SZÁMÍTÁSTECHNIKA
COMPUTERWORLD
IKT-STRATÉGIA DÖNTÉSHOZÓKNAK / ALAPÍTVA 1969 /
2012. SZEPTEMBER 26. / XLIII. ÉVFOLYAM 39. SZÁM

ITT AZ ADAT, HOL AZ ADAT?

A mobil- és cloudtechnológiák térhódítása azt is jelenti, hogy a hagyományos védelmi megközelítések önmagukban már nem képesek helytállni.

Összeállításunk a 8–10. oldalon

IPARI KÉMKEDÉS

A vállalatok jó része maga is hozzájárul megfigyelhetőségéhez. A kiszivárogtatás ellen lehet és kell is tenni.

» 12. oldal

KIDUMÁLT INFORMÁCIÓK

Drámaian megemelkedett a társadalmi érintkezéseken keresztüli adatlopások száma: 1-ről 37 százalékra.

» 18. oldal

9 770587 151006 12039
www.computerworld.hu
Ára: 495 Ft
IDG HUNGARY

COMPUTERWORLD /IMPRESSZUM

KIADJA AZ IDG HUNGARY KFT.
1075 Budapest, Madách I. út 13–14. A épület
HU ISSN 0237-7837
Postacím: 1374 Budapest 5, Pf. 578.
» www.idg.hu

Bankszámlaszám:
10300002-20328016-70073285

FELELŐS KIADÓ:
Bíró István ügyvezető – ibiro@idg.hu

MŰSZAKI VEZETŐ:
Babinecz Mónika – mbabinecz@idg.hu

NYOMÁS ÉS KÖTÉSZET:
Mesterprint Kft. 1191 Budapest,
Vak Bottyán utca 30-32/b
Ügyvezető igazgató: Szita Lajos

SZERKESZTŐSÉG
Főszerkesztő: Dervenkár István
Vezető szerkesztő: Sós Éva, Szilágyi Szabolcs
Online igazgató: Odrovics Szonja
Olvasószerkesztő, korrektor: Sz. Erdős Judit
Munkatársak: Dávid Imre, Kis Endre, Kömlődi Ferenc, Meixner Zoltán, Tóth Lívia, Vass Enikő
Tipográfia: Berényi István
Szerkesztőségi ügyelet:
Csereszny Anita – acsereszny@idg.hu
Telefon: 577-4302, fax: 266-4343

Munkatársaink elérhetőségeit megtalálja weboldalunkon: » www.computerworld.hu

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

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

MEDIASHOP: MEDIASHOP.IDG.HU

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.

AKTUÁLIS

FÓKUSZ

KÉMEK

FECSEGŐK

ÁLLANDÓ ROVATAINK

COMPUTERWORLD /ONLINE

18/S
A kiberbűnözés új szintre lép – kihasználja a kezünkben levő okostelefonok lehetőségeit.
» computerworld.hu/cikk/18-per-szekundum

BIZTONSÁGOS MOBIL
A PCI Security Standards Council olyan dokumentumot tett elérhetővé, amely a mobilfizetés biztonságosabbá tételét szolgáló iránymutatásokat tartalmazza.
» computerworld.hu/cikk/biztonsagos-mobil-fizetes

ITT AZ ÚT VÉGE
Az utolsó szabad IPv4 címek Európában. Szerencsére a megoldás már évek óta elérhető.
» computerworld.hu/cikk/utolso-ipv4-cimek

AGGÓDÓ ANDROID
Az utóbbi hónapok rosszak voltak az Android-készülékeket gyártó cégek számára, a Windows 8 és a Windows Phone 8 bemutatása pedig alaposan felforgathatja a piaci erőviszonyokat.
» computerworld.hu/cikk/androidos-gyartok-baja

JAKAB PÉTER
elnök
Magyar Bankszövetség
Bankbiztonsági
Bizottság

ITBN előtt
Szubjektív számvetés

Az ITBN, mint a legnagyobb és legátfogóbb hazai, informatikai biztonsággal foglalkozó rendezvény, mindig okot ad annak végiggondolására, milyen kihívásokkal, kockázatokkal, fejlődési és fejlesztési trendekkel kell vagy érdemes számolni az IT-rendszereket fejlesztőknek, illetve felhasználóiknak. Ezek közül néhányat igyekszem számba venni a következőkben. A „leltár" természetesen szubjektív és nem a teljesség igényével készült.

> Az elkövetkezendő évek egyik fontos IT-védelmi „harctere" lesz a kritikus infrastruktúrák védelme.

Az informatika és az IT-rendszerek minden kétséget kizáróan olyan szinten épültek be mára mindennapjainkba az államigazgatástól, a termeléstől, termékektől, a szolgáltatásoktól az oktatásig vagy a szórakozásig, hogy már régen egyértelmű: az IT-rendszerek igen jelentős része önállóan is és közvetve is kritikus infrastruktúrának minősül. Ez azt jelenti egyrészt, hogy a telekommunikációs infrastruktúrák önmagukban is rászolgáltak a kritikus infrastruktúra besorolásra és nehezen vitatható, hogy azon más infrastruktúrák, amelyeket minden definíciós metódus ebbe a kategóriába sorol (például energiaellátás, pénzügyi rendszerek, közlekedés, egészségügy stb.) oly mértékig függnek az őket támogató IT-rendszerektől, hogy azok kiesése gyakorlatilag teljes működésképtelenségüket jelentheti.

A fentiekre és az elmúlt egy-két évben nyilvánosságra került súlyos kiberincidensekre (Stuxnet, Flame, Duqu, Gauss stb.) tekintettel azt gondolom, hogy az elkövetkezendő évek egyik fontos IT-védelmi „harctere" lesz ezen kritikus infrastruktúrák védelme. Véleményem szerint Magyarország ebből a szempontból nem tartozik a kifejezetten fenyegetett országok közé, de az IT-infrastruktúrák beágyazottsága és globális tulajdonságai miatt ezeknek a kockázatoknak az elemzésével és kezelésével feltétlenül foglalkozni kell. E kockázat természetéből adódóan a feladat igen sokrétű, komoly szakmai felkészültséget és társadalmi összefogást igényel az ilyen védelemmel hivatásszerűen foglalkozó szervezetek és a civil szféra között.

Prognosztizálhatóan igen jelentős fejlődés és előretörés várható az ún. felhőalapú (cloud) infrastruktúrák területén, amelyek több szinten kínálnak az alkalmazóknak a gyakran változó igényekhez jól igazítható és költséghatékony IT-környezetet. Biztonsági oldalról ezen infrastruktúrák számos problémát vetnek fel, amelyek mindegyikére nincsenek még igazán kiforrott válaszok, ugyanakkor napjainkban, amikor a költséghatékonyság az egyik fő vezérlő elv az IT-fejlesztések területén, jól érzékelhető tendencia a költségcsökkentés jegyében megjelenő magasabb kockázatvállalási készség az alkalmazó szervezetek részéről. Biztonsági szempontból ma még jelentős kockázatot hordoz az a nem először tapasztalható helyzet, hogy az IT-fejlesztések eredményeit és ezek alkalmazhatóságát nem, vagy csak igen lassan, jelentős késésekkel követi az a szabályozási és jogi környezet, amely lehetővé teszi e megoldások jogi szempontból is aggálymentes alkalmazását. Ez a helyzet különösen jól kitapintható a cloud rendszerek adatvédelmi és független auditálhatóságának kérdéseit illetően. Az egyértelmű és így jól tervezhető, betartható és ellenőrizhető követelmények hiányában e rendszerek fejlesztői sincsenek könnyű helyzetben. Természetesen azt gondolom, hogy egy folyamatos iteráció eredményeként ez a helyzet fokozatosan és jelentősen javulni fog, hiszen ehhez igen jelentős felhasználói, alkalmazói és fejlesztőoldali üzleti érdekek fűződnek.

A mobilkommunikáció és szolgáltatások példátlan terjedésével véleményem szerint nem tartottak lépést ezen szolgáltatások és eszközök biztonsági megoldásai és alkalmazóik biztonságtudatossága sem. Ez utóbbi hordozza talán a legnagyobb kockázatot, hiszen a hétköznapi felhasználók igen jelentős része a kényelmes szolgáltatások igénybevétele mellett nem, vagy alig törődik okostelefonja vagy tablet PC-je biztonsági kérdéseivel, az ezeket fenyegető veszélyeket nem ismeri vagy alábecsüli. E területen a forgalmazóknak, fejlesztőknek, oktatóknak és a biztonsági szakembereknek igen komoly felelősségük van azon elv érvényesítése mellett, amely szerint a biztonság megteremtésének felelősségéből a lehető legkevesebbet szabad a felhasználóra terhelni.

Hyde Tech Corner

Ezen a héten *G. Németh György* és *Szittya Tamás* kommentálja híreinket. / összeállította: Sós Éva

Heti összeállításunkból megtudhatják, hogy ma már több tízezer, a mindennapi egészségügyi ellátásban használható alkalmazás áll rendelkezésre, valamint minimális informatikai többletköltséggel felügyelhetők és biztonságossá tehetők a saját tulajdonú mobileszközök.

MÁR NEM INFORMATIKAI KÉRDÉS A BIZTONSÁG

Amíg tíz éve elég volt egy jól konfigurált tűzfal és antivírus szoftver a számítógépek védelméhez, addig mára sokkal összetettebbé vált a kép.

» computerworld.hu/cikk/nem-IT-kerdes-a-biztonsag

SZITTYA TAMÁS

ÜGYVEZETŐ IGAZGATÓ, NETIQ NOVELL SUSE MAGYARORSZÁGI KÉPVISELET

Nagy változáson ment keresztül az utóbbi időben a vállalati biztonság világa. Számos új kihívás jelentkezik napjainkban a vállalati biztonság terén, beleértve a szofisztikált támadásokat, az informatika konzumerizációját, a BYOD trendet, valamint a mobileszközök terjedése következtében veszélybe kerülő vállalati adatokat. Ezek az új kihívások szerencsére orvosolhatók, a vállalati informatikával foglalkozó cégek gyorsan reagálnak az új problémákra. Egy megfelelően beállított és alkalmazott végpont-felügyeleti eszközzel például egyszerűen kezelhető napjaink egyik sok fejtörést okozó jelensége, a BYOD, azaz a saját tulajdonú eszközök használata a szervezeteken belül.

A legújabb megoldások, köztük az általunk Magyarországon forgalmazott és támogatott Novell ZENworks Mobile Management is, már képesek garantálni, hogy a saját tulajdonú mobileszközök minimális informatikai többletköltséggel legyenek felügyelhetők és biztonságossá tehetők a vállalati infrastruktúrán belül. A legfejlettebb végpontbiztonsági és felügyeleti eszközök számára nem okoz gondot az iOS, Android, Symbian vagy Windows Mobile rendszerű, illetve egyéb ActiveSync-kompatibilis eszközökkel történő együttműködés sem.

A dolgozók igényei és a vállalatvezetők elvárásai, valamint a biztonsági előírások közötti határmezsgye rendkívül keskeny. De az egyensúly fenntartható az olyan különleges funkciók segítségével, mint például a személyre szabható biztonsági beállítások vagy a készülékeken található, vállalati és privát tartalmak külön kezelése. Ez utóbbi különösen fontos, ha a vállalatok azt a szolgáltatást is kihasználják, amellyel a távoli készülékeken lévő adatokat is törölhetik, például elveszett vagy ellopott mobiltelefonok esetében. Megoldásunk ugyanis erre is lehetőséget nyújt, a teljes körű biztonság fenntartása érdekében.

OKOSTELEFONOK AZ EGÉSZSÉGÜGYBEN

Magyarországon évente akár 40 ezerrel is csökkenthető a kórházban töltött éjszakák száma. A titok nyitja: otthonápolás, távkezelés mobilkommunikációs eszközökkel.

» computerworld.hu/cikk/okostelefon-az-egeszsegugyben

G. NÉMETH GYÖRGY

IGAZGATÓ, BOK, ALVÁSDIAGNOSZTIKAI ÉS ALVÁSTERÁPIÁS LABORATÓRIUM

Nagy elmaradásai vannak a hazai egészségügynek a new médiaeszközök gyógyításban való felhasználási területein. Ezért is örömteli minden kezdeményezés, amely a korszerű technológiát alkotó és egészségvédő módon alkalmazza. Az mHealth megoldások tulajdonképpen már a kezünkben vannak, legalábbis az eszközök és a technológia vonatkozásában. A legfontosabb a szándék, amely azonban még nem elég erős ahhoz, hogy felismerjük: életmentő, élethosszabbító, életminőséget javító lehetőségről van szó. A jó ötletekért nem kell messzire menni: az internet folyamatosan frissülő tárháza kínálja az új megoldásokat, sőt a korszerű ötletek házhoz is jönnek. De az ellátás minőségéhez, a betegbiztonság javításához, a gyógyszeres kezelések hatékonyságához és gazdaságosságuk növeléséhez szintén hozzájárulhatnak az IT-alapú megoldások. Így például az elektronikus vényírási rendszer bevezetése vagy az adatok elektronikus hozzáférése. Egyre inkább szükség lesz ugyanis arra, hogy a betegek kezelési adatai ne csak az ellátó intézményben, hanem szükség esetén bárhol, bárhonnan hozzáférhetők legyenek, az országhatárokon belül és uniós szinten egyaránt. Az okostelefonok számára ma már több tízezer, a mindennapi egészségügyi ellátásban használható alkalmazás áll rendelkezésünkre. Mi például már jó ideje alkalmazzuk az alvásdiagnosztikában az éjszakai alvásciklus-mérési programot, amely információt tud adni az ember éjszakai alvási szokásairól. De elkészült és hozzáférhető például az a program is, amely az alvásciklusok elemzése alapján a legmegfelelőbb időpontban segít felébredni, ezzel kellemesebbé téve a reggeli órákat. Mindezek az alkalmazások nem jelenthetnek anyagi kérdést, a felismerés pedig már adott: kezünk ügyében, legtöbbször a szó valódi értelmében kezünkben vannak azok az eszközök, amelyekkel egészségesebben élhetünk.

[HÍRMOZAIK]

PRIVÁT / A NetIQ Novell SUSE Magyarországi Képviselet bejelentette, hogy elérhetővé vált a SUSE első, vállalati szintű támogatással érkező, privátfelhő-megoldása, a SUSE Cloud.

SZAKDOLGOZAT / A Hétpecsét Információbiztonsági Egyesület kihirdette az *„Év információbiztonsági diploma és szakdolgozata”* pályázat nyertesét, aki idén *Boda Károly*, a Budapesti Műszaki Egyetem hallgatója.

SILVER / Alig két évvel a piacra lépést követően Silver minősítéssel díjazta a Cisco a NET'54 Üzleti Kommunikáció Kft. szakmai és üzleti teljesítményét. A NET'54 számára éves szinten az árbevétel jelentős részét képező Cisco-értékesítés mellett a minősítés alapját a kiválóan képzett szakembergárda jelentette.

[ESEMÉNYNAPTÁR]

SZEPTEMBER 27. BUDAPEST
IDC Manufacturing 2020 Roadshow
» www.computerworld.hu/cikk/idc-man-2020

OKTÓBER 4-5. BUDAPEST
Budapest Conference on Cyberspace 2012
» www.cyberbudapest2012.hu

OKTÓBER 11-12. BUDAPEST
Hungarian Software Testing Forum (HUSTEF) konferencia és workshop
» www.computerworld.hu/konferencia/73

OKTÓBER 12-13. BUDAPEST
Hacktivity 2012
» www.hacktivity.com

TOVÁBBI ESEMÉNYEK
» www.computerworld.hu/esemenyek

VILÁGELSŐ!

Forráskód-minősítő eszközt fejlesztettek Szegeden

A FrontEndART Kft. most vezeti be a piacra a világviszonylatban is új, a szoftverek forráskódjának vizsgálatára épülő minősítési eljárását, amelynek alapjait a Szegedi Tudományegyetem Szoftverfejlesztési Tanszékének kutatásai adják. /Computerworld

A szoftverek nehezen megfogható, mérhető termékek, így a fejlesztőcégeknek komoly szakmai kihívást jelent a szállított termékek színvonalának garantálása, a megrendelők oldaláról pedig annak ellenőrzése. A problémát felismerve kezdett többéves közös projektbe a FrontEndART Kft. a Szegedi Tudományegyetem Szoftverfejlesztési Tanszékével, ahol lassan már 15 éve folyik a fejlesztés. Jelenleg több mint 100 kutató-fejlesztő dolgozik a forráskód-minőségbiztosítási technológiák innovációján – tudtuk meg *Bakota Tibortól,* a cég vezetőjétől. Közös munkájuk eredményeként született meg végül az ISO/IEC 25000 szabványon alapuló objektív kódminősítési eljárás.

„A forráskód minőségének mérése nagyon fontos üzleti szempontból, elsősorban a szoftverüzemeltető cégek számára, hiszen a beszállított rendszerekről gyakorlatilag semmit sem tudni, így minőségük sem ismert. Ez olyan, mintha valaki vesz egy autót, de nem tudja, hogy Trabantot vagy Cadillacet vett" – magyarázta Bakota Tibor.

A világszinten is újdonságnak számító fejlesztés alkalmazásával a szoftverfejlesztő cégek számára mérhetővé és fejleszthetővé válik termékeik karbantarthatósága, emellett az üzemeltető cégek is ellenőrizni tudják a megvásárolt szoftverek valós minőségét, ezáltal csökkentve tesztelési költségeiket és az üzemeltetési kockázatokat.

> A FrontEndART Kft. a Szegedi Tudományegyetem Szoftverfejlesztési Tanszékével közösen **15 éve dolgozik a forráskód-minőségbiztosítási technológiák innovációján.**

„Egy rendszert nem elég megvenni, fenn is kell tartani, mindazonáltal sok esetben ez utóbbi jóval többe kerül, mint maga a beszerzési ár" – figyelmeztetett a szakember. A szolgáltatás az objektív tanúsítvány mellett részletes elemzést is ad a megrendelők számára: kritikussági sorrendben mutat rá a szoftver gyenge pontjaira, a fejlesztés gátjaira, elhárítandó hibáira.

A bejelentés már csak azért is figyelemre méltó, mert hazánkban számos innovációs eredmény nem kerül át a piaci gyakorlatba. Ezt a fejlesztést egy piaci igény hívta életre, valós problémára kínál megoldást. Ez biztosítja, hogy a jövőben a fejlesztésre lesz fizetőképes piaci kereslet – hangzott el a minősítési eljárás bemutatóján, amelyen a bank- és biztosítószektor szakemberei mellett főként a szoftverüzemeltetéssel és szoftverfejlesztéssel foglalkozó cégek voltak jelen. Az eseményen *Rozenberszki Zsolt,* az R&R Software értékesítési igazgatója és *Nagy Péter,* az ERSTE Bank CIO-ja közös előadásukban bemutatták a mindennapi használat eredményeit és vázolták azokat a célokat, amelyeket a forráskód-minősítés segítségével kívánnak elérni.

„A mai kiélezett piaci helyzetben a megrendelőinknél extrém árérzékenység tapasztalható, amelynek elsősorban a minőség eshet áldozatul; döntő szerepe sokszor szinte kizárólag az ajánlati árnak van. A minőséget középpontba helyező szállítók versenyhátrányba kerülhetnek a tiszavirág életű, rövid távú sikerekben érdekelt cégekkel szemben. Középtávon azonban már a megrendelői oldalon is egyértelművé válik, hogy a rendszer fejlesztése közben megspórolt kiadások a későbbiekben többszörös költséget jelenthetnek a karbantartás és az üzemeltetés, illetve a szükségessé váló csere során. Az R&R Software éppen ezért minden lehetőséget megragad a szoftverminőség jelentőségének hangsúlyozására, valamint a partnereink számára fejlesztett rendszerek minőségének garantálására. Cégünk az elsők között volt a minősítésre használt modell ipari alkalmazásában, az eredményeket pedig jelenleg is saját kódbázisunk minőségének javítására, a minőség fenntartására használjuk" – összegezte a megoldás előnyeit Rozenberszki Zsolt.

Mint ismeretes, a forráskód-minőségbiztosítás egyik alapját a Szegedi Egyetem Szoftverfejlesztés Tanszékének egy 2002-ben megjelent publikációja adja, amit az idei International Conference on Software Maintenance (ICSM) – a világ egyik legfajsúlyosabb szoftver-karbantarhatósági konferenciája – az elmúlt 10 év legnagyobb hatású *(most influential)* publikációjának választott.

SCI-NETWORK ZRT.

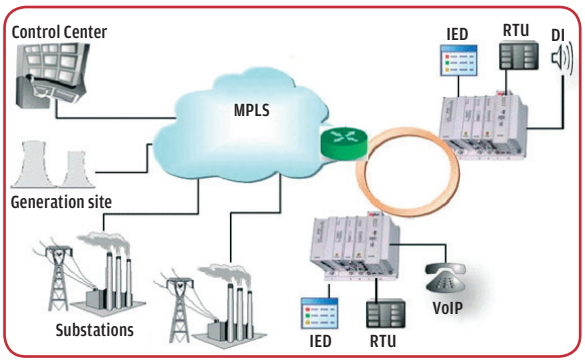
RADiFlow dedikált switchekkel az ipari szolgáltatások IT-biztonságáért

A modern ipari alkalmazások hatékony és biztonságos kommunikációt kívánnak meg az üzemeltetési szintek között. Ez az ipari folyamatok optimalizálásának záloga. Az utóbbi években az Ethernet hálózatok, amelyek alapját képezik a nyílt szabvány alapú hálózati kapcsolatoknak, preferált infrastruktúrává váltak a kritikus biztonsági igényeket támasztó ipari szolgáltatói környezetben.

A RADiFlow az izraeli RAD-csoport tagjaként az ipari szolgáltatásspecifikus Ethernet hálózati berendezések vezető szállítója.

Magyarországon a SCI-Network zRt. több mint 15 éve értékesítő partnere a RAD-csoportnak a professzionális vezetékes és vezeték nélküli hálózati megoldások területén. E hagyományos tevékenységei mellett kiemelt szerepet szán a RADiFlow ipari hálózatinformatikai eszközök értékesítésének is. Hálózatintegrátorként vállalja a RADiFlow switchekre épülő, nagy megbízhatóságú, magas rendelkezésre állású ipari Ethernet hálózatok tervezését, meglévő hálózatba integrálását, valamint felügyeleti rendszerének kialakítását.

A RADiFlow ipari Ethernet switch eszközeinek – RADiFlow 3000-es sorozat – tipikus alkalmazási területei a gyártóüzemi környezet, a több telephelyes közműszolgáltatók, a különböző típusú és biztonsági fokozatú erőművek, a Smart Grid rendszerek, közlekedésbiztonsági területek, a veszélyeztetett, cyber-betörésnek kitett SCADA rendszerek elosztott védelmének biztosítása beépített tűzfalak segítségével és hasonló ipari szolgáltatói környezetbeli alkalmazások.



Az ábrán egy innovatív erőmű hálózati alkalmazása látható

Az ellenőrző központ és az alállomási RTU-k közötti kiemelt biztonságú kapcsolatok megvalósítása elosztott SCADA tűzfal használatával történik.

A WAN gerinchálózati kapcsolat Ethernet VLAN-okkal vagy az MPLS routeren keresztül valósul meg. A protokoll gateway funkcionalitással ellátott integrált soros interfészek a hagyományos IED-ekhez történő zökkenőmentes migráció megvalósítását szolgálják. ■

Itt az adat, hol az adat?

Az információbiztonság egyik alapvető követelménye, hogy pontosan tisztában legyünk adataink tárolási helyével, valamint az azokat körülvevő védelmi megoldásokkal. A mobil- és cloudtechnológiák terjedése azonban mindezt igencsak megnehezíti. Témánk: az adatok feletti kontroll megteremtése a mobil és felhőalapú technológiák tükrében.

KRISTÓF CSABA

Amikor az információbiztonság megteremtése szóba kerül, akkor meglehetősen sokszor lehet arról hallani, hogy a védelem kialakítása során az adatközpontúságot sem célszerű figyelmen kívül hagyni. A megóvandó értékek közül ugyanis sok esetben éppen az adatok jelentik a legféltettebb kincset.

Vállalati környezetekben az adatok védelmének megvalósítása komplex megoldásokat, intézkedéseket követel meg, amelyek között jó esetben az adatszivárgás-megelőzés *(DLP – Data Loss Prevention)* is szerephez jut. Ezért emeljük ki most éppen a DLP-t, mert egy adatszivárgás-megelőzésre alkalmas rendszer bevezetése során az adatok klasszifikálására, illetve azok helyének és kezelésének miképpen mindenképpen választ kell találni. Ekkor kiderül, hogy melyek az érzékeny adatok, azokat kik, hol és milyen módon érhetik el és kezelhetik a szervezeteken belül. Igen ám, de mi történik akkor, ha az adatoknak el kell hagyniuk a vállalatok, intézmények határait, és ezáltal a felügyelet is csorbát szenved. Márpedig mindez egyre gyakrabban történik meg, hiszen a mobil- és cloudtechnológiák térhódítása éppen ebbe az irányba visz minket. A következőkben megvizsgáljuk, hogy az adatok feletti kontroll megteremtése milyen nehézségeket jelent a szervezetek számára, és miként lehet csökkenteni a felmerülő kockázatokat.

Kiszolgáltatott adatok a mobilokon

A boltok polcaira kerülő mind nagyobb teljesítményű és kapacitású okostelefonok, táblagépek a felhasználók körében igen népszerűek, de a vállalatok is egyre inkább igyekeznek kihasználni az új technológiákban rejlő lehetőségeket. Eközben azonban az egyes cégek, intézmények biztonságáért felelős szakemberek vállára mind nagyobb teher rakódik, hiszen a rohamosan fejlődő mobiltechnológiákkal védelmi szempontból is lépést kell tartaniuk. Ellenkező esetben jelentős rések nyílhatnak az informatikai infrastruktúrákon.

A védelmi eszközöket fejlesztő cégek is pontosan látják, hogy a mobilbiztonság az érdeklődés középpontjába került, és egyre fokozottabb kereslet mutatkozik azon termékek iránt, amelyek képesek a mobilkészülékek felügyeletét megvalósítani, központosítani. Az IDC szerint az *MDM- (Mobile Device Management)* megoldások piacán 2009-ben 265 millió dolláros forgalmat lehetett elkönyvelni, és azóta évente mintegy 9 százalékos növekedés tapasztalható. Az is elképzelhető, hogy a jövőben az MDM-piac átlépi a 10 százalékos növekedési ütemet.

Az MDM-eszközök piaca napjainkban már több mint 40 jelentős szereplővel büszkélkedhet, ezek olyan megoldásokat fejlesztenek, amelyek a konfigurációmenedzsmentet, a hibaelhárítást, az esz-

közleltárak készítését, a távoli felügyeletet, valamint a jelentéskészítést is támogatják a mobilkészülékek esetében. E termékek fontos feladata, hogy az elkallódott eszközök kapcsán lehetőséget biztosítsanak a távoli adattörlésre vagy zárolásra, és betarthatóvá, érvényre juttathatóvá tegyék a vállalatok körében kialakított biztonsági szabályokat.

Rafal Los, a HP Software Worldwide biztonsági szakértője szerint azonban nem elég csak a mobilkészülékekre fókuszálni és azt várni, hogy ettől majd nagyobb lesz a biztonság. „A rendszereket holisztikus módon kell szemlélni. Ez magában foglalja az infrastruktúrát, az alkalmazásokat, az adatelérési és adathasználati technikákat is. Az eszközökre telepített alkalmazások kezelése mellett azon alkalmazásszerverek, valamint adatbázisok védelméről is gondoskodni kell, amelyekhez mobilok csatlakozhatnak" – vélekedett a szakember.

Az MDM szerepe az informatikában

SZOLGÁLTATÓVÁLASZTÁS ADATVÉDELMI SZEMPONTBÓL

Vinod Bange, a Taylor Wessing nemzetközi ügyvédi iroda adatvédelemmel foglalkozó szakértője szerint a legnagyobb gondot az Európai Unió és az Amerikai Egyesült Államok adatvédelmi gyakorlatában tapasztalható ellentmondások jelentik, amiket a jelenlegi jogszabályok alapján korántsem könnyű kezelni. Az EU adatvédelmi direktívája kimondja, hogy ha adatokat kell mozgatni az EU határain kívülre, akkor érvényben maradnak az EU-s jogszabályok, vagyis a jogok követik az adatokat. A szakember szerint azonban az USA jogszabályai mindennek bizonyos értelemben keresztbe tesznek.
Az USA-ban a szeptember 11-i terrortámadást követően *Bush* elnök aláírta a Patriot Act törvényt, amely különleges jogokkal ruházta fel az amerikai hatóságokat és nemzetbiztonsági szerveket az elektronikus megfigyelés tekintetében. A cloud computing szempontjából a törvény azt is jelenti, hogy az amerikai szolgáltatók által kezelt adatokra az USA erre feljogosított szervei egyszerűbben tehetik rá a kezüket. A szolgáltatókat kötelezhetik az adatok kiadására akár úgy is, hogy minderről a cloudszolgáltató ügyfele nem szerez tudomást. A problémát tovább fokozza, hogy a törvény azon infrastruktúrákban kezelt adatokra is vonatkozik, amelyek ugyan nem az Egyesült Államok területén helyezkednek el, de azokat amerikai szolgáltató üzemelteti vagy üzemeltetteti.
„Azt szoktuk tanácsolni az ügyfeleinknek, hogy a saját kockázatértékelésüket figyelembe véve tekintsék át, mennyire felelnek meg az elvárásaik a jogszabályi környezetnek az egyes országokban. A szervezeteknek nagyobb átláthatóságot kell kiharcolniuk a cloudszolgáltatóktól adataik tárolásával kapcsolatban. A hagyományos IT-outsourcing esetében a döntés világosabb, de egy olyan modellben, ahol az adatok bárhol lehetnek, a megállapodásoknak is másoknak kell lenniük" – mondta *Denis Verdon,* a KPMG szakértője.

MDM vagy MAM

A mobil eszközmenedzsmentet támogató megoldások mind átfogóbban teljesítik a velük szemben támasztott követelményeket, és mind hatékonyabban képesek bevonni a mobilokat a központi felügyelet alá. Azonban az MDM-eszközök működését egyre inkább hátráltatja az a tény, hogy az alkalmazottak a saját okostelefonjaikat, táblagépeiket üzleti célokra is használják. Ekkor ugyanis a biztonsági óvintézkedések meghozatalát adatvédelmi megfontolások is jelentősen befolyásolják.

Az MDM akkor tudja a legjobb eredményt hozni, ha a vállalatok saját tulajdonban lévő eszközeit kell menedzselni. Ekkor ugyanis a készülékek esetleges távoli törlése, felügyelete, nyomon követése nem vezet olyan fokú adatvédelmi aggályokhoz, mintha a munkavállalók magántulajdonában lévő készülékeinek kontrolljára lenne szükség. Ez utóbbi esetben egy védelmi szempontból szükségszerű adattörlés a felhasználó saját adatait is megsemmisítheti, nem beszélve a készülékek folyamatos GPS-alapú nyomon követéséről, ami megint csak jogszabályokba ütközhet.

Egyre több biztonsági szakértő véli úgy, hogy a mobilok magán- és üzleti célra történő párhozamos használata miatt az MDM mellett a *MAM- (Mobile App Management)* megoldások szerepe jelentősen fokozódni fog. A mobilalkalmazás-kezelésre specializálódó technológiák ugyanis lehetővé teszik az

üzleti és a magáncélú alkalmazások, adatok hatékonyabb szeparálását, ezáltal a cégeknek lehetőségük nyílhat arra, hogy a felhasználók személyes adatainak érintetlenül hagyásával felügyeljék a készülékeket. A MAM egyik legfontosabb feladata, hogy a védelem fókuszát az eszközökről az alkalmazásokra, illetve az adatokra terelje.

Kacsingatunk a felhők felé

A mobiltechnológiák népszerűségének növekedése mellett a felhőalapú szolgáltatások is jelentős mértékben befolyásolják az adatok feletti kontroll megteremtését. A cloud computing üzleti szempontból számos előnyös jellemzővel rendelkezik, ami egyben azt is eredményezi, hogy a felhőalapú megoldások előbb vagy utóbb minden szervezet életében szerephez fognak jutni. Az üzlet ugyanis ki fogja kényszeríteni azt, hogy a költséghatékonysággal kecsegtető, egyszeri beruházásokat többnyire nem igénylő cloud megoldások helyet kapjanak a vállalatoknál, intézményeknél. A Ponemon Institute egy nem régi felmérésére hivatkozva úgy vélekedett, hogy jól körvonalazódnak azon trendek, amelyek azt támasztják alá, hogy a vállalatok mind nagyobb mennyiségben helyezik ki bizalmas adataikat a felhőkbe. Ráadásul ezek a tendenciák tartósnak bizonyulhatnak, ugyanis a felmérésben részt vevők egyharmada jelezte, hogy a következő két éven belül nagy valószínűséggel bizalmas adatokat fog kezelni cloudszolgáltatások bevonásával. Tehát haladunk afelé, hogy a cégek berkein belül oldódjon a „feszültség", és megfelelő óvintézkedések mellett elkezdődjön a vállalati adatok, illetve alkalmazások felhőkbe való intenzívebb kihelyezése.

Védelem a felhőkben

Amikor egy vállalat úgy dönt, hogy az adatait, alkalmazásait kihelyezi egy nyilvános, felhőalapú környezetbe, akkor hamar felmerül az igény a meglévő védelmi megoldások kiterjesztésére a felhők felé. Ennek az a legalapvetőbb magyarázata, hogy a cloudszolgáltatások esetében is biztosítani kell az adatok sértetlenségét, valamint hitelességét, a hozzáférés-szabályozást, a rendelkezésre állást, az SLA-kat, az incidenskezelést, a megfelelőségi követelmények maradéktalan betartását és nem utolsósorban a felhasználói biztonságtudatosság megteremtését.

A védelem kialakítása ugyanakkor számos nehézségbe ütközhet, már csak azért is, mert a megfelelő biztonsági szint eléréséhez mostantól két szereplő, a szolgáltató, valamint ügyfelének hatékony együttműködésére van szükség. Másfelől pedig a cloudszolgáltatásokhoz illeszthető biztonsági megoldások sokszor még csak gyerekcipőben járnak, így a megfelelő technológiai védelem kiválasztása is fejtörést okozhat.

A cloud környezetek felé való terjeszkedés során alapvető szerep hárul a titkosításra, ugyanis ezzel mind adatvédelmi, mind adatbiztonsági szempontból számos kockázatot lehet minimalizálni. Mindezt szerencsére a szervezetek egyre nagyobb számban felismerik. A Ponemon Institute egyik felméréséből az derült ki, hogy a felhőalapú szolgáltatásokat igénybe vevő vállalatok 35 százaléka még azelőtt felvértezi tikosítással az adatait, mielőtt azok elhagynák a belső hálózatot, vagyis a cloud rendszerekre már úgy teszik fel az állományokat, adatbázisokat stb., hogy azok védettek a jogosulatlan hozzáférésekkel szemben. A többi szervezet pedig vagy magában a cloud infrastruktúrában végzi a titkosítást, vagy azt teljes mértékben a szolgáltatójára bízza.

Kontroll nélkül nincs biztonság

Összefoglalásként elmondható: a mobil- és cloudtechnológiák térhódítása azt is jelenti, hogy a hagyományos védelmi megközelítések önmagukban már nem képesek helytállni. Ezért szükségszerűvé válik az eddigi védelmi intézkedések átgondolása és azok új kockázati tényezőkhöz, követelményekhez való igazítása. E nélkül az adatok feletti kontroll könnyen kicsúszhat a kezünkből.

PSZÁF: KOCKÁZATOK A FELHŐKBEN

A PSZÁF 2012 júliusában kiadott egy olyan vezetői körlevelet, amelyben a pénzintézetek figyelmét felhívta a közösségi és publikus felhőszolgáltatások igénybevételéből eredő kockázatokra. Ebben a dokumentumban a felügyelet többek között az ENISA (az EU hálózatbiztonsági szervezete), illetve a BSI (német információbiztonsági hivatal) biztonsági követelményei alapján számos olyan mérlegelendő szempontot tett közzé, amelyek megfontolása korántsem csak a pénzintézetek számára lehet hasznos. Néhány fontos gondolat a körlevélből a teljesség igénye nélkül:

– azt a folyamatot, amit az intézmény maga sem tud megfelelő kontrollok mellett biztonságosan működtetni, megfelelő kontrollok nélkül nem javasolt CSP-hez kiadni.

– az adattovábbítás és tárolás korszerű titkosítással történjen, emellett az adatokhoz való távoli hozzáférés (jellemzően interneten keresztül) korszerű azonosítótechnológián alapuljon.

– a főszerződés és az SLA vagy SLA-k folyamatos monitorozása és az aktív visszacsatolás garanciáinak megteremtése.

– a szolgáltatónak való kiszolgáltatottságot elkerülendő, fontos olyan feltételek meghatározása a szerződésben, amelyek nem nehezítik meg a szolgáltatóváltást.

– legyenek magas rendelkezésre állási kontrollok, kiváló DRP-készültség és erős incidenskezelési eljárások.

– független auditok a CSP üzleti és biztonsági érdekeinek figyelembevételével az ügyfél számára elérhetővé tett tartalommal.

– a felelősségi, biztosítéki szabályok precíz kidolgozása és a magyar jogintézményekhez való illesztése.

Forrás: http://www.pszaf.hu/data/cms2364896/vezkorlev_4_2012.pdf

HP STOREONCE D2D2T

Fájó pontok és a megoldások az adatmentésben

Válaszok az exponenciálisan növekvő adatmennyiség gyors, biztonságos, hatékony mentésének és helyreállításának kérdéseire.

Az elmúlt évtizedekben folyamatosan nőtt az előállított digitális információ mennyisége, melynek kezelése egyre nagyobb kihívás a vállalatoknak. A hazai cégeknél is kibontakozott egy új trend, az adatvagyon védelmének kezelése, ám ennek minősége közel sem egyenletes. A tapasztalatok szerint – mind a külföldi, mind a magyar vállalatoknál – e téren komoly üzemeltetési nehézségek figyelhetők meg – összegezte *Molnár Zoltán,* a HP adatmentési szakértője.

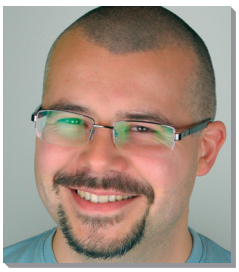
Ezek egyik legfontosabb fájó pontja a mentési ablak problémája. Vagyis az, hogy miközben egyre nő a mentendő adattömeg, ennek az „ablaknak" a mérete változatlan maradt. Kihívás a visszaállítási idő minimalizálása, illetve a mentések végrehajtásának stabilizálása is. Ezek elsősorban a szalagos adattárolásból adódó nehézségek, amelyekre a válasz nem a bevált szalagos technika elhagyása, hanem annak célirányos kiegészítése, támogatása. A HP szerint a szalagos adatmentést a folyamat végére kell helyezni, a köztes kihívásokra – holtidő minimalizálása, mechanikai kockázatok megszüntetése, azonnali adathozzáférés stb. – pedig a diszkalapú mentés a válasz. A strukturálatlan adatok mentésében ez nagyságrendekkel gyorsabb megoldást jelenthet – ráfordított időben, pénzben, energiában –, miközben a véges kapacitásra a deduplikáció (D2D), vagyis az ismétlődő adatcsoportok egyszeri tárolása a válasz.

Deduplikációval megoldódnak az olyan problémák is, mint a több adatközpontos mentési rendszerekhez szükséges nagy sávszélesség vagy az adatok fizikai szállításának kockázatai (károsodás, elvesztés) és a távoli telephelyek mentési megoldásai, hiszen ezekre a Hewlett-Packard mérései szerint akár néhány megabites – azaz költséghatékony – átlagos hálózati kapcsolat is elegendő lehet. Az adat-deduplikáció, illetve az ilyen adatok keskeny sávszélességű replikációja emellett megszünteti az irodánkénti helyi karbantartási igényeket is, és centralizálttá teszi a telephelyek menedzselését, csökkentve az elosztott szakemberi erőforrás szükségességét.

Sokszor kihívást jelent a virtualizált környezetek adatmentési és helyreállítási feladatainak ellátása is, holott a két probléma gyökere azonos. A virtualizáció ugyanazt jelenti a számítási erőforrásoknál, mint a deduplikáció a backup esetében: 20-30-szor hatékonyabb üzemeltetést. A virtuális gépek klónozása miatt itt még magasabb lehet a deduplikáció aránya, az image-ekből pedig akár objektum szintű helyreállításra is lehetőség nyílik. A HP StoreOnce deduplikációs (D2D), szalagos és diszkes megoldása másodpercekre csökkentheti az üzletkritikus alkalmazások mentési idejét. Tehát ebben a megoldásban a HP megtartja a jól bevált szalagos mentést, de optimalizálja és gyorsabbá teszi diszkes mentési kiegészítéssel, így alkotva ezáltal az új D2D2T stratégiát. ■

Vállalati hírszerzési szolgáltatások...

Az apró, Facebook-profilokból, vállalati blogokból, Twitter-bejegyzésekből származó információmorzsák összerakosgatásával olyan részletes kép rajzolódik ki egy-egy vállalatról, amelynek megszerzéséhez korábban komoly hírszerzési munkára volt szükség. A vállalatok egyre nagyobb része él is a lehetőséggel, konkurensei után kémkedve a közösségi terekben...



SZILÁGYI SZABOLCS

Careless talk cost lives – hirdette a második világháborús brit plakát, amely arra hivatott felhívni a szigetországbeliek figyelmét, hogy lehetőleg ne fecsegjenek semmilyen, az ország védelmével kapcsolatos információról nyilvánosan. Noha – szerencsére – a háborúskodást Európa java már rég maga mögött hagyta, az immár hetvenéves intelem ugyanúgy érvényben van, csak egy egészen más színtéren: a cégek konkurenciaharcában. Az ipari kémkedés ugyan nem dönt nyomorba nemzeteket, de komoly pénzügyi veszteséget/nyereséget képes okozni, nézőponttól függően. Nem csoda, hogy a technológia és az ügyfélkor iránt való érdeklődés évszázados hagyományokkal bír. Az pedig semmit sem változtat az alapokon, hogy immár a 21. században élünk – csak az eszközök haladnak a korral.

A vállalatok már évek óta használnak olyan eszközöket, mint a HootSuite vagy a Radian 6, hogy figyelemmel kísérjék, mit mondanak róluk az emberek a közösségi médiában. Ez a megfigyelési szokás azonban idővel finomodott, célt változtatott: most már nemcsak arra keresnek választ a cégek, hogy általánosságban milyen vélemény alakult ki róluk, de a riválisukról alkotott képről is minél többet akarnak tudni –, árulta el *Richard Plansky.* A New York-i szakértő vezető tisztséget tölt be a Kroll kockázatelemző cégnél, amely egyebek mellett „vállalati hírszerzési" szolgáltatásokat is nyújt.

„A közösségi hálózatokon korábban inkább magánjellegű, nyilvánosságtól elzárt-eltitkolt információk is egyre inkább felbukkannak. Ez jóval egyszerűbbé teszi a vállalati tevékenységről szóló információk összegyűjtését és rendszerezését, melyhez régen megfigyeléssel jutottunk hozzá. Manapság már közvetlenül a számítógépünkről megtehetjük ugyanezt" – foglalta össze Plansky.

Mi számít értékes információnak?

Termékadatok, terméktesztelések, promóciós ajánlatok, gazdasági adatok, munkaerő-toborzási tevékenységek, elbocsátások, ipari demográfiák, felhasználói elégedettségi szintek – csak néhány azon adatok közül, amelyeket alig pár forrás (Facebook-profilok, Twitter- és blogbejegyzések) figyelésével meg lehet szerezni. Ugyan

ezek az információmorzsák önmagukban közel értéktelennek tűnnek, de ha összerakjuk az apró részeket, azokból igen jó képet lehet alkotni egy-egy vállalatról –, erősítette meg Plansky megállapítását *Shane MacDougall,* a kanadai Tactical Intelligence tanácsadó cégtől.

A kiszivárogtatás ellen lehet és kell is tenni, de dőreség lenne azt gondolni, hogy erővel, szigorral maximális eredményt lehet elérni. Ugyanis hiába rendszabályozza meg a cég a közösségi média iránt rajongó alkalmazottjait, ha nem csak tőlük jut ki bizalmasnak szánt információ. A vállalatok jó része kvázi „maga" is hozzájárul a könnyebb megfigyelhetőséghez azzal, hogy olyan adatokat tesz közzé, mint az értékesítési dokumentumok, konferenciabemutatók vagy a cég saját weboldalán tárolt, ámde rosszul-elégtelenül titkosított információk.

Közösségi kémkedés a gyakorlatban

Lássunk egy példát, hogy közérthetőbb legyen az egész! Egy startup vezetője riválisának üzleti modelljére vonatkozó kérdést tett fel a Quora közösségi kérdezz-felelek oldalon. Arra volt kíváncsi, hogy legerősebb konkurense hogyan képes az ő cégénél nagyobb haszonra szert tenni. Ez amolyan végső, szinte már elkeseredett próbálkozás volt, amit egy hosszas – eredménytelen – online keresgélés előzött meg. Alig néhány nap telt el, amikor a kiszemelt vállalat egyik üzletfejlesztési vezetője saját maga adott választ, természetesen anélkül, hogy tudta volna: versenytársának árulja el a titkokat.

Vagy egy másik technika: a fenti példában szereplő startup vezetője – akinek a példák alapján igencsak sok szabadideje lehet – azzal is „múlatja idejét", hogy versenytársai ügyfeleire „vadászik" Twitteren keresztül. Állítása szerint sokat meg lehet tudni a konkurenciáról, ha azok felhasználóinak teszünk fel olyan kérdéseket, mint: miért nem tetszett egy bizonyos termék vagy mit kedvelt benne.

Nem elég az adatgyűjtés

Noha a fecsegő szájak „életekbe kerülhetnek", de a részletek mit sem érnek, ha a megszerzett információdarabkákat nem tudja összeilleszteni a kíváncsiskodó. A versenytársakról való hírszerzés nem csupán adatgyűjtés, végül szükség van egy igazán jó elemzésre, ami rávilágít a konkurencia gyengeségére-erejére. Ennek ismeretében már gyorsabban és jobb döntést lehet hozni, mint a riválisok –, véli *Leonard Fuld,* a massachusettsi vállalati hírszerzéssel foglalkozó Fuld and Co. alapító-tanácsadója. Ezzel a megállapítással Plansky is egyetértett, aki szerint jóval több rejlik tevékenységükben pár Twitter-account figyelésénél és néhány fontos név interneten való rákeresésénél. A titok a szakképzett vizsgálatban és az „ösztönökre hallgatásban" rejlik –, állítja a szakértő. Éppen ezért nem érdemes tapasztalatlanul belevágni: sokat ugyan nem veszít a kíváncsiskodó, csak az idejét, ám azt jobban is beoszthatja úgy, hogy közben a „kémkedés" feladatát külső szakértőkre bízza. Nekik ugyanis nem csupán ez a munkájuk, de rendelkeznek az ehhez szükséges megfigyelőeszközökkel és betekintést nyernek szinte mindenféle-fajta információhalmazba és forrásba.

Gondoljunk az etikai kérdésekre is! Egyes helyzetekben elég egyértelmű lehet, hol a határ, más szituációkban viszont sokkal elmosódottabbak a vonalak.

Lebeszélni természetesen senkit sem akarunk, hiszen a lehetőségek tárháza igen széles. Aki a „csináld magad" mozgalom elkötelezett híve, azt több száz, közösségi médiát megfigyelni képes eszköz „várja", hogy képet alkothasson akár saját cégéről, akár riválisairól. A Radian 6 például több mint 100 millió, különböző közösségi hálózatokban található oldalt követ nyomon, azzal kecsegtetve a hozzá forduló kíváncsiakat, hogy valós időben képes számukra információt szolgáltatni versenytársaik termékbejelentésétől kezdve egészen az őket érő ügyfélkritikákig. Alternatívát jelent a Lithium névre keresztelt megfigyelőeszköz, amellyel a vállalatok felkutathatják a róluk szóló online véleményeket. Ezeket az eredményeket aztán benchmarknak vethetik alá versenytársaik hasonló megjelenéseivel, képet alkotva arról, hogy hol is helyezkednek el egymáshoz képest, az internetes megjelenések alapján.

Természetesen, ahogy a kínált szolgáltatások is széles körűek, úgy az áruk is tág spektrumon mozog. Lehet találni teljesen ingyen használható eszközöket, de akár havonta több száz dollárba kerülő, előfizetéses modellre alapuló megoldásokat is választhatnak az érdeklődők.

Túl sok az információ

Legyen szó akár ingyenes, akár fizetős szolgáltatásról, saját megoldásról vagy külső partner bevonásáról, a közösségi hálózatok bányászatának legnehezebb része a túl sok információ kezelése. A kihívást ugyanis nem az adatok megtalálása jelenti, hiszen azok relatíve könnyen elérhetők. A kihívás abban rejlik, hogy túl sok információ áll rendelkezésre. Tudni kell elválasztani a búzát a ocsútól, ez a kulcsa a sikeres „közösségi kémkedésnek" –, állítja Plansky.

Mint szinte mindenhez, ehhez is a jól átgondolt terven keresztül vezet az út. Kritikus fontosságú, hogy a konkurenseire kíváncsi vállalat meghatározza, milyen jellegű információhoz szeretne hozzáférni, és ami talán még ennél is fontosabb: a megszerzett adatokkal mihez kezd. El kell dönteni, melyek a kulcsfontosságú adatok, és melyek azok, amelyekre jelenleg nincs szükség. Például egy felhőbevezetés esetén nem érdemes a konkurensek teljes feltérképezésére költeni, sokkal inkább az olyan információkat kell követni, mint például a riválisok ügyfeleinek reakciói a cloudszolgáltatásokra és a termékfunkciókra. Ezzel számos problémára rá lehet világítani, aminek tudatában a mások számára megélt-megszenvedett buktatók elkerülhetők (vagy legalább fel lehet rájuk készülni).

Etikai kérdések

Cikkünk zárásaként érdemes pár szót szánni az etikai kérdésekre is. Egyes helyzetekben elég egyértelmű lehet, hol a határ – az már annál kevésbé, hogy vajon átlépi-e azt a kíváncsiskodó, saját cége érdekében –, más szituációkban viszont sokkal elmosódottabbak a vonalak. Például hamis Facebook-profilt létrehozni abból a célból, hogy azzal aztán bejelölje versenytársát a kémkedni vágyó a közösségi hálózatban, teljes mértékben etikátlan. De a versenytárs Twitter-csatornáján elégedetlen ügyfelekre vadászni vajon még elfogadható? Ezeket a kérdéseket mindenkinek magának kell megválaszolnia...

IT-KONZUMERIZÁCIÓ

Munkavállalók, hozott eszközökkel

KIS ENDRE

A saját célra vásárolt okostelefonokat és táblagépeket mind többen használják munkavégzésre is. A vállalati környezet konzumerizációjaként ismert trend a hatékonyság növekedését eredményezheti. A szabad eszközválasztás, az üzleti és a magánéletben használt alkalmazások vegyítése azonban első ránézésre úgy hat, mint az IT-biztonságról és a felhasználók támogatásáról alkotott eddigi kép éles ellentéte.

A Cisco *Bring Your Own Device – Device Freedom Without Compromising the IT Network* című fehér könyvében Borderless Network alapú, átfogó BYOD megoldásarchitektúrájának ismertetése mellett azt taglalja, hogy a konzumerizáció támogatására készülő informatikai szervezet miként nőhet fel a feladathoz.

Az eddigi gyakorlat szerint az IT-osztály előre meghatározta a vállalatnál használható támogatott klienseszközök – asztali és hordozható számítógépek, esetleg mobil- és okostelefonok – körét, amelyből az alkalmazottak legfeljebb választhattak, ha erre egyáltalán lehetőséget kaptak.

Az alkalmazottak által saját célra vásárolt eszközök munkahelyi használatának engedélyezése *(bring your own device,* azaz hozd a saját eszközöd, amit HSE-ként rövidítheténk) másfajta megközelítést követel. A lakosság körében népszerű okostelefonok és táblagépek olyan gyorsan fejlődnek, hogy minden egyes számításba jöhető eszköz előzetes jóváhagyása aligha kivitelezhető. Az IT-szervezettől az sem várható el, hogy az alkalmazottak által behozott eszközök, márkák és modellek mindegyikéhez ugyanolyan szintű támogatást adjon. A járható út az lehet, ha az informatikai osztály házirend, szabályok szintjén zárja ki azt a kategóriát vagy márkát, amelyet biztonsági vagy más okokból nem engedélyez, a többi eszközhöz pedig nagyrészt önkiszolgáló támogatási modelleket dolgoz ki.

Szabadság és biztonság

A felhasználói szabadság mértéke fordítottan arányos a vállalati IT-biztonság szintjével, legalábbis hajlunk arra, hogy a kettő viszonyát ilyennek ítéljük. A munkavégzésre használható eszközök megválasztása terén azonban a vállalat nagyobb szabadságot adhat alkalmazottjainak anélkül, hogy ezzel aláásná a biztonságot.

Az IT-osztály meghatározhatja azokat a minimális biztonsági követelményeket, amelyeket minden mobileszköznek teljesítenie kell ahhoz, hogy hozzáférést kapjon a vállalati hálózathoz, és ellenőrizheti, kikényszerítheti a szabályok betartását. Ilyen előírás lehet például a szoftverfrissítések és biztonsági szoftverek telepítése és naprakészen tartása, a nem engedélyezett alkalmazások, beépülő szoftvermodulok eltávolítása. Az azonosságkezelés, a hálózatra bejelentkező eszköz és a felhasználó azonosítása ugyancsak kulcsfontosságú a biztonság szempontjából.

Ezzel együtt a vállalati hálózaton első ízben megjelenő eszközök csatlakoztatását minél gördülékenyebb folyamattá kell tenni. Ideális esetben ehhez nincs szükség kliensszoftver előzetes telepítésére az eszközön, és a folyamat lépésein a felhasználó önállóan is végig tud menni. A vállalat így nemcsak alkalmazottjainak, hanem a telephelyére látogató vendégeknek, partnereknek és ügyfeleknek is hasonló eleganciával adhat hálózati hozzáférést. Vészhelyzetben azonban – például az eszköz elvesztése vagy ellopása esetén –, az alkalmazott cégtől való távozásakor vagy akár más pozícióba kerülésekor az IT-osztálynak a lehető leggyorsabban lépnie kell, ezért a hálózati elérés megvonását érdemes ugyanolyan egyszerűvé tenni, mint az új eszközök beléptetését.

Mivel a felhasználók ugyanazon az eszközön érik el az üzleti és a magánéletben használt alkalmazásokat, a szabályozásnak különbséget kell tennie a két terület között (erre még visszatérünk), és ha a vállalatnak tanúsítania kell a törvényi megfelelést, az auditálás folyamatát is segítenie kell. A személyi tulajdonban levő eszközök esetében ez bonyolultabb, mint a vállalat által adott és teljes egészében felügyelt eszközökön.

Az IT-osztálynak megfelelő eszköztámogatásra lesz szüksége ahhoz, hogy hatékonyan felügyelhesse és támogathassa az okostelefonok és táblagépek munkahelyi használatát. Az alkalmazottak korábban jellemzően egy asztali vagy hordozható PC-n dolgoztak, ezért amikor az IT-osztálytól kértek segítséget, elég könnyű volt megtalálni gépüket a hálózaton. A munkahelyi környezet konzumerizációjának velejárója, hogy egy-egy alkalmazott egyszerre több eszközzel is csatlakozik a vállalati hálózatra. Az okostelefonok és táblagépek egyszerre többféle – vezetékes, Wi-Fi, 3G/4G – hálózati üzemmódot is támogathatnak, amelyek között át is válthatnak. Az eszközök láthatóvá tétele a hálózatokon az IT-menedzsment szempontjából kulcsfontosságú feladat.

Miután a céges hálózatra csatlakozó eszközök száma ugrásszerűen megnő, a vállalat IP-cím készlete is gyorsan kimerülhet, így a vártnál hamarabb szükség lehet az IPv6 protokoll használatára való áttérésre, a hálózat peremén és házon belül egyaránt. Az okostelefonok és táblagépek munka jellegű használatával az irodai vezeték nélküli hálózat szerepe is megváltozik, kényelmi szolgáltatásból üzletkritikussá válik, így az IT-osztálynak az addiginál magasabb szolgáltatási szintet kell biztosítania.

Alkalmazási stratégiák

A különböző területeken működő vállalatok eltérő mértékben fogják támogatni a munkahelyi környezet konzumerizációját, azonban ki kell dolgozniuk az erre vonatkozó stratégiát, még akkor is, ha az továbbra is csak az IT-osztály által jóváhagyott és felügyelt eszközök használatát fogja engedélyezni.

A szigorúan szabályozott, pénzügyi, kormányzati és más területeken tevékenykedő szervezetek inkább korlátozó, az érzékeny adatok védelmét mindenek fölé helyező stratégiát fognak kidolgozni. A vállalatok többsége azonban a hozott eszközök használatát jobban megengedő vagy azt egyenesen szorgalmazó modellt fog követni. Az eszközválasztás szabadságát az alkalmazáshasználat korlátozá-

sával ötvöző stratégiát éppúgy alkalmazhat a vállalat, mint a szabályalapú biztonsági intézkedések mellett az eszközök széles palettájáról sokkal nagyobb hozzáférést engedő megközelítést. Olyan vállalatok is lesznek, amelyek a nagyobb hatékonyság és versenyképesség reményében házon belül fejlesztett alkalmazásaikat először okostelefonokra és táblagépekre készítik el, és a lehető legtöbb eszköz használatát engedélyezik.

Bármilyen mértékben nyitja meg a vállalat IT-környezetét az alkalmazottak által hozott eszközök előtt, az érzékeny adatok védelméről mindenképp gondoskodnia kell. Az adatbiztonság szempontjából fontos döntés, hogy a felhasználók miként – natív módban vagy böngészőből, illetve virtualizálva – fogják elérni az üzleti alkalmazásokat okostelefonjukon és táblagépükön.

Natív módban az eszközre telepítve egy mobilkliens program fut, amely közvetlenül kommunikál a vállalat vagy a felhőszolgáltató adatközpontjában működő alkalmazással. Ez a felállás biztosítja a legnagyobb teljesítményt és a legjobb felhasználói élményt. Az üzleti alkalmazás ugyanúgy működik az eszközön, mint a többi app, így az okostelefon vagy táblagép képességei a lehető legteljesebb mértékben hasznosíthatók. Az adatok az eszközre is lementhetők, ilyenkor az alkalmazás offline, hálózati elérés nélkül is használható.

A böngészőalapú megközelítés annak köszönheti népszerűségét, hogy az alkalmazásokat hordozhatóvá teszi a különböző eszközök és operációs rendszerek között. Kevésbé gazdag felhasználói élményt ad, mint a natív mód, ugyanakkor ahhoz hasonlóan itt is hátrányt jelent, hogy az adatkommunikáció közvetlen, és az adatok lementhetők az eszközre – az adatbiztonság így sérülhet, és fennáll az adatvesztés kockázata.

Virtuális módban ezzel szemben az alkalmazás a vállalat vagy a felhőszolgáltató adatközpontjában, virtualizált környezetben fut, és azt egy VDI-kliens jeleníti meg a mobileszközön. Más szóval, csak kijelzőinformációk utaznak a hálózaton, az adatok nem kerülnek az eszközre. Ez a módszer kínálja a legmagasabb szintű adatbiztonságot, ami azonban a felhasználói élmény, a teljesítmény és a válaszidők rovására mehet.

Miután mindhárom megközelítésnek vannak előnyei és hátrányai, a vállalatok hibrid modell mellett is döntenek, amelyben a natív módban futó kliensalkalmazásokat kevésbé kritikus alkalmazásokhoz, míg az alkalmazásvirtualizálást a legérzékenyebb adatok kezeléséhez használhatják.

A munkavégzéshez azonban az üzleti alkalmazások és adatok elérése mellett az együttműködést támogató eszközök – telefon-, video- és konferenciahívás, üzenetküldés, tartalommegosztás és jelenlét-érzékelés – használata is szükséges. A vállalat konzumerizációs stratégiájának ezért meg kell határoznia, hogy az alkalmazottak, valamint a velük kapcsolatban álló partnerek és ügyfelek miként érhetik el ezeket a szolgáltatásokat okostelefonjukon és táblagépükön.

Szerződésbe foglalva

Jóllehet nem a hálózati architektúra vagy a szabályalapú felügyelet része, a konzumerizáció sikeres támogatásához azonban ugyanúgy elengedhetetlen a jól átgondolt, a személyes tulajdonban levő eszközök munkahelyi használatának feltételeit rögzítő, és az alkalmazottakkal előre tisztázott végfelhasználói szerződés elkészítése.

Az üzleti adatok védelme érdekében az IT- osztálynak akkor is cselekednie kell, ha az alkalmazott elhagyja mobileszközét, vagy ellopják tőle, illetve amikor a munkavállaló kilép a cégtől.

A vállalatvezetésnek és az IT-osztálynak a vonatkozó jogszabályokkal is meg kell ismerkednie, mielőtt meghatározná az eszközhasználat szabályait az üzenetküldéstől kezdve a böngészésen át az alkalmazásletöltésig és tartalomtárolásig. Azt is egyértelművé kell tenni, hogy milyen korlátozások lépnek életbe munkaidőben, illetve amikor az eszköz a vállalati hálózatra csatlakozik, és az IT osztály a kommunikáció mely formáit fogja monitorozni.

A cég például tartalomszűrővel korlátozhatja a vállalati hálózatról elérhető weboldalak körét. Az okostelefonok és táblagépek azonban közvetlenül is elérik az internetet nyilvános Wi-Fi vagy 3G/4G kapcsolaton keresztül, amelyre nem terjeszthető ki a korlátozás, ha az alkalmazott saját tulajdonban levő eszközt használ munkaidőn kívül. Hasonló módon a személyes jellegű üzenetküldés és tartalommegosztás szabályozása is gondos mérlegelést kíván ebben a felállásban.

Az üzleti adatok védelme érdekében az IT-osztálynak akkor is cselekednie kell, ha az alkalmazott elhagyja mobileszközét, vagy ellopják tőle, illetve amikor a munkavállaló kilép a cégtől. Az ilyen helyzetekben alkalmazott módszer a távoli törlés, minden adat, tartalom és alkalmazás eltávolítása, az eszköz „téglává" változtatása. Milyen kellemetlen meglepetés éri azonban a felhasználót, ha csak utólag jön rá, hogy magáncélra vásárolt eszközének munkahelyi használatával ehhez, vagy magánjellegű üzenetváltásainak monitorozásához is hozzájárult. Előfordult már, hogy egy-egy hasonló incidens miatt a munkáltató és a munkavállaló a bíróságon kötött ki.

A végfelhasználói szerződés körültekintő kidolgozásával és a feltételek egyértelmű kommunikálásával a felek elejét vehetik az ilyen pereskedésnek. Célszerű azonban, ha a felhasználó a munkavégzésre is használt okostelefonján vagy táblagépén tárolt személyes adatokról és tartalomról rendszeresen biztonsági mentést készít egy külső, fizikai vagy felhőben elérhető tárolóra – a konzumerizáció nem egyedül a vállalati IT-osztály számára tartogat kihívásokat.

HARDVER KÖZELI BIZTONSÁG

Mélységi vírusvédelem

Egyre több olyan kártékony program terjed, amely felismerése jelentős megpróbáltatások elé állítja az antivírus alkalmazásokat. Az egyik megoldást a hardver, illetve processzor szintű védelem szolgáltathatja.

KRISTÓF CSABA

Önmagukban már nem képesek helytállni napjaink egyre kifinomultabb kártékony programjaival szemben a hagyományos vírusvédelmi technológiák, ezért újak bevezetése vált szükségessé. Ebből a szempontból a cloud copmuting és a hardver közeli biztonság is fontos szerephez jut.

A cloud computing alapú vírusvédelmi technológiákkal bizonyos értelemben szöges ellentétben állnak azok a megoldások, amelyek kiemelten kezelik a hardvert mint védelmi réteget. Miközben a felhős eljárások a biztonsági feladatok egy részét egyre távolabb viszik a védendő számítógépektől, eszközöktől, aközben a hardver szintű biztonság nagyon is mélyére hatol a rendszereknek. Egyes vírusvédelmi cégek ugyanis úgy vélik, hogy a biztonság megteremtését nem lehet kizárólag az operációs rendszer szintjén végezni, hiszen olyan károkozók, rootkitek is akadnak, amelyek a BIOS, az MBR stb. megfertőzésére is képesek, és még azelőtt aktivizálódnak, mielőtt az operációs rendszer szóhoz juthatna.

BARNA TAMÁS

rendszermérnök
McAfee

Segítenek a chipek

A processzoralapú vírusvédelem és biztonságmenedzsment területén a McAfee az Intel technológiáinak, erőforrásainak felhasználásával fontos fejlesztéseket végzett, és egy évvel ezelőtt bejelentette a Deep Defender, valamint a Deep Command technológiáit. *Barna Tamást,* a McAfee rendszermérnökét e technológiák elmúlt egyéves fejlődéséről kérdeztük.

COMPUTERWORLD: Milyen tapasztalatokat sikerült leszűrni a két hardver közeli biztonsági technológia, a Deep Defender és a Deep Command eddigi pályafutása alatt?

BARNA TAMÁS: A biztonság mára elengedhetetlen részévé vált az internetes hozzáféréssel rendelkező végpontoknak. Lassan minden egyes termék, amely IP-n keresztül kommunikál, végpontként kezelendő. A tapasztalat egyértelműen az, hogy bizonyos támadástípusok észleléséhez, és persze az ezt követő kivédésükhöz mindenképpen szükséges a fizikai és az alkalmazói szintek közelebb hozása egymáshoz. A hardveresen beépített biztonsági szolgáltatások használata napjaink egyik legfontosabb kérdése a hatékony és proaktív védekezés szempontjából. Nem utolsósorban pedig a biztonsági kérdések mellett e technológiák használatán keresztül sokkal hatékonyabb üzemeltetést lehet megvalósítani. Különösen elosztott, több telephelyes, távoli kapcsolattal rendelkező hálózatok esetében – ezzel csökkentve a karbantartási időablakokat és egyben növelve az úgynevezett Green IT jellegű folyamatokat a kevesebb energiafelhasználás révén.

CW: Melyek azok a fenyegetettségek, kockázati tényezők, amelyek kezelésében a Deep Defender processzoralapú megközelítésével segítséget tud nyújtani?

B.T.: Elsősorban a memóriában futó valós idejű, kernelalapú rootkitek. Ezek detektálása szinte lehetetlen az alkalmazói szinten, ahol a vírusvédő vagy végponti behatolásmegelőző programok működnek. A kernelalapú rootkitek sokszor saját, rosszindulatú boot loader meghajtóként futnak az I/O folyamatok részeként, amelyek már régen betöltődtek a gép indulása során. Nem véletlenül mondják, hogy egy számítógép az indulása során a legsérülékenyebb. A Deep Defender képes, mint védett, elsődleges boot loader driverként futó alkalmazás, ellenőrizni a többi boot loadert, és kiszűrni a káros vagy a rendszer működése szempontjából lényegtelen meghajtók betöltését. Emellett a detektálás, blokkolás tényéről információt szolgáltat a McAfee Global Threat Intelligence felhőalapú, reputációs elven működő adatbázis felé, amely proaktívan képes az alkalmazói szinten futó programokat értesíteni a káros eseményekről.

CW: Miként segíti elő a biztonságmenedzsmentet a Deep Command integrálása az ePO környezetekbe?

B.T.: Az üzemeltetési és karbantartási folyamatok sokkal hatékonyabban és gyorsabban megvalósíthatók egy központi menedzsmentkonzol alól. Ezek a folyamatok szerves részét képezik a biztonsági kérdéseknek, hiszen azonos felügyeleti konzol esetében sokféle korreláció elvégezhető. Sok fertőzés esetében csak az adott gép újratelepítése lehet megoldás. A Deep Commanddal ez elkerülhető, és számos remediációs folyamat távolról, a gép bekapcsolása nélkül elvégezhető.

CW: Vannak-e elképzelések arra vonatkozóan, hogy a McAfee e technológiái az AMD processzorok esetében is elérhetővé válnak?

B.T.: Egyelőre biztosan nincsenek, mert a McAfee 100 százalékban Intel-tulajdonban működik mint önálló leányvállalat. A hardveres szinten futó biztonsági megoldásaink pedig teljes mértékben támaszkodnak az Intel által fejlesztett, a chipsetben megtalálható biztonsági modulokra, amelyekre közös fejlesztői együttműködés keretében hozzuk létre a megoldásainkat.

IDC
Analyze the Future

PIACELEMZÉS

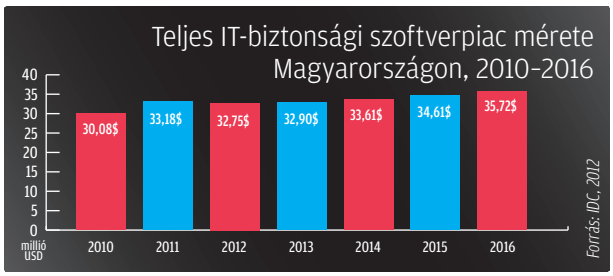
Védekezni szükséges

Az IT-biztonsági szoftverek lakossági piacát szinte teljes egészében az ingyenes megoldások uralják Magyarországon. A vállalati szegmensben az egyes termékkategóriák eltérően teljesítenek, de kivétel nélkül növekedni tudtak – legalábbis mostanáig.

KIS ENDRE

A biztonsági szoftverek piacát az International Data Corporation (IDC) négy fő termékkategóriára – jogosultság- és hozzáférés-kezelő, tartalomvédő és fenyegetéskezelő, sérülékenységkezelő, valamint az egyéb besorolású szoftverek csoportjára – osztja. A piac legnagyobb szeletét a tartalomvédelem és fenyegetéskezelés adja, amelyet a piacelemző további négy alkategóriára – hálózatbiztonság (tűzfalak, például a hazai BalaBit Zorp terméke), végpontbiztonság (a kliensgépekre telepített antivírus és más biztonsági szoftverek), üzenetkezelés-biztonság (levélszemétszűrők) és webbiztonság – bontja.

Az IDC adatai szerint a biztonsági szoftverek piaca 2011-ben 10,03 százalékkal 33,18 millió dollárra nőtt. Ez szép, a várakozásokat kissé még felül is múló teljesítmény, de történeti összehasonlításban nem túl kiemelkedő; a piac mérete 2008-ban még 38 millió dollár körül alakult. Bár a felhasználók az IT-biztonságot érthető módon kiemelten kezelik, a gazdasági válság hatása ezt a piacot sem kerüli el. Az utóbbi 2-3 évben azonban élesen eltérő trendek tapasztalhatók a lakossági és vállalati szegmensben.



– Az ingyenes vírusvédők, mint például az AVG és az Avira, kezdetben korlátozott funkcionalitást kínáltak, ez azonban már a múlté – mondta *Fauszt Gábor,* az IDC Hungary vezető elemzője. – A Microsoft Security Essentials csomagja a lakosság mellett 50 felhasználóig a kkv-k számára is ingyenes, System Centerből menedzselhető megoldást ad. A helyzetet az árháború fokozta, amelyet az Eset indított a NOD32-vel. Mindezt a jelentős engedményekre kényszerülő, piacvezető Symantec is megsínylette.

A lakossági szegmensben a fizetős biztonsági szoftverek piaca mára gyakorlatilag megszűnt. A Windows tűzfala is felnőtt a feladathoz, a 8-as verzióba a Microsoft már beépíti biztonsági szoftvereit, így azokat külön telepíteni sem kell. Tekintettel a Windows 90 százalék feletti penetrációjára az operációs rendszerek lakossági piacán, az IT-biztonsági szállítók itt már aligha számíthatnak licenc- és előfizetési díjakból befolyó, különösebb bevételekre.

Biztonság készülékekben...

Az IT-biztonsági szoftverek piacának növekedéséhez így a közép- és nagyvállalatok adtak hajtóerőt.

– Az első belépési ponton a vállalatok általában valamilyen egységes fenyegetéskezelést (UTMS), tűzfal vagy VPN készüléket telepítenek hálózatuk védelmére – mutatott rá Fauszt Gábor. – Ez az átállás, amely gyártói oldalon is lemérhető például a CheckPoint esetében, szintén közrejátszott abban, hogy a szoftveres megoldások piaca veszített lendületéből. A mindent egyben tartalmazó készülékek népszerűsége azonban érthető. Többe kerülnek ugyan, mint a tisztán szoftveres megoldások, viszont karbantartási díjuk alacsonyabb, és üzemeltetés szempontjából szinte semmilyen feladatot nem adnak, így a beruházás már két év alatt megtérülhet.

A biztonságiappliance-piac tavaly darabszámot tekintve több mint 10, szállítói bevétel alapján közel 30 százalékkal nőtt. Egy ilyen készülék telepítése mellett azonban házon belül is adódik bőven feladat, amelyhez a vállalatnak megfelelő biztonsági szoftvert szükséges bevezetnie.

– Különösen így van ez az érzékeny információkkal dolgozó, illetve megfelelőségi követelmények teljesítésére kötelezett vállalatok esetében – fejtette ki az elemző. – A jogosultság- és hozzáférés-kezelést például nagyon komolyan kell venniük, amit a kategória 10 százalékos növekedése is tükröz. Mára a virtuális gépek védelme is fókuszba került. Ennek eszközeit a tartalomvédelem és fenyegetéskezelés főkategóriába soroljuk, amely tavaly mintegy 5 százalékkal, 21,3 millió dollárról 22,2 millióra nőtt. Ebben az is közrejátszott, hogy az ugyancsak ide tartozó antivírus programokra a nagy klienskörnyezettel rendelkező szervezetek, például a kormányzati szféra intézményei továbbra is jelentős összegeket költenek. A végpontbiztonsági szoftverek piaca így a lakossági szegmens kiesése ellenére is nőtt, 11,96 millió dollárról 12,25 millióra.

...és a felhőben

A növekedés üteme kategóriánként ugyan eltérést mutat, de az IT-biztonsági szoftverek piacán alapvetően mindegyik terület nőni tudott.

– Az üzenetkezelés biztonságát szolgáló szoftverek alkategóriája 4,3-ról 4,6 millió dollárra bővült – mondta Fauszt Gábor. – Azok a vállalatok, amelyek ezt megtehetik, mert nem kötik őket például megfelelőségi követelmények, a levelezést elsőként viszik a felhőbe, ami a hostingszolgáltatók körében növeli a beruházások mértékét. A nyilvános felhőben elérhető szolgáltatások, a Google Alkalmazások és az Office 365 növekvő népszerűsége azonban valamelyest visszafogja a növekedés ütemét. A sérülékenységkezelő eszközök szelete, jóval a piaci átlagot meghaladva, 2,8 millió dollárról 3,3 millióra nőtt, ami mutatja, hogy a gyártók és a felhasználók egyaránt kiemelten kezelik ezt a területet. Az egyéb kategória robbanásszerűen, 0,8-ról 0,96 millió dollárra nőtt, elsősorban az okostelefonokra telepíthető biztonsági szoftverek iránti keresletnek köszönhetően. Ez a trend csak erősödni fog, idén már 1,2 millió dollárra, közel 30 százalékos növekedésre számítunk ezen a téren.

Ezzel együtt az IDC előrejelzése szerint az IT-biztonsági szoftverek piaca a kedvezőtlen gazdasági környezetben idén összességében 1,3 százalékkal csökkenni fog, és a jövő évi stagnálást követően, 2014-től indulhat ismét növekedésnek.

Kidumált információk

MEIXNER ZOLTÁN

A Data Breach Investigations Report – amelyet a Verizon szakemberei az adatok biztonsági helyzetéről állítanak össze évente – idei kiadása szerint 174 millió kártételt regisztráltak 2011-ben. Ebből 55 millió esetben a social engineering taktikáját alkalmazták, ami a legmagasabb valaha mért ilyen szám. Ráadásul – állítja a jelentés – ezek 97 százaléka elkerülhető lett volna.

> Az SE-támadások igen hatékonyak, mert azt az alapvető emberi tulajdonságot használják ki, hogy normális közeledés esetén szinte mindig udvariasak és segítőkészek vagyunk.

A társadalmi érintkezéseken keresztüli adatlopások száma tavaly drámaian megemelkedett – az összes adatlopáson belül 1-ről 37 százalékra. Ez önmagában indokolja, hogy többet törődjünk az úgynevezett *social engineering (SE)* típusú támadásokkal. Az ilyen – pszichológiai manipulációval, csalárd kommunikációval történő – információhappolás elszenvedői általában azok a cégek, szervezetek, amelyeknél az elővigyázatlanság miatt könnyű a kerítés mögé kerülni. Nyilvánvalóan az SE-támadások száma sokkal nagyobb a napvilágra kerülteknél, csak jelentős részük nem vezet eredményre, s anélkül fejeződik be, hogy kiderülne a (csalárd) kommunikáció valóságos célja. Kész szerencse, mondhatni, hiszen az SE-támadások nemcsak a leggyakoribbak, hanem a legpusztítóbbak közé is tartoznak. Ezért megelőzésükhöz meg kell érteni logikájukat, a felismerésükhöz fel kell készíteni a munkatársakat, és megfelelő informatikai védelemre is szükség van. Szerencsére gyakran egy automata call center már elég, hogy távol tartsa az ügyeskedőket, de ennél azért sokkal több kell az adatok integritásának biztos megőrzése és az ügyfelek bizalmas információinak megbízható védelme érdekében.

Az SE használata teljesen természetes mindannyiunk életében. Ezzel vesszük rá például a gyermekinket, hogy egyenek még egy kanál spenótot, vagy mossák meg a fogukat. Azaz olyan dolgok, amelyeket egyáltalán nem tartunk jónak, egy új kontextusban pozitívnak látszhatnak, ami megváltoztatja gondolkodásunk menetét, a pillanatnyi értékítéletünket. Az SE ezért alkalmas arra, hogy az emberek manipulálásával bizalmas információkat „csiklandozzon ki" a célszemélyekből információgyűjtés, csalás vagy éppen belépési kódok megszerzése érdekében. Tehát az SE egyetlen dolgot akar: információt. Azt pedig nem is olyan nehéz megszerezni.

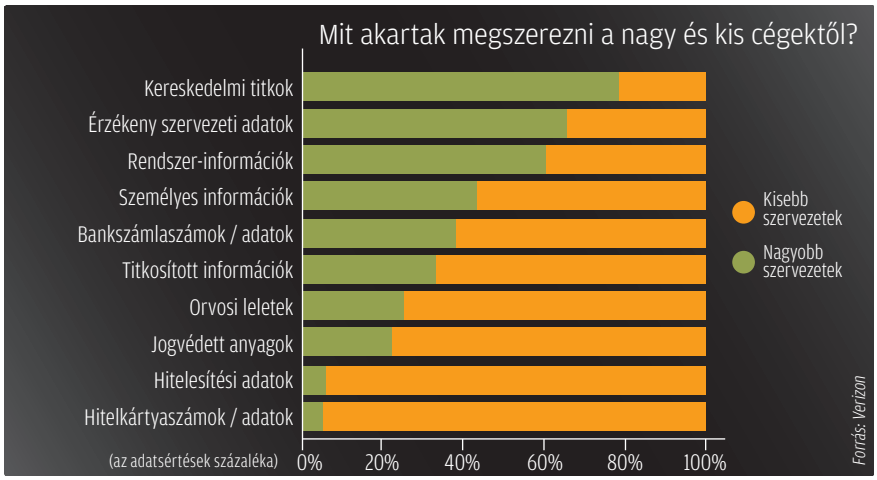
Kevin Mitnick, az SE (megtért) királya, *„A megtévesztés művészete"* című könyv szerzője egy *hvg.hu*-nak adott interjúban erről a következőket mondta: „Minden támadás első fázisa a kutatás. Meg kell keresni minden szabadon hozzáférhető információt a cégről, mint például éves riportok, marketingbrossúrák, szabadalmazott alkalmazások, újságcikkek, iparági folyóiratok, honlapok tartalma, és még különböző információk, amelyeket a célpont szemeteskukájából ki lehet halászni, valamint meg kell tanulni mindent, amit a cégről és az emberekről meg lehet. Kinek van hozzáférése azokhoz az adatokhoz, amelyeket keresünk? Hol dolgoznak? Hol laknak? Milyen operációs rendszert használnak? Mi a szervezeti felépítése a cégnek? Ki melyik irodában dolgozik, és az hol helyezkedik el földrajzilag? Mindig úgy kell kiadnunk magunkat, mintha jogosultságunk és szükségünk lenne az adatra. Ahhoz, hogy ezt elhiggyék rólunk, ismernünk kell a céges szakzsargont, a belső rendszereket, és képben kell lennünk a társasággal kapcsolatban. A kutatási szakasz után jön maga a támadás, amelynél ki kell találni az ürügyet, a cselt, amivel elnyerhetjük a megcélzott személy bizalmát és támogatását. Ha a támadást véghezvittük, megszereztük a bizalmat, és a kívánt információ már csak egy lépésre van, akkor visszatérünk a korábbi lépésekhez, mígnem sikerül megszerezni a kívánt információt. ... Szerintem az emberek nagyon bíznak másokban és nagyon hiszékenyek. Hajlamosak azt hinni, hogy morálisan mások is ugyanolyanok, mint ők maguk. Nem próbálkoznának rászedni vagy megtéveszteni senkit, ezért nem feltételezik, hogy ez velük megtörténhet. A profi social engineer képes manipulálni kívánságainkat, hogy segítőkészek legyünk, hatással van együttérzésünkre, hiszékenységünkre és még a kíváncsiságunkra is" – fejtette ki Mitnick.

Az interjú elkészülte óta a social engineerek helyzete még kényelmesebb lett, mert az igen elterjedt közösségi média (Facebook, LinkedIn, MySpace, Twitter stb.), illetve a blogok, a wikik, a fotómegosztó oldalak tálcán kínálják az információkat. Ilyesmiket: e-mail címek, telefonszámok, lakcímek, munkahelyek, megbízások, hobbik, de még a házi kedvencek fajtája és neve is, legújabban pedig az aktuális fizikai tartózkodási hely is könnyen azonosítható a célpont által használt autó- vagy a mobil-GPS adatok alapján.

Az átverés két fő módszere

Az adatok megszerzésének két fő módszere, iránya van. Az egyik az úgynevezett *reagáltatás (elicitation)*, a másik pedig a *színlelés (pretexting)*.

A *reagáltatás* tulajdonképpen a szükséges információ finom módszerekkel való kibányászása egy látszólag megszokott és ártatlan beszélgetésből. Ilyenkor az első lépés a bizalom megnyerése például azzal, hogy a csaló a célpontjával közös érdeklődési területükről beszél. Amint a bizalom vagy összhang kialakult, a rábeszélő lassan igyekszik akcióra serkenteni áldozatát, hogy adjon meg mélyebb információkat.



Ebben a taktikában egy sor jól azonosítható elem jelenik meg: a célszemély egójának legyezgetése, a közös érdeklődés kifejezése, szándékosan hamis kinyilatkoztatások, kéretlenül feltárt információk, ismeretek feltételezése, rávezető kérdések, feltevésszerű kérdések. Egy óvatlan ügyfélszolgálatostól – Mitnick ennek volt a nagymestere – a social engineer e módszerekkel igen hatékonyan csalhat ki olyan adatokat, amelyekkel ellophatja egy ügyfél identitását vagy hozzáférhet az adataihoz.

A *színleléssel* – hiszen a célpont másnak hiszi beszélgetőpartnerét, mint aki valójában – szintén elég egyszerűen ki lehet nyerni valakinek a privát információit. A színlelés annyiban több az egyszerű hazugságnál, hogy a nyilvánosan hozzáférhető információkból gyakran egy teljesen új identitást gyúr és használ információk megszerzésére vagy a célpont meggyőzésére, hogy lépjen valamilyen akcióba.

Az ügyfélszolgálatok felhívásakor a színlelők e nyilvánosan elérhető információk bevetésével igyekeznek rávenni a célpontjukat, akár még az automata hívásközpontokon keresztül elhelyezett üzenetekkel is, hogy olyan akciókba kezdjen, amelyek szándékuk ellenére megsérthetik egy valós ügyfél magánszféráját vagy az identitását. Az álca mögött sündörgők igyekeznek e-maillel vagy otthoni címmel elérni a belépést. A jelszó általában nem probléma, mert a legtöbben a házi kedvencük nevét, a kocsijuk márkáját vagy a hobbijukhoz, családjukhoz kötődő kifejezést használnak ilyen célra, hogy el ne felejtsék. Ha egyszer sikerült átverni a telefonközpontot vagy az ügyfélszolgálatost, az adatok szinte már biztosan sérülnek.

Ezek a csalók technikai eszközöket is használnak, amelyekkel megkönnyíthetik a tevékenységüket. Az úgynevezett ANI (automatic number identification) svindlinél az eszköz más telefonszámot jelenít meg a hívott fél készülékén, mint amilyen számról a csaló valójában hívja őket. A kijelzőn megjelenő szám így hitelesíti, hogy a beszélő egy ügyfél, egy cég vezetője, egy alvállalat képviselője, egy cégen belüli másik irodában dolgozó munkatárs vagy éppen egy beszállító stb. Az ANI csalásoknak sok formája van, mert olcsó és hatékony. Ez a svindli lehetővé teszi, hogy a célpont akár azt higgye, hogy más nemű a beszélgetőpartnere, mint valójában. Vannak olyan mobiltelefonos applikációk is, amelyekbe csak be kell írni a hívni és megjeleníteni kívánt számot, és a többi megy magától. A legfejlettebb formája ezeknek az átveréseknek a szabad forráskódú, ingyenesen letölthető VOIP telefonközpont, az Asterisk hátára telepített alkalmazásokon keresztül zajlik, amelyekkel a csalók leplük alól korlátlanul hívogathatják potenciális áldozataikat.

Az SE-támadások igen hatékonyak, mert azt az alapvető emberi tulajdonságot használják ki, hogy normális közeledés esetén szinte mindig udvariasak és segítőkészek vagyunk. A támadások megelőzésére ezért a legjobb eszköz a svindlizők megakadályozása abban, hogy elérjék a rendszer legsérülékenyebb elemét, az embert.

Hogyan lehet védekezni?

Az SE elleni védelem kiemelt feladata mind a cégnek, mind a szervezetnek. Nincs olyan ember vagy szervezet, aki/amely védve lenne a gátlástalan emberek kutakodásaitól, az identitáslopásoktól vagy az elektronikus kártevőktől. A károk megelőzéséhez a Voxeo biztonsági cég egy háromlépéses tervet ajánl, amelyben az oktatás, az auditok és a technológiai megoldások kapnak helyet.

A munkatársak oktatására azért van szükség, mert általában nem érzik a veszélyt, így meg kell tanítani nekik a céges és a személyes adatok védelmének szükségességét. Az alkalmazottaknak (igazából az ügyfeleknek is) ismerniük kell az SE-taktikákat, a manipuláció és az adatszerzésre való törekvés ismertetőjegyeit.

Sok vállalat a PCI-adatbiztonsági szabványnak (vagy más biztonsági szabványoknak) való megfelelést auditáltatja, amely az elektronikus kártevők vagy hackertámadások elleni védelemre való előírásszerű felkészültséget ellenőrzi. Az SE azonban kimarad ezekből az auditokból, azaz a gyengeségek rejtve maradnak. Ezért olyan felkészítőt és auditort érdemes választani, akinek ezen a területen (is) megfelelő tapasztalata van, de nem hág át jogi vagy etikai normákat.

A reagáltatás és rejtőzködés technikáit alkalmazó csalók ellen a legjobb módszer, ha nem találnak embert, akit rávehetnének a céljaikat segítő akciókra. De ha ez nem sikerül, legalább olyan eszközök kellenek, amelyek azonnal megállíthatják a fondorkodót. Ehhez vannak hatékony eszközök. Például az ANI manipulációt detektáló szoftverek, a biometrikus hangazonosítás, az automata telefonközpontokba a hívó fél tartózkodási helyét meghatározó alkalmazások telepítése, vagy az ügyfél korábbi vásárlásai, kártyahasználata, szokásai alapján generált úgynevezett dinamikus biztonsági kérdések alkalmazása, amelyekkel mind kiszűrhető a hackelési kísérlet. E módszerek együttes alkalmazása már nagyon hatékony védelmet jelenthet a social engineerek ellen. Az ügyfelek ugyan kisebb kényelmetlenséget érezhetnek e gyakorlat miatt, de a nagyobb biztonságérzet bizonyosan kompenzálja ezt.

SERVAL

Megoldás a szolgáltatásközpontú internet kihívásaira?

Ha a felhasználót adatokkal kell kiszolgálni, a web tökéletesen működik. Más fontos funkcióit, például userek vezeték nélküli hálózatok közti mozgását vagy cégek adatforgalmának szerverek közti váltogatását illetően már kevésbé. A problémák orvoslásához fejlesztők, üzemeltetők általában csak ideig-óráig működő, egyre nehezebben kivitelezhető megoldásokat találnak ki, anélkül, hogy mélyebbre bányásznának.

Vajon a szervál megoldás lehet a szolgáltatásközpontú internet kihívásaira? A Princeton Egyetem kutatói a közeljövő internetezését megkönnyítő, a mobilkornak és a szolgáltatásközpontú hálózatiságnak jobban megfelelő javaslattal álltak elő.

A szolgáltatás-hozzáférési réteg szerepe

Az infokommunikációs technológiák gyors térhódítása, és e folyamat részeként az internet elképesztő tempójú és dimenziójú elterjedése következtében más megoldások iránt mutatkozik igény, mint az ős- és a hőskorban, amikor csekély számú számítógép között kellett adatokat továbbítani. Ami akkor kiválóan funkcionált, ma már kevésbé, megkopott, túlszaladt rajta a technológia – a gépek számának drámai növekedésével egyre több szükségmegoldás került a korábban szinte hibátlan rendszerbe, a tervezők a már előzőleg is toldozgatott-foltozgatott rétegeket, a régi architektúrát újabb és újabb, állandónak hitt, de átmenetinek bizonyuló kiegészítésekkel, „hackelgetésekkel” bővítik.

KÖMLŐDI FERENC

Az internetet eleve nem arra tervezték, nem is tervezhették, hogy kapcsolatot létesítsen mobilfelhasználók és a számítási felhő (cloud computing) között, hogy első számú platformja legyen ennek a kommunikációnak, hogy bárhonnan bárki – adatközpontok szerveréről, otthoni gépről, utcai séta közben, zsebben lapuló okostelefonról, esetleg nem is személy, hanem hálózati vagy „magányos” szenzor – hozzáférhessen a gombamód szaporodó szolgáltatásokhoz. Egy alkalmazás különböző helyeken, különféle szervereken futhat, akármikor átköltözhető/automatikusan migráltatható egy másik gépre, ráadásul a mind a gazdasági-társadalmi, mind a technológiai változások következtében a userek is sokkal mobilabbak, lényegesen változatosabb körülmények között neteznek, mint tíztizenöt esztendeje. A jelen szolgáltatásai pedig (technológiai szempontból legalábbis) sokszínűbbek, dinamikusabbak az akkoriaknál. Az internet „nyelvére” fordítva: egyre kevesebb az összhang a hosztközpontú TCP/IP megoldás és a szolgáltatások sokszínűsége, dinamizmusa között.

A Princeton Egyetem Mérnöki és Alkalmazott Tudományok Iskolájának megoldása ugyan egyszerű, ám sok jelenlegi és jövőbeli probléma kezelhető vele. Az IP-hálózati (harmadik) és a felhasználók közötti adatszállításért felelős (szállítási, negyedik) réteg közé helyezett *Service Access Layert (szolgáltatás-hozzáférési réteget)* rövidítő *SERVAL* egyrészt az új (3,5) réteg köré épített architektúrára vonatkozik, másrészt a szervál nevű afrikai vadmacskafajra. Utóbbi gyorsaságára, elegáns mozgására és ügyességére való jelképes utalás a kutatók célkitűzéseit, elvárásait fejezi ki. (A kutatásfejlesztést az Egyesült Államok Nemzeti Tudományos Alapítványa, a DARPA, a Haditengerészeti Kutatóügynökség és a Cisco Systems együttesen támogatják.)

A rendszer csak kismértékben változtatja meg a programok letöltésének és az adatok kezelésének módját, ugyanakkor ez a csekély változás nagyon komoly hatással lehet a web további fejlődésére, és mivel már létező IP-hálózatokra épül, nem kell átalakítani az egész networköt. A SERVAL a számítógépeket és más eszközöket azonosító, az információtovábbítás és az adatkezelést végző programok számára egyaránt alapvető IP-címek szerepének csökkentésével, címek és portok helyett közvetlen szolgáltatásnevek bevezetésével kezeli a problémákat. Egy szolgáltatásnév az azonos szolgáltatást nyújtó, valószínűleg változó folyamatok csoportjának felel meg. A megoldás annyiban viszont megerősíti az IP-hálózati réteg szerepét, hogy az utóbbi könnyebben hajtja végre azt, amiben a legjobb: adatcsomagok továbbítását hierarchikusan aggregálható, topológiafüggő hálózati címek között.

A kutatócsoport saját miniatűr hálózat kiépítésével kezdte a tesztelést (megoldásuk természetesen a projekt honlapján is fut), a későbbiekben viszont terveik szerint nagyobb és komplexebb rendszerekkel is vizsgálják majd.

A SERVAL előnyei

Ahhoz, hogy az információcsomagok eljussanak a rendeltetési helyükre, úgy kell kezelniük az IP-címeket, mint a postásoknak az utcát, házszámot stb. Ha az információ megérkezik, a továbbító számítógép címe szintén fontos: lehetővé teszi, hogy gépünk felismerje a speciális alkalmazásokhoz (például YouTube videók futtatásához) nélkülözhetetlen adatokat. Mindez tökéletesen működött a korai interneten, amikor egyetlen számí-

tógépet használtunk. Manapság viszont már nem egy jól meghatározható, térbeli koordinátáit illetően egyszerűen lokalizálható géphez, hanem főként különféle szolgáltatásokhoz kívánunk kapcsolódni. A XXI. századi dinamikus hálózati környezetben a szolgáltatások elérése a legfontosabb, miközben az IP-cím változatlanul az adott gépre vonatkozik, ráadásul, ha a cím megváltozik, minden, például a vele összefüggő programok működése is összezavarodik, sőt, beavatkozás nélkül (általában) le is állnak. Ráadásul a mobileszközök elterjedésével, funkcióik bővülésével egyre nagyobb az IP-cím megváltozásának esélye. Alkalmazások újraírásával ugyan titokban tartható, hogy a kapcsolatot megszakítottuk, majd később újraélesztettük, csakhogy ez az út feleslegesen és túlzottan bonyolult, arról nem is beszélve, hogy még drágább is, mint a megszokott módon működő IP-címet nem helyettesítő, hanem az adatfolyam egyes csomagjaihoz újabb információs szint, a szolgáltatás-hozzáférési szint hozzáadásával újító, számítógépek helyett szolgáltatásokat (Facebook, Google, Twitter stb.) azonosító SERVAL implementálása, eredményes működtetése.

> **A SERVAL egyrészt az új (3,5) réteg köré épített architektúrára vonatkozik,** másrészt a szervál nevű afrikai vadmacskafajra, annak gyorsaságára, elegáns mozgására és ügyességére való jelképes utalás.

Ez azt eredményezi, hogy a program – mivel a szolgáltatás-hozzáférési szinten megkapja a szükséges információkat – akkor sem áll le, ha más lesz az IP-cím. A felhasználó úgy nézhet például meccset, hogy közben a tabletje Wi-Fi streamről mobilra vált, gépe egyszerre vehet igénybe vezeték nélküli és mobilszolgáltatásokat (3G, 4G), a kapcsolatmigráltatás szakadás nélküli és automatikus. Internetcégek könnyebben kezelhetik az adatforgalmat különféle szervereken, egyikről a másikra váltást.

A SERVAL eleinte egyébként főként vállalatok számára lesz fontos, míg az egyéni felhasználók valószínűleg csak később profitálnak igazán belőle. Az előbbieknél drasztikus hatékonyságnövekedés lesz az első tapasztalható eredmény. Például a több ezer szerverrel, fiókirodával rendelkező Google-nál lehetővé válik, hogy a bevett gyakorlat, azaz drága és nehezen kezelhető javítgatások helyett a célirányos szolgáltatás-hozzáférési szinttel biztosítsák a gördülékeny adatkezelést.

Az új megoldás egy másik előnye, hogy a rendszer fokozatosan, inkrementálisan telepíthető, és nem kell hozzá jelentős mértékben átalakítani a jelenlegi hálózatokat. A SERVAL-t nem használó userek számára a csomagokban lévő pluszadatszint észrevétlen, az IP-cím változatlanul azonosító marad. Azokban az esetekben, amikor élnek vele, a Princeton Egyetem számításai szerint az adatforgalom majdnem egy százalékkal gyorsabb lesz.

További tervek és kételyek

A fejlesztésben ugyan nem közreműködő, de a projektet figyelemmel kísérő *Gary Berger,* a Cisco Systems egyik főmérnöke szerint a hálózat nagyobb flexibilitását minden vállalat örömmel fogadja. Az internetcégek természetesen nemcsak egy, hanem több megoldást keresnek, viszont úgy véli, hogy a SERVAL a web további növekedését hátráltató, korlátozó, hozzátoldással már nem korrigálható, alapvető problémáit orvosolja.

„Mivel a szóban forgó hibák az architektúra legalapvetőbb szintjét is érintik, nem lehet őket a jelenlegi felépítmény inkrementális bővítésével, lényeges újítások bevezetése nélkül kezelni – nyilatkozta a Cisco keretében kivitelezendő majdani teszteket fontolgató Berger. – A SERVAL lehetővé teszi, hogy teljesen másként gondoljunk a problémára, ami magától értetődően, minden szereplő számára hasznos."

Elmondta, hogy már foglalkoznak a SERVAL technikailag legkomplexebb, legjobban kidolgozott (és természetesen legfontosabb) részéhez, a szolgáltatás-hozzáférési réteghez fejlesztendő alkalmazásokkal, ugyanakkor több gyorsan megválaszolandó, kritikus kérdést is felvet: hogyan működik a rendszer a világháló egészén, milyen potenciális problémák merülhetnek fel szélesebb körű elterjedése esetén?

Erik Nordström, a fejlesztőcsoport egyik tagja, a kutatásról készült és a konferenciákon, bemutatókon ismertetetendő tanulmány első számú szerzője internetcégekkel és szolgáltatókkal történt találkozókról számolt be, amelyeken felvázolták nekik a SERVAL előnyeit. Nagyvállalatok, fontosabb szervezetek meggyőzése egyelőre azonban nem tűnik egyszerű feladatnak. Több okból is ódzkodnak az alapvető változtatásoktól – elsősorban például azért, mert komoly összegeket fektettek a rendszereiket működtető szoftverbe, így még várnak a hosszú távú megoldással. Nyilvánvaló kényelmi szempontok szintén hozzájárulnak idegenkedésükhöz.

„Rá szeretnénk jönni, mit kell tennünk ahhoz, hogy a SERVAL-t mások is elfogadják, különösen olyan esetekben, amikor nagy léptékű webszolgáltatásokat kell kezelniük" – elmélkedett Nordström, majd a laboratóriumi kereteknél „valódibb" környezetek (a világháló egészének) mérnöki kihívásaira is felhívta a figyelmet.

A projekt következő fázisában a korlátok és előnyök pontosítása és a bevezetési stratégia kidolgozása mellett ezzel a kérdéskörrel kívánnak még behatóan foglalkozni.

M2M SZERVER

Szerverszolgáltatások kommunikáló gépeknek

A mobilhálózaton kommunikáló gépek jellemzően nem közvetlenül, hanem egy szerver közvetítésével teremtenek kapcsolatot egymással. Az M2M szerver lehet saját üzemeltetésű, de létezik szolgáltatói modell is.

/ Írta: Majláth Judit

Közel három évvel ezelőtt jött el az a pillanat, amikor a mobilhálózatokon folyó adatforgalom meghaladta a hangforgalmat. Azóta a rés (szakadék) tovább nőtt, és egyes becslések szerint 2020-ban már 50 milliárd eszköz küld adatokat, illetve kommunikál a mobilhálózatokon. Gép a gépnek, azaz *machine-to-machine (M2M).*

Az M2M kommunikáció során a végberendezések általában egy szerver közbeiktatásával állnak kapcsolatban egymással. Az egyik oldalról a berendezések által mért vagy begyűjtött adatok a mobilhálózaton (vagy a vezetékes interneten) keresztül, csomagkapcsolt technológiával, IP-alapon jutnak el a távoli szerverre. Az adatok sokfélék lehetnek, például mérőóraállások, kameraképek, hőmérsékleti adatok, élettani adatok, riasztóberendezések állapotai, riasztások, vészjelzések.

Egyre jobban terjedő alkalmazás, hogy mérőórák adatait továbbítják a hálózaton. Ilyenkor jellemzően nagy tömegű adatról van szó, hiszen egy-egy mérőórától akár napi vagy óránkénti gyakorisággal is érkezhetnek az információk, ráadásul a hálózatba kötött berendezések száma is folyamatosan nő. Kellően intelligens M2M szerverszolgáltatás esetén figyelemmel kísérhető például, hogy nincs-e valamilyen kiugró, szokatlan érték a beérkező adatok között. Durva eltérés esetén a rendszer riasztást küldhet.
A szervernek tehát alkalmasnak kell lennie az adatok fogadására, feldolgozására és szükség esetén a megfelelő akciók végrehajtására. Lehet, hogy csak egy tájékoztató SMS-t kell küldenie a fogadóoldali végpontra, de lehet, hogy vészjelzést kell kiadnia, és azzal párhuzamosan riasztania a megfelelő szervezeteket (például biztonsági szolgálat, tűzoltóság).

A végberendezések egy köztes adatátalakító és -továbbító eszköz közbeiktatásával kommunikálnak a szerverrel. Ezen eszköznek – nevezzük kommunikátornak – magához az ipari végberendezéshez (általában valamilyen PLC-hez), valamint a szerverhez is illeszkednie kell. A kommunikátor elláthat egyéb funkciókat is, például vezérelheti vagy figyelheti az adatküldés gyakoriságát.

„A szerverprotokollok elméletben lehetnek akár publikusak is, de egyelőre nem ez a jellemző. Ezért általában egyeztetni kell az adott szerverszolgáltató kommunikációs protokolljáról" – tájékoztatott *Tárnok Péter,* a WM Rendszerház műszaki igazgatója.

A felhasználók, azaz a szerverről továbbított adatok címzettjei a szerver túloldalán találhatók. E végberendezések az előre beállított módon, kapják meg az őket illető adatokat.

> **Vannak bizonyos interfészek, amelyek az M2M-technológiában elfogadottak és használatosak,** de nincs szabványosítva, hogy a szerverbe milyen formátumban kell az adatoknak beérkezniük.

Árképzési szempontok

„Az M2M szerverszolgáltatás mögött bonyolult hardverkonfiguráció és robusztus szoftver áll. Erre azért van szükség, mert a felhasználói igények rendkívül eltérőek, mind a beérkező és továbbítandó információ jellegét, mind a mennyiségét, gyakoriságát illetően" – hívta fel a figyelmet Tárnok Péter.

Amennyiben az M2M szolgáltatás hosting tevékenységgel is párosul, úgy azt is figyelembe kell venni, hogy ugyanazon időben hányan szeretnék a szolgáltatást igénybe venni, tehát hányan csatlakoznak egy időben a szerverhez. Ehhez igazodva kell ugyanis a szerver kapacitását, erőforrásigényét megtervezni. Ha például egy felhőszolgáltatásról van szó, ami gyakorlatilag egy virtuális szerverszolgáltatásnak tekinthető, akkor a szerverelérés sávszélességének van ténylegesen jelentősége.

A szerverszolgáltatások árának kialakítása természetesen az üzleti modelltől függ. A szolgáltatásokért végberendezésenként kell fizetni, havi alapdíjat, adattovábbítási díjat, valamint az igényelt szolgáltatási szinttől függő pluszdíjat. Természetesen olcsóbb, ha valaki csak probléma esetén kér értesítést, mintha folyamatosan, egy térképen szeretné figyelemmel kísérni eszközei működését, sőt szükség esetén be is szeretne avatkozni a távolból. Az árak meghatározásánál azt is célszerű figyelembe venni, hogy egy adott berendezésről általánosságban hány jelzés érkezik a szerverre, továbbá hogy maguk a jelzések (adatcsomagok) milyen méretűek, illetve fix vagy változó hosszúságúak.

Nincs szabványos interfész

Az M2M kommunikáció egyik forró pontja a szabványosítás. Vannak olyan területek, ahol a szabványosítás már elért egy bizonyos fokot, de minden végponti (terepi) eszközre általánosítható, szabványos interfész egyelőre nincs. A vagyonvédelmi piacon például a riasztóberendezések kommunikációja szabványos Contact ID protokollal történik. A gépjárműveknél meglehetősen elterjedt a CAN FMS csatlakozó. Vannak tehát bizonyos interfészek, amelyek az M2M-technológiában elfogadottak és használatosak, de az nincs szabványosítva, hogy a szerverbe milyen formátumban kell az adatoknak beérkezniük.

„Minden fejlesztővállalat a saját adatstruktúrájának megfelelően építi fel a szerverét, így a jelzésrendszerek is jellemzően cégspecifikusak. Több vállalat együttműködésekor az érintetteknek természetesen meg kell egyezniük valamilyen közös interfészben. Soros porti csatlakozásnál bizonyos esetekben, bizonyos eszközöknél általában megállapodnak a felek valamilyen

szabványos kommunikációs protokollban, de ez a gyakorlat egyáltalán nem általánosítható. És ez talán nem is baj" – vélekedett *Havasi Zoltán,* a MOHAnet elnök-vezérigazgatója.

Dedikált hálózat, fix IP-cím

Az M2M szerverszolgáltatók a mobilhálózat szokásos biztonsági elemein kívül természetesen további biztonsági elemeket is beépítenek szolgáltatásukba. Ez elengedhetetlen. Sok cég azonban dobozos termékként árulja eszközeit, amit Havasi Zoltán nem tart elfogadhatónak: „E téren ütköznek a vélemények a szakmán belül. Vannak olyan szolgáltatások, amelyeknél nem tudom elképzelni, hogy megveszem a boltban a terméket, beleteszem a SIM-kártyát, feljelentkezem a hálózatra, és minden rendben, az eszköz máris küldi a jelzéseket az általam beállított szerverre. Megítélésem szerint ez felelőtlen magatartás mind a gyártók, mind a felhasználók részéről. Ez utóbbiak természetesen nem tudatosan hibáznak, hanem bizonyára a termék kedvező árfekvése miatt hoznak téves döntéseket."

A szakember szerint az M2M-technológiájú rendszereknél egy bizonyos szolgáltatási szint fölött mindenképpen dedikált hálózatot kell alkalmazni. Egy egészségfelügyeleti, egy vagyonvédelmi, vagy bármilyen más szolgáltatás ugyanis megköveteli a fokozott megbízhatóságot. A GPRS-technológiánál ezt úgynevezett corporate APN-nel (Access Point Name) oldják meg, ahol az eszközök nem dinamikus, hanem fix IP-címeket kapnak, és már önmagukban egy dedikált hálózatba jelentkeznek fel, nem pedig a publikus internethez csatlakoznak. Csak így oldható meg a hálózat minden elemének, a szervernek, a hálózati és a végponti eszközöknek a folyamatos, 24 órás felügyelete.

Felfutóban a hazai piac

Szakértői vélemények szerint Magyarországon az M2M szerverszolgáltatások piaca még csak most kezd felfutni. Sokan egyelőre inkább saját távfelügyeleti központot üzemeltetnek, és csak a kommunikációs szolgáltatásokat veszik igénybe. Elméletileg az sem kizárt, hogy a berendezések szerver nélkül, tehát közvetlenül kommunikáljanak egymással a mobilhálózaton, ám ez technikai okokból nem szerencsés. Az internetszolgáltató (vezetékes vagy mobil) ugyanis általában dinamikus IP-címeket oszt ki, és így a berendezések nem találják meg egymást, következésképpen nem biztosítható a folyamatos felügyelet. Jóllehet vannak e problémára különböző megoldási módszerek, a teljes rendszer így sokkal nehezebben tartható kézben. Egyszerűbb és megbízhatóbb, ha csillag topológiájú hálózatban gondolkozunk, aminek a közepén egy szerver működik, és a végberendezések azon keresztül kommunikálnak egymással.

Számos olyan terület van, ahol a gép-gép kommunikáció nagy jövő előtt áll. Terjedése várható – többek között – a biztonságtechnikában (lakások, irodák, liftek stb.), a mérésadatgyűjtésben (áram-, gáz-, távhőszolgáltatás stb.), az egészségügyben (otthoni távfelügyelet, vérnyomás, vércukor és egyéb élettani adatok távmonitorozása stb.), az intelligens otthonokban.

A LENOVO A WINDOWS 7 OPERÁCIÓS RENDSZERT AJÁNLJA

A LEGENDA FOLYTATÓDIK

intel inside CORE i7 Ultrabook Inspired by Intel

20 ThinkPad 20 YEARS OF INNOVATION

BEMUTATKOZIK A
THINKPAD X1 CARBON
AZ ELSŐ ÜZLETI ULTRABOOK™

- akár Intel® Core™ i7 processzorral
- kevesebb mint 1,4 kg
- 18,8 mm vékony
- szénszálas megerősítés

lenovo FOR THOSE WHO DO.

www.lenovo.com/hu