SZÁMÍTÁSTECHNIKA
COMPUTERWORLD
ICT-STRATÉGIA DÖNTÉSHOZÓKNAK / ALAPÍTVA 1969 / 2011. NOVEMBER 30. / XLII. ÉVFOLYAM 48. SZÁM

/ ADVANCED PERSISTENT THREAT – APT

Kegyelmet nem ismerő támadások

Építs többszintű, mélyreható védelmi infrastruktúrát! **Figyelj az emberi tényezőre!**

Összeállításunk a 9–11. oldalon

AZ ADATSZMOG ELLENSZERE

Egyesek szerint a Palantir elemzőszoftvere lesz a következő milliárd dolláros durranás.

» 14. oldal

FELHŐREPERTOÁR

Folyamatosan bővül a hazai felhőszolgáltatások kínálata – és egyre nagyobb a kereslet is.

» 18. oldal

9 770587 151006 11048
Ára: 495 Ft
IDG Communications HUNGARY
www.computerworld.hu

VTCD VIDEOTON
Kompaktlemez-gyártó Kft.

DVD Authoring
CD, DVD sokszorosítás
Egyedi CD, DVD írás
Csomagolás és logisztika

H-8000 Székesfehérvár
Aszalvölgyi u. 7.
Tel.: +36-22/533-571
Fax.: +36-22/533-599
E-mail: vtcd@vtcd.hu www.vtcd.hu

BUSINESS TRAVELLER HUNGARY
Az üzleti utazás hazai iránytűje
A magazin, amely bepillantást enged a céges utaztatás kulisszatitkaiba és hasznos tanácsokkal, praktikus ötletekkel segíti az utazó üzletembereket.

40% KEDVEZMÉNY + AJÁNDÉK CORPORATE CLUB KÁRTYA*

COMPUTERWORLD – A világ IT-szemmel
A lap, amely megmutatja, hogyan lesz az információtechnológiából üzlet!
Cégvezetőknek, pénzügyi vezetőknek, informatikai vezetőknek

1 ÉVES COMPUTERWORLD-ELŐFIZETÉS
1 ÉVES BUSINESS TRAVELLER HUNGARY ELŐFIZETÉSSEL
Fizessen elő vagy hosszabbítsa meg előfizetését!

26 940 Ft helyett **most csak 16 200 Ft**

Hívja a **06-1/577-4301**-es telefonszámot vagy kattintson a **piacter.idg.hu** oldalra!

*A kártya névre szól, egy évig érvényes. Egyedülálló kedvezményekre jogosít hazai és külföldi turisztikai szolgáltatóknál. A kedvezmények magán- és üzleti utakhoz is felhasználhatók.

Az akció az IDG Hungary Kft.-nél 2011. december 15-ig megrendelt és befizetett előfizetésekre vonatkozik. Az előfizetés időtartama alatt az előfizetés nem mondható fel. További információért hívja a **06-1/577-4301,** nem emelt díjas telefonszámot vagy írjon a **terjesztes@idg.hu** e-mail címre. Megrendelése egyben önkéntes adatközlés is. Az adatközlő hozzájárul, hogy megadott adatait a kiadó előfizetői adatbázisában nyilvántartsa és az előfizetői akcióban szereplő másik kiadvány kiadójának átadja. A megrendelő megrendelésével továbbá hozzájárul, hogy a kiadó tájékoztató- és reklámanyagot küldjön marketingcélból. A hozzájárulás visszavonásig él, a kiadó címére (IDG Hungary Kft. 1075 Budapest, Madách I. út 13-14. A.ép. IV.em.) írt levélben bármikor visszavonható. Minden jog fenntartva!

TARTALOM / 2011. NOVEMBER 30. / 48. SZÁM

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: Szalay Dániel
Online igazgató: Odrovics Szonja
Olvasószerkesztő, korrektor: Sz. Erdős Judit
Munkatársak: Dávid Imre, Egri Imre, Kis Endre, Mallász Judit, Odrovics Szonja, Szilágyi Szabolcs, 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
Hirdetési igazgató:
Melovics Csaba – csmelovics@idg.hu
Telefon: 577-4310, fax: 266-4274
Lapreferens:
Rodriguez Nelsonné – irodriguez@idg.hu
Telefon: 577-4311
Kereskedelmi asszisztens:
Bohn Andrea – abohn@idg.hu
Telefon: 577-4316, fax: 266-4274
» e-mail: keriroda@idg.hu

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

Ipsos | Gemius | eset | print-audit | adverticum

AKTUÁLIS

FÓKUSZ

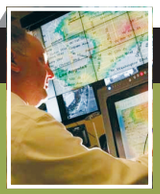
HÁLÓBAN

KKV-CORNER

MELLÉKLET

ÁLLANDÓ ROVATAINK

COMPUTERWORLD /ONLINE



ANALITIKÁVAL A BŰNÖZÉS ELLEN
Az elemzőrendszerek előre megjósolhatják egyes bűnözési fajták elkövetését. Az amerikai rendőrség lecsapott a lehetőségre.
» computerworld.hu/cikk/bunozes-ellen-analitika

A PENTAGON KATONAI ERŐVEL SÚJTHAT LE
Hackereket eddig még sohasem fenyegettek fizikai megsemmisítéssel, ám a Pentagon katonai csapást is megengedhető lépésnek tart a kiberterroristák ellen.
» computerworld.hu/cikk/kibertamadok-pentagon

EGYRE ÜTŐSEBBEK A DOS-TÁMADÁSOK
Az egyik ázsiai vállalatot egy nagyszabású, elosztott szolgáltatásmegtagadási támadás érte. Ez az eset is alátámasztja a DDoS-akciók kapcsán megfigyelhető trendeket. Mire számíthatunk?
» computerworld.hu/cikk/utos-dos-tamadasok

MIT SEM ÉR AZ INNOVÁCIÓ?
A nehézsúlyú tőzsdei befektetők szemében a világ legértékesebb techcége, az Apple csak annyit ér, amennyit aktuális slágertermékei hoznak. Sokkoló vélemények.
» computerworld.hu/cikk/innovacio-garas

SÍK ZOLTÁN NÁNDOR

biztonságpolitikai szakértő

Mégis, kinek az adata?

Informatikai biztonság, információbiztonság, kiberbiztonság – sokan keverik ezeket. Nem csoda, hiszen olyan gyorsan változik a világ, hogy mire egy-egy fogalomnak a megértése, definiálása, köztudatba való bevezetése megvalósul, addigra már egy másik fogalom veszi át a helyét.

> Mit is jelentenek adataink nekünk, egyes embereknek, mit jelentenek az üzleti élet, a tudomány világa és mit az állam számára? Az információs társadalmak korában erre azt kell válaszolnunk: mindent.

Vegyük sorra! Az informatikai biztonság (IT-biztonság) az informatikai rendszerekre vonatkozó követelmény: itt a rendszerek biztonsága a meghatározó elem. Az információbiztonság fókuszában az információ van, az informatika a technikai „kellék". Igaz azonban, hogy az információbiztonsághoz nemcsak az elektronikus, hanem például a papíralapú információk biztonságát is hozzá kell venni (dokumentumbiztonság), sőt időnként nemcsak információbiztonságról, hanem adatbiztonságról is beszélnek (holott az értelmezett adatokat hívjuk információknak), mi több, az információbiztonságnak köze van a biztonság több más ágához is (például a fizikai és a személyi biztonsághoz).

Az információbiztonság azon ágát, amely az elektronikus „cyber" (kiber) térben értelmezett adatok biztonságával foglalkozik, jobb híján kiberbiztonságnak hívjuk. Bár még abban sincs egyetértés, hogy mi is az a kibertér: csak az internetes világ, vagy bármilyen infokommunikációs infrastruktúrán értelmezett elektronikus adat?

A fiatalabbaknak a kiberbiztonság kb. a fentieket jelenti, az idősebbeknek azonban a kibernetika, az információfeldolgozás tudománya is eszükbe jut róla. Jó példa erre *Moldova György: Ferencvárosi koktél* című könyvében megjelent novellája, a *Verebes, a túl művelt bokszoló* azon része, amikor a címszereplő arról panaszkodik, hogy a kezébe került kibernetikai mű címének is csak a felét értette meg: „A »kiber« az rendőr, de mi az, hogy »netika«?"

A keveredő és még nem magyarosított, sőt nem is igazán értelmezett fogalmak erdejében tehát eléggé nehéz eligazodni, hát még fontosságukat, az ezzel kapcsolatos szerepköröket azonosítani, a feladatokat definiálni és végrehajtani. Holott a kérdés nem is olyan bonyolult, csak el kell gondolkoznunk azon, hogy mit is jelentenek adataink, információink, nekünk, egyes embereknek, mit jelentenek az üzleti élet, a tudomány világa és mit az állam számára. Az információs társadalmak korában erre azt kell mondanunk: mindent. Az adatok és információk, sőt leginkább ezek elektronikus formája (az egyszerűség kedvéért a továbbiakban csak adatok) nélkül ugyanis ma már semmi sem működik, összeomlana a társadalom, annak minden ága: a politikai, alkotmányos rendszer, a gazdaság, a kultúra, a környezet és maga a védelem.

Az adatok lassan kivívják azt a helyet, mint életünk többi pillére: család, munka, egészség. Ennek pedig egyik fő – hanem a legfőbb – oka, hogy a társadalom számára a rólunk nyilvántartott adatok alapján létezünk, életünk minden egyes mozzanatát elektronikus adatok áramlása jelzi. Ezek nélkül a digitális kor Robinson Crusoe-jává válnánk, igaz, kicsit rosszabb életben maradási eséllyel, mint Defoe hőse a lakatlan szigeten.

Ugyanígy ki vannak szolgáltatva az adatoknak az üzleti élet, a tudomány szereplői, de maga az állam is. Adatok nélkül összeomlana az államhatalmi rendszer, a közigazgatás, és a kialakuló anarchia maga alá temetné a társadalmat. Így az államnak kiemelt felelőssége van az adatok biztonságát illetően akkor is, ha ezek jó részét nem az állami, hanem az üzleti vagy a civil szféra kezeli. Az adatok egy kiemelt halmaza méltán nevezhető a nemzet elektronikus adat- és információvagyonának, röviden Nemzeti Adatvagyonnak.

Ez az adatvagyon azonban nem önmagában létezik, hanem valahol létrejön, tárolják, feldolgozzák, átviszik, megjelenítik, felhasználják stb. Az, ahol mindez megvalósul, az információs infrastruktúrák egy speciális formája: a kritikus információs infrastruktúrák birodalma. Ezért ennek védelme kiemelt feladat, amiért elsősorban az állam tartozik felelősséggel, holott ennek nagy része nincs is állami kézben.

S ha már a kiberteret emlegettük, még egy fogalom ide kívánkozik, aminek igen sok köze van a kritikus információs infrastruktúrákhoz mint célpontokhoz: ez a kiberterrorizmus. Igaz, mondhatjuk, hogy nemcsak terroristák támadják a kritikus (információs) infrastruktúrát, hanem hackerek, bűnözők, kémek, sőt államok is (ez utóbbira példa a közelmúltból a Stuxnet vírus). Sőt, a kibertámadáson kívül létezik és bevethető az információs hadviselés fegyverarzenáljának összes eleme, a vezetési hadviselési eszközöktől a pszichológiai hadviselésig. Így az sem véletlen, hogy az USA egy esetleges atomtámadás mellett egy információs hadviselési támadástól tart a legjobban.

Mindezekből látszik, hogy átalakuló világunk az információs társadalom előnyei mellett kénytelen szembesülni annak veszélyeivel is. Újfajta sebezhetőségek, veszélyek, lehetséges következmények – egyszersmind újfajta kockázatok jelentek meg. Ezeket a kockázatokat pedig minimalizálnunk, folyamatosan kezelnünk kell mindannyiunknak, nem csak az államnak.

Hyde Tech Corner

Ezen a héten *Miyazaki Jun* keresőmarketing-szakértő és *Jóri András* adatvédelmi biztos kommentálja a hét híreit, eseményeit.
/ összeállította: Tóth Lívia

Heti összeállításunkból megtudhatják, győzedelmeskedhet-e egy olasz matematikus keresője a Google felett, valamint az is kiderül, hogy vajon mennyire kényes kérdés a munkavállaló levelezése.

MEGSZORONGATJÁK A GOOGLE-T?

Egy olasz matematikus – aki a Google keresőalgoritmusának fejlesztésében is részt vett – azt tervezi, hogy még idén bemutatja saját projektjét, amely versenyképes lehet a legnagyobb keresőkkel szemben is. A várhatóan Volunia nevet viselő keresőmotor mögött egy teljesen újfajta szemlélet húzódik – állítja Massimo Marchiori, aki nem adná a nevét a projekthez, ha nem hinne abban, hogy egy nagy jelentőségű dolog készül.

» computerworld.hu/cikk/olasz-matematikus-vs-google

LEVÉLTITOK

Csakúgy, ahogy a munkaadó sok esetben elvből szabályozza alkalmazottjai munkahelyi internethasználatát, ajánlatos ugyanezt tenni az e-mail forgalom kapcsán is, hiszen a munkavállalók „privát kommunikációs ügyeinek" munkaidőben való intézése számos nem kívánt hatást eredményezhet. Egyértelmű belső szabályozást kell kialakítani, amelyben minden érintett munkavállaló megismerheti az e-mail fiók megengedett és tiltott használatának eseteit.

» computerworld.hu/cikk/ceges-munkavallaloi-fiok

MIYAZAKI JUN

KERESŐMARKETING-SZAKÉRTŐ

Korai lenne találgatásokba bocsátkozni a Voluniával kapcsolatban, hiszen gyakorlatilag semmit nem tudunk azonkívül, hogy „forradalmian új" lesz. Az ilyen „Google-killer" jelzők azonban általában inkább bombasztikusak, mintsem megalapozottak.

Ha megnézzük, a legkomolyabban vehető próbálkozás az elmúlt években a Bing volt, amibe a Microsoft beleadott apait-anyait és egy nagy talicska pénzt sem sajnáltak tőle. E háttér ellenére sem tudott mit kezdeni a Google-lal, inkább az egyéb, kisebb amerikai keresők piacát kannibalizálta.

Az efféle alternatív próbálkozások inkább az innováció szempontjából fontosak. A közeljövőben nem várható, hogy akár egy anyagiakkal jól ellátott multi vagy pedig egy kicsi, kezdő, de zseniális garázscég (mint ahogyan a Google is indult) meg tudja rengetni a piacot. Egy teljesen friss fejlesztés legnagyobb reménye az lehet, hogy szemléletben, technológiában tényleg valami gyökeresen újat és egyedit alkot, ami van annyira értékes, hogy valamelyik multicég megvegye azt, és beépítse a saját keresőjébe.

Teljesen más világ van, mint amikor a Google elindult: korának elfeledett konkurensei ugyanis nem voltak jó keresőalkalmazások, sokan használták őket ugyan, de senki sem volt megelégedve velük. Emlékszünk még azokra a szoftverekre, amelyek egyszerre kerestek több különböző keresőben, és a begyűjtött találatokat rangsorolták valamilyen saját algoritmus szerint? Azért volt igény ezekre, mert a legtöbb ilyen kereső borzasztóan rossz találatokat adott.

A Google azért tudott sikeressé válni, mert a felhasználók elégedetlenek voltak a konkurensekkel szemben, és a fejlesztők erre az elégedetlenségre adtak nagyon jó választ. A mai felhasználók túlnyomó többsége azonban teljesen elégedett a Google-lal: nincs bennük igény egy jobb keresőre, hiszen a Google 100%-ig kiszolgálja őket. Új keresőt fejleszteni pont ugyanolyan hálátlan feladat, mint vadiúj kólát kitalálni – a Coca-Cola mellett nincs szükség újabbra. A Google ugyanígy az egyik legnagyobb globális márkává lépett elő – az ő megszorongatása alapvetően nem fejlesztési kérdés, nem egy jobb algoritmuson múlik a siker.

DR. JÓRI ANDRÁS

ADATVÉDELMI BIZTOS

A munkavállalók e-mail postafiókjának ellenőrzése az adatvédelmi biztos munkajogi vizsgálatainak egyik gyakori tárgya. Az állásfoglalásokban többek között arra hívom fel a munkáltatók figyelmét, hogy önmagában nem teremt jogalapot az ellenőrzéshez, ha az e-mail postafiókot a munkáltató adja át a munkavállalónak. Például az e-mail postafiókba érkező levelek címzettjei nem feltétlenül vannak tudatában annak, hogy a levelük tartalmát a címzetten kívül más, harmadik személy is megismerheti. Ezzel az érintett személy levéltitok-védelméhez való jogát, illetőleg a személyes adatok védelméhez való jogát sértenék meg.

Az e-mail postafiók ellenőrzésével kapcsolatosan a biztos gyakorlatában kialakult jogszerű megoldás az lehet, ha a munkáltató tájékoztatja a munkavállalóit arról, hogy az e-mail postafiókot kizárólag hivatali célból használhatja, és mindenképpen szerencsés, ha az ellenőrzéssel kapcsolatos szabályokat utasítás formájában közzéteszi.

Lényeges, hogy a vezető a levél tartalmát közvetlenül soha nem ellenőrizheti, hanem a levelek fejlécének áttekintését követően a munkavállalótól kérheti meg a kiválasztott leveleket. A munkavállaló ilyen esetben csak akkor tagadhatja meg a levél átadását, ha azzal a saját vagy a küldő, illetőleg a fogadó levéltitokhoz vagy a személyes adatok védelméhez való jogát sértené meg.
Szintén jogszerű megoldás lehet, ha a munkáltató informatikai megoldások révén korlátozza az e-mail levélhez csatolható fájlok fajtáját, terjedelmét, így akadályozva meg, hogy a munkavállaló jogosulatlan adatokat fogadjon, vagy a munkáltató üzleti érdekét sértő adatokat továbbítson harmadik személy részére.

HÍR MOZAIK

MEGJELENT AZ OPENSUSE 12.1 / Az új disztribúció olyan platformfejlesztéseket és könnyen használható eszközöket tartalmaz, amelyek lehetővé teszik a felhasználók számára a legújabb ingyenes és nyílt forrású technológiák használatát fizikai, virtuális és felhőkörnyezetben egyaránt.

LIBREOFFICE-GYAKORLAT A NOVELLNÉL / Gyakorlati helyeket biztosít végzős informatikus-hallgatók számára a Novell Magyarország – HuEdu programjának keretein belül. Az ELTE Informatikai Karáról érkező diákok például a LibreOffice irodai programcsomag fejlesztéséhez járulhatnak hozzá a hathetes időszak során. A szakmai gyakorlat alatt a hallgatók olyan programozási feladatokat oldanak meg, amelyek elvégzése néhány hét alatt reálisan kivitelezhető, ilyen például a kódtisztítás, a refactoring vagy a hibajavítás. A nyáron elindult programban elsőként négy hallgató vett részt.

SIKERES FELÜLVIZSGÁLAT A MAGICOMNÁL / Idén is integrált felülvizsgálat keretében vizsgálták át az SGS Hungária auditorai a MagiCom által üzemeltetett ISO9001 alapú minőségirányítási, ISO27001 alapú információvédelmi, illetve az ISO14001-es környezetirányítási rendszereket. Az előző évekhez hasonlóan a MagiCom egyik rendszerében sem találtak az auditorok a szabványoktól való eltéréseket. A MagiCom elsőnek szerezte meg az ISO27001 alapú információvédelmi tanúsítványt, amit azóta is folyamatosan fenntart.

ESEMÉNYEK

NOVEMBER 30–DECEMBER 1. BUDAPEST
Telecom Loyalty and Retention
» allanlloyds.com

DECEMBER 1. VOIP
Hangrögzítési megoldások az analóg telefontól a mobilig
» gloster.webex.com

DECEMBER 7. VOIP
A vSphere platformhoz kapcsolódó legfontosabb VMware megoldások
» gloster.webex.com

DECEMBER 15. BUDAPEST
IT-menedzsmentről egymás közt
» balabit.com/hu/techreggeli

TOVÁBBI ESEMÉNYEK
» www.computerworld.hu/esemenyek

HACKERTÁMADÁS A MARRIOTT-LÁNC ELLEN

Magyar hacker a pácban

TÓTH LÍVIA / Az Amerikai Igazságügyi Minisztérium hivatalos közleménye szerint bűnösnek vallotta magát az a magyar férfi, aki a felhozott vádak szerint feltörte a Marriott International számítógépes rendszerét és megszerezte a szállodaláncot, hogy közzéteszi a társaság bizalmas adatait, amennyiben nem hajlandók őt alkalmazni.

A baltimore-i 26 éves magyar állampolgárságú hacker, N. Attila a marylandi kerületi bíróság előtt egy vádalku részeként vallotta bűnösnek magát. A vádlott 2010. november 11-én e-mailben arról értesítette a Marriottot, hogy hónapokkal korábban behatolt a számítógépes rendszerébe. A magának állást követelő férfi a titkos adatokhoz való hozzáférést egy Marriott-alkalmazottnak címzett e-mail csatolmányban juttatta be a rendszerbe. A csatolmány segítségével gyakorlatilag egy hátsó ajtón keresztül tudott hozzáférni a cég adataihoz.

A hacker megzsarolta a hotelláncot, hogy ha nem kap állást, belső információkat fog kiszivárogtatni. Mivel levelére semmilyen választ nem kapott, N. Attila két nappal később egy 8 csatolmányt tartalmazó e-mailben küldte el a szavainak hitelességét igazoló bizonyítékot: a levél a Mariott-tal kapcsolatos pénzügyi dokumentációkat és egyéb, bizalmas információkat tartalmazott.

A Marriott együttműködést színlelt, de közben jelentette az esetet az amerikai elnököket is védő Secret Service-nek. A szervezet egy fiktív Marriott-személyzetis nevében levelezni kezdett a zsarolóval. N. Attilát egy állásinterjú reményében Washingtonba csalták, ahol a repülőtérre való megérkezése után letartóztatták. Repülőjegyét a Marriott fizette...

Büntetéséről 2012. február harmadikán döntenek. A férfira rosszindulatú kód terjesztéséért 10 évig, a bizalmas információk nyilvánosságra hozásával való fenyegetőzésért pedig 5 évig terjedő szabadságvesztést szabhatnak ki.

20 ÉVES A MULTISOFT

Mobilitás a vállalatirányításban

Jubileumi ügyfélnapot tartott a fennállásának 20. évfordulóját ünneplő MultiSoft Kft., ahol bemutatta legújabb termékét, a Microsoft vállalatirányítási rendszerét okostelefonokon is elérhetővé tevő MobileNAV kliensalkalmazást.

A MultiSoft 1991-ben hétfős vállalkozásként indult, és kezdetben a Siemens-csoport megbízásából német, illetve osztrák projekteken dolgozott. Szakembereit ezt követően is bérbe adta nyugat-európai projektekhez, többek között így került kapcsolatba a Philipsszel és a dán Navisionnel. A Philips egyik üzletága, a Dictation Systems 2006-ban teljes szoftverfejlesztését kihelyezte a MultiSofthoz. Azóta, hogy a Microsoft felvásárolta a Navisiont, melynek vállalatirányítási rendszere Dynamics NAV-ként él tovább, a MultiSoft a szoftverország egyik legsikeresebb, többszörösen díjazott partnerévé vált Magyarországon és nemzetközi összehasonlításban egyaránt.

Kelemen Gábor ügyvezető igazgató nyitó előadásában arra is kitért, hogy a nehéz gazdasági körülmények ellenére a cég árbevétele az elmúlt két évben sem csökkent, tavaly is több mint 200 projekten dolgozott, és többek között olyan új ügyfeleket szerzett, mint a Hídépítő Zrt., a Pannónia Ethanol, a KA-VOSZ, a Sodexo és a Renault Trucks, miközben a cég szakemberei harmincnál több új szakmai minősítést is szereztek. A jövő évi tervekről szólva az igazgató kiemelte, hogy a MultiSoft az ügyfelek még hatékonyabb támogatására fog törekedni. Ennek érdekében frissíti és funkcionálisan is bővíti az online ügyfélszolgálat felületét, és 2012-ben is tartani fog ingyenes oktatásokat a felhasználóknak. Az igények feltérképezésétől a megvalósításon át a támogatásig a cég olyan élményt kíván szerezni ügyfeleinek, amelyből egyértelműen kitűnik, hogy nem szoftvertermékeket értékesít, hanem megoldásokat szállít. Kelemen Gábor kiemelte, hogy a MultiSoft stratégiai szerepet szán a mobilplatformokra való alkalmazásfejlesztésnek.

A vállalat legújabb fejlesztését, a MobileNAV alkalmazást *Ádám Zoltán,* a MultiSoft értékesítője és *Major Tibor* projektvezető mutatta be. A jelenleg Android platformon futó alkalmazással az ajánlatadástól a riportkészítésig a Microsoft Dynamics NAV vállalatirányítási rendszerének számos funkciója okostelefonról is használható. A MobileNAV ráadásul olyan extra lehetőségeket is kínál, mint például az ügyfélkartonon szereplő telefonszám hívása egy kattintással, vagy a cím megjelenítése térképen, illetve a beépített kamerát tartalmazó okostelefon egyúttal vonalkód-olvasóként is használható. A MultiSoft már dolgozik az iOS platformon futó változaton, és az alkalmazás a jövő év első felében Windows Phone-alapú okostelefonokon is elérhető lesz.

A 20 éves MultiSoft ügyfélnappal ünnepelt

A rendezvényen előadott *Ludwig Neer,* az iparági CRM-megoldásairól ismert CAS Software AG magyar származású alapítója is. A MultiSoft partnere a dizájn szoftverfejlesztésben betöltött szerepét hangsúlyozta. A résztvevők emellett előadásokat hallhattak a Microsoft Dynamics-termékek legújabb verzióiról és megismerhették annak a projektnek a tapasztalatait is, amelynek eredményeként a Fujifilm Magyarország tavaly 3 hónap alatt átállt a Dynamics NAV használatára.

INVITEL INNOMAX-DÍJ 2011

Innováció újratöltve

Idén is sokat nyerhetnek a kkv-k az Invitel pályázatán. Az InnoMax-díj hagyományteremtő jelleggel jött létre. Az Invitel célja, hogy a hazai kkv-szektor szakértő, tele- és infokommunikációs partnereként felhívja a figyelmet a körülöttünk működő – nehéz piaci szituációkban is helytálló – valóban kreatív, innovatív cégekre. Másképpen fogalmazva, teret és lehetőséget kíván adni a fejlődni képes vállalatoknak, hogy megmutassák magukat a szélesebb közvéleménynek és persze, hogy nyerjenek.

ZSEMBERY GYÖRGY

vezérigazgató-helyettes, Invitel

Innováció, hatékonyság, maximalizmus, kreativitás – ezek a kulcsszavai az InnoMax-pályázatnak, amelyet az Invitel a tavalyi és a tavalyelőtti évben elért sikerek biztató eredményeit követően idén már harmadik alkalommal hirdet meg. Az InnoMax-díjra kis- és középvállalatok nevezhetnek megvalósult ötletekkel, a hatékonyságot javító innovációkkal, üzleti fejlesztésekkel. De nemcsak szolgáltatás- vagy termékfejlesztéssel lehet pályázni! A lényeg: az üzleti innováció. Így például termelési, logisztikai, illetve akár HR-területről is érdemes nevezni.

„Az InnoMax-díjjal az Invitel támogatni és ösztönözni szeretné az innovatív kis- és középvállalatokat, hogy merjenek új dolgokat létrehozni, új irányokba elindulni, hogy példát mutatva teremtsenek biztos alapot az innovatív gondolkodás elterjedésének. Az ország versenyképessége is múlik azon, hogy miként teljesítenek majd ezek a cégek a következő években" – fogalmazott *Zsembery György,* az Invitel vezérigazgató-helyettese, aki egyben az InnoMax-díj zsűrijének elnöke is.

A szervezők további célja, hogy az üzleti maximalizmus, az innováció megkapja azt a kiemelt figyelmet, amit megérdemel – és amiről a gazdasági válság, a visszaesés miatt ritkábban esik szó mostanában. A verseny arra is lehetőséget ad, hogy a tehetséges vállalkozások egy kicsit másképpen is megmutatkozzanak. Bemutassák azt, amire büszkék, amit a maguk erejéből, tehetségéből hoztak létre.

MIÉRT ÉPPEN A KKV-K?

Az InnoMax a kkv-knak szól. Az Invitel választása azért esett a kis- és középvállalkozásokra, mert egyrészt ügyfélkörének is jelentős részét teszi ki ez a szektor – és ez is hozzájárult a cég sikeréhez –, másrészt ezek a cégek nem elhanyagolható mértékben, nagyságrendileg 45 százalékkal járulnak hozzá a hazai GDP-hez, így tehát jelentős a gazdaságban betöltött szerepük is. A korábbi felhívásokra a résztvevők mintegy fele az informatika területéről érkezett, de mellettük a gazdaság szinte valamennyi szegmenséből nyújtottak be pályázatot, vagyis igen széles volt a skála.

INNOMAX-DÍJASOK: ELIT KÖR

Az előző két év nyertesei között vannak olyan cégek, amelyek számára az innováció üzleti kérdés, mert ilyen iparágban dolgoznak, ebből élnek. Ilyen például a Hedz Magyarország Kft., amely iziSHOP, mTicket és eTicket rendszerével pályázott két éve. De ugyanígy az első InnoMaxon nyert díjat a 3D-s televíziózásban élenjáró iPONT International Kft. vagy az Opten Informatikai Kft. is. Ez utóbbi vállalat professzionális cég-adatbáziskezelő rendszerével érdemelte ki az elismerést.

A tavalyi évben az InnoMax zsűrije díjazta a GISDATA Kft. pályázatát – a cég egy térkép alapú internetes keresőmotort (GISearch) fejlesztett. De díjat nyert a NetLock is eGyűlés alkalmazásával, amelyen keresztül oly módon tarthatunk hiteles és biztonságos virtuális taggyűlést vagy megbeszélést, hogy annak eredménye (például jegyzőkönyv, határozat) bárhol, így – többek között – cégbíróság előtt is felhasználható. A legnagyobbak között, legalábbis méretben, azaz a 70–250 fős vállalati kategóriában a NEXON lett a győztes. A vállalat a dolgozók elégedettségét növelő, dolgozói portál funkcióval is rendelkező humán erőforrás és vállalatirányítási menedzsment megoldást fejlesztett, amely felhőszolgáltatásként is elérhető, így – mivel kezdő beruházást nem igényel – kevésbé tőkeerős kkv-k számára is előnyös.

Az InnoMax azonban nemcsak az informatikai piac innovátorairól szól. A Medicover Zrt. például a gyógyítást segítő, az orvos–beteg kommunikációt hatékonyabbá tevő rendszer fejlesztésével nyert különdíjat. A tavalyi évben pedig egy kertészettel foglalkozó kisvállalkozás, az Mg Park nyerte el a Kürt Zrt. különdíját. Ők azt mutatták be, hogyan használják az internetet az üzletszerzésben.

FIATAL TEHETSÉGEK VERSENYE: INNOAPPS

A tavalyi év kedvező tapasztalatai kapcsán ismét lesz InnoApps pályázat is, azaz a felsőoktatásban tanuló, illetve középiskolás „applikátorfejlesztők" versenye. Két kategóriában nevezhetnek a fiatalok: az üzlethez, munkához kötődő „komolyabb" témájú fejlesztésekkel a *Ne szórakozz!* kategóriában, a „könnyedebb" hangvételű fejlesztésekkel pedig a *Szórakozz!* kategóriában lehet pályázni. „Az Invitel számára fontos, hogy a legtehetségesebb fiatal fejlesztők is teret kapjanak tehetségük megmutatásához, és persze forrást további ötleteik megvalósításához. Az idei év újdonsága, hogy az Invitel a középiskolások számára is megnyitja a pályázati lehetőséget.

A tavalyi évben, a *Szórakozz!* kategóriában *Kátai Imre József* nyert díjat pályázatával, amellyel mozgó, interaktív háttérképet varázsolhatunk régen hallgatott albumaink felidézéséhez. A *Ne szórakozz!* kategória érdekessége, hogy nyertesét, *Huszár Csabát* szerződtette egy közös projektre az InnoMax-díjas térinformatikával foglalkozó GISDATA. Azt hiszem, ennél jobban semmi sem igazolhatná, hogy van értelme folytatni, sőt bővíteni az InnoApps díj lehetőségeit" – mondta az Invitel vezérigazgató-helyettese.

KLUBBÁ NŐTTE KI MAGÁT A VERSENY

Az InnoMax pályázat idei, második eredményhirdetésén merült fel az egyik pályázóban, hogy jó lenne, ha a résztvevők nemcsak egy-egy ilyen alkalommal, hanem gyakrabban, a két pályázati időszak között is találkozhatnának, így is tanulva egymástól. Így született meg az InnoMax Klub ötlete. „Ezeken a reggeliken elhangzó rövid előadásokkal azt szeretnénk elérni, hogy olyan tippeket és ötleteket kapjanak a résztvevők, amelyeket saját vállalkozásuk fejlesztésében is felhasználhatnak" – mondta Zsembery György. ■

HOGYAN LEHET PÁLYÁZNI AZ INNOMAX-DÍJRA?

Az innovatív kis- és középvállalatok versenyére 2011. november 28-tól 2012. február 21-ig lehet nevezni. Ehhez elegendő felkeresni a **www.invitel.hu/innomax** oldalt, majd a „Nevezés"-re kattintva kitölthető a rövid pályázati űrlap.

25 ÉVES AZ OMIKRON INFORMATIKA KFT.

Negyed évszázadnyi IT

Az IT világában 25 év már történelemnek számít, és az OMIKRON folyamatosan aktív részese volt ennek az izgalmas időszaknak. Az információtechnológia gyors fejlődése, a számítógépek hálózatba kapcsolása, a kapcsolatok minőségi változása, az összetett rendszerek, valamint az internet térnyerése pontosan jellemzik cégünk fejlődését is.

Törökbálinti székhellyel 1986. augusztus 13-án alakult meg az OMIKRON Számítástechnikai Kisszövetkezet. Tevékenységében már ekkor kiemelkedő szerepet kapott a hálózattervezés, emellett azonban jelentős részt képviselt a TANDON személyi számítógépek és FISKARS szünetmentes áramforrások értékesítése, telepítése, karbantartása, a szervertelepítés, de még a szoftverfejlesztés is.

1992. december 31-én az OMIKRON Számítástechnikai Kisszövetkezet OMIKRON Számítástechnikai és Informatikai Szövetkezetté alakult át, és a tevékenység egyre inkább a nagy kiterjedésű, nagy bonyolultságú hálózatok tervezése, kivitelezése és üzemeltetése felé fordult. Első partnereink (ODS, MADGE, 3COM) termékei ma már múzeumba kerültek.

1997 áprilisában új területtel bővült a cég tevékenysége: megalakult az AMP NETCONNECT Center üzletág. Az üzletág létrejöttének története 1989-ig nyúlik vissza, ugyanis a hálózatok építéséhez már ekkor is az AMP termékeit alkalmaztuk.

Húszéves szövetkezeti múlt után az OMIKRON Számítástechnikai és Informatikai Szövetkezet 2005. december 31-én OMIKRON Informatika Kft.-vé alakult át. Az új szervezeti formában megmaradt a magas hozzáadott értéket adó Informatikai Szolgáltatások és a szakértői központként nagykereskedelmet folytató AMP NETCONNECT Center üzletág.

AMP NETCONNECT CENTER ÜZLETÁG

Az OMIKRON Informatika Kft. 1997 óta az AMP System Master disztribútora. E minőségben Magyarországon az AMP legnagyobb kereskedelmi és egyetlen szakmai támogatást is nyújtó partnere. Az OMIKRON AMP NETCONNECT Center munkatársai magas szintű AMP-képesítéssel és termékismerettel rendelkeznek. A gyors kiszolgálásra 50 millió Ft-os raktárkészlet áll rendelkezésre, amely ma már a webáruházon keresztül is elérhető **https://webshop.omikron.hu**. Specialitás, hogy nagy rendszerek kivitelezésénél akár 25 éves rendszergarancia is elérhető, és egyedülálló felügyeleti megoldások (AMPTRAC, QUAREO) is növelik a hálózatok biztonságát.

INFORMATIKAI SZOLGÁLTATÁSOK

Az OMIKRON 25 évvel ezelőtt felismerte, hogy a hálózatba kapcsolt számítógépek a termelés, a gazdaság, a kis- és nagyközösségek számára egy új növekedési pályát, új gazdasági és életminőséget nyitnak meg. Hozzáfogtunk, hogy megtanuljuk és megvalósítsuk ezt a technológiát, és tanuljuk tovább, egyre bonyolultabb tételek formájában. Legfontosabb értékünket magasan képzett munkatársaink jelentik.

Alkalmazott megoldásainkban kiforrott, az informatikai piacon jól ismert, megfelelő támogatottsággal rendelkező gyártókra támaszkodunk. E gyártókkal nem csupán kereskedelmi viszonyban állunk, mindig törekszünk a szakmai alapú partneri viszony kialakítására.

Legfontosabb partneri kapcsolataink

- Cisco Premier Partner – 15 éve foglalkozunk Cisco hálózati megoldások tervezésével, telepítésével és üzemeltetésével.
- Trend Micro Partner – 8 éve foglalkozunk a cég biztonsági megoldásainak nagyvállalati környezetben történő alkalmazásával.
- BalaBit kiemelt support partner – cégünk az elsők között alkalmazta a BalaBit biztonsági megoldásait. Jelentős műszaki tudásbázisunk is hozzájárult a kiemelt support partneri fokozat eléréséhez.
- RSA SecurID partner – RSA SecurID és Authentication Manager integrált megoldásokat alkalmazunk nagyvállalati környezetben.
- Microsoft partner – a Microsoft TMG-megoldását alkalmazzuk nagyvállalati környezetben.
- Rittal RimatriX szervizpartner – géptermi megoldásainkban hangsúlyos szerepet kapnak a Rittal megoldásai. Munkáink során megszerzett speciális tudásunkat is elismerte a Rittal e partnerségi fokozattal, amellyel jelenleg egyedül az OMIKRON rendelkezik Magyarországon.

Az OMIKRON legfontosabb szolgáltatásai az integrált hálózatok tervezéséhez, telepítéséhez és üzemeltetéséhez kapcsolódnak.

Rendszerintegráció

- teljes vállalati informatikai környezet, hálózatok és kommunikációs rendszerek
- informatikai hálózatok biztonsági megoldásai
- szerverek virtualizációja
- vezeték nélküli kommunikáció
- hangátvitel IP-hálózaton, IP-telefonrendszerek
- nyílt forráskódú rendszereken alapuló felügyeleti rendszerek fejlesztése
- géptermek, adatközpontok teljes infrastruktúrájának tervezése és kivitelezése
- telepített rendszerek dokumentálása, ezen belül netViz-alapú online dokumentációs rendszer készítése.

Integrált kommunikációs rendszerek üzemeltetése és felügyelete

Az üzletág stratégiailag legfontosabb szolgáltatási tevékenysége a telepített hálózatok, számítógépes és kommunikációs rendszerek üzemeltetése. Szerződéseinkben 7×24 órában állunk ügyfeleink rendelkezésére az alábbi szolgáltatásokkal:

- teljes vállalati informatikai infrastruktúra üzemeltetése, a működés felügyelete, hibaelhárítás
- védelmi rendszerek üzemeltetése
- hálózatfelügyeleti rendszerek telepítése, paraméterezése, üzemeltetése
- a hálózati elemek, szerverek, szolgáltatások működésének monitorozása, naplózása, a működés, rendelkezésre állás analízise.

Az OMIKRON saját alkalmazásfejlesztése eredményeként – a kommunikációs rendszer eszközeinek működéséről folyamatosan gyűjtött adatokból – a cég sajátosságait tükröző online és időszakos értékelést készítünk az üzemeltetők és IT-vezetők számára (loganalízis, adatbázisok létrehozása, megjelenítés, havi jelentések).

Rendelkezésre állás: hálózati eszközök, szerverek, kapcsolatok és alkalmazások
Forgalomanalízis: adatforgalom, URL-statisztikák, sávszélesség-kihasználás, protokoll statisztikák
Kritikus helyzetek adatai: támadások, hibás állapotok, beavatkozások, vírusok
Felhasználói statisztikák: internethasználat, felhasználói adatok, autentikációs adatok.

ADATKÖZPONTOK TERVEZÉSE, KIVITELEZÉSE

Az OMIKRON az elmúlt években több nagy gépterem informatikai infrastruktúráját tervezte a TIA–942 szabvány ajánlásai szerint. Kiemeljük a géptermek szerverszekrényeinek folyadékhűtéses rendszereit. A géptermi speciális hűtőrendszereket a Rittal LCP vízhűtéses technológiájára alapozva tervezzük. Ezzel a technológiával szekrényenként akár 20 kW koncentrált hűtőteljesítményt tudunk biztosítani. A géptermi áramellátó és hűtőrendszerek telepítését üzemeltetését és karbantartását Rittal RimatriX szervizpartnerként végezzük.

AZ ÜZLETI SIKER ZÁLOGA

25 év alatt szándékunk szerint soha nem fordult elő, hogy rövid távú üzleti siker érdekében kockára tettünk volna hosszú távú együttműködést. Meggyőződésünk, hogy komoly szakmai és üzleti eredményt csak tartós üzleti kapcsolat keretében lehet elérni, aminek az alapja a tudás, a munka, a minőség és a bizalom. ■

KRISTÓF CSABA

> Az APT-k esetében a korai felismerés kulcsfontosságú a károk megelőzése, illetve csökkentése érdekében.

Kegyelmet nem ismerő támadások

A fejlett, célzott támadások az informatikai infrastruktúrákra, illetve az azok által tárolt, kezelt adatokra nézve igencsak jelentős kockázatokat hordoznak. E fenyegetettségek ellen a technológiai védelem korántsem elegendő, annál jóval többre van szükség.

Idén az informatikai biztonság – a már hagyományosan sok problémát okozó kártékony programok mellett – elsősorban a mobileszközök által jelentett kockázatokról, a cloud computing kapcsán felmerülő védelmi nehézségekről és az internetes fenyegetettségekről szólt. Eközben azonban egy jól megfigyelhető trend bontakozott ki, amely szerint a kiberbűnözés sok esetben már nem vaktában lövöldöz, hanem célzott támadásokat hajt végre. Méghozzá olyan módon, hogy azok a kiszemelt szervezetek védelmi infrastruktúráját a lehető legtöbb szinten próbára tegyék. A célzott támadások elszaporodása némileg hasonlít a vírusok világában elmúlt években tapasztalható fejleményekhez. Napjainkban ugyanis a kártékony programok terjesztőinek már többnyire nem az a céljuk, hogy globális, a saját hírnevüket növelő fertőzésekhez járuljanak hozzá, hanem az, hogy kisebb területeken terjedő, sok variánsból álló víruscsaládokat hozzanak létre. Ezek révén a lehető legtovább tudnak észrevétlenek maradni mind az antivírus cégek, mind a felhasználók előtt. Céljuk pedig egyértelműen az anyagi haszonszerzés és az adatlopás. Nagyon hasonló a helyzet a fejlett támadások kapcsán is.

Az elmúlt évek során egyre többször lehetett találkozni az APT (Advanced Persistent Threat) rövidítéssel, amely napjainkban kezd olyan felkapott kifejezéssé válni, mint például a virtualizáció vagy a cloud computing. Azonban ez esetben olyan problémáról van szó, amelyet minden szervezetnek nagyon komolyan kell vennie. Kétségtelen, hogy a biztonsági cégek az APT-t is egyre többször említik meg marketingkampányaikban, azonban – mint látni fogjuk – most nem egy termékről, szolgáltatásról vagy egy hype-olt technológiáról beszélünk, hanem olyan fenyegetettségről, amely ellen csak összetett, többszintű védelem kialakításával lehet felvenni a küzdelmet, és a siker még ekkor sem garantált.

MI IS AZ AZ APT?

Az APT (Advanced Persistent Threat) a fejlett, perzisztens fenyegetettségek összefoglaló neve, rövidítése. Rögtön adódik a kérdés, hogy a „fejlett", a „perzisztens" és a „fenyegetettség" kifejezések ezúttal pontosan mit is takarnak.

Fejlett: a támadók számos eszközt használnak fel céljuk eléréséhez. Vagy rendelkeznek azokkal az erőforrásokkal, amelyek révén nulladik napi sebezhetőségek kihasználására alkalmas exploitokat tudnak készíteni, vagy a feketepiacon vásárolnak ilyen kódokat, illetve azokat magukban foglaló kártékony programokat. Céljuk, hogy elkerüljék a célkeresztbe állított rendszert körülölelő vagy az abban működő védelmi eszközöket. A NIST (National Institute of Standards and Technology) mindezt így fogalmazta meg: *a támadók alkalmazkodnak a védők erőfeszítéseihez annak érdekében, hogy azokkal szembeszállhassanak.*

Perzisztens: a támadók egy jól meghatározott céllal tevékenykednek, és többnyire nem véletlenszerűen, találgatás útján próbálnak rájönni, hogy milyen sebezhetőségeket tudnak kihasználni, hanem már felkészülten, alapos felderítőmunka után lépnek akcióba. Ameddig el nem érik a céljukat (például meg nem találják az általuk keresett bizalmas adatokat), addig nem hagyják el a rendszert. Gondoskodnak arról, hogy a hozzáférésük fenntartható legyen. Sok esetben több hozzáférési pontot is kialakítanak, hogy a jelenlétüket huzamosabb ideig biztosítani tudják.

Fenyegetés: a támadók általában nem egyszerű portszkenneléseket, SQL injection támadásokat stb. hajtanak végre, és legtöbbször nem alkalmaznak automatizált károkozásra alkalmas programokat sem. Nyilván ezek is megjelenhetnek az eszköztárukban, azonban ez esetben célzott, irányított és komplex akciókról beszélünk, amelyek komoly fenyegetést jelenthetnek az informatikai rendszerekre és az adatokra. Ennek megfelelően a védekezés sem kivitelezhető hatékonyan csupán hagyományos biztonsági eszközök bevetésével.

AZ APT-TÁMADÁSOK FELÉPÍTÉSE

Az APT-támadásokat általában három vagy négy szakaszra bonthatjuk, de a lényeg minden esetben ugyanaz. Az első vagy nulladik fázisként a támadó pontosan feltérképezi a célpontot, és olyan személyeket, alkalmazottakat keres, akiket social engineering trükkök révén rászedhet. Ezzel pedig el is érkeztünk az APT-k talán legfontosabb jellemzőjéhez, amely nem más, mint az emberi tényezőkre, tulajdonságokra épülő károkozások megjelenése a fejlett fenyegetettségekben. Mint arról még később szó lesz, a védelmet ez alapvetően befolyásolja.

Második lépésként a megtévesztett felhasználónak le kell futtatnia egy kódot, akár úgy, hogy megnyit egy

RSA VS. APT

A 2011-es Informatikai Biztonság Napjának egyik előadása az APT-k kapcsán sok érdekességet tartogatott, hiszen az RSA úgy határozott, hogy a magyar konferencián részletesen is beszámol tavaszi biztonsági incidensének részleteiről. *James Lugabihl,* az RSA CIRC vezetője először arról beszélt, hogy miként következett be az az APT- (Advanced Persistent Threat) támadás, amely bizalmas adatok kiszivárgásához vezetett. Az incidenshez egy olyan Excel fájlt tartalmazó e-mail járult hozzá, amelyet a cég egyik alkalmazottja a spamekre fenntartott mappából állított helyre, majd megnyitotta. Amint az Excel fájlt megtekintette, a háttérben egy nulladik napi Flash-hibát kihasználó exploit futott le. Ennek segítségével a támadók először átvették a hatalmat a felhasználó PC-je felett, majd rögtön hozzáfogtak a hálózat feltérképezéséhez. Egészen addig keresgéltek, amíg rá nem akadtak a titkos SecurID információkra, amelyeket egy hálózaton megosztott könyvtárba importáltak. Végül egy jelszóval védett RAR-fájl formájában juttatták ki az adatokat egy külső szerverre. Lugabihl elmondta, hogy az incidens után mélyreható forensic vizsgálatot végeztek annak érdekében, hogy a valós károkat és az eset körülményeit feltárják. Emellett átfogó védelmi intézkedéseket foganatosítottak, amelyek magukban foglalták a tartományvezérlőkhöz, a felhasználói fiókokhoz, a munkaállomásokhoz, valamint a webes tartalmak kezeléséhez tartozó biztonsági szabályok szigorítását. Továbbá újragondolták a felhasználói oktatásokat és a naplózást. A szakember a hasonló problémák elkerülése érdekében mélyreható védelem megvalósítását javasolta és felhívta a figyelmet az incidensreagálási képességek fokozására, a káros események korai felismerésére alkalmas eszközök bevezetésére és a forensic elemzések fontosságára.

> A fejlett fenyegetettségek ellen csak többszintű, mélyreható védelmi infrastruktúra felállításával és gondos üzemeltetésével lehet védekezni.

e-mailben lévő ártalmas állományt, vagy megtekint egy kártékony weboldalt. Egy – általában nulladik napi – sérülékenység kihasználásával a támadó egy hátsó kaput tud felépíteni, amelyen keresztül hozzáfér a szervezet belső informatikai infrastruktúrájához. Az ilyen módon megfertőzött számítógép tehát nem a végső célpont, az csak egy „ugrópont" a hálózat és más rendszerek alapos feltérképezéséhez. Amennyiben az elkövető ráakad a számára fontos szerverre, adatbázisra, akkor harmadik lépésként megpróbál ahhoz is hozzáférést szerezni, majd az értékes adatokat különböző módokon, de általában titkosított és tömörített formában interneten keresztül továbbítja saját magának, miközben gondoskodik arról, hogy a rendszerben a jelenléte folyamatosan, huzamosabb időn keresztül biztosított legyen.

IZZASZTÓ VÉDEKEZÉS

Ahogy azt az előbbiekben már említettük, az APT-k egyik kulcstényezője a social engineering, amelynek esetében csupán technológiai védelemmel nem lehet megfelelő mértékben csökkenteni a kockázatokat. Az APT-k további fontos összetevői a nulladik napi sebezhetőségek kihasználására alkalmas, sokszor egyedi exploitok is feladják a leckét, nem beszélve az adatszivárgások felismeréséről. Mindebből az is következik, hogy a fejlett fenyegetettségek ellen csak többszintű, mélyreható védelmi infrastruktúra felállításával és gondos üzemeltetésével lehet védekezni.

A védelemben a biztonsági eszközök és az emberi tényezők kezelésének is kulcsfontosságú szerepet kell betöltenie. Azonban csak akkor lehet hatékony intézkedéseket hozni, ha egy szervezet tisztában van azzal, hogy pontosan mit is kell megvédenie a támadóktól, és normál működés esetén milyen események következhetnek be. Ez utóbbi azért fontos, mert az APT-k során felmerülő anomáliákat csak ezek ismeretében lehet kiszűrni.

A biztonsági eszközök szintjén a vírusvédelmi megoldások, tűzfalak, behatolásdetektáló és megelőző rendszerek nyilvánvalóan fontosak, de korántsem elégségesek. Szükség

TÁMADÁSÉSZLELÉS ÉS VÉDEKEZÉS

Barna Tamás, a McAfee CEE technikai vezetője szerint nemcsak az APT-támadások jelentenek veszélyforrást, hanem minden támadás jelentős és veszélyes. A szervezeteknek ugyanis nem terminológiák ellen kell védeniük magukat, hanem megbízható biztonsági gyakorlatok alapján kell működniük. Az APT és más hasonlóan célzott támadások egy szervezet legfontosabb értékeit veszik célba, ez lehet szellemi tulajdon, kereskedelmi és üzleti titok. A szellemi tulajdont ért incidensek sokkal nagyobb károk okozására képesek, mint a pénz által motivált támadások. Az APT-k esetében az a legrosszabb, hogy a támadók újra és újra megpróbálják megtámadni – akár éveken keresztül – az adott célpontot, miközben megfelelően szervezett erőforrásokkal rendelkeznek ahhoz, hogy elérjék a céljukat. A szakember úgy látja, hogy a nyilvánvaló célpontok Magyarországon vagy bárhol máshol a világban a high-tech cégek, a katonai objektumok, a kritikus infrastruktúrák és természetesen a kormányzati szervek. De ez nem egy exkluzív lista, bármilyen szervezet célponttá válhat.

BARNA TAMÁS
technikai vezető, McAfee CEE

Barna Tamás véleménye szerint a biztonság megteremtésében a legfontosabb alapkövetelmény a felhasználói biztonságtudatosság. Az első védelmi lépések között kell szerepelnie a szükségtelen felhasználói privilégiumok megszüntetésének és a külön hálózat alkalmazásának a napi tevékenységekhez –, utóbbinak jól szegmentáltnak kell lennie a szellemi tulajdont tároló, működtető rendszerektől. Fontos eszköznek számít a központosított patch menedzsment és jelentéskészítés. Léteznek e célokra optimalizált, jól működő biztonsági megoldások, ilyenek például a DLP-k, az IPS-ek, a hálózati viselkedést elemző rendszerek, valamint az adatbázis biztonsági és alkalmazásintegritás-ellenőrző lehetőségek. „Amikor védekezünk, azt kell feltételeznünk, hogy néhány felhasználó vagy rendszer előbb-utóbb fertőzött lesz. A legfontosabb kérdés: hogyan tudom észlelni, ha a támadó használja ezeket az accountokat, gépeket, és ezzel egyidejűleg azt, hogy egyre mélyebbre hatol a hálózatba" – nyilatkozta a szakember.

SZERENCSÉS HELYZETBEN VAGYUNK

Bódis Ákos, a NETASQ közép-kelet-európai regionális vezetője szerint az APT-támadások jelentőségét katonai, kormányzati hátterük adja, mivel nem egyszerű, hasznot kereső kiberbűnözők, hanem professzionális titkosszolgálatok állnak mögöttük. Éppen ezért nem is a gyors és automatizált haszonszerzés, hanem a lassú, de biztosan sikeres információszerzés, szabotázs az APT-támadások valódi célja. „Fontosnak tartom kiemelni, hogy az APT-támadások eszköztárában nem a hagyományos értelemben vett hackerek szokásos módszerei állnak, hanem sokszor olyan katonai és kormányzati eszközök, amelyek egy hacker számára elérhetetlenek. Például a mobilhálózatok vagy internetes gerinchálózatok lehallgatásának képessége, kémműholdak használata adott egy titkosszolgálat számára, de a bűnözők ezekhez nem férhetnek egyszerűen hozzá; egy tipikus kibertámadást sokkal inkább tudnék egy alvilági leszámoláshoz hasonlítani, míg egy APT-támadást egy katonai, tankokkal és vadászgépekkel végzett művelethez. Egyértelműen mások az eszközök és a képességek a két esetben, ezért nem is lehet az APT-támadásokat a hétköznapi kiberbűnözéssel összevetni – mondta Bódis Ákos.

– Az EU kicsiny tagországaként sem katonai, sem gazdasági célpontot nem találnék Magyarországon APT-támadásokhoz – folytatta. – Sem ipari kémkedéshez nem áll rendelkezésünkre értékes technológia, sem egy terrorista támadásnak nem lennénk jó célpontjai, hiszen egy esetleges magyarországi támadás nem riasztaná el sem az EU, sem az Egyesült Államok állampolgárait, mindössze Budapest kerülne le az utazási irodák ajánlatából. Tudom, hogy ez nagyon sarkított nézőpont, de a lényegen nem változtat: ugyanúgy nem vagyunk APT-támadások célpontjai, mint a régió más országai, amelyek gazdasági, katonai és politikai téren sem hoznak globális döntéseket. Úgy gondolom viszont, hogy ez rendkívül szerencsés helyzet, és örülök neki, hogy ez a távoli jövőben sem fog megváltozni" – vélekedett a szakember.

BÓDIS ÁKOS
regionális vezető, NETASQ

VÁLOGATÁS A LEGJELENTŐSEBB APT-TÁMADÁSOKBÓL

Operation Aurora – 2010. január 12.
A támadássorozat valójában 2009 közepén kezdődött, de annak részleteit a Google csak 2010 elején hozta nyilvánosságra. Ekkor kiderült, hogy a Google mellett célkeresztben voltak olyan vállalatok is, mint például az Adobe és a Juniper. Az akció legalább egy tucat nagyvállalatot érintett, de sok cég nem erősítette meg hivatalosan, hogy az Aurora számukra is gondokat okozott. A Google a támadások kapcsán Kínát okolta, de Kína cáfolta, hogy bármilyen köze lenne a történtekhez. A károkozások alapjául egy nulladik napi Internet Explorer sérülékenység szolgált, amelyet az elkövetők e-mailekben vagy azonnali üzenetküldőkön keresztül célzottan terjesztett JavaScriptek segítségével igyekeztek kihasználni hátsó kapuk létesítéséhez. Később az F-Secure arról számolt be, hogy a támadásokban egy Adobe Reader sebezhetőség, valamint kártékony PDF-állományok is szerephez juthattak.

RSA – 2011. március 18.
Az RSA egy olyan APT-támadás bekövetkezését ismerte el, amely bizalmas SecurID információk jogosulatlan kezekbe kerüléséhez vezetett, és a SecurID-alapú többfaktoros hitelesítés kapcsán kockázatokat vetett fel.

Oak Ridge National Laboratory – 2011. április 21.
Április elején az Oak Ridge laboratórium számítógépes rendszere ellen APT-támadás indult. Április 21-én az illetékesek elismerték, hogy az elkövetők bizalmas adatokhoz fértek hozzá az Internet Explorer egyik nulladik napi biztonsági résének kihasználásával. A támadóknak több mint 50 számítógépet sikerült az irányításuk alá vonni, és több mint egy gigabájtnyi titkos adatot tulajdonítottak el.

van olyan monitorozó, naplózó és eseménykezelő rendszerek bevezetésére, amelyek a nemkívánatos történéseket a kliensek, a szerverek és a hálózati adatforgalom figyelésével ki tudják szűrni, és gyanús tevékenység esetén gyors riasztást, illetve incidensreagálást biztosítanak. Az APT-k esetében ugyanis a korai felismerés kulcsfontosságú a károk megelőzése, illetve csökkentése érdekében. Mindezek mellett nem szabad megfeledkezni a patch menedzsmentet támogató eszközök, valamint az adatszivárgás-megelőzésre alkalmas megoldások használatáról sem.

Mint az oly sokszor elhangzik, a védelem leggyengébb láncszemét maguk az emberek jelentik, amit az APT-k esetében a támadók könyörtelenül ki is használnak. Ezért a technológiai védelem mellett a biztonságtudatosság fokozására is komoly hangsúlyt kell helyezni. A felhasználók oktatása, rendszeres képzése elengedhetetlen ahhoz, hogy már a kezdetek kezdetén megállíthatók legyenek a fejlett támadások. Nyilvánvalóan arról is gondoskodni kell, hogy minden felhasználó csak olyan rendszerekhez és annyi adathoz férhessen hozzá, amennyi a munkájához feltétlenül szükséges.

Gavin Reid, a Cisco Security Incident Response Team vezetője úgy látja, hogy az APT-k detektálása nem könnyű feladat, ugyanis azok ellen nincsenek olyan megoldások, mint például a vírusvédelemben a szignatúra-adatbázisok, amelyekkel fel lehetne azokat ismerni egy hálózatban. A szakember szerint a szervezeteknek az APT-fenyegetettségek ellen több fronton kell felvenniük a küzdelmet. Így például fontosak a mélyreható csomagvizsgálatokra épülő hálózati ellenőrzések, valamint a naplózó rendszerek használata. „Attól, hogy egy szervezet még nem észlelt APT-támadást, korántsem biztos, hogy nem került célkeresztbe, vagy a védelme tökéletesen működik" – nyilatkozta a szakember, aki szerint sok múlik azon is, hogy az ilyen támadások felismerésére rendelkezésre állnak-e a megfelelő eszközök, illetve intézkedések. Majd hozzátette: „Ha valaki azt állítja, hogy az ön cége számára olyan hardvert vagy szoftvert ad el, amely megoldást jelent az APT-kre, akkor az vagy nem érti az APT-k lényegét, vagy nem tudja, hogy valójában hogyan működnek a számítógépek." Reid ezzel igyekezett érzékeltetni, hogy az APT-k elleni védekezést egyetlen eszközzel nem lehet megoldani.

MIT HOZ A JÖVŐ?

A fejlett támadások az idő előrehaladtával még kifinomultabbakká fognak válni, és egyelőre semmiféle jel nem látszik, amely az APT-k visszaszorulását mutatná. Sőt, a jövőben a célzott támadások számának további növekedésével kell számolni, ami egyben az összetett, többszintű és mélyreható védekezési feladatok fontosságára hívja fel a figyelmet. Az ugyan kétségtelen, hogy a fejlett támadásokkal szemben nem könnyű felvenni a küzdelmet, de a kockázatok kezelésére nagy szükség van.

Kockázat- és megfelelőségkezelés SAP módra

Információbiztonsági szempontból a GRC-nek (Governance, Risk, Compliance) fontos szerepet kell kapnia a kockázatok, valamint a megfelelőség korszerű kezelése érdekében. A GRC szerepéről és megvalósítási lehetőségeiről *Pintér Szabolcsot,* az SAP Hungary Kft. üzletágvezetőjét kérdeztük.

COMPUTERWORLD: Melyek a GRC legfontosabb összetevői?
PINTÉR SZABOLCS: A GRC fontos biztonsági tényező. Azonban erre elsősorban nem úgy kell gondolni, mint a klasszikus IT-biztonságra, ugyanis sokkal inkább üzleti megközelítésről beszélünk: az irányítás, a kockázatkezelés és a megfelelőség kerül előtérbe. Ennek megfelelően a GRC az SAP terminológiájában több megoldást is takar, amelyek számos nemzetközi és hazai referenciával rendelkeznek. Például a Risk Management a kockázatkezelést támogatja, a Process Control a vállalati kontrollpontok létrehozását, megjelenítését, monitoringját biztosítja, míg az Access Control a jogosultságkezelést és az összeférhetetlenségek feltárását, kontrollálását segíti.

CW: A hazai vállalatok miként viszonyulnak a GRC-hez?
P. SZ.: A leginkább keresett megoldás az Access Control. Ennek az az egyik oka, hogy egy közép- vagy nagyvállalatnál több rendszer is működik párhuzamosan, és az alkalmazottak összeférhetetlenség-kezelése jellemzően nem megoldott. Sokszor nem vizsgálják a szervezetek, hogy mindez mekkora kockázatot jelent. Az SAP megoldása összetett kockázatkezelésre alkalmas, és nemcsak SAP-n belül képes ellátni a feladatát, hanem rendszerek közötti összeférhetetlenségi vizsgálatokat is le tud folytatni.

CW: Melyek azok a megfelelőségi követelmények, amelyeknek teljesítését az SAP GRC támogatja?
P. SZ.: Például az egyik a SOX (Sarbanes–Oxley Act), melynél az összeférhetetlenség-vizsgálat fontos kritérium. De ha egy vállalati környezetre gondolunk, akkor a külső szabályozók mellett sok belső követelmény merülhet fel, amelyek üzlet- és iparágfüggők lehetnek. E szabályozók kezelése is támogatott.

CW: Miként zajlik az SAP GRC-eszközök bevezetése, üzemeltetése?
P. SZ.: Maguknak az eszközöknek a telepítése egyszerűen elvégezhető. Először azokat a rendszereket szükséges definiálni, amelyeket hozzá kell csatolni a GRC-megoldásokhoz, majd meg kell határozni a kockázati és összeférhetetlenségi mátrixokat. Az általunk biztosított mátrixok több száz szabályt tartalmaznak, de ezek természetesen testre szabhatók az egyedi, akár iparági igényeknek megfelelően. A kockázatelemzést követően következik egy tisztítási fázis, melynek során a szerepek felülvizsgálata is megtörténik. Ezután már lehet automatizálni a jogosultságkezelést és a szerepmenedzsmentet a kockázatoknak megfelelően, azaz biztosított a fenntarthatóság. Az üzemeltetés során hiteles, mélyreható naplózásra, valamint auditálásra van mód, miközben a menedzsment – a szervezetek különböző szintjeinek megfelelően – pontos rálátást ad a rendszer működésére. ■

PINTÉR SZABOLCS
üzletágvezető
SAP Hungary Kft.

Cisco NAC statisztikák

A Cisco Network Admission Control (NAC) rendszerkörnyezet segítségével valamennyi vállalati, intézményi munkaállomás, távoli eléréssel rendelkező PC, illetve az ideiglenesen kapcsolódó vendég számítógépek aktuális állapotának ellenőrzése minden egyes felhasználói belépéskor megtörténik. A Cisco által a rendszerhez szállított konzolprogram gyári lehetőségeivel nehézkes a teljes rendszerre vonatkozó, adott időszakra összegzett, általános statisztikákat készíteni és megjeleníteni. A NAC üzemeltetői számára ugyanakkor alapvető fontosságú, hogy átfogó statisztikai képet kaphassanak a rendszerről, és ezáltal azonosíthatóvá válhassanak a rendellenességek.

Az SCI-Network zRt. szakemberei – akik évek óta foglalkoznak a Cisco biztonsági megoldásaival – a NAC-rendszerek bevezetésekor szerzett tapasztalataik alapján rugalmasan konfigurálható programot fejlesztettek. A *NAC Reporter Program* folyamatos kapcsolatot tart a Cisco NAC szerverekkel. A Cisco gyártói API-felületén keresztül elérhetők a NAC naplóbejegyzései. Ezeket speciális szempontok szerint formázva saját SQL-adatbázist épít fel a program. Ebből az adatbázisból aztán átfogó, részletes kimutatásokat lehet készíteni, és egy testre szabott grafikus felületen megjeleníteni. A vállalati szintű statisztikák alapján egyértelműen látható, hogy mely kritériumok bizonyulnak túl szigorúnak (például nagyszámú munkaállomás nem felel meg az elvárásnak), vagy melyek a csak időszakosan felmerülő biztonsági hiányosságok (például egy szoftverfrissítés átvezetése a vállalat összes munkaállomására).

Az SCI-Network zRt. által fejlesztett *NAC Reporter Program* aktuális verziója egy adott nagyvállalati környezet számára kialakított beállításokkal készült, de rugalmas alapkoncepciója és szabványos interfészei miatt bármelyik Cisco NAC-környezethez egyszerűen adaptálható. ■

Kiszervezett logmenedzsment

A logmenedzsment az információbiztonság kapcsán felmerülő kockázatok csökkentésének egyik nélkülözhetetlen eszköze. *Dani Istvánt,* a KFKI Zrt. Biztonsági Kompetencia-központjának műszaki igazgatóját arról kérdeztük, miként lehet a naplókezelést hatékonyan megvalósítani.

COMPUTERWORLD: Miként győződhet meg egy szervezet arról, hogy valóban szüksége van központi logelemzésre?
DANI ISTVÁN: A bevezetést latolgató cégeknek fel kell tenniük maguknak néhány alapvető kérdést. Az első, hogy volt-e az elmúlt időszakban biztonsági eseményük. Egyáltalán észlelték volna az incidenst? Ha igen, képesek lennének visszakövetni a naplókból, hogy pontosan mi történt? Ha az incidens gyanújának árnyéka például egy dolgozóra vetül, egy munkaügyi perben megállnák-e a helyüket azok a bizonyítékok, amelyeket a jelenlegi naplózás biztosít? Végül, de nem utolsósorban: vannak-e törvényi kötelezettségek, iparági elvárások a szervezettel szemben ezen a téren?

CW: Milyen alapvető elvárásoknak kell megfelelni a naplókezelő rendszerek üzemeltetése során?
D.I.: Egy logelemző rendszer bevezetése inkább folyamatnak tekinthető, mint egyszeri projektnek. A naplózó szabályokat az üzemeltetés során rendszeresen felül kell vizsgálni, és a finomhangolást, a logelemzők tanítását sem szabad abbahagyni. Emellett napi szinten szükséges ellenőrizni, hogy mi történik az infrastruktúrában, és ha az események korrelációja incidens gyanúját veti fel, annak értékelését követően utána kell járni a történteknek. Ez azonban munkaigényes tevékenység.

CW: Hogyan lehet csökkenteni a logmenedzsment kapcsán felmerülő erőforrás-szükségleteket?
D.I.: A cégeknél egyre kevesebb erőforrás jut az informatikai területre, különösen az IT-biztonságra. Sokszor nincs elég – megfelelő szakképzettséggel rendelkező – emberi erőforrás, amivel biztosítani lehetne az akár profi naplóelemző rendszerek menedzselését, és az események megbízható értékelését. A KFKI, a Magyar Telekom Csoport tagja, közép- és nagyvállalatok által igénybe vehető távfelügyeleti szolgáltatást kínál, amellyel ezeket a feladatokat át tudjuk venni. Értékeljük a naplókat, kiszűrjük a releváns eseményeket és felhívjuk az ügyfél figyelmét a kockázatokra. A naplóelemző rendszerek inkább technikainak mondható riportjai helyett fókuszált, áttekinthető összefoglalót adunk a napi történésekről.

CW: Milyen biztonsági intézkedésekkel biztosítja a KFKI távfelügyeleti szolgáltatásának biztonságát?
D.I.: Az adatok nem kerülnek át a KFKI-hoz. Mi csak a logelemző eszközök felületeit látjuk. Ahhoz, hogy mindez biztonságos legyen, egy Menedzselt Információs Biztonsági Központot hoztunk létre, amely teljesen független a KFKI belső hálózatától. Biztonsági elemző szakembereink tevékenysége folyamatosan monitorozott és hitelesen naplózott. Szolgáltatásunk akár a PSZÁF ide vonatkozó előírásait is kielégíti. ■

DANI ISTVÁN
műszaki igazgató
KFKI Zrt. Biztonsági Kompetencia-központ

BalaBit IT Security
www.balabit.com

Felhők között a teljesítmény és a megbízhatóság kritikus

syslog-ng log server
A világ első HSRL naplózó technológiája

HIGH-SPEED RELIABLE LOGGING
- több mint 650.000 üzenet másodpercenként
- megbízható továbbítás és tárolás
- üzenetvesztés nélkül

Tudjon meg többet a termékről, és töltse le a syslog-ng próbaverzióját.

Az adatszmogban túl sok információ, túl sok minőségben és alakban jelenik meg, térben és időben túl sok helyen található.

MEIXNER ZOLTÁN

Világrengető durranás az adatszmogban

Van egy cég, amely elemzőszoftvere segítségével a tömeges adatok káoszából képes kinyerni a releváns információkat, megtalálni közöttük a valódi kapcsolatot, feltárni és bizonyítani az összeesküvést, csalást, politikai és gazdasági fondorlatot. Bennfentesek szerint a Palantir Technologies lesz a következő milliárd dolláros durranás.

ALEXANDER KARP

CEO
Palantir Technologies

A frankfurti egyetemen szerzett társadalomfilozófiából doktorátust, majd a Stanford Egyetemen helyezkedett el *Alexander Karp.* Mellesleg a PayPal online fizetési szolgáltatást kínáló társaságnál is dolgozott, ahol barátja, *Peter Thiel* volt a főnök és főtulajdonos. A PayPal egy ideje már küszködött az orosz szervezett bűnözés megismétlődő mesterkedéseivel, amikor Karp felvázolta elképzelését a probléma megoldására. Ez olyan jónak tűnt, hogy 2004-ben Palantir Technologies néven stanfordi számítógéptudósokkal és paypalos szakemberekkel céget is alapítottak a megvalósítására. Ahogy a dolgok most kinéznek, ebből lehet a következő milliárd dolláros, életünket felforgató internetcég a Facebook után, ahol – milyen meglepetés! – Peter Thiel szintén a főbefektetők között van. A Facebook az orrunk előtt fejlődik, a Palantir azonban egyáltalán nem. Nincs nyilvános marketingje, vezetői nem vágynak a reflektorfénybe, s ha a sajtó nem kutakodna utánuk, talán nem is érthetnénk meg, hogy a világra a Palo Altó-i cégnek máris komoly befolyása lehet.

A Világgazdasági Fórum választása szerint Alexander Karp bekerült 2012 technológiai úttörői közé. Ebből az alkalomból a Palantir Technologies társalapítója és vezérigazgatója így foglalta össze cége céljait: „A nagyvállalatoknál, nagy szervezeteknél vannak különféle bizalmas területek, ahol nem egy adatkészlet van, hanem számos, ezeknek az adatoknak az összefüggéseit kell megérteni, hasznosítani, de úgy, hogy a bizalmas információk és személyiségi jogok ne sérüljenek. Az adatokban rejlő titkok megfejtésével dolgoztak már a kibercsalások ellen, például a dalai lámát ért támadások elhárításán, a gyanús jelzáloghitelek kiszűrésén, banki csalások leleplezésén és állami intézmények megvédésén. Nem a vállalati haszon növelésének eszközét akarjuk kifejleszteni, hanem olyat, amelyik gazdagítja a társadalmat. Az a célunk, hogy a társadalmat jobb hellyé tegyük mindannyiunk számára."

A WIKILEAKS-ÜGY

Az emberi jogi problémákkal foglalkozó, tudósként is ismert Alexander Karp szájából jól hangzanak ezek a szavak, de a tényfeltárás világa tele van buktatókkal, amely a Palantir életében is gyorsan bekövetkezett. De talán ez az ügy is hozzájárult a társaság csillagának gyors emelkedéséhez. Tavaly év elején ugyanis nyilvánosságra került egy a cégtől származó javaslat, amely a nagyvállalatok biztonságát védő HBGary és a Berico Technologies számára készült. Az említett cégek a Bank of Amerika érdekében a WikiLeaks és támogatói ellen indítottak volna kibertámadást, illetve a ThinkProgress weboldal ellen az USA kereskedelmi kamarája megbízásából – persze a javaslat szerint. Végül a Palantir Technologies a dokumentumot egy munkatársa magánkezdeményezésének nyilvánította, amelyet visszavont és bocsánatot kért minden érintettől. Annyi azonban világossá vált, hogy a rendszer rossz kezekben rosszra is használható.

A kormányzati megbocsátást mi sem mutatta jobban, mint az a tavaly júniusi sajtótájékoztató a Fehér Házban, ahol *Joe Biden* alelnök és a költségvetési tanács igazgatója, *Peter Orszag* bejelentette a pénzügyi csalások elleni testület (RATB) sikereit. Biden a sikert annak tulajdonította, hogy a szövetségi kormány bevetette a Palantirt. Kilátásba helyezte, hogy további kormányügynökségek is megkapják a szoftvert, legelőször is az egészségügyi szolgálatok.

A kormányzati elismertséget az üzleti világ megbecsülése is követte. Jól mutatja ezt, hogy a JPMorgan Chase, a világ egyik leghatalmasabb bankháza, a Palantirt nemrégiben beválasztotta a legjelentősebb innovációk csarnokába (Hall of Innovation) az üzleti életre gyakorolt hatása, technológiájának konvenciókat szétromboló természete és az üzleti érték előállítására való képessége miatt. *Guy Chiarello,* a JPMorgan Chase vezérigazgatója a szoftvert olyan ablaknak nevezte, amelyen keresztül általában és konkrétan is rálátnak azokra

az adatokra, amelyek befolyással vannak az ügyfeleikre, s ezzel több értéket állíthatnak elő. A pénznek ugyan nincs szaga, de a New York-i megabank hálálkodása azt mutatja, Peter Thiel szimata alighanem a helyén van.

Az amerikai pénzügyi rendszerre amúgy nagyon ráfért egy ilyen fejlett elemzőeszköz. Üzletiintelligencia-megoldásokat eddig is használtak, de ahogy Karp mondja: „A BI olyan algoritmus, amelyet senki sem ért" –, a Palantir viszont a legkülönfélébb elemzőeszközöket kínálja a felhasználóknak, akiknek ezek segítségével saját észjárásuknak megfelelően van lehetőségük feltárni a rejtett információkat, tendenciákat. Az ingatlanpiacról elinduló válságot egy olyan pénzügyi fondorlat váltotta ki pár évvel ezelőtt, amelyről bárki bizonyossággal hihette, hogy a trükközés sohasem derülhet ki, mígnem a piac a teljes összeomlás határára jutott. A módszer egyszerű volt: mesterségesen felpumpálták az ingatlanok eladási árát, aztán a pénzt bevitték jelzálogügyletekbe és származékos ügyletekbe, ahol az újra és újra átcsomagolt pénzpiaci termékek között a túlértékelt, „mérgezett" papíroknak nyomuk veszett.

Azóta a legnagyobb hitelintézetek már használják a Palantirt. A jelzálogpiaci elemzések során a szoftver segítségével néhány igen kemény és nyomasztó tényre derült fény, de a válság eseményeinek ismeretében ezek már nem is igazán voltak meglepők. Azt találták, hogy a származékos ügyletek piacán (ahol a teljes portfólió értéke időnként elérheti a kétezermilliárd dollárt is) folyamatosan 1 százaléknyi részt csalással és piszkos ügyletekkel összefüggő ingatlanpanamák tették ki – állítja *Avivah Litan,* a Gartner piackutató cég elemzési alelnöke. Ebből az is sejthető, hogy csak az USA tízezermilliárd dolláros jelzálogpiacán mekkora csalásokkal összefüggő pénzösszegek forroghatnak. De Litan szerint az amerikai egészségügyben is elcsaltak vagy 60 milliárdot. Ezért azt követeli a Kongresszustól, hogy olyan intézkedéseket léptessen életbe, amelyek alapján széles körben használnák a minták alapján működő hírszerzési szűrőrendszereket (a Palantir éppen ilyen) az illegális tevékenységek visszaszorítására és a nemzetbiztonság javítására. És valóban, nem csak a pénzügyi világban teremtett veszélyes helyzetet az adatszmog, amelyben túl sok információ, túl sok minőségben és alakban jelenik meg, térben és időben túl sok helyen található.

A váratlan összefüggések és a megoldhatatlannak tűnő rejtélyek kulcsai gyakran lényegtelen, zavaró adatok sötét gomolyagai alatt rejtőznek. Ha e füstködből kiszűrhettük volna a releváns információkat, kapcsolatokat, összefüggéseket, tendenciákat talán be sem következtek volna az elmúlt években egész világot megrázó olyan események, mint a 9/11-es Al-Kaida-merénylet, a pénzügyi válság vagy akár a fukushimai atomerőmű katasztrófája.

A dalai láma és az indiai hadügyi tárca esete erre némiképp rávilágít. Tavaly áprilisban egy Palantirt használó torontói egyetemi csapat internetbiztonsági szakemberekkel együttműködve feltárt egy webes kémhálózatot, amely az indiai védelmi minisztériumból titkos dokumentumokat lopott el. De nemcsak ezeket lelték meg a kémszervereken, hanem a dalai láma egész éves személyes levelezését is. „A támadók egyre okosabbak lesznek, és olyan technikákat használnak, amelyek a közösségi médiumokra kapcsolódva megnehezítik, hogy automatizált rendszerekkel elkapják őket" – mondta *Shreyas Vijaykumar,* a Palantir kibercsapatának vezetője a *Forbes* magazinnak.

HONNAN VAN A PALANTIR PÉNZE?

A Palantir Technologiesnak közel 200 millió dollárja lehet fejlesztései folytatásához egy olyan körtől, amelynek sajtóhírek szerint legalább 2,5 milliárd dollárnyi befektetésre váró tőkéje áll készenlétben. A Palantir már négy körben is hatalmas tőkeinjekciókat kapott. Legutóbb két meg nem nevezett New York-i fedezeti alaptól a *Wall Street Journal* szerint 68, más források szerint mintegy 70 vagy 75 millió dollárhoz jutottak, de a korábbi befektetőktől (Peter Thieltől, és a CIA befektetési részlegétől, az In-Q-Teltől) és egyetemi alapítványoktól is van pénzük bőven. A beszámolók szerint kezdetben egy 12 milliós majd egy 50 és 90 milliós csekket is kaptak.

Ma már a cég jelentős mennyiségű bevételre is szert tesz. S annak ellenére, hogy tevékenysége igen keresett a (főleg amerikai) kormányzati ügynökségek (például az FBI) berkeiben, üzleteinek 60 százalékát már a kereskedelmi piacon köti. Olyan óriáscégek vannak ügyfelei körében, mint a JPMorgan Chase vagy a Thomson Reuters pénzügyi információszolgáltató, de az SAP is globális viszonteladói szerződést kötött velük.

A cég tavalyi árbevétele – azok után, hogy az előző két esztendő után harmadszor is sikerült dupláznia – sajtóhírek szerint már elérte a 90 millió dollárt. A cég értékét pedig 735 millió dollárra becsülik, de ez legalább olyan gyorsan emelkedik, mint az árbevétel. Alexander Karp egyenesen arról beszél, hogy öt éven belül a bevételek elérhetik az 1 milliárd dollárt.

A piaci elemzők mindegyike azonban nem ennyire lelkes, s a Palantirban csak egy túlságosan ambiciózus céget látnak, amely nem a szerves fejlődés, hanem a mesterséges felpumpálás útját választotta. A Gartner elemzője, *John Pescatore* viszont arra hívja fel a figyelmet, hogy a „helyzeti tudatosság eszközei", mint amilyen a Palantir csak töredékét teszik ki a biztonsági és titkosszolgálatok költségvetésének, amelyet olyan társaságoknál költenek el, mint a Boeing, a Raytheon és a Lockheed Martin.

E megállapítást igazolja, hogy a *Politico* hírmagazinon keresztül napvilágra került a hadsereg részére 2,7 milliárd dollárért kifejlesztett DCGS-A kódjelű informatikai rendszer blamázsa. Ennek az lett volna a feladata, hogy valós idejű tájékoztatást adjon az Irakban és Afganisztánban harcoló csapatoknak a hírszerzési eredményekről. A lap hírforrása szerint az afganisztáni katonai hírszerzés vezetője, *Michael Flynn* tábornok és kongresszusi képviselők fontolgatták, hogy más megoldást keresnek a használhatatlan rendszer helyett. A DCGS-A egy felhőalapú hálózat, amelyet az információk számos forrásból való összegyűjtésére, valós idejű feldolgozására és szétosztására terveztek a harctéri parancsnokok támogatására. Ha például a parancsnoknak meg kell találnia egy gerillavezért, a rendszer a beszámolók alapján azonosítja a gerilla helyzetét, s térképen prezentálja a legegyszerűbb becserkészési útvonalat. De a DCGS-A-nak még az egyszerű elemzési feladatokkal is gondjai voltak. Az elégedetlenség híre egészen a washingtoni törvényhozásig jutott, ahol a szenátus hírszerzési bizottsága szerette volna elérni, hogy a hadsereg fontolja meg a Palantir használatát, amely az FBI és a CIA berkeiben jól segítette terroristák felkutatását. A hadsereg végül mégsem dobta ki a régi beszállítói által fejlesztett rendszert.

MI AZ A PALANTIR?

J. R. R. Tolkien fantasy eposzában, a *Gyűrűk Urában* hívták palantirnak a távolba látó mágikus kristálygömböket. A való világban viszont egy Java-alapú elemzésre, integrációra és adatok megjelenítésére szolgáló szoftver. A rendszer erőteljes háttér-adatbázist és szerverarchitektúrát kombinál az intuitív felhasználói felülettel. A Palantirnak két alplatformja van, a Palantir Finance (a vállalatok számára) és a Palantir Government (kormányzati célokra), amelyek felölelik a teljes elemzési spektrumot az adatintegrációtól a keresésig és felfedezésig, az ismeretmenedzsmentig, az együttműködésig és az emberi szabadságjogok védelméig. A platformok természetüknél fogva sokféle adat kezelését támogatják, így a strukturált, strukturálatlan, relációs, átmeneti és térinformatikai adatokat.
A Palantir tulajdonképpen egy hírszerzési infrastruktúra, amely nagy szervezetek, vállalatok valós idejű adatelemzését teszi lehetővé a biztonságra, a skálázhatóságra, az egyszerű használatra és az együttműködésre fókuszálva.
A Palantirt az adatokban gazdag környezetben lehet igazán hatékonyan használni. Például egy kereskedelmi bankban, ahol az adatok megértése és információvá változtatása kulcskérdés a cég sikeres működésében. Ráadásul nemcsak speciálisan kiképzett technikai személyzet használhatja, hanem a szervezet bármely területén lévő szakemberek is elsajátíthatják a számukra szükséges eszközeinek kezelését.

SZILÁGYI SZABOLCS

WLAN-MENEDZSMENT

Szolgáltatások a felhőben

Kiszervezhető-e a vállalati szintű vezetékmentes hálózati felügyelet a felhőbe? És ha igen, milyen feltételek mellett? Cikkünk ezekre a kérdésekre keresi a választ.

> Nem meglepő, ha egyre többen kínálnak felhőre alapuló vezetékmentes hálózatmenedzsment-szolgáltatásokat.

Ugyan már az elmúlt évtized derekán is voltak felhőszerű szolgáltatások (gondoljunk csak a Gmailre), napjainkra valóban kiteljesedni látszik a folyamat. Gyakorlatilag nem létezik olyan IT-szolgáltatás, amit ne lehetne software-as-a-service (SaaS) módon elérni; így többek között WLAN-menedzsmentre is lehetőség van. Érthető ugyanakkor az ezzel szembeni ellenérzés, hiszen a hálózatkezelés mindig is kritikus pontja volt az IT-rendszerek működésének. Cikkünkben megvizsgáljuk, mit nyerhetünk a feladat felhőbe való kihelyezésével, és ennek milyen ára van. A nyilvánvaló feltételezések szerint csökkenni fog a rendszer működési költsége, a hatékonyság javul, és úgy bővülhet az elérhető funkciók köre, hogy az nem von maga után jelentős befektetési költséget.

A vezetékmentes helyi hálózat kezelését számos, az IT-piacon érdekelt szereplő tartotta annyira érdekesnek, hogy saját szolgáltatásokat kínáljon; ilyen például a D-Link CloudCommand, az Aerohive Networks HiveManager és a Meraki Cloud Controller. A nagy kérdés az, hogy mi a különbség a hagyományos és a felhőalapú WLAN-menedzsment rendszerek között; amire választ az említett szolgáltatások elemzésével kaphatunk. Ehhez azonban először nézzük meg a hagyományos megoldást!

A vállalati szintű WLAN-kezelési funkciók tradicionálisan egy WLAN-vezérlőbe, egy különálló applianceba vagy egy szerverbe integráltan érhetők el – néha ezek kombinációjában. A kis és közepes szintű üzleti termékek firmware-je általában hozzáférési pontonként állítható, secure-HTTP felületen keresztül. Ahhoz, hogy ez a feladat hatékonyan legyen elvégezhető egy központosított menedzsmentkonzol révén, a teljes hálózaton keresztül elérhetőnek kell lennie az ehhez szükséges összes funkciónak, függetlenül az adott hálózat méretétől, (de)centralizáltságától.

KÖNNYEBB, MINT GONDOLNÁ

Közel sem olyan nehéz feladat ezt a szolgáltatást a felhőbe mozgatni, mint amilyennek elsőre tűnik. A helyi szinten alkalmazott hardver megszűnése ugyanis – a kezelés szempontjából nézve – egyáltalán nem okoz olyan nagy megrázkódtatást.

A modern rendszerek már évek óta böngészőalapú elérést kínálnak, amelynél – legalábbis a hozzáférés és az interfész kezelését illetően – teljesen lényegtelen, hogy egy pár tíz, száz méterre levő hardvert vagy a felhőben működő vezérlőt érjük el.

A Network Worldon pár hónapja megjelent vizsgálat szerint a nagy rendszerek közötti funkcionalitásbeli különbség mértéke elhanyagolható. Mindegyik „kézen fogva” vezeti a felhasználót a beállítás során, így a felhőszolgáltatások tekintetében kezdő rendszergazdák is relatíve könnyen konfigurálhatják a WLAN-kezelést. Azaz csupán a képességekre alapozva kijelenthető, hogy a vezetékmentes hálózatok menedzselése ugyanolyan jól – illetve az extra képességeknek köszönhetően még részletesebben – végezhető, mintha különálló hardvert alkalmaznánk.

Ennek természetesen ára van, havonta jelentkező költség képében. Éves szinten hozzáférési pontonként 95–150 dollárért kínálják a lehetőséget a nagy vendorok; természetesen az ár növekedésével egyre nagyobbá válnak az egyes szolgáltatások közötti különbségek. Ugyanakkor alapképességeik megegyeznek: hozzáférési pontok hozzáadása és konfigurálása, kivételkezelés és jelentéskészítés könnyen és gyorsan végezhető általuk, mindez úgy, hogy közben a felhő láthatatlan marad (eltekintve attól az esettől, ha hálózati hiba miatt elérhetetlenné válik a WLAN-kezelés – erre később még kitérünk). Emellett – bár ez nyilván függ az adott internetkapcsolat sebességétől is – a vezérlők elérése és reagálókészsége sem hagy kívánnivalót maga után, semmivel sem lassabb a művelet annál, mintha a felügyelet alatt álló hálózatba helyezett szerveren keresztül zajlana a konfigurálás.

AGGÁLYOK...

Sokakban, elsősorban az idősebbekben él a félelem a felhő kapcsán a 80-as, 90-es évek mainframeekből és terminálokból álló hálózataihoz való visszatéréstől. Azt azonban nem szabad elfelejteni, hogy azokban az évtizedekben még igen fejletlen volt a hálózati infrastruktúra, ami sokat rontott a felhőalapú rendszerek előfutárainak is tekinthető IT-networkök használhatóságán. És nem csupán a hálózatok, a szerverek és a rajtuk

futó alkalmazások is lendületes fejlődésen estek át az elmúlt két évtizedben. Vagyis a terminálrendszerek eredeti formájukban való visszatérésére nem kell számítani – az infrastruktúra észrevétlenül alakulhat át, jelentős rész kerülhet a felhőbe.

A felhőre való áttérés tehát sokkal inkább a képességeken – költséghatékonyan, megbízhatóan és helyfüggetlenül használható szolgáltatásokon – múlik, nem pedig hardveres szempontból kell megközelíteni a kérdést. A WLAN felhőalapú menedzselésekor felmerülő aggályok rávilágítanak a cloud computinggal szemben álló alapvető ellenérzések létére, ugyanakkor nemcsak választ adnak rá, hanem jól bemutatják azt is, miért érdemes váltani. A beruházási és működési költségek csökkentése anélkül vihető végbe, hogy ehhez fel kellene áldozni valamit a funkcionalitás oldalán. Természetesen a migrálást minden egyes esetben alapos költségbecslési tervezésnek kell megelőlegeznie, de az előbbiekben ismertetett árakból kiindulva a legtöbb szervezet számára – pusztán anyagi szempontokat szem előtt tartva – érdemes megfontolni a váltást.

Látható tehát, hogy a felhőre való áttérés legnagyobb kihívása nem is költségoldalról jelentkezik, hanem, amint arról már szó volt, a folyamatos hozzáférés megszűnésének bekövetkeztétől adódik a legelemibb félelem. Mi történik akkor, ha megszakad az internetkapcsolat, vagy az internetszolgáltató, illetve a menedzselt szolgáltatást kínáló kénytelen elszenvedni egy szolgáltatáskiesést? Ez a probléma azonban sokkal inkább túlmutat a WLAN-kezelés kihívásain. Ha a felhő és az abban hostolt szolgáltatások elérhetetlenné válnak, akkor az adott gazdálkodó szervezetnek nagyobb problémái is akadnak, mint a vezetékmentes hálózat konfigurálása. Ez ugyanis azzal jár, hogy minden, a felhőbe telepített funkcionalitás – adatokhoz való hozzáférés, szolgáltatások futtatása stb. – ideiglenesen megszűnik.

Ezt a kihívást azonban nem a WLAN-menedzselés, hanem az üzletfolytonossági tervezés és az IT működtetésére kidolgozott eljárások szintjén kell kezelni. Ebből következően, ha az utóbbiak tekintetében felkészült a vállalat, a vezetékmentes hálózat kezelésének pillanatnyi elérhetetlensége sem fog komoly megrázkódtatást okozni.

...ÉS MEGOLDÁSOK

Természetesen a megoldásban is partnernek bizonyulnak a vendorok. Vizsgálata során a Network World megkérdezte a felmérésben részt vevő cégeket azok hibatűréséről, például arról, mennyire elosztott rendszerben dolgoznak ahhoz, hogy egy tetszőleges hálózati hiba – beleértve egy földrengést is, de eltekintve az ügyféloldali problémáktól – ne befolyásolja a szolgáltatás működését. Mindannyiuktól pozitív választ kapott. A D-Link például arról számolt be, hogy CloudCommand szolgáltatása az Amazon EC2 cloudjában működik, ami az egyik legnagyobb a maga nemében. Természetesen nem lehet elhallgatni, hogy az EC2 nemrég átesett egy kisebb kimaradáson, de a WLAN-menedzsmentet tekintve ennek a szolgáltatást igénybe vevő vállalatok üzletmenetére gyakorolt hatása a nullához konvergált.

Nem meglepő tehát, hogy egyre többen kínálnak felhőre alapuló vezetékmentes hálózatmenedzsment-szolgáltatásokat. Az AirTight például nemrég jelentette be szolgáltatásának biztonsági kiterjesztéseit, a WaveLink Avalanche platformja is a közelmúltban kapott felhőalapú, kifejezetten a mobileszközök kezelését célzó változatot (illetve azt is elárulta, hogy hamarosan cloudos WLAN-menedzsment képességekkel is elő fog rukkolni). De hazai példát is hozhatunk: a szeptember végén tartott ITBN 2011 egyik előadója az a *Nemes Dániel* volt, aki a Biztributor képviseletében beszélt a WLAN biztonsági kérdéseiről és a következő generációs hálózati architektúrákról. A téma tehát hazánkban is érdeklődésre tart számot. *(Az igazgató előadását lásd videónkon: **computerworld.hu/cikk/wlan-biztonsag**.)*

Érdekes látni ugyanakkor, hogy a mobilkörnyezet felügyeletére szánt felhőmegoldások megjelennek a vezetékes hálózat kapcsán is. A LAN-menedzsment cloudba való átültetésére mutat példát a Meraki Systems Manager szolgáltatása, amellyel az IT-menedzsment funkciók jelentős része vagy akár teljes egésze kiterjeszthető a felhőre. Ebben az esetben pedig már tényleg mindegy, hogy a rendszert felügyelő adminisztrátor a szerverközpontban, az irodában vagy bárhol máshol látja el feladatát – amíg a felhőhöz való kapcsolódása biztonságosan zajlik.

Felhőrepertoár

Idehaza is egyre nagyobb kínálatból választhatnak azok a vállalkozások, amelyek valamilyen felhőalapú szolgáltatást szeretnének igénybe venni. Cikkünkben néhány Magyarországon működő cég cloudos szolgáltatásának bemutatásával próbálunk rávilágítani a lehetőségekre.

Miközben a cloud egyik nagy előnye, hogy az ügyfeleknek nem kell nagyobb beruházásba vágniuk, az új, felhőszolgáltatások elindításához a szolgáltatóknak jelentős beruházásokat kell végrehajtaniuk.”

SZALAY DÁNIEL

A két közismert nemzetközi brand, a Google és az Amazon mellett ma már jó néhány hazai szolgáltatás közül is választhatnak azok az ügyfelek, akik részben vagy egészben a felhőbe helyeznék át különböző vállalati szolgáltatásaikat. CRM, dokumentum-központú integrált vállalatirányítási rendszer, dokumentumalapú projektkövetés, kiszervezhető iktatási szolgáltatás, naptár és kontaktkezelés (PIM), voice center, fax to e-mail, e-mail, tömeges SMS, valóságos vagy virtuális szerverbérletek, szerverarchiválás, online konferencia, csoportmunka-támogatás közös tárterülettel – csak néhány szolgáltatás a példa kedvéért, amit ma már a magyarországi vállalkozások és szervezetek is áthelyezhetnek a felhőbe, ezáltal mentesítve önmagukat egy nagyobb beruházástól és a folyamatos üzemeltetéssel kapcsolatos nyűgöktől, valamint élvezhetik az online kollaboráció adta előnyöket, amelyekről többször is írtunk már lapunkban *(l. Computerworld 2011/41. sz. Tapasztalatok a felhőből)*.

Miközben a cloud egyik nagy előnye, hogy az ügyfeleknek nem kell nagyobb beruházásba vágniuk, az új felhőszolgáltatások elindításához maguknak a szolgáltatóknak jelentős beruházásokat kell(ett) végrehajtaniuk. Kérdés, hogy ezek az invesztíciók mikorra térülhetnek meg. Cikkünkben a WireCorner, a Magyar Telekom és az ElastOffice szolgáltatásait mutatjuk be, de szó esik arról is, hogy milyen cloudos szolgáltatásokkal készül a piac meghódítására a mostanáig inkább csak adatbiztonsági, adatmentő tevékenységéről ismert Kürt.

WIRECORNER

Elsőként a WireCorner céget kérdeztük arról, mekkora beruházást hajtottak végre a cloudszolgáltatás elindítása érdekében, illetve miből adódtak legjelentősebb költségeik. Közel 100 millió forintos beruházást hajtottak végre a cloud infrastruktúra kialakítására. Ennek legnagyobb részét a kiszolgáló szerverek storage és hardveres tűzfal eszközeinek beszerzése tette ki, de jelentős tétel volt a szerverek operációs rendszereinek, a virtualizációs, a tűzfal, a mentési és vírusfigyelő szoftverek licence is. A WireCornernél jelenleg 60 nagy teljesítményű fizikai szerver biztosítja a kiszolgálói hátteret. További költség az infrastruktúra kiépítése mellett az eszközök konfigurálása, illetve az üzemeltetés munka- és egyéb költségei (áram, hűtés, kommunikáció, karbantartás, javítás); ezenfelül természetesen az üzleti tervekben a marketing- és PR-költségekkel is kalkulálni kellett. Számításaik szerint megtérülési mutatójuk körülbelül 3500 felhasználónál fordulhat pozitív irányba.

Cloudszolgáltatását a levelezéstől a CRM-en át az előre konfigurált ERP-ig SkyPort néven kínálja a cég. Ez nem sablonmegoldás, mivel maximálisan testre szabható és rugalmasan változtatható. A WireCorner hostingban a testre szabott rendszereket egyedi megoldásként felhőből üzemeltetve, a hibrid vagy hagyományos módú üzemeltetésig kínálja, beleértve a desktop virtualizációt is. A SkyPort szervererőforrás kapacitásbérlést is tartalmaz. A WireCorner az üzleti folyamatok irányából közelítette meg a szolgáltatás csomagelemeinek kialakítását. Ennek megfelelően levelezés- és csoportmunka-támogatás, valamint különféle kereskedelmi, gazdasági és logisztikai folyamatok működtetésének transzparenssé tételét, támogatását elősegítő szabványos rendszerekből képeztek csomagokat.

A szolgáltatás egyes komponensei más-más funkcionalitást takarnak, ezért az árat intervallumban tudják meghatározni, ami általában nettó 3200–20 000 forint közé esik havonta és felhasználónként. Komplett vállalatirányítási rendszercsomagot kínálnak havi 42 000–63 000 Ft-ért felhasználónként, ami már tartalmazza a bevezetés költségeit is. Az árakat egyértelműen az befolyásolja, hogy a rugalmasan összeállítható felhasználói csomagok milyen alkalmazásokat, illetve milyen háttérkapacitásokat foglalnak magunkban. Azoknak éri meg igénybe venni a szolgáltatást, akik beruházás helyett ha-

vi költséget szeretnének elszámolni, le akarják venni saját vállukról a szerverek és szoftverek tulajdonlásának, karbantartásának és üzemeltetésének minden költségét és nyűgét. Regisztrációs díj nincs. Az egyes üzleti rendszerek testre szabási, bevezetési díjainak fizetési ütemezését az ügyfél döntheti el: lehet egy összegben, vagy pedig rákerülhet a havi előfizetési díjra.

Kérdésünkre, hogy ki áll a cég mögött, és ki szavatolja, hogy egy esetleges csőd vagy más problémák esetén az adataikhoz az ügyfelek továbbra is hozzáférhetnek, azt a választ kaptuk, hogy a WireCorner 100 százalékban magyar tulajdonban áll, szerverparkja Budapesten található két adatközpontban: az egyik az Invitel, a másik az Opticon datacentere, amelyek a legmagasabb szintű katasztrófa, adatbiztonsági és környezetvédelmi minősítésekkel rendelkeznek. Az adatokat redundánsan (több szerveren és két helyszínen) tárolják, valamint napi ütemezett mentést készítenek, ügyféligény szerint akár naponta többször is. „Az ügyfél igényei alapján külső adattárolóra is exportáljuk az adatokat, amelyeket időről időre meg is kap a megrendelő – ezt a standard mentéseinken felül adjuk. A mentések egy vis maior esetén nélkülünk is hozzáférhetők" – mondták a cégnél. A vállalat működése stabil, a cégcsoportot nagyon tudatos, nyugati nagyvállalati standardok alapján folytatott gazdálkodással működtetik, és a tavalyi évben 2,2 milliárd forintos árbevételt értek el, idén pedig már november elején átlépték a 2,1 milliárd forintot. A SkyPort cloudszolgáltatást bemutató honlapon (**www.skyport.hu**) legnagyobb referenciaként a cég Pécel Önkormányzatát emelte ki. A Pest megyei város azért jó példa, mert a meglehetősen elavult IT-környezet frissítése csak hosszabb és költségesebb folyamat árán valósulhatott volna meg, ha nincs a cloud.

MAGYAR TELEKOM

Az egykori Matáv, azaz a mai Magyar Telekom cégcsoport nemcsak internet- és telefon-előfizetést kínál havidíjas alapon, hanem irodai informatikai eszközöket és szolgáltatásokat is, és ezek között szép számban vannak cloudos megoldások. Ilyen az idehaza egyedülállónak számító Virtualoso VoiceCenter menedzselt callcenter-szolgáltatás, amelylyel intelligens IVR-szolgáltatásokhoz juthatnak a vállalkozók anélkül, hogy drága telefonközpontot kellene vásárolniuk, ráadásul olyan mögöttes IT-háttértámogatást kaphatnak hozzá a Telekomtól, mint például a 7×24 órás rendszerfelügyelet, amit a kkv-k többsége valószínűleg nem tudna megfizetni, ha saját alközpontot üzemeltetne. A vállalkozók egy weboldalon keresztül tudják telefonos menürendszerüket kialakítani, a különféle beállításokat elvégezni, a rögzített hívásokat visszahallgatni, az eligazító szövegeket felmondani stb. Mindez havi 2900 forinttól indul, de egy 10 fős cég esetében is kihozható körülbelül havi 6–10 ezer forintból a teljes cégre, nem számolva a meglévő mobil és vezetékes előfizetések havidíjával, amelyekre ráteszik ezt az értéknövelt szolgáltatást.

A Virtualoso persze nem csak a VoiceCenterből áll. Az **uzletitelekom.hu**-n megtalálható a teljes szolgáltatási paletta. Nagyon hasznos lehet többek között a fax2 e-mail szolgáltatás kb. havi 2 ezer forintért. Ennek előnye, hogy a vállalkozók megspórolhatják egy faxkészülék beszerzését és a faxüzenetek papír nélkül érhetnek célba, az adatok digitálisan archiválhatók.

A kérdésre, hogy mekkora beruházásra volt szüksége a német Deutsche Telekom többségi tulajdonában lévő MTelekomnak a cloud infrastruktúrájának kiépítéséhez, nem egyszerű válaszolni. A cégnek korábban is létezett szerverbérlet szolgáltatása, illetve adatközpontja, ami önmagában véve is több százmillió forintos tétel, vagyis a cloud bevezetésekor így már nem teljesen nulláról kellett az új szolgáltatási infrastruktúrát kiépíteni. A Virtualoso cloud infrastruktúrájának kiépítése számítások szerint 10 ezer felhasználónál térülhet meg, mivel nagyságrendje több százmillió forint volt.

A Virtualoso-előfizetők száma nemrég meghaladta már a 3000-et is, emiatt a cloudos infrastruktúra kinőtte a Telekom Petőfi Sándor utcai géptermét, és mindent átköltöztettek a maga 14 400 négyzetméterével Kelet-Közép-Európa legnagyobb géptermének számító, szuperbiztonságos DataPlex adatközpontba. Pedig az üzleti szolgáltatások elindítása eleinte döcögősen ment, mert az ügyfeleknek nehéz egyszerűen elmagyarázni ezeknek a teljesen új típusú szolgáltatásoknak a működését. Itt egészen másfajta kommunikációra van szükség, mint egy mobiltelefon-előfizetés vagy egy internetszolgáltatás értékesítésekor. Mostanra azonban a Telekom megtalálta a hatásosabb módját a kommunikációnak, ráadásul optimálisabban ki tudják használni a cégcsoporton belüli szinergiákat is.

ELASTOFFICE

Dokumentum-központú integrált vállalatirányítási rendszert kínál az ElastOffice Magyarország Cloud9 szolgáltatása. Ezt a cég privát cloudból vagy az ügyfél saját szerverein futó felhő felhasználásával is biztosítja. A cég felhős szolgáltatásai között dokumentumalapú projektkövetést, kiszervezhető iktatási szolgáltatást, naptár és kontaktkezelést is találunk. Ami a költségeket illeti, a cég vezetője, *Taivainen Krisztián* lapunknak elmondta: egy irodai adminisztratív munkatárs induló költsége mintegy 250 ezer forint, és ennek feléért már egy körülbelül 20 fős vállalkozás teljes vállalatirányítási szolgáltatásainak folyamatos üzemeltetése és dokumentumainak adattárolása elérhető az ElastOffice Magyarország Kft.-nél. A Cloud9 rendszert egy előzetes (fizetett) felmérés alapján az ügyfél igényeire és üzletmenetére szabják, ami a havi üzemeltetési költségen kívül a rendszerindítás részeként fizetendő. A rendszerre egyébként modularitás jellemző, vagyis szinte észrevétlenül, az ügyfél megszokott üzletmenetének megzavarása nélkül vezethető be.

A Cloud9 teljes egészében a cég saját fejlesztése, és az elmúlt 5 évben közel 10 millió eurót fordítottak az induló infrastruktúra beruházására. Az üzleti tervek szerint mintegy ezer közepes méretű vállalat folyamatos kiszolgálása biztosíthatja a megfelelő cash flow-t, megtérülést és a folyamatos szolgáltatás bővítéséhez szükséges újabb forrásokat. Géptermeket egyébként az ElastOffice nem vásárolt, helyette a rendszer üzemeltetéséhez nagy megbízhatóságú, minősített datacenterek szolgáltatását veszi igénybe. A vállalat ügyfelei (saját igényeiktől függően) dönthetnek, hogy adataikat svájci, németországi, magyarországi, romániai és USA-beli szerverparkokban kívánják-e tárolni, feldolgozni, sőt igény esetén bármikor bevonhatók új datacenterek is az ElastOffice (**www.elastoffice.com**) szolgáltatásaiba. A cloudban tárolt adatok folyamatos mentését és a mentéseknek független szolgáltató(k)nál történő úgynevezett „biztonsági letétjét" is vállalja az ElastOffice (külön díjazás ellenében), így a nem várt események bekövetkezte esetén az adatok egy hagyományos IT-infrastruktúrába való áthelyezése gyorsan megvalósítható. Az adatmentéseknek harmadik félnél való megőrzésén kívül a cég felelősségbiztosítása is védi az ügyfeleket. Az ElastOffice Magyarország egyébként a svájci ElastOffice AG tulajdonában áll. Az anyavállalat tulajdonosai magánbefektetők, akik annyira bíznak a cloudalapú szolgáltatások sikerében, hogy a cégcsoportot akár már 1-2 éven belül a tőzsdére vinnék. Meglátjuk, álmuk végül valóra válik-e...

> Az infrastruktúra kiépítése mellett az eszközök konfigurálása, illetve az üzemeltetési munka- és egyebek költségei mellett az üzleti tervekben a marketing- és PR-költségekkel is kalkulálni kell.

KÜRT

Legutóbb már az adatbiztonsággal foglalkozó Kürt is új sebességbe kapcsolt a cloud irányába tartó úton. Egy minap tartott sajtótájékoztatón arról beszéltek a cég vezetői, hogy az iparági trendeket, valamint saját ügyfelei révén szerzett tapasztalatait alapul véve, a vállalat (uniós pályázati források felhasználásával) olyan projektet indított, amely a hazai vállalatok cloudfelhasználási lehetőségeit és a ma még nem ismert biztonsági kockázatait, megoldási alternatíváit vizsgálja. A projektben a vállalat fejlesztői olyan cloud infrastruktúrára alapozott megoldások fejlesztésén dolgoznak, mint például a fejlesztői labor biztonságos felhőben, amelynek keretében a különböző intézmények saját belső fejlesztéseikhez erőforrást bérelhetnek a Kürt által üzemeltetett biztonságos felhő-infrastruktúrán. Ezenkívül dolgoznak egy biztonsági felhőben lévő üzemeltetési tesztlabor-szolgáltatás beindításán is, amelynek keretében az ügyfél saját fejlesztésű alkalmazásait telepítheti a cég cloud környezetébe, ahol lehetőség nyílik egy termék teljes tesztelésére. Lenne továbbá egy alkalmazássérülékenység-vizsgáló labor is, ahol a szakemberek a sérülékenységvizsgálatot az ügyfél által a felhőbe telepített, emulált rendszeren végeznék.

PIACELEMZÉS

Felhősödés a szolgáltatáspiac egén

A hazai vállalatok a felhőben is a testre szabott megoldásokat keresik, ami versenyelőnyt ad a helyi viszonyokat ismerő szolgáltatóknak. A lehetőséget felismerve több magyar szoftvercég is arra készül, hogy jövőre felhőalapú megoldásokat jelent be – fejlesztéseik azonban már az idén hozzájárulnak a piac két számjegyű növekedéséhez.

Tavaly óta külön is méri a cloudszolgáltatások piacát Magyarországon az International Data Corporation (IDC); azt megelőzően regionális szintű, összesített adatokon keresztül jelenítette meg ezt a szegmenst a hostingpiacról készített elemzésében.

A co-location, a hosting és a cloudszolgáltatások közös vonása a megosztott infrastruktúra. A co-location szolgáltatások esetében ez elsősorban az adatközpont épületét jelenti, a hosting, majd a cloudszolgáltatások felé haladva azonban a megosztott infrastruktúra-elemek köre jelentősen bővül. Az infrastruktúrahosting-szolgáltatók például megosztott monitorozó és felügyeleti rendszert használnak, az alkalmazáshosting esetében már a szerverkörnyezet is megosztott lehet.

– A felhőszolgáltatásokat ezért nem különböztethetjük meg pusztán annak alapján, hogy virtualizált infrastruktúrán futnak, ez ma már a hostingszolgáltatásokra is jellemző – mutatott rá *Balicza Gábor,* az IDC Hungary elemzője. – A cloudszolgáltatások esetében is alapvető kritérium, hogy megosztott környezetben, virtualizált infrastruktúrán, interneten keresztül elérhető szolgáltatásról legyen szó. Önkiszolgáló jellegüknél és a használatalapú díjszámításnál fogva azonban markánsan eltérnek a többi szolgáltatástól. A felhőszolgáltatásokat a felhasználók egy portálon keresztül önállóan választhatják ki és vehetik használatba, operátori közreműködés nélkül. Ehhez magas fokú automatizálás szükséges a szolgáltató adatközpontjában, a virtualizált és szabványosított szerverkörnyezetet és azt a rendszert is beleértve, amely követi, hogy egy-egy felhasználó milyen erőforrásokat igényelt, és azokat meddig használta.

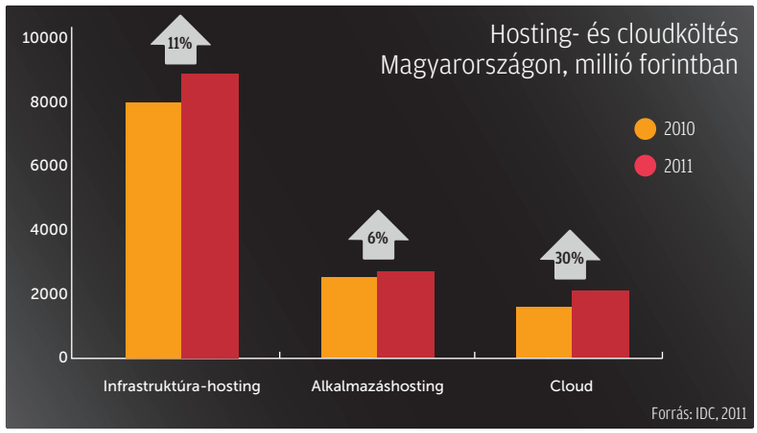
A nyilvános felhőszolgáltatások további sajátossága, hogy dobozos, kevéssé testre szabható alkalmazásokra épülnek. Magánfelhő környezetben egyedi alkalmazások felhősítésére is sor kerülhet, de a felhasználók ezeket is szabványosított szolgáltatáscsomagok formájában érik el.

IMPLEMENTÁCIÓ ÉS ÜZEMELTETÉS

Az így meghatározott felhőszolgáltatások piacát az IDC elemzése is két szegmensre, nyilvános és magánfelhő szolgáltatásokra osztja, utóbbiak vállalaton belüli vagy külső szolgáltató által adott, mások számára nem hozzáférhető szolgáltatásokat jelölnek. A piacelemző mindkét kategóriában felhőimplementációs és felhőüzemeltetési szolgáltatások alapján méri a piaci szereplők bevételeit. Az implementációs szolgáltatások a nyilvános vagy magánfelhő környezetek kialakítására irányuló, projekt jellegű szolgáltatások, míg a havidíjas vagy más konstrukcióban elszámolt, szűkebb értelemben vett felhőszolgáltatás számít üzemeltetésnek.

– Ennek alapján a magyar felhőpiac mérete 2010-ben 1,6 milliárd forint volt – mondta Balicza Gábor. – Összehasonlításképp ugyanebben az időszakban a teljes hostingpiac 10,5 milliárd forintot tett ki Magyarországon. A felhőpiac 65 százalékát a nyilvános felhőszolgáltatások adták. Ezenbelül a szolgáltatói bevételek 85 százaléka üzemeltetésből származott, ami a kínálati oldal összetételével magyarázható. A hazai piacon jelen levő legnagyobb felhőszolgáltatók többsége nemzetközi cég, mint például a saleforce.com. Ezek a szereplők nem magyarországi adatközpontokból szolgáltatnak, így a beruházásaikhoz kötött, felhőimplementációs bevételek is más országokban jelentkeznek. Az olyan hazai felhőszolgáltatók pedig, mint az ugyancsak a TOP10-es listán szereplő CEOD, már korábban, 2008-ban megvalósították legnagyobb adatközpont-beruházásaikat.

– Bár a nemzetközi jelenlét sok tekintetben előnyös egy felhőszolgáltató számára, a dolog azért nem ilyen egyszerű – tette hozzá Balicza Gábor. – A minél nagyobb méret eléréséhez a globális piaci szereplők szigorúan szabványosítják szolgáltatásaikat, ugyanakkor kevésbé



A magánfelhő szolgáltatások esetében kissé árnyaltabb a kép. Egyrészt ebben a szegmensben is jelen vannak a nagy, nemzetközi adatközpontokkal rendelkező szereplők, mint például az IBM, amelyek nem helyben alakítják ki a szolgáltatáshoz szükséges infrastruktúrát. A hazai szolgáltatók némelyike pedig, ahogyan azt az NK Services is teszi, a felhőszolgáltatás üzemeltetési díjába építi be az implementációs költségeket, így azok nem jelennek meg külön mérhető módon.

TESTRE SZABOTT FELHŐ

A 2010-es adatok alapján a magyar piacon jelen levő felhőszolgáltatók száma 20 alatt maradt. A nemzetközi szereplők piacra lépését egy-egy országban rendkívüli módon megkönnyíti maga a technológia, mivel a felhőszolgáltatások az interneten keresztül a világ bármely pontján elérhetők. Ehhez csupán a rugalmas méretezhetőséget kell biztosítani, ami egy virtualizált adatközpontban napi rutinnak számít. A helyi infrastruktúra kiépítése így nem hátráltatja megjelenésüket, és piaci ismertségük is megkönnyíti számukra az új szolgáltatások bevezetését.

nyílik lehetőségük arra, hogy részletesen megismerjék egy-egy piac helyi sajátosságait. A közép-kelet-európai régióban, és ezen belül Magyarországon viszont a felhasználók elvárják, hogy technológiai partnerük közel álljon hozzájuk, és a felhőben is testre szabott megoldásokat adjon speciális igényeikre. A Microsoft ezt azzal hidalja át, hogy felhőszolgáltatásait magyar partnerein keresztül értékesíti, a felhasználók szemléletmódja azonban kétségtelenül nagy üzleti lehetőséget teremt a hazai felhőszolgáltatók számára.

Mint arról korábban beszámoltunk, több magyar cég is arra készül, hogy jövőre felhőalapú megoldásokkal lép piacra. Az IDC szerint ezek a fejlesztések a felhőimplementációs szolgáltatásokból származó bevételek növekedését fogják hozni 2011-ben, jövőre pedig a felhőüzemeltetési szolgáltatások terén is a piac bővülését eredményezhetik. A piacelemző arra számít, hogy a felhőszolgáltatások hazai piaca idén 30 százalékkal, 2012-ben további 32 százalékkal fog bővülni. Középtávon várhatóan a magánfelhő szolgáltatások is nagyobb teret nyernek majd a jelenleg túlsúlyban levő nyilvános felhőszolgáltatások mellett.

KIS ENDRE

A mellékletet hirdetőink támogatták.
Elkészítésében közreműködtek:
Mallász Judit szerkesztő, **Sz. Erdős Judit** olvasószerkesztő
Berényi István tördelőszerkesztő
Felelős kiadó: Bíró István, az IDG Magyarországi Médiaszolgáltató Kft. ügyvezetője

A hálózat: stratégiai fegyver

A hálózatok egyre inkább stratégiai eszköznek számítanak. A 14. Cisco Expo szlogenje – *Hálózatok újratöltve* – kettős üzenetet hordoz. Egyrészt azt, hogy egyre többféle módon és egyre több célra lehet adatokat „tölteni" a hálózatba, másrészt azt, hogy a hálózatok mindinkább egyfajta stratégiai fegyverként szolgálhatnak a vállalatok számára; nélkülük hátrányba kerülhetnek a versenyben.

Bár a gazdasági környezet nagyon nehéz, hiba csak rövid távon gondolkozni, hiszen a cégek nagy része évek múlva is a piacon lesz és versenyezni fog. Ha egy cégvezető hálózatokat érintő döntéséről már ma sejthető, hogy közép- és hosszú távon költségnövekedést eredményez, akkor nem történik más, mint a versenyhátrány bebetonozása. Bár egyes esetekben lehet létjogosultsága egy olcsó, taktikai jelleggel kiépített hálózatnak, azonban folyamatos működtetése, bővítése és az új üzleti kihívásoknak való megfelelés hiánya hosszú távon akadályt jelent az üzleti szervezetek számára – mutatott rá *György László,* a Cisco Magyarország ügyvezető igazgatója.

Tény, hogy a technológia adott az üzletet legjobban támogató hálózatok kialakításához. Az igazi feladat az optimális megoldást kínáló kombináció megtalálása. Lehet, hogy pusztán informatikai fejlesztésre van szükség, de előfordulhat, hogy az üzleti folyamatokat kell az informatika adta lehetőségekhez igazítani. Ez utóbbihoz innovációs szemléletre és sokszor a céges kultúra felülvizsgálatára van szükség. Például arra, hogy a vállalat felülvizsgálja a tárgyak, az eszközök és adatok fizikai birtoklásáról alkotott képét, és ezzel megnyissa az utat a virtualizációval elérhető hatékonyság előtt, legyen szó akár adatközpontokról, akár munkaállomásokról.

Napjaink kulcsfontosságú trendjei a virtualizáció és a cloud computing felé mutatnak. Mindez természetesen csak biztonságos, megfelelő szolgáltatási szintű, egyszerűen menedzselhető, energiahatékony, a mai kor igényeihez igazodó üzleti modellek szerint működő hálózatokkal képzelhető el. A közös pont, a kapocs tehát a hálózat.

Mindezt számos adat támasztja alá a közeljövő hálózati trendjeiről: 2013-ra a világ internetforgalmának 91 százaléka videó lesz; a munkavállalók 60 százaléka már ma úgy véli, hogy a hatékony és eredményes munkavégzéshez nem szükséges az irodában lenni; a nagyvállalatok éves bevételeik 3,6 százalékát veszítik el a hálózatos leállások miatt; tízből nyolc informatikai vezető 3 éven belül felhőszolgáltatások igénybevételét tervezi; 2014-re a nagyvállalatok alkalmazottainak 20 százaléka virtuális munkaállomásokat fog használni. ■

PARTNERI KAPCSOLATOK

Idén először a Kapsch is képviselteti magát kiállítóként a Cisco Expón. A cég szeretné az eddig megszerzett Cisco-kompetenciáit tovább erősíteni. – A partneri kapcsolatok szorosabbra fűzésének egyik fontos mérföldköve a Cisco Expón való részvétel – fogalmazott *Fülöp István,* a Kapsch Kft. ügyvezető igazgatója.

A cloud mint közmű jellegű szolgáltatás

Még csak néhány hónapja vezeti *Jutasi Zoltán* vezérigazgató a Synergon Csoportot, de a társaság részvényárfolyama máris növekedési pályára lépett. A vezérigazgató szerint a cloud technológia az ágazat jövőjét fogja meghatározni.

– Mivel tudja a Synergon kivédeni az informatikai ágazatot is érintő válságot, illetve az állami megrendelések hiányát?

– Az állami megrendelések hiánya számunkra nem meglepő, hiszen amíg a kormányzatnak az államadóssággal kell küzdenie, nekünk a beruházások visszafogása okoz gondot. Ez az informatikai szektort is érinti. Az elmúlt évek gazdasági és üzleti eseményei elkerülhetetlenné tették a cégcsoport szervezeti átalakítását. Új előadáshoz persze új zenészek is kellenek, úgyhogy szinte a teljes Synergon-vezérkar átalakult. Ütőképes és nagy tudású, tapasztalt szakemberekből álló menedzsment működteti ma már a Társaságot, melynek eredményeit a napi munkában én már most látom. Jövő évtől ez a tendencia a számainkban is megjelenik, bár előszeleit az év végére is lehet már érezni. Mivel az állami megrendelések elenyészők, ezért vezetőtársaimmal a hazai, illetve külföldi piacokon próbálunk újabb termékportfólióval megjelenni. Cseh leányvállalatunk, az Infinity sikerein felbuzdulva azt láttuk, vannak még fehér foltok a térképen, ahol a mi kompetenciáink aranyat érnek, így újabb nemzetközi vállalatalapítási lehetőségeket kerestünk és találtunk is. Az új leányvállalatok alapításáról a közeljövőben tájékoztatni fogjuk a részvényeseket és a sajtót is. A Társaság számára a másik új irányt a felhő, azaz a cloud technológián alapuló szolgáltatás jelenti.

– Ha már a cloud technológiát vetette fel, mit gondol, a felhőalapú szolgáltatások milyen méretekben fognak elterjedni a jövőben?

– Évekkel ezelőtt az outsourcing volt a csodaszer. Mára világossá vált, hogy a szolgáltatások kiszervezése adott feltételek figyelembevétele mellett, a mértékletesség betartásával valóban jó üzleti döntés. Azt hiszem, ez a lényeg! A cloud elsősorban üzleti modell kérdése. Minden olyan technológiai eszköz, amit a cloud kapcsán használunk, évek óta rendelkezésre áll. Éppen csak nem így hívták. A cloud rendkívül sok előnnyel bír. Nincs szükség eszköz- vagy ingatlanberuházásra, a kisebb cégek esetében ügyféloldali üzemeltető személyzetre, folyamatos licencvásárlásra és sok más korábbi horribilis költségeket felemésztő kiadásokra. Vagyis igen költséghatékony. Ugyanakkor mérhető, flexibilis, de egyúttal biztonságos is. A felhasználókat a legtöbb esetben nem érdekli a mögöttes infrastruktúra, ők egy biztonságos, felhasználásalapú elszámolási lehetőséget ígérő szolgáltatást szeretnének. Egy-két esetet leszámítva, amikor megszakad a telefonos kapcsolat, kevesen gondolkodnak el azon, hogy a mobilszolgáltatások mögött milyen technikai megoldások vannak. Véleményem szerint a cloud jövője a közmű jellegű szolgáltatássá válás lehet, amikor a vállalatok felismerik azt a tényt: nem akarnak internet, telefon, szoftverlicenc, amortizációs és egyéb költségeket fizetni, helyette inkább havidíjas elszámolás alapján bérelik az imént felsoroltakat magában foglaló IT-szolgáltatást. A Synergon készen áll ezen igények kielégítésére. A Társaság nemcsak értékesíti, de használja is a rendszert, hiszen cégünk dolgozói ma már a felhőalapú szolgáltatást használva és kihasználva érik el a belső informatikai rendszert. ■

MELLÉKLET

A vállalatok akár milliókat is veszíthetnek a régi adatközpontok miatt

A cégeknél, amelyek szerverek tucatjaiból vagy akár százaiból álló adatközpontokat működtetnek, a villanyóra számlálója igen gyorsan pöröghet. A vállalkozások épp ezért rengeteg energiát takaríthatnak meg, amennyiben a modern, energiatakarékos technológiákat választják. Még egy közepes méretű vállalkozás is, amely például tizenöt darab ötéves szerverrel rendelkezik, éves szinten mintegy 1,5 millió forintot, a teljes adatközpontra vetítve a jelenlegi költségek kb. 30 százalékát spórolhatja meg az új technológiák alkalmazásával.

A KPMG Tanácsadó Kft. által közzétett adatok szerint a beszerzési költségek folyamatosan csökkentek az IT-szektorban, míg az eszköz élettartamára vetített teljes költség (TCO, amely többek között magában foglalja az energiaköltségeket is) folyamatosan növekszik. Egyes források szerint 2000 óta hatszorosára nőttek ezek a költségek. A helyzet példátlan. „Az adatközpontok hűtésére és működtetésére fordított éves díjak egyes esetekben megközelítik akár a hardver értékét is" – mondta *Gacsal József,* az Intel Hungary üzletfejlesztési igazgatója.

Az Intel elemzése szerint egy cég Magyarországon éves szinten átlagosan 4,3 millió forintot költ egy tizenöt darabos – ötéves szerverből álló – adatközpont hűtésére és működtetésére, a teljes eszközparkot tekintve. Ilyen méretű adatközpont általában a közepes méretű, mintegy 250 főt foglalkoztató vállalatoknál található. A probléma megoldása az új technológiákban rejlik, amelyek magasabb teljesítményre képesek, ugyanakkor elavult elődeiknél energiatakarékosabbak. A virtualizációs technológiák bevezetésével pedig a működtetett fizikai szerverek tekintetében további konszolidáció érhető el. Az elemzés szerint egy új, energiatakarékos szerver hűtési és működtetési költsége virtualizáció után fajlagosan mindössze az eredeti költségek egyharmada.

„Mivel az energiaárak folyamatosan nőnek, a vállalatok vezetőinek ezentúl még inkább oda kell figyelniük a fogyasztásra" – hangsúlyozta Gacsal. – Egy vállalat költségvetésében a gyártást és bérezést követően a harmadik legnagyobb tételt az energiafogyasztás jelenti. Ez azonban számos vállalat esetében eléggé homályos tételnek tekinthető, amely nem kapcsolódik közvetlenül az IT-részleghez, ugyanakkor a számítástechnikai eszközök nagyban hozzájárulhatnának az energiaszámlák csökkentéséhez. A beszerzési és szolgáltatási díjakkal ellentétben az informatikai személyzet nem érzi magát felelősnek ezért a költségért, így nem is motivált aziránt, hogy új, energiatakarékosabb eszközökbe ruházzon be" – tette hozzá Gacsal József.

CSÖKKENTHETŐ ENERGIASZÁMLÁK

Kálóczy Csaba, a 99999 Informatika Kft. szolgáltatási igazgatója szintúgy ezen a véleményen van. A cég adatközponti technológiákkal foglalkozik, így virtualizációs technológiákkal is, ennek kapcsán pedig magyar cégek szerverszobáinak villamosenergia-használatát vizsgálja. „A vállalatok esetében a számítástechnikai eszközök fogyasztják a legtöbb áramot, ezért a vezetőknek fontos részletesen elemezniük az IT-részleg energiafogyasztását. A magyar IT-szektor állapota a megtakarításokat tekintve hatalmas lehetőséget kínál, hiszen a szerverszobák és az adatközpontok nagyon nagy tartalékokat élnek fel" – mondta a szakember. Ami az áram elosztását illeti, Kálóczy Csaba és kollégái munkájuk során leginkább olyan problémákba ütköznek, amelyek sokkal inkább „kusza hosszabbítókábelekhez" hasonlítanak, mintsem egy intelligens elosztórendszerhez, amely lehetővé teszi a fogyasztás és a működtetés részletes ellenőrzését. Az adatközpontokat tekintve Kálóczy Csaba elmondta: az új technológiák használatában rejlő lehetséges megtakarítások teljes összege a jelenlegi működési költségek mintegy 30-35 százaléka.

A MAGYAROK IGEN IGÉNYESEK, AMI AZ ENERGIAFOGYASZTÁST ILLETI

Manapság nemcsak a vállalatok áramszükséglete növekszik egyre jobban, hanem az energia ára is – ez utóbbi 2011-ben mintegy 10 százalékkal nőtt. A KPMG Tanácsadó Kft. szerint a magyar gazdaság energiaintenzitása hosszú idő óta csökken, azonban még mindig 40 százalékkal magasabb, mint az európai uniós átlag. Ráadásul az energiaintenzitás csökkenését ellensúlyozzák a növekvő energiaárak. „A helyi forrásoknak köszönhetően a magyar gazdaságnak inkább alacsony az energiafüggőségi rátája, de növekszik az energiaforrások importjától való függőségük, ugyanakkor a villamos energia exportja lassan csökken. Az alternatív energiaforrások csak kismértékben hozhatnak változást ezekben a tendenciákban. Az egyik kulcsfontosságú stratégiai megoldás tehát az energia megtakarítása lenne" – mondta *Sallai György,* a KPMG tanácsadója.

Az információs technológiák kiemelkedő szerepet játszanak az energiamegtakarításban és az üvegházhatást okozó gázok kibocsátásának csökkentésében. A McKinsey-riport szerint az infokommunikációs ipar csupán 2 százalékát adja a teljes szén-dioxid-kibocsátásnak – a világszerte működtetett adatközpontok fogyasztása például jelenleg ugyanolyan mértékű károsanyag-kibocsátásért felelős, mint a légi közlekedés. A megfelelő megtakarítási intézkedések végrehajtása azonban 15 százalékos csökkentést eredményezne a károsanyag-kibocsátás tekintetében. ■

PÉLDA

Kereskedelmi cég, 250 alkalmazottal, 15 darab ötéves szerverrel: a jelenlegi 15 szerver helyettesíthető egy darab új szerverrel, amely ugyanazt a teljesítményt biztosítja – a megtérülés már nyolc hónapon belül garantált. ▪ Az adatközpont teljes működtetése tekintetében éves szinten 1,2 millió forint, 30 százalékos megtakarítás érhető el. ▪ A rövid távú megtérülést az új szerverek teljesítményében tapasztalható éles növekedés okozza. ▪ Egy hasonló cég éves szinten 1,2 millió forintot takaríthat meg a hűtési és működtetési költségeken. ▪ Az Intel Xeon processzorait alkalmazó új rendszerek energiatakarékosak, nem termelnek annyi hőt, így nem szükséges a korábban megszokott mértékű energiát felhasználni a hűtésükre. ▪ A teljes villamosenergia-megtakarítás elérheti akár a 90 százalékot is.

INFORMÁCIÓK

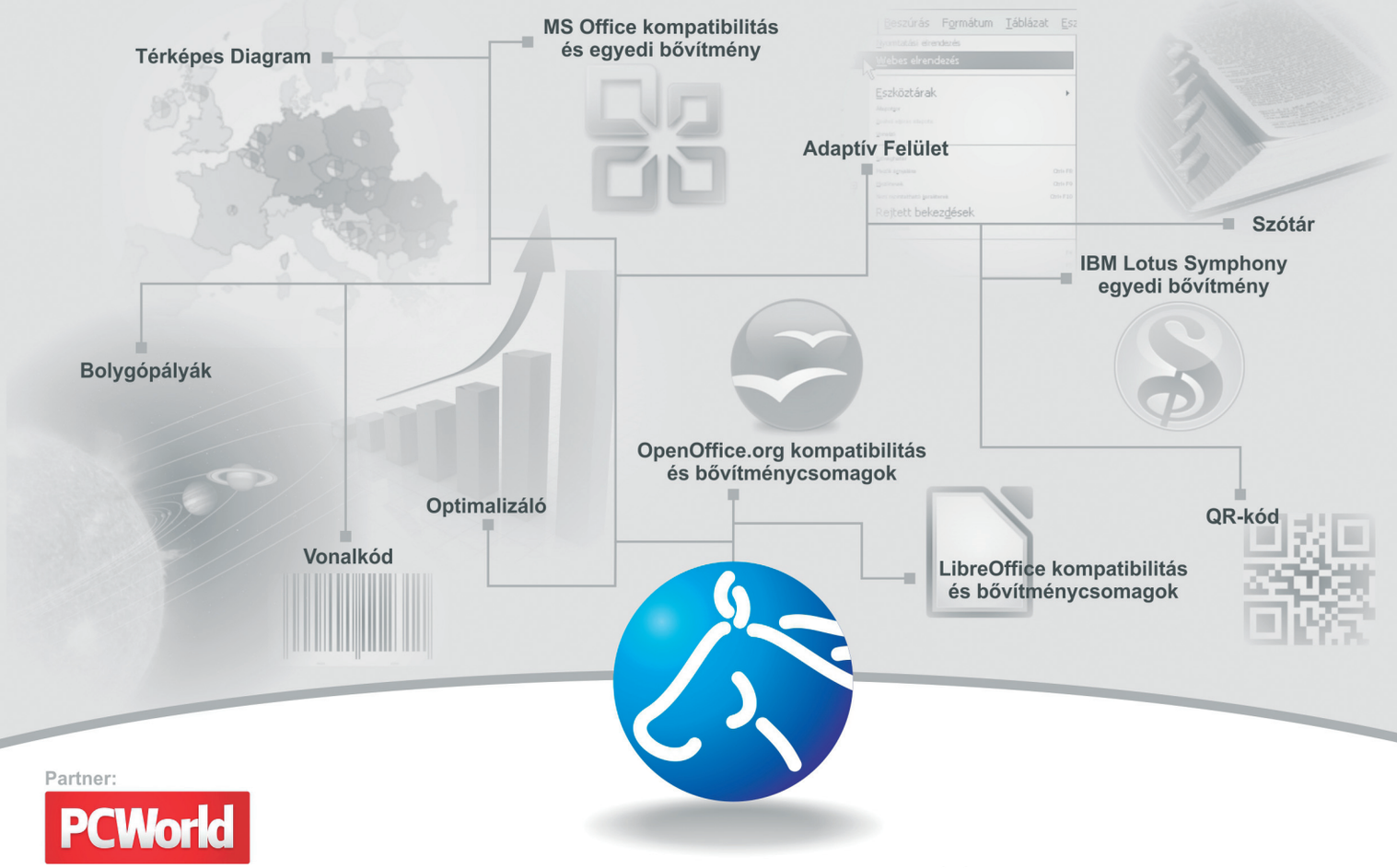
Az új technológiákon alapuló energiamegtakarítást világszerte megoldásnak tartják az egyre növekvő energiafogyasztással szemben. A Nemzetközi Energiaszövetség (EIA) szerint 2030-ra az áramigény 60 százalékkal fog nőni, főként a fejlett országok megállíthatatlan iparosodásának következtében, amely egyúttal jelentős növekedést okoz a szén-dioxid-kibocsátásban is.
A technológiai innovációk azonban megállíthatják ezt a növekedést. Az EIA állítása szerint a technológia jelenti az egyetlen olyan megoldást, amelyet mind az ortodox környezetvédők (akik az alternatív energiaforrásokat javasolják), mind a szkeptikusok (akik megkérdőjelezik a globális felmelegedést) elfogadnak.

sokoldalú megoldások

MULTIRÁCIÓ

Új irányzat — testreszabható megoldások az irodai programkörnyezetre

A MultiRáció Kft. által kínált EuroOffice integrált irodai szoftver teljes megoldást kínál mind az intézmények, mind az üzleti világ számára. Az irodai alkalmazáscsomag a MultiRáció Kft. 2003-ban innovációs díjnyertes MagyarOffice irodai szoftvercsaládjának továbbfejlesztése. A nyílt szabványokra épülő, nyílt forráskód alapú megoldás az Európai Unió főbb nyelveit is támogatja. További előnye, hogy Windows és Linux operációs rendszereken egyaránt futtatható. A szoftver képes minden elterjedtebb fájlformátum kezelésére, beleértve az MS Office által használt fájlokat is. Saját fájlformátuma az Európai Unió által is ajánlott ODF nemzetközi ISO szabvány fájlformátum.
Az EuroOfficehoz készített bővítmények további szolgáltatásokkal – például új eszköztárakkal, adaptív felülettel, térképes diagrammal, optimalizálóval, árfolyam-kiírásokkal, oktatási segédletekkel és további nyelvi eszközöket tartalmazó funkciókkal – egészítik ki az alap irodai programcsomagot. Számos bővítmény használható OpenOffice.org, illetve LibreOffice alatt is, emellett egyes bővítmények elérhetők MS Office, illetve IBM Lotus Symphony alá.



Partner:

PCWorld

Copyright © 2001-2011
MultiRáció Ltd.

http://www.multiracio.com


SUZUKI
Way of Life!
20 éves
A MAGYAR SUZUKI
SWIFT
Sport
SWIFT
Sport
www.swiftsport.hu
Üzemanyag-fogyasztás (kombinált): 6,4 l/100 km. CO_2-kibocsátás: 147 g/km.