SZÁMÍTÁSTECHNIKA
COMPUTERWORLD BUSINESS
IKT-STRATÉGIA DÖNTÉSHOZÓKNAK / ALAPÍTVA 1969 / 2012. NOVEMBER 28. / XLIII. ÉVFOLYAM 48. SZÁM

A FÉLELEM SZÁZMILLIÁRDJA

A technológiai változások nagy trendjei egyre hangsúlyosabbá teszik a céges adatok és tartalmak megóvásának fontosságát. Ezért a kártevők és a kiberbűnözés elleni védelem változatlanul fontos prioritása marad a cégeknek.

Összeállításunk a 8–11. oldalon

A HÁLÓZATI KAMERÁK JÖVŐJE

A témát feltalálójukkal, Martin Grennel, az Axis alapítójával fürkésztük.

» 14. oldal

PÁRHUZAMOS FOLYAMATOK

Nincs miért szégyenkeznünk a mobilfizetés miatt – még csekély, de meredeken nő.

» 18. oldal

9 770587 151006 12048
www.computerworld.hu
Ára: 495 Ft
IDG HUNGARY

COMPUTERWORLD /IMPRESSZUM

KIADJA AZ IDG HUNGARY KFT.
1075 Budapest, Madách I. út 13–14. A épület
HU ISSN 0237-7837
Postacím: 1374 Budapest 5, Pf. 578.
» 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:
Mesterprint Kft. 1191 Budapest,
Vak Bottyán utca 30-32/b
Ügyvezető igazgató: Szita Lajos

SZERKESZTŐSÉG
Megbízott főszerkesztő: Szilágyi Szabolcs
Vezető szerkesztő: Sós Éva
Online igazgató: Odrovics Szonja
Olvasószerkesztő, korrektor: Váczy Laura
Munkatársak: Dávid Imre, Kis Endre, Kömlődi Ferenc, Meixner Zoltán, Tóth Lívia, Vass Enikő
Tipográfia: Berényi István
Szerkesztőségi ügyelet:
Csereszny Anita – acsereszny@idg.hu
Telefon: 577-4302, fax: 266-4343
Munkatársaink elérhetőségeit megtalálja weboldalunkon: » www.computerworld.hu

HIRDETÉSFELVÉTEL
Kereskedelmi igazgató:
Dr. Farkas Viola – vfarkas@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
» e-mail: terjesztes@idg.hu

MEDIASHOP: MEDIASHOP.IDG.HU

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.
A Computerworld az IVSZ hivatalos médiapartnere.
A Computerworld Online látogatói szokásait a gemius/Ipsos Audience vizsgálja. A Computerworld Online hirdetéseit az Adverticum AdServer szolgálja ki.

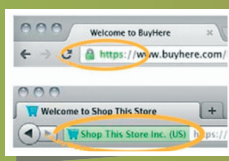
A szerkesztőségi anyagok vírusellenőrzését a **NOD32 Antivirus** programmal végezzük, amelyet a szoftver magyarországi forgalmazója, a **Sicontact Kft.** biztosítja számunkra.

COMPUTERWORLD /ONLINE

SZABAD-E A SZABADALOM?
A keresőóriás szerint szabadalmain a Microsoft tízmilliárdokat kasszíroz.
techcorner.hu/computerworld/google-a-microsoft-tizmilliardokat-kereshet-a-szabadalmainkon.html

KEVÉS AZ ÉRINTŐKÉPERNYŐ?
Robbanás volt egy alapanyagokat gyártó japán üzemben, a helyreállítások sok időbe telnek.
techcorner.hu/computerworld/gond-lehet-az-erintokepernyok-hozzaferhetosegevel.html

VÁSÁRLÁSI LÁZBAN
Az ünnepek közeledtével az internetes átverések száma is növekszik.
techcorner.hu/biztonsagportal/a-kiberbunozok-is-keszulnek-a-karacsonyi-bevasarlasra.html



KELETI ARTHUR

főszervező, ITBN alapító, Önkéntes Kibervédelmi Összefogás (KIBEV)

„Stux, maga vérbeli párizsi lett”

Az 1930-as évek népszerű kuplénótáját a közelmúlt informatikai eseményei juttatták eszembe. Az iráni atomprogram működését hátráltató amerikai-izraeli szupervírusról (ha úgy tetszik, kiberfegyverről) ugyanis a napokban derült ki, hogy 2010-ben „kiszabadult gazdái laboratóriumából”, és nemcsak az ellenségnek okozott gondot, hanem a világ több baráti iparvállalatának is.

> ...az egész kibertér egy szigorúan ellenőrzött hálózattá válik, ahol minden „internetezőt” egyértelműen lehet majd azonosítani...

Köztük volt az amerikai olajipari óriás, a Chevron is, amelynek egyik vezetője kijelentette: „Nem gondolom, hogy az amerikai kormány tisztában van vele, hogy a vírus milyen messze jutott. Azt hiszem, annak, amit csináltak, a negatív hatása sokkal nagyobb lesz, mint amit elértek vele.” Tehát a kibervírus elszabadult, és most már saját útját járja a világ kritikus infrastruktúráinak rendszereiben, de ugyanez elmondható a többi azóta megjelent, továbbfejlesztett verzióról is.

Az ilyen és ehhez hasonló kiberfegyvereket ma már legalább annyira a kormányok által megbízott szervezetek, mint a kiberbűnözők készítik, és csak a felhasználás céljában, valamint az alkalmazók motivációjában térnek el. Sőt, a világban ma már kiberfegyver-kereskedők is dolgoznak, akik – megfelelő szabályozás hiányában – legális keretek között hirdetik szolgáltatásaikat, és ismert programokban feltáratlan informatikai sérülékenységeket árulva darabonként 100 000 – 200.000 dollárt is keresnek.

Eközben a világ informatikai és katonai vezetői kiberháborúról beszélnek, amelyet leginkább a hidegháborúhoz hasonlítanak – legalábbis azon tulajdonságaiban, hogy csendben, a lakosság háta mögött zajlik, nagyon sokba kerül, és az olyan kritikus infrastruktúrákon keresztül, mint az áram- és vízszolgáltatás kiesése, nagy hatással lehet az életünkre. A védelmünkre kiberhadseregeket szerveznek; Anglia például nyíltan toboroz kiberkatonákat, és 650 millió fontot különített el egy kiberfegyver építésére.

Vajon el tudja-e helyezni magát egy hazai vállalatvezető, egy magánember vagy egy kritikus infrastruktúrát üzemeltető az informatikai szuperkatasztrófák baljós képével fenyegető félelmek koordinátarendszerében? És vajon tudjuk-e, hogy hova vezet mindez?

A tavalyi Informatikai Biztonság Napjára felkértem *Marcus J. Ranum*ot, a híres amerikai informatikai biztonsági gurut, az alkalmazásalapú tűzfalak atyját, hogy pillantson bele a kristálygömbjébe, és mondja meg nekünk, mi vár ránk 100 év múlva 2111-ben. Bár ne kértem volna erre. Egyre lejjebb csúsztam a székemben, ahogy arról mesélt, miképpen fogják majd a kormányok kiterjeszteni hatalmukat a kibertérbe, miképpen válik majd a mobiltelefonunk a testünkbe épített összes személyes ügyünket intéző „titkárrá” – és hogy az egész kibertér egy szigorúan ellenőrzött hálózattá válik, ahol minden „internetezőt” egyértelműen lehet majd azonosítani, mozgásáról pedig részletes információja lesz az üzemeltetőknek, kormányoknak. Akkor azt hittem, hogy ez egy olyan sci-fi, amelynek megvalósulását szerencsére én már nem fogom látni. A napokban pedig rájöttem, hogy nemcsak látni fogom, hanem részt veszek az építésében.

Az informatikai rendszereink komplexitása az egekbe szökött. Ma már nem létezik olyan informatikus, aki átlátná a rendszereket, pontosan értené az összes bonyolult alkalmazás együttműködését. Ez jó a kiberbűnözőnek, rossz a védelemért dolgozóknak. Ebből táplálkozik az az igény, hogy próbáljuk meg valahogyan jobban kontrollálni, hogy mi zajlik a vállalati hálózatainkban, az interneten, vagy éppen a kritikus infrastruktúrák informatikai rendszereiben. Rövid agytornával eljuthatunk oda, hogy már ma is van létjogosultsága a teljes kontrollnak, a mindenen átívelő azonosítási megoldások bevezetésének, és ha ehhez hozzáképzeljük a szerzői jogok és digitális tartalmak védelméért harcosan küzdő médiavállalatok igényeit, akkor már majdnem eljutunk Marcus sötét ecsettel festett 2111-es informatikai jövőképéhez.

Mégis asszisztálnunk kell hozzá. Mert magunkat védjük. A vállalatvezető a cége adatvagyonát, hírnevét. Az állami döntéshozó a nemzeti adatvagyont. A létfontosságú infrastruktúrák vezetői a stratégiai szolgáltatásokat. A magánemberek pedig a családi adatvagyont és a magántitkot. Minél bonyolultabb társadalmat építünk, annál sérülékenyebb informatikával támogatjuk meg, amelynek stabilitása vitális, védelme pedig megkerülhetetlen feladat.

Azt javaslom, hogy gondolkozzunk el viszonyunkon a saját biztonságunkkal, és cselekedjünk! Mindenki a saját szintjén mérlegelje, hogy mennyit áldoz fel a privát szférájából, a költségvetéséből és az önállóságából, mert az óránként változó és egyes kimutatások szerint évente több mint 300 milliárd dollár kárt okozó kiberfenyegetések és az ellenük küzdő kormányok, biztonsági szakemberek már most betörtek csendes és kényelmes világunkba. Ott vannak a mobiltelefonunkban, a számítógépünkön, a vállalati rendszereinkben, az állami adatbázisokban, az áram- és vízszolgáltatók rendszereiben – vagyis mindenhol.

Lelki füleimben cseng a Stux-kuplé refrénje: „ha az ember nem látná, én úgy éljek, el se hinné...”

Hyde Tech Corner

Ezen a héten *Dienes-Oehm Tivadar,* a Dell Magyarország sales managere kommentálja szakcikkünket.

Az előrejelzések szerint három éven belül a saját mobilkészülékek használata lehet az általánosan elterjedt szokás a legtöbb vállalatnál. A cégeknek kell az „ingyen" eszköz, de félnek is a felhasználói gondatlanságtól. Pontos szabályozással azonban megvédhetők a vállalati adatok.

BYOD: KIS VÁLLALATOK NAGY GONDBAN

A saját eszközök munkára való használata (BYOD) egyre elterjedtebb. Ennek következményeiről főleg azoktól a nagyvállalati szakemberektől hallani, akik nagyon tudatosan és előre gondolkodva menedzselik cégük IT-erőforrásait. De mi a helyzet a kisebb cégekkel, ahol nincsenek kistafírozott nagy létszámú informatikai részlegek, ám BYOD van?

» http://computerworld.hu/byod-kis-vallalatok-nagy-gondban-20121107.html

Az otthoni készülékek valóban egyre inkább munkaeszközzé is válnak, és ezen keresztül hozzájárulnak a saját eszközök munkahelyi célú használatát szorgalmazó BYOD (Bring Your Own Device) kezdeményezés terjedéséhez. 2010-ben világszerte 302 millió okostelefont vásároltak, és az ABI Research adatai szerint 2016-ig további 19 százalékos növekedés várható ezen a területen. A vállalatok részéről tehát felmerül az igény, hogy munkatársaikat egyre inkább ösztönözzék a különböző személyes mobil számítástechnikai eszközök munkára történő használatára.

Azzal, hogy a vállalati információk a mobileszközök révén utazás közben, illetve az irodán kívül is elérhetővé válnak, a munkatársak jelentős időt és energiát takaríthatnak meg a munka hatékonyságának növelése mellett. Az AMI-Partners kutatása szerint ez hozzájárul a nagyvállalatok üzleti hatékonyságának növeléséhez, sőt ugyanezen okokból a BYOD-mozgalom egyre inkább terjed a KKV-k körében is. Egy közelmúltbeli tanulmány szerint azok a KKV-k, akik pártolják a saját eszközök munkahelyi használatát, az elmúlt évben 40 százalékkal nagyobb bevételnövekedést értek el, mint azok, akik ezt nem támogatják. Véleményem szerint a vállalatok a többiektől való lemaradást kockáztatják a BYOD elutasításával, és szerencsére a kis- és középvállalatok részéről is egyre többen ismerik fel a BYOD jelentőségét, amelynek bevezetéséhez nem feltétlenül szükséges szerteágazó IT-infrastruktúra és külön IT-részleg.

A bevezetést azonban jobb szabályozottan csinálni: proaktívan, tervek segítségével ösztönözni a munkatársakat saját mobileszközeik használatára. A proaktív bevezetési tervben nagyon fontos tisztázni, milyen célokra használnák az eszközöket, milyen eszközök vannak már jelenleg is használatban, milyen operációs rendszereket támogat a cég, a munkatársak milyen módon férnek hozzá távolról a vállalati adatokhoz, illetve hogy ezeket az adatokat és magát a hálózatot hogyan védik meg az illetéktelen hozzáférésektől. Fontos meghatározni azt is, a BYOD bevezetésekor milyen alapokon szabványosítják a használható mobileszközöket. Ennek egyik leghatékonyabb módja, ha a használt operációs rendszer típusa alapján határozzák meg, milyen eszközökkel dolgozhatnak kollégáik. Ha azonban egy olyan eszköz is bekerül a rendszerbe, amelyen nem a támogatott operációs rendszer fut, a Dell partnere, a Good Technology Good For Enterprise nevű szoftvere segít, hogy akár iOS, Android, Windows Mobile vagy Symbian alatt is minden munkatárs hozzáférjen a szükséges adatokhoz.

A Dell az asztali- és táblagépek, valamint a laptopok terén is választ ad a BYOD kihívásaira: az új XPS modellek a fogyasztók által elvárt teljesítményt és kialakítást a vállalatok által elvárt biztonsági és felügyeleti szolgáltatásokkal ötvözik. Az XPS 10, az XPS Duo 12 és az XPS One 27 modellek a BYOD-mozgalom alapgondolatait, valamint a fogyasztói és vállalati ügyfelek körében végzett felmérések eredményeit ötvözik, így a formaterv, a kialakítás és a felhasználói élmény szempontjából egyaránt mérföldkövet jelentenek. Ezen kívül a Dell teljes termékportfóliójával is támogatja a BYOD-mozgalmat – az adattároló központoktól egészen a végfelhasználók számára szánt számítástechnikai eszközökig.

[HÍRMOZAIK]

BYOD / A NetIQ Novell SUSE Magyarországi Képviselet felmérése kimutatta, hogy a hazai vállalatok a mobileszközök használata kapcsán az adatok védelme és a megfelelőségi előírások teljesítése miatt aggódnak leginkább. Az összes fontosabb platformot és rendszert támogató Novell ZENworks Mobile Management teljes körű megoldást kínál a mobileszközök használatából adódó biztonsági, eszköz- és alkalmazásfelügyeleti, leltárkezelési, illetve megfelelőségi problémákra.

A SAS A LEGJOBB / A Great Place to Work intézet idén is összeállította a világ legjobb multinacionális munkahelyeinek rangsorát, amelynek élére az üzleti analitikai megoldások vezető szállítójának számító SAS került. A budapesti irodával is rendelkező vállalat az inspiráló munka, a nyitott kommunikáció, a juttatások, valamint a magánélet és a munka egyensúlyának megteremtésére tett erőfeszítései miatt bizonyult a legjobbnak.

EXTRÉM / A HP tovább bővítette nyolcadik generációs HP ProLiant (Gen8) portfólióját. Az új szerverek soha nem látott processzorteljesítménnyel gyorsítják a vezető kormányzati, tudományos és ipari intézmények fejlett kutatási tevékenységét.

HÁROM SZINTEN

Hatékony szoftverek a keményedő üzleti világban

Két vezető üzleti és informatikai tanácsadó cég, a Provice és a Telvice Kft. – a Computerworld és CIO.hu szervezésében – szakmai összejövetelén a Compuware szoftvereinek gyakorlati hasznosítását mutatta be két magyarországi nagyvállalat tapasztalatain keresztül. /Computerworld

A Compuware detroiti székhelyű szoftverfejlesztő társaság többek között olyan szoftvereket kínál a vállalatoknak, amelyek segítenek a stratégiai célok elérésében. Mint *Veréb Elemér*, a Provice ügyvezetője elmondta, az utóbbi években – részben a válság hatására – gyors változásoknak lehettünk tanúi. A vállalatok egyre komplexebb módon működnek, egyre nagyobbak az üzleti igények (azaz többet és gyorsabban kell teljesíteni), az informatikával szemben nőnek a felhasználói igények, és az IT-től egyben nagyobb teljesítményt várnak el kevesebb pénzért. Egy portál esetén a szempillantásnyi idő alatt érkező válasz (ami 0,4 szekundumnak felel meg) már kevés, s akkor következik be a felhasználók számára érzékelhető javulás, ha ennek csak a felére van szükség. A Compuware termékei segítenek megfelelni az ilyenfajta kihívásoknak is.

A lassulás gyors felszámolása

Melegh Csanád, a Raiffeisen Bank alkalmazás-üzemeltetési osztályának vezetője a pénzintézet Java-alapú portálrendszerénél jelentkező működési problémák felderítéséről és kijavításáról beszélt előadásában, amelyhez a Compuware DynaTrace szoftverét használták fel.

A portálrendszer hosszú évek fejlesztéseinek eredményeként alakult ki, így sok komponensből áll, sok klasztertagot tartalmaz, sok rétege van – azaz elég bonyolult ahhoz, hogy egy-egy (néha rendkívül súlyos lassulást okozó) hiba elbújhasson benne. Ennek megtalálása és kijavítása ezért hatalmas feladat volt. A rendszer lassulását először a felhasználók, majd a belső munkatársak is jelezték, de az ellenőrző rendszerek minden szegmensben azt mutatták, hogy a működés rendben van. Nem tudták kideríteni, hogy mi a hiba, s utólagos elemzésre kényszerültek a hiba fellépésekor készített memóriaképek, a rögzített logok, a hardverteljesítmény-adatok és az emberi hibák felmérése alapján.

Akkor értek csak el áttörést, amikor külön munkacsoportot állítottak fel a baj okának feltárására és kijavítására olyan szakemberekből, akiknek korábban nem volt közük a fejlesztéshez, illetve beszerezték azt az eszközt (a DynaTrace-t), amely lehetővé tette a folyamatok nyomonkövetését és analizálását.

A DynaTrace installálása után az ágense beépül a felügyelt környezetbe, a szerverről minden információt begyűjt, képes követni a klasztereken áthaladó folyamatokat, figyeli az egymást hívó rendszereket, majd rögzíti és egy szerverre küldi tovább a megszerzett adatokat, ahol lehetővé válik az elemzés. Akár hosszú időre is vissza lehet tekinteni, s trendek kiszűrésére, változásaik megfigyelésére is mód van. A fejlesztő ezekből az adatokból már meg tudja állapítani, hogy a rendszer egy adott időpontban milyen hibát produkált. Nem kell reprodukálni semmit, hiszen az eredeti hiba adatait kapja kézhez, ami lehetővé teszi a gyors javítást is.

A hibakeresés az eszköz alkalmazásával a 30-szorosára gyorsult, ahogy az átlagos válaszidő is sokkal gyorsabb lett – például a portál login-időigénye 12-14 másodpercről 4-5-re csökkent. Végül 20-30 százalékos teljesítménynövekedést értek el kevesebb erőforrás felhasználásával. Ráadásul a fejlesztés minősége is javult, hiszen már a fejlesztés fázisában is tesztelhetővé váltak a kódok, azaz hibás kód az éles rendszerbe gyakorlatilag nem kerülhet be.

Egyedül nem megy

Sárközi László, a Telenor fejlesztési portfóliómenedzsment osztályának vezetője egy másik Compuware-eszköz, a Changepoint üzleti portfóliómenedzsment-rendszer alkalmazásának tapasztalatairól beszélt. A Telenor már hosszú ideje működteti központi projektirodáját, ahol főállású projektmenedzserek dolgoznak 40-50 különféle méretű, párhuzamosan futó projekt irányításán. Emellett számos kisebb, a projektméret alatt maradó fejlesztésről is gondoskodniuk kell. Ahhoz, hogy az erőforrásaikat jól ki tudják használni, szükségük van rá, hogy a vállalat igényeit és a fejlesztési feltételeket felülről, áttekintő nézetből is szemügyre vehessék. Korábban egy egyedi fejlesztésű projektportfólió-menedzsment (PPM) alkalmazást használtak. Ez integrált rendszerek sokaságát jelentette, de még így sem volt megoldva az emberi erőforrás-menedzsment a rendszerben.

A saját fejlesztést az indokolta, hogy a piacon sokáig nem volt olyan fejlett eszköz, amely az igényeiknek megfelelt volna, s minden egyes piaci keresgélés után arra jutottak, hogy az egyedi fejlesztés még mindig hatékonyabb lesz. Aztán a nagy szoftvercégek felismerték, hogy ez ugyan nem egy nagy piac, de a bonyolult struktúrájú nagyobb vállalatok életében a PPM-szoftverek nagyon fontos szerepet játszhatnak, ami hirtelen fejlődést hozott a kínálatban. Kiderült, hogy egy olyan szoftver megvásárlása, amely mindazt tudja, amit az egyedi rendszerük, és még egy sor másik lehetőséget is megnyit számukra, kevesebbe kerül, mint a régi rendszer további szükséges fejlesztései.

A Changepoint három szinten fogja össze és jeleníti meg a szervezet működését. A vezetői szinten, ahol a szervezet teljes működése egy pillanat alatt áttekinthető; az üzleti folyamatok szintjén, ahol az átláthatóság elérése és a hatékonyság növelése a fontos; illetve a munkavégzés szintjén, az egyéni- és csoportmunka-menedzsmentben. A rendszer ráadásul integrálható más rendszerekkel, például a Telenor által is használt SAP, OpenText megoldásokkal.

A Telenornál a rendszernek mintegy 300 felhasználója van, amelyből 100 projektvezető, s közülük 20-an kifejezetten nagy projektekkel foglalkoznak. A felhasználók nem csak IT-sek, hanem hálózatüzemeltetési szakemberek és üzleti felhasználók, például termékmenedzserek. De ebben a rendszerben tudják nyomon követni a kisebb fejlesztések alakulását is.

A rendszer képességeit még messze nem használják ki, további lépések következnek (például az emberi erőforrás-menedzsment-rendszer régóta tervezett bevezetése, illetve a termékfejlesztési folyamatok megtámogatása). De ezek javarészéhez nem kellenek külön fejlesztések, ahogy az eddig alkalmazott funkciók bevezetésének túlnyomó többsége (mintegy 90 százalékához) is installálással és konfigurálással történt, azaz a Changepoint eleve tartalmazta a szükséges funkciókat. Emiatt a rendszer gyorsan használatba vehető. Részben a magyar tapasztalatok alapján a Changepoint a Telenor Groupnál is standard alkalmazás lesz, amelynek a bevezetése a cég 11 országot lefedő hálózatában hamarosan megkezdődik, valószínűleg magyar szakemberek közreműködésével.

ELSZIGETELŐDÉS ELLEN

Nemzetközi szabvány lett a web-akadálymentesítési útmutató

COMPUTERWORLD / A World Wide Web Konzorcium (W3C), a Nemzetközi Szabványügyi Szervezet és a Nemzetközi Elektrotechnikai Bizottság jóváhagyta a Web Akadálymentesítési Útmutató 2.0 (WCAG 2.0) szabvánnyá minősítését. A döntés jelentőségét az adja, hogy hatására felgyorsulhat a WCAG 2.0 használatának elterjedése, ezáltal csökkenhet a látássérült emberek internetes elszigetelődése.

Az ENSZ fogyatékkal élő emberek jogaira vonatkozó előírásainak betartása érdekében egyre több ország keresett olyan megoldásokat, amelyek elősegítik az infokommunikációs akadálymentesítést. A WCAG 2.0-t már a jóváhagyása előtt is számos kormány és szervezet alkalmazta vagy tekintette hivatkozási alapnak. A WCAG 2.0-t először 2011 októberében terjesztették elő a nyilvánosan hozzáférhető előírások közé történő felvételre.

Jeff Jaffe, a W3C ügyvezető igazgatója abban látja az útmutató szabvánnyá minősítésének jelentőségét, hogy mostantól az eddiginél is ismertebbé és a gyakorlati alkalmazásban elterjedtebbé válik ez a rendkívül fontos dokumentum.

„A szabvánnyá válás új utakat nyit az akadálymentesítési technológiák és útmutatók alkalmazásában" – mondta *Judy Brewer*, a Webes Akadálymentesítés Kezdeményezés (Web Accessibility Initiative -WAI) igazgatója. „Több országban az előírás, hogy az államigazgatásban használt technikai szabványoknak ISO/IEC által minősítetteknek kell lenniük. A döntés gyorsítja a WCAG 2.0 használatának elterjedését, csökkenti a fogyatékkal élők internetes elszigetelődését, és elősegíti az együttműködést a világháló összes használója között. Bízunk abban, hogy Magyarországon is egyre több intézmény és szervezet követi a 2012-es Nemzetközi Fehér Bot napján szabvánnyá minősített WCAG 2.0 előírásait honlapjának megtervezésekor."

ORSZÁGOS PROGRAM

Zökkenőmentesen halad a digitális átállás

Az alapos előkészítés eredményeként a terveknek és a jogszabályoknak megfelelően, jó ütemben halad a digitális átállás folyamata Magyarországon. /Computerworld

A Digitális Átállás Támogatási Program keretében az önkormányzatoknak már több mint kétharmada rendelkezésre bocsátotta a rászorulók adatait, ami ahhoz szükséges, hogy a Nemzeti Média- és Hírközlési Hatóság (NMHH) minden jogosult számára ingyenesen beszerelhesse a digitális adások vételéhez szükséges berendezéseket.

Az NMHH feladata, hogy az információkhoz való hozzáférést televíziókészülékeken keresztül is egyenlő eséllyel tegye elérhetővé mindenki számára. Önhibáján kívül senki nem maradhat televízióadás nélkül, sehol nem sötétülhet el egyetlen tévéképernyő sem.

A Nemzeti Média- és Hírközlési Hatóság Digitális Átállás Tesztprogramja keretében Sopronban és a Barcsi kistérségben – a helyi önkormányzatok és az Antenna Hungária Zrt. együttműködése mellett – októberben sikeresen megvalósította az átállást. Az országos programot az NMHH a tesztprogram során szerzett tapasztalatok birtokában indította el.

A digitális átállásban elsődlegesen 570 ezer háztartás érintett, ami azt jelenti, hogy ezekben kizárólag analóg, tető- vagy szobaantennával televíziónak. További 100 ezer háztartásban a digitális átállás megtörtént, de itt van olyan tévékészülék is – például a nyaralókban –, amelyen analóg módon nézhetők az országos földfelszíni csatornák, azaz az M1, az RTL Klub és a TV2. Ez utóbbiak a másodlagosan érintett háztartások.

Körülbelül 57 ezer olyan háztartás van, amely szociálisan rászorulónak számít. Az ezekben élők önerejükből nem, vagy csak jelentős anyagi áldozatok vállalásával tudják beszerezni azokat a műszaki eszközöket, amelyekhez a digitális tévézéshez szükség van.

Ezekre a háztartásokra az NMHH kiemelt figyelmet fordít: megvásárolja számukra a szükséges berendezéseket és ingyen beszerelteti, vagy számukra egy előfizetéses kedvezményes programcsomagot ajánl fel.

A digitális átállásnak 2014. december 31-ig kell megvalósulnia.

A legnagyobb biztonsági kockázatokat változatlanul a cég munkatársai jelentik, akik többnyire véletlenül nyitnak rést a biztonsági rendszeren.

A félelem százmilliárdja

A világgazdaság lassulása az IT-költségvetéseket alacsonyabb szintre szorítja vissza, de ez nem érinti a biztonsági kiadásokat, mert a kártevők és a kiberbűnözés elleni védelem változatlanul fontos prioritása marad a cégeknek. Annál is inkább, mert a technológiai változások nagy trendjei (konzumerizáció, számítási felhők, nagy adat stb.) még hangsúlyosabbá teszik a céges adatok és tartalmak megóvásának fontosságát.

MEIXNER ZOLTÁN

A globális kiberbiztonsági piac mérete – 11,3 százalékos éves növekedés mellett – 2017-re elérheti a 120 milliárd dollárt, állítja a dallasi MarketsandMarkets (M&M) piackutató cég. Egy másik, kissé szerényebb becslés szerint viszont az idén várhatóan 60 milliárd dollárt költ a világ informatikai biztonságra, ami 8,4 százalékkal haladja meg a 2011-es 55 milliárdot. Sőt a Gartner piacelemző társaság azt jósolja, hogy a piac tovább bővül majd a következő években, és 2016-ban eléri a 86 milliárd dolláros határt. Akárhogy is, ez rengeteg pénz, amit a félelem mozgat.

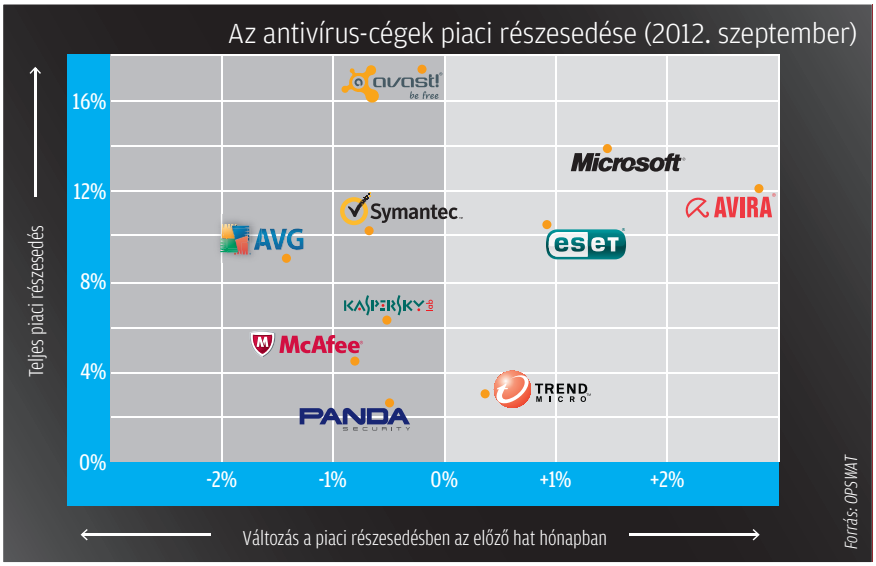
A Gartner a biztonsági infrastruktúra-piacba olyan szoftvereket, szolgáltatásokat és hálózatbiztonsági berendezéseket vett bele, amelyek a vállalati és fogyasztói IT-eszközök védelmére szokás használni. Továbbá számba vette az IT-kiszervezést (menedzselt biztonsági szolgáltatások – MSSP), a biztonságos webes átjárókat (eszközök), és a biztonsági információ- és eseménymenedzsmentet, amelyek a leggyorsabban növekedő biztonsági szegmensek. A felhőalapú biztonsági megoldások iránti kereslet szintén hatást gyakorol a legfontosabb biztonsági piacokra, s a korábban említett bővülés különösen ezen az új platformon keresztül lesz erőteljes.

A Gartner arra számít, hogy a biztonsági termékek és szolgáltatások iránti keresletet az a folyamatos félelem hajtja fel, amelyet az egyre sokszínűbb, célzottabb és kifinomultabb támadások keltenek szerte a világon. Ilyen környezetben a különféle szervezetek és cégek folyamatosan keresik azt a szaktudást és a biztonságtechnikai és szolgáltató cégek támogatását, amellyel csökkenthetik a kockázataikat és mérsékelhetik a sérülékenységüket.

Egy másik piacelemzés – amelyet a Trustwave készített – szintén a piac bővülését vetíti előre. A következő fontos részleteket tárták fel a kutatás során:

- A fogyasztói adatok értékes célpontjai maradnak a kiberbűnözők támadásainak, a felderített sérült adatok 89 százaléka e körbe tartozik.
- Már második éve, hogy az élelmiszeripar területén regisztrálják a legtöbb támadást, a felderített esetek mintegy 44 százaléka innen származik.
- A franchise-hálózatokat működtető iparágak jelentik az új fontos célpontokat, már tavaly is több mint a támadások egyharmada ide irányult.
- Az incidensek 76 százalékánál azt találták a vizsgálatok, hogy az üzleti környezet fejlesztéséért, fenntartásáért és támogatásáért felelős külső szervezet ismerte a biztonsági hiányosságokat.
- A jogsértések növekedési üteme a 2010-es 7 százalékról tavaly 33 százalékra emelkedett.
- Az adatgyűjtési technikák továbbra is az áldozatok környezetében zajló adatforgalomra fókuszálnak, s az ebben elkövetett támadások aránya tavaly 62,5 százalék volt.

- Az antivírus-eszközökkel felfedezett támadások kevesebb mint 12 százaléka kötődik olyan kártevőkhöz, amelyeket 2011-ben azonosítottak.
- A webes támadások, SQL-behatolások maradtak az első számú támadási módszerek már negyedik éve.
- A legközönségesebb jelszó a globális üzletben a „Password1" maradt, ami megfelel az alapértelmezett Microsoft Active Directory beállításnak.



Annak érdekében, hogy a cégek javíthassák biztonsági helyzetüket, a Trustwave azt ajánlja, hogy a szakemberek hat területre különösen komoly figyelmet fordítsanak.

A munkatársak oktatása. A legjobb behatolásazonosító rendszert nem a biztonsági szakértők és nem a drága technológiák adják, hanem a munkatársak. A biztonsági felvilágosítás gyakran az első vonalát jelenti a védekezésnek.

A felhasználók azonosítása. Egy olyan állapot elérésére kell törekedni, amelyben minden felhasználók által kezdeményezett művelet azonosítható és hozzákötheto egy adott személyhez.

A hardverek és szoftverek homogenizálása. A vállalati számítógéppark fragmentáltsága a biztonság komoly ellensége. E káosz felszámolása a hardverek és szoftverek szabványosításán keresztül, valamint az öreg rendszerek üzemen kívül helyezése homogén környezetet hoz létre, amelyet könnyebb menedzselni és biztonságban megtartani.

Az eszközök regisztrációja. Az eszközök komplett felleltározása vagy nyilvántartásba vétele segít felfedezni a kártevők jelenlétét vagy a rosszindulatú támadásokat.

A tevékenységnaplók egységesítése. A fizikai és a digitális világ megoldásainak kombinálásával a szervezetek olyan új lehetőségekhez jutnak, amelyek segítségével gyorsabban lehet azonosítani a biztonsági eseményeket.

Az események vizualizációja. A logbejegyzések felülvizsgálata önmagában már nem elég hatékony. A vizualizációs módszerek jól segítik a biztonsági események felderítését – különösen a szűk biztonsági résekben.

Ezek után a Trustwave egész világra kiterjedő konklúziója a következő: bármilyen vállalkozás vagy üzlet a támadás célpontja lehet. Azok a cégek különösen nagy veszélyben vannak, amelyek sok fogyasztó adatait tartják nyilván, s ahová az ügyfelek, vásárlók, felhasználók gyakran visszatérnek: éttermek, kiskereskedelmi üzletek és szállodák. A veszély még nagyobb, ha ezek valamilyen hálózatnak a részei vagy láncot alkotva dolgoznak. Amire ezért feltétlenül fókuszálni kell, az a dolgozók biztonsági felvilágosítása, az antivírusszoftverek és a tűzfalak alkalmazása. Érdemes továbbá mások szerencsétlenségéből vagy sebezhetőségéből tanulni, és olyan – az imént felsorolt szempontokat is tartalmazó – taktikai és stratégiai változtatásokat végrehajtani, amelyek képesek csökkenteni a biztonságot veszélyeztető események valószínűségét és az ezekből eredő adatvesztést.

TOP 10 fenyegetés 2012

A gyors technológiai változások következtében újfajta fenyegetésekkel is meg kell ismerkednünk. Például korábban elképzelhetetlen volt, hogy egy telefont hálózaton terjedő kártevő fertőzzön meg, ma viszont ez már komoly fejtörést okoz a cégeknél a digitális fenyegetések elhárítására alkalmazott szakembereknek. Nem csoda, hogy ez áll a Booz Allen Hamilton (BAH) tanácsadócég fenyegetési toplistájának élén.

A BIZTONSÁGI SZOFTVERPIAC

Az Opswat szoftvercég negyedévente felmérést készíttet az antivírusszoftverek piacáról. A legutóbbi, szeptemberben kiadott felmérés szerint a cégek versenyében az Avast a világpiac 17,5 százalékát birtokolja, ezzel a stabilan álló részesedéssel a legnagyobb szereplő. Az Avira 2,8 százalékos növekedést produkálva 12,1 százalékos részesedést szerzett, amivel az 1,4 százalékos növekedést produkáló, 13,9 százalékot birtokló Microsoft mögé szorult a harmadik helyre. Az Eset 0,9 százalékot nőtt és 10,6 százalékot birtokol. Az ötödik helyezett Symantecnek 0,7 százalékos piacvesztéssel még mindig 10,2 százalékos a részesedése. Az utóbbi hónapokban általában a nagyobb cégek enyhén erősödtek, a kisebbek pedig gyengültek a részesedését folytatott harcban.
A szoftverek világpiaci versenye nem pontosan tükrözi a szállítók rangsorát, így érdemes erre a listára is rápillantani. A prímet az Avast ingyenes antivírus-program viszi 13,8 százalékos részesedéssel, aztán a Microsoft Security Essentials következik 13,6 százalékkal, majd az Avira ingyenes antivírus-alkalmazás kerek 10 százalékkal, aztán az Eset Nod32 következik 7,1 százalékkal, s az ötödik helyre az AVG antivírus ingyenes kiadása futott be. A tíz között van még a McAfee VirusScan, az Eset Smart Security, a Norton AntiVirus, a Kaspersky Internet Security, és éppen csak kilóg az AVG Anti-Virus. Ez a 11 termék a piac 71 százalékát fedi le.

TOP 10 FELHŐKOCKÁZAT

A Coalfire IT-audit cég értékelése szerint a következők jelentik a legnagyobb fenyegetést a számítási felhőket igénybe vevő cégekre:

1. Lazuló irányítás
A felhő legnagyobb előnye a hagyományos adatközpont-modellel szemben a szolgáltatások könnyebb elérése. De nem tarthatják kézben és szemmel az összes folyamatot azokon a rendszereken, ahol a legértékesebb adataikat tárolják, és a működésükhöz nélkülözhetetlen számos erőforrást – például a folyamatos üzletmenethez nélkülözhetetlen szoftvereket – nyerik.

2. Adatlokáció
A biztonság érdekében a felhőszolgáltatók különböző helyeken működtetnek (redundáns) adatközpontokat. Gyakran több országban is, ahol többféle szabályozás vonatkozik az adatok tárolására és forgalmára. Azok a cégek, amelyek igénybe veszik e szolgáltatásokat (különösen, ha több szolgáltatótól is), sohasem tudhatják, hogy fizikailag hol vannak az adataik, s azok valóban teljes fizikai és jogi biztonságban vannak-e.

3. Megnövekedő támadási felület
A virtualizáció a felhők alaptechnológiája. A felhőszolgáltatók sokféle eszközt használnak az infrastruktúrájuk működtetésére és karbantartására. A sérülékenységek menedzselésének komplexitása egyre nő, s új szoftverek sora kerül be az IT-környezetbe, s ezek persze új támadási felületet is hoznak magukkal.

4. Adattulajdonlás
Aki a felhőben helyezi el az adatait – hacsak nem jár el igen gondosan és szigorúan a szerződéskötéskor –, beleütközhet, hogy olyan adatokat, amelyeket a sajátjának gondolt,

1. A mobileszközök számának exponenciális növekedése növeli a biztonsági kockázatokat
Minden okostelefon, tablet, vagy másféle mobileszköz újabb ablakot nyit a kibertámadásoknak, s mindegyik egy újabb sérülékenységi pontot jelent, ahol be lehet hatolni a hálózatba. Ezért a BAH szerint semmiféle adatforgalmat nem szabad megengedni ezeken az eszközökön, kivéve, ha monitoringszoftverrel vannak ellátva. Ugyanakkor ezeket a „konténer"szoftvereket, amelyek hatékonyan elkülöníthetik a magántartalmú kommunikációt az üzletitől, még a legnagyobb cégek (például SAP vagy RIM) is csak most fejlesztik.

2. Növekszik a felsővezetők támadásának esélye
A szenior döntéshozók korábban elszigetelhették magukat a külvilágtól, de ma már online látszanak, azaz célba is lehet venni őket. A cégeknek figyelni kell rá, hogy a hackereknek komplett profiljaik vannak a felsővezetői garnitúrákról, sőt a kezük alá dolgozó munkatársaikról is, akiken keresztül elérhetik őket. Ezért ki kell képezni a vezetőket, hogy ne osszanak meg személyes információkat a közösségi médiában vagy más nyilvános weboldalakon. A „social engineering" veszélye miatt szűrjenek minden felsővezetőkhöz beérkező elektronikus küldeményt, még akkor is, ha látszólag jól ismert forrásból jön.

3. A közösségi média használatának terjedése hozzájárul a személyes fenyegetettséghez
Egy profil vagy komment a közösségi médiában (még a vezérigazgató rokonaitól is) segíthet a hackereknek felépíteni egy olyan információs portfóliót, amely megkönnyíthet egy jövőbeli támadást.

Ezért a vezető tisztségviselőknek és hozzátartozóiknak nem szabad nyilvános oldalakon olyan információt közölniük, amelyből kiderülhet bármi, ami igénybe vehető profilok építéséhez vagy jelszavak és egyéb hitelesítő hozzáférési információk kitalálásához. A vezetőkről el kell távolítani minden új információt, s ennek érdekében monitorozó szoftvereket érdemes használni.

4. Ha a cég már megfertőződött, meg kell tanulni együtt élni vele
A biztonsági fenyegetések mára olyan kiterjedté váltak, hogy képtelenség a teljes védelem. A kiberbiztonsági taktikák fókusza mindinkább a helyet belső elemzésére, a kártevők, támadók detektálására és a rendszerből kiszorítására irányul. Ezért több időt kell fordítani a belső kommunikáció szűrésére. Állandóan szkennelni kell a céges hálózat szervereit a meghatározatlan eredetű fájlok felkutatására vagy szoftverkódok töredékei után, és igyekezni kitalálni a taktikákat, ahogy az illegális kódokat a tűzfal mögé juttathatják.

5. Minden, ami fizikai – digitális lehet
Egy kézzel írt feljegyzést tartalmazó darab papír a szemétkosárból, egy kép a falon vagy egy jelentés fedőlapja is reprodukálható digitális formában, s ez máris lehetőséget ad a hackereknek a biztonságot sértő lépésekre. S ez a probléma, amikor minden telefonban van fényképezőgép, videófelvevő és hangrögzítő, egyre erőteljesebb. Ez ellen csak a tájékoztatás véd igazán. Arról nem is beszélve, hogy nem szabad a képernyőn bizalmas információkat hagyni, de még az email-kliens sem maradhat nyitva, amelyen látszik, hogy kiktől érkeztek be levelek. Mert ami nem szerezhető meg online, az megkaparintható offline.

6. Egyre több cég használ számítási felhőket
A jelentős költségmegtakarítás és hatékonyságnövekedés miatt a cégek szívesen költöztetik adataikat a felhőkbe, s vesznek igénybe felhőalapú szolgáltatásokat. A jól megtervezett architektúra és a biztonsági tervezés lehetővé teszi a vállalatoknak, hogy hatékonyan menedzseljék a felhők jelentette biztonsági kockázatokat. Ennek érdekében szükség van biztonsági „cellák" létrehozására, ahol el lehet helyezni az értékes algoritmusokat, érzékeny adatokat stb. Ezekre a védett szerverekre csak különösen magas szintű hozzáférésvédelemmel (például két külön felhasználó együttes jelenléte mellett és biometrikus azonosítással) és titkosítási kulcsok használatával lehessen belépni.

7. A globális rendszerkockázat a kiberkockázatokat is tartalmazni fogja
Ahogy a bankok és befektetési cégek tovább haladnak a globalizációs úton, mindinkább össze lesznek kötve egymással. A biztonsági sérülések egyetlen cégnél rendszerszintű veszéllyé növekedhetnek a pénzügyi piacokon, s ezen keresztül az egész világgazdaságban. Emiatt szűrni kell a bejövő üzeneteket a bankok SWIFT vagy FIX tranzakciós rendszereiben, mint ahogy az e-mail-

egyszer csak mások is elkezdenek használni. Nem kizárt, hogy például egy cég felhőbe telepített levelezési rendszeréből kinyert listák alapján valaki más marketingkampányba kezdjen, vagy a megszerzett adatokat, s a belőlük képzett profilokat felhasználják hirdetési tevékenységhez.

5. Gyenge láthatóság a virtuális hálózatokon

A hálózatok monitorozása tipikusan olyan eszközökkel történik, amelyek fizikailag létező hálózatokra fejlesztettek ki. A felhőszolgáltatók azonban előszeretettel virtualizálják a rendszereiket, s a rajtuk zajló forgalmat és az esetleges támadásokat ezért igen nehéz virtuális szerverről virtuális szerverre követni.

6. Identitásegyesítés

A felhasználóknak szükségük van rá, hogy a házon belül és kívül egyaránt hozzáférjenek a munkaanyagaikhoz, méghozzá ugyanazokkal az azonosítókkal. Amikor ezt lehetővé teszik számukra, azt identitásegyesítésnek nevezik. A folyamat, amelyek a két különböző (külső és belső) azonosítási rendszer együttműködését teremti meg, lehetőséget adhat a támadásra.

7. Új támadási irányok

A különféle szervezetek virtuális szerverei ugyanazon a fizikai hardveren futhatnak. Ez a többfelhasználós gépbérleti szisztéma olyan új sérülékenységet teremthet a rendszeren, amely egyébként nem jelenhetne meg. Ha ugyanis egy virtuális szerver sérül, arról a támadó átveheti az uralmat a fizikai eszköz felett, s továbbléphet a rajta futó többi rendszer felé.

8. Értékkoncentráció

A nagy felhőszolgáltatók adatközpontjaiban egyre több értékes adat halmozódik fel különféle megbízóktól. Ez önmagában is egyre értékesebb célponttá teszi ezeket a létesítményeket. És nem minden szolgáltatónak vannak meg az eszközei, hogy megvédje őket a rosszindulatú és nagyon felkészült támadások ellen.

9. Bukik a szolgáltató

A felhőszolgáltatás is csak olyan üzlet, mint a többi. Lehet vele nagy profitot elérni, és csődbe is lehet jutni. Kisebb leállásokat még csak képes túlélni, amelyeket egy-egy programhiba vagy egy ügyfél elleni hackertámadás okoz, hiszen a redundáns rendszerek áthidalják a bajt. De amikor már egy-egy hosszú leállás veszteséget okoz az ügyfeleknek is, hamar megindulhat – és akár káoszba is torkollhat a menekülési hullám.

10 Gyengülő ellenőrzés

A monitorozás a támadásra való reakció alapeszköze, hiszen ebből ismerhető a hálózat pillanatnyi állapota. Ha nem elég erős a monitoringrendszer, az megnehezíti a rendszerhibák felderítését és a szisztematikus nyomozást. A szolgáltatók ugyan elvégzik ezt a tevékenységet, de nem oszthatják meg az eredményeiket, mert más ügyfelek adatait is kiadnák vele. Ezért a támadások alapos felderítése is nehézkesebbé válhat.

eket ellenőrzik. Sőt ismeretlen programkódok, ismeretlen formattálási üzenetek, ismeretlen csatolmányok után kell kutatni a legváratlanabb helyeken is. Szűrni kell a kereskedelmi partnerektől, piaci adatkereskedőktől és más ismert együttműködő cégektől érkező adatforgalmat, és ugyanezt kell tenni sokkal keményebben a cégeken belül is. Auditálni kell a biztonsági eljárásokat bármiféle csereügylet esetében azoknál a partnereknél, akiknek a cég megengedi, hogy kapcsolatba lépjen a hálózatával.

8. Mutációk: a szervezett támadások száma és ereje tovább nő

Nemcsak a gonosz és alattomos vírusok mutálódnak, hanem azok az eszközök is fejlődnek és változnak, amelyeket a számítógépes bűnözők használnak, így a régi védelmi megoldások haszontalanok. A vállalkozásoknak fel kell készülniük, hogy gyorsan alkalmazkodjanak a kibertéren át támadó ellenségeikhez, például a friss kibocsátású, nulladik napjukon támadó rosszindulatú programok ellen is védve legyenek, mert ezt a taktikai fegyvert a szervezett bűnözés és különféle országok ügynökségei növekvő mértékben használják.

Olyan eszközök használatára van szükség, amelyek kutatják és felismerik a rosszindulatú szoftvereket. Belső erőforrásokat kell szánni a kibertér trendjeinek figyelésére, hogy átláthatóvá váljanak a gyakran kiválóan képzett és felkészült hackerek megállítására. Gyakran olyan szoftvereket kell kiszűrni, amelyek korábban ismeretlenek voltak, s esetenként hónapokat vagy éveket töltöttek a támadók a csiszolgatásukkal.

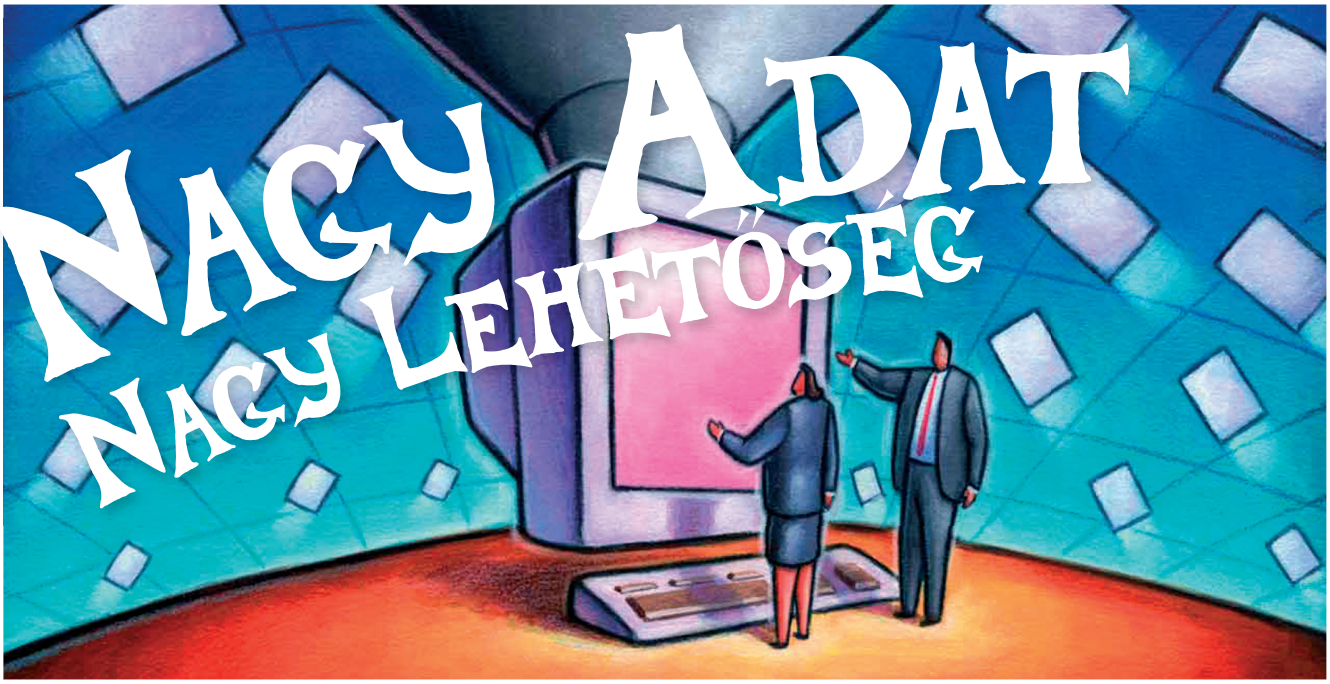
9. A belső fenyegetés maga a realitás

A legnagyobb biztonsági kockázatokat változatlanul a cég munkatársai jelentik, akik többnyire véletlenül nyitnak rést a biztonsági rendszeren, ahol a türelmesen várakozó támadó bekerülhet a külső védelem mögé – s ezzel további támadásokhoz nyithat kapukat vagy szerezhet meg értékes információkat.

Emiatt az alkalmazottakat rendszeresen biztonsági oktatásban kell részesíteni, és belső monitorozással fel kell deríteni a véletlen vagy szándékos belső rendszersértéseket. Az adatokat a cégeknek osztályozniuk kell az értékük szerint, hogy a legértékesebb adatokat csak a legilletékesebbek érhessék el. Egy szint felett már biometrikus azonosítás és más szigorú eljárások alkalmazása is indokolt lehet. Az értékes adatok elérésére tett kísérleteket pedig biztonsági rendszereknek kell folyamatosan figyelemmel kísérni.

10. Egyre nagyobb szigor az ellenőrzésben

A növekvő fenyegetések a különféle szervezeteket, például kormányhivatalokat és az üzleti szféra szereplőit – különösen a nagy és hálózatban dolgozó vállalatokat – arra kényszerítik, hogy szigorúbb szabályokat és ellenőrzési rendszert vezessenek be. A Nemzetközi Szabványügyi Hatóság (ISO) és a Nemzetközi Elektrotechnikai Bizottság (IEC) biztonsági szabványai lefedik minden iparág követelményeit. Az ISO/IEC 20002-es szabvány alkalmazása a nagyobb szervezeteknél ma már biztonsági alapkövetelmény, a mellőzése önmagában is veszélyes.



Nagy Adat
Nagy Lehetőség

A világ legnagyobb, adattárházakra és vállalati elemzőrendszerekre szakosodott vállalata, a Teradata idén is megrendezte a Teradata User Group Konferenciát. A Bécsben tartott konferencia fő témája természetesen a Big Data, az abban rejlő lehetőségek és azok kiaknázása volt.

PAVLOVIC JOVAN

Elsőként *Gerd Gabriel* lépett a mikrofon mögé, kifejtve, hogy a Teradata kicsivel több mint öt éve lett független az NCR-tól, és a menedzsment azóta sem bánta meg a szétválást. Az elmúlt 5 év alatt a bevételek nőttek, a cég dolgozóinak száma majdnem megduplázódott, akárcsak az ügyfeleké, és a fél évtized alatt 2600 implementációt szállítottak le a világ 71 országába. Gabriel mindezen eredményekért köszönetet mondott a Teradata ügyfeleinek, mert szerinte nélkülük, az ő hitük nélkül ez nem lett volna lehetséges.

Innováció, mint hajtóerő

Az első előadást *Boris Nemsic*, a Delta Partners dubai ügyvezetője tartotta, aki a telekommunikációs piac jövőjéről beszélt. Mint elmondta, az új digitális korban a telekom cégeknek muszáj lesz változniuk, mert jelenlegi megítélésük többnyire negatív. Egy új vásárlói csoport van felnövekvőben, akik számára az adat, a telekommunikáció, az informatika olyan természetes, mint mondjuk a fogkefe használata. A cégeknek ehhez a változó környezethez kell igazodniuk, ha fenn akarnak maradni.

A média területén ez a dominancia egyértelmű. Napjainkban több mint egymilliárd aktív Facebook-felhasználó van, akiknek egy jelentős része mobileszközt használ a közösségi hálózatok eléréséhez. Példának hozta fel a közel 8 és félmillió lakossal rendelkező Ausztriát, ahol a mobilpenetráció eléri a 150%-ot, és a lakosság 80%-a aktív internetfelhasználó. Minden második ember használja a Wikipédiát, aminek adatait megbízhatónak találják, az országban több mint 5000 blogger van, és a lakosság 19%-a birtokol tabletet.

Nemsic idézte a Cisco felmérését, amely szerint ma már a legyártott mobiltelefonok száma nagyobb, mint a Földön élő embereké. És ezeknek a készülékeknek egy jelentős része okostelefon, elsősorban androidos készülék vagy iPhone. Az nem meglepő, hogy ezek a mobil készülékek rengeteg adatot termelnek, az már sokkal inkább, hogy az adatok 80%-át a négy nagy, a Facebook, a Google, az Amazon és az Apple termeli. Az ok az IT innovációja.

A nagy innovációk közös jellemzője, hogy maradandó hatással vannak a társadalomra, hatásukra új iparágak születnek és generációk életmódja változik meg. Ilyen innováció volt a könyv, az izzó, az autó, a számítógép, a mobiltelefon és az internet. Az innováció járul hozzá talán a legnagyobb mértékben a profit növekedéséhez. Napjainkban a telekommunikációs cégek bevételének 80%-a olyan termékekből származik, amiket az elmúlt 20 évben találtak fel.

Ami a jövőt illeti, a változás egyre gyorsabb lesz. A civilizáció hajnala óta 2003-ig az emberiség összesen 3,5 exabájt (EB) adatot termelt. 2010-ben ugyanennyi adat termeléséhez 48 órára volt szükség, és 2020-ban egy óra alatt termelődik majd ennyi. A jövő az alkalma-

> A nagy innovációk közös jellemzője, hogy maradandó hatással vannak a társadalomra, hatásukra új iparágak születnek és generációk életmódja változik meg.

zásoké lesz, hiszen ma a világ fele „alkalmazásolható” – noha a technológia 5 éve még nem is létezett.

A jövő zenéje

Ezután *Martin Willcox*, a Teradata marketingigazgatója vette át a szót, és röviden vázolta a Teradata technológiai stratégiáját, valamint ismertette azokat a főbb területeket, melyekre a Teradata K&F fókuszál. Mint azt elmondta, az idei Teradata Partners konferencián jelentették be a Unified Data Architecture-t, egy új, egységes keretrendszert, ami a Teradata adattárházas technológiája mellett a tavaly felvásárolt Aster Data analitikai képességeit és a Hadoopot foglalja magában.

A Teradata ügyfelei között több olyan vállalat is van, akiknek adattárházában több mint egy petabájt adat található. De ez a rengeteg adat mit sem ér, ha nem képesek feldolgozni. Az SQL-H az elemzők és az adattudósok számára kínál egyszerűbb megoldást a Hadoopban tárolt adatok elemzésére. Egyszerűsíti az adatelérést, nincs szükség programozói tudásra, hogy bármihez hozzáférjen az ember.

Bemutatták továbbá a Teradata Big Analytics Appliance-t, ami az első ilyen berendezés az iparágban. A hatékonyabb felhasználás érdekében a Teradata egy szervertoronyba tette az Astert és a Hadoopot. De szóba került a Teradata Data Labs is, aminek segítségével könnyedén le lehet tesztelni az új ötleteket.

Megatrend

Willcox ezek után rátért a jövő megatrendjeire: ezek szerint a globalizáció hatására egyre gyorsabban egyre összetettebbé válik az üzletmenet, az internet – különös tekintettel a közösségi hálózatokra – egyre nagyobb szerepet tölt be a mindennapi életben. A „szenzorkonómia” jelenségnek köszönhetően a több billió összekötött gép adatok petabájtjait termeli majd. Nagyon fontossá válik majd a „zöld IT” is.

A Teradata jövőjéről szólva megemlítette az intelligens memóriát, ami bár konvencionálisan nem tárolótechnológia, de jelenleg sokkal gyorsabb, mint az SSD. Persze a tárolt adatoknak kellően értékeseknek kell lenniük, hogy igazolják a nagyösszegű befektetést. Végezetül elmondta, hogy legalább egy új „feldolgozó motor” érkezik valamelyik Aster platformra a közeljövőben.

Duncan Ross, a Teradata adattudósa elmondta, hogy a Big Data továbbra is egyike lesz a legfelkapottabb témáknak az informatikában, hiszen a döntések meghozatalakor nem elég, ha megérzésekre hagyatkozik az ember, szükség van az adatokra és a statisztikákra. A cégeknek meg kell tudniuk, hol helyezkednek el térben a vevőik, és képesnek kell lenniük megérteni őket.

A Crowdsourcing mellett nagyon fontosnak tartja a nyílt adat fogalmát. A vállalatok kezdik eladni vagy akár csak odaadni adataikat, amiben nagy segítségükre vannak az adatpiacok. Itt egyszerűen lehet értékesíteni vagy megvásárolni az adatokat, ráadásul lehetőség van egyszerre csak keveset venni belőlük, letesztelni, majd az eredmények ismeretében dönteni egy nagyobb beruházás mellett.

Szintén új jelenség a „gamification”, amely során a folyamatokat játékká alakítják – erre kiváló példa a Foursquare. De az adatok segítenek az embereknek saját maguk ellenőrzésében és megfigyelésében is. A különböző életmód-alkalmazások nyomon követik a tulajdonos egészségi állapotát, azt, hogy mit eszik, merre jár, mit csinál – és ezek segítségével analizálják saját viselkedésüket. A jövőben valószínűleg a különböző vállalatok – különösen a telekom cégek – ügyfelei is hozzájuthatnak majd a saját magukra vonatkozó adatokhoz. Ezekkel a kinyert adatokkal azután egyszerűen átsétálhatnak a konkurenciához és megkérdezhetik, mennyit kellene náluk fizetni ugyanezért a tevékenységért.

Mobil

Svilen Stoyanov, a Mobiltel BI vezetője ismertette azokat a trendeket, amik leginkább jellemzőek a telekommunikációs piacra. Az egyre több ügyfél, a növekvő termékportfólió, a termékek magasabb üzemeltetési költsége, a nagyszámú szabályozás mind arra kényszeríti a piaci résztvevőket, hogy rengeteg erőfeszítést fektessenek be a megfelelő tarifacsomagok elkészítésébe. A marketingosztályoknak szükségük van a megfelelő eszközre, ami segíthet előrejelezni a piac reakcióját egy új tarifa bevezetésekor. Ebben segített a Clintworld alkalmazás, aminek segítségével gyorsan piaci előnyhöz jutottak.

Klas Eckervald, a Teradata rendszertervezője előadásában kiemelte, hogy a vállalkozások sokkal több értéket nyerhetnek ki az adattárházakból, ha lehetővé teszik a végfelhasználók számára az elemzés agilisabb megközelítését. Jelenleg az ilyen irányú innováció akadályai lehetnek az adatokhoz történő nehézkes hozzáférés, az integráció, az, hogy jogosultság kell az adatokkal történő műveletekhez, és hogy nem osztják meg az adatokat.

A Teradata Data Lab Analytic Sandboxot úgy tervezték meg, hogy egyszerre tegye lehetővé a szigorú irányítást, ugyanakkor rugalmas legyen. Kísérleti adatokkal lehet dolgozni, és rengeteg felhasználó számára hozzáférhető.

Johannes Rupp, a Teradata vezető tanácsadója bemutatta, milyen módszerekkel lehet az üzleti igényeket BI-irányítópulttá változtatni, míg *Wolfgang Neurauter* tanácsadó a következő nagy dologról, a Mobil BI-ról tartott előadást.

Az üzleti témák mellett párhuzamosan az adattárházak gyakorlati használatával kapcsolatos előadások is zajlottak, utána pedig az érdeklődők kerekasztal-beszélgetéseken vehettek részt, ahol egy-egy témát a szakértők bővebben kifejtettek. Másnap egy félnapos SAS integrációs workshop került megrendezésre.

INTERJÚ

Hálózati kamerák a feltaláló szemével

KIS ENDRE

Az Axis Communications 1996-ban mutatta be a világ első IP kameráját, amely azóta új távlatokat nyitott a megfigyelés, a kapcsolattartás és együttműködés területe mellett olyan vertikumokban is, mint a kereskedelem. A hálózati kamerák jövőjét feltalálójukkal, Martin Grennel, a svéd cég alapítójával fürkésztük.

COMPUTERWORLD: Mielőtt a jövőbe tekintenénk, avassa be olvasóinkat az IP kamera születésének kulisszatitkaiba! Egyetlen ihletett pillanatban vagy hosszabb folyamat eredményeként jutott a felismerésre, hogy a kamerát hálózatra kellene csatlakoztatni?

MARTIN GREN: Abban az időben elsősorban print szervereket készítettünk, melyek legnagyobb piaca Japán volt. Üzleti úton jártam az ázsiai szigetországban, hogy új termékünket, a hálózatra csatlakoztatható CD-ROM-tároló szervert bemutassam, amikor egyik ügyfelünk, aki minden bizonnyal túl nagy raktárkészletet halmozott fel analóg kamerákból, megkérdezte tőlem: ha már mindenféle eszközt hálózatra csatlakoztatunk, a kamerákkal miért nem próbálkozunk?

Ez megragadt bennem, tetszett az ötlet. Odahaza, Svédországban egyik mérnökünk elképzelése viszont az volt, hogy hálózati videókonferencia-rendszer fejlesztésébe kellene beruháznunk. Elkészítettük a prototípust, amely tetszett ugyan, de úgy láttam, hogy a videókonferencia-felszerelés nem illik cégünk értékesítési modelljébe. Ezért javasoltam, hogy a fejlesztést felhasználva készítsünk hálózati kamerát, amelyet sikerrel forgalmazhatunk partnereinken keresztül. A technológia mellett a dolog üzleti oldalát is szem előtt kell tartani.

A szakmai vásárokon, többek között az egyesült királyságbeli IFSEC biztonsági kiállításon persze láttuk, hogy a kamerás megfigyelőrendszerek teljes egészében analóg technológiára épülnek. De a '90-es években már egyértelmű volt, hogy az analóg technológiát digitális váltja fel mind több területen, ezért nagy lehetőséget láttunk az IP kamerában.

CW: Kimondottan a biztonsági piacra, a megfigyelés területére fókuszáltak, amikor bemutatták az AXIS 200-at, az első IP kamerát?

MG: Nem, az IP kamera teljesítménye – amely kezdetben másodpercenként 1 kép volt, nagyon kis felbontás mellett – ezt nem tette volna lehetővé, miként az akkori betárcsázós internetkapcsolat sávszélessége is akadályt jelentett. Egy nagy, VGA-felbontású kép előállítása 17 másodpercbe telt, de ez tökéletesen elegendőnek bizonyult a távoli monitorozáshoz, ami az IP kamera első alkalmazása lett.

Ugyanakkor biztosak voltunk abban, hogy mind a képráta és -felbontás, mind a sávszélesség javulni fog. Egy év után saját ASIC (alkalmazás-specifikus processzor) fejlesztésébe fogtunk, amellyel elértük a biztonsági alkalmazások által megkövetelt 30 kép/másodperc teljesítményt és nagy képfelbontást. Olyan IP kamerát készítettünk, amely versenyképessé vált és elterjedt a megfigyelés területén.

CW: Ha gyorsan előretekerünk a mába, azt látjuk, hogy a széles körben hozzáférhető, nagy sebességű vezetékes és vezeték nélküli internetelérés hatására a kamerás megfigyelés területén gyorsan terjednek a tisztán digitális rendszerek. Véleménye szerint mely technológiák gyakorolják a legnagyobb hatást az IP kamerák fejlődésére?

MG: Moore törvénye, a kedvencem, a kameráinkhoz fejlesztett ASIC esetében is útmutatónak bizonyult, és még jó ideig az is marad. Processzorunk, amely ma már negyedik generációjánál tart, egyszerre több csatornát kezel és H.264-es tömörítést támogat. Mindez fölényes teljesítményt és képminőséget ad, amely esetenként az emberi szem képességeit is felülmúlja. Egyedülálló LightFinder technológiánkkal például a biztonsági kamerák sötétben is látják a színeket.

Hasonló ütemben fejlődnek a kameráinkba építhető, beágyazott tárolók. Ma a 32 GB-os SD kártyák képviselik a főáramot, de már érkeznek a 64 és a 128 GB-os kártyák, amelyek akár többheti felvétel tárolását is lehetővé teszik a biztonsági kamerán belül. Más szóval a felvett videóanyag zömét nem kell majd átküldeni a hálózaton egy központi szerverre, ami pár éven belül jelentősen meg fogja változtatni a kamerás megfigyelő rendszerek ökonómiáját.

Fontos trendet látok a felhőalapú adattárolásban is, amely a hálózati kamerák használatára is kihat, úgy a felvett videó, mint maguk a kamerák kezelése, felügyelete tekintetében. Csehországban (*interjúnk az Axis regionális központjában készült, Prágában – a szerk.*) is van már olyan partnerünk, aki rendezvényekhez kínál alkalmi kamerás megfigyelést Video-as-a-Service-típusú felhőszolgáltatás keretében. Ebben a modellben rendkívül egyszerűen telepíthető, majd az esemény végén leszerelhető az egész rendszer, ami analóg technológiára épü-

MARTIN GREN

alapító,
Axis Communications

lő megoldással összehasonlíthatatlanul drágább lenne. A technológia fejlődése nemcsak az eszközökben érhető tetten, az üzlet előtt is egészen új távlatokat nyit.

CW: Az IP kamerák a videokonferencia-rendszerek mellett ma már minden mobil számítógép, tablet és számos okostelefon részét képezik, a személyes kommunikáció mind fontosabb eszközévé válnak, legjelentősebb alkalmazási területük azonban a megfigyelés. Lát-e olyan alkalmazási területeket, amelyeken a hálózati kamerák hasonlóan fontos szerepet tölthetnek be a jövőben?
MG: Az IP kamerák piacán véleményem szerint ma a kereskedelem a legfontosabb vertikum, ahol többről van szó, mint biztonságról. A kamerák itt a vásárlók számáról és mozgásáról, a leglátogatottabb polcokról, az előttük töltött időről is információkat szolgáltathatnak analitikai alkalmazásokhoz. Így nem csupán a bolti lopások megakadályozásában, a veszteségek csökkentésében, hanem az üzleti lehetőségek azonosításában és kiaknázásában is fontos szerepet játszanak.

CW: Azon analitikai alkalmazások szerepe nő majd a jövőben, amelyek az IP kamerák által szolgáltatott videót mint bemenetet, adatot képesek hasznosítani?
MG: Igen. Kameráinkat ezért tettük alkalmassá arra, hogy a felhasználók szoftvereket tölthessenek le rájuk. A kereskedelem területén például ilyen, kamerán futó alkalmazás számlálja a vásárlókat az eladótérben.

Ezeket az alkalmazásokat partnereink fejlesztik, ezen a téren – csakúgy, mint az értékesítésben – nagyon lojálisak vagyunk irányukban, nem kívánunk versenyezni velük. ADP (Axis Development Partner) programunkon keresztül ugyanakkor támogatjuk őket, és segítünk az elkészült alkalmazások piacra vitelében, népszerűsítésében. Stratégiánk a partnerségre épül, és ehhez következetesen tartjuk magunkat, a kamerák alapfunkcióit érintő szoftverfejlesztéseket azonban magunk végezzük. Egyik kedvenc példám az Active Tampering funkció, amely riasztást küld, ha a biztonsági kamerát valaki megpróbálja hatástalanítani, például elfordítja, festékkel fújja be az eszközt, vagy ajakrúzst ken a lencsére. Ez a képesség minden alkalmazási területen egyaránt fontos, míg a vásárlók számlálása olyan iparági alkalmazás, melynek fejlesztését átengedjük partnereinknek.

CW: A piaci adatokból leszűrhető, hogy a kamerás megfigyelés területe az analóg technológia irányából egyértelműen a tisztán digitális rendszerek irányába halad. Az IMS Research előrejelzése szerint a szállító bevételek alapján az IP kamerák 2014-ben túlsúlyba kerülhetnek az analóg kamerákkal szemben, de utóbbiak az eladott darabszámot tekintve továbbra is fölényben maradnak. Mikorra várható, hogy az IP kamerák darabszám tekintetében is a piac nagyobb szeletét fogják adni?
MG: Az analóg kamerák ma már csupán az alacsonyabb, így olcsóbb termékkategóriákban fogynak, ami nagyszámú, de egyenként kevés kamerát tartalmazó, kisebb telepítést jelent. Csúcskategóriában már napjainkban is kizárólag digitális kamerákra épülő rendszereket vezetnek be a felhasználók. Több kezdeményezésünk is arra irányul, hogy a belépőszinten, ahol jelenleg kevesebb kamerával vagyunk jelen, bővítsük kínálatunkat. Személy szerint egyébként arra számítok, hogy a szállítói bevételek alapján az IP kamerák már 2013-ban lekörözhetik az analóg kamerákat.

> **Az IP kamerák piacán véleményem szerint ma a kereskedelem a legfontosabb vertikum,** ahol többről van szó, mint biztonságról.

CW: Milyen szerepe lesz ebben a lakossági piacnak? Tekintettel a vezeték nélküli hálózatok, a felhőalapú tároló- és eszközfelügyeleti szolgáltatások elérhetőségére, milyen gyorsan terjedhet az IP-alapú kamerás megfigyelés az otthonokban?
MG: A védelemmel övezett, őrzött lakóközösségek, amelyek felénk kevésbé, az Egyesült Államokban viszont igen elterjedtek, nagyon jó felvevőpiacot jelentenek a kamerás megfigyelőrendszerek számára. Arra azonban még várnunk kell pár évet, amíg rajtuk kívül, a magánotthonokban is elterjednek a biztonsági kamerák. Könnyű egy IP kamerát az asztali számítógép tetejére ültetni, de ahhoz, hogy a megfigyelés valóban eredményes legyen, a jellemző környezeti hatásokkal, például az időjárási viszonyokkal szemben ellenálló eszközöket megfelelő módon kell telepíteni a lakásban vagy a ház körül, ami nem is olyan egyszerű.

CW: A köz- és magánterületeket megfigyelő kamerás rendszerek mind nagyobb mennyiségű adatot rögzítenek és tárolnak az emberek napi tevékenységéről, és ezt az információmennyiséget egyre kifinomultabb alkalmazások elemzik. Véleménye szerint a jelenlegi szabályozások elegendőek az érzékeny adatok, a személyi jogok védelméhez, vagy szükség lehet a vonatkozó előírások felülvizsgálatára és frissítésére?
MG: A biztonsági kamerák használatára és a felvételek tárolására vonatkozó szabályok országonként változnak. Előrelépést jelentene, ha ezt egységesíteni tudnánk, legalább az Európai Unión belül. De szerintem az előírt képfelbontást is szabványosítani kellene a kamerás biztonsági rendszerekre nézve, méghozzá a HDTV szintjén. A bulvársajtóban gyakran szerepelnek a biztonsági kamerák által rögzített felvételek, amelyeken alig ismerhető fel bárki is.

A rögzített videóanyag tárolásának feltételeit szintén szabályozni kellene az érzékeny információk, a személyi jogok védelme érdekében, méghozzá az adott alkalmazásnak megfelelően. A bankok számára például lehetővé kell tenni, hogy legalább 1 hónapon át megőrizzék a kamerák felvételeit, mert a bűncselekményt megelőző hetekben a bűnözők jellemzően felkeresik a kiszemelt helyszínt. A kereskedelemben viszont indokolatlan lenne a videók hosszabb idejű tárolása.

Ezzel együtt ne feledkezzünk meg arról sem, hogy a biztonsági kamerák által rögzített felvételek több mint 99 százalékát soha senki nem nézi meg – erre csak biztonsági esemény bekövetkeztekor kerül sor. Elenyésző annak esélye, hogy valaki egy köztéri biztonsági kamerán keresztül lát, figyel bennünket, amikor végigmegyünk az utcán, így az is valószínűtlen, hogy a személyünkhöz köthető, érzékeny információk valamilyen módon sérülnek. Mindannyian biztonságosabb városokat, utcákat és tömegközlekedést szeretnénk, amihez a kamerás megfigyelés is szükséges. Azt hiszem, a cél érdekében az emberek többsége hajlik a kompromisszumra. Egészen más a helyzet otthoni környezetben, senki sem szeretné kamerák előtt élni a magánéletét. A megoldás nem a végletekben keresendő, a megfigyelés terén is arányosságra, egyensúlyra kell törekednünk.

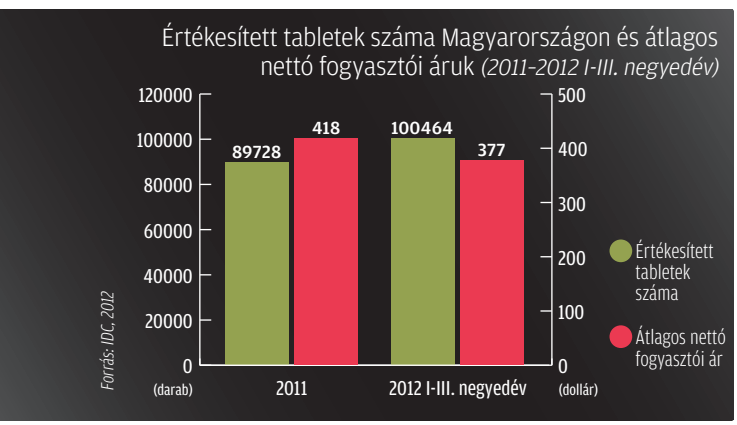
PIACELEMZÉS

Terítéken a tabletek

A tabletek és okostelefonok hazai piaca egyaránt erőtől duzzad. Mobilitás terén lépést tartunk a világgal, bár a felhasználók árérzékenysége miatt az alacsony árkategóriában fogy a legtöbb eszköz, és ez a szállítói erőviszonyokat is hosszú időre meghatározhatja. /Írta: Kis Endre

Magyarországon az International Data Corporation (IDC) 2011 első negyedévétől kezdve méri a tablet-piacot, amely azóta látványos, mintegy 4-szeres növekedésen ment keresztül – az idei harmadik negyedév végére az eddig eladott tabletek száma megközelítette a 200 ezer darabot.

– Míg tavaly az első negyedévben 11 ezer darab tablet, idén az első negyedévben már ennek háromszorosa, a harmadik negyedévben közel négyszerese talált gazdára – mondta *Bagi Bence*, az IDC Hungary elemzője. - A tabletpiacot két operációs rendszer, az iOS és az Android uralja hazánkban is, a felhasználók árérzékenysége miatt azonban a gyártók rangsora nálunk más-



képp alakul, mint a világpiacon. Az Apple iPad eladásai valamelyest visszaestek, míg a Samsung az utóbbi két negyedévben továbbnövelte piaci részesedését Magyarországon. A két legnagyobb szállítót a ConCorde és a WayteQ követi a listán – a két cég együttes részesedése kb. 10 százalék, ami egy rendkívül szegmentált piacon kifejezetten nagynak számít.

A magyar felhasználók a csúcskategóriás, 130 ezer forintnál drágább, valamint a nagyon olcsó, 30-60 ezer forintért kapható tableteket keresik. Utóbbi csoportba tartoznak a ConCorde és a WayteQ termékei, miként a rangsor ötödik helyén szereplő Huawei eszközei is. Míg idehaza a Samsung, világszinten az Apple vezeti a tabletgyártók listáját. A két céget a világranglistán az Amazon, az Asus és a Lenovo követi. Ők nálunk nem jutottak az első öt közé: az Amazon Kindle Magyarországon hivatalosan nincs forgalomban, az Asus és a Lenovo elsősorban üzleti felhasználóknak szánt tabletjei pedig drágák. Világszinten a gyártók közel 28 millió tabletet szállítottak a harmadik negyedévben, ami 50 százalékos növekedésnek felel meg - a hazai piac 30-40 százalékos bővülése ezzel jól összemérhető.

Búcsú a netbooktól

A hazai tabletpiac másfél éven belüli négyszeres növekedése természetesnek is vehető, mivel új termékkategóriáról van szó, de a tempó arra is utal, hogy a tablet – különösen a lakosság körében, az elsősorban tartalomfogyasztó felhasználók számára – a PC vonzó alternatíváját kínálja.

– A tabletek mára szinte teljesen kiszorították a netbookokat a piacról – mutatott rá Bagi Bence. – Az idei harmadik negyedévében a netbookok forgalma az egy évvel korábbi, azonos időszakhoz képest a negyedére esett vissza, ezért a jövő évtől már nem fogjuk mérni ezt a termékkategóriát. A felhasználók átpártolása egyáltalán nem meglepő. Egy netbook áráért sokkal jobb műszaki paraméterekkel rendelkező és korszerűbb, vonzóbb funkcionalitást kínáló tabletet vásárolhatnak. A táblagépek hasonló módon az olcsó notebookoktól is elhódítanak vásárlókat.

Várhatóan az év végén megérkezik a hazai piacra a Microsoft Surface táblagépe, aminek 2013-tól elsősorban a vállalati piacon lehet hatása.

– Az iOS és Android-alapú tabletekkel szemben a Windows RT operációs rendszert futtató Surface előnye, hogy vállalati IT-környezetben a meglévő felügyeleti eszközökkel ugyanúgy menedzselhető, mint a Windows-alapú PC-k és szerverek – mondta az elemző. – A két vezető mobilplatform esetében a dolog nem ilyen egyszerű. Bár a hazai vállalatok is érdeklődnek az alkalmazottak által vásárolt tabletek és okostelefonok támogatása iránt, a gyakorlatban ezzel viszonylag kevés cégnél találkozunk. Ahol él a gyakorlat, ott jellemzően iOS-alapú eszközöket, illetve BlackBerry okostelefonokat támogat az IT osztály. Lakossági piacon élvezett népszerűségét az Android egyelőre nem tudta megismételni vállalati környezetben. A saját tulajdonban levő eszközök támogatása a továbbiakban minden bizonnyal elterjed, és majd eldől, hogy a későn piacra lépő, de könnyebben menedzselhető tabletet kínáló Microsoft mekkora részesedést tud szerezni.

Okostelefon-áradat

Világszinten az eladott mobiltelefonok 80 százaléka okostelefon – és ez az arány az IDC szerint Magyarországon is hasonló, 70 százalék körüli.

– Idén, az első három negyedévben összesen 220 ezer okostelefont vásároltunk – mondta Bagi Bence. – Ez drasztikus növekedésnek számít, amelyet az Android-alapú eszközök hozzáférhetősége hajt. Az Apple drága iPhone modelljei a távközlési cégeken keresztül találnak vásárlókra. Piaci részesedést tekintve az Android 70-30 százalék arányban vezet, és a nyílt forráskódú platform fölénye tovább fog nőni, mivel a rá építő gyártók egyre alacsonyabb árkategóriákban tudnak megjelenni okostelefonjaikkal.

A piaci szereplők listáját itt is a Samsung vezeti, elsősorban Galaxy S sorozatának köszönhetően, amely az iPhone-éhoz hasonló felhasználói élményt 30-40 százalékkal olcsóbban kínálja. Az okostelefonok piacán is a 130-150 ezer forintnál drágább, prémium kategóriás eszközök, és az olcsó, 20-40 ezer forintért kapható ZTE, Huawei és más modellek népszerűek Magyarországon.

– A harmadik mobilplatform, a Windows Phone nálunk eddig csekély, mintegy 1,5 százalékos részesedést ért el – tette hozzá az elemző. – A Windows Phone és a Windows 8 azonban már egységes platformot képvisel, amelyet a vállalatok jól menedzselhetnek IT-környezetükben. Terveikből ítélve ez a lehetőség a hazai cégek figyelmét sem kerüli el. Az új verzióra épülő készülékek megjelenésével a Microsoft részesedése 2016-ig közel a négyszeresére, 5-6 százalékra nőhet az okostelefonok piacán.

Az IDC előrejelzése szerint 2013-ban a tabletpiac 30-40 százalékkal, az okostelefonoké 10-15 százalékkal bővülhet Magyarországon.

TENNIVALÓK A SÚLYOS BÜNTETÉS ELLEN

Szigorúbb lett az új adatvédelmi törvény

Közel 100 ezer vállalatot érint az év elején hatályba lépett új adatvédelmi törvény, melynek megsértését akár 10 millió forint összegű bírsággal is sújthatja a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIF). Az IT-vezetők most ingyenes tréning keretében ismerhetik meg a szabályozást és a megfeleléshez szükséges tennivalókat.

2012. január 1-én lépett hatályba az Információs önrendelkezési jogról és az információszabadságról szóló (2011. évi CXII.) törvény, rövidebb nevén az új adatvédelmi törvény. Ezzel a korábbi gyakorlatilag szankciókat nem tartalmazó szabályozást egy jóval szigorúbb gyakorlat váltotta fel, amely az adatkezelést vagy adatfeldolgozást végző szolgáltató cégek működését nagymértékben befolyásolja. A szabályozás hatálya alá tartozik gyakorlatilag valamennyi személyes adatot kezelő vállalkozás, különösen érintettek a tömeges ügyfélkapcsolat-kezelést végző cégek, mint például a pénzügyi, távközlési, közüzemi és online szolgáltatók.

A törvény ugyanis kimondja, hogy az adatkezelő köteles teljes körűen gondoskodni az általa kezelt személyes adatok biztonságáról, és köteles megtenni az ehhez szükséges technikai és szervezési intézkedéseket. A személyes adatok automatizált feldolgozása során biztosítani kell például a jogosulatlan adatbevitel megakadályozását; annak ellenőrizhetőségét, hogy a személyes adatokat mely szerveknek továbbították; a személyes adatokat mikor és ki vitte be az adatfeldolgozó rendszerbe; valamint a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát.

A törvény a Nemzeti Adatvédelmi és Információszabadság Hatóságot is létrehozta, melynek jogköre jelentősen kiszélesedett a korábbi Adatvédelmi Biztos intézményéhez képest. Az új hatóság ugyanis már szabálysértési-, büntető-, sőt akár bírósági eljárást is kezdeményezhet a törvényt megszegő szolgáltatókkal szemben, megtilthatja a további adatkezelést, és – akár többször is – 10 millió forintig terjedő bírságot szabhat ki. Ezzel, mint az az elmúlt hónapokban a sajtóban is többször nyilvánosságra került, egyre többször él is a hatóság. 2013 januárjától pedig szigorodó ellenőrzések várhatók.

Érdemes tehát felkészülni a következő évre a magas szintű adatvédelem és adatbiztonság megvalósítását lehetővé tevő megoldások alkalmazásával. Legyen szó akár technikai eszközökről, akár az új adatvédelmi szabályzatokról. Az egyedülálló IT-biztonsági megoldásairól ismert BalaBit IT Security ennek jegyében szervezi meg informatikai döntéshozók, felelősök számára azt az ingyenes tréninget, melyen a résztvevők megismerhetik a törvény előírásait, az ingyenes adatvédelmi audit lefolytatásának módját, és bemutat olyan eszközöket is, melyek elősegítik a törvényi megfelelést. Amennyiben szeretne további információt megtudni a törvényről és a tréningről, látogasson el a következő weboldalra: **www.balabit.hu/adatvedelmi-training** ■

BalaBit IT Security

INVITEL ZRT.

InnoMax: folytatódik az innovációs pályázat

Az Invitel újra meghirdeti üzleti innovációs versenyét, az InnoMax pályázatot. A kis- és középvállalkozások mellett idén már a 250 munkatársnál többet foglalkoztató vállalatok is pályázhatnak az InnoMax Díjra. Emellett tovább folytatódik az InnoApps is, melyen felsőoktatási intézmények hallgatói és középiskolák diákjai vehetnek részt valamilyen újszerű, ötletes alkalmazás fejlesztésével. Innováció, hatékonyság, maximalizmus, kreativitás: ezek a kulcsszavai az InnoMax Díjnak, amelyet az Invitel már negyedik alkalommal hirdet meg partnerei számára. A pályázatokat november végétől február 25-ig lehet benyújtani, ehhez pedig elegendő felkeresni a **www.invitel.hu/innomax** oldalt és kitölteni a rövid pályázati űrlapot. Az Invitel célja, hogy az innováció megkapja azt a kiemelt figyelmet, amit megérdemel, és amelyre a válság miatt egyre kevesebb figyelem irányul napjainkban. A vállalat felkarolja és a díjjal támogatja a korszerű ötleteket, a hatékonyságot javító innovációs törekvéseket, és teret kíván biztosítani ennek a kultúrának.

„Az Invitel számára az innováció nem lehetőség, hanem kötelezettség. Olyan nagyvállalatokkal dolgozunk együtt, mint például a MOL, a Wizz Air, az MKB vagy éppen a hazai legnagyobb kórházak, ahol pénzről, biztonságról, életekről van szó. Itt a középszerűség nem megengedhető, az üzleti maximalizmus minimumnak számít. Az InnoMax Díjjal támogatni és ösztönözni szeretnénk azokat a vállalatokat, akik ugyanúgy gondolkodnak az üzletről és az innovációról, mint az Invitel" – mondta lapunknak *Zsembery György*, az Invitel vezérigazgató-helyettese.

InnoMax Díjasok: Elit kör

Az előző év nyertesei között olyan cégek vannak, akik számára az innováció üzleti kérdés, mert ilyen iparágban dolgoznak, ebből élnek. Ilyen például a HBO, amely világújdonságnak számító hazai fejlesztésű HBO GO szolgáltatásával nyert, vagy a Rádió Tele5 Taxi Holding, amely komplex vállalati innovációjáért kapott díjat, illetve a DataLogic, amely egy újszerű, kimondottan kis- és középvállalatoknak fejlesztett vállalatirányítási rendszerrel lett InnoMax-győztes.

ZSEMBERY GYÖRGY
vezérigazgató-helyettes
Invitel

Az Invitel az InnoMax mellett elindította az InnoApps pályázatot is, a társaság ugyanis az innováció iránt fogékony felsőoktatásban és középiskolákban tanuló diákokat is szerette volna bekapcsolni a versenybe. A versenyben két kategóriában osztanak díjat: az üzlethez, munkához kötődő „komolyabb" témájú fejlesztésekkel a „Ne szórakozz!" kategóriában, a „könnyedebb" hangvételű fejlesztésekkel pedig a „Szórakozz!" kategóriában lehet pályázni. ■

„...sokféle elektronikus, illetve mobilfizetési megoldásnak van létjogosultsága, és azokat nem lehet egymással szembeállítani.

Mobilfizetés – még csekély, de meredeken nő

A különféle mobilfizetési megoldások nem versenytársai egymásnak, hanem kiegészítik egymást. Az NFC-nek is lenne létjogosultsága, ha lennének szabványok, kialakulna az ökoszisztéma, és átgondolt pilotprojekteket indítanának. /Írta: Majláth Judit

Nincs miért szégyenkeznünk a mobilfizetés terjedését, népszerűségének növekedését illetően. Magyarország e területen világviszonylatban példaértékű helynek számít – fogalmaz *Inotay Balázs*, a Cellum csoport stratégiai igazgatója. Állítását igazolandó hozzáteszi: arányaiban nálunk töltik le a legtöbb alkalmazást, valamint nálunk van a legtöbb felhasználó.

Mindez természetesen nem jelenti azt, hogy abszolút értékben óriási számokról beszélhetünk, hiszen egy bank vagy kereskedő forgalmához képest egyelőre roppant kis értékekről van szó, a mobilfizetés árbevétel-termelő képessége tehát e pillanatban még alacsony. A tendencia azonban egyértelmű. Még az Egyesült Államokban és a fejlett nyugat-európai országokban sem tapasztalható egy-egy mobilfizetési alkalmazás olyan meredek felfutása, mint Magyarországon. A szakember azt várja, hogy 2013 tavaszán a jelenleginél is meredekebb felfutásra vált a hazai mobilfizetés terjedése.

Az, hogy egy ügyfél milyen fizetési eszközt választ, jellemzően a pillanatnyi élethelyzetétől függ. Magától értetődő, hogy egy bevásárlóközpontban más eszköz az előnyösebb, mint mondjuk egy uszoda medencéjének a partján. Éppen ezért sokféle elektronikus, illetve mobilfizetési megoldásnak van létjogosultsága, és azokat nem lehet egymással szembeállítani. Sokkal inkább egyfajta párhuzamosság, konvergencia mutatkozik a különböző fizetési folyamatok között.

Bankkártya-integráció iPhone-ba

Nemrégiben például a Cellum csoport olyan technológiát fejlesztett ki, amelynek segítségével az iPhone-on elérhető PassBook-alkalmazással már nemcsak belépőjegyek, kupon- és hűségkártyák tárolhatók és használhatók digitális formában, hanem lehetővé válik a bank- és hitelkártyák integrációja is. A PassBook egyfajta általános értéktároló eszköz, amit a különböző alkalmazások elérhetnek, és a benne tárolt ada-

tokat közösen kezelhetik. Mivel azonban a PassBook önmagában nem rendelkezik magas szintű biztonsági elemekkel, az iPhone-felhasználóknak eddig nem volt lehetőségük a banki fizetési megoldásokra és így a bankkártya-adatok tárolására sem.

A banki szintű biztonságot a Cellum úgynevezett „eltört titok"-technológiája garantálja, amit a MasterCard Mobile már egy éve használ. Lényege, hogy a telefonos alkalmazás a bankkártya-adatoknak csak egy részét tárolja, a másik részét biztonságos szervereken őrzi a rendszer. Ezzel a megoldással jelentősen csökkenthető a mobilfizetés kockázata, ugyanakkor a különböző kiskereskedelmi logikák képesek ugyanazokat az elemeket kivenni a PassBookból és használni egy adott tranzakciós folyamat során.

„Első lépésként az iOS-be integráltuk megoldásunkat. Várható, hogy rövidesen az Androidban is megjelennek azok az elemek, amelyek hasonlóan kezelik a fájlstruktúrákat, így az Android-alapú készülékekre is kiterjeszthetjük a bank- és hitelkártyák biztonságos integrációját" – mutat rá Inotay Balázs.

NFC – kombinált alkalmazásokban

A PassBook, valamint az azt felhasználó fizetési lehetőségek gyakorlatilag szoftveres úton oldják meg mindazt, amit a plusz hardver- és szoftverelemeket egyaránt tartalmazó, mobiltelefonokba is beépíthető NFC technológia. Az NFC-vel kapcsolatban sokféle a tapasztalat, és ennek megfelelően sokféle vélekedés kering. A tapasztalatok jó része negatív, hiszen az NFC-alapú rendszerek bevezetése viszonylag nagy beruházást igényel, ugyanakkor kézzel fogható haszna – egyelőre legalábbis – meglehetősen csekély. Nyilván ezen tapasztalatokra is alapoznak azok, akik szerint az iOS-ből kiinduló, majd a többi mobil operációs rendszerre is átterjedő, tisztán szoftveres megoldások az NFC végnapjait jelenthetik.

Inotay Balázs némileg másképpen vélekedik. Szerinte lenne lehetőség az NFC-alapú fizetés terjedésére, csak kombinált alkalmazásokban kellene gondolkozni. Az NFC-s megoldásokat a mostaninál hatékonyabb, szélesebb rendszerintegrációs környezetbe kellene helyezni, és nem pusztán arra használni, hogy a bankkártyás fizetéseket kiváltsák.

Nem véletlen, hogy az Apple nem implementálja az NFC-t az iPhone-ba, hiszen a technológia ökoszisztémája sehol a világon nem terjedt el, és annak üzleti lehetőségei egyelőre nem láthatóak. Nincs még kialakult kvázi-szabvány sem, nemhogy kipróbált, használt valódi szabvány lenne. Az Apple kiváró taktikája tehát nem meglepő.

„Semmiképpen sem gondolom, hogy a PassBook-típusú alkalmazásokra épülő szoftveres fizetési megoldások az NFC végnapjait okoznák. Az NFC nehézségeit maguknak az NFC-s projekteknek az elkapkodása okozza. A világban látható pilotprojekteket ugyanis nem átgondolt stratégiák mentén szervezik, ezért azok jelentős része elhal, és ez egyértelműen rossz üzenet. Ha egy ügyfél egyszer már részt vett egy sikertelen pilotban, azt nagyon nehéz visszaédesgetni egy más, hasonló alkalmazáshoz" – hangsúlyozza Inotay Balázs.

Szélesíteni kell az értékláncot

A mobilfizetés terjedésének egyik alapvető feltétele az értéklánc szélesítése, valamint a fizetési megoldások testre szabása. Nagyon fontos, hogy a kereskedők olyan alkalmazássablonokat kapjanak, amelyeket könnyedén hozzá tudnak igazítani saját üzletükhöz, és amelyek segítségével megújíthatják, leegyszerűsíthetik működésüket.

Annak dacára, hogy a mobilfizetés az elmúlt másfél-két évben több oldalról is támogatást kapott, a bankok továbbra is meglehetősen passzívan szemlélték a fejleményeket. A közelmúltban azonban némileg változott a helyzet, sőt a bankok afelé mozdultak el, hogy bizonyos szempontból húzóerői legyenek a folyamatnak.

A mobilfizetés elterjesztésének fontosságát tekintve a három hazai mobiltársaság többé-kevésbé azonos nézetet képvisel. Ezt jelzi, hogy mindhárman tagjai a Mobil Tárca Egyesületnek. Az azonban még nem alakult ki pontosan, hogy az ökoszisztémában mi legyen (mi lehet) a mobilszolgáltatók szerepe. A SIM-kártyák rendelkezésre bocsátása egyértelmű feladat, de ezen kívül kézenfekvőnek tűnik például az is, hogy az operátorok – jól bejáratott csatornáikon keresztül – alaposan kivegyék a részüket az ügyfelek edukálásában.

ELŐREJELZÉSEK

Juniper Research (2011. június): 2014-re az NFC-alapú mobilfizetési tranzakciók száma világviszonylatban megközelíti az 50 milliárd dollárt. Az elkövetkező 18 hónapban várhatóan 20 ország jelent be NFC-alapú szolgáltatásokat.
Yankee Group (2011. június): az NFC-képes telefonok száma a 2011-es 7 millióról 2015-re 203 millióra nő.
Juniper Research (2011. március): 2015-re több mint 750 millió felhasználó mobiltelefonjára érkezik valamilyen jegy, vagy vásárol mobiltelefonjával valamilyen jegyet. A jegyek továbbítása SMS-ben, vonalkóddal, a mobil weben keresztül, okostelefon-alkalmazásokkal vagy NFC-technológiával történik.
Juniper Research (2011. április): 2015-re világviszonylatban 500 millió ember használja mobilkészülékét metró- vagy buszjegyként. Ez 2010-től számítva több mint ötszörös növekedést jelent.
Juniper Research (2011. március): 2010-ben a légitársaságok 160 millió mobil beszállókártyát bocsátottak ki. 2013-ra ez az érték 480 millióra nő, vagy minden 7 beszállókártyából 1 mobil lesz.

MODELLPORTFÓLIÓ

Bankolás 2016-ban: új világ határán

Itt az idő, hogy a kereskedelmi bankok megváltozzanak – állítja az Accenture nemzetközi tanácsadócég tanulmánya. A következő években a különféle információs csatornákon szerzett tapasztalatok, a közösségi média és a mobiltechnológia adhatják a jövőbeli siker sarokpontjait a bankok számára.

/Írta: Meixner Zoltán

A bankok még mindig félnek a jövőtől, mert szembesülnek egy sor ijesztő piaci, működési, költségekkel kapcsolatos, szabályozási vagy az ügyfelektől érkező kihívással, s ezek miatt még mérsékelt növekedést sem nagyon mernek tervezni – állítja az Accenture. A nemzetközi tanácsadó cég szerint 2011 és 2014 között 30 globális bank folyamatainak vizsgálata alapján az átlagos növekedés 6,5 százalék lesz (Európában és Észak-Amerikában csak 4 százalék). A bankárok kezdenek ráébredni, hogy ezek a szerény növekedési tervek is veszélyben lehetnek, ha nem sikerül három kritikus területen előre lépniük. Először is vissza kell szerezniük az ügyfelek bizalmát és elkötelezettségét, meg kell védeniük a fizetési üzletágukat a közvetítő szervezeteket kiiktató versenytársaktól (például Google Wallet, PayPal stb.), és el kell kerülniük, hogy a termékeik, szolgáltatásaik, márkáik elveszítsék egyedi értékeiket. Ehhez vissza kell térniük az alapokhoz és újra kell gondolniuk a működési modelljeiket. Azok teszik lehetővé ugyanis, hogy az ügyfeleiket gyorsan és egyszerűen tudják kiszolgálni, s közben a növekedésüket megalapozó profitra is szert tehessenek. A régi, szigorúan üzletágakra bontott modellek mára szinte működésképtelenekké váltak. Az Accenture szerint ezek helyén három új alapmodell van kibontakozóban, amelyek ismeretében az egyes bankoknak lehetőségük van a saját változatuk, kombinációjuk kialakítására.

Az egyik modell a különféle csatornákon szerzett tapasztalatokra építkezik, s „bevonja" tevékenysége alakításába az ügyfeleit, hogy minél hatékonyabban szolgálhassa ki az igényeiket. Az ilyen intelligens többcsatornás bank működési modelljének centrumában a stratégiai-analitikai eszközök használata áll.

A másik megoldásban a bank a közösségi médiát használja fel, hogy ügyfeleivel szoros „baráti" kapcsolatot alakítson ki. Ez a modell a közösségi szemléletű bankoké.

A harmadik modellben a pénzintézet pénzügyi és nem pénzügyi szolgáltatások egész ökoszisztémáit építi fel, különösen a mobiltechnológiában rejlő potenciált kiaknázva. Ez a pénzügyi és nem pénzügyi digitális ökoszisztémát építő bankok modellje.

A bankok e három modell felhasználásával akár meg is duplázhatják a növekedési rátájukat, a fejlett piacokon nem lehet kizárni a 8 százalékos bővülést sem, miközben a költségeket legalább 20 százalékkal csökkentik. A sikerekhez azonban szükséges, hogy néhány mutató megfelelő súlyt kapjon. A hírnév, a kereskedelmi teljesítmény, a szolgáltatási teljesítmény, az értékesítési teljesítmény, és az ezek megtámogatására való képesség feltétlenül a kulcselemek közé tartoznak.

Az új modellek

Jól művelni az alaptevékenységet – ez lehet a bankok végső célja. Ugyanakkor ez lehet az alap az új innovatív képességek kifejlesztéséhez is, amelyek segítenek formálni az ügyfelek viselkedését, és támaszt adnak a versenyhez a piacra újonnan érkezőkkel, a kiskereskedőkkel, a mobilszolgáltatókkal, a célirányosan alapított startupokkal a kritikus fizetési üzletágban. Az új képességek a három már említett modellben formálódnak meg, amelyek az Accenture szerint 2016-ra meghatározóak lehetnek a bankok életében.

Az intelligens többcsatornás bank

Azok a bankok, amelyek ezt a modellt használják, gyakran lépnek kapcsolatba az ügyfelekkel különféle csatornákon, észben tartva, hogy ki melyik csatornát preferálja. A kulcs ebben a modellben az analitikák kiterjedt használata, amelyek lehetővé teszik a banknak, hogy sokkal hatékonyabban értse meg az ügyfelek igényeit. *A modell kulcselemei a következők:*

- Fejlett többcsatornás integráció (amely a digitális csatornákra fókuszál), illetve integrált architektúra, amely képes az ügyfelek mindenféle igényét együtt kezelni.
- Jó minőségű ügyféladatokon alapuló erőteljes analitikák, mikroszegmentáció és prediktív modellezés a leghatékonyabb termékkosár meghatározásához.
- Valósidejű interakció-menedzsment, amely képes növelni az átváltási hozamokat a bejövő és kimenő kapcsolatok esetében is.
- Digitális csatornákat használó fejlett tanácsadószolgálat és személyes elemzési eszközök használata.
- A mikroszegmenseken és az optimalizált csatornákon alapuló termékajánlatok és ezekhez kapcsolódó árazási sémák.

Az első lépés e modell felállítására, hogy a bank megtervezi az úgynevezett integrált ügyféltapasztalatot, amely a többcsatornás megközelítésen és architektúrán alapul. Magyarán az ügyfeleknek többféle igénye többféle formában és helyen jelenik meg, a bank mégis képes ezeket – a központba állított ügyfél szempontjait figyelembe véve – kezelni. Amint a bank aktiválja az új csatornákat, az ügyfelek több adatot szolgáltatnak magukról (nő az inputjuk), de a bank szolgáltatásairól való ismereteik is várhatóan növekedésnek indulnak. Ez lehetővé teszi a pénzintézeteknek, hogy kialakítsák a mikroszegmenseket: azokat a legkisebb vásárlói egységeket, amelyekbe a demográfiai és társadalmi helyzetük, magatartásuk alapján közelálló ügyfeleket sorolják be. Ezek a csoportok alkotják aztán az alapját a meghatározott stratégiát követő úgynevezett profitpooloknak. Ahány pool, annyi stratégia, annyi profitszerzési út. Ez a módszer lehetővé teszi a bankok számára, hogy ne a bevételek növekedésére, hanem a profit nagyságára koncentráljanak.

Az ügyféladatok egyre szélesebb körű megszerzése és alkalmazása segít karbantartani és frissíteni azt a fejlett CRM-platformot, amely növelheti a termékkatalógusok érték- és profittermelő képességét, támogatja a valósidejű ajánlatokon alapuló kereskedelmi kampányokat, valamint a mikroszegmensek preferenciáit figyelembe véve az értékesítési költségeket alacsonyabb szinten optimalizálja.

A többcsatornás ügyféltapasztalat az online és offline eljárások valóságos kombinációján alapul, és fejleszthető a dedikált tanácsadói szolgáltatásokra való fókuszálással. Az ügyfél testre szabott szolgáltatást kaphat a személyi bankárától.

A közösségi szemléletű bank

Ez a bankmodell a közösségi média erejét kívánja kihasználni arra, hogy a pénzintézet szinte barátjává, társává váljon szolgáltatásain keresztül az ügyfelének. Az a szándék, hogy a kölcsönös érdekeken alapuló kapcsolatot alakítsanak ki, amely-

AZ ÚJ BANKMODELLEK

Forrás: Accenture

ben befolyásolják egymást. *A közösségi szemléletű bank legfontosabb jellemzői a következők:*

- A közösségi média monitorozása a lehetőségek azonosítására, az ügyfelek bevonására, a kockázatok csökkentésére és a kérdésekre való azonnali reagálásra.
- A közösségi digitális marketing az ügyfelek csoportosításán alapul annak érdekében, hogy a bank pontosabban meg tudja határozni az ügyfelek egyéni profiljának leginkább megfelelő tartalmat és vonzhassa őket.
- A közösségi CRM-et természetesen a közösségi médiából származó ügyféladatokkal teszik gazdagabbá, ezáltal hatékonyabb ajánlatokat téve lehetővé.

A bankok manapság az ügyfelek csoportosítását hagyományos mutatók alapján hajtják végre (átlagos jövedelem, keresztköltési hajlandóság stb.), és ezek alapján látják el őket ajánlatokkal. A közösségi szemléletű bank interakciói sokkal személyreszabottabbak, az ügyfelek érdekeit figyelembe véve folynak, és a kommunikáció javrészt a közösségi médiában zajlik, például linkelési és megosztási technikákat használva. Ezzel a módszerrel akár napi kommunikáció is kialakítható az ügyfelekkel a releváns témákról, és csak akkor kap ajánlatot az ügyfél, ha igényli. A bank következetesen napi partner marad – felkészülve, hogy kielégítse kliense kívánságait, és segítse az egész vásárlási folyamatban.

A több kommunikáció szélesebb lehetőséget teremt az ügyfelekről való információszerzésre, az életük, viselkedésük jellemzőinek feltárására, ami a profilok finomítását segíti. Ez aztán beletorkollhat egy valóságos közös alkotási folyamatba, amelynek során új termékek és szolgáltatások jönnek létre, amelyeket következetesen ajánlanak ki a különböző profilú ügyfeleknek. További haszon, hogy a gondoskodó bank képének kialakulásával az ügyfelek elkötelezettsége megnő, és csökken a valószínűsége, hogy másik pénzügyi szolgáltatót keressenek.

A digitális ökoszisztéma bankja

A pénzügyi és nem pénzügyi ökoszisztéma bankjai reprezentálják azokat a pénzintézeteket, amelyeknél az ügyfelek pénzügyi és nem csak pénzügyi ajánlatokra számíthatnak. Ez a modell igyekszik kihasználni a mobiltechnológia nyújtotta előnyöket, s ezzel elterjeszti a hagyományos banki termékeket az ügyfelei, partnerei hálózatában. A bank el tudja dönteni, hogy létrehoz egy digitális ökoszisztémát vagy a részévé válik egy ilyennek, a fizetési megoldásoktól és a betölteni kívánt szereptől függően. *E modell legfontosabb jellemzői a következők:*

- A mobilfizetés az érintés nélküli tranzakciókat lehetővé tévő NFC-technológián vagy mobilpénztárcán alapul, ami javítja a bank versenyképességét a fizetési piacon és segít megtartani a már meglévő ügyfeleket.
- A gazdagabbá váló szolgáltatási kínálat a mobilkereskedelmen keresztül a pénzügyi ajánlatokon túltekintve a mobil marketingre, a mobil lojalitásra és mobil analitikákra is koncentrál.
- A nem banki szolgáltatókkal való szövetségek és partneri kapcsolatok, illetve a hozzájuk kötődő szolgáltatások kialakítása az üzletmenet részét képezik.

A banknak megvan a lehetősége az „egy megállásos" üzleti megoldás létrehozására, amelyben megfelelhet az összes felmerülő ügyféligénynek, s egyedi kapcsolattartási lehetőséget, partnerséget építhet ki, amivel megnő a fogyasztói bizalom.

Az első lépésben a banknak meg kell határoznia a számára legvonzóbb nem pénzügyi partnereket és a hozzájuk kapcsolódó ajánlatokat, amelyek lehetővé teszik az ügyféltapasztalatok teljes körű megtervezését. A működés összerendezése és menedzsmentje kritikus része a teljesítésnek, azaz a hatékony és biztonságos integrált szolgáltatásoknak, amelyek konzisztensek a bank víziójával és imázsával – és amelyben megbíznak az ügyfelek.

A bank ebben a modellben akkor tud attraktív ügyleteket összehozni és az ügyfelek elkötelezettségét növelni, ha az analitikák és a marketingképességek a mobilszolgáltatásokhoz kapcsolódnak. Ez azt jelenti, hogy a pénzintézetnek muszáj az ügyfeleiről információkat gyűjteni a mobileszközök használata alapján (mobil tranzakciók, földrajzi helymeghatározás stb.) Az újfajta marketinglehetőségek kombinációjával a pénzintézet kezdeményezhet mobilhirdetéseket, napi üzleti ajánlatokat tehet, hűségprogramokat indíthat, s egy átfogó koncepció kialakításával pedig megkönnyíti az ügyfelekkel való valósidejű interkaciókat.

A mobilfizetés lehetősége ebben a modellben kulcskérdés, mert lehetőséget teremt a mobilfizetési piacra újonnan belépők (telekom-cégek, kiskereskedők stb.) kiszolgálására. Az m-fizetés magával hozhat másfajta szolgáltatásokat, kézenfekvően az m-kereskedelem igénybevételét.

Ebben a rendszerben a bank mint megbízható tanácsadó szerepelhet, amely támogatja az ügyfelét pénzügyi és nem pénzügyi ajánlatokkal, lehetőségeket tár elé, például ingatlanvásárlására, autóvásárlásra stb. Az ügyfél összes kívánsága, igénye, amit megoszt a bankkal, gazdasági döntéshez vezet, amelyben a bank képes támogatni ügyfelét a pénzügyi és azon túli területeken is. Ezt pedig az az igény alapozza meg, hogy az ügyfél a lehető legkevesebb céggel akar kapcsoltba kerülni ezeknek az ügyleteknek a során, inkább az ismerős környezetben bonyolítaná le a lehető legtöbb tranzakciót. Ezért megbízik az ökoszisztémát működtető szervezetben, bankban, s a jó együttműködés érdekében hajlandó sok adatát megosztani vele.

Az Accenture elemzői szerint a piacon a szolgáltatást különböző cégek együttműködése alapozhatja meg. A Facebook a tapasztalatok megosztását intéző ökoszisztéma vezetője lehet, a Google a keresési ökoszisztémáé, a nagy telekom-cégek a „lépj kapcsolatba velem"-ökoszisztémáké, a „gazdasági választások"-ökoszisztémáké pedig a nagy bankok. A tanácsadó cég által a „Banking 2016—Next Generation Banking"-tanulmányban vázolt modellek nem a végállomást jelentik, de az érettebb állapotában mutatják be a piacot, amelyre a digitális technológián keresztül elég nagy nyomás nehezedik, azaz a változások nem maradhatnak el. A bankok különbözőképpen fejleszthetik képességeiket, amiből másféle kapacitásportfóliók jöhetnek létre – de az biztos, hogy ha versenyben akarnak maradni, olyan világos stratégiát kell kialakítaniuk, amelynek a közepén az ügyfél és a személyesen neki tett vonzó ajánlatok állnak.

VÉDELMI MEGOLDÁSOK

Trendek az információbiztonságban

Az információbiztonság érthető okokból a számítástudomány egyik legdinamikusabban fejlődő szakterülete. Gépeink, rendszereink és hálózataink bármikor, bárhol és bárhonnan – földön, vízen, levegőben – támadhatók. Az élővilággal mind több hasonlóságot mutató malware-ek és botnetek gombamód szaporodnak.

Egyértelmű, hogy a hagyományos módszerek mellett és helyett új, a mesterségesintelligencia-kutatások egyre több eredményét magukba integráló megoldások szükségesek, amelyek akár nyílt forráskódúak is lehetnek. Hogyan derítheti fel időben egy szervezet a számítógépes hálózata elleni támadást, miként reagáljon gyorsan, és állítson le bármilyen rossz szándékú behatolást, adatrongálást? Mert hiába a sok tűzfal és más biztonsági megoldások, a pusztítást felettébb nehéz megakadályozni; ismert hálózatok szinte minden hónapban szenvednek el nagyobb volumenű attakokat.

Információbiztonság és játékelmélet

Heechang Shin, az Iona College (New Rochelle, New York állam) szakembere a játékelmélet segítségével dolgozott ki a korábbi megközelítéseknél hatékonyabbnak tűnő hálózatvédelmi mechanizmust. Úgy véli, a támadások nemcsak felhasználók tízezreit érintő szolgáltatás-kimaradást okoznak, de a kereskedelemben el is viszik az éves eladás egy százalékát, ami átlagos amerikai vállalatok esetében tízmillió dollárnál magasabb összeg.

Shin játékelméleti modellen alapuló, a behatolást valós időben felfedező hatékony programot fejlesztett. Lényege az úgynevezett „védekező előrejelzés." A program valóság kontra előrejelzést játszik, és akkor győz, ha a valóság megegyezik az előrejelzéssel. Ilyen esetekben a behatolás blokkolását javasló figyelmeztetést küld a rendszernek. Előnye, hogy a támadást már csak utólag felfedező módszer, a logok elemzése helyett valós időben figyeli a hálózat kimenő és bejövő adatforgalmát. A tipikus behatolási kísérletek és a belső támadások mintáit mesterségesintelligencia-módszerrel, folyamatos tanulás eredményeként ismeri fel.

Hatékonyságát tesztelve Shin arra a következtetésre jutott, hogy a játékelméleti megközelítés legalább annyira jó, de (a valós idő miatt) talán jobb is, mint a hálózati behatolások detektálására használt más, hagyományosabb módszerek.

Hogyan védekezzünk a következőgenerációs vírusok ellen?

A Texas Egyetem (Dallas) Kiberbiztonsági Kutatóközpontjában dolgozó *Kevin Hamlen* számítógépes vírusok tevékenységét prognosztizáló új eljárást dolgozott ki, amely a malware-ek elleni küzdelemben használt eszközök és stratégiák következő generációját vetíti előre. Ezek a megoldások szerencsére hasznosítani tudják a legtöbb jelenlegi gép számítási adottságait, a működésükhöz szükséges utasításokat.

A vírusok általában véletlenszerűen terjednek, szaporodnak a hálózaton; mutációjuk szintén random jellegű, megakadályozva, hogy azonos másolatuk legyen, azaz nehezebb felfedezni őket. Hamlen és munkatársai vizsgálták, hogy random helyett képesek-e közvetlen mutációra, rájönni a megfertőzött gép által használt védelmi eljárásokra, és fejlett gépitanulás-módszerek segítségével hálózati szinten hatástalanítani ezeket a védelmi megoldásokat.

Javaslatuk: proaktívan ki kellene találni, mi várható a jövőben. A programozási nyelvek kutatását, az ott használt programok aktivitását, hibáikat prognosztizáló algoritmusokat próbálják a szoftverbiztonságra alkalmazni. Tapasztalataik alapján ugyanezzel a módszerrel az utasítások kivitelezése és a mutáció előtti mikroszekundumokban a malware-ek tevékenysége is előrejelezhető.

Hamlen biztatónak tartja, hogy a laptopoktól a felhőszámítások hálózati szervereiig a legszélesebb skálán használt CPU-chipeket nem kell újakra cserélni, hanem különböző tulajdonságaikat kell szinkronba hozni, kompatibilissé tenni egymással. A közeljövőben arra szeretne választ kapni, hogy mely algoritmusokkal hozhatók létre minden eddiginél masszívabb antivírus-programok.

Botnet az égből

A telekommunikációs hálózatok elleni támadások szintén egyre kifinomultabbak, ráadásul onnan is jöhetnek, ahonnan eddig senki nem számított rájuk.

Képzeljük el, hogy egy pilóta nélküli, távirányított légi járművet vezeték nélküli hálózatok felderítésére és veszélyeztetésére alkalmas technológiákkal szerelünk fel, majd a drón a légtérből vezérli a megfertőzött számítógépekből kialakuló, további gépeket, rendszereket támadó botnetet.

Sven Dietrich, a Stevens Technológiai Intézet (Hoboken, New Jersey) kutatója e célra felépített tökéletes szerkezettel: alig 400 dollárért vásárolt, majd vezeték nélküli hálózatokat detektáló és támadó szoftverrel rendelkező ultrakönnyű számítógéppel felszerelt, kamerákkal és 3G-s modemmel irányított kvadrokopterrel szemléltette egy tavalyi szakkonferencián, hogy a művelet 600 dollárból kivitelezhető. A drón a célhelyszínhez közel landol, ha napenergiával működik, újratölti magát, aztán folytatja a körülötte lévő összes hálózat elleni támadást. A vezeték nélküli hálózat gyenge pontjait kihasználó hacker internetes irányítószerver helyett közvetlenül a drónon keresztül vezérli a botnetet, azaz gyakorlatilag azonosíthatatlan marad.

A szinte hangtalanul közlekedő apró légi járművek más veszélyeket is tartogatnak számunkra: észlelik, majd nyomon követik a mobiltelefonokat, amelyek alapján célszemélyeket azonosítanak be, és megtámadják otthoni hálózatuk legsebezhetőbb pontját.

Tanulságos, és a jövőre nézve elgondolkoztató, hogy egyik esetben sem az információs hálózat féltve őrzött „főkapuja", hanem a vezeték nélküli rendszerek kevésbé védett hátsó bejáratai, belső hálózatok hozzáférési pontjai szolgálnak célpontként.

Önvédő hálózatok

Talán a hátsó kapun támadók ellen is megoldást jelenthet a Kansasi Állami Egyetem az amerikai

KÖMLŐDI FERENC

légierő kutatási központja által támogatott projektje. A kutatók ugyanis az önmagát beállításainak és konfigurációjának automatikus változtatásaival hackertámadásoktól megvédő intelligens hálózat kivitelezésének lehetőségeit tanulmányozzák.

A légierő elvárása, hogy a tudósok mutassák ki, milyen hatásai lennének egy számítógépes rendszerben annak, ha a támadók célpontjai mozognának. A jelenlegi állapotban az üzemeltetők képtelenek megvédeni rendszereiket, és ha legalább ideig-óráig előnybe akarnak kerülni a támadókkal szemben, a kiberbiztonság egészét érintő koncepcionális változtatásokra van szükség.

Ha az eredmények kimutatják, hogy a „mozgócélpont-védekezés" (*moving-target defense*) hatékony, a későbbiekben megvizsgálják a rendszer kiépítéséhez szükséges befektetéseket és a várható előnyöket: arányban állnak-e egymással, megéri-e kivitelezni a hálózatot?

A „mozgócélpont-védekezés" kifejezés 2008-as, ötlete azonban már az ezredforduló környékén felmerült. Lényege, hogy a számítógépes hálózatok statikus konfigurációit érdemes lenne dinamikussá alakítani, mert így hatékonyabban lehetne védekezni a támadókkal szemben. A hálózat automatizáltan és véletlenszerűen változtatná konfigurációs beállításait: cserélgetné a szoftverek hálózati címeit, időnként áthelyezné a kritikusnak számító rendszeradatokat stb.

A legfontosabb, hogy a változtatások a támadónak kaotikusnak tűnjenek, de az üzemeltetők számára átláthatók maradjanak. Egy mai támadás tipikus forgatókönyve: a hacker felderíti például a webszervert, hogy hol található, milyen szoftver fut rajta. Ezt követően alaposan átvizsgálja, szoftveres és konfigurációs gyenge pontokat keres rajta, majd kiválasztja az ideális időpontot, és a biztonsági résen bejuttat egy kártékony kódot. Dinamikus hálózattal szemben nem működne ez a módszer.

Levélszemét-szűrés közösségi alapon

Egyre sűrűbben érik támadások a nem megfelelően védett elektronikus levelezőládákat is. A gyanútlan felhasználót levélszeméttel (*spam*) bombázzák, adathalászatnak (*phishing*) és más csalásoknak eshet áldozatul. A védekezés hatékonyabb, mint néhány esztendeje, optimálisnak azonban távolról sem nevezhető...

A legtöbb spamszűrő minden egyes elektronikus levelet elemezve próbálja kiszűrni a kéretlen üzeneteket: fejlécet, tartalmat, a feladó domainjét és egyéb elemeket egyaránt vizsgálnak. Nagyjából ugyanaz történik, mint a vírusellenes küzdelemben: a fejlesztők új technológiákkal próbálják azonosítani a legfrissebb levélszemét-típusokat, az „ellenoldal" kidolgozza az e technikákat kivédő módszereket, aztán a „jók" lépnek, és így tovább.

> ...a nyílt forráskódú alternatívák valójában biztonságosabbak, mint a drágább, védjegyzett (proprietary) programok.

A spamszűrők többsége vagy túl „szigorú" és valódi üzeneteket, főként hírleveleket is kiselejtez, vagy – a „hamis pozitívok" elkerülésével – egyszerűen nem végzi elég jól a munkát, és a levélszemét-küldemények mintegy negyede postaládánkban köt ki.

A mindenféle fiókot (POP3, IMAP, Exchange) és webalapú maileket is filterező Cloudmark DesktopOne különösen azért tűnik komoly előrelépésnek, mert egyrészt eltávolítja a szemetet, másrészt meghagyja a nehezen megkülönböztethető tényleges üzeneteket.

A spamet egymilliárdnál több felhasználó tapasztalatai alapján azonosítja: ha bárki gyanúsnak talál egy levelet, annak „ujjlenyomatával" ellátott üzenetet küld a központi adatbázisba. Ha ugyanazt az üzenetet sokan felcímkézik, a Cloudmark kiszűri a többi közül. A folyamatosan „jól teljesítő" felhasználók bónuszpontokat kapnak, a rendszer jobban megbízik bennük, ráadásul a módszerrel a magukat segítőkész usernek álcázó spamküldők megtévesztő tevékenysége is könnyebben felismerhető.

A Cloudmark ugyan nem végez 100 százalékos munkát, de a tapasztalatok alapján sokkal ritkábban hibázik, mint a többi a spamszűrő.

Védjegyzett vagy nyílt forráskódú programok?

Az információbiztonsági problémák egy érdekes kérdést is felvetnek: mennyire bízzunk a nyílt forráskódú megoldásokban?

Az egészségügy-informatikai rendszerek eladása világviszonylatban sokmilliárd dolláros iparág és üzlet. A magas költségek, a gyakran csődöt mondó, egymással kommunikációképtelen rendszerek ellenére a szakterület döntéshozói egyelőre idegenkednek a problémák nagy részére megoldást jelentő nyílt forráskódú szoftverektől (OSS – Open Source Software). Aggályaik legfőbb oka a biztonság és a megbízhatóság. Az angliai Warwick Egyetem Digitális Egészségügy Intézetének és a londoni UCL Egészségügyi Informatika és Multiprofesszionális Oktatás Központjának szakemberei arra a következtetésre jutottak, hogy a nyílt forráskódú alternatívák valójában biztonságosabbak, mint a drágább, védjegyzett (*proprietary*) programok.

Carl Reynolds (UCL) szerint ha a kód nyilvános és több fejlesztői közösség dolgozik rajta, a szoftver jobb minőségű lesz. *Jeremy Wyatt* (Warwick Egyetem) szerint kutatásaik megdöntik azt az elterjedt véleményt, hogy „mivel a kód nyilvános, a támadók könnyebben megtalálják és kihasználják a gyengeségeit." Bebizonyították, hogy nincs így, sőt, az OSS biztonságosabb más rendszereknél. A védjegyzett szoftverek gyakran az úgynevezett „biztonságos, mert homályos" érvelésen alapulnak, azaz mivel a rendszerek működése nem látható át, védettebbek a potenciális támadókkal szemben. Igen ám, de léteznek olyan eszközök, amelyekkel a kód felderíthető, módosítható. Még rosszabb, hogy ez az alapkoncepció gyakran eredményez gyenge minőségű kódot. Viszont ha a kód nyílt, a biztonsági rendszerhez független szakértők is hozzáférhetnek, többen több energiát fordítanak a hibák korrigálására.

A kutatók azt az érvelést is visszautasítják, mely szerint az OSS – mivel a szoftver bármely hibájára megbízhatatlanná válik – alapvetően sokkal kockázatosabb megoldás. A nagyvállalatok ugyanis az OSS implementálásáért és a supportcsomagért ugyanúgy fizetnek a beszállítóknak, mintha védjegyzett szoftvert használnának.

telenor Hipernet

Új Hipernet Heavy internetcsomaghoz *ajándék* okostelefon!

extra

- 2 év hűség, 2 év tarifamegtartás esetén
- ajándék Telenor OneTouch C androidos okostelefon Praktikum +Net csomagban

Az ajánlat 2012. 11. 13. és 2013. 01. 14. között, illetve a készlet erejéig érvényes. A kínált sávszélesség és a garantált le- és feltöltési sebesség a lefedettségi terület bármely kültéri pontján a mobil technológia sajátosságaira tekintettel: 0 Mbit/s. A minőségi mutatókra vonatkozó részletes szabályok az ÁSZF 4. sz. mellékletében találhatóak. Az ajánlat 5 napos visszavételi garanciával, illetve eszköz (pl. netbook, laptop, tablet) vásárlása esetén nem vehető igénybe. Telefonos Ügyfélszolgálat: 1220. www.telenor.hu, facebook.com/telenorhungary