SZÁMÍTÁSTECHNIKA

COMPUTERWORLD

ICT-STRATÉGIA DÖNTÉSHOZÓKNAK / ALAPÍTVA 1969 / 2012. MÁRCIUS 21. / XLIII. ÉVFOLYAM 11–12. SZÁM

/ INFORMÁCIÓBIZTONSÁG 2012-BEN

TRENDI BIZTONSÁG

AZ INFORMÁCIÓBIZTONSÁG ALAPVETŐ FELTÉTELE, HOGY A VÉDELEM KÖVESSE A LEGÚJABB FENYEGETETTSÉGEKET. CSAKHOGY A KOCKÁZATI TÉNYEZŐK RENDKÍVÜL GYORSAN VÁLTOZNAK, EZÉRT ÚJRA ÉS ÚJRA ELEMEZZÜK: MILYEN VESZÉLYEKKEL KELL SZÁMOLNI.

ÖSSZEÁLLÍTÁSUNK A 9–11. OLDALON

MODERNKORI VÁRVÉDELEM

A digitális erődítményeknek sokkal kifinomultabb technikákkal kell szembenézniük, ha adataikat biztonságban szeretnék tudni. » 16. oldal

CEBIT 2012

Mit mond a világ legnagyobb infokommunikációs szakkiállítása az iparág, a piac és a technológia állapotáról? » 18. oldal

9 770587 151006 12012

Ára: 495 Ft

IDG Communications HUNGARY

www.computerworld.hu

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
Főszerkesztő: Dervenkár István
Vezető szerkesztő: Sós Éva, Szilágyi Szabolcs
Online igazgató: Odrovics Szonja
Olvasószerkesztő, korrektor: Sz. Erdős Judit
Munkatársak: Dávid Imre, Kis Endre, Kömlődi Ferenc, Mallász Judit, Meixner Zoltán, Szalay Dániel, Tóth Lívia, Vass Enikő
Tipográfia: Berényi István
Szerkesztőségi ügyelet:
Cseresznye Anita – acseresznye@idg.hu
Telefon: 577-4302, fax: 266-4343
Munkatársaink elérhetőségeit megtalálja weboldalunkon: » www.computerworld.hu

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

TERJESZTÉS ÉS ÜGYFÉLSZOLGÁLAT
Terjesztési igazgató:
Babinecz Mónika – mbabinecz@idg.hu
Telefon: 577-4301, fax: 266-4343
» e-mail: terjesztes@idg.hu

MEDIASHOP: MEDIASHOP.IDG.HU

MARKETING
PR-munkatárs: Kovács Judit – jkovacs@idg.hu

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

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

AKTUÁLIS

FÓKUSZ

CÉGADAT

HORIZONT

ÁLLANDÓ ROVATAINK

TARTALOMKONCENTRÁCIÓ

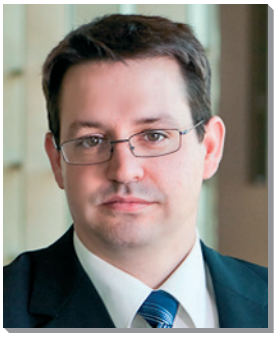
Aki a *Computerworld-Számítástechnika* több évtizedes történetét végigkísérte, jó néhány formátumváltást megélhetett. Lapunknak persze volt honnan inspirációt nyernie e téren is. Amerikai „Computerworld anyánk" ugyanis mindig a legkorszerűbb trendeket követte mind a formátum, mind a dizájn, mind pedig a tipográfia terén. Alapos előkészítés, több belső és olvasói teszt után döntöttünk: mi is követjük az anyacéget a tengerentúlon már bevált úton – átalakítjuk lapunk méretét.

Lezajlott a pilot projekt. Az Open Source 2012 konferenciánkra készített speciális lapszámunkon teszteltük, hogyan fogadják az új formátumot és az azzal járó szerkezeti változásokat olvasóink. A visszajelzések pozitívak voltak: koncentráltabb tartalom, gyorsabban áttekinthető cikkek, azaz – hogy egy informatikai rendszereknél gyakran használt fordulattal éljek – *user friendly* kezelőfelület párosul hatékonyabb funkcionalitással. Grafikusunk, *Berényi István* jó munkát végzett.

Lapszámunk mérete alig nagyobb egy iPadnél, így aki esetleg digitális kiadványokat terjesztő partnereinknél, a Dimagnál vagy a Digitalstandnál beszerezhető elektronikus *Computerworldöt* részesíti előnyben, tabletjén kényelmesen áttekintheti lapunk egy teljes oldalát anélkül, hogy folyton nagyítgatásra-kicsinyítgetésre kényszerülne. Amikor az átalakítást megvitattuk, fontos szempont volt az is, hogy lapunk új mérete emészthetőbbé tegye a nyomtatott formában megjelenő információkat az online tartalmakon szocializálódott olvasóink számára is.

Továbbra is várjuk véleményüket, javaslataikat a *Computerworld* új formátumával, tartalmával, az információk tálalási módjával kapcsolatban, hogy a jövőben is a leghatékonyabb formában szolgálhassuk olvasóinkat.

DERVENKÁR ISTVÁN
főszerkesztő



SCHEIDLER BALÁZS

ügyvezető
BalaBit Kft.

Biztonság motívum

Gyártóként megvan rá a lehetőségünk, hogy kívülről szemléljük a vállalatok IT-biztonsággal kapcsolatos törekvéseit. Ebből a kényelmes, megfelelően távoli pozícióból olyan áttekintés nyerhető, amelyet IT-vezetőként valószínűleg sosem kaphatnánk meg.

Ebből a bölcselkedésre is alkalmat adó helyzetünkből jól látszik, hogy mi az informatikai biztonsággal kapcsolatos alapvető probléma. Ez pedig a rossz motiváció miatt félresiklott cél. A szervezetek számára az IT-biztonság nem más, mint saját maguk védelme. Törekvéseik azt a célt szolgálják, hogy ne történjen incidens, ne terhelje a szervezetet kár.

A védelemre szánt erőforrások mennyiségét a kár lehetséges mértéke és valószínűsége alapján határozzák meg. Vagyis a saját maguk számára fontos folyamatokat, adatokat védelmezik leginkább. Vajon mi ezzel a probléma? Az, hogy a vállalatok nem csupán a saját adataikat és folyamataikat kezelik, hanem az alkalmazottakét, partnerekét és ügyfelekét is. E külső felek számára teljesen más például a kár várható mértéke, amit a másik oldalról sok esetben nem is lehet felmérni. Ezért a gyakorlatban a másik felet is érintő biztonsági intézkedések gyakran nincsenek összhangban az elvárásokkal.

Az ilyen típusú kockázatokra a szervezetek gyakran válaszolnak reaktív folyamattal. Vagyis egy alapszintű biztonsági szintet működtetnek, majd amennyiben mégis bekövetkezik az incidens, akkor szigorítanak. Az ebből következő szituációkban pedig gyakran az incidens eltitkolása a szervezetek racionális válasza, hogy az alapvető célnak megfelelően a saját kárukat minimalizálják.

Miért is kell a problémával globálisan foglalkozni? Azért, mert az üzleti világot nem egy és nem egyirányú üzleti folyamatok szövik át, kötik össze. Amíg az egyik folyamatban ránk van bízva mások adata, addig egy másikban mi vagyunk kénytelenek megbízni másban. Viszont a szervezetek alapvető motivációiból következően így senki nincs igazán biztonságban.

Aki tanult közgazdaságtant vagy kibernetikát, az tudja, hogy a hasonló anomáliákat a piac iterációs (evolúciós) folyamattal oldja fel. Vagyis lassan kialakulnak azok az ellenhatások, amelyek biztosítják a szervezetek számára a működésükhöz szükséges biztonságot. Például, ha az én hanyagságomból tönkremennek az ügyfeleim, akkor én is tönkremegyek. De már előbb is, mert az ügyfeleim elvándorolnak tőlem. Minél hatékonyabb ez a negatív visszacsatolás, annál magasabb lesz a globális biztonság.

A jelen problémája az, hogy a természetes folyamatok nem elég hatékonyak, illetve hogy a technológiai környezet olyan sebességgel változik, amely – átmenetileg legalábbis – komoly biztonsági deficitet teremtett.

A szabályozó (és önszabályozó) szervezetek fel is ismerték ezt a jelenséget, és ki is találtak rá egy kezelést. Ezt nevezzük ma *compliance*-nek, ez az a trend, amely ma leginkább mozgatja az IT-biztonsági beszerzéseket. A compliance vagy IT-megfelelőség tulajdonképpen a vállalatokra kényszerített biztonsági folyamat, amely nem a szervezetet védi, hanem a külső feleket a szervezettől. Az elképzelés jó volt, a gondot itt is a motivációk okozzák. A regulációk folyamatokat írnak elő, amelyek helyes működését rendszeres auditokkal ellenőrzik. Aki nem tudja teljesíteni az auditot, az szankciókkal szembesül.

A problémát az okozza, hogy az üzleti folyamat működtetőinek célja így nem a biztonság, hanem a sikeres audit. Az üzemeltetők az auditorban ellenérdekelt személyt látnak, akivel nem szabad megosztaniuk a két audit között tapasztalt problémákat, így az audit tervbe nem kerülnek be a tapasztalatok, a folyamat nem javul, vagyis a visszacsatolás nem valósul meg. A sikeres audit nem garantálja a megfelelő biztonságot, a vállalatok compliance ráfordításai idegen testként, kényszerű költségként türemkednek ki a szervezetből. Pedig megfelelő motiváció esetén lehetnének ezek a költések versenyképességet növelő beruházások is.

Nézzük, mi a megoldás! Nevezhetjük *Compliance 2.0*-nak vagy *Szakszerű Biztonságnak*. Ha a piac vagy a szabályozó szervezetek megfelelően szankcionálnák a biztonsági incidenseket, akkor helyére kerülnének a motivációk, ahol az audit csak eszköz, nem cél lehetne. Annyit elárulhatunk, hogy valamit már főznek Brüsszelben...

> A jelen problémája az, hogy a természetes folyamatok nem elég hatékonyak, illetve hogy a technológiai környezet olyan sebességgel változik, amely komoly biztonsági deficitet teremtett. – Scheidler Balázs, BalaBit Kft.

Hyde Tech Corner

Ezen a héten *Kiss Attila,* a BalaBit IT Security marketingvezetője, és *Fejes Zoltán,* a Telenor lakossági értékesítési igazgatója kommentálja a hét híreit, eseményeit. / összeállította: Tóth Lívia

Heti összeállításunkból megtudhatják, miért lyukas a Google pénztárcája, és az is kiderül, hogy mi állhat az okostelefon diadalmenetének a hátterében.

RÁJÁR A RÚD A WALLETRE

A Google fejlesztőinek egy súlyos sebezhetőséget kell megszüntetniük a Google Wallet alkalmazásban, ugyanis az bizonyos körülmények között jelentősen megkönnyítheti a tolvajok, csalók számára a károkozást.

» computerworld.hu/cikk/lyukas-google-penztarca

PC-TREND

Az okostelefonok világpiaci értékesítési száma tavaly megelőzte a személyiszámítógép-eladásokat, a Canalys azonban 2012-re már az okostelefon-értékesítések növekedési ütemének lassulását várja.

» computerworld.hu/cikk/tobb-smartphone-mint-pc

KISS ATTILA

MARKETINGVEZETŐ, BALABIT IT SECURITY

A Google által elkövetett hiba annyira alapvető, hogy akár alapjaiban kérdőjelezheti meg egy születőben lévő iparág jövőjét. Ha nem a Google az elkövető, akkor az ember még meg is tudna egyébként bocsátani. De az isten szerelmére! a Google a felhőalapú adattárolás egyik élharcosa. A Google az Android platform szülőatyja. A Google vezető szerepre tör a mobilfizetésben.

Itt nem egy programhibáról van szó, amit egyetlen ember követett el! Egy stratégiai termék alapvető működési elvéről beszélünk, amit normális esetben több tucat embernek kellett áttekinteni, köztük fejlesztőknek, felelős vezetőknek, biztonsági szakembereknek és marketingeseknek. Közülük egynek sem jutott eszébe, hogy a mobiltelefon egy apró számítógép, amit viszonylag könnyű elveszíteni? Vagy ezzel a kockázattal a készpénzhasználat teljes élményét akarták kínálni? Milyen lehet a Google termékeinek – de legalábbis az Androidnak a biztonsága, ha a vállalati folyamatok nem képesek egy ilyen banális, de iszonyú hiba kiszűrésére? A Microsoft a jó példa arra, hogy ha egy cég egyszer kiöli magából a képességet, hogy a felhasználók helyébe tudja magát képzelni, azt nagyon sokáig nem tudja visszaszerezni. De szintén a Microsoft a jó példa arra is, hogy versenytársak nélkül ez csak nekünk – felhasználóknak – probléma, a cég attól még szépen növekedhet.

FEJES ZOLTÁN

LAKOSSÁGI ÉRTÉKESÍTÉSI IGAZGATÓ, TELENOR

Szolgáltatásaink kialakításakor mi is folyamatosan figyeljük a hazai és nemzetközi trendeket. Saját, Magyarországon végzett kutatásaink is alátámasztják a nemzetközi piackutatók sajtóban publikált iparági megfigyeléseit: az online tartalomfogyasztás iránti növekvő fogékonyságot, a mobiltelefonon való internetezés iránti egyre nagyobb nyitottságot, valamint az okostelefonok népszerűségének erőteljes növekedését.

A Telenor több hullámban, a Free Association Kft.-vel közösen Magyarországon végzett felmérése szerint a mobiljukon internetezők aránya megközelíti a 30 százalékot. Emellett a mobilon való internethasználat intenzitása, rendszeressége is növekvő tendenciát mutat. 2011. februárban a megkérdezettek 37 százaléka, míg novemberben már 60 százaléka állította, hogy naponta többször kapcsolódik az internetre mobilján keresztül.

Az adatok alapján az okostelefon-tulajdonosok száma 2011. február és november között 7 százalékponttal növekedett. A növekedési tendencia a fiatalok körében egyébként szembetűnő: a 20–29 évesek 40 százaléka, a 15–19 éves korosztály 66 százaléka használ okosmobilt. Ez utóbbi korcsoportban három hónap alatt 20 százalékpontos a növekedés. Az emberek emellett egyre inkább mindennapos dolognak tartják, ha valaki okostelefont használ.

UNIT4: STABIL NÖVEKEDÉS / Növekvő árbevételről és a Software as a Service (SaaS) ágazat további erősödéséről számolt be 2011-es évre vonatkozó pénzügyi eredményeit illetően a UNIT4, amely a világ vezető vállalatiszoftver-szállítója a folyamatos változásban lévő vállalatok (Businesses Living IN Change – BLINC) piacán.

SAP BUSINESS ONE ONDEMAND / Az SAP bejelentette új megoldását, a kisméretű cégeknek kínált vállalatirányítási rendszerének felhő verzióját. Az SAP Business One OnDemand Magyarországon az első kibocsátási hullámban, 2012 második negyedévében jelenik meg. A rendszer 100 euró/hó/fő árazástól indul, de ez országonként és partneri ajánlatonként változhat.

ESET MOBILE SECURITY / A Mobilworld Congress 2012 konferencián és kiállításon mutatta be a vállalat a mobilkészülékek védelmére kifejlesztett termékeik zászlóshajóját, az ESET Mobile Security for Androidot. A rosszindulatú szoftverek elleni megoldás egyesíti a NOD32 antivírus hatékonyságát egy spamszűrő védelmével, sőt, a szoftverben még egy lopásgátló funkció is található.

[HÍRMOZAIK]

IDG-DELOITTE FELMÉRÉS

A vállalatok kezdik felmérni az IT-fenyegetések üzleti kockázatait

Az IT-terület legnagyobb kihívásának a biztonsági kérdések megoldását tartják a hazai vállalati vezetők –, derül ki az IDG és a Deloitte közelmúltban készült, közös felméréséből.

Az IT-területen a legnagyobb kihívást a biztonsági kérdések jelentik a hazai vállalati vezetők szemében, ami *Antal Lajos,* a Deloitte Zrt. informatikai biztonság és adatvédelem üzletágának vezetője szerint azzal magyarázható, hogy a vezetők (köztük a legnagyobb számban válaszadó első számú vállalati vezetők, illetve az IT-terület felső és középvezetői) kezdik felismerni a hiányos IT-biztonságban rejlő hatalmas üzleti kockázatokat vállalkozásukra nézve. Érdekes adat, hogy az IDG és a Deloitte Zrt. közös kutatása szerint bár sokan érzik a fenyegetések legkritikusabb formájának a külső támadásokat (hackertámadás, vírusok), a válaszadók többsége (59%) szerint ennél is nagyobb fenyegetést jelentenek a cégen belüli, emberi tényezők. Ilyen belső tényező lehet az akár véletlen hibából adódó, akár szándékos károkozás, de az adatszivárgás is, amelynek csatornái (és sokszor vétlen eszközei) szinte kivétel nélkül a saját alkalmazottak, még ha az értékes üzleti adatok megszerzésére irányuló támadás jó eséllyel a cégen kívülről indul is.

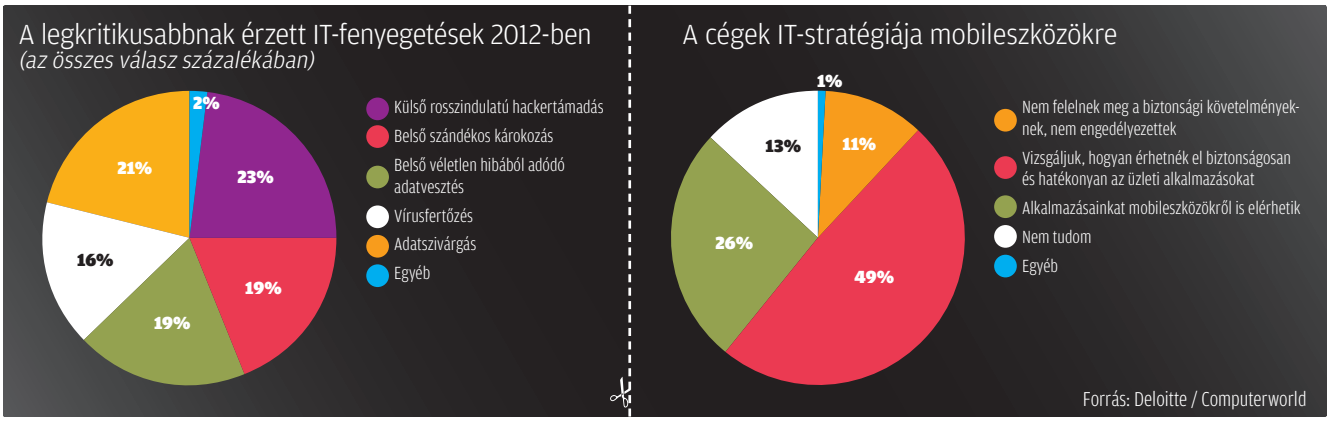
A felsorolt fenyegetések mindegyik típusa valós veszélyt jelent a vállalati, üzleti adatok biztonságára nézve. Az óvatosság azért is indokolt, mert a számítógépes bűnözői csoportok nemcsak egyre prominensebb áldozatokat ejtenek világszerte, hanem a tapasztalatok szerint a támadások száma is sűrűsödik, a célba vett vállalkozások köre pedig lényegesen bővül azóta, hogy a szervezett bűnözés felfedezte magának ezt a jelentős, illegális jövedelemforrást – mondta Antal Lajos. – Tévedés azt hinni, hogy a támadásoknak Magyarországon működő cégek nem lehetnek célpontjai, vagy hogy a bűnözők bizonyos vállalatméret alatt nem látnak fantáziát egy-egy célpontban. A támadások felépítése és a célpontok kiválasztása szinte minden esetben tudatos, a döntő szempont pedig a megszerezhető adatok „piaci" értéke, illetve az, hogy a kiszemelt cég óvatlansága mennyire könnyíti meg az illegális hozzáférést ezekhez a fontos vállalati adatokhoz.

A felhőalapú technológiák terjedésére utal, hogy a válaszadók 36 százaléka alkalmazza, további 28 százalékukat pedig komolyan foglalkoztatja a cloud computing alkalmazása saját cégénél. Ennek is megvannak a korlátai, mert az ilyen megoldásokat jellemzően azok a cégek választják, amelyek számára a módszer közvetlen, kézzelfogható előnyöket biztosít. Sok cég esetében eleve fel sem merül az igény, 23 százalékuk pedig a felhőalapú rendszerekkel összefüggő biztonsági kihívások miatt teljesen elzárkózik a technológia alkalmazásától. Hátráltathatja a cloudra épülő modellek és szolgáltatások széles körű terjedését az a múlt év decemberében megalkotott törvény is, amely korlátozza az adatok kiadását másnak.

A munkatársak saját mobileszközeinek vállalati hálózatba való „beszivárgása" egyre erősödő tendencia az elmúlt évek során. Fontos azonban megjegyezni, hogy a mobilitás számos előnye mellett mindez felkészülést is igényel a cégek részéről: a munkavállalók többsége saját eszközéről szeretné elérni a céges alkalmazásokat, ez pedig komoly biztonsági kihívásokat rejt magában. Mindenekelőtt le kell fektetni a mobileszközök használatának pontos irányelveit a vállalaton belül, és ezeket tudatosítani az érintett munkatársakban is. A hozzáférést biztosító platformok egységesítésén kívül az adatbiztonsági kérdésekre is megnyugtató válaszokat kell találni – magyarázta a Deloitte információbiztonsági szakértője.

Az IDG és a Deloitte Zrt. felmérésének további fontos megállapítása, hogy a 2012-ben tervezett vállalati IT-fejlesztéseknél a válaszadók várakozása szerint az üzleti igények diktálnak majd, míg a vállalatcsoporti elvárások és a compliance megfontolások sokkal kisebb súllyal befolyásolják majd a fejlesztések irányát.

Antal Lajos szerint a közeljövő IT-trendjeit az fogja meghatározni, hogy a hazai vállalatok hogyan birkóznak meg az új, vagy egyre lendületesebben terjedő eszközök és technológiák (például mobileszközök, cloud-technológia) kapcsán tömegesen felmerülő biztonsági kérdésekkel. A biztonságra fordított források általános szűkössége miatt kérdéses, hogy az informatikai költségvetésekben hajlandók lesznek-e a cégek elkülöníteni a szükséges újítások költségeit, kellő figyelmet fordítanak-e ezekre a kritikus biztonsági szempontokra, és képesek-e a fenyegetéseket komplex, körültekintő módon elemezni és kezelni.



CEBIT 2012, HANNOVER

Nagy memória és a folyamatok

A Software AG új generációs adatmenedzsment platformja, amely a cég in-memory és eseményelemző technológiáit egyesíti, áthidalja a tranzakciós és az analitikai alkalmazások közötti szakadékot, és 1000-szeres teljesítménynövekedést hozhat a Big Data típusú alkalmazásokban.

KIS ENDRE

A nagy teljesítményű analitikával a vállalatok nagy adattömegből is közel valós időben nyerhetnek ki üzleti szempontból értékes információt, így egyrészt felpörgethetik a döntéshozatal folyamatát, másrészt a működés monitorozásából származó adatok eddiginél sokkal nagyobb mennyiségét is röptében elemezhetik. Ezek alapján innovatív és rendkívül rugalmas folyamatokat tervezhetnek a jövőben.

A Software AG következő generációs adatmenedzsment platformja (Next-Generation Data Management Platform) a cég BigMemory, valamint webMethods Business Events technológiáját integrálja. A BigMemory, amely az amerikai Terracotta tavalyi felvásárlásával került a Software AG portfóliójába, egy Java-alapú in-memory technológia, amellyel a különböző forrásokból származó, akár több száz terabájtos adattömeg is rendkívüli gyorsasággal kezelhető a gépi memórián belül. A webMethods Business Events, amelyet a Software AG a tavalyi CeBIT-en jelentett be, az adatfolyamok valós idejű elemzésével az üzleti folyamatokban bekövetkező változások azonnali észlelését teszi lehetővé.

– A nagy adattömegek valós idejű elérésének és elemzésének lehetősége olyan transzparenciát biztosít, amely látványosan felgyorsítja a döntéshozatalt, lerövidíti az üzlet reakcióidejét – mondta *Karl-Heinz Streibich,* a Software AG vezérigazgatója Hannoverben, az idei CeBIT előestéjén megtartott sajtótájékoztatón. – A vállalatok így azonnal válaszolhatnak a piac változásaira, ami kulcsfontosságú sikertényező, platformunkkal jelentősen javíthatják majd versenyképességüket.

Valós idejű üzleti analitika

A Software AG következő generációs adatmenedzsment platformja ugyanis azokra a problémákra ad megoldást, amelyek a Big Data hagyományos adatmenedzsment eszközökkel történő kezelésekor lépnek fel, beleértve a vállalati IT-környezetben kialakult adatsilók egymástól elszigetelt működését, az új típusú adatbázisok megjelenését, valamint az alkalmazások által maximálisan lefoglalható memóriaterület méretének meghatározását.

A bejelentés szerint az új adatmenedzsment platform a nagy teljesítmény és méretezhetőség mellett rugalmasságot is biztosít, mivel a meglévő adatbázisokkal, az új típusú adatfolyamokkal és a vezető analitikai eszközökkel egyaránt könnyen integrálható lesz. A BigMemory adataggregációs szolgáltatásainak köszönhetően a vállalatok például a különböző környezetekből – tranzakciós és analitikai rendszerekből, relációs és nem relációs, Hadoop, NoSQL adatbázisokból és fájlrendszerekből, valamint közösségi hálókból – származó, strukturált és nem strukturált adatokat egyetlen, memórián belüli adattárban elemezhetik majd.

– BigMemory és Business Events technológiáink integrálásával az üzleti analitikát valós idejűvé tesszük – mondta *Wolfram Jost,* a Software AG technológiai igazgatója. – In-memory adatmenedzsment platformunkkal áthidaljuk a tranzakciós és az analitikai alkalmazások közötti szakadékot, és a rendszerek számára minimális késleltetésű, nagy teljesítményt biztosító hozzáférést adunk a nagy adattömegekhez, a hagyományos és az új típusú adatforrásokhoz. Ebben az értelemben a vállalati informatika jelene és jövője között építünk hidat.

A technológiai igazgató szerint a Software AG új generációs adatmenedzsment platformjának első elemei a BigMemory következő főverziójában jelennek majd meg, amely még az év vége előtt várható a Terracottától.

Extrém együttműködés

A Software AG hannoveri technológiai előadásain arról is beszámolt, hogy Extreme Collaboration néven keretrendszert fejleszt, amely közösségi funkciókkal fogja felruházni meglévő termékeit. A cég Pulse néven olyan mikroblog alkalmazást is készít, amely a vállalaton, valamint a partner- és ügyfélkörön belül segíti majd az együttműködést az alkalmazásokban és folyamatokban bekövetkező események követésén keresztül.

– A Forrester ezernél több vállalat körében készített felmérést a közösségi funkciókat biztosító szoftverek használatáról. A tanulmány rávilágított, hogy a szervezetek 34 százaléka már bevezetett, vagy jelenleg telepít ilyen alkalmazást – mondta *Matt Green,* a Software AG termékmenedzsmentért felelős alelnöke. – A cégek 26 százaléka a funkciók bővítésénél, a használat kiterjesztésénél tart. Az alkalmazottak új nemzedéke ugyanis nem a levelezést, hanem a közösségi alkalmazásokat használja együttműködésre, jobb híján a nyilvánosan elérhető szolgáltatásokat, és ez kockázatot jelent. A tiltás hiábavaló, ráadásul frusztrálja a munkavállalókat, ezért biztonságos megoldásokra van szükség.

Az Extreme Collaboration 2012 végén elsőként a Software AG Modelling-as-a-Service és Process Intelligence termékeit fogja közösségi funkciókkal gazdagítani, önálló termékként nem fog megjelenni. A Pulse viszont – amely a cég hannoveri standján már látható volt – az év közepétől elérhető lesz.

A Software AG standja több mint 30, referenciafolyamatokat tartalmazó iparági megoldást vonultatott fel

OPEN SOURCE 2012 – AZ INNOVÁCIÓ MOTORJA

2012 open source projektje: SuliX

A Computerworld idén is megrendezte a nyílt forráskódú fejlesztést feldolgozó konferenciáját. Az Open Source 2012 – Az innováció motorja című rendezvényen átadták az Év Informatikai Projektje díjat is. / *Computerworld*

Valóban innovatívak a nyílt forráskódú fejlesztések? Valóban lehet üzletet csinálni abból, hogy valaki szabadon hozzáférhetővé teszi terméke forráskódját? Valóban azt csinálhatunk a nyílt forráskóddal, amit akarunk? Valóban megbízhatók az opensource-fejlesztések? Egy sor kérdés, amelyekre az előadók megpróbálták megadni a választ.

Szentiványi Gábor (ULX) nyitó előadásában az innovációról beszélve kiemelte: több százezer nyílt forrású projekt van a világon, de ezek töredéke csupán vállalati szinten is megfelelő. Azok azonban olyanok, hogy egyre inkább felveszik a versenyt a tulajdonosi szoftverekkel. *Scheidler Balázs,* a múlt évben a syslog-ng fejlesztője erre hozott egy személyes példát, bemutatva, hogyan lett az általa még egyetemistaként készített syslog-ng-ből először közösségileg fejlesztett szoftver, majd jól jövedelmező kereskedelmi termék úgy, hogy közben a közösség is aktív maradt. *Puskás Norbert* (IQSYS) pedig azt mutatta be, hogyan lehet hasznosítani akár vállalati szinten is azt a tudást, amit a munkatársak hobbijuk során szereztek a nyílt forráskóddal. Az IQPortál rendszert például ilyen elemekből fejlesztették. *Banai Miklós* az EuroOffice-ban rejlő lehetőségeket taglalta, *Basa Richárd* pedig azt, hogy hogyan érdemes kialakítani opensource-stratégiát. Plenáris záró előadásában *Opre Zoltán,* az NFM Informatikai Helyettes Államtitkárság főosztályvezetője az elmúlt év eredményeiről, az állami szervezeteknél lefolytatott pilot projektek sikereiről számolt be, valamint megerősítette a *Vályi-Nagy Vilmos* által egy éve, az első Open Source konferencián megfogalmazott kormányzati szándékot: a nyílt forráskódú rendszerekkel is kell segíteni az infokommunikációs megoldások közötti verseny erősödését. Ebbe a tendenciába illik a tavaly év végén kiadott ODF kormányhatározat is. Az ebéd után az ODF Workshoppal, majd pedig két szekcióban folytatódott a munka.

A *Vállalattól az államig* című szekcióban terítékre került az open source ökoszisztéma működése vállalati rendszerekben *(Török Tamás, ULX),* a hallgatók iránytűt kaptak a nyílt forráskódú licencek útvesztőjéhez *(Telek Eszter, IPR Insights),* izgalmas összefoglalót az open source BI-rendszerek piacáról és piaci potenciáljáról *(Arató Bence, BI Consulting). Magyar Dénes,* az ISACA Budapest Chapter képviseletében az auditorok szempontjaival szembesítette az open source vállalati rendszereket. *Szegfű László* (Szeged, Polgármesteri Hivatal) pedig egy jól bevált, alapvetően nyílt forráskódú megoldásokra épülő rendszer működését mutatta be, nem elhallgatva a rendszer korlátait. Emellett nagy teret kapott az oktatás: *Mátó Péter* (FSF.hu), *Bánhegyesi Zoltán* (Leöwey Klára Gimnázium), Szentiványi Gábor (ULX) és *Koren Balázs* (GeoGebra) előadásaiban volt szó problémákról, például az oktatási intézmények folyamatainak bonyolultságáról, valamint lehetséges megoldásokról, például a SuliX rendszerről, illetve a GeoGebra és a Szabad út projektről.

A *DevCorner* szekcióban fejlesztők cserélték ki tapasztalataikat. A szekciónyitó előadásban *Koleszár Kázmér* és *Rakyta Péter* (Multiráció) az innovatív szoftverfejlesztésről beszélt az EuroOffice kiterjesztéseinek kapcsán. *Fischer Erik* pedig a OpenSolaris példáján mutatta be, hogyan élheti túl egy open source projekt az akvizíciót. Emellett volt Drupal–Joomla párbaj *(Palócz István és Perián János* előadásában), terítékre került az Android-fejlesztés *(Nagy Péter),* az open source fejlesztések tesztelése *(Beszédes Árpád),* a gyártói szoftverek és az open source rendszerelemek illesztése *(Eőry Szabolcs, IQSYS),* de a keresztplatformos fejlesztés kapcsán a QT-ről *(Gecse Attila, LogMeIn),* valamint az open source projektek fejlesztésében rejlő biztonsági problémák megoldásáról *(Pfeiffer Szilárd, BalaBit)* is hasznos ismereteket szereztek a jelenlévők.

A konferencia előadásairól készített felvételeink megtekinthetők a tv.computerworld.hu oldalon.

2012 OPEN SOURCE PROJEKTJE

A konferencia zárásakor lapunk főszerkesztője, *Dervenkár István* átadta a tavaly alapított Az Év Open Source Projektje díjat. Idén az öttagú zsűri – *Braun Péter,* a VISZ elnöke, az OTP Bank elnök-vezérigazgatói főtanácsadója, *Scheidler Balázs,* a BalaBit ügyvezetője, a 2011-ben díjazott syslog-ng kifejlesztője, *Mozsik Tibor,* a Bitport főszerkesztője, *Varga Perke Bálint* blogger (Buhera blog), valamint lapunk főszerkesztője – egyhangúlag az ULX Kft. pályázatát tartotta a legjobbnak. A SuliX szoftverrendszer, amelyet a Szentiványi Gábor vezette csapat oktatási intézmények részére fejlesztett ki, közel egy évtizedre visszatekintő fejlesztés végeredménye. A bírálók kiemelték a szoftvercsomag komplexitását, felhasználó-központú megközelítését, valamint hogy nagyszámú felhasználó áll mögötte – már több száz iskolában bevezették. Az ULX projektjében a nyíltság nemcsak jogi kategória, hanem a fejlesztés során alkalmazott irányelv is volt. „A létrehozott termék ígéretes lehetőséget teremt a nyílt forrású megoldások népszerűsítésére és az open source üzleti modellek létjogosultságát is jól példázza" – fogalmaztak a döntnökök.

> Eredményes védekezésre csak akkor van igazán esély, ha a mobileszközök felügyelete összekapcsolódik a már meglévő védelmi infrastruktúrákkal.

Trendi biztonság

Az információbiztonság megteremtésének egyik alapvető feltétele, hogy a védelemnek követnie kell a legújabb fenyegetettségeket. Mivel azonban napjainkban a kockázati tényezők rendkívül gyorsan változnak, célszerű áttekinteni, hogy az idei évben milyen veszélyekkel kell a leginkább számolni.

Már megszokhattuk, hogy a biztonsági cégek és a kiberbűnözés között kiélezett macska-egér háború alakult ki az elmúlt években, amely ahhoz vezetett, hogy egyre többfajta és mind kifinomultabb fenyegetettség jelent meg. Ezek egy része olyan biztonsági incidensekhez vezetett, amelyek nagyon komoly veszteségeket okoztak a cégeknek. Sajnos jelenleg semmiféle jel nem utal arra, hogy 2012-ben ez a kedvezőtlen helyzet jelentősebb mértékben javulna. Ezért a következőkben számos releváns biztonsági terület áttekintésével számba vesszük az idei év legtöbb figyelmet igénylő kockázati tényezőit.

Töretlen vírusterjesztés

A biztonsági trendek elemzését mivel is kezdhetnénk mással, mint a kártékony programokkal kapcsolatos fejlemények feltérképezésével, hiszen – nem meglepő módon – a védelmi eszközök fejlesztésével foglalkozó cégek többsége továbbra is meghatározó szerepet tulajdonít az ártalmas kódoknak. A számítógépes és egyre gyakrabban a mobilkárokozókra épülő támadások már eddig is sok esetben bizalmas adatok kiszivárgásához, illetéktelen kezekbe kerüléséhez vezettek. Az ilyen jellegű incidensek kormányzati szerveket, biztonsági beszállítókat, számos Fortune 500 vállalatot, valamint emberjogi és egyéb szervezetet is érintettek. „Biztos vagyok benne, hogy ez a trend 2012-ben és azt követően is folytatódni fog. A kémkedés sok száz éves története során mindig kihasználták az aktuális technológiai vívmányokat. Ugyan az internetes kémkedés sem mostanában kezdődött, de még nem is fejeződött be" – mondta *Rik Ferguson,* a Trend Micro kutatási és kommunikációs igazgatója.

A kártékony programok világában tavaly leginkább a Stuxnet és az utódjaként emlegetett Duqu károkozó hívta fel magára a figyelmet. A trendek arra engednek következtetni, hogy e két károkozó még csak a kezdetét jelentheti egy olyan folyamatnak, amelynek végkimenetelét nagyon nehéz megjósolni, hiszen már a Stuxnet is igazolta, hogy kritikus infrastruktúrák esetében is képes fejtörést okozni.

– Nagyon valószínű, hogy a közeljövőben látni fogjuk e fejlett károkozók újabb variánsait. Amíg a Duqu eredetileg dokumentumok összegyűjtésére specializálódott, aközben már előrevetítette, hogy képes lehet a Stuxnet felhasználásával elkövetett támadásokhoz hasonló akciók elősegítésére is – nyilatkozta *Gerry Egan,* a Symantec egyik igazgatója. Hasonlóan vélekedett *Jeff Hudson,* a Venafi elnök-vezérigazgatója is, aki szerint a Duqu következő variánsai hónapokon belül megjelenhetnek. Ezért már most olyan előkészületekre van szükség, amelyek révén az ilyen károkozásokra megfelelően lehet reagálni, illetve megelőző lépéseket lehet tenni.

Biztonsági szakértők szerint az olyan kártevők, mint amilyen a Stuxnet vagy a Duqu a jövőben ugyan előidézhetnek nemzetközi konfliktusokat, azonban jelenleg a kormányok, vállalatok inkább a kémkedések, illet-

KRISTÓF CSABA

TOVÁBBI BŐVÜLÉS ELŐTT AZ ANTIVÍRUS PIAC

A Canalys kutatói szerint a biztonsági piac idén tovább fog növekedni. Az elemzések szerint 2012-ben a vállalati szférában a biztonsági szoftverekre fordított kiadások akár 8,7 százalékkal is nőhetnek. Ha ez a jóslat beigazolódik, az egyben azt is jelentené, hogy e piacon világszinten 22,9 milliárd dolláros forgalmat lehetne elkönyvelni. Az elemzők úgy vélik, az antivírus szoftvereket az elmúlt időben egyre több kritika érte annak kapcsán, hogy azok nem tudják tartani a lépést a fenyegetettségekkel. A kritikák ellenére azonban ezek az alkalmazások továbbra is olyan alapvető védelmi eszközként funkcionálnak, amelyet nem lehet nélkülözni. A piaci előrejelzések szerint a vírusvédelmi termékek esetében 6,8 százalékos növekedés várható.
Az antivírus-fejlesztőknek 2012-ben kiemelt figyelmet kell fordítaniuk a kisvállalkozásokra. A Canalys szerint ugyanis e cégek sok esetben még mindig nem ismerték fel, hogy őket is számos fenyegetettség veszélyezteti, és nemcsak a nagyvállalatok kerülhetnek a kiberbűnözés látókörébe. A kisebb vállalkozások esetében az online értékesítést kell erősíteni, ugyanis ezek a cégek fogékonyabbak arra, hogy a szoftvereket interneten keresztül szerezzék be.

ve a bizalmas adatok kiszivárgása miatt aggódnak. Ezért előtérbe kerülnek az APT (Advanced Persistent Threat) fenyegetettségek, amelyek már eddig is jelentős károkat okoztak még a legkomolyabb védelmi arzenállal felvértezett rendszereknél is.

Célzott támadások

A fejlett, perzisztens fenyegetettségek több ízben bizonyították már, hogy a vállalatok, intézmények egyik legjelentősebb kockázati tényezőjének számítanak. Sajnos semmiféle jel nem utal arra, hogy az APT-alapú támadások a közeljövőben visszaszorulnának. Ez azért is problé-

léma, mert a védekezést jelentősen megnehezítik, és nemcsak a technológiai védelmet teszik próbára, hanem azon biztonsági intézkedéseket is, amelyek az emberi tényezők kezelésére irányulnak. Pedig nagyon sok vállalat esetében még mindig az emberek jelentik a védelem leggyengébb láncszemét, ugyanis ez teszi könnyű célponttá a szervezeteket. Ezért a rendszeres biztonsági oktatásokat nem szabad elhanyagolni.

A HTML5-re vár a kiberbűnözés

Az online támadások száma töretlenül növekszik, és a kiberbűnözés minden népszerű webes platformot, szolgáltatást célkeresztbe állít. Különösen sok kockázati tényező merül fel a közösségépítő webhelyek kapcsán. Miközben ezek biztonsági szempontból azt sugallják, hogy tiltani kell a munkahelyeken való elérésüket, aközben számos olyan üzleti, marketing szempont merül fel, amely pont a közösségépítők fontosságára hívja fel a figyelmet. A Barracuda Networks felmérése szerint a vállalatok 20 százaléka tiltja a LinkedIn használatát, míg például a Facebookot a szervezetek 31 százaléka blokkolja. Szabályozásra ugyanakkor nagy szükség van, méghozzá megfelelő kontrollok, ellenőrzés és felügyelet megvalósítása mellett. Ennek oka, hogy a közösségi oldalak egyrészt jelentős kockázatot jelentenek az adatszivárgást illetően, másrészt idén is arra lehet számítani, hogy egyre több hamis profil, spammelt üzenet jelenik majd meg, és mind intenzívebb vírusterjesztés fog zajlani e népszerű online felületeken.

A Sophos szerint 2012-ben a webbiztonság szempontjából a HTML5 hozhatja a legjelentősebb változást. Ahogy a HTML5 támogatottsága és népszerűsége nőni fog, úgy kerül majd mindinkább a támadások középpontjába. A biztonsági cég kutatói szerint a HTML5 egyrészt újabb fenyegetettségek forrásául szolgálhat, másrészt azonban számos szempontból hozzá is járulhat a biztonsághoz, például a validációs lehetőségek kiterjesztésével, valamint a böngészőkhöz használt bővítmények számának bizonyos mértékű csökkentésével. Ami a kockázatokat illeti, a legjelentősebb problémákhoz a nem megfelelően kivitelezett helyi adattárolás, a cookie-k elhanyagolt kezelése, illetve a clickjacking vezethet. Emellett nem szabad figyelmen kívül hagyni azt a tényt sem, hogy a böngészőkre mind több feladat hárul, ezért azok sérülékenységeinek kockázata a jelenleginél is fokozottabban jelentkezhet majd.

Egyre ütősebb DDoS-támadások

Egyes hackercsoportok előszeretettel alkalmazzák azokat a támadó technikákat, amelyek révén képesek lehetnek megbénítani egyes rendszereket, vagy akár teljes infrastruktúrákat. Az idén is több alkalommal volt már példa arra, hogy egyes csoportosulások, például szerzői jogi kérdések, az internetezés szabadsága vagy hatósági intézkedések miatt jelentős szervezeteket állítottak célkeresztbe. Az egyik legnagyobb port kavart esemény a Megaupload leállítása kapcsán következett be, amikor az FBI, az Amerikai Igazságügyi Minisztérium és más

A kémkedés sok száz éves története során mindig kihasználták az aktuális technológiai vívmányokat. Ugyan az internetes kémkedés sem mostanában kezdődött, de még nem is fejeződött be.

nemzetközi szerverezetek weboldalai is hosszabb-rövidebb időre megbénultak.

Az Arbor Networks felmérése szerint tíz szervezet közül kilencnek havonta átlagosan minimum egy elosztott szolgáltatásmegtagadási támadással kell szembenéznie, ami az előző évekhez képest a DDoS-akciók számának jelentős növekedését jelenti. Azonban a DDoS kapcsán nem kizárólag a támadások számának emelkedése okozza a problémát, hanem az is, hogy az incidensek mind intenzívebben ostromolják az informatikai infrastruktúrákat. Tavaly az elosztott szolgáltatásmegtagadási események 13 százaléka több mint 10 Gbps-os sávszélességet emésztett fel.

Az összehangolt támadások kapcsán fontos megjegyezni, hogy azok a korábbi évektől eltérően már elsősorban nem a versenytársak megbénítását célozzák, hanem sokkal inkább politikai és ideológiai indíttatásúak. A tapasztalat azt mutatja, hogy az ilyen célokkal tevékenykedő támadók sokkal makacsabbak és kitartóbbak, s emiatt az incidensek mind rendszeresebben következnek be. A DDoS jövőjének latolgatása során a biztonsági kutatók arra jutottak, hogy több, de a korábbiaknál rövidebb ideig tartó támadásokra kell felkészülni, amelyek alkalmanként egyre jelentősebb túlterhelést okoznak majd a célkeresztbe került rendszerek esetében.

Fókuszban a mobilbiztonság

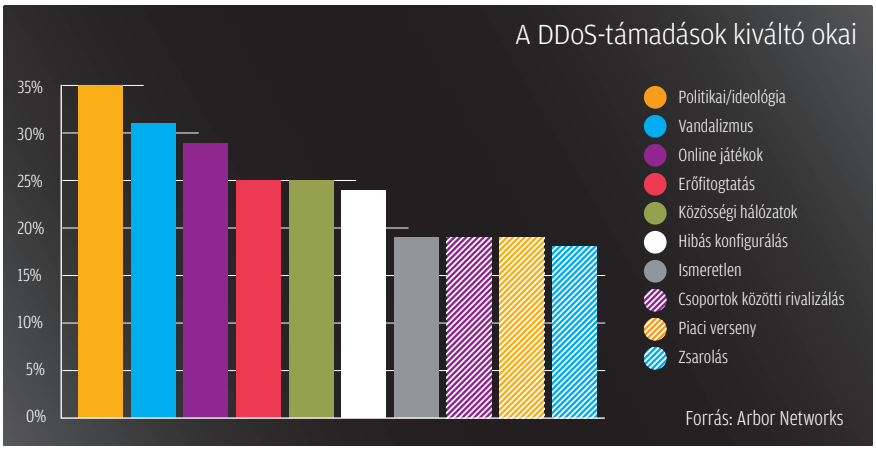
Megfigyelhető, hogy a vállalatok életében egyre meghatározóbb szerephez jutnak az okostelefonok és a mobileszközök, amelyekhez mind több tevékenység és üzleti folyamat kapcsolódik. Miközben a mobilkészülékekkel kapcsolatos „függőség" növekszik, aközben a biztonsági kockázatok is fokozódnak. Ennek elsősorban az az oka, hogy az okostelefonok terjedésével párhuzamosan a munkavállalók mind gyakrabban kezdik a saját, magántelefonjaikat üzleti célokra is használni, ez pedig amellett, hogy adatbiztonsági problémákat vet fel, a felügyeletet is jelentősen megnehezíti.

A mobilbiztonsági trendeket számos kockázati tényező befolyásolja, hiszen nem lehet figyelmen kívül hagyni, hogy a mobilkészüléknek könnyedén lába kelhet, és a rajta tárolt bizalmas adatok illetéktelen kezekbe juthatnak. Emellett az adatlopásokat kártékony programok is elősegíthetik. Noha napjainkban a legtöbbször Android-kompatibilis károkozókról lehet hallani, ez nem jelenti azt, hogy egyéb platformok esetében ne kellene kockázatokkal számolni. Eredményes védekezésre csak akkor van igazán esély, ha a mobileszközök felügyelete összekapcsolódik a már meglévő védelmi infrastruktúrákkal. Ezért idén számítani lehet arra, hogy a biztonsági cégek egyre gyakrabban fognak olyan termékeket bejelenteni, amelyek a mobilbiztonságot a lehetőségekhez mérten platformfüggetlenül, egységes módon teszik majd kezelhetővé és kontrollálhatóvá. Mindehhozzá olyan módon, hogy a központi adminisztráció az okostelefonokra és a hordozható készülékekre is kiterjeszthetővé váljon.

Cloud computing

A cloud computing térnyerését továbbra is jelentősen befolyásolják a biztonsági aggodalmak. Ahhoz azonban, hogy pontosabb képet lehessen kapni a jelen és a közeljövő kockázatairól, ketté kell választani a felhőalapú rendszerek értékelését. Ennek oka, hogy a cloud-technológiák a biztonságra negatív és pozitív hatást gyakorolhatnak. Az előbbi hatások elsősorban abban nyilvánulnak meg, hogy a szervezetek nem tudnak megfelelő kontrollt kialakítani a saját adataik felett, és esetenként a hozzáférés-kezelés megfelelő megvalósítására vagy annak helyi védelmi rendszerekkel történő integrálására sincsenek meg a kellő eszközök. Ugyanakkor a felhőalapú megoldásoknak számos pozitív hozadékuk van a biztonságra nézve. Elég, ha csak a cloud-technológiákat felvonultató vírusvédelemre vagy az offsite adatmentésekre gondolunk. Nyilvánvalóan e védelmi megoldások még jelentős fejlődés előtt állnak, de néhány feladat elvégzéséhez már napjainkban is segítséget nyújtanak. Kétség sem férhet hozzá, hogy a biztonsági cégek idén sok felhőalapú, védelmi fejlesztésről fogják lerántani a leplet, de nagy kérdés, hogy a piac miként fogadja majd ezeket.

Összefoglalásul elmondható, hogy a szervezetek IT-biztonsági és compliance csapatainak idén is mozgalmasan telnek majd napjaik, ugyanis a kiberbűnözésnek továbbra is komoly mennyiségű muníciója van.



HARDVERALAPÚ VÍRUSVÉDELEM

Az antivírus technológiák kapcsán egyre inkább olyan nézet kezd terjedni, miszerint a hagyományos, szoftveralapú védelem nem elégséges, ugyanis számos számítógépes károkozó terjed, amely képes megkerülni a víruskereső alkalmazások által jelentett védelmi vonalakat. A biztonsági trendek egyértelműen azt mutatják: mélyebb szinten kell megvalósítani a vírusvédelmet annak érdekében, hogy például az MBR-t vagy akár a BIOS-t veszélyeztető kártékony kódok felismerésére is legyen lehetőség. A McAfee Intel általi felvásárlása is a hardveralapú technológiák létjogosultságát sugallta.

Mitől féljünk 2012-ben?

Ne a világ végétől!

A mobileszközök egyre nagyobb mértékű elterjedése és az ehhez szorosan kapcsolódó hiperkonnektivitás, a Big Data mind nagyobbá válása, a felhő térnyerése és a szárnyait bontogató kiberterrorizmus fogják a leginkább kihívások elé állítani az IT-biztonság világát a közeljövőben.

SÓS ÉVA

Egy felmérés szerint 2012-ben mindenki legalább egy, internetelléréssel rendelkező új eszközt birtokol majd. Annak pedig, hogy lassan egy kávéautomata is képes csatlakozni a világhálóra, mind a cégek, mind a magánszemélyek számára rengeteg veszélyforrása van. Az adatok megóvása ebben a dinamikusan fejlődő és változó környezetben kulcsfontosságú kérdés lesz az IT-biztonság szakértői számára.

Hiperkonnektivitás. A szó, amely leginkább tükrözi a technológia mai világát, valamint azt, milyen biztonsági kihívásokkal néznek szembe a vállalatok és a vásárlók 2012-ben. Az internetkapcsolat elterjedése hihetetlen méreteket ölt. A mobileszközök és a webes alkalmazások hivatottak megkönnyíteni életünket, és új lehetőségeket teremteni számunkra. De ebben a „hiperkapcsolt" világban, amikor az üzlet és a magánélet közötti határvonal elmosódik, fontossá válik, hogy felelősen használjuk a technológia vívmányait. A személyes adataink megszerzésére irányuló támadások száma az elmúlt öt évben megháromszorozódott, pedig az okostelefonok és a tabletek igazán csak az elmúlt két-három évben kezdtek elterjedni.

A közeljövő fenyegetései

Nézzük meg, milyen biztonsági fenyegetésekkel nézünk szembe a közeljövőben!

A mobileszközöket célzó malwarek száma növekedni fog, a cégeknek komoly kihívást jelent majd, hogy felvegyék velük a küzdelmet. A nyilvánvaló célpontok az okostelefonok és a tabletek, főleg az Android operációs rendszer, „köszönhetően" egyre növekvő piaci részesedésének és annak, hogy a Google üdvöskéje nyitott innovatív platform. De minden más elterjedtebb OS-t használó mobileszköz is fokozott mértékű támadásnak lesz kitéve.

A támadások forrása – főleg Androidon – immár nem a böngészővel történő letöltések, hanem a fertőzött alkalmazások lesznek. Mivel ezek még gyerekcipőben járnak és nincsenek megfelelően felügyelve, az ellenőrizetlen alkalmazásboltok lesznek a mobil malwarek fő fészkei. De a kiberbűnözők megtalálják majd a módját, hogy ártalmas alkalmazásaikat a hivatalos app store-okba is bejuttassák. A fertőzött alkalmazás aztán az okostelefon segítségével könnyen szétterjed az ismerősök között, vagy a céges hálózaton.

Hogy a felhasználók biztonságát szavatolják, a szolgáltatók harmadik féllel fogják bevizsgáltatni alkalmazásaikat. Mindemellett a vállalatok elvárják majd, hogy az alkalmazottak által használt alkalmazások megfeleljenek bizonyos elvárásoknak. Az iparág várhatóan bevezet egy pontozási rendszert, amely segíti a felhasználókat, hogy megfelelő, a vállalatok által jóváhagyott alkalmazásokat töltsenek le céges eszközeikre.

Ahogy az emberek egyre gyakrabban használják majd a mobileszközöket banki információk megtekintésére, pénzátutalásra, jótékony célú adakozásra, valamint szolgáltatásokért és árucikkekért való fizetésre, megnyílik az út a kiberbűnözők előtt, akik megtalálják a megoldást, hogy kikerüljék a védelmeket.

Ahhoz, hogy biztonságosabbá tegyék az online bankolást, a bankszektor olyan alkalmazásokat kínál majd, amelyeknek erős beépített védelmi rétegeik vannak.

A hiperkonnektivitással együtt járnak az egyre növekvő személyazonossági és magánéleti kihívások. A mai üzleti környezetben mind több felhasználónak kell egyre több adathoz hozzáférni egyre több helyről. Emiatt erősebb adatvédelemre lesz szükség a hozzáférési pontokon, méghozzá erősebb tanúsítványok használatával és biztonságosabb access control rendszerek telepítésével, valamint fejlett naplómenedzsment- és naplóelemzéssel.

Ahogy növekszik a mobileszközök és az egészségügyi alkalmazások száma, egyre könnyebb lesz mondjuk, egy okostelefont diabétesz teszterré vagy pulzusmérővé alakítani. Egyes szakértők szerint ennek egyenes következménye lesz, hogy az egészségügy a mobileszközöket diagnosztikai eszközökként kezeli majd vagy a diagnosztikai eszközök vállnak mobillá. Ahogy ezek a kategóriák egybemosódnak és egyre több adatot osztanak meg más eszközökkel és felhasználókkal, ugyanazoknak a veszélyeknek lesznek kitéve, mint a számítógépek és más hálózatra kötött eszközök.

Az IPv6-ra való átállás, valamint az azt használó eszközök új kihívásokkal állítják majd szembe az otthoni felhasználókat és a profikat egyaránt. Ráadásul az internet két másik alapvető mechanizmusa a BGP (border gateway protocoll) és a DNS (domain name system) is új generációs verzióval áll elő. Az új szabványok felgyorsítják a régi, úgynevezett *legacy* rendszerek cseréjét, élénkítve a piacot, de átmenetileg akár komolyan is visszafogva bizonyos üzleti folyamatokat.

A Big Data tovább nő, akárcsak az általa igényelt biztonság is. Ahogy a cégek felismerik a nagyobb adatbázisok üzleti előnyeit, úgy még több adatot kezdenek gyűjteni, még több adatmennyiséget lesznek kénytelenek kezelni, és ez a trend jelenleg egyre gyorsulni látszik. Az üzleti felhasználók mind több üzleti lehetőséget teremtenek adataik elemzésével, eközben erősödik a megbízhatóságon alapuló döntéshozatal is. A cégek arra használják fel az adatokat, hogy új üzleti lehetőségeket teremtsenek, ugyanakkor a siker érdekében erősítik a bizonyítékokon alapuló döntéshozatalt. De erre csak akkor lesznek képesek, ha az adathalmazt biztonságban tudják.

Az online személyazonosság-lopások növekvő száma miatt az online identitás biztosítása többé nem lesz opcionális. Az ügyfelek, a cégek és a kormányzati hivatalok megoldást keresnek identitásuk jobb megőrzésére. Ezek a csoportok a magánszektor felé fordulnak majd, hogy költséghatékony megoldást szerezzenek identitásuk biztosítására, és hogy nyugodtabban élhessék online életüket.

> **Az adatsértéssel (data breach) járó esetek több mint kilencven százalékáért** külső támadás, és nem belső probléma tehető felelőssé.

A közösségi hálózatok egyre népszerűbbekké válnak, ami növekvő mértékben vonzza az adathalászokat. Ahogy az okos készülékek felhasználóinak száma nő, még szükségesebb lesz a tudatos és biztonságos számítógép-használat oktatása. A közösségi hálózatoknak pedig egyre jobb védelmet kell biztosítaniuk a spammerek és az adathalászat ellen, noha elkerülhetetlen, hogy szofisztikált módszerekkel továbbra is elcsábítsák a usereket veszélyes weboldalakra, vagy rávegyék őket, hogy kiadják személyes adataikat.

Cloud computing

A tavalyi év tapasztalata, hogy egyre több cég választott felhőalapú megoldásokat az IT-költségek csökkentése érdekében. Szakértők szerint 2012-ben a cloud megoldások további expanziója várható. A cégvezetők egy része már egy ideje aggódik a felhőalapú szolgáltatások biztonsága miatt, hiszen még mindig nincs meg a tökéletes gyakorlat, ami a felhő biztonságát illeti. Várhatóan 2012-ben ez változni fog, az IT és az üzleti menedzsmenteknek le kell fektetniük a szabályokat arról, hogy milyen körülmények között, milyen felhőt lehet használni.

A felhőszolgáltatóknak fontos lesz, hogy megfeleljenek a konkrét szabályozási irányelveknek, és biztonságos megoldásokat kínáljanak a komoly biztonsági kívánalmakat követelő szervezeteknek. Ez a trend már elkezdődött, hiszen a szolgáltatók már annak alapján kapnak tanúsítványt, hogy megfelelnek-e a specifikus iparági szabványoknak.

A közelmúltban lezajlott RSA-konferencián nem kisebb személyiség hívta fel a jelen lévő szakértők figyelmét a felhő fontosságára, mint *Michael McConnell,* az amerikai Nemzetbiztonsági Hivatal, az NSA korábbi igazgatója.

McConnell szerint globális gazdasági háború zajlik, ahol a kibergazadasági kémkedés a frontvonal, az USA pedig folyamatosan elveszíti a csatákat. Szerinte az Egyesült Államoknak nincs olyan jól kialakult gazdasági kémhálózata, mint más országoknak. A témával kapcsolatban egy igen érdekes hasonlatot hozott fel. „Nincs a bolygón olyan entitás, amely védett lenne a behatolástól. Egy sem! A szervezetnek, amit magam mögött hagytam, hatalmas örököse van. A második világháborúban feltörtük és elolvastuk a kódokat még a náci frontparancsnokok előtt. Gondoljanak ennek jelentőségére egy globális konfliktus esetén."

2012 a kiberterrorizmus éve lesz?

Ha már háború, nem szabad elmenni szó nélkül a hadviselés átalakulása mellett. Ma már kevés konfliktus számít a hagyományos értelemben vett háború kategóriájába; a harcokat elsősorban nem nemzet vívja nemzet ellen, hanem a nyugati demokráciák küzdenek a „terroristák", „felkelők" és „milicisták" legyőzése érdekében. E szélsőségesek eszköztárában az internet még főképpen mint kapcsolattartó vagy tagtoborzó eszköz szerepel. De amiképpen az RSA-konferencián San Franciscóban is elhangzott, aggodalomra ad okot, hogy a terroristák között akadnak olyanok, akik elég tudással rendelkeznek ahhoz, hogy különböző rendszerekbe betörjenek.

Mikko Hypponen, az F-Secure vezető kutatója kiberterrorizmusról szóló előadása során elmondta: a szélsőségesek – radikális iszlamisták, csecsen terroristák, fehér felsőbbrendűséget hirdető csoportok – egyre inkább odafigyelnek arra, hogy biztosítsák internetes kommunikációjukat és elrejtsék a terhelő bizonyítékokat számítógépeiken. Hypponen szerint saját fájl- és e-mail titkosító eszközöket fejlesztettek ki, amelyeket lehetetlen feltörni. Ennél azonban sokkal aggasztóbb, hogy egyes tagok valószínűleg komoly hackertudás birtokában vannak, amely tudást szívesen meg is osztják hasonszőrű társaikkal. Fórumaikon egyes felhasználók olyan eszközök használatát segítő útmutatókat tesznek közzé, mint a Metasploit, BackTrack Linux vagy a Maltego.

Az ipari folyamirányítási, azaz SCADA rendszerek például a kiberterroristák elsődleges célpontjai lehetnek a jövőben. Mára ott tartunk, hogy nem kell feltétlenül odamenni például a felrobbantani vagy megrongálni kívánt gáthoz, hanem akár távolról, egy kibertámadás keretében is elvégezhetjük az akciót. Az ehhez szükséges technológiák bizony már léteznek.

BIZTONSÁGOS ARCHIVÁLÁS KKV-KNAK

Itt az adat, hol az adat...

SZALAY DÁNIEL

Ma már léteznek olyan megoldások, amelyekkel akár emberi beavatkozás nélkül, teljesen automatikusan és ingyen vagy nagyon kedvező díjért készülhetnek biztonsági mentések akár a felhőbe, akár egyszerűen egy külső merevlemezre. Mivel és hogyan archiváljanak a kkv-k?

Bár egy adatvesztés súlyosabb esetben egy céget akár örökre elsodorhat a piacról, főleg a kisvállalkozások még mindig elhanyagolják ezt a kérdést. Aligha van manapság olyan vállalkozás Magyarországon, amely ne használna munkája során legalább egy számítógépet. Legtöbbször ezen végzik a számlázást, a vevőkkel és szállítókkal való kapcsolattartást, tárolják a kimenő árajánlatokat és még számtalan más, a cég szempontjából ma már mindennapos, ám üzletkritikusnak tekinthető adatot. Ha e feladatok közül valamit akár csak egy-két napig nem tudnak elvégezni, annak súlyos következményei lehetnek a vállalat üzleti eredményeire és az ott dolgozók életére. Mindezek ellenére a magyarországi kkv-k hozzáállása ma még sokszor nem annyira professzionális ezekhez a kérdésekhez, helyenként még informatikus sincs, aki odafigyelne például az adatok biztonságára, az archiválásra. Tudták-e például, hogy az 1–9 főt foglalkoztató vállalkozások mindössze 23 százaléka veszi igénybe rendszergazda vagy professzionális informatikai cég segítségét? Ezek után lehet tippelni, vajon hány helyen figyelnek oda kellőképpen az adatok biztonságos archiválására...

Teljesen automatikussá tehető

Amikor e sorokat írni kezdtem, az Ubuntu Linuxomon a képernyő jobb felső sarkában épp megjelent egy figyelmeztető ablak, hogy immár több mint két hete nem készítettem biztonsági másolatot a számítógépem tartalmáról, többhetes munkával készülő cikkeimről, fényképeimről és más, számomra fontos, sokszor pótolhatatlan állományaimról. A rendszer azt javasolta, hogy csatlakoztassam a géphez az amúgy archiválásra használatos külső merevlemezemet. Miután engedelmeskedtem, az ebben a linuxos disztribúcióban „gyárilag" megtalálható biztonsági megoldás azonnal megkezdte az archiválás előkészítését. Csak a titkosításhoz használt PGP-s jelszavamat kellett megadni, amivel megakadályozható, hogy ha az amúgy távfelügyeletre kötött, riasztóval is védett objektumból eltulajdonítanák a kizárólag backupra használt külső merevlemezemet, annak tartalmához illetéktelen személyek hozzáférjenek.

Amennyiben a számítógépemet esetleg ellopnák tőlem, vagy meghibásodna a merevlemezem tartalma, biztos vagyok benne, hogy a legfontosabb adataim helyreállíthatók lennének, a munkát szinte ugyanott tudnám folytatni, mint a történtek előtt. Kivéve talán a két archiválás között képződött dokumentumokat, de ha ez súlyos rizikót jelentene számomra, egyrészt csökkenthetem az archiválások között eltelő időt, másrészt az Ubuntu azt is támogatja, hogy a gépemről folyamatosan automatikusan biztonsági másolat készüljön akár az Ubuntu One privát felhőjébe is. (A tárhely 5 gigabájtig ingyenes, a felett havi 2,99 vagy évi 29,99 dollárért további 20-20 gigabájtnyi helyet bérelhetünk. Erről bővebben itt: **https://one.ubuntu.com/services**)

Bizonyos dokumentumaimat egyébként eleve a felhőben, a Google Docsban készítem és tárolom. És bár vannak, akik szkeptikusak a cloud-technológia biztonságát illetően, egy igazán megbízható szolgáltató esetében aligha lehet ebből probléma. Ráadásul az Ubuntuba beépített Déjà Dup (így hívják az előbbiekben említett „gyári" archiváló megoldást) támogatja az adatok titkosított formában való archiválását is, így még ha valaki hozzá is férne a felhőhöz, ott is csak .GPG végű, azaz titkosított fájlokat találna.

Aki amúgy nem bízik a cloudos megoldásokban és külső egységre sem tud menteni, még jó néhány mentési alternatíva közül választhat. A Déjà Dup így például FTP szerverre, WebDAVra, SSH-ra, és Windows-megosztásra (Windows Network) is archivál. Beállítható az is, hogy a biztonsági másolatokat mennyi ideig őrizze meg a tároló, ami azért fontos, mert célszerű, hogy ne csak egy mentésünk legyen.

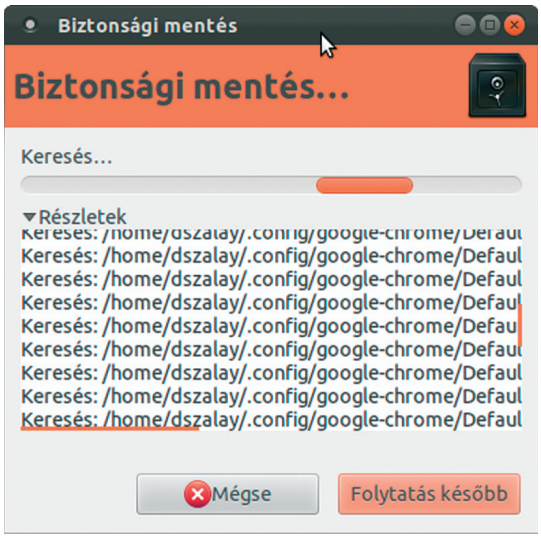
Régebben egyébként – sokakhoz hasonlóan – én sem voltam ilyen előrelátó. Bár tudtam, hogy a biztonsági mentések adott esetben egyszer még jól jöhetnek – mivel a backup-készítés túlságosan körülményes és időigényes volt, és a határidők szorításában mindig akadt valami fontosabb teendőm –, a hónap előrehaladtával egyre ritkábban készítettem mentéseket. Végül pedig el is feledkeztem erről. Ennek a fajta lazaságomnak meg is lett a következménye: többévnyi adat, köztük pótolhatatlan cikkeim, családi és más képeim, levelezésem és egy számlázóprogram adatállománya veszett el egy hirtelen fellépett merevlemez-hiba következtében. És bár próbálkoztam adatmentéssel foglalkozó cégnél is, sajnos ők sem jártak sikerrel. A sérült merevlemezt azóta is szétcsavarozva,

> Aki amúgy nem bízik a cloudos megoldásokban és külső egységre sem tud menteni, még jó néhány mentési alternatíva közül választhat.

dekorációként őrzöm, tartalmáról pedig végérvényesen le kellett mondanom.

Amikor kezdtem felocsúdni az első sokk után, még azon is elgondolkodtam, hogy esetleg RAID-es adattárolót kellene beszerezni, hogy ha az egyik merevlemez megsérülne, mindig legyen másolat mindenről. Erre ugyan nem került sor végül, de azóta sokkal komolyabban veszem az archiválást, főleg, amióta a közelmúltban megjelent archiváló programok jobbá váltak, mint elődeik. Nagyon egyszerűen és sok részletre kiterjedően beállíthatók, és ma már egyáltalán nem „macerás" a backupkészítés. Képesek arra ezek a megoldások, hogy egy mentés készítésekor, akár a háttérben dolgozva, az érdemi munkavégzést nem akadályozva gyorsan összehasonlítsák a backupban lévő fájlok tartalmát a gépünkön lévő állományok tartalmával. Így csak a megváltozott tartalmakat kell újra kiírni. Az egész folyamat lényegében felhasználói beavatkozást nem igényel, minden automatizálható, és legfeljebb egy kis ablak megjelenéséből értesül a felhasználó, hogy a biztonsági mentés elindult, illetve ha nem egy szerverre vagy a cloudba történik a mentés, akkor kéri a gép a külső merevlemez csatlakoztatását az USB-portra. (Egy ilyen merevlemez ára – 1 terabájtos méretben – körülbelül 20 ezer forint, ez aligha vethető össze azzal a kárral, amit egy adatvesztés egy kkv számára okozhat.)

És hogy a biztonsági mentések készítése mennyire nem pénz kérdése, arról sokat elmond, hogy számtalan, a Déjà Duphoz hasonló, ingyenes, nyílt forráskódú és GNU/GPL licenc alá eső megoldás létezik a piacon, amelyek legalább alapvédelmet jelenthetnek egy kkv-nak, természetesen nem csak Linuxon. Nagyon kedvelt és ingyenes megoldás például az Areca Backup, amelyből windowsos és linuxos változatot is találunk az interneten, de a sort még hosszan folytathatnánk.



Munkában a Déjà Dup

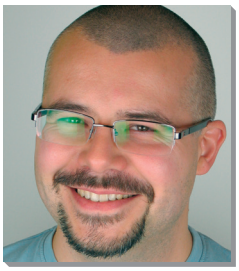
Magyar felhős megoldások kkv-knak

A kis- és középvállalati mentésekre egyébként idehaza is egyre több szolgáltató szakosodik, és mindinkább jellemző trend, hogy beruházást nem igénylő, felhőalapú szolgáltatást kínálnak. A Magyar Telekom például ezt a szegmenst célozza a belső adatok és információk szakszerű tárolására és védelmére specializálódott, bérelhető Virtulaso Server termékével és az online archiválási rendszert nyújtó Virtualoso BackUp megoldásával. Ezek a havidíjas termékek lehetővé teszik a vállalkozások számára, hogy nagyobb beruházási költség nélkül gondoskodhassanak a biztonságról. A Virtualoso BackUp használatával a cégeknek nem kell napi szinten foglalkozniuk informatikai problémáikkal, hiszen a szolgáltatás olyan online archiválási rendszert kínál, amely automatikus biztonsági mentést készít a saját telephelyen üzemelő szerverekről és az egyedi IP-címmel rendelkező számítógépekről, majd a Telekom rendkívül magas rendelkezésre állású, fegyveres őrök és különböző technikai eszközök által védett adatközpontjában tárolja azokat. A szolgáltatás havi nettó 20 Ft/gigabájt/nap áron igénybe is vehető. Nagy előnye, hogy nem igényel beruházást, és 24 órás szakértői támogatás is tartozik hozzá, ráadásul jól kiegészítheti a távközlési cég más, kkv-knak szóló felhőalapú megoldását. De épp lapzártánkkor a GTS is elindult egy nagyon hasonló konstrukciójú megoldással, a GTS Backuppal. „A vállalatok egyre gyakrabban ismerik fel, hogy az IT nem az alaptevékenységük. Új outsourcing szolgáltatásunk segít nekik abban, hogy a vállalkozásukra koncentráljanak, mivel nem kell foglalkozniuk a tervezéssel, a beszerzéssel, a szerződéskötéssel és a konfigurálással" – mondta *Marcin Kotlarski,* a GTS termékigazgatója, aki szerint egy ilyen megoldás segít csökkenteni a fejlődő üzleti igények által okozott stresszt. Olyan platformfüggetlen biztonsági, adatmentési és helyreállítási szolgáltatásról van szó, amely garantálja az üzletmenet folytonosságát, függetlenül a forrásadatok fizikai elhelyezkedésétől. A GTS Backup a legegyszerűbb módon gondoskodik az ügyfelek adatainak biztonsági mentéséről, illetve helyreállításáról. A szolgáltatást úgy tervezték, hogy biztosítsa és fenntartsa az üzleti adattárolás folytonosságát, akár a GTS adatközpontjaiban, akár az ügyfelek saját helyszínein elhelyezett szervereken. A szolgáltatások fő előnyei közé tartozik a rugalmas méretezhetőség, vagyis több száz gigabájttól akár több terabájtig is használható; továbbá a költségek tervezhetősége, hiszen a szolgáltatás – csakúgy mint az MTelekom megoldása – az ügyfél aktuális igényeihez igazodva havidíjért vehető igénybe. Végül a többszintű tárolási rendszer három tárolási teljesítménnyel alkalmas a különböző igények kielégítésére. További előny a megbízható D2D (disk-to-disk) adatmentés, amit nem érint az egyedi meghajtók meghibásodása.

Mivel az adatok mindkét cég esetében professzionális adatközpontokon belül találhatók, az iparág vezető fizikai védelmi és adatbiztonsági rendszereivel felszerelve (CCTV-rendszer, biztonsági chip belépőkártyák, tűzvédelem, 24 órás megfigyelés/ellenőrzés, zárható termek, és egyéb fizikai biztonsági eszközök), úgy gondoljuk, aligha tudnak a kkv-k ezeknél a megoldásoknál biztonságosabb módon adatot tárolni. Persze van, aki számára ez sem elég.

A hibrid mentés

A cloudos mentési lehetőségek megjelenésével párhuzamosan felmerült az igény az úgynevezett hibrid mentésre is. Ennek lényege, hogy ötvözik a helyi és a felhőalapú adatmentő, illetve helyreállító eszközöket, ezzel tovább fokozva a redundanciát. Így egy plusz védelmi szintként jelentkezik a felhőalapú szolgáltatás, de attól sem kell tartani, hogy mi történik akkor, ha a cloudos szolgáltató eltűnne egyik pillanatról a másikra a süllyesztőben, vagy a cloudos tárhelyszolgáltatónál következik be valamilyen technikai zűr. Ilyen hibrid biztonsági megoldást mutatott be például pár napja a CA Technologies kifejezetten kisvállalkozásokat célozva, *ARCserve D2D On Demand néven.* Az új megoldás a távoli adattároláshoz a Windows Azure-t hívja segítségül. A CA ARCserve D2D On Demand támogatja a szabadalmaztatás alatt álló Infinite Incremental (I2) technológiát is, melynek célja, hogy a gyakori mentésekből eredő erőforrás-használatot minimalizálja, és a biztonsági feladatok által okozott esetleges teljesítménycsökkenés hatását mérsékelje. Emellett hozzájárul a gyorsabb helyreállításhoz, és lehetőséget biztosít teljes rendszerek eltérő hardverre vagy akár virtuális környezetbe való visszaállítására. Az ARCserve D2D On Demandhoz alapesetben 25 GB kapacitású tárhely tartozik a Microsoft Azure infrastruktúrájában, és havi vagy éves díjért vehető igénybe.



SZILÁGYI SZABOLCS

ADATKÖZPONTOK FIZIKAI VÉDELME

Modernkori várvédelem

Nemcsak a digitális behatolóktól kell megvédeni a kritikus központokat, hanem a fizikai betörésektől is. Biometria, kártyás azonosítás, belépőkódok – ilyen a modernkori várvédelem.

Anno ostromgépekkel, gyalogsági rohammal és kiéheztetéssel próbálták bevenni a középkori várakat; az épületek jelentőségének elvesztésével átalakult a foglalásra éhes betörők repertoárja is. Immár a digitális erődítmények jelentenek célpontot, ennek megfelelően sokkal kifinomultabb technikákkal kell szembenézniük az adataikat biztonságban tudni vágyó szolgáltatóknak. Szerencsére a forró szuroknál és a gyilokjáróra telepített íjászoknál már fejlettebb védelmi megoldások állnak rendelkezésre.

Mielőtt akárcsak egyetlen eurót is kiadnánk egy adatközpont fizikai védelmére, alaposan meg kell tervezni, mire és mennyit költünk – ideális esetben még az adatközpont létrehozása előtt. Természetesen gondos mérlegelést követően kell kiválasztani az adott helyzetnek legmegfelelőbb megoldásokat, amelyeknek nemcsak hatékonyaknak, hanem költségtakarékosaknak is kell lenniük. Közel sincsenek tehát egyszerű helyzetben a CIO-k, amikor tervezésre kerül a sor.

Minél kevesebb ember, annál kevesebb hibalehetőség

A fizikai védelem ráadásul nem csak direkt, szándékos tevékenység ellen kell, hogy biztonságot nyújtson. Számos tanulmány – köztük a Schneider Electricé – igazolja, hogy az adatközponti leállások mintegy 60 százaléka emberi beavatkozás miatt következik be. Véletlen balesetek és tévedések sora – rosszul felcímkézett eszközök, leejtett vagy eláztatott berendezések, elgépelt parancsok stb. – vezethet a kritikus rendszerek ideiglenes lebénulásához. Mivel az emberi tényező teljesen nem iktatható ki ebben a környezetben sem, ezért törekedni kell a humán beavatkozás minimalizálására, illetve ezen esetek konzekvens ellenőrzésére és naplózására.

Ennek egyik fontos elemét képviseli az azonosítási technológia, amely ugyanolyan gyorsan változik, mint az általa védeni hivatott létesítmény. Ugyanakkor az alkalmazott technikától függetlenül változatlan a cél: távol tartani a jogosulatlan és/vagy károkozási szándékkal közelítő embereket a rendszerhez való hozzáféréstől. Az ehhez vezető út első lépéseként meg kell határozni a védeni kívánt területeket, illetve a hozzáférési szabályokat. Ennél sokkal nagyobb kihívást jelent a következő fázis, vagyis annak eldöntése, miként lehet a tervet a sosem tökéletes technológiával megvalósítani.

Legyen szó akár ujjlenyomat- és tenyérmintázat-ellenőrzésről, íriszszkennelésről, okoskártyák vagy arcjellemzők használatáról, a lényeg ugyanaz: biztonsággal azonosítani kell a belépni szándékozót, és tudni kell, hogy mit is akar a rendszerben. Ez a *„ki? és miért?" – who and why? – alapprobléma.* Száz százalékig kijátszhatatlan rendszer nem létezik, emellett nagyjából ökölszabálynak mondható, hogy minél magasabb arányú védelmet akarunk, annál többe kerül. Egy egyszerű kártyás azonosítást például jóval könnyebb becsapni, mint egy íriszazonosításra épülőt, ám utóbbi jóval drágábban is valósítható meg. Ott van még a szigorú költségvetés korlátja. Hiába tudja egy CIO, hogy mennyire fontos egy magas szintű (és drága) megoldás, ha annak szükségességéről nem tudja meggyőzni a pénzügyi vezetőt, akkor kénytelen beérni egy alacsonyabb védelmi rendszerrel.

Mit védjünk?

Lássuk kicsit konkrétabban, milyen területek védelmét is kell megszervezni! A Schneider Electric kétféleképpen csoportosítja a biztosítandó tereket: koncentrikus, azaz körkörös és egymás melletti régiókra osztja őket. Előbbi tovább oszlik a terület határára, az épülethatárra, a számítógépes területre, a számítógépteremre és az eszközök közvetlen környezetére (rackek), utóbbi pedig a következőképp osztható fel: látogatói területek, irodák és eszközpark. Koncentrikus védelmi stratégia esetén a védekezésnek mélysége van; ahogy haladunk befelé, az egyre kényesebb részek felé, úgy kell szigorodniuk, erősödniük a biztonsági rendszereknek is.

Ugyanakkor eltérő védelmi megoldásokat kell alkalmazni eltérő biztonsági fenyegetéseknél. Amíg egy biztonsági ajtó esetében a lopás veszélye gyakorlatilag kizárt, addig a szervereket kiszolgáló infrastruktúra egyes elemeinél – tartalék áramforrások, aggregátorok stb. – inkább ilyen jellegű incidensnek nagy az esélye.

Mindegyik módszernek vannak előnyei és hátrányai, kombinálásukkal tovább fokozható az adatközpont védelme.

Kitől védjük?

Háromféle módon azonosíthatjuk az adatközpontba bejutni kívánókat. Vagy annak alapján, hogy mit birtokol, vagy a tudására alapozva, illetve arra, hogy ki is ő valójában. Az első a legolcsóbb – és legkevésbé biztonságos – módszer: ilyenkor az illetőnek elegendő valamilyen tárgyat (kulcs, kártya, token stb.) magánál tartania. Értelemszerűen ez az azonosítás nem garantálja, hogy tényleg jogosult-e az illető a belépésére, csak azt, hogy a tárgyat eredetileg birtoklónak van rá engedélye.

Nagyobb biztonságot jelent a tudásalapú védelem, hiszen az nem lopható el, ugyanakkor – akaratlanul is – megosztható. Ezt a szintet képviseli egy kódzáras ajtó vagy a jelszavas számítógép-beléptető rendszer. Az emberi tényező azonban gyakran csökkenti a védelem szintjét, hiszen az egyszerű jelszavakat viszonylag könnyű kitalálni vagy feltörni, a bonyolultakat pedig egyszerűvé teszik maguk a felhasználók azzal, hogy leírják.

Sok tekintetben a harmadik megoldás jelenti a legjobb védelmet. A felhasználó valamely fizikai jegyein – ujjlenyomat, írisz, retina, arc, hang, kéz, kézírás, esetleg ezek kombinációján – alapuló, azaz biometrikus azonosítása azonban többnyire a legdrágább módszer is. Amint említettük, a biometrikus ellenőrzés nagyon megbízható abban az esetben, ha sikerrel jár az azonosítás. Ha nem sikerül, akkor is többnyire fals negatív eredményt ad a rendszer, vagyis nehéz átverni, inkább annak nagyobb az esélye, hogy a legitim felhasználót sem engedi át a rendszer.

Mindegyik módszernek vannak tehát előnyei és hátrányai, kombinálásukkal pedig tovább fokozható az adatközpont védelme. A korábban említett koncentrikus védelmi megközelítés esetén például a külső, kevésbé érzékeny területek biztosítása történhet tárgyalapú azonosítással, a rackekhez való hozzáférés pedig biometrikus alapokon. Az egyes területeken belül is lehet variálni a felsorolt megoldásokat: például a létesítmény területére való belépéshez azonosító kártyára és PIN-kód használatára van szükség, a számítógépteremhez viszont már egy másik azonosító kódra és egy biometrikus adatra. E rendszerek többségének hálózati csatlakozása is van, így távolról felügyelhető, ellenőrizhető, szükség esetén riasztás továbbítására használható. Ezzel kezelhetők maradnak a költségek, és az adatközpont minden része az elvárt szintű védelmet kapja.

Eszközök a védelemben

Természetesen különböző eszközöket igényelnek az egyes védelmi rendszerek. Az első esetben a belépést valamilyen tárgyiasult azonosító kulcs adja, leggyakrabban valamilyen kártya. Számos paraméter határozza meg, hogy milyen típust használnak adott környezetben: a token újraprogramozhatósága, hamisíthatóságának nehézsége, a rajta eltárolt adatok mennyisége, a kártya és a leolvasó költsége stb.

Leggyakrabban a mágnescsíkos kártyák teljesítenek szolgálatot, amelyek csíkja hordozza az információt, ezt ellenőrzi a leolvasó készülék. Nagyon alacsony szintű védelmet ad a vonalkódos kártya, könnyű hamisíthatósága miatt, míg az RFID-del szerelt, azaz rádiófrekvenciás kártyák a kényelmet szolgálják azzal, hogy nem igényelnek közvetlen érintést az olvasóval. A legfejlettebb szintet az úgynevezett okoskártyák képviselik, amelyek szilíciumlapkát tartalmaznak. Parányi chipjük révén komolyabb mennyiségű adat tárolására is képesek, és mivel csupán ez a parányi elektronika jelenti a lényeget, akár a korábbi kártyás rendszer frissítésével is használatba vehetők.

A második szintet képviselő tudásalapú védelem már nem a felhasználónál levő tárgy birtoklására épít, hanem a fejében levő tudásra. Ez a fajta hozzáférés-védelem jellemzően kódokkal dolgozik, amelyeket kicsiny numerikus billentyűzeten vagy komplett számítógépes klaviatúrán kell begépelni. Hatékonysága fokozható a kódok rendszeres időközönkénti cseréjével.

Végül a korábban említett biometria eszközeire is érdemes néhány szót szánni. Kétségtelen, hogy egy íriszalapú azonosító rendszer kialakítása többe kerül, mint egy belépőkártyás megoldásé, ám az ember fizikai paraméterein alapuló védelmi szisztémák a számítástechnika fejlődésével egyre olcsóbbá válnak. Gondoljunk csak a vállalati felhasználásra tervezett laptopokra, amelyek billentyűzetén szinte kivétel nélkül megtalálható a többnyire a touchpad környékére helyezett ujjlenyomat-olvasó – tehát nem is olyan ritka a biometrikus azonosítás, mint gondolnánk.

Amint azt az előbbiekben is tárgyaltuk, ezeknek a rendszereknek komoly hátulütője az úgynevezett hamis elutasítás. A védelem szigorúsága miatt nagyon érzékenyre kalibrált rendszerek azon felhasználók hozzáférési kérelmét is elutasíthatják, akik egyébként legitim tevékenységet végeznének az adott helyszínen, nem várt frusztrációt okozva ezzel számukra. Pont e működési módszer miatt nagyon ritka a hamis pozitív, azaz téves elfogadás, amikor illetéktelen számára tesz lehetővé belépést egy rendszerbe a biometrikus azonosítás. Természetesen az azonosító megoldás érzékenysége, küszöbértéke kalibrálható, így az egyes telepítések között – még akár ugyanazon gyártótól származó eszközök használata esetében is – jelentős eltérés mutatkozhat a hamis negatív/pozitív identifikáció arányát illetően.

A biometrikus beléptető rendszereknél nemcsak a téves eredmény okozhat frusztrációt a felhasználóknál, de a teljes eljárással szemben is kialakulhat ellenszenv. Ennek oka, hogy egyes megoldásokat túlságosan invazívnak találnak a létesítményben tartózkodók; jellemzően ilyenek a retinaszkennerek, amelyekhez alig pár centiméteres közelségbe kell hajolnia a belépni szándékozónak, amikor a szemét bántó fénysugár pásztázza át.

Kiegészítő megoldások

Hiába azonosítottuk a felhasználót kétséget kizáróan, ha mögötte esetleg valaki más be tud jutni az ellenőrzési procedúra alatt. Ennek elkerüléséhez általában olyan beléptető rendszereket alkalmaznak, amelyek megakadályozzák, hogy egyszerre egynél több ember haladhasson át az azonosítási ponton (gyakran használnak ilyen megoldásokat a nyugat-európai metrókban). Fokozható a védelem zárt láncú kamerahálózat telepítésével, melynek révén vizuális adat nyerhető minden, a kamerák látóterében tartózkodó emberről.

A fontosabb belépési pontokra humán erőforrás állítható, az őröknek ugyanis egyszerre van biometrikus és tárgyalapú azonosítási funkciójuk, ráadásul a digitális rendszerek átverésére kieszelt trükkök is hatástalanok maradnak velük szemben. Emellett érzékelők garmadája állhat a védelmi rendszerek rendelkezésére: hőt, nyomást, mozgást és sok egyéb környezeti paramétert figyelhetnek, illetve riaszthatnak a megadott intervallumtól való eltérés esetén.

Igen változatos módszerekkel lehet tehát megvédeni egy adatközpontot a fizikai behatolási kísérletektől. Az alkalmazott megoldások számának és minőségének csak a költségvetés szab határt, amelyet a védelmi eljárások megfelelő kombinálásával lehet maximálisan kihasználni. Noha egy adatközpont egészét nézve marginális annak esélye, hogy a telepítés többe kerül, mint a védendő adatok értéke, az egyes, kevésbé fontos területek biztosításánál előfordulhat a költségek elszaladása. Komplex tervezéssel nemcsak megelőzhető ez a nem kívánt jelenség, hanem az elvártnak megfelelő magas szintű biztonság is létrehozható.

A CeBIT üzleti IT-megoldásokat felvonultató pavilonjaiban a felhőben és mobileszközökön elérhető üzleti alkalmazások, valamint innovatív analitikai eszközök uralták a standokat.

Bizaloméptés a felhőkben

Egyetlen mondatban nehéz lenne összefoglalni, hogy a CeBIT, amely a korábbi években elszenvedett méretcsökkenés ellenére továbbra is a világ legnagyobb infokommunikációs szakkiállításának számít, mit mond az iparág, a piac és a technológia állapotáról. Ha mégis kísérletet tennénk erre, akkor a mondat a számítási felhőkről szólna.

KIS ENDRE

A hannoveri vásárváros 24 pavilonjában ugyanis a standokon jóformán nem szerepelt olyan hardver- vagy szoftvertermék, lakossági vagy vállalati, kormányzati piacra szánt alkalmazás, megoldás, amely nem kötődött volna valamilyen módon az interneten, a felhőben elérhető szolgáltatásokhoz, adatokhoz és erőforrásokhoz.

A technológia készen áll –, üzente az idei CeBIT a szervezők által választott vezérmotívumán – a bizalom kezelésén – keresztül. A felhasználók biztonságérzetét szükséges erősíteni ahhoz, hogy a cloud computing lehetőségei igazán kibontakozhassanak és a számítási felhők újabb lendületet adjanak a piacnak, illetve szélesebb értelemben véve a gazdaságnak.

A felhőalapú megoldások potenciáljára világított rá az Experton Group tanulmánya is, amelynek CeBIT-en közzétett adatai szerint a piaci szegmens szereplői idén egyedül Németországban 5,3 milliárd eurós árbevételre számíthatnak – ez 47 százalékos növekedés lesz a tavalyi forgalomhoz képest. A tanulmány készítői úgy vélik, a felhőalapú megoldások piaca 2016-ra 17 milliárd euróra nőhet Németországban.

Vállalatirányítás, ahogy tetszik

Az Experton Group derűlátását a kiállítók kínálata híven tükrözte. Egyetlen példát kiragadva, az SAP a CeBIT-en jelentette be Business One OnDemand felhőalapú vállalatirányítási rendszerét. A szolgáltatás a tervek szerint az év második felétől egyszerre 18 országban válik elérhetővé a szoftvercég partnerein – idehaza a Magyar Telekomon – keresztül, havidíja felhasználónként várhatóan 100 euró körül alakul majd.

Az SAP Business One OnDemand a vállalatirányítási rendszer teljes funkcionalitását kínálja, amely az értékesítés, a beszerzés, a raktárkezelés és a pénzügy területét egyaránt lefedi. Az SAP folyamatos licencopciókat fog kínálni a vállalatirányítási rendszert helyben telepítő, illetve felhőben elérő vállalatoknak, ami még nagyobb rugalmasságot biztosít a Business One alkalmazás igény szerinti használatához.

A szolgáltatás az SAP jelenleg is elérhető, szintén felhőalapú Business ByDesign megoldásait fogja kiegészíteni, melyek a középvállalatokat célozzák. A cég ezek körét is bővítette, illetve frissítette. Hannoverben mutatta be utazásiköltség-kezelő alkalmazását, valamint a beszerzést és az értékesítést segítő on-demand megoldások következő verzióját. Az SAP a múlt év végén vásárolta fel a kaliforniai SuccessFactors céget, amely 3500 vállalat, 15 millió felhasználó számára biztosít humántőke-menedzsmentszolgáltatásokat. A most lezáruló akvizíció is jelzi, hogy a felhőszolgáltatások egyre fontosabb szerephez jutnak az SAP stratégiájában, a szoftver-

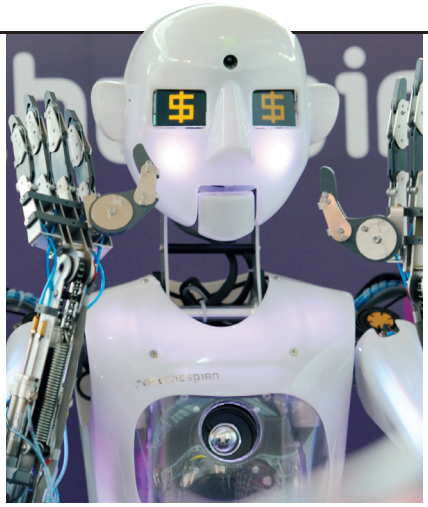
cég 2015-ben már 2 milliárd euró árbevételre számít ezen a területen.

Urbánus megoldások és a robotok

A bizalom és a biztonság kérdése persze a felhőszolgáltatásokon túl is számos összefüggésben releváns. A BITKOM – az infokommunikációs iparág német szakmai szervezete – például arra hívta fel a figyelmet, hogy minden harmadik vállalat elégtelennek tartja eddigi IT-biztonsági intézkedéseit. Amíg az informatikai cégek 95 százalékának van katasztrófaelhárító terve, addig ez az arány más iparágakban csupán 50 százalék. Összességében a CeBIT Global Conferences, a kiállítás konferenciaprogramjának másfél ezer előadása foglalkozott a bizalom és a biztonság problémakörével, amelyeken 130 kormányküldöttség is részt vett; az eszmecserébe bekapcsolódott *Neelie Kroes* és *Viviane Reding* európai uniós biztos is.

Az adatok biztonsága és a felhasználók bizalma különösen fontos az e-government szolgáltatások és a kormányzatoknak adott más informatikai megoldások vonatkozásában, amelyek idén is pavilonokat töltöttek meg Hannoverben. Az IBM például a CeBIT díszvendégével, Brazíliával karöltve mutatta be azt a projektet, amely a közbiztonság javítására irányul Rio de Janeiróban. A 2014-es foci vb-nek és a 2016-os nyári olimpiának otthont adó város infrastrukturális fejlesztései a figyelem középpontjában állnak. Brazília – amely épp a CeBIT idején vált a világ 6. legnagyobb gazdaságává, megelőzve az Egyesült Királyságot – nyolc év alatt 130 milliárd dollárt költ ezekre a projektekre.

Rio de Janeiro intelligens irányítóközpontja az IBM Smarter Cities kezdeményezésének keretében valósul meg, amely a városok hatékonyabb működtetését, az élhetőbb és fenntartható urbánus környezet kialakítását célozza. A központ több mint 30 kormányzati és közhivatali informatikai rendszer adatait integrálja annak érdekében, hogy a 6,3 milliós város gyorsabban reagálhasson a különböző krízishelyzetekre, és azokat hatékonyabban kezelhesse – mondta *Jose Carlos Duarte Goncalves,* az IBM brazil leányvállalatának technológiai igazgatója. A favelákban, a hegyoldalakra épült negyedekben különösen nagy veszélyt jelentenek a kiadós esőzéseket követő áradások és földcsuszamlások – 2010 áprilisában egy trópusi ciklon 200 halálos áldozatot követelt és több millió dolláros kárt okozott. Az IBM Research kutatói ezért egy nagy felbontású időjárás-előrejelző és hidrológiai modellező rendszert is fejlesztenek Rio de Janeiro számára,



RoboThespian: az ékesszóló, kifinomultan gesztikuláló robot tárlatvezetőként dolgozik

amely 48 órával előbb jelzi, ha nagy mennyiségű csapadék várható, így a lakosok szükség esetén időben evakuálhatók lesznek.

A CeBIT üzleti IT-megoldásokat felvonultató pavilonjaiban a felhőben és mobileszközökön elérhető üzleti alkalmazások, valamint innovatív analitikai eszközök uralták a standokat. A közösségi hálókban rejlő üzleti lehetőségeket például a salesforce.com támogatásával működő Social Command Center szemléltette, amely egy világtérképen valós időben megjelenítette, hogy az idei kiállítás milyen párbeszédet generál az interneten.

Az E.On mobil, intelligens otthonná alakított teherautójában a látogatók az energiaszolgáltatás közeljövőjét formáló smart grid, elosztott áramtermelés és okos mérőórák működésébe pillanthattak bele, míg az Audi Hannoverben tartotta az A3-as németországi bemutatóját – a gépkocsi beépített tablettel érkezik. Mobileszközök népesítették be a CeBIT i-land nevet viselő 22-es pavilont, közöttük a HTC és a Samsung első LTE okostelefonjai, amelyek a 3G-s elődöknél 10-szer gyorsabb letöltést hoznak. A Webciety ezúttal a konzumerizáció, az online üzleti tevékenységet érintő törvényi szabályozás, valamint az adatvezérelt, kontextus alapú és könnyen kezelhető, valós idejű szolgáltatásokat adó „web operációs rendszer" témakörével foglalkozott.

Idén első ízben önálló szekcióként jelentek meg a kiállításon a logisztikai IT-megoldások, de a látogatókra alighanem a CeBIT Labs pavilonjában szereplő robotok tették a legnagyobb benyomást. Az angol Engineered Arts RoboThespian humanoidjában az ember már nem gépet lát, hanem ösztönösen úgy viszonyul hozzá, mint egy másik személyhez – ami a bizalom és a biztonság kérdését újabb dimenzióba emelheti a nem is olyan távoli jövőben.

> **Az adatok biztonsága és a felhasználók bizalma különösen fontos az e-government szolgáltatások** és a kormányzatoknak adott más informatikai megoldások vonatkozásában.

SZTRÁJKKAL TARKÍTVA

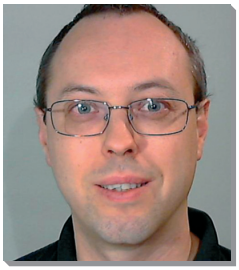
Az idei CeBIT-en március 6–10. között 70 ország színeiben több mint 4200 cég állított ki Hannoverben – ez megegyezik a tavalyi adatokkal. A látogatók számáról egy ideje már csak becsléseket közöl a Deutsche Messe. *Ernst Raue,* az igazgatótanács illetékes tagja szombaton, a záró napon ezúttal úgy fogalmazott, hogy az jóval meghaladja majd a 300 ezret, a külföldről érkező látogatóké pedig az 50 ezret. A tavalyi becslés is 350 ezer látogatóról szólt, vagyis a CeBIT elvileg megkapaszkodott a lejtőn, a 2011-et megelőző időszakra jellemző, éveken át tartó negatív trend idén sem tért vissza.

A látogatottság alakulását idén a villamosvezetők csütörtöki sztrájkja is befolyásolhatta. Március 8-án villamospótló buszok, a német vasút járatai, valamint a hannoveri lakosok saját gépkocsival szállították a CeBIT-re érkező vendégeket a vásárvárosba. A bizalom fogalma így ebben a megvilágításban is napirenden volt – bár a közlekedési káosz elmaradt, Raue szerint a sztrájk miatt sokan lemondtak a részvételről. Jövőre a CeBIT március 5–9. között várja látogatóit Hannoverbe.

ZENTYAL

Az admin barátja – 2.

Folytatjuk cikkünket, amelyben olyan Linuxot mutatunk be, amelynek megvannak az ismert pozitív tulajdonságai és frappáns választ ad a vele szemben felhozott kifogásokra.



CZAKÓ KRISZTIÁN

Előző számunkban *(Computerworld 2012/9–10.)* bemutattuk a Zentyalt. Most sorra vesszük a Zentyal adta funkciókat, mint a fájlszerver, a levelezés, a csoportmunka és más hálózati szolgáltatások.

Fájlszerver, tartományvezérlő

A Zentyal fájlszervere és tartományvezérlője a samba, amely jó ismerős mindenkinek, aki használt már Linuxot vagy Linux-alapú NAS-t. Kapunk hozzá valós idejű vírusellenőrzést (ClamAV-al) és szemetest (RecycleBin), hogy a törölt fájlok gyorsan visszanyerhetők legyenek. Ezek megosztásonként ki/be kapcsolhatók. A hozzáférések kezelését leegyszerűsítették: nincs külön „Fájlszerver" rész. Ha csoportnak akarunk megosztást készíteni, akkor a csoport jellemzőinél kell ezt megtennünk. Ha felhasználónak, akkor ott. Ha olyan megosztást szeretnénk, amelynél a jogokat külön be akarjuk állítani, arra van egy külön menü. Adhatunk hozzáférést felhasználóknak és csoportoknak is, ahogy a sambában ezt megszokhattuk.

Levelezés, csoportmunka

A levelek fogadását és elküldését a Postfix végzi, melyet a kezelőfelületen állíthatunk be az integrált spam- és vírusszűréssel együtt (Amavisng, SpamAssassin és ClamAV). A beérkezett levelek két helyre kerülhetnek. Ha „mezei" levelezőrendszert készítünk, akkor a leveleink Maildir formában a fájlrendszerben tárolódnak, ahonnan a Dovecot szolgál ki IMAP és POP3 protokollal. Használhatunk SSL-t és STARTTLS-t is, amihez a rendszer részeként elérhető tanúsítványkiadót tudjuk segítségül hívni. A webmail funkciót a RoundCube biztosítja, amely mögött egy Apache webszerver dolgozik. Mivel minden integrált és a kezelőfelületről állítható, sem a parancssor ismeretére, sem olyan extra tudásra nincs szükségünk, amely „hagyományos" Linux-környezetben elengedhetetlen lenne.

A Dovecot helyett használhatunk csoportmunka-szoftvert is, a Zarafát. Ez alatt is a Postfix/Amavis-ng/SpamAssassin/ClamAV csapat dolgozik, csak a Dovecot/RoundCube részt cseréljük le.

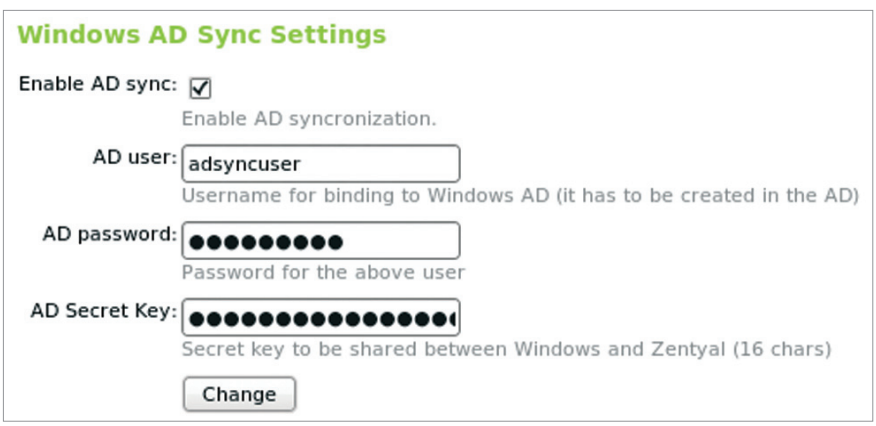
A Zarafa alkalmas az Exchange kiváltására: van benne levelezés, naptár, címjegyzék, teendők és jegyzetek. Ezeket a felhasználók meg is oszthatják egymással. Támogatja az ActiveSyncet, így szinkronizálhatjuk adatainkat okostelefonunkkal is (push funkcióval). A Zarafa migrációs segédprogramjával az Exchange kiszolgálóról vagy tömeges Outlook PST fájlokból pedig egyszerűen átemelhetjük az adatokat. A Zarafa webes felülete rendkívül emlékeztet az Outlook Web Access (OWA) felületére, ami segíti a váltást. A Zarafa is nyújt IMAP és POP3 szolgáltatást, így az azt ismerő levelezőprogramjainkat nem kell lecserélni. A naptárhoz szabványos iCal és CalDAV felületen hozzáférünk kívülről is.

Ha a Zarafával az Exchange-t akarjuk kiváltani, meg kell emlékeznünk egy kereskedelmi komponensről, az Outlook MAPI-támogatásról. Ehhez két zárt forrású szoftver kell. Az egyik ingyenes és a Windows munkaállomásra telepítendő, hogy az Outlook kapcsolódni tudjon a Zarafához. A másikat a Zarafa kiszolgálóra kell feltenni – a Zentyal telepíti automatikusan –, amely három párhuzamos Outlook-klienst tud ingyenesen kiszolgálni MAPI-val. Ha több felhasználóval szeretnénk Outlookot használni, legalább a Zarafa Small Business változatát kell megvennünk. A licenc folyamatosan a legfrissebb Zarafa-verzió használatát teszi lehetővé, és kapunk extraként egy külön mentőszoftvert, amellyel a visszaállításokat gyorsan és felhasználónként, azon belül mappánként végezhetjük el.

A Zarafa – főleg sok párhuzamosan dolgozó felhasználóval – jelentősen növeli a Zentyal hardverigényét, ami a kezelőfelület miatt eleve nagyobb, mint az ugyanarra képes csupasz Linuxé. Egy Zentyal szerverhez Zarafa nélkül 2 GB memória ideális a gyors működéshez, Zarafával ez inkább 4 GB. Ennek a fő oka, hogy a Zarafa MySQL adatbázisból dolgozik, amelynek optimalizálva is sokkal nagyobb a memóriaigénye, mint az ext4 fájlrendszernek, de még így is messze elmarad egy Microsoft Windows Server és az Exchange igényeitől.

Távoli elérés, VPN

Az aktuális Zentyal-verzió három VPN-technológiát kínál a hálózatunk elérésére, illetve két Zentyal szerver (és a mögöttük lévő hálózatok) összekapcsolására. Az OpenVPN régi ismerős. Ennek használatához szükségünk van egy saját hitelesítésszolgáltatóra (CA) a felhasználók és a szerver hitelesítéséhez. Ilyen CA-t létrehozni a Zentyalban pár kattintás: meg kell adni a szervezetünk nevét, az országkódot, a helységet, a megyét és a lejárati napok számát. A Zentyalban kész „VPN-csomagot" tölthetünk le a felhasználónak. Van csomag Windows, Linux, Mac-OS és két Zentyal szerver összekötésére, sőt Windows esetén az OpenVPN telepítőt is betehetjük a csomagba a beállítások és a tanúsítványok mellé.



A Zentyal képes Microsoft Active Directory rendszert szinkronizálni

Az IPSec támogatás a jelenlegi változatban még csak az osztott kulcsos hitelesítést támogatja, elsősorban két hálózat összekötésének céljából. Azok számára pedig, akik a PPTP-t kedvelik, jó hír, hogy ez is megtalálható a rendszerben.

Kommunikációs szolgáltatások

Itt két funkcióról érdemes szót ejteni. A szabványos XMPP üzenetküldő Jabber kiszolgáló is része a rendszernek, természetesen ez is integrálva, így a bejelentkezéshez a rendszerben felvett felhasználói neveket és jelszavakat lehet használni. Külön érdekesség, hogy a belső felügyeleti rendszer is – amely monitorozza a szolgáltatásokat és erőforrásokat – képes XMPP-vel jelezni, ha gondja van. Erre is használhatjuk a saját Jabber kiszolgálónkat (persze más XMPP szerverre, mint például a Google Talk rendszerre is küldhetünk üzenetet).

Emellett egy alap-telefonközpont funkciót is kapunk, amely az Asterisk PBX rendszerre épül. Itt csak a telefonáláshoz tényleg nélkülözhetetlen funkciók lettek a kezelőfelületen implementálva, (még) nem említhető egy lapon mondjuk a Trixboxszal. Ami benne van, az viszont korrektül illeszkedik a rendszerbe. Az alapbeállításoknál felvehetünk egy külső szolgáltatót (szabványos SIP), amelyen keresztül a kimenő hívásokat intézhetjük és ahonnan a bejövő hívásokat fogadjuk. Emellett minden felhasználónkhoz rendelhetünk egy melléket (ezt a felhasználó jellemzőinél). Támogatja még a konferenciabeszélgetést is: felvehetünk „konferenciatermeket", oda a megfelelő teremszám és kód ismeretében tudunk belépni („kívülről" is, ha van külső SIP-kapcsolatunk). VoIP (SIP) telefonkészülékek használatához beállíthatunk melléket, jelszót, a hangposta számát és egy értesítési e-mail címet, ahová levelet küldhet a rendszer, ha üzenetünk érkezett.

További hasznos holmik

Van még pár funkció, amelyre itt most csak az említés szintjén térek ki. Ilyen az FTP kiszolgáló (vsftpd, integrálva, ahogy kell), a „captive portal" (Wi-Fi hotspotok mögé), a Radius szerver (vállalati Wi-Fi hitelesítéshez), nyomtatómegosztás (CUPS), „felhasználói sarok" (a felhasználóink beléphetnek és saját adataikat módosíthatják; ha van levelezőszerverünk, akkor külső pop3 szerverről levélletöltést állíthatnak be) és virtualizáció (választhatunk a KVM- és a VirtualBox-alapú rendszerek között; a virtuális gépeket létrehozhatjuk és menedzselhetjük a Zentyal felületéről).

Mentés

A végére hagytam a minden rendszer kihagyhatatlan részét jelentő mentő funkciót. A Zentyal esetén két mentési részről beszélhetünk. Az egyik a beállítások és felhasználók mentése. Ez kevés adat, de ez kell a rendszer helyreállításához, ha azt újra kell telepíteni. Ezt exportálhatjuk egy fájlba magunknak, vagy az ingyenes felhő előfizetésünk segítségével tárolhatjuk központilag is. Utóbbiból a telepítéskor automatikusan helyreállíthatjuk a rendszerünket, vagy egy teljesen új kiszolgálót építhetünk egy alap beállításcsomagot felhasználva sokkal gyorsabban.

A fontosabb természetesen az adatok mentése. Itt a jól ismert duplicity mentő szoftvert kapjuk. Ezt állíthatjuk be a kezelőfelületen. Használhatjuk helyi mentésre egy könyvtárba, vagy a helyi hálózaton sftp, rsync vagy FTP szerverre (e célra egy olcsó NAS kiváló megoldás lehet egy kisvállalatnál). De menthetünk a felhőbe is (pl. Zentyal cloud). Utóbbi esetben a biztonságot a mentés titkosításával érhetjük el. A mentések időzíthetők, beállíthatjuk, milyen gyakran kérjük a rendszer teljes mentését és milyen gyakran a változásokét. A mentésekben kereshetünk, és pár kattintással visszaállíthatjuk a hiányzó adatainkat.

***

Ha önt érdekelik a Zentyal nyújtotta lehetőségek, regisztráljon a **zentyal.hu** partneroldalán!

HÉTKÖZNAPI ALAPFUNKCIÓK

Hálózati infrastruktúra kezelése A kezelőfelületről vehetjük fel a domaineket a DNS-kiszolgálóba és az IP-tartományokat a DHCP-be. Ha a DHCP esetén beállítjuk a DNS automatikus frissítését, akkor a DNS-oldal beállítása automatikusan megtörténik (direkt és fordított feloldáshoz is).

Hálózatvédelem Alaptelepítéssel is beállított tűzfalat kapunk, amely csak a szükséges funkciókhoz enged hozzáférést (a belső hálózatról is!). Ha két csatolónk van, és az egyiket külsőnek jelöljük, akkor a külsőn letiltja a bejövő forgalmat, a belső felől pedig beállítja a címfordítást. Ha felteszünk egy új szolgáltatást, annak használatához automatikusan kinyitja a megfelelő portokat a belső hálózat felől, és beteszi a szolgáltatások listájába a megfelelő portbeállításokat. A biztonságunkról ezenfelül a Snort IDS gondoskodik, amelyet csatolónként állíthatunk, ahogy azt is, mire figyeljen és mire ne.

QoS A Linux kernel QoS rendszerét kapjuk, emészthető formában, egyszerű beállíthatósággal, Layer7 protokollfelismeréssel. Csatolónkként, portra és protokollra szabályozhatjuk a sebességeket és a prioritást. A rendszer képes kezelni a többirányú internetkapcsolatot is. Pár kattintással beállíthatjuk a terhelés elosztását vagy hiba esetén a nem működő irány automatikus le- és felkapcsolását, valamint a kapcsolat-működőképesség ellenőrzésének módját.

Proxy A proxy-cache szerver a Squid, mely javítja a böngészési élményt, a Dansguardian segítségével pedig a forgalom szűrését is ellátja. A tartalom vírusszűrése mellett öt fokozatban állíthatjuk a szűrési szintet. Alkalmazhatunk egyedi szabályokat vagy előfizethetünk a szabálygyűjtemény-frissítésre is. Korlátozhatjuk a böngészési sávszélességet is.
Készíthetünk több szűrőprofilt, amelyeket aztán objektum- vagy csoportházirendhez kapcsolhatunk. Az objektumházirend a hálózati objektumok (IP-címek, tartományok) alapján állítja be a megfelelő profilt, míg a csoportházirend az egyes felhasználói csoportokhoz rendeli azt.

IDC PREDICTIONS 2012: COMPETING FOR 2020

Nyertesek és vesztesek a harmadik platform évtizedében

Az infokommunikációs iparág nagy horderejű átalakuláson megy keresztül, miután a növekedés alapját immár a mobil, a felhőalapú, a közösségi és a Big Data technológiákra épülő harmadik platform alkotja. Az International Data Corporation szerint az átállás 2012-ben olyan mértékben felgyorsul, hogy az év végére már az is körvonalazódik, mely szállítók alkotják majd az élbolyt 2020-ban, és melyek maradnak le végképp ebben a versenyben.

Három évtizedes hagyományához híven az IDC 2011 végén is előrejelzést kért több mint ezer elemzőjétől arra nézve, hogy az új év mit tartogat az ICT-iparág számára. Ezek összesítésével született meg az *IDC Predictions 2012: Competing for 2020* című tanulmány, melynek rövid, áttekintő kivonatát az IDC Hungary jóvoltából adjuk közre.

A piacelemző szerint idén világszinten 6,9 százalékkal fog nőni az IT-költés. A jelenlegi gazdasági helyzetben meglepően erősnek tűnő növekedés hajtóerejét azonban a fejlődő piacok, valamint a mobileszközök és alkalmazások forgalma fogja adni, míg a legnagyobb gátló tényezőt továbbra is az európai adósságválság képviseli. A fejlődő piacokon ugyanis az IT-költés várhatóan 13,8 százalékkal fog nőni, így ezek az országok adják majd a világ IT-piacának 53 százalékát. Az év második felében Kína elveszi Japántól a világ második legnagyobb IT-piacát megillető címet.

A mobilitás, a felhő és az adat éve

2012 a mobilitás éve lesz, miután a mobileszközök forgalma darabszám alapján eléri a PC-eladások kétszeresét, és első ízben nagyobb szállítói bevételeket generál, mint a személyi számítógépek értékesítése. A felhasználók 85 milliárd mobilalkalmazást fognak letölteni, és idén első alkalommal többet költenek majd mobil adathálózatok használatára, mint vezetékesinternet-elérésre.

A nyilvános és magánfelő szolgáltatásokra, valamint azok építésére a felhasználók 2012-ben 60 milliárd dollárt fognak költeni. Az Amazon IT-szállítói bevételei meghaladják az 1 milliárd dollárt, és a felhőben az infrastruktúra-szolgáltatások után az alkalmazásplatformok kerülnek a figyelem középpontjába. Ennek megfelelően a verseny is arról szól majd, hogy melyik szállító tudja a legnagyobb portfóliót és fejlesztői-partneri ökoszisztémát kiépíteni alkalmazásplatformja körül.

Világszinten a tárolt és kezelt adatmennyiség 2012-ben el fogja érni a 2,7 zetabájtot (1 ZB 1 milliárd terabájtnak felel meg), ami 48 százalékos növekedést jelent a múlt évhez képest, 2015-ben pedig már 8 ZB adatmennyiségről fogunk beszélni. A rendkívül nagy adatmennyiségek (Big Data) tárolásához, kezeléséhez és elemzéséhez fűződő kompetenciák ezért – a mobilitás és a felhőszolgáltatások terén kiépített szakértelemhez hasonlóan – nélkülözhetetlenné válnak a piaci szereplők számára, ezért az IDC arra számít, hogy idén számos Big Data indíttatású cégfelvásárlásnak és összevonásnak leszünk tanúi.

A legnagyobb piaci szereplők üzenetértékű akvizíciókat fognak végrehajtani a közösségi hálók és technológiák terén is. A Facebook megkísérli majd, hogy a lakossági piacon meglévő fölényét a vállalati szegmensben, a B2C kereskedelemben is kamatoztassa.

Idén már közel kétszer annyi intelligens eszköz fog az internetre csatlakozni, mint ahány számítógép és okostelefon. Ez kihat majd az emberek hálózati kommunikációs szokásainak további fejlődésére – a közösségi hálókat például már nem csupán egymással való kapcsolattartásra, hanem dolgok, intelligens eszközök követésére is használni fogják.

A harmadik platformon a szállítói bevételek nagyobb hányada nagy értéket képviselő, iparági megoldásokból származik majd. Az ilyen vertikális megoldások piaca 2012-ben lendületet fog venni az egészségügy, az energiaipar, a pénzügyi szolgáltatások és a kereskedelem területén, valamint a kormányzati szektorban – ami a szükséges iparági kompetenciákkal nem rendelkező IT-szállítókat a pálya szélére fogja állítani.

Infokommunikációs maraton

Lévén 2012-t írunk, a piaci erőviszonyok évtized végére várható állapotára vonatkozó előrejelzés kissé merésznek tűnhet. Az IDC szerint azonban a szállítóknak és a vállalati IT-vezetőknek már idei döntéseiket is annak tudatában kell meghozniuk, hogy hová kívánnak eljutni 2020-ra.

A piacelemző tavalyi előrejelzésében is figyelmeztetett a platformváltásra, amelyen az iparág jelenleg keresztülmegy – ilyen horderejű változásra 20-25 évente kerül sor. Az évtized végén, amikor a világ

KIS ENDRE

ICT-piacának mérete a mostani 3,3 trillió dollárról 5 trillióra nő, a szállítói bevételek legalább 80 százaléka az új, harmadik platformot alkotó – mobil, felhőalapú, közösségi és Big Data – technológiákból származik majd, mivel felhasználói oldalon is ezek, valamint a rájuk épülő megoldások fogják adni a legnagyobb értéket a vállalatoknak.

Napjainkban a harmadik platformot alkotó technológiák és a köréjük épített szolgáltatások együttes részesedése a szervezetek teljes IT-költéséből csupán 20 százalék, de ez évi mintegy 18 százalékkal nő, ami hatszorosan felülmúlja az IT-iparág egészének növekedési ütemét. Az IDC ezért arra számít, hogy a 2020-ra kialakuló, a maitól lényegesen eltérő ICT-piacon elfoglalt pozíciókért folyó küzdelem a szállítók között már idén eldőlhet – a maratonfutáshoz hasonlóan, amelyben azok a versenyzők, akik nem kerülnek az élbolyba a futam első negyedében, gyakorlatilag esélytelenek a dobogós helyezésre.

Mobil, felhőalapú, közösségi és Big Data-technológiákról, fejlődő piacokról azonban az elmúlt évben is sok szó esett, így joggal merül fel a kérdés, hogy mi az újdonság mindebben. Az ICT-iparágat átformáló változást az IDC már 2007-ben azonosította. Az idei év egyszerűen a legújabb szakasza annak a többéves folyamatnak, melynek során az iparág alapvetően új technológiák és üzleti modellek alkalmazására tér át. Ebből azonban még nem következik, hogy 2012 ugyanolyan év lesz, mint a tavalyi. A harmadik platform vonatkozásában az elmúlt évben minden eddiginél több szereplő szállt versenybe, és az érintett technológiák felhasználói oldalon is főáramba kerültek. A piac mindkét oldalon sokat fejlődött 2011-ben, ezért az idei év több tekintetben is merőben más lesz.

Szállítók választ előtt

Az IDC előrejelzése szerint 2012-ben a mobileszközök és alkalmazások végérvényesen a digitális világ első számú portáljává válnak, maguk mögé utasítva a PC-ket, amit a szállítók termékstratégiájának változása is tükrözni fog. A felhőplatformok arénájában idén válhat igazán élessé a verseny. Tavaly a salesforce.com és a Microsoft kivételével a szállítók még nem kínáltak kiforrott felhőplatformokat, de 2012-ben több új, felhőalapú alkalmazásplatform is megjelenik a piacon, fejlesztők és megoldásszállítók ökoszisztémáját gyűjtve maga köré. Ezek a platformok már 2011 folyamán az új vállalati megoldások első számú disztribúciós csatornájává és implementációs környezetévé váltak, és idén ugyanez válik érvényessé a hagyományos alkalmazásokra nézve is. A szoftverértékesítés eddigi modellje rövidesen túlhaladottá válik, ezért azok a szállítók, amelyek erre építették üzleti modelljüket, tevékenységük alapos átalakítására kényszerülnek.

Három szállítói kompetencia – a közösségi hálókhoz, a Big Data-technológiákhoz és a vertikális megoldásokhoz fűződő szakértelem –, amellyel a piaci szerelők némelyike eddig csupán kacérkodott, az idei évtől nélkülözhetetlenné válik a versenyben maradás szempontjából.

A harmadik platformra történő áttérés következtében az iparág legnagyobb szállítói 2012-ben választ elé kerülnek. A HP új vezérigazgatójának például el kell majd döntenie, hogy mit kezdjen azokkal a tételekkel, amelyeket elődje a Big Data játszmában helyezett el, és határoznia kell a mobileszközöket érintő stratégiáról is. A Microsoft hasonlóan nagy és sorsdöntő választások elé néz mobil- és felhőplatformját illetően, amelyeket meg kell szabadítania a második platform technológiai örökségétől. Az SAP tavaly határozottan elkötelezte magát a mobil-, a felhőalapú és a Big Data-technológiák mellett, de a fejlesztések lendületét 2012-ben is tartania kell. Nem lesz könnyebb dolga az Apple új vezérigazgatójának sem, mivel az Android nyílt modellje következetesen egyre nagyobb kihívást jelent a cég számára az okostelefonok, az alkalmazások és a tabletek piacán.

Az új versenyzőkre többé nem lehet úgy tekinteni, mint a régi rendet megbontó jövevényekre, mostantól ugyanis ők szabják meg a rendet. ICT-szállítóként idén az Amazon és a Google bevétele is meg fogja közelíteni vagy meghaladja az 1 milliárd dollárt, méghozzá könnyedén. Ezek és a hozzájuk hasonló szállítók, mint például a Facebook, eséllyel pályáznak arra, hogy 2020-ban az ICT-iparágat vezessék. A jelenlegi legnagyobbaknak is szembe kell nézniük ezzel, és felkészülniük a megmérettetésre a harmadik platformon.

2012-ben több új, felhőalapú alkalmazásplatform is megjelenik a piacon, fejlesztők és megoldásszállítók ökoszisztémáját gyűjtve maga köré.

Ezért annak ellenére, hogy a tavalyi évhez hasonlóan 2012 is a mobil-, a felhőalapú, a közösségi és a Big Data-technológiákról fog szólni, az események, a döntések és a tétek merőben mások lesznek, mint az eddigiek. A harmadik platformot érintő stratégiák megalkotása és gyakorlatba ültetése szállítói és felhasználói oldalon is első számú prioritást kap, a helyes döntések meghozatala, a jó irányba tett lépések kényszere sürgetővé válik.

Az IDC 2012-es előrejelzése – az év eleje óta közzétett, az ICT-piac szegmenseivel külön, behatóbban is foglalkozó elemzésekkel együtt – a www.idc.com/research/Predictions12/Main/index.jsp címen érhető el.

Színház

Kiállítás

Étterem

Kocsma

Party

Koncert

Sport

Szórakozol velünk?

www.funzine.hu

Már magyarul is!

Megmutatjuk, hol, mikor és miért jó Budapesten.

FUNZINE