osan hibamentes alkalmazás gyártója csődbe megy.

Van egy bizonyos határ, ameddig a selejtmentesítésben gazdaságosan el lehet jutni. Minden további lépés egyre növekvő anyagi és időráfordítást igényel. A függvény exponenciális, tehát hibátlan szoftver nem létezik.

Itt két dolgot érdemes megfigyelni. Egy: versengő piaci szereplők esetén senkinek sincs lehetősége tökéletesre csiszolt, agyontesztelt alkalmazást készíteni. Kettő: a piaci környezet lehetetlenné teszi, hogy egy gyártó abbahagyja a folyamatos kódolást és fejlesztést, tehát a bugok gyártása folyamatos.

Ha ezt így elfogadjuk, igazán könnyedén válaszolhatunk a bevezetőben feltett kérdésre: milyen jövő elé néz a hekkerszakma? Szép jövő elé! És meddig lesz ez így? Amíg a világ világ…

Most nézzük meg az érem másik oldalát!

Az emberi tényező. Persze nem csak buffer overflow-ra épülő exploit segítségével lehet adatokat lopni, van ennél egyszerűbb módszer is: a kényes információt egész egyszerűen el kell kérni annak jogos tulajdonosától. Megy ez, mint a WikiLeaks! Vagy oda kell neki küldeni e-mailben egy csábos vírust. Lefuttatja? Nem kétséges!

Az átejtéses csalások, hivatalos nevükön social engineering támadások a hekkelés egy másik vetületét tárják elénk: ez az az eset, amikor nem a számítógép, hanem a homo sapiens szoftverét hekkelik meg. E támadástípusnál az az érdekes, hogy az emberek 100%-a – még a becstelen zsiványok is – becsületesnek tartja önmagát, nem beszélve Mari néniről, aki annyira becsületes, hogy ha talál egy teli pénztárcát egy sötét sikátorban, akkor sem vesz ki belőle egy árva garast sem, ha éppen az éhenhalás szélén áll. És mégis, gigabájtszámra juttat titkos adatokat illetéktelen kezekbe. Mi történik itt?

Nem meglepő módon ez is egy rendszerhiba. Vegyük azokat az eseteket, amikor az „adatgazda" szánt szándékkal lopja el az adatokat, mert ha öntudatlanul teszi, az teljesen más kérdéskör. A jelenség magyarázata egyszerű: a becsületesség egy adott kontextuson belül érvényes. A zöldségesnél nem dugunk a zsebünkbe egy marék meggyet, míg az utcán járva ismeretlenek meggyfájáról – hm-hm! mégis-csak-jaj – hát igen. Ráadásul lelkiismeret-furdalás nélkül!

A Social Engineering lényege, hogy a támadó olyan kontextusba helyezi az áldozatot, amelyben az adott cselekedet elfogadottá, böcsületessé válik. Ez az egyik leggyakoribb alapminta. (Vannak más esetek, például zsarolás stb., amelyekkel most nem foglalkozunk.) Néhány példa: hogyan vegyünk rá egy minden létező kiképzésen átesett, kőkemény, hazájához és az elveihez hű tengerészgyalogost, hogy tagadja meg a parancsot? Hitessük el vele, hogy a felettese áruló. Szegény pára ezt követően olyan szépen tagadja meg a parancsot, hogy „öröm" nézni. Hogyan vegyük rá Mari nénit, hogy adja ki a támadó által igényelt hipertitkos adatot? Változtassuk meg a környezeti feltételeket oly módon, hogy ő ezt önként és dalolva, segítségnyújtásképpen adja oda. Ennek tipikus példája, amikor az informatikus „bajban van", akár ki is rúghatják, a Mari néni jelszava azonban kimentheti őt a slamasztikából.

Se szeri, se száma a különböző átejtéseknek, és ebben az a szomorú, hogy ezek valamelyike működni fog a kiszemelt áldozat ellen. A szoftverekhez hasonlóan a felhasználókon is végezhetünk minőségi javításokat – ezt oktatásnak nevezzük. A zéró selejt azonban ezen a területen sem érhető el.

Tehát milyen jövő elé néz a hekkerszakma? Szép jövő elé. És meddig lesz ez így? Amíg a világ világ.

Hyde Tech Corner

Ezen a héten Borek András, a nyílt forráskódú rendszerek szakértője, és Nyéki Zsolt, a Vodafone Magyarország üzletfejlesztési vezetője kommentálja a hét híreit, eseményeit.

Összeállította: Tóth Lívia

Heti összeállításunkból megtudhatják, mi a véleménye a szakmának arról, hogy az Oracle fizetőssé teszi a MySQL-t, valamint az is kiderül, hogyan vélekedik a Vodafone a Google mobilpénztárcájáról.

Pénztárca a Google-tól

A készpénz eltűnésével párhuzamosan egyre erőteljesebbé válnak a különböző mobilfizetési megoldások. A Google Wallet szolgáltatást az amerikai óriásvállalat még május 26-án jelentette be, most viszont már nemcsak tesztelési céllal használható a lehetőség, hanem Sprint Nexus S 4G okostelefonokon élesben is lehet költeni a pénzt (egyelőre csak az USA-ban). A Google Wallet a near-field communications (NFC, közeltéri kommunikáció) technológiát használja, amely nagyon kis hatótávolságban (néhány centiméter) képes jeleket küldeni, így kommunikálva az adatfolyamot értelmezni képes terminállal. Vagyis mindössze arra van szükség egy gyors fizetéshez, hogy okostelefonunkat hozzáérintsük az elfogadóhely termináljához, és máris megtörténik a tranzakció.
computerworld.hu/cikk/google-mobilpenztarca

Nyéki Zsolt
üzletfejlesztési vezető, Vodafone Magyarország

NYÉKI ZSOLT ÜZLETFEJLESZTÉSI VEZETŐ, VODAFONE MAGYARORSZÁG

Az NFC-technológia olyan eszközzé változtatja az okostelefonokat, mely teljesen új dimenzióba emeli vásárlási szokásainkat. A sikerhez alapvetően fontos, hogy a megoldás egyszerűen és mindenki számára teljes körben elérhető legyen, természetesen a pénzügyi szolgáltatásoknál megszokott magas biztonsági szinten. Fontos, hogy a pénzügyi szolgáltatásoknál meglegyen az ügyfelek számára a teljes körű kontroll és szabadság, függetlenül attól, hogy milyen NFC-s telefonkészüléket használnak.

A Vodafone részéről úgy gondoljuk, hogy erre a SIM-alapú mobil NFC-s megoldások jelentik az egyetlen megnyugtató választ – ezt a Szigeten teszteltük is. A SIM-alapú biztonságos NFC-megoldások elterjesztésére a piac többi szereplőjével közösen létrehoztuk a Mobiltárca Egyesületet, ennek célja olyan piaci keretek kialakítása, amelyek biztosítják, hogy a hamarosan bevezetendő kereskedelmi mobil NFC-szolgáltatások minden szempontból megfeleljen az említett szempontoknak.

Így lesz pénze a MySQL-ből az Oracle-nek

Az Oracle újabb kereskedelmi bővítményeket készített a nyílt forráskódú MySQL adatbázis-kezelő szerver vállalati verziójához, amely így egyre jobban leválik az eredeti, az open-source közösség által fejlesztett, bárki számára elérhető ingyenes verzióról. Az eredeti, közösségi kód fejlesztői egy részének ez nem annyira tetszik.
computerworld.hu/cikk/oracle-mysql

Borek András
szakértő
nyílt forráskódú rendszerek

BOREK ANDRÁS SZAKÉRTŐ, NYÍLT FORRÁSKÓDÚ RENDSZEREK

Nagyon érdekes a téma, több oldalról is. Vajon mennyire etikus egy nyílt fejlesztés bizonyos funkcióit csak fizetős ügyfeleknek elérhetővé tenni? Ez nagyon régi dilemma nem csak a MySQL esetében, sok más hasonló nyílt fejlesztés van, ahol a licencelési modell hasonlóan működik. Ezeket jellemzően *freemium* szoftvereknek szokták nevezni. A pénzért kínált többletszolgáltatás/funkció nem feltétlenül ellentétes a szabad szoftveres elvekkel. Az ugyanis nem az ingyenességről szól, hanem a szoftverhasználathoz fűződő egyéb jogokról (forráskód megismerése, módosítása stb.). Persze mindig lesznek olyanok, akiknek ez a modell nem szimpatikus, de ezzel egészen addig együtt kell élni, amíg a freemium modell létezik és működőképes.

A *governance* kérdésköre még érdekesebb téma, ugyanis a fejlesztési irányok meghatározásának kérdésével foglalkozik. Sajnos pont az Oracle esetében problematikus ez, hiszen autokratikus vezetési stílusával a szabad fejlesztői közösség nem találja meg a megfelelő együttműködést. Volt már máshol is hasonló példa, de az utóbbi időben az OpenOffice és a MySQL fejlesztőiből is kivált már egy csoport, amely a saját fejlesztési roadmapjét követi, természetesen más licencelési struktúrával. Az Oracle vagy bármelyik cég, amelyik hatalmi szóval próbálja meg rendezni a vitás helyzetet, nagyon hamar fejlesztők nélkül találhatja magát, mert a GPL-licenc lehetővé teszi, hogy a korábbi fejlesztésre építve egy új, független fejlesztési ág induljon el, azaz forkolják a projektet.

HÍRMOZAIK

Piacvezető a SAS

Az IDC üzletiintelligencia-eszközök globális piacát bemutató jelentése szerint 2010-ben a bevételek alapján továbbra is a SAS vezette a fejlett analitikai megoldások szegmensét 35,2 százalékos piaci részesedésével. Az eredmény növekedést jelent a 2009. évi 34,7%-hoz képest.

Pénzügyben is hasít az SAP

Piacvezető az SAP AG – az IDC elemző cég felmérése szerint – a pénzügyi-számviteli szoftverek világpiacán az ebből származó árbevétel, valamint a piaci növekedés és részarány alapján. E szoftverpiac globális mérete elérte a 13,7 milliárd dollárt, mely 4,6%-os növekedést jelent 2009-hez képest.

Novell-elismerések

Rangos elismerést kaptak a Novell termékei a személyazonosság- és jogosultságkezelés területén. Pár napon belül két különböző felmérés ismerte el a Novell Identity Managert, illetve az Access Governance Suite programcsomagot. Előbbit a SearchSecurity.com internetes oldal olvasói minősítették a legjobbnak, 2007 után immár másodszor, míg utóbbi erősségeit a Forrester Research legfrissebb elemzése méltatta.

2012 a biztonságé

A Ponemon Institute HP által finanszírozott felmérése, a *Kiberbűnözés éves költségének vizsgálata* megállapította, hogy a számítógépes támadások a széles körű tájékozottság ellenére komoly költségeket generálnak a vállalatoknál és a kormányszerveknél. A Coleman Parkers szintén a HP megbízásából készített vizsgálatából pedig kiderült, hogy a nagyvállalatoknál a legmagasabb, gazdasági jellegű kockázatot szorosan követi a technológiai jellegű kockázat.

Támad a láthatatlan ellenség

Kristóf Csaba ▪ A Hacktivity konferencián *Szőr Péterrel*, a McAfee kutatójával a jelen és a jövő vírusvédelmi kihívásairól, illetve a biztonsági piac helyzetéről beszélgettünk.

Computerworld: Mi volt az első gondolata, amikor meghallotta, hogy az Intel felvásárolja a McAfee-t?
Szőr Péter: Rögtön értettem, hogy mit szeretnének, mert húsz évvel ezelőtt azzal zártam a diplomamunkámat, hogy amíg a hardveres biztonság nem lesz jobb, vagy a biztonság nem a hardverből indul ki, addig szoftverrel nagyon nehéz lesz védekezni bármi ellen. Például egy egyszerű dátumcserével elő lehet idézni érdekes dolgokat, vagy ki lehet kerülni egy másolásvédelmet. Régóta látszott, hogy amikor exploitokról van szó, akkor a processzornak szerepe van. Mivel a processzor futtatja az utasításokat, a segítségével lehet a biztonságot javítani. Ez sokkal eredményesebb, mint amit csupán szoftverekkel el lehet érni. A napokban jelentette be a McAfee az első inteles koprodukciót DeepSafe néven. Ez gyakorlatilag egy hypervisor alapú védelem, amely az operációs rendszert az Intel meglévő technológiáival virtuális gépen tudja futtatni. Ezután kívülről lehet kontrollálni a gép működését. Például, ha egy rootkit megváltoztat valamit a memóriában, az azonnal észlelhető, és még azelőtt meg lehet állítani, mielőtt teljesen be tudna töltődni.

CW: Ez csak Intel platformon, Intel processzorokkal fog működni? Az Intel ugyanis az EU-val is megállapodott, hogy versenyjogi szempontokból más gyártókat nem hoz hátrányba a McAfee felvásárlásával.
Sz.P.: Egyelőre inteles (i3, i5, i7) processzorokkal működik a DeepSafe, de a jövőben biztosan lesznek más fejlesztések is. Az Intel szigorúan be fogja tartani a megállapodásokat.

CW: Az MBR- (Master Boot Record) alapú rootkitek kapcsán vita alakult ki, hogy teljes körű, biztos eltávolításukhoz szükséges-e a Windows újratelepítése, hiszen nem lehet tudni, hogy milyen hátsó kapuk nyíltak a fertőzött rendszeren, és arra milyen nemkívánatos kódok kerültek fel. Ön mit gondol erről?

„Ha az informatikára nincsenek források, akkor a biztonságra sincs törvényszerűen pénz....”

Szőr Péter
MCAFEE

Sz.P.: A rootkiteknek ez az egyik veszélye. Ezért akarjuk korán megállítani őket, mert minél később kerül erre sor, annál komolyabb a következmény. Általában a szoftveres megoldások működnek a károkozók irtása során, de ezt a rootkitek próbálják megakadályozni. Van egy rootkit, amely igyekszik meggátolni, hogy újraírják az MBR-t. Ezért először a memóriában meg kell változtatni a rootkit kódját, hogy ki tudjuk irtani, majd dekódolni kell az eredeti MBR-t, és az összemásolást el kell végezni. Ez nagy akrobatika. A sima fdiskes megoldás is ugyanilyen hatékony, ha a partíciós tábla tartalma nem változik meg; azonban a korai bootszektor-vírusok megjelenése óta tudjuk, hogy ez nincs törvényszerűen így. Az eredeti állapot helyreállítása egyre bonyolultabb. Kaptunk például Kínából egy BIOS-t fertőző rootkitet, ami elen tényleg nem lehet csak szoftveresen védekezni, vagy csak az MBR helyreállítására fókuszálni, mert a flash BIOS-ból is ki kell szedni a kódot.

CW: Az említett rootkit csak Award BIOS-szal rendelkező számítógépeken működik. Más BIOS-ok is célkeresztbe kerülhetek?
Sz.P.: Először valóban úgy tűnt, hogy csak az Award BIOS-t veszélyezteti, de vannak olyan nyílt forráskódú kitek hozzá, amelyek segítik a BIOS programozását. Ezért szerintem sokkal szélesebb körben el tud terjedni.

CW: Idén számos jelentős biztonsági incidensre derült fény, amely célzott támadásokra vezethető vissza. Lesznek ezekkel szemben hatékonyabb védelmi megoldások?
Sz.P.: Úgy látjuk, hogy az APT-k (Advanced Persistent Threat) jelentős része rootkitet használ. A védekezés célja tehát nemcsak a rootkit probléma megoldása, hanem hogy az APT-k ellen is fellépjünk. Sokféle megoldáson törjük a fejünket, de ezekről még korai lenne beszélni. Nagy fejlődési lehetőségek vannak a felhőalapú védelmekben, ugyanakkor vannak hátrányaik is. Ezért a legnagyobb fantáziát a hardver közeli megoldásokban látom.

CW: Amerikából is kedvezőtlen hírek érkeznek a gazdaság helyzetét illetően. Ön szerint a pénzügyi nehézségek mennyire befolyásolják a biztonsági piacot?
Sz.P.: Jelentősen. Idefelé a repülőn olvastam *Andrew Grove*-tól – aki az Intel magyar származású vezetője volt – egy cikket a gazdaságban zajló folyamatokról. Például, hogy Amerikában majdnem kétmillió informatikusi állás tűnt el, közben vannak kínai cégek, amelyeknél több mint egymillió ember dolgozik outsourcing területen. Önmagában az állások száma is probléma. A mindenhol jelen lévő, globális világválság hatására sokakban felmerül, hogy nem kellene-e a kiberbűnözés területén tevékenykedni, hiszen rengeteget lehet vele keresni. Még a vírusterjesztő ügynökök is heteken belül képesek 150 ezer dollárt bezsebelni. Óriási pénzekről van itt szó. Én inkább kiberbűnözői oldalon látok növekedést, mint a szakmában, mivel nincsenek állások. A cégek az IT-biztonságot is kiszervezik. Persze nem minden amerikai szervezet akarja az IT-biztonságot Indiából megcsináltatni, de gyakori, hogy egy amerikai vállalat több cégnek is nyújt teljes informatikai támogatást és biztonsági felügyeletet.

A biztonság az IT része, és ha az informatikára nincsenek források, akkor a biztonságra sincs törvényszerűen pénz. Nagyon gyakran azzal intézik el, hogy vesznek egy programot, mert az „mindent megold”, pedig szakemberekre lenne szükség. Különösen az APT-k kivédéséhez kellene folyamatos hálózatfelügyelet.

CW: Mit tanácsol a sokszor szűkös anyagi forrásokkal rendelkező magyar vállalatoknak?
Sz.P: Ha Amerikában ilyen a helyzet, akkor el sem tudom képzelni, hogy Magyarországon mekkora nehézségek lehetnek ezen a területen. Ha a biztonságot komolyan akarják venni, akkor azt közelebbről is meg kell nézni, és a felhasználóknak tudatosabbaknak kellene lenniük. Mindez azonban számomra jelenleg fantazmagória, pedig egyre többen szembesülnek azzal – főleg a web révén –, hogy jobb vigyázni. Az oktatás területén ezzel foglalkozni kell. A Hacktivity és az ehhez hasonló konferenciák a biztonságot helyezik a középpontba, és sokan beszélnek róla, olyanok is, akik minderről a hétköznapokban nem nagyon hallanak.

CW: Egy éve jelent meg „A vírusvédelme művészete” című könyve Magyarországon. Milyen visszajelzéseket kapott? Lesz folytatás?
Sz.P.: Nagyon jó visszhangja volt, az első kiadás nagy része el is fogyott. Reményeim szerint lesz második kiadás is, de csak valamikor a Windows 8 megjelenése után, amiben a mobilfenyegetettségekről, a rootkitekről és a hardveres védelemről is szívesen írnék.

Kibertámadások is sújtják Japánt

Kristóf Csaba ▪ Az elmúlt időszak számos jelentős biztonsági incidense után kijelenthető, hogy az internetes támadások több esetben olyan célpontok ellen irányulnak, amelyeknek súlyos nemzetbiztonsági következményei lehetnek. E támadások közé tartoznak bizonyos amerikai energetikai vállalatok, kritikus infrastruktúrákat üzemeltető cégek, valamint védelmi beszállítók elleni akciók is. Az incidensek azonban korántsem csak az amerikai szervezetek ellen irányulnak – Japánt a természeti katasztrófák mellett a kiberbűnözés is egyre inkább sújtja. Az ország jelentős katonai beszállítóját súlyos incidens érte.

A Mitsubishi Heavy Japán egyik legjelentősebb védelmi beszállítója. Informatikai infrastruktúrájában olyan adatok is vannak, amelyek illetéktelen kezekbe kerülése nagyon komoly következményekkel járhat. Márpedig megvolt az esélye, hogy bizalmas információk szivárogjanak ki a szervezettől, ugyanis az informatikusok számos – kémprogrammal – fertőzött számítógépre akadtak.

A Mitsubishi Heavy szerint a támadás még augusztusban következett be, amikor eddig ismeretlen elkövetőknek különféle kártékony programokat sikerült bejuttatniuk egyes rendszerekbe. A problémára akkor derült fény, amikor augusztus 11-én a cég szakemberei az egyik szerveren nemkívánatos kódokat fedeztek fel. A vizsgálatok szerint 45 szerver és 38 munkaállomás fertőződött meg többek között egy olyan trójaival is, amely kifejezetten jelszavak megszerzésére specializálódott. A fertőzés Japán-szerte összesen tíz telephelyen és létesítményben volt kimutatható. Ezeken a helyeken többek között védelmi és ipari berendezések gyártásával foglalkozik a vállalat, sőt az egyik érintett üzemben rakétahajtóművek készülnek. Az eddigi vizsgálatok szerint a vállalattól valószínűleg nem szivárogtak ki értékes adatok, azonban egyelőre nem lehet biztosan kijelenteni, hogy titkos információk nem kerültek a támadók birtokába.

Biztonsági szakértők szerint a Mitsubishi Heavy esete kísértetiesen hasonlít azon incidensekhez, amelyek korábban amerikai szervezeteket sújtottak, illetve többek között a Google egyes rendszereit is érintették. A Google akkor úgy nyilatkozott, hogy Kínának köze lehet a történtekhez, amit utóbbi rögtön cáfolt. Ez ideig semmiféle olyan bizonyíték nem került elő, amely azt támasztaná alá, hogy a Mitsubishi Heavy elleni akció mögött valamely állam húzódna meg.

ESEMÉNYNAPTÁR

Szeptember 27–28. BUDAPEST
ITBN 2011
» http://itbn.hu

Szeptember 29. BUDAPEST
Üzleti reggeli: CRM
» www.multisoft.hu

Október 6. VOIP
Biztonság mindenekfelett! – Hálózati eszközök
» https://gloster.webex.com

Október 6. BUDAPEST
Open Source BI Fórum
» www.opensourcebi.hu

További események
» www.computerworld.hu/esemenyek

REGISZTRÁLJON

Ha szeretné hétről hétre a legfontosabb szakmai résztvevőkhöz eljuttatni az Ön cégével kapcsolatos információkat, regisztráljon Céginfó szolgáltatásunkra oldalunkon.

ceginfo.computerworld.hu

Google-erő: veszély vagy lehetőség?

Szalay Dániel ▪ Az amerikai szövetségi versenyhatóság trösztellenes vizsgálata a Google keresőtechnológiájával kapcsolatban felfedheti a keresőmotor által képzett találati rangsor működését, illetve a hirdetések és az organikus keresőtalálatok közötti lehetséges összefüggéseket – véleledett néhány Google-kritikus egy washingtoni fórumon. – Azzal, hogy a Google keresőjébe integrálja többi szolgáltatását is, illetve lehetővé teszi a fizetett hirdetések megjelenítését az ingyenes találatok mellett, hatalmas lett a visszaélés veszélye – mondta *Eric Clemons*, a Pennsylvaniai Egyetem információs menedzsment professzora. Abban látja a veszélyt, hogy a Google fizetős keresőszolgáltatását igénybe vevő hirdetők esetleg előnybe kerülhetnek az organikus találatoknál is. Clemons erről a Technology Policy Institute (TPI) fórumon beszélt Washingtonban.

– Az amerikai versenyhatóság, az FTC (U.S. Federal Trade Commission) júniusban indított antitröszt vizsgálata lehetőséget adna a nyomozóknak, hogy lássák, hogyan működik a Google találatainak rangsorolása, és felléphetnének egyes, versenyellenes folyamatok ellen – ezt már *Oren Bracha*, a Texasi Egyetem technológiára szakosodott jogászprofesszora mondta. Az egész keresőmechanizmus működése teljesen titokban van tartva – adott hangot véleményének Bracha. Szerinte az egész olyan, mint egy nagy sötét doboz, és a Google kivételével senki sem tudja, hogy mi folyik belül. Néhányan azonban most kinyithatják a dobozt.

Amíg Clemons és Bracha a Google vizsgálata mellett foglalt állást, addig más felszólalók megkérdőjelezték, hogy van-e értelme egy antitröszt vizsgálatnak. Bár sokan panaszkodnak a Google keresőjének egyre erősödő dominanciájára és a keresőrobotok találatainak üzleti érdekek szerinti manipulálására, az antitröszt ügyek egyesek szerint kárt okozhatnak az ügyfeleknek, vagyis a felhasználóknak – mondta *Geoffrey Manne*, a Google támogatását élvező International Center for Law and Economics alapítója. Csak azért, mert a Google óriásvállalat lett, még nem fogadhatjuk el, hogy trösztellenes eljárást indítsanak a cég ellen – mondta Manne, valamint *Michael Katz*, a kaliforniai Berkeley Egyetem üzleti tudományok professzora. Az amerikai törvények lehetővé teszik, hogy a cégek monopolhelyzetbe kerüljenek, egészen addig, amíg a vállalatok tisztességesen működnek – tette hozzá Katz, akinek a véleménye persze annyiban semmiképp sem tekinthető elfogulatlannak, hogy dolgozott a Googlenál. – Az Egyesült Államokban semmi rossz nincs abban, ha valaki sok pénzt csinál – mondta Katz. – Meg kell hagyni a Google számára a lehetőséget, hogy új szolgáltatásokat vezessen be és integrálja a kereső funkcionalitást más termékeibe is, ha ezzel jobban ki tudja szolgálni az embereket – folytatta.

A trösztellenes fórum egyfajta előzetese is lehet annak, ami a következőkben az amerikai szenátusban várja majd a Google vezetőjét. Ott a *Google ereje: az ügyfelek szolgálata, avagy fenyegető veszély?* címmel tartanak meghallgatást, és várják *Eric Schmidtet*, a Google első emberét is.

Árulják a BUILD-en kiosztott tableteket

Dávid Imre ▪ Az eBay online árverési oldalon 3500 dollárnál is többet kérnek a Microsoft közelmúltbeli, fejlesztők számára rendezett BUILD konferenciáján szétosztott, a Windows 8 korai verzióját futtató Samsung táblagépekért.

A Microsoft ugyanis ötezer, a Windows 8 nem publikus bétájával telepített Samsung Slate tabletet osztott ki a konferencián részt vevő fejlesztők között. A jelek szerint a leleményes szakemberek közül többen úgy döntöttek, pénzt csinálnak *Steve Ballmerék* ajándékából, és az eBay-en árulni kezdték a különféle extrákkal felpöccentett mobileszközöket.

A gépeket eredetileg azért kapták a fejlesztők, hogy alkalmazásokat készítsenek a Windows 8 érintésérzékeny Metro platformjára. Az Intel 1,6 gigahertzes, dupla magos Intel Core i5 processzorával felszerelt eszköz a Samsung augusztusban bemutatott Series 7 Slate-jének alapjaira építkezik, ám számos egyedi komponenssel – különféle szenzorokkal, portokkal, 3G-s internetkapcsolattal – is ellátták. Mi több, a fejlesztők egy egyéves ingyenes 3G-előfizetést is kaptak az AT&T-től.

Az eBay szerint szeptember 14-e óta több mint 12 speciális tablet talált gazdára az oldalon, darabonként 1800 és 4000 dollár közötti áron. A Series 7 Slate-et október másodikán dobja piacra a Samsung, modelltől függően 1099 és1349 dollár közötti kiskereskedelmi áron.

Az Apple elégedetté tesz

Dávid Imre ▪ A Beyond Philosophy elemző cég ötvenhárom üzleti vezető bevonásával készült nemzetközi felmérése, a *Global Customer Experience Management Survey* szerint az Apple termékei és szolgáltatásai nyújtják a legjobb felhasználói élményt az informatikai piacon nemcsak a magánfelhasználók, hanem az üzleti vezetők körében is. A kutatás célja az volt, hogy felmérjék, melyek azok a gyártók és termékek, amelyekhez a leginkább ragaszkodnak a felhasználók, és milyen veszélyeket rejthet az újramárkázás (re-branding) a fogyasztói élmény szempontjából. (A kutatás teljes anyaga letölthető a Beyond Philosophy weboldaláról.) A megkérdezettek túlnyomó többsége szerint jelenleg az Apple a világ legerősebb márkája; a top tízben olyan cégek szerepelnek még, mint az Amazon, a Starbucks, a Disney, a Virgin Atlantic és a Vodafone.

A válaszadók szerint az Apple népszerűségének legfontosabb okai: innovatív marketingstratégia, minőségi termékek és az, hogy az iPodhoz és iPadhez hasonló „kategóriateremtő" fejlesztések révén az iparág vezető vállalatává nőtte ki magát.

Scott Merritt, a Beyond Philosophy szóvivője a *Macworldnek* nyilatkozva kijelentette: „Az Apple az egyik leginnovatívabb márka a világon, ez a legfőbb oka globális népszerűségének. Már a boltjaik is varázslatosan néznek ki. Egyszerűen menő dolog Apple-termékeket vásárolni." A közelmúltban az Apple a mértékadó fogyasztóielégedettség-index szerint is az első helyre került. Az American Consumer Satisfaction Index (ACSI 2011) a számítógépgyártók termékeit vizsgálta, 70 ezer felhasználó bevonásával.

Rutinos innováció

A kezdetek: tervezés. Az IQSYS Zrt. csapata évtizedes tapasztalattal rendelkezik a közösségi közlekedési társaságoknál. Tervezőrendszerekkel kezdődött: menetrendek, sofőrök beosztása, teljesítményelszámolás és statisztikák. A felhasználók a „nagyok", azaz a BKV és a Volánbusz, a fővárosi régió szolgáltatói voltak akkoriban. A rendszerek fejlődnek, segítségükkel több mint 3000 jármű és azok vezetői napi munkáját szervezik, de nemcsak forgalmi vonalon; kereskedelmi rendszerek is üzemelnek, amelyekkel a jegy- és bérlet-értékesítés menedzsmentje kap informatikai támogatást.

A folytatás: GPS! A GPS műholdak hamar életre hívták a flottafelügyeleti rendszereket. Az IQSYS a közösségi közlekedés céljai szerint specializált rendszert fejlesztett ki partnerei segítségével. Ez egy tervező- és elszámoló rendszerhez illesztve teljes körűvé teszi egy közlekedési társaság szakmai háttérrendszerét. A GPS-technológia és a mobil adatátvitel minden járművet állandó kapcsolatban tart a központtal, ismertté válik azok pozíciója, pontossága. Az adatokból információ lesz – az utasok tájékozódhatnak az aktuális menetrendről a megállókban és az interneten. Az adatkapcsolatot más célra is fel lehet használni, ez az e-ticketing – a készpénzkímélő és kényelmes fizetési mód, amely gyorsítja a vásárlási és ellenőrzési folyamatokat; hosszan sorolhatnánk az előnyöket. Az IQSYS az elmúlt években már három Volán társaságnál vezetett be ilyen rendszert, így megalapozta a fejlődés irányát, elsősorban az e-ticketing megoldás fejlesztésére koncentrálva. A megoldás jelenleg az Elektra Hungária ajánláson alapuló rendszertechnikával dolgozik. Az utasok elektronikusan és nyomtatottan is megszemélyesített – azaz a nevükre szóló – érintésmentes chipkártyát kapnak, ezekre tudnak ún. díjtermékeket tölteni, azaz így válnak jogosulttá az utazásra. Felszálláskor a járművezető pénztárgépén (amely egyben a GPS-rendszer lelke, a fedélzeti multifunkciós eszköz), illetve jegyellenőri készüléken utazás közben lehetséges elektronikusan az utazási jogosultság ellenőrzése.

A jelen és a jövő: kártya és mobiltelefon. Az IQSYS megoldásai tehát az érintésmentes kártyákra alapozva kínálnak e-ticketing funkciókat. A szakemberek azonban dolgoznak a kiterjesztésen, a kártyát ugyanis be kell szereznie az utasnak ahhoz, hogy „része" legyen a rendszernek, míg mobiltelefonja manapság már szinte mindenkinek van. A mobilok cserélődése felgyorsult, embert próbáló feladat az újítások figyelése. Ezek egyike az NFC, amellyel a mobiltelefon multifunkcionális eszközzé válik: kártyaként tud működni, azaz helyettesíthet egy közlekedési kártyát is. Használata egyszerű, biztonságos és a legfontosabb: rövidesen a mobiltelefonok többsége NFC-képes lesz. Tehát ezek válhatnak a világon a legelterjedtebb közlekedési kártyává…

Előfordulhat, hogy a plasztikkártyák rövid életűek lesznek és az e-ticketing jövője az NFC? Arról, hogy pontosan milyen jellemzői is vannak az NFC-nek, illetve mi mindenre lehet még használni egy NFC-képes mobiltelefont a közlekedésben vagy az élet megannyi területén, sok-sok információt és gyakorlati példát ismerhet meg az *IQSymposium – Operatív Információtechnológia 2011 konferenciánkon.* ■

Hogyan fenyegeti a Gmail a Microsoftot?

Szilágyi Szabolcs ▪ A Gartner piackutató vállalat szerint a Google e-mail szolgáltatása hamarosan komolyan meg fogja csapolni a redmondiak vállalati szférából származó bevételeit.

A Google vállalati e-mail piacból való részesedése nagyjából 1 százalék – közölte a Gartner, ám néhány éven belül el fogja érni a 10 százalékot, becsülte meg a jövőt a piackutató. Napjainkban elsősorban az 5 ezer vagy annál több főt alkalmazó vállalatok körében válik egyre népszerűbbé a Gmail, függetlenül attól, hogy a magán- vagy az állami szektor szervezeteiről van szó.

Olyan ügyfeleket tudhat magáénak a Google e-mail szolgáltatása, mint a Motorola Mobility 22 ezer alkalmazottal, az Egyesült Államok szövetségi hivatalainak munkáját segítő General Services Administration 17 ezer alkalmazottal, a Los Angeles-i polgármesteri hivatal szintén 17 ezer alkalmazottal, a Jaguar Land Rover autógyártó 15 ezer alkalmazottal, az InterContinental szállodalánc 25 ezer alkalmazottal és a wyomingi állami vezetés 10 ezres felhasználói létszámmal.

„Jelenleg az e-mail felhőháború eszkalálódásának kezdetét látjuk" – írta *Matthew Cain*, a Gartner elemzője a Google vállalati térhódítását kutató, nemrég kiadott jelentésben. A piackutató szerint a felhőalapú elektronikus levelezőrendszerek a teljes vállalati e-mail piac mintegy 4 százalékát teszik ki. A szegmenst egyébként a Microsoft dominálja – a redmondi felhőalapú Exchange szolgáltatás még 2010-ben jelent meg, a lehetőségeket pedig az Office 365 idei kiadásával bővítette tovább a vállalat.

Természetesen a Google sem tétlenkedett az elmúlt egy évben. Több mint kéttucatnyi változtatást eszközölt a Gmailben, melyek révén jelentősen fejlődött többek között a biztonság és a kezelhetőség. Ide tartozik például a felhasználói bejelentkezéseket tároló sütik (cookie) alaphelyzetbe állításának, illetve a felhasználói csoportokra vonatkozó szabályok kezelésének lehetősége. Ezzel az ütemmel a Microsoft úgy próbálja felvenni a harcot, hogy a cloudban használt Exchange-ben teszi közzé először az új fejlesztéseket, nem a különálló szoftverben. „Ez jelentős változást jelent a Microsoft gyakorlatában" – összegezte Cain.

A piackutató szerint nem azért alacsony a Gmail vállalati felhasználásának szintje, mert azt a Google üzemelteti, hanem azért, mert a vállalatok – ma még – túlságosan komplex igényeket támasztanak egy felhőalapú levelező- és irodai szolgáltatással szemben. Cain vélekedése szerint az olyan területek szabályozása, mint a belső routing, alkalmazásintegráció és megfelelőség, egyelőre túl nagy falatot jelentenek a cloudalapú szolgáltatások számára. „Egy fejlett, integrált rendszerrel bíró vállalat nem fogja egyhamar az e-mail szolgáltatást felhőben kínáló lehetőségeket keresni. A cloudszolgáltatók egyszerűen nincsenek abban a helyzetben, hogy mindezt a szervezetre szabást megtehessék" – összegezte véleményét az elemző.

Nem maradt válasz nélkül a Gartner jelentése. A Microsoft hivatalosan is reagált a piackutató vállalat megállapításaira. Eszerint: „A piacon található egyéb megoldások elérhetősége ellenére az Office 2010 lett az Office történetének leggyorsabban fogyó változata; hatalmas érdeklődést látunk az üzleti szegmens részéről vállalati mérettől függetlenül, felhőalapú irodai szolgáltatásunk, az Office 365 iránt." Fontosnak tartották hangsúlyozni azt is, hogy a Microsoft Office egy vállalati piacon már régóta bizonyított, „páratlan" felhasználói élményt biztosító megoldás, amely akár a felhőben, akár azon kívül is megállja a helyét. A Microsoft szerint ezt a lehetőséget egyetlen más gyártó sem kínálja jelenleg.

De mit tehet a Google, hogy birokra kelhessen a Microsoft felhalmozott tudásával, tapasztalatával és erőforrásaival? Nos, például előre ütemezetten további funkciókat integrálhat szolgáltatásába, illetve azzal is sokat lendíthetne a felhőalapú e-mail szolgáltatás terjedésén, ha átláthatóvá tenné azt. Ez a probléma egyébként nem a Google sajátja, a cloud megoldásokra általánosságban jellemző. Persze arról szó sincs, hogy a keresővállalat outsiderként nézné a piaci folyamatok zajlását: a Google Apps szoftvereket már több mint 4 millió cég használja, és napi szinten 5 ezerrel bővül számuk – derült ki nemrég (miközben a nyár elején még szerényebb számokat tett közzé a keresőóriás).

Tesco Mobile januártól

Jövő év első felében megkezdi szolgáltatását a hazai piacon a Tesco Mobile. A Vodafone és a Tesco 50-50 százalékos tulajdonában lévő vegyesvállalat független, virtuális mobilszolgáltatóként működik majd; a Vodafone hálózatát használja, szolgáltatásait a Tesco áruházakban kínálja. A Tescónak már vannak a nemzetközi piacon hasonló együttműködései, ám most először választotta mobilpartneréül a Vodafone-t.

A tervezett szolgáltatásról részleteket egyelőre nem árultak el. Annyit lehet tudni, hogy a Tesco Mobile hívószámai nem 70-essel kezdődnek majd, hanem új előhívót kapnak. Az új szolgáltató saját árképzést alkalmaz, és ügyfelei mind hang, mind internetes szolgáltatásokat vásárolhatnak.

A biztonság rögös útjai

Az informatikai biztonság az elmúlt években minden korábbinál gyorsabban fejlődött, aminek eredményeként komplex IT-területté nőtte ki magát. Kezelése komoly erőforrásokat, szakértelmet és figyelmet követel. Írta: Kristóf Csaba

Mostanában gyakran jelennek meg biztonsági incidensekkel kapcsolatos beszámolók az informatikai hírek között. Ezek egy része olyan (katonai, biztonsági, pénzügyi stb.) szervezetek berkein belül következik be, amelyekről azt gondolnánk, hogy sem pénzügyi, sem szakmai, sem elkötelezettségbeli nehézségek nem hátráltatják a hatékony védelem kialakítását. Ez valószínűleg így is van. Ugyanakkor **a kiberbűnözés nap mint nap bizonyítja, hogy százszázalékos biztonság márpedig nem létezik, és a legkisebb biztonsági réseket is könyörtelenül kihasználja. Ha az infrastruktúrán nem talál gyenge pontot, akkor az emberi tényezők felé fordul,** és a social engineering alkalmazásával igyekszik hozzáférést szerezni egyes rendszerekhez. Amikor pedig egy jelentős károkat okozó incidensről utólag kiderül, hogy a támadók milyen módszereket alkalmaztak, sokszor pofonegyszerű trükkökről hull le a lepel. Joggal merülhet fel a kérdés: az ilyen triviális módszerekre – különösen kormányzati és nagyvállalati környezetekben – miért nem lehet felkészülni és megelőző intézkedéseket tenni. Az egyik legkézenfekvőbb válasz a védelem komplexitásában keresendő.

EGY KIS TÖRTÉNELEM

Amikor a fekete kalapos hackerkedés történeti elemzésével foglalkozunk, érdekességként megjegyezzük, hogy sok esetben az 1960-as évekig nyúlnak vissza az események szálai, azonban a tényleges károkozások inkább a 70-es és 80-as években vették kezdetüket. Először többnyire telefontársaságok kerültek célkeresztbe: különösen az AT&T-nek kellett hadakoznia a hackerek első nemzedékével. A fekete kalaposok tevékenységére viszont akkor irányult rá jelentősebb mértékben a figyelem, amikor a híres 414-es csoport feltörte a Los Alamos National Laboratory egyes rendszereit. Az FBI első, számítógépes bűncselekményekkel kapcsolatos letartóztatásai is ezekre az időkre vezethetők vissza.

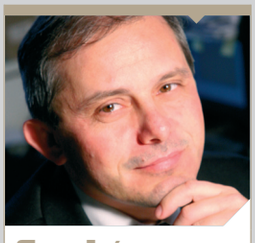
Az informatikai rendszereket és adatokat veszélyeztető tevékenységek elleni fellépés azonban nem igazán szegte kedvét az elkövetőknek, és sorban következtek be az egyénileg, illetve csoportosan elkövetett bűncselekmények. Közben-közben pedig olyan hírességek is színre léptek, mint például *Kevin Mitnick* vagy a Morris féreg megalkotója, *Robert T. Morris*. A támadásoknak áldozatul esett szervezetek száma folyamatosan nőtt, és a NASA-tól kezdve az Amerikai Védelmi Minisztériumon át a CIA-ig bezárólag minden jelentős intézménynek el kellett könyvelnie különféle biztonsági incidenseket. **A nemkívánatos események száma évről évre drasztikus mértékben emelkedett. Az FBI 2000-re vonatkozó jelentése szerint például 1999-hez képest 79 százalékkal nőtt az informatikai rendszereket ért támadások száma, és ezzel együtt újabb és újabb fenyegetettségek ütötték fel a fejüket.**

ÖRÖK TÉMA: A VÍRUSVÉDELEM

Az informatikai biztonság szempontjából hosszú évek óta a kártékony programok jelentik a leggyakoribb fenyegetést. A védelmet több tényező is jelentősen nehezíti. Ezek közül a legfon-

Élet a vírusokon túl

Gombás László, a Symantec magyarországi képviseletének szakértője úgy látja, hogy az elmúlt évek gazdasági problémái visszahúzták az IT-biztonsági területet. Inkább stagnálásról beszélhetünk, ami a fenyegetések számának és veszélyének ismeretében a terület hanyatlását jelenti. A végpontvédelem esetében kijelenthető, hogy a vírusvédelem elavult terminológia, önmagában hatástalan. Olyan megoldások tudnak hatékonyak lenni – beépített alkalmazás és portkontroll révén –, amelyek a végpont higiéniájának ellenőrzése mellett szabályozzák a hálózati erőforrásokhoz való hozzáférést is. A szakember segítségével összeállítottuk a jelen és jövő biztonsági kihívásait.



Gombás László
szakértő
Symantec magyarországi képvisele

Amitől leginkább fokozódik a védelem komplexitása:
– összetett fenyegetettségek, komplex, profi támadások
– a mobileszközök és a mobilinternet elterjedése
a privát és üzleti adatkezelés összemosódása.

Amire jobban kellene figyelni:
– végpontvédelem
– sérülékenységek és megfelelőségvizsgálatok
– adatszivárgások felderítése és megelőzése.

A jövő fenyegetettségei:
– adatszivárgás
– célzott támadások
– mobilkockázatok.

tosabb, hogy a korábban globálisan fertőző károkozók helyett napjainkban – sokkal nagyobb számban és változatosságban – olyan ártalmas kódok terjednek, amelyek egyes régiókban célzott módon okoznak problémákat. **Amíg például 1991-ben mintegy ezer vírusról számoltak be a kutatók, addig napjainkra már minták milliót tartják nyilván az antivírus eszközöket fejlesztő cégek.** További probléma, hogy a számítógépes kártevők sokat fejlődtek a rejtőzködés terén. Ugyanis napjainkban a legtöbb esetben nem az a céljuk, hogy a készítőiknek hírnevet szerezzenek, hanem hogy a terjesztőiket minél több pénzhez juttassák, többek között bizalmas adatok kiszivárogtatásával. Nem utolsósorban pedig a terjedési csatornák köre is kiszélesedett, hiszen napjainkban az e-mailektől kezdve a cserélhető adattárolókon és mobilkészülékeken át az internetig mindenhol jelen vannak a nemkívánatos kódok.

A vírusok fejlődése természetesen szükségessé tette a védelmi eszközök fejlesztését is. Jó ideig a szignatúraalapú technológiák segítségével viszonylag hatékonyan lehetett felvenni a küzdelmet, azonban napjainkban a hagyományos módszerek önmagukban már nem vezetnének eredményre. A heurisztika, a viselkedésalapú vizsgálatok, a hírnévalapú (reputációs) eljárások és egyre inkább a cloud computingra épülő védelmi lehetőségek kerülnek reflektorfénybe.

Növekvő kiadások

Az informatikai biztonság összetettsége maga után vonta a védelmi költségek növekedését is. A Harris Interactive által készített és a Novell által közzétett kutatás szerint a szervezetek jelentős része IT-költségvetésének több mint felét a biztonságra fordítja. Ennek ellenére a válaszadók 55 százaléka beismerte, hogy képtelen biztonságossá tenni virtualizált és felhőalapú munkakörnyezetét. Továbbá kevésbé bízik abban, hogy sikeresen felügyelheti az olyan fogyasztói eszközöket, mint például az okostelefonok és a tabletek.

KINYÍLÓ HATÁROK

A vállalatok, intézmények a víruskeresők telepítése mellett sokáig kizárólag a tűzfalak alkalmazását tartották szem előtt. Sajnos – főleg a kisebb méretű cégek körében – még napjainkban is sokszor e két eszköz igyekszik lépést tartani az időközben jócskán megszaporodó fenyegetésekkel, ami nyilvánvalóan nem eredményez hatékony védelmet.

Jó esetben a tűzfalakat UTM (Unified Threat Management) megoldások váltják fel, amelyek az átjárókon számos kockázati tényezőt képesek kezelni, és ezáltal hozzájárulnak a többszintű védelem kialakításához. Ezzel pedig el is érkeztünk a védelmi infrastruktúrák egyik legfontosabb jellemzőjéhez, a többrétegűséghez, ami gondos tervezést, implementálást és átfogó felügyeletet igényel. A kihívásokat azonban nemcsak ez fokozza, ugyanis amíg korábban a határvédelem egyik célkitűzése az volt, hogy a belső hálózatokat minél inkább sikerüljön szeparálni a külső környezettől, addig napjainkra – a távmunka, a mobil munkavégzés és a cégek közötti kommunikációs kapcsolatok miatt – **már az a fő kérdés, hogy a hálózatokat miként lehet a legbiztonságosabb módon „megnyitni" az arra jogosult felhasználók és a megbízható külső rendszerek felé.** A szóba jöhető védelmi lehetőségek (a VPN vagy az azt helyettesítő megoldások, a hálózati hozzáférés-szabályzást lehetővé tevő eszközök, a többfaktoros azonosítást támogató technológiák stb.) száma jelentős, és megfelelő kockázatértékelés, illetve tervezőmunka nélkül nem egyszerű kiválasztani az optimális megoldást.

ADATOK ÚTON-ÚTFÉLEN

Mobilizálódó világunk nemcsak a határvédelem kapcsán követel változtatásokat, hanem a biztonság számos más területén is. A megfelelő intézkedések nélkül használt hordozható eszközök, notebookok, táblagépek és okostelefonok komoly adatbiztonsági kockázatot jelentenek. A szervezetek határain kívül kezelt adatok felett ugyanis gyorsan el lehet veszíteni a kontrollt. A védelmet nehezíti, hogy az egyre népszerűbbé váló mobil operációs rendszerek (különösen az iOS és az Android) egyre inkább felkeltik a kiberbűnözők figyelmét, miközben sok mobilbiztonsági technológia még igencsak gyerekcipőben jár. Ezért kétség sem férhet hozzá, hogy a jövőben e téren jelentős fejlődés várható, amit a szervezetek biztonsági csapatainak követniük kell, legyen szó akár mobilokat érintő vírusvédelemről, titkosításról, azonosításról vagy biztonsági mentésről.

A mobilbiztonság sem hagyatkozhat csupán a technológiai védelemre. A szabályozás és a biztonságtudatosság növelése rendkívül fontos. Különösen azért, mert egyre gyakoribb, hogy az alkalmazottak a vállalati okostelefonjaikat, hordozható számítógépeiket magáncélra is használják, ami az adatvédelem szempontjából kezelendő kockázatokat hordoz. (A Trend Micro egyik felmérése szerint a munkavállalók 44,57 százaléka használja a telefonját üzleti és magáncélokra egyaránt.)

AZ INTERNET ÉS A WEB 2.0

A védelem összetettségének fokozásához nagyon jelentős mértékben járult hozzá az internet és a Web 2.0. A támadási felüle-

Egyre távolabb a korszerű védelemtől

Nemes Dániel, a biztributor ügyvezetője arra a kérdésünkre, hogy melyek azok a fenyegetettségek, kockázati tényezők, amelyek az elmúlt évek során a leginkább fokozták a védelemi feladatok komplexitását, úgy válaszolt, hogy a kívülről érkező támadások sokkal kifinomultabbak, célzottabbak lettek. Ráadásul ma már sokkal több adatbázis érhető el weben keresztül, ezért egyértelműen a webes alkalmazások váltak a külső támadások fő célpontjaivá. Ugyanakkor – részint a válság hatására – a belülről jövő támadások aránya nő, illetve a véletlen adatszivárogtatás is egyre gyakoribb. A védelmi eszközök mind komplexebbé válnak, sokkal inkább együttműködnek, így ezek összehangolása kiemelt feladattá vált.

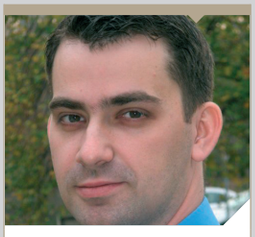
„Úgy látjuk, hogy a hálózati hozzáférések biztosítása nemcsak a WLAN-hálózatokat, hanem a vezetékeseket is mindinkább érinti. Ezenkívül a webes alkalmazások, webszerverek és adatbázisok biztonságára célszerű volna nagyobb hangsúlyt fektetni. Az adatszivárgás elleni (DLP) eszközök még mindig nem terjedtek el. Érdekes új terület a rendszergazdák kontrollja: jelszavaik menedzsmentje, illetve munkamenetük naplózása is" – vélekedett a szakember.

Nemes Dániel
ügyvezető
biztributor

Nemes Dániel a hazai biztonsági helyzet kapcsán elmondta: „Sajnos azt látjuk, hogy a 2000-es évek közepére jellemző örömteli felzárkózás megfordult, és – nyilván a válság hatására – egyre komolyabb lemaradást gyűjtünk össze. A már bevált megoldások (például tűzfalak, IPS-eszközök) modern verziókra történő frissítése elmarad, az újabban beszerzendő eszközöknél (WLAN, webszűrő stb.) a szakmai és biztonsági szempontok alulmaradnak az árakkal szemben. Ha pedig mégis csúcsminőségű eszközöket sikerül megvásárolni (például DLP-területen), akkor a bevezetésre nem szánnak elég pénzt és időt. Ezért egyre nehezebb igazán szép projekteket találni".

Lassú reakció

„Az utóbbi években egyértelműen a mobilitás az egyik legnagyobb kihívás. Pár éve még csak a hordozható gépek védelmét kellett megfelelően megoldani, napjainkban már az okostelefonok elterjedése jelent új kihívásokat" – nyilatkozta *Csósza László,* a Check Point Software magyarországi képviseletének rendszermérnöke.



Csósza László
rendszermérnök
Check Point Software

A szakember szerint szinte minden szervezetnél vannak már cloud alapú megoldások, legyen szó akár saját, akár szolgáltatásként igénybe vett felhőről. E megoldások bevezetésénél az egyszerűbb és hatékonyabb üzemeltetés, valamint a költséghatékonyság érdekében a biztonság gyakran háttérbe szorul. Amíg a hagyományos informatikai környezetekben a különböző funkciók szegmentálása, elkülönítése már bevett gyakorlat, addig a virtuális környezetekben ezek általában ömlesztve jelennek meg. Nagyobb hangsúlyt kellene fektetni a belső védelmi rendszerek kialakítására is, amelyek esetében a szervezetek sokszor teljesen megfeledkeznek például az adatszivárgás elleni védelemről, vagy az adathordozók és hordozható munkaállomások titkosításáról. De nem szabad figyelmen kívül hagyni a felhasználókat sem, hiszen ők jelentik az első védelmi vonalat. Csósza László sem túl optimista az informatikai biztonság magyarországi helyzetét tekintve, ugyanis a fenyegetettségekre való reagálás sok esetben kívánnivalót hagy maga után. A szakember szerint a technológiai vállalatok általában gyorsan cselekszenek, mivel számukra fontos, hogy mindent megtegyenek szervezetük védelme érdekében. Általánosságban mégis azt mondhatjuk, hogy a kockázati tényezők változására nagyon lassan vagy szinte egyáltalán nem reagálnak a szervezetek, mivel úgy gondolják, hogy egy adott fenyegetés Magyarországon talán nem jelentkezik. „Talánokra" azonban egy informatikai biztonsági rendszert nem lehet építeni! A leggyakoribb probléma, hogy sokan még mindig csak tűzfalakban gondolkodnak, és nem komplex védelmi megoldásokban.

tek és ezáltal a fenyegetettségek száma megsokszorozódott, ami ahhoz vezetett, hogy a biztonsági eszközök mind számosságukban, mind funkcionalitásukban gyarapodtak.

Napjainkban jelentős kockázatot jelentenek a spamek, amelyek már nemcsak hirdetési célokat szolgálnak, hanem gyakran segítik a kártékony programok terjesztését, illetve az adathalászatot is. Vállalati és intézményi környezetekben a célzott támadások *(lásd spear phishing)* elleni védekezés jelent különösen komoly kihívást. Ezek ugyanis kizárólag technológiai védelemmel nem kezelhetők hatékonyan, mivel e támadások sok esetben az emberi tényezőkből fakadó gyengeségekre apellálnak. Mindez azt is jelenti, hogy a spamek, a közösségépítők és a különféle webes szolgáltatások napjainkban már nemcsak a termelékenység rovására mehetnek, hanem nagyon komolyan veszélyeztetik az informatikai infrastruktúrákat is.

VIRTUALIZÁCIÓ ÉS CLOUD COMPUTING

A manapság nagyon divatos kifejezések sok esetben összefonódnak a költséghatékonysággal, legalábbis a marketinganyagokban biztosan. Azonban a használatuk kockázatokat is hordoz, amelyek csökkentése nélkülözhetetlen ahhoz, hogy a legkorszerűbb technológiák meg tudják mutatni, hogy valójában mire is képesek. A virtualizáció esetében gondoskodni kell például az egyes virtualizált rendszerek megfelelő szeparálásáról, a szegmentálásról, a hypervisor szintű védelemről és a rendelkezésre állás biztosításáról. A cloud computing kapcsán pedig az adatok megóvásának kell középpontba kerülnie. A publikus felhőalapú szolgáltatások esetében az adatok titkosított továbbítása és tárolása, a hozzáférések szabályozása, valamint a jogszabályok, illetve iparági előírások fokozott szem előtt tartása elengedhetetlen. A cloud computingra is igaz, hogy a védelmi megoldások gyakran még gyerekcipőben járnak, de jelentős fejlesztések folynak a biztonsági és a szolgáltató cégek berkein belül egyaránt.

BELSŐ FENYEGETETTSÉGEK

Eddig leginkább olyan kockázati tényezők kerültek szóba, amelyek külső fenyegetettségekre voltak visszavezethetők. Láthattuk, hogy ezek ellen sem egyszerű felvenni a kesztyűt, azonban van egy olyan terület, amely még erre is „rátesz egy lapáttal". Ez pedig nem más, mint a belső károkozások felismerése és megakadályozása. Legyen szó véletlenül vagy szándékosan elkövetett káros cselekményekről, a védelem elengedhetetlen, ugyanis a károk értéke hamar magasra szökhet. A 2011-es *CyberSecurity Watch Survey* című tanulmányból az derül ki, hogy ugyan a külső okokra visszavezethető incidensek aránya (58 százalék) még mindig meghaladja a belső támadásokét, ez utóbbiak viszont az esetek jelentős részében nagyobb összegű károkhoz vezetnek. Meg kell jegyezni azonban, hogy az egyes felmérések ebből a szempontból jelentős eltéréseket mutatnak, és arra is van példa, hogy a belső támadások kerülnek fölénybe. Egy azonban biztos: számolni kell a szervezeteken belüli károkozásokkal. A védelem szempontjából jelentős hangsúly helyeződik a hozzáférések, jogosultságok központi kezelésére, a naplózásra, az adatszivárgás megelőzésére (DLP) és a szabályozásra.

MEGFELELŐSÉG

A cikkünkben említett veszélyforrások elleni fellépés önmagában is nagy terhet ró a biztonsági szakértőkre, csapatokra. Azonban arról sem szabad megfeledkezni, hogy a compliance szerepe egyre inkább fokozódik, ami a szabályok kialakítására és azok betartatására ösztökél. Megfigyelhető, hogy sok esetben a szabványok, előírások szükséges rosszként jelennek meg a szervezeteken belül. Pedig ezek – amellett, hogy nem kevés munkát adnak, és adott esetben sok erőforrást kötnek le – segítséget nyújtanak a védelem teljesebb körű kialakításához, valamint annak fenntartásához, fejlesztéséhez.

ITT A VÉGE...? SAJNOS NEM

Amikor 1993-ban megrendezték az első DEF CON hackerkonferenciát, még viszonylag kevés téma volt terítéken. Noha e cikk keretei korántsem tették lehetővé, hogy az összes releváns kockázati tényezőre kitérjünk, és azokat részletesen elemezzük, mégis számos olyan terület került szóba, amelyek figyelembevételével nem csoda, hogy a biztonsági rendezvények napjainkban már többnaposak, és jelentős figyelem övezi azokat. Ez is jól mutatja, hogy a védelem komplexitása olyan szintet ért el, amelynek kezelése izzasztó munkát követel meg. Sajnos a jelenlegi ismereteink szerint a kedvezőtlen tendenciák megfordulására egyelőre nincs remény, sőt!

A mobilitás árnyoldalai

A Carnagie Mellon Egyetem idei kutatása szerint a legnagyobb biztonsági kockázatot az ellopott és elvesztett mobileszközök jelentik. A vállalatok 40 százalékánál okozott már károkat, hogy a rossz kezekbe került mobilok érzékeny vállalati adatokat is tartalmaztak, és az elkallódott eszközök egyharmada járult hozzá pénzügyi veszteségekhez. A szervezetek kétharmada javított biztonsági rendszerén az ilyen jellegű incidensek után.

Biztonság a felhőben

A felhőszolgáltatásokkal kapcsolatban a felhasználók részéről felmerülő legfontosabb kérdések a biztonságra és a rendelkezésre állásra vonatkoznak. A vállalatok tudni szeretnék, mi a biztosíték arra, hogy adataik nem kerülnek illetéktelen kezekbe, ők maguk viszont mindenkor megbízható módon elérhetik azokat. Írta: Kis Endre

A piaci szereplőktől gyakran halljuk, hogy egy felhőszolgáltatásokat kínáló adatközpont sokkal biztonságosabb és magasabb szolgáltatási szinteket tarthat fenn, mint egy vállalaton belüli szerverterem, annál az egyszerű oknál fogva, hogy sokkal több ügyfelet szolgál ki, ezért üzemeltetője többet költhet a szükséges technológiákra. Négy szolgáltatót kérdeztünk ennek részleteiről, valamint a felhő biztonságával kapcsolatos jogos és megalapozatlan felhasználói várakozásokról.

Az adatbiztonság sérülését okozó események több mint felét vállalaton belüli felhasználó idézi elő akár szándékosan, akár hibázásból, felelőtlenségből, a vállalati biztonsági előírások megsértéséből adódóan. Az is gyakori, hogy a heterogén, olykor részben elavult infrastruktúra áttekinthetetlensége miatt kiskapuk maradnak a biztonsági rendszeren, olyan szolgáltatások, amelyek megkönnyítik a behatolást és adatszivárgáshoz vezetnek.

– **A nyilvános felhőben elérhető szolgáltatások esetében a felhasználó biztonsági adminisztrátori lehetőségei korlátozottabbak, a biztonsági előírások áthághatatlanok, mivel betartásukat a szolgáltató kikényszeríti** – mondta *Sepp Norbert*, az IBM Magyarország hardvertechnikai szakértője. – Ebben a tekintetben a felhőszolgáltatások magasabb biztonsági szintet adnak, mint a vállalaton belüli infrastruktúra. Az adatokhoz való hozzáférést, az egyes alrendszerek elszigetelését illetően az igényelt szolgáltatási szint és a tervezett munkatípusok határozzák meg az izoláció fokát. Egy nyilvános adatokat tartalmazó webkiszolgálónál a szigor enyhébb lehet, míg egy bérszámfejtő alkalmazás esetében sokkal komolyabb szint kérhető.

A nyilvános felhőben a legtöbb szolgáltatás szabványos, jelentős testre szabásra (beleértve a biztonsági beállításokat is) csak felár ellenében nyílik lehetőség, ha a szolgáltató ezt kínálja egyáltalán. Ha ez nem felel meg az igényeknek, a vállalati hálózat logikai határán belül kialakított, privát felhő jelenthet megoldást.

A szakértő arra is felhívta a figyelmet, hogy a felhőszolgáltatók adatközpontjai méretgazdaságosságukon túl sok felhasználós cloud infrastruktúrájuk folytán technikai előnyöket is kínálnak. Amíg a virtualizáció szokásos felhasználásban egy fizikai gépen belül alakít ki különböző virtuális szervereket, addig felhő környezetben a virtuális gépek, az erőforrások a munkafolyamatok megszakítása nélkül a fizikai rendszerek között. Így magasabb rendelkezésre állással, kevesebb szolgáltatáskieséssel, versenyképes áron kínált, magas szolgáltatási szintekkel (SLA-kkal) lehet számolni.

– Általános tévhit, hogy a felhőszolgáltatásokra való átállás könnyű és zökkenőmentes – fogalmazott Sepp Norbert. – **Amíg egyes munkafolyamatoknál valóban könnyű a váltás, bizonyos alkalmazások vagy üzleti igények esetében ugyancsak alapos tervezésre és gondos kivitelezésre van szükség.** Sok múlik azon, hogy az egyes gyártók milyen támogatást adnak termékeikhez felhő környezetben. Az IBM-nél külön üzleti részleg foglalkozik a tanácsadási, elemzési, előkészítési, implementálási és oktatási feladatokkal, szakembereink segítségével akár „dobozolt", akár teljesen egyedi kialakítású felhő is rövid idő alatt birtokba vehető.

BIZALMI KÖZPONT

A Microsoft adatközpontjaiban a biztonság egyik fontos tényezője az Online Risk Management Program, amely a biztonsággal, az adatvédelemmel, a szolgáltatásfolytonossággal és a törvényi megfeleléssel kapcsolatos szabályozásokat tartalmazza. A keretrendszerbe foglalt bevált gyakorlatot a szoftvercég 1994 óta, első online szolgáltatásának elindításától kezdve folyamatosan fejleszti és finomítja. Ma a Microsoft Online Risk Management Program az ISO 27001 szabvány szerint tanúsított környezetet képvisel. A szoftvercég emellett részt vesz a cloudsecurityalliance.org nonprofit szakmai szervezet munkájában annak érdekében, hogy felhőszolgáltatásainak értékelését többek között előre kidolgozott feltételrendszer-sablonokkal is megkönnyítse a felhasználók számára.

A Microsoft olyan szoftvertechnológiákat fejleszt, amelyek fontos szerephez jutnak a felhőszolgáltatásokat kínáló adatközpontok kialakításában, üzemeltetésében és különböző fenyegetésekkel szembeni védelmében. A szoftvercég Trustworthy Computing kezdeményezése értelmében a fejlesztők képzésétől kezdve a termékek specifikálásán át a kód teszteléséig és a termékkibocsátásig a biztonság a folyamat szerves része.

– Gyártóként az adatközpont-tervezéstől a felhasználói adatok védelméig a szolgáltatások teljes palettájával rendelkezünk – mondta *Rideg Márton*, a Microsoft Magyarország megoldásértékesítési vezetője. – Ennek megfelelően mind a fizikai, mind a logikai védelem területén egy ún. Defense in Depth mélységvédelmi megközelítést alkalmazunk, amely a létesítmény külső védelmétől kezdve a belső, szervezeti működés szabályozásán át a hálózatvédelemig részletes követelményrendszert határoz meg. Ilyen például a kétfaktoros védelem a belső hálózaton vagy a host gépeken alkalmazott hozzáférés-szabályozási, monitoring, behatolásvédelmi és konfigurációkezelési gyakorlat, amelyet egyébként is ajánlunk ügyfeleinknek.

A Microsoft felhőszolgáltatásairól – a biztonság és az adatvédelem területét is beleértve – a lehető legtöbb információt nyilvánosan is hozzáférhetővé teszi Trust Centerén keresztül. Ennél részletesebb tájékoztatást, például az adatközpontról készült audit jelentéshez való hozzáférést a szerződött ügyfelek, illetve titoktartási szerződést aláíró felhasználók kapnak.

– Windows Azure felhőplatformunk, Windows Server Hyper-V virtualizációs és System Center felügyeleti megoldásunk alkalmazásával biztonságosan, egyúttal költséghatékonyan üzemeltetjük felhőszolgáltatásokat kínáló adatközpontjainkat – folytatta Rideg Márton. – Ezt példázza a termékszinten kezelt multi-tenant környezet és adatizolálás: az Exchange egyszerre sok vállalat levelezését is képes elkülönített módon, megbízhatóan és biztonságosan kiszolgálni, így nem kell külön szervereket üzembe állítani. Termékeinket energiahatékonyságra optimalizáljuk, ügyfeleink számára ezzel is gazdaságosabbá tesszük a kívánt szolgáltatási szint fenntartását, az Exchange például olcsóbb tárolórendszerekkel is megbízhatóan működik.

A Microsoft felhőszolgáltatásai konfigurálhatók, de nem teljes mértékben testre szabhatók. A szolgáltatási szinteket a szolgáltatási szerződések pontosan definiálják, beleértve a kiesés percei után járó kompenzációt is. Ez azt jelenti, hogy a Microsoft pénzügyi felelősséget vállal arra az esetre, ha a meghatározott SLA-t nem tartaná be.

– **A felhőszolgáltatások kapcsán a felhasználók olykor azt is feltételezik, hogy a törvényi megfelelést a szolgáltató fogja tanúsítani helyettük** – hívta fel a figyelmet Rideg Márton. – Ez nincs így, viszont minden információt meg tudunk adni számukra, hogy ezt maguk megtehessék. Emellett felhasználói oldalon továbbra is biztosítani kell azt a szabályozást, amellyel például megakadályozható, hogy a felhőben levő postaládát használó alkalmazott illetéktelenek ne adhassa ki a vállalat bizalmas információit.

HITELES SZOLGÁLTATÓ

A HP Cloud Services szolgáltatásai jelenleg béta-változatban érhetők el, de az éles üzem indítása is várható a közeljövőben. A vállalatoknak kínált felhőalapú szolgáltatások védelmét az a biztonsági megoldásportfólió hivatott garantálni, amelyet a HP a múlt év folyamán felvásárolt technológiák integrálásával most bővített ki. A HP Enterprise Security Solutions olyan biztonsági eszköz- és szolgáltatáscsomag, amellyel nagyvállalati ügyfelei számára a HP is átfogó biztonsági stratégiát dolgozott ki és ültetett át a gyakorlatba.

– A HP Enterprise Security Solutions a felvásárolt ArcSight, TippingPoint és Fortify technológiák mellett saját fejlesztéseinket és tanácsadói kompetenciáinkat is felvonultatja, amelyek birtokában hiteles felhőszolgáltatóként tudunk piacra lépni – mondta *Nagy Tibor*, a HP Magyarország IT-biztonsági tanácsadója, a HP felhőbiztonsági referense. – A felhőszolgáltatásokat multi-tenant környezetben használó vállalatok adatainak izolálásához, az adatközpont üzemeltetői szerepköreinek szétválasztásához, a törvényi megfelelőség feltételeinek megteremtéséhez és az auditálás támogatásához ugyanis önmagában kevés egy fejlett IPS (Intrusion Prevention System), ISM (Information Security Management) vagy SIEM (Security Information and Event Management) megoldás, ehhez kiforrott módszertan, magas szintű, holisztikus megközelítés alkalmazása is szükséges. Kevés piaci szereplő kínálhatja mindezt saját portfóliójában, és a HP ebbe a szűk körbe tartozik.

A HP abban a tekintetben is speciális piaci pozíciót tudhat magáénak, hogy a felhőszolgáltatásokat biztosító adatközpontok építéséhez és üzemeltetéséhez szükséges hardver és szoftvereszközök, szolgáltatások jelentős része saját termékkínálatában megtalálható. Üzemeltetési, szolgáltatásmenedzsment szakértelmét és biztonságiszolgáltatás-portfólióját a HP két évvel ezelőtt a világ legnagyobb outsourcing cége, az EDS felvásárlásával bővítette tovább. Ezek a komplex ismeretek teszik lehetővé, hogy a HP a felhőszolgáltatási stratégia kiválasztásában és annak megvalósításában segíteni tudja a vállalatokat.

– A felhőszolgáltatásokkal kapcsolatban felhasználói oldalon kialakulhat az a tévhit, hogy a szerződés aláírásával a vállalat a biztonság és az üzemeltetés teljes problémakörét átrakja a szolgáltató vállára, átlép egy olyan világba, amelyben nincsenek többé kockázatok és biztonsági események – mutatott rá Nagy Tibor. – Ez túlzott elvárás. **A felhőszolgáltatók potenciálisan képesek arra, hogy egyes fenyegetéseket hatékonyabban kezeljenek, mint az ügyfelek önállóan. Ezzel bizonyos kockázatok csökkenni fognak felhasználói oldalon, de a felhőszolgáltatásra való áttérés új kockázatok forrásaivá is válik. Ez a kockázati profil vállalatonként más; pontos feltérképezése, a továbbra is felhasználói oldalon maradó feladatok megértése elengedhetetlen ahhoz, hogy a felhőszolgáltatások használata valóban biztonságos legyen.**

A FELHASZNÁLÓHOZ KÖZEL

A CE On-Demand Ausztriától Törökországig 11 országban kínál felhőszolgáltatásokat, felhasználóinak száma meghaladja az 1 milliót. Szolgáltatásait többszintű biztonsági rendszer védi, melyet az ISO 27001 szabvány szerinti ISMS (Information Security Management System) rendszer fog össze. Ez az egymást tartalékoló, egymástól minden téren független kialakítású adatközpontok létesítményvédelmétől kezdve a redundáns infrastruktúrán és a duplikált szolgáltatásfelügyeleti rendszereken át a folyamatosan rendelkezésre álló üzemeltető csapatig és ellenőrzött üzemeltetési folyamatokig a biztonság és a rendelkezésre állás minden területére kiterjed.

– Az adatizolálás több szintjét is kínáljuk adatközpontjainkban – mondta *Tüdős András*, a CE On-Demand műszaki igazgatója. – A legköltséghatékonyabb megoldás a megosztott publikus felhőalapú szolgáltatás, amelyben úgynevezett multi-tenant képességek, azaz a szolgáltatáshoz használt szoftverek szintjén kialakított logikai izoláció biztosítja minden ügyfél adatainak, címlistájának, adminisztrációs felületének szeparálását. A következő szintet a privát felhő képviseli. Itt az ügyfél egyedi igényei szerint kialakított szerver-, illetve szolgáltatásfarmot biztosítunk, mely egyedi fejlesztések, nem multitenant-képes szolgáltatások futtatására vagy egyedi rendszerintegrációra is alkalmas. Ez általában saját adatközpontjainkban történik, de az ügyfél adatközpontjában is vállaljuk a költséghatékony, távolról menedzselt szolgáltatás kialakítását. Ebben az esetben fizikai szeparáció és dedikáció ad védelmet.

További lehetőségként a CE On-Demand – elsősorban szolgáltató vállalatok számára – egyedi felhő platformot is kialakít, amellyel a cégek saját ügyfélkörüket, egy adott régiót vagy zárt felhasználói csoportot szolgálhatnak ki költséghatékony módon, speciális szaktudás és hosszas fejlesztések nélkül.

– A felhőalapú informatikai szolgáltatások szinte minden esetben szigorúbb biztonsági szabályok szerint üzemelnek, mint amit egy átlagos vállalkozás képes megvalósítani a saját hatáskörében, és mentesek a legkritikusabb emberi kockázati tényezőktől is – tette hozzá Tüdős András. – Ennek előfeltétele, hogy a szolgáltató partner megfelelő kompetenciákkal és minősítéssel rendelkezzen. **Tévhit azonban, hogy minél nagyobb egy szolgáltató, szolgáltatásai annál biztonságosabbak. Amíg a globális szolgáltatók egyes problémái kezelhetetlen mértékű kieséseket okozhatnak, addig a helyi vagy regionális szolgáltatók a legtöbb esetben felkészültebben, az adott ügyfélre több figyelmet fordítva, helyben adott támogatással működnek, ami nagyobb biztonságot ígér a felhőszolgáltatások felhasználóinak.**

IDC Analyze the Future elemzés

Piaci átlagon felül teljesít a BI

Mind több hazai középvállalati cégvezető ismeri fel az üzleti intelligencia értékét. Különösen a gazdasági válság első hulláma után, az újabb recessziótól tartva látják be, milyen hasznos lenne, ha nehéz időkben az adatokat nem különböző lekérdezésekből kellene összevadászniuk, hanem rendelkezésükre állna egy olyan döntéstámogató eszköz, amely strukturált módon tárja eléjük az összefüggéseket. Írta: Kis Endre

A BI-alkalmazások – az International Data Corporation (IDC) terminológiájával *üzleti elemző szoftverek* – szegmense Magyarországon is együtt mozog a szoftverpiac egészével, amelytől ugyanakkor néhány lényeges ponton eltérést is mutat. A legfrissebb trendekről és piaci adatokról a cég magyar leányvállalata az IDC Üzleti Intelligencia Konferenciáján adott áttekintést.

– **A hazai cégek többsége, elsősorban a kis- és középvállalati szegmensben még egyáltalán nem használ BI-rendszert** – mondta lapunknak *Fauszt Gábor*, az IDC Hungary vezető elemzője. – A nagyvállalati felhasználók többsége külföldi cégek leányvállalatai közül került ki, amelyek nem helyi stratégiai döntés nyomán, hanem globális kezdeményezés részeként vezettek be üzletiintelligencia-alkalmazást. Ezen BI-rendszerek finomhangolása még nem ért véget, ami érthető is, mivel az üzleti környezettel együtt a döntéstámogatással kapcsolatos igények is folyamatosan változnak. Mindez azt jelenti, hogy a magyar piac a további növekedés tág terét kínálja a BI-megoldások szállítóinak.

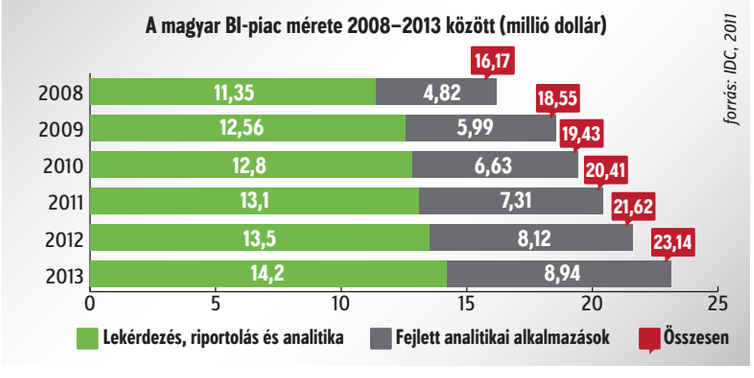
OPERATÍV ÉS STRATÉGIAI DÖNTÉSEK

Az IDC adatai szerint dollárban számolva az üzleti elemző szoftverek piaca 2010-ben 4,7 százalékkal nőtt Magyarországon az azt megelőző évhez képest – ami a teljes szoftverpiac 1 százalékos éves növekedésének közel háromszorosa. A piacelemző arra számít, hogy a 2013-ig tartó időszakban a növekedés üteme töretlen lesz *(lásd az ábrát)*, és a BI szoftverek hazai piaca idén 5, két év múlva pedig már 7 százalékkal bővülhet.

– A növekedés hajtóerejét elsősorban az adja majd, hogy a középvállalatoknál is beindulnak az üzleti intelligenciával kapcsolatos projektek – világított rá Fauszt Gábor. – Ezek a rendszerek nem nagy, *stand-alone* BI-megoldások lesznek, a kkv-szektorban az üzleti-intelligencia-szoftverek a vállalatirányítási rendszer részeként jelennek meg. Az ERP-piacon már jelenleg is a BI a legkeresettebb kiegészítő modul, dollárban számolva a bevezetett modulok több mint 20 százaléka ilyen. Ez arra vezethető vissza, hogy a klasszikus, például pénzügyi vagy logisztikai ERP-modulokat nem szükséges évente továbbfejleszteni, bővíteni. Másrészt mind több hazai középvállalati cégvezető ismeri fel az üzleti intelligencia értékét. Különösen a 2008-tól kibontakozó gazdasági válság első hulláma után, az újabb recessziótól tartva látják be, milyen hasznos lenne, ha nehéz időkben az adatokat nem különböző lekérdezésekből kellene összevadászniuk, hanem rendelkezésükre állna egy olyan döntéstámogató eszköz, amely rendszerben, strukturált módon tárja eléjük az adatokat és az összefüggéseket.

A piacelemző kiemelte, hogy a magyar kkv-k elsősorban rövid távú üzleti célok elérésére, és nem stratégiai döntések előkészítésére használják BI-rendszerüket. A kiszámíthatatlan üzleti környezetben ezek a cégek ugyanis képtelenek hosszabb távon tervezni, csak sodródnak a gazdaság és a törvényi, adóügyi szabályozás viharos vizein. Jellemző igény például az ügyfélmegtartás, a kinnlevőség-kezelés javítása. Amikor 1 százalékos gazdasági növekedés elé nézünk, minden meglévő ügyfél felértékelődik, ami lemérhető azon is, hogy milyen gyakori a BI és a CRM összekapcsolása azon vállalatoknál, amelyek üzletiintelligencia-projektet indítottak.

– A nagyvállalati szegmensben már Magyarországon is nyomon követhető az operatív és az analitikai BI-rendszerek különválása – folytatta az elemző. – Ebben a környezetben a döntéshozatali skálán megkülönböztetjük a napi munka részeként hozott, viszonylag alacsony kockázatot hordozó és a nagy horderejű, hosszabb távra szóló, stratégiai döntéseket. Egy középvezető naponta több tíz vagy száz operatív jellegű döntést is hozhat, így gyorsan kialakul az a bevált gyakorlat, amelynek alapján egy operatív BI-rendszerben ez a folyamat automatizálható. Ez jelentős hatékonyságnövekedést eredményez, lerövidíti a vállalat reakcióidejét, ugyanakkor több időt hagy az összetettebb, fontosabb kérdések eldöntésére. Az ilyen stratégiai jelentőségű döntéseket általában nem egyének, hanem vezetői csoportok hozzák meg, ezért az előkészítésüket segítő BI-megoldásokat fejlett együttműködés-támogató és analitikai, illetve szimulációs képességek jellemzik, amelyekkel előre jelezhetők a tervezett döntés várható hatásai is.



INTELLIGENCIA A FELHŐBEN

Az IDC a vállalatirányítási rendszerek kiegészítéseként bevezetett BI-rendszerek piacát méri, amelyet Magyarországon négy gyártó – IBM, Oracle, SAS és SAP – ural, összesen 80 százalék körüli arányban.

– **Általános érvényű trend, hogy a BI-rendszerek és a vállalat más üzleti alkalmazásai közötti integráció mind szorosabbá válik – mutatott rá Fauszt Gábor. – Az Oracle és az SAP mindinkább elmélyíti ezt a kapcsolatot ERP-, CRM- és BI-rendszerei között.** Ez idővel oda vezet, hogy valamely más gyártó BI-rendszerének bevezetése Oracle- vagy SAP-környezetben, bár technológiailag lehetséges, olyan többletráfordítással jár majd, hogy a felhasználók inkább lemondanak róla.

A fejlődés másik irányaként a BI-rendszer néhány év távlatában az adatbázis-kezelő részévé válhat. Ezek a megoldások a ma is elérhető adatbázis-gépek, például az Oracle Exadata következő nemzedékeként jelenhetnek meg a piacon, és az olyan technológiák által, mint amilyen az SAP HANA memóriában futó adatbázisa is, még nagyobb BI-teljesítményt fognak adni a felhasználóknak.

– A következő két évben arra is számíthatunk, hogy a BI-megoldások felhőben elérhető szolgáltatásként is megjelennek a hazai piacon – tette hozzá a piacelemző. – A felhőalapú CRM- és ERP-szolgáltatások eddigi térhódításának üteme alapján valószínűsíthető, hogy az első BI-szolgáltatások a jövő év második felében jelennek meg a nagy szolgáltatók kínálatában, és azokat 2013-ban kezdik majd használni az ügyfelek. Ez mind szállítói, mind felhasználói oldalon demokratizálhatja az üzleti intelligencia területét, mivel a felhőben a kisebb piaci szereplők is megfelelő BI-megoldást adhatnak a kis- és középvállalatok széles körének.

Nagyok nagy bukásai

Elhibázott termékkoncepciók, rossz időzítés, túlzásba vitt forradalmiság vagy éppen a felhasználók életét megkeserítő hibákkal tűzdelt korán kiadott verziók... A Google és a Microsoft kiadásában. Írta: Molnár József

Bár a mamutvállalatok esetében a kis bukások is óriási összegek elfecsérlését jelentik, az sem ritka, hogy nemcsak presztízsben, de a konkrét költségek szintjén is hatalmasat buknak egy-egy kiemelt projekten. Ha górcső alá vesszük legnagyobb bakijaikat, úgy tűnik, mintha hajlamosak lennének ismételni önmagukat. De talán ez a következetesség vezeti őket a sikerre is?

A MICROSOFT BAKLÖVÉSEI

Kin. Vélhetően hatalmas kínokat kellett átélnie annak a Microsoft-sajtósnak, aki a Kin telefonok megszűnéséről szóló közleményt írta. A többéves fejlesztéssel és becslések szerint 1 milliárd dollár költséggel életre keltett eszközök kapcsán a cégnek ugyanis talán az IT-történelem legcsúfosabb bukását kellett elkönyvelnie: 6 hét alatt mindössze 500 darabot adtak el belőlük, amely eladási adatokat látva a Microsoft rögtön visszavonta a piacról a tiniknek szánt mobiljait. Ugyanis bár olcsón adták, mégis drága előfizetéssel kínálták őket. Mindent összevetve szinte még a kutyának sem kellett a Kin, amely a fejlesztőivel együtt csúfosan megbukott.

Vista. Ma már az IT-szlengben a Vista neve egyet jelent a bukással. Habár a platform a Kinnél egy fokkal szerencsésebben járt, mégis alaposan megtépázta a Windowsok hírnevét. E ballépést csak a Windows 7 tudta kiküszöbölni, amely valójában az, aminek a Vistának kellett volna lennie. A gond nem az innovációval volt, hanem azzal, hogy a Microsoft nem követni, hanem vezényelni akarta az IT-ökoszisztémát. Ráadásul sietve dobták piacra a terméket, amelynek inkompatibilitási problémáin az SP1 érkezéséig még a Microsoft vezetői is élcelődtek. A rossz sajtó miatt az emberek nem váltottak a platformra, maradtak inkább a jó öreg, megbízható XP-nél.

Zune. A Zune HD megjelenésekor a szakmai sajtó ódákat zengett a zenelejátszóról. A kütyü életpályája mégsem nevezhető diadalmasnak, a felhasználók ugyanis nem haraptak rá az eszközre. Jellemző módon anno nekünk is hajtóvadászatot kellett indítanunk, hogy szerezzünk egyet, majd összehasonlítsuk azt a sikeres iPod Touch-csal; a készülék marketingesei ugyanis teljes egészében az Egyesült Államokra fókuszáltak. Emellett amíg az iPod mögött az App Store áll, addig a Zune-nál szegényes az alkalmazásellátottság. Utóbbi egyébként magasabb áron került forgalomba, mint fejlettebb vetélytársa, ami egyértelműen rossz döntés volt.

MS-DOS 4. A Vistához hasonlóan az MS-DOS negyedik kiadása is megelőzte a korát, amikor a párhuzamos feldolgozást akarta bevezetni a DOS világába. Nem sikerült! Sőt a próbálkozás sok apró hibával járt, ami miatt a felhasználók menekültek a 4-es kiadástól; vagy az MS-DOS 3.3-as verzióját használták a továbbiakban is, vagy áttértek a DR-DOS 3.41-re.

Bob. Nemes volt az 1995-ben kiadott program célja: megkönnyíteni Windows 3.1 és Windows 95 alatt a laikusok munkáját. A szoftver mégis leszerepelt. Egyrészt túl nagy volt az erőforrásigénye, másrészt túlságosan barátira sikeredett, s a felhasználóknak már az a gondolatuk támadhatott, hogy idiótáknak képzelik őket.

AMIKOR A GOOGLE LÖVI A BAKOT

Wave. A Google Wave bejelentésekor a keresőcég szakértői nem bántak csínján a nagy szavakkal. Egyenesen az e-mail hegemóniájának megtörését remélték az eszközüktől, egyúttal megteremtve a webes kommunikáció új sztenderdjét. Sőt néhányan még azt is megkockáztatták, hogy a Wave komolyan megszorongathatja a Facebookot is. Nem így lett, és egy év után nem sokkal a Google bejelentette, hogy megszünteti egységes kommunikációs eszközét, mivel az „nem érte el azt a használati rátát, amit vártak tőle". Talán túl forradalmira sikeredett, a felhasználók nem ugrottak rá, és így érdeklődés hiányában lassan megszűnt.

Buzz. A Google Buzz indulásakor sokan úgy gondolták, hogy a Gmail levelezőrendszerbe integrált közösségi szolgáltatás alaposan odacsaphat a Facebooknak. Telt az idő, és *Mark Zuckerberg* közösségi oldala hónapról hónapra erősebb lett, míg a Buzz – magyarul Zümm – a teljes érdektelenség felé haladt. Az emberek nem haraptak rá, nem töltötték meg friss információkkal, s így szépen lassan elhagyták a felhasználók. Ráadásul a Google számára jelentős költségeket emésztett fel a Buzz, hiszen az indulása után felmerülő adatvédelmi aggályok miatt a keresőcég 8,5 millió dollárt fizetett egy civil szervezetnek, hogy elsimítsák az ügyet.

Google Video. A Google saját videomegosztója 2005-ben indult, nem sokkal a YouTube rajtja után. A bevált recept alapján meg akarták szorongatni, majd meg szerették volna előzni az egy évvel korábban indult megoldást. Nem sikerült, hiszen a két fiatal egyetemista által alapított szolgáltatást már nem lehetett utolérni, így a Google egy másik fegyverhez nyúlt: a felvásárláshoz. 1,86 milliárd dollárért bekebelezték a YouTube-ot, amelynek előtérbe helyezésével befellegzett a Google Videónak. Ráadásul az sem biztos, hogy jó vásárt csináltak, hiszen a mai napig nem találták meg a módját, miként lehetne nyereségessé tenni a YouTube-ot.

Orkut. Nehéz lenne a 2004-ben indult közösségi oldalt a Google sikeres projektjei közé sorolni. Hazánkban észrevétlen a piaci súlya, hasonlóan a többi európai országéhoz, sőt az Egyesült Államokban is nagyítóval kell keresni a felhasználóit. Egyedül Brazíliában és Indiában erős a fapados felületű szolgáltatás.

Jaiku. A Google 2009-ben vásárolta fel a finn mikroblog-szolgáltatást, sokakat meglepve ezzel. A Twitter riválisának kódját nyílttá tették, hogy így állítsanak erős konkurenciát. A megoldás mégis a felejtés útjára lépett, hiszen nem tudott konkurálni fő vetélytársával, így a fejlesztése 2009-ben megállt.

Kérdéses: Windows Phone 7

„Egyelőre bukás a Windows Phone 7" – ismerte el *Steve Ballmer* egy nyilvános rendezvényen. Nehéz titkolni az operációs rendszer sikertelenségét, mivel a ComScore adatai szerint a platform érkezése óta 38 százalékkal csökkent a Microsoft részesedése az amerikai okostelefonok piacán. Persze minden kezdet nehéz, így talán a Mango és WP7-es Nokiák érkezése növekvő pályára állítja majd a platformot.

Kérdéses: Google+

Nehéz ítéletet mondani a Google+ felett, hiszen fiatal szolgáltatásról van szó. A Google eddigi közösségi próbálkozásai miatt mégis bizalmatlanok vagyunk, hiszen a megoldás eddig látszólag a Buzz és a Wave életpályáját járja be. Először lelkesednek érte, majd érdektelenné válik a szolgáltatás – ez a Google+-ra is igaz, ahol egyelőre csak a barátkozás folyik, az adatok és információk megosztása viszont ritka.

Behálózott kamerák

A korszerű megfigyelőrendszerek kamerái ugyanúgy kapcsolódnak a hálózatra, mint a számítógépek. A rendszerek egyre intelligensebbek, a videókat különböző szempontok szerint képesek elemezni. Írta: Mallász Judit

Napjaink korszerű videomegfigyelő rendszerei hálózati, azaz IP-kamerákra épülnek. E digitális kamerák felbontása általában 1-től 5 megapixelig terjed, de a piacon már megjelentek a 10 megapixeles változatok is. Az IP-technológiának köszönhetően ezek a kamerák ugyanúgy köthetők a hálózatra, mint bármely más informatikai eszköz, az alkalmazott gyakorlat tehát igen széles körben ismert.

A hálózat másik oldalán található adatrögzítő szerverek manapság már nem egyedi gyártásúak, hanem főként PC-alapúak; általában Linux vagy Windows operációs rendszer alatt működnek. **A legújabb videokódolási technológia, a Blu-ray lemezek előállításánál is használt H.264 az utóbbi időben a kameráknál is megjelent. Ez a kódolási eljárás körülbelül 5-10-szer nagyobb tömörítést eredményez, mint a régebbi technológiák (például az MJPEG vagy az MPEG4).** Ennek nyomán a kamera közvetítésével a hálózaton átvitt adatok mennyisége, illetve az adatrögzítő szerverek tárhelyigénye drasztikusan lecsökkent.

A modern IP-kamerák – maximális felbontásuk mellett – támogatják a HDTV szabványokat, azaz 720p/30fps, 1080p/30fps videoátvitelre is képesek. A kamerákról egy időben többféle felbontású, kódolású és képsebességű videofolyamokat kérhetünk le (multistreaming). A hálózati videorendszerek egyszerűen bővíthetők, akár kameránként is. Mivel a rögzítő szerverek gyakorlatilag szokásos számítógépek, könnyen karbantarthatók, meghibásodás esetén gyorsan cserélhetők.

RÉGI ANALÓGBÓL KORSZERŰ DIGITÁLIS

Mivel az IP-alapú rendszerek csak az utóbbi években nyertek teret, jócskán találhatók még a piacon régebbi, más technológiájú megoldások. A legrégebbi és a mai rendszerek közti legfőbb különbség, hogy az előbbiek analóg rendszerek voltak. A kamerák a régi tévészabványnak megfelelő, tehát PAL vagy NTSC rendszerben működtek, és természetesen analóg berendezések rögzítették a felvételeket. A fejlődés következő lépcsőfokán az analóg rögzítést digitális eljárással váltották fel; megjelentek az úgynevezett DVR-ek (Digital Video Recorder), amelyek a kamerák analóg jeleit először digitalizálták, majd digitális formában tárolták. A 4-5 évvel ezelőtt elterjedt rendszerek még ilyen felépítésben működtek. A kamerákból kijövő analóg jel koaxiális kábelen jutott el a DVR-be, ahol megtörtént a digitalizálás és a tárolás. Ebben az architektúrában a szűk keresztmetszetet, illetve a minőség gátját az analóg kamera jelentette, amelynek felbontása legfeljebb a PAL/NTSC szabványok megfelelő 576/480 váltottsoros volt. Szóba se jöhettek tehát megapixeles eszközök. Miután az analóg jeleket nagyon nehéz minőségromlás nélkül nagy távolságra eljuttatni, a fejlődés következő szakaszában (úgy 3 éve) az analóg kamera után beillesztettek egy videoszervert. Ez az eszköz a kamera analóg jelét digitalizálta, majd egy informatikai hálózaton továbbküldte.

„A videoszerverekkel modernizálni lehet a régi, analóg kamerarendszereket. Az átalakított konfiguráció ugyanúgy működik, mint a korszerű, hálózati megoldások, egyetlen különbséggel: a kamerák 576/480 soros maximális felbontását nem lehet megnövelni" – mutatott rá *Czuprik Zoltán*, a CNS Digitál Média Kft. ügyvezető igazgatója.

NAGY TEREKRE LEGALÁBB 1-3 MEGAPIXEL

Minél nagyobb felbontású egy kamera, annál részletesebb képet ad. Ebből következően a nagyobb felbontású kamerával sokkal nagyobb területet lehet megfigyelni ugyanabból a távolságból, mint egy kisebb felbontásúval. Egy 5 megapixel (2560×1920 pixel) felbontású digitális kamera például 16 (vagy esetleg még több) analóg kamerát tud helyettesíteni, azaz ugyanakkora területet lát be, mint 16 analóg kamera (feltételezve, hogy a kétfajta eszközt ugyanolyan optikával szerelték fel).

Természetesen mindig az adott alkalmazás dönti el, hogy milyen felbontású kamerát célszerű alkalmazni. Egy szűk folyosó megfigyelésére nyilván megfelelő egy kisebb felbontású eszköz is, azonban a nagyobb terek – például iparcsarnok, pályaudvar, kikötő vagy repülőtér – megfigyelésére legalább 2-3 megapixeles eszközöket ajánlott választani. Természetesen adott felbontás mellett különböző objektíveket lehet alkalmazni. Az objektívek általában cserélhetők, de elég nagy számban találhatók a piacon olyan kamerák, amelyeknek eleve változtatható fókuszú gyári optikájuk van.

NŐ AZ INTELLIGENCIA

Az utóbbi idő egyik fontos tendenciája, hogy a videorendszerek egyre intelligensebbekké válnak. Azon túlmenően, hogy például képesek a rögzített eseményeket visszakeresni, intelligens videoelemzéseket is végezhetnek. Az elemzések egyik legalapvetőbb fajtája a mozgásérzékelés. Lényege, hogy amikor a rendszer valamilyen mozgást érzékel, riasztást ad. Egy másik intelligens funkció az objektumkövetés, objektumszámlálás, aminek nyomán a rendszer meg tudja számolni például a parkolóba behajtó autókat vagy az áruházba bemenő vásárlókat. A korszerű videorendszerek akár 90-95 százalékos pontossággal végzik az objektumszámlálást. További elterjedt intelligens videomegoldások az elvitt vagy ottfelejtett tárgyak érzékelése, és természetesen a kamera elfordítását,

letakarását jelző szabotázsvédelmi funkciók.

AZ IPARTÓL AZ EGÉSZSÉGÜGYIG

A kamerás megfigyelőrendszerek alkalmazási területe meglehetősen széles, ám országonként némi eltérést mutat. **Magyarországon leginkább az ipari létesítményekben, csarnokokban, raktárakban és természetesen bankokban alkalmaznak kamerákat, elsősorban vagyonvédelmi szempontok miatt. További ipari alkalmazás, amikor a gyártási folyamat kritikus pontjait tartja szemmel a kamera.** Ennek célja, hogy időben felfedezhessék a veszélyt hordozó eseményeket, és jó eséllyel megelőzhessék azok nemkívánatos következményeit.

A térfigyelő rendszerek közlekedési alkalmazásai jellemzően a vasútállomások, autóbusz-pályaudvarok, autópályák és repülőterek köré csoportosulnak. Ezeken a helyeken az elsődleges cél az utazóközönség biztonságának védelme, a torlódások megelőzése és kezelése, valamint a bűncselekmények megelőzése.

A bankoknál nagy hagyományuk van a biztonsági célú alkalmazásoknak. Ezek célozhatják a készpénzzel és bankkártyákkal kapcsolatos lopás és csalás megelőzését, továbbá a bekövetkezett eseményekről készült felvételek rögzítését és visszajátszását. A felvétel automatikus indításával például minden bankkártyás tranzakcióról külön-külön felvétel készülhet, ami a visszakeresést rendkívül egyszerűvé és gyorssá teszi. A videofelvételek hálózaton történő továbbítása a rendőrségi vizsgálatokat is gördülékennyé teszi.

Az IP-alapú kameratechnológia előnyeit a kereskedelem is kihasználja. Mivel a boltokban történt eseményekről (esetleges támadásokról, rablásokról) készült felvételeket távoli szervereken is tárolják, azokat a bűnözők nem tudják megsemmisíteni. A biztonságtechnikai, vagyonvédelmi szempontok mellett a videorendszer a vásárlói szokások elemzésére is kiválóan alkalmas. Az objektumkövetési funkció egy nagy áruházban például láthatóvá teszi, hogy a vásárlók milyen gyakori útvonalakon járják körbe az eladóteret, átlagosan melyik pultnál mennyit időznek. Ezekből az értékes információkból kiindulva a termékek elhelyezése optimalizálható.

Alkalmaznak már kamerás megfigyelőrendszereket az egészségügyben is. Az egyik fő terület, amikor a páciensek adatait, valamint a kutatási adatokat és egyéb kritikus információt tároló szerverek szobáit kísérik figyelemmel. A másik – meglehetősen kritikus – terület a betegek távoli megfigyelésével kapcsolatos (például távfelügyelet akár a kórházban, akár otthon, de a jó minőségű kép- és hangátvitelnek köszönhetően már a betegek távdiagnózisa is szóba kerülhet). A kamerás megfigyelés ezen alkalmazásai esetén különösen nagy figyelmet kell fordítani a személyiségi jogok tiszteletben tartására.

KAMERAVÁLASZTÉK

A kameráknak két alaptípusa különböztethető meg. A *beltéri kamerák* szokásos irodai környezetben működnek, azokat nem érheti eső, fagypont alatti hőmérséklet vagy egyéb környezeti ártalom. Működésükhöz általában minimális beltéri megvilágítás szükséges.

Kültéren legtöbbször úgynevezett *éjjel-nappali kamerákat* szerelnek fel. Ez azt jelenti, hogy sötétben az eszköz éjszakai üzemmódra vált át. Ilyenkor a beépített infravörös szűrő elhúzódik a képérzékelő elől, így a kamera érzékeli az infravörös tartományba eső fénysugárzást is. Hogy a kamera jól lásson a sötétben, a megfigyelendő terület sokszor infravörös megvilágítást igényel.

A kültéri kamerákat természetesen az időjárásnak ellenálló házba kell helyezni. Elég sok gyártó hoz már forgalomba eleve integrált házba helyezett kamerákat. Ezeket az eszközöket úgy alakítják ki, hogy a kamerák áramellátásához nem szükséges a 230 voltos hálózat, táplálásuk az Ethernet hálózaton keresztül történik. Mivel csak egy FTP-kábelt kell a kamerához elvezetni, ez a megoldás (Power over Ethernet) kifejezetten költségtakarékos. Mind a beltéri, mind a kültéri kameráknak vannak forgatható, dönthető, zoomolható (PTZ kamerák) változataik. Napjainkra megjelentek e kamerák 18-20-szoros optikai zoommal felszerelt HDTV felbontású változatai is. Ezek kilométeres távolságból képesek leolvasni a kikötőben lévő hajók vagy akár konténerrakományuk feliratait.

Egy jó minőségű videorendszerben az egy kamerára eső költség 300–500 ezer forint körül mozog. Tehát egy 10 kamerás rendszer mintegy 3–5 millió forintba kerül, beleértve a szerelési költségeket is. Beltéri IP-kamerát – természetesen nem prémium minőségűt – már akár 30-40 ezer forintért is lehet vásárolni. A kültéri, csúcsminőségű kamerák ára a felbontástól függően 200–400 ezer forint között mozog. A professzionális HDTV speed dóm (PTZ) kamerák ára akár az egymillió forintot is megközelítheti. Általános tendencia, hogy a kamerák választéka mind típusban, mind felbontásban, mind szolgáltatásban nő, miközben az árak folyamatosan csökkennek. Átlagos élettartamuk 8-10 év, de ez alatt az idő alatt – hasonlóan a számítógépekhez – el is avulnak. A kiváló minőségű termékekre a gyártók 2-3 év gyári garanciát adnak.

Megjegyzendő, hogy léteznek más technológiájú, egyelőre meglehetősen drága, úgynevezett hőkamerák is, amelyek sötétben, mindenfajta megvilágítás nélkül is használhatók. Gyakorlatilag olyan hőképet adnak, amely az embereknek, illetve a tárgyaknak csak a sziluettjét mutatja, a valós kép részletei nem láthatók. A hőkamerák kiválóan alkalmasak mozgásdetektálásra teljes sötétségben, füstben, ködben, sűrű hóesésben.

Esésdetektálás – kép nélkül

Rövidesen lezárul az a négy ország részvételével indított európai uniós projekt, amelynek célja egy speciális optikai szenzor, valamint annak adatait feldolgozó algoritmus fejlesztése. A rendszer alkalmazásával felismerhető a lakásban élő személyek elesése, továbbá megfelelő jelzés, riasztás küldhető egy távoli felügyeleti központ felé. A CARE *(Biztonságos otthonok idős embereknek)* projekt magyar résztvevője a Budapesti Műszaki és Gazdaságtudományi Egyetem.
A munka megkezdése előtt több etikai kérdést kellett tisztázni. A fejlesztők választ kerestek például arra, hogy az idős vagy beteg személyek menynyire tartanak elfogadhatónak egy kamerát a környezetükben. Alapvető feladat volt annak tisztázása, hogy egyáltalán mi tekinthető esésnek. Ezt követően meg kellett határozni az esés érzékelésének módszerét.
A hagyományos kamerával való folyamatos megfigyelés esetén hatalmas adatmennyiség keletkezik, aminek nagy része felesleges. Ráadásul ennél a megoldásnál tényleg úgy érezheti magát az idős ember, mintha valaki állandóan lesné minden lépését, személyiségi jogai sérülhetnek Ezért a CARE projektben olyan speciális optikai érzékelőt választottak, amely csak a változó pontokról továbbít információt. A rendszer a változás jellegéből (például világosból sötét), pozíciójából (legmagasabb pont, tömegközéppont, a határoló téglatest és henger pontjai), időpontjából, sebességéből stb. hámozza ki azt az információt, amiből az elesésre lehet következtetni. A személyről igazi képet még ideiglenesen sem rögzít a rendszer. Maga a készülék csak az értékelést adja ki: jelzi, hogy az idős ember elesett-e vagy sem.

Avatárvadászat

Az internet-technológiák mindennapos használatával megállíthatatlanul terjedni kezdett a cyberbűnözés is, többek között azon válfaja, amelyben az elkövető egy virtuális személyiség álarca mögé rejtőzik. Vajon milyen eszközök állnak a bűnüldözés rendelkezésére a virtuális térben egy valós elkövetővel szemben? Írta: Kömlődi Ferenc

A digitális média, például a bővített valóság (Augmented Reality, AR) fejlődésével, a telejelenlét népszerűvé válásával és az elektronikus kereskedelem térhódításával párhuzamosan az online bűnözés (zaklatás, csalás, pénzmosás, adat- és identitáslopás stb.) is elterjedt, kialakult a digitális alvilág. A világháló és különösen a tömegesen látogatott virtuális világok biztonsága komoly fejlesztői kihívást jelent.

AVATÁROK A VIRTUÁLIS TEREKBEN

Az infokommunikáció és az automatizáció elterjedésének egyik következményeként az utóbbi két évtizedben előszeretettel alkalmazzák az információbiztonsági szempontból több mint kielégítőnek nevezhető biometrikus megoldásokat személyek azonosításához. Az alkalmazások biológiai (nyál, vér, DNS), fiziológiai (arc, hang, retina, írisz, ujjlenyomat) vagy viselkedésbeli (aláírás, mozgás, gépelés) karakterjegyeken, illetve előrevetítve a jövőt, azok valamely kombinációján alapulnak. Azért hasznosak és biztonságosak, mert ezek a vonások egyénspecifikusak, és általában egész életünk alatt ugyanazok maradnak. **A biometrikus rendszerek – közülük is főként az arcot vizsgálók – fokozatosan és folyamatosan javulnak; olyannyira, hogy virtuális (és közvetve, az általuk megjelenített) személyekre elvileg szintén alkalmazhatók már.**

Az avatárok arca, viselkedése segít az őket irányító személyek azonosításában. Karakterjegyeiket vizsgálva kidolgozhatók olyan eljárások, amelyekkel megállapítjuk, hogy a digitális személyiségek tényleg azoké, akiknek tűnnek, akiknek mutatják magukat. Közelebb jutunk a mögöttük lévő élő emberekhez. Az összegyűjtött információk különféle szituációkban bizonyulnak hasznosnak: ha egy honlapon, játék közben nem látjuk az éppen belépő személy adatait, ha nem tudunk utánanézni a bejelentkezési részleteknek, ha gondosan figyeljük az adott oldal látogatóit, vagy ha – nem utolsósorban – a törvény le akar csapni az internet zavarosában (alkalmasint féltve őrzött adatokat) halászókra. De üzleti tranzakcióknál is fontos, hogy a kommunikációs fél biztos legyen benne: a monitoron megjelenő online reprezentáns valóban az, akinek hiszi, és akivel tárgyalnia kell.

Valóság és virtualitás, fizikai és cybertér határainak egymásba mosódásával, a határok fokozatos eltűnésével egyre komolyabb problémát okoz az avatárok azonosítása. A tendencia a közeljövőben még markánsabban érvényesül. Az évtized második felében sokszereplős számítógépes játékok, közösségi web, virtuális világok, bővítettvalóság-elemekkel kiegészített térképek egymásba integrálódásával metaverzumszerű online közeg(ek) jön(nek) létre. A globális információs térben a tökéletes szimuláció (majdnem) teljes immerzív élményt biztosít, az ottlét érzetét helytudatos rendszerek és interfészek fokozzák. Számos előnye (információcsere, ötletek megosztása, virtuális konferenciák, új ismeretségek, munka és üzleti lehetőségek, oktatási tevékenységek, szórakozás) mellett azonban nagy hátrány, hogy védtelenebb a fizikai valóságnál. Ebben a környezetben – pontosabban, ezekben a környezetekben – lényegesen több, hitelesebb, intelligensebb, de ha úgy akarjuk, a maiaknál sokkal nehezebben azonosítható, anonim avatár mozog, kommunikál, lép interakcióba egymással. Nem mindig tudjuk, melyik jó és melyik rossz szándékkal, melyik közeledése őszinte, és melyik vadászik gondosan őrzött titkokra.

Az avatárok egyelőre elsősorban online játékok résztvevőit (World of Warcraft, Guild Wars stb.) és virtuális közösségek (Second Life, Entropia Universe) tagjait személyesítik meg. Felhasználási körük bővülésével az internet más területein is hasonló/ugyanolyan fontos szerepet töltenek be, mint a játékok mesés terében. Márpedig, ha ennyire meghatározó tényezővé válnak, azonosításuk szintén kitüntetten fontos feladat (lesz). Legalábbis azoké, amelyekkel rendszeresen találkozunk valahol.

BIOMETRIKUSAN AZONOSÍTOTT AVATÁRARCOK

Roman Yampolskiy, a Louisville Egyetem (Kentucky állam) számítástudományi szakembere és munkatársai az arcfelismerést és az azon alapuló biometrikus megközelítést próbálják alkalmazni biztonsági rések okozta veszélyforrások elhárítására. Egyben arra is felhívják a figyelmet, hogy az avatár mögötti személy azonosítása (vagy legalább, ha lényeges információkkal rendelkezünk róla) nemcsak biztonsági, bűnüldözési, hanem kereskedelmi szempontból is fontos és kifejezetten hasznos. Például komoly előny, ha ismerjük az illető nemét. Marketingcélú profil készíthető róla, és könnyen megtudjuk, hogy a virtuális piacterek mely szegmenseiben bukkan fel sűrűn. Amennyiben avatárjait közegenként váltogatja, közösségenként más online reprezentánst használ, az azonosítás – törvényszéki esetekben is – még nagyobb előnyökkel jár. Például gyorsabban kideríthető, ha meghekkelt és ellopott egy játékaccountot.

A kutatók emberi arcokat azonosító, klasszikus mintafelismerő modellt követő rendszert választottak kísérleteikhez. Első lépésként meg kellett tanulnia biológiai minták felismerését, máskülönben képtelen lenne később hasznos információkat gyűjteni a vizsgált személyekről, amelyeket aztán a korábban, még a gyakorlás/tanulás közben összeszedett adatokkal hasonlít össze. Mindegyik állapot két modult tartalmaz: az egyik képeket detektál és készít elő feldolgozásra, a másik karakterizál, osztályoz, és végül döntést hoz. Mindezek után a különböző lépések pontos leírása következik.

A képek összegyűjtése a folyamat egyik legfontosabb része. Változatos forrásokból, hagyományos és digitális kamerával, szkennerrel felvettekből válogattak. Kezdéshez a Second Life-

ból összeszedett gyűjteményt használták, és próbálták megfigyelni az avatárok külsejének és tulajdonságainak lehetséges változásait, illetve levonva belőlük a következtetéseket, újabb anyagokkal (forma-, bőrszín-, hajtípus-változatok) bővített, gazdag adatbázist alakítottak ki. Az avatárokról, arckifejezésük (mosoly, szomorúság, meglepettség stb.) változásáról meghatározott kameraszögben pillanatfelvételeket (snapshots) készítettek. Közben az adatbázist folyamatosan összehasonlították a virtuális személyek készítésére előszeretettel használt MyWebFace honlap bőséges anyagával.

Először az avatár neméről, majd külsejéről (arcforma, különböző arcvonások színe, kiegészítők) döntöttek, végül a kész avatár pillanatfelvételeit speciális (captimage) szoftverrel rögzítették, meghagyva a változás lehetőséget. Ezt követően a több tényező (orientáció, elhelyezkedés, térhatás, fényviszonyok, méretváltozások) figyelembevételével a képből részleteket kiemelő, levágó, manuálisan kezelhető PhotoFiltre programot tesztelték. Az előfeldolgozás (filterezés és szabványosítás) befejezéseként minimalizálták az információt nem hordozó részeket, illetve a későbbiekben használandó ikonszerű kis képeket (thumbnails) készítettek.

A karakterizálás során a kivonatolt ismertetőjegyek alapelemeiből állítottak össze sorozatot, amely – amennyire csak lehetséges – leírja a képek legfontosabb variációit. A folyamat végén úgynevezett wavelet transzformációval (képek négyszögjel alapú spektrális felbontására, szűrésére és tömörítésére használt eljárással) nyertek ki az eredeti textúrára vonatkozó információt.

Az osztályozásnál algoritmus hasonlította össze az azonosításkor megfigyelt matematikai-geometriai jellemzőket a tanuláshoz használt alapképekkel. A folyamat összegyűjtött minták és adatreferenciák összevetése, célja a virtuális világba belépő személy azonosítása: a legszembetűnőbb hasonlóságok alapján megállapítani, hogy az avatár szerepel-e az adatbázisban vagy sem. Maga az osztályozás speciális módszerrel (szupport vektor gépekkel) történt. A hitelesítés egyaránt lehetett pozitív és negatív, majd ezt követően megszületett a végső döntés: az arcosztályozóhoz társított legmagasabb értékű output lesz „az arc identitása”. Amennyiben ez nem felelt meg egy előre meghatározott küszöbértéknek, az osztályozó azonosítatlanul dobta vissza a bemenő képet (és a rajta látható arcot).

BIZTATÓ EREDMÉNYEK

Az emberi arcfelismerésre használt legismertebb speciális adatbázisokat (FERET, YalesFaces, AT&T, AR) figyelembe véve a kutatók megállapították, hogy az azonosító rendszer eredményes működését a képek mérete, felbontása és a formátumuk közti hasonlóság garantálja. A beállítás, kontraszt és megvilágítás szintén sokat segíthetnek. „Inkognitóban” lévő avatárok felismeréséhez képekben rendkívül gazdag, a korábbi gyakorlás során használt konzisztens matériával kiegészült adatbázis szükséges, máskülönben az arckifejezések, bőrszín- és egyéb változások ellehetetlenítik a munkát; ugyanazon virtuális ember ezer és egy arca teljesen megbolondítja a rendszert. Természetesen minél jobb a kép (méret, felbontás, kontraszt stb.), minél több kiegészítő elemmel, speciális külső jeggyel (bajusz, szemüveg, kalap stb.) egészül ki az arc, annál valószínűbb a siker.

Yampolskiy és munkatársai pontosan efféle megfontolásokból rögzítették a képméretet, növelték a felbontást, miközben arra is vigyáztak, hogy a módosítások ne lassítsák le az algoritmus futtatási idejét. A legjobb eredményeket 90 ppi rezolúciójú, 150×175 pixeles képekkel érték el. Minden egyes avatárhoz sok és változatos pillanatfelvételt kapcsoltak: bajusz nélkül és bajusszal, szemüveggel és szemüveg nélkül, és így tovább. Száz különböző avatárhoz 1800, azaz mindegyikhez tizennyolc arcképet sikerült rendelniük. Tizennégy érzelmeket (öröm, szomorúság stb.), a többi négy pedig a külső potenciális változásait/megváltoztatását ábrázolja. Az összes kép színes, szemből, azonos háttér előtt és szintén azonos világítás/fényviszonyok mellett vették fel őket. A tizennyolc képből tizenkettőt a gyakorláshoz, hatot a teszthez használtak fel.

Az azonosítást komolyan hátráltatja, hogy – az emberrel összehasonlítva – az avatárok arca nem vagy csak nagyon korlátozott mértékben változik. A számítógép által generált képek (CGI) egyértelmű geometriája miatt viszont viszonylag könnyű mérni, számszerűsíteni a korlátozott opciókat. Yampolskiy kutatócsoportja a Second Life és később az Entropia Universe csomó lehetséges arcából hozott létre hatalmas adatsorokat, majd azokat tanulmányozva próbált kulcsfontosságú karakterjegyeket kimutatni. Egyelőre ugyan még mindig gyűjtik az adatokat, de az eddigi eredményeket már most sikerként könyvelik el. amíg egy korábbi tesztjük során száz avatárral, avatáronként tíz, azaz ezer 72 ppi felbontású képnél 4,07 százalékos hibarátával dolgoztak, addig 90 ppi-nél kis híján a felére, 2,2 százalékra minimalizálták/optimalizálták a hibarátát. Pedig (az avatárok számán nem módosítva) változatosabb képekkel, többféle kiegészítő elemmel, jóval bonyolultabb „sminkeléssel” dolgoztak. A kimagaslóan sikeres azonosítás bizakodásra ad okot – úgy tűnik, a jövőben tényleg könnyebb lesz lefülelni a hamis avatárokat és virtuális álarc mögé bújt, arcukat és álarcukat állandóan cserélgető csalókat, bűnözőket.

A virtuális arcok biometrikus alapokon nyugvó hitelesítése és azonosítása mellett a viselkedéselemzés (gesztusok, mozgások és egyéb megkülönböztető karakterjegyek monitorozása) szintén célszerű, ugyanis így még jobban kimutatható, hogy az adott esetben az avatárt az a személy irányítja, aki általában szokta, vagy sem. A hús-vér személyek biometriájához hasonlóan, a kombinált eljárások a virtuális lények esetében szintén teljesebb képet adnak, kisebb a tévedés esélye. Amennyiben az avatár a megszokottól eltérően cselekszik, egy-egy szituációra teljesen másként reagál, valószínűleg nem az eredeti tulajdonos mozgatja.

A kutatócsoport újabb virtuális világokat (Active worlds, LeVillage3d, There) vizsgál, és gyűjt belőlük avatárképeket. Az arcjegy-kivonatolás bonyolult műveletének teljes automatizálásához speciális platformot (Luxand FaceSDK) hoztak létre. Mivel egyre több gép dolgozik az emberek mellett, könnyebben hozzáférnek a fontos adatokhoz. Az engedélyezés viszont csak akkor biztonságos, ha ugyanarról a gépről és nem (esetleg rossz szándékú) hasonmásról van szó. Yampolskiy ezért úgy döntött, hogy az azonosítást és a viselkedésmonitorozást hamarosan robotokra is kiterjesztik.

Szoftvervédelem – már az alapoktól

Hogyan lehetnek még ellenállóbbak a jövő alkalmazásai? Úgy, ha nemcsak a hagyományos tesztelési módszerek, de az automatizált szoftvertesztelés során is kellő figyelmet fordítanak a biztonságra. Írta: Szilágyi Szabolcs

A puding próbája az evés – tartja a mondás, de szerencsére nem feltétlenül kell ennek így lennie a szoftveriparban. Ha az elvárt feladatok átgondolására és a tervezésre elég időt fordítottak, akkor a fejlesztés során létrejövő program éles használatakor nem érheti nagy és kellemetlen meglepetés az ügyfelet. Ehhez azonban szükség van még egy közbülső lépésre is: miután elkészült a szoftver, és mielőtt hétköznapi használatba vennék, tesztelni is kell.

Egy program jóságát, hacsak nem vizsgamunkáról vagy házilag „barkácsolt" számlázószoftverről van szó, ma már nem kizárólag manuálisan vizsgálják, hanem különböző automatizált módszerek segítségével is. Ennek során **fény derülhet olyan hibákra, amelyek megkeseríthetik a leendő felhasználók életét, vagy – bizonyos körülmények között – egyenesen ellehetetleníthetik a rendeltetésszerű használatot.**

Tesztelésre tehát szükség van, de nem csupán azt kell felmérni, hogy van-e a szoftverben algoritmizáltan felismerhető programozási vagy logikai hiba, ami lefagyáshoz vezethet, hanem azt is, hogy biztonsági szempontból mennyire felel meg a 21. századi kihívásoknak. Ebben nyújthat nagy segítséget a kockázatelemzés, különösen, ha arra a tervezési szinten kerül sor: általa felmérhetők a lehetséges biztonsági problémák, és – ami legalább ennyire fontos – a várható hatásuk. A sebezhető pontok (melyek tipikusan két kategóriára, implementációs szintű és tervezési szintű hibákra oszthatók) és veszélyességük azonosítása segíthet a szoftverbiztonsági tesztelés elvárt szintű lefutásában.

A legnagyobb fejtörést a tervezéskor elkövetett hiányosságok okozzák, mivel ezeket a legnehezebb kezelni. Egyben az ekkor keletkezett sérülékenységek jelentik a legnagyobb bajt is. Továbbá annak meghatározása, hogy vajon egy programnak vannak-e tervezési szintű hibái, nagy tapasztalatot igényel, ami egyben sajnálatosan azt is jelenti, hogy az ilyen sebezhetőségeket nemcsak nehéz észlelni, de különösen problémás automatizálni ezt a folyamatot. Milyen hibákról van szó? Például az objektumorientált rendszerek hibakezeléséről, az objektumok megosztásáról, védtelenül maradt külső és belső adatcsatornákról, rossz vagy hiányzó hozzáférés-ellenőrző mechanizmusokról, az auditálás/logolás hiányáról vagy annak nem megfelelő kialakításáról, valamint – különösen a többszálas rendszerekben – időzítési, illetve utasítás-sorrendi hibákról. A fentiek valamelyikének elkövetése szinte mindig az adott szoftver biztonsági kockázatának növekedéséhez vezet.

KOCKÁZATKEZELÉS ÉS BIZTONSÁGI TESZTELÉS

A kockázatelemzés számos feladat végrehajtását jelenti, többek között meg kell állapítani, mi számít biztonsági szempontból visszaélésnek, melyek a biztonsági követelmények előírásai, architekturális kockázatelemzést kell futtatni, létre kell hozni kockázatalapú biztonságiteszt-terveket és biztonsági teszteket kell futtatni. Az utóbbi három egymással szoros együttműködésben kell, hogy végbemenjen, mivel a biztonsági tesztelés jelentős részben támaszkodik a felmért kockázatok elemzésére.

„A szoftverbiztonság nem egyenlő a biztonsági szoftverrel" – ez az örök érvényű igazság arra világít rá, hogy habár az olyan funkciók, mint a titkosítás, az erős autentikáció és a hozzáférés-ellenőrzés kritikus szerepet játszanak a szoftverbiztonságot illetően, a biztonság maga a teljes rendszer jóságára vonatkozik, nem csak az implementált biztonsági technológiákra. Közérthetőbben megfogalmazva: egy puffer-túlcsordulásos hiba biztonsági veszélyt jelent, függetlenül attól, hogy az egy biztonsági funkcióban vagy például a nem kritikusnak számító grafikus kezelői felületben található. Ennek megfelelően a biztonsági tesztelésnek szükségszerűen figyelembe kell vennie, hogy a védelmi mechanizmusok tesztelése során meggyőződhetünk-e megfelelően történt alkalmazásukról, illetve a kockázatalapú biztonsági tesztek végrehajtását egy támadó szemszögéből kell lefolytatni.

A hagyományos, funkcionális biztonsági tesztelés a könnyebbik vége a feladatnak, a kockázatalapú biztonsági tesztelés ugyanis jóval nagyobb szakértelmet kíván. Először is egy komplett exploit-vizsgálat nehezebben hajtható végre, mivel – amint azt már említettük –, a támadó fejével kell gondolkodni az automatizált teszt létrehozása során. Másrészt a kapott eredmény könnyen alakulhat a várttól merőben eltérően, így azt értelmezni kell (tehát manuális beavatkozást igényelhet), esetleg további, kifinomultabb elemzésnek alávetni.

MI VAN A DOBOZBAN?

Általánosan nézve kétféle tesztelési és elemzési eljárás létezik: az úgynevezett fehér és a fekete dobozos tesztelés. Mindkettő a szoftver megértésére törekszik, ám ezt eltérő módszerekkel teszi. Az egyik, illetve a másik eljárást attól függően kell alkalmazni, hogy a teszteléskor rendelkezésre áll-e az eredeti forráskód. Ha igen, akkor a fehér dobozos analízis segíthet felmérni az adott szoftver jóságát a forráskód és a tervezés elemzésével. Ez a módszer nagyon hatékony a programozási hibák – automatikus kódellenőrzéssel és kockázatelemzéssel való – felderítésében. Ugyanakkor hátránya, hogy akkor is potenciális sebezhetőséget jelenthet a tesztelést végzőnek, ha valójában nem is létezik a tesztelési algoritmusok által „megtalált" hiba (azaz fals pozitív eredményt adhat).

Fekete dobozos elemzésről beszélünk, ha az eredeti forráskód nem elérhető, vagy ugyan rendelkezésre áll, ám azt mégsem használják fel. Ilyen esetben a program futtatására van szükség, és a bemenő adatok (input) változtatása mellett figyelni kell a kijövő információ (output) karakterisztikáját. Egy ártalmas input, ha az adott szoftver érzékeny rá, ráveheti a futó alkalmazást az elvárttól eltérő, kártékony működésre. Ha a program lefagy vagy hibát eredményez adott tesztelési eljárásnál, akkor az akár potenciális biztonsági rést is jelezhet.

A LEGFŐBB PROBLÉMA

Az említett két eljárás egymás mellett vagy külön-külön alkalmazva egyaránt felfedhet olyan szoftveres kockázati tényezőket és exploitokat, amelyek később súlyos biztonsági incidenseket okozhatnak. Függetlenül attól, milyen tesztelésről van szó, a legnagyobb probléma mindegyikkel ugyanaz: többnyire nem alkalmazzák őket. A fejlesztők – költségvetési szempontoktól vezérelve, vagy pedig azért, mert inkább funkcióvizsgálatra fordítják erőforrásaikat – hajlamosak kihagyni ezt a lépést.

Óriási kockázatot jelenthet azonban a biztonsági hibák felkeresésének és megértésének „elsunnyogása", melynek árát ráadásul nem is azonnal kell megfizetni. **Abban ugyanis biztos lehet a fejlesztő, hogy előbb-utóbb valaki ártó szándékkal fogja megvizsgálni alkalmazását, és ha talál rajta gyenge pontot, azt ki is fogja használni. Ha a szoftvert közben már több százezer, esetleg millió példányban telepítették, nagyon nehéz helyzetbe kerülhetnek a felhasználók**: potenciális – és ami még nagyobb baj,0 ismeretlen – biztonsági rés lapul számítógépeiken, gyakran még akkor is, ha egyébként minden előírt védelmi szabályt (rendszeresen frissített víruskereső és tűzfal használata, ismert biztonsági javítások, patchek telepítése stb.) betartanak.

Velünk többre képes vállalkozása

Akciós számlacsomagok számlavezetési havidíj nélkül 2011. szeptember 19-től november 30-ig!

A **Széchenyi50** program olyan **hiteleket és számlacsomagokat** tartalmaz, melyek kimondottan mikro- és kisvállalkozások számára biztosítanak kiegyensúlyozott pénzügyi hátteret.

Nyisson az akciós időszak alatt új vállalkozói számlacsomagot, és a **számlavezetés havidíját 6 hónapon keresztül nem számítjuk fel** (kivéve Gold és társasházi számlacsomagok). Bankunknál biztosan megtalálja az Ön vállalkozása számára leginkább megfelelő megoldást.

Ahhoz, hogy a kedvezményt igénybe vehesse, nem kell mást tennie, mint felkeresni egy OTP bankfiókot, és kollégáink segítségével kiválasztani az Önnek legmegfelelőbb vállalkozói szolgáltatást.

A tájékoztatás nem teljes körű, az akciós termékek leírása megtalálható a vonatkozó hirdetményekben és üzletszabályzatokban, valamint a www.otpbank.hu honlapon.

www.otpbank.hu
06 1/20/30/70 366 6666 • 06 40 366 666 • 06 1 366 60 30

otpbank
Megbízunk egymásban

otp vállalkozói akciók