SZÁMÍTÁSTECHNIKA
COMPUTERWORLD
IKT-STRATÉGIA DÖNTÉSHOZÓKNAK / [illegible] / 2013. MÁJUS 22. / XLIV. ÉVFOLYAM 12. SZÁM

Üzleti támasz bajmenedzsment

Az üzletfolytonosság tervezésének sosincs vége: a belső változások, az új fenyegetések és kockázatok miatt fontos a felkészültség folyamatos fenntartása.

9 770587 151006 13012
www.computerworld.hu
Ára: 495 Ft

COMPUTERWORLD /IMPRESSZUM

KIADJA A PROJECT029 MEDIA AND COMMUNICATIONS SZOLGÁLTATÓ KFT.
1037 Budapest, Montevideo utca 9.
HU ISSN 0237-7837
Postacím: 1374 Budapest 5, Pf. 578.
Bankszámlaszám: 10300002-20328016-70073285

FELELŐS KIADÓ:
Virágh Márton ügyvezető – mviragh@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: Mester Sándor
Főszerkesztő helyettes: Sós Éva
Online főszerkesztő: Pavlovic Jovan
Olvasószerkesztő, korrektor: Váczy Laura
Munkatársak: Kis Endre, Kömlődi Ferenc, Mallász Judit, Meixner Zoltán
Tipográfia: Berényi István
Szerkesztőségi ügyelet: Csereszny Anita – acsereszny@idg.hu Telefon: 577-4302, fax: 266-4343
Munkatársaink elérhetőségeit megtalálja weboldalunkon: » http://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

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 10 860 forint, fél évre 5460 forint, negyed évre 2745 forint. Lapunkat a MATESZ auditálja. A Computerworld az IVSZ hivatalos médiapartnere. A Computerworld Online látogatói szokásait a gemius/Ipsos Audience vizsgálja. A Computerworld Online hirdetéseit az Adverticum AdServer szolgálja ki.

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

ÜZLETMENET

JAMES BOND ÉS AZ ÜZLETFOLYTONOSSÁG

14 A vállalatoknak manapság ahhoz, hogy működni tudjanak, hozzá kell férniük az adataikhoz, különben igen rövid idő alatt teljesen megbénulhatnak. Ennek ellenére a cégek jelentős részének nincsen rá terve, hogy mihez kezd, ha előáll egy vészhelyzet. A megoldást az üzleti folytonosság tervezése és menedzsmentje (BCM) adhatja. Összeszedtük hozzá a legfontosabb elemeket.

INFORMATIKA NÉLKÜL MEGÁLLHAT AZ ÉLET

CIO-MAPPA | 16 A katasztrófaelhárítási terv elkészítésénél az informatikai szakembereknek és a vállalat üzleti vezetőinek együtt kell dolgozni.

A VÁLLALATI IT MÁR NEM MINDENTUDÓ

FINANCIO | 18 Drótos Györggyel, az IFUA Hováth & Partners partnerével, a Corvinus Egyetem tanszékvezetőjével tekintettük át a változásokat.

ADATKÖZPONT | 7 Rendszerodüsszeia / Tizennyolc ország harminc városát érintő bemutató körútján Budapesten állomásozott a HP teherautója, rakterében a szerverarchitektúrák egyesítésére indított Odyssey-projekt első fejlesztéseivel. **| 8 Üzleti alkalmazások a HANA-felhőből /** Az SAP memóriaalapú vállalatirányítási, ügyfélkapcsolatkezelő- és adattárház- megoldásait felhőszolgáltatásként is kínálja új HANA Enterprise Cloud platformján. **| 10 Centrális vonzások és taszítások /** Őt évre szóló előrejelzése szerint a virtuálisszerverbérletszolgáltatás nő majd a leggyorsabb ütemben, a kolokáció pedig mindössze évi 2 százalékkal bővül – a piackutató IDC egy regionális kutatás eredményeiről.

ÁLLANDÓ ROVATAINK
| 4 Vélemény / Mester Sándor: Birtokos eset és a hozzáférés **| 5 reakCIO /** Szittya Tamás kommentjéből megtudhatják, hogy miért jár minden bitnek a védelem. **| 5 Hírmozaik | 6 Vélemény /** Bozsó Julianna: Ébresztő! Avagy élet a VirusBuster után. **| 12 Vélemény /** Illés Márton: Teszt a kezdet, avagy a TDD természetrajza

Még többet akar? Látogasson el a www.computerworld.hu-ra!

MESTER SÁNDOR

főszerkesztő, Computerworld

Birtokos eset és a hozzáférés

Adatközponttal mélyebb ismeretségbe úgy nyolc éve kerültem. Régen történt tehát, de olyan tisztán emlékszem rá, mintha ma lett volna. Úgy esett, hogy az ország egyik leglátogatottabb hírportálján teljesen váratlanul évekkel korábban publikált hírek kezdtek véletlenszerűen megjelenni – és én voltam éppen az ügyeletes vezető.

Tisztán emlékszem a pánikra, ami hatalmába kerített engem és illetékes kollégáimat, amikor megbolondult a rendszer. Eleinte ilyen, szakmainak kevéssé mondható módon írtuk le a jelenséget. Hosszú órákba tellett, mire megtaláltuk a hiba valódi okát.

A weboldal megjelenítésében kulcsszerepet játszó szerver adta meg magát. Ilyen a legjobb házban is előfordulhat, ezért a rendszer architektje eleve úgy tervezte meg e részegységet is, hogy hiba esetén azonnal vegye át a prímet egy másik gép, amelyen minden mindig ugyanúgy megvan, mint a másikon (ínyenceknek: lásd még failover).

Csakhogy.

Az elszállt szerveren voltaképpen a merevlemez adta meg magát, elérte már a kritikus üzemórát, így aztán minden oka megvolt arra, hogy kilehelje szegény lelkét. Általában ha van tartalék, ilyenkor is zökkenőmentes az üzem, a rendszer bevonja a körbe a tartalékot és megy minden tovább, mintha mi sem történt volna.

Csakhogy.

Amint a későbbi vizsgálatok során kiderült, a tartalék szerveren pontosan annyi időt pörgött a merevlemez, mint a meghibásodottban, ezért aztán ő is úgy vélte, hogy eljött az ideje az örök pihenésnek. Végül napokba tellett, mire visszaállt a normális működés, a mentésekből sikerült fájlról fájlra visszanyerni mindent, ami elveszni látszott.

Ha túléljük, a rendkívüli incidens is értékkel bír, éppen annyival, amennyit okulunk belőle.

Külön adatbázist nyitottak a rendszerüzemeltetők a merevlemezek futási idejének nyilvántartására, és kínosan ügyeltek arra, hogy a kritikus futási idő közelébe kerülő lemezeket újra cseréljék, továbbá arra is figyeltek, hogy az egymás tartalékaiként működő gépekben még véletlenül se legyen azonos korú a lemez.

Ez az eset jutott eszembe, amikor e lapszám egyik írását olvastam. Az IDG-vel egy tőről fakadó nemzetközi cég, az IDC kutatói az adatközpontok szolgáltatásainak (kolokáció, hoszting és hardver- és virtuálisszerver-bérlet) regionális jelenéről és jövőjéről készítettek tanulmányt, amelynek lényegét foglaljuk össze.

Én egy olyan eset elszenvedője voltam, amely a körülményeit tekintve ma már aligha tekinthető tipikusnak. A hírportál informatikai rendszereinek felügyeletét saját informatikusaink látták el, és azt az adatközpontot, amelyben a szervereink nyertek elhelyezést, az anyacégünk működtette. Mondhatjuk tehát, hogy házon belül volt mindenünk, így ha probléma támadt, azonnal érkezett a segítség.

Az IDC kutatását olvasgatva azon merengtem, hogy vajon amikor a szerverünk – hogy úgy mondjam – kolokál vagy éppen hosztingban van, vagy amikor már nincs is szerverünk, hanem valamilyen hatalmas gépen virtuálisan szorítanak nekünk egy kis erőforrást, akkor baj esetén milyen figyelem jut a mi kis gondunkra.

Azon a kis- és közepes vállalkozások vezetőinek fejében, amelyek növekvő számban költöznek be az adatközpontokba, valószínűleg meg sem fordul, hogy az adatközpontban jut-e majd kellő figyelem az adataikat őrző, alkalmazásaikat futtató gépek jó működésére. Nem engedhetik meg maguknak, hogy saját kis adatközpontot létesítsenek, így nem tehetnek mást, minthogy bíznak a szolgáltatóban. És – meglehet – igazuk van. Az adatközpontok működtetői valódi specialisták, rendelkeznek a folytonos működéshez szükséges tapasztalatokkal és erőforrásokkal.

> Az adatközpontok működtetői valódi specialisták, rendelkeznek a folytonos működéshez szükséges tapasztalatokkal és erőforrásokkal.

Amikor egy szolgáltatás iránti igény felmerül és igazolódik üzleti szükségessége, a vállalkozás menedzsmentje és informatikai vezetője egyaránt megfogalmazza a kérdést, hogy saját (épített vagy vásárolt) rendszerrel vagy külső szolgáltatóval oldják meg a feladatot.

Ha megtehetik, választanak a birtoklás és a hozzáférés között. Döntésük függhet a konkrét feladattól, attól, hogy a vállalat a fejlődési pályáján éppen hol tart, s attól is, hogy milyen a belső informatikai kultúra.

reakCIO

Ezen a héten *Szittya Tamás,* a NetIQ Novell SUSE Magyarországi Képviselet ügyvezető igazgatója kommentálja szakcikkünket.

Heti összeállításunkból megtudhatják, hogy minden bitnek jár a védelem.

SZITTYA TAMÁS
ÜGYVEZETŐ IGAZGATÓ, NETIQ NOVELL SUSE MAGYARORSZÁGI KÉPVISELET

INGYEN BACKUP OLCSÓBB, MINT AZ ADATVESZTÉS

Ha leégne az iroda, fel tudná-e valaha is újra venni a munka fonalát a cég? Egy nemrégiben készült felmérés alapján a PC-felhasználók 35 százaléka soha nem készített biztonsági mentést adatairól, 51 százalékuk pedig évente egyszer vagy ritkábban teszi ezt. Kétéves merevlemezek esetében már 8 százalék esélyünk van a meghajtó összeomlására, így jó eséllyel bármikor bekövetkezhet az adatvesztés.

» http://techcorner.hu/pcworld/ingyen-backup-olcsobb-mint-az-adatvesztes.html

Minden vállalatvezetőnek fel kellene tennie saját magának a kérdést, hogy egy katasztrófa után miként tudná újraindítani a cég üzleti működését. Sokan mégis inkább elhessegetik a témát, abban bízva, hogy velük nem történik baj. Úgy gondolják, fölösleges pénzkidobás lenne egy olyan eseményre felkészülni, amely jó esetben soha nem következik be.

Pedig ma már nem kerül óriási összegbe és erőfeszítésbe egy hatékony, katasztrófa utáni helyreállítási terv összeállítása és a szükséges megoldások bevezetése. Néhány évvel ezelőtt még nem volt választásuk a cégeknek, és komoly költségeket kellett áldozniuk az infrastruktúrájuk tükrözésére, ha azonnali visszaállításra vágytak egy esetleges katasztrófa után. Ez a módszer rendkívül jó eredményeket garantál a két legfontosabb mutató, az RTO (Recovery Time Objective, kiesés és újraindítás közötti idő) és az RPO (Recovery Point Objective, adatvesztési tűrés) terén, viszont a duplájára emeli az informatikai infrastruktúra működtetési költségeit. A másik lehetőség az olcsóbb, ám nehézkes archiválási metódus, amely viszont lassú és körülményes rendszer-újraindítást és adat-visszaállítást nyújt.

A jó hír, hogy ma már létezik olyan megoldás, amely a legjobbat ötvözi a két módszerből. A titok nyitja egy olyan technológia, amely az informatikai szolgáltatásokat készenléti virtuális gépekre másolja. Katasztrófa vagy leállás esetén ezek a virtuális gépek percek alatt beindíthatók és futtathatók közvetlenül a virtuális infrastruktúrában. Ez a bootolható backup-rendszer rendkívül gyors helyreállítást garantál, hiszen a biztonsági másolat adathordozója egyben a helyreállítási környezet is.

A szervezetek az igazán hatékony megoldásokkal – mint amilyen a kínálatunkban is megtalálható NetIQ PlateSpin Forge – a teljes informatikai szolgáltatást, tehát az adatokat, alkalmazásokat és operációs rendszereket is védelem alá helyezhetik egyetlen helyreállítási környezetben anélkül, hogy a forrásszervereket leállítanák vagy újraindítanák. A replikáció csak minimális erőforrást igényel a forráskiszolgálóktól, ezért a felhasználók még a biztonsági mentés alatt is közel változatlan teljesítmény mellett használhatják az éles szervereket.

Ez a módszer összességében olyan teljesítményt nyújt, mint a tükrözéses eljárás, ám a költsége nagyjából az archiválási módszerével azonos, ráadásul rendkívül egyszerűen kivitelezhető. Így tehát sem a nagy kiadás, sem az időhiány nem lehet akadálya a megoldás bevezetésének.

A katasztrófák megelőzéséhez és enyhítéséhez otthoni környezetben elengedhetetlen egy külső merevlemez. Az üzleti életben azonban még inkább előrelátónak kell lennünk, mint magánemberként, így vállalati oldalon a minimum egy megfizethető, de hatékony disaster recovery megoldás.

REGISZTRÁLJON

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

[HÍRMOZAIK]

KURZUS / A ZyXEL online képzések sorát tette elérhetővé weboldalán, megkönnyítve ezzel a viszonteladók dolgát a kompetenciájuk kiterjesztésére. Az online tananyag egyelőre csak angol nyelven érhető el, magyarul várhatóan 2014 elején jelenik meg.

KÉPBEN / A Sharp BIG PAD multi-touch érintőképernyőjének és az új, táblagépes, valamint okostelefonos kapcsolatot biztosító Touch Display Link szoftverének köszönhetően az üzleti találkozók, projektbemutatók vagy tudományos előadások interaktívabbá és hatékonyabbá válhatnak.

CLOUD / Felhőszolgáltatásként is kínálja üzletkritikus nagyvállalati rendszereit az SAP. A szoftvercég a memóriaalapú (HANA) vállalatirányítási, ügyfélkapcsolat- és adattárház-megoldásait kínálja gyorsan hozzáférhető szolgáltatásként. A felhőalapú szolgáltatás egyben alacsonyabb költségeket, skálázhatóságot ígér. Az SAP HANA Enterprise Cloud-ot nagyvállalatok számára kínálja a cég, iparágaktól függetlenül.

BOZSÓ JULIANNA

ügyvezető
NewCo Trading Kft.

Ébresztő!

Az utóbbi hónapokban sokan kérdezik tőlem, hogy vagyok? Mi történt? Hogyan telnek a napjaim? Milyen az életem a "VirusBuster" után (nélkül)? A kérdések hangneme aggodalmat mutat, és félve teszik fel őket, nehogy megbántsanak vagy sebeket szakítsanak fel bennem.

Aztán elkezdünk beszélgetni, és már régen nem rólam vagy a VirusBusterről beszélünk, hanem arról, hogyan is tud ma talpon maradni egy magyar tulajdonú, saját finanszírozásban működő cég, mit tud tenni a tulajdonos, az ügyvezető, illetve a menedzsment annak érdekében, hogy ne legyen katasztrófa, és lehetőleg ne csak "túléljen", hanem biztosítsa a cég folyamatos fejlődését.

Még mindig sokan vannak, akik úgy gondolkoznak, hogy nem probléma, ha nem tud minden évben fejlődni a cég, most egy-két nehéz évet kell kibírni, addig összehúzzuk magunkat, nem fejlesztünk, kivárunk. És kivárnak, vegetálnak és reménykednek, aztán elkezdenek etikátlan dolgokat csinálni, nemcsak a munkatársaikkal, de a vevőikkel és a partnereikkel szemben is. És nincs egy pillanatra sem lelkiismeret-furdalásuk, hiszen azzal nyugtatják magukat, hogy más is ezt csinálja, mert belekényszeríti a válság, a konkurencia, a kormány... és mindenki hibás, ő csak áldozat!

Véleményem szerint itt lenne az idő, hogy felébredjünk végre! Felébredjünk, mielőtt teljesen szétzilálnánk a hosszú évek alatt korrektül és felelősségteljesen felépített cégeinket és piacainkat! Felébredjünk és felmérjük, hogy a magunkban okozott kárt továbbvetítjük a Felhasználóinkra is, akiket etikátlan árharccal és egyéb presszúrákkal kényszerítünk – egyre többször – a nem szakmai alapokon hozott döntésekhez. Egyre többen gondoljuk úgy, hogy a gazdasági válság valahol mégis jót tesz nekünk, hiszen belekényszerít minket abba, hogy alaposan átvizsgáljuk a folyamatainkat, racionalizáljunk és optimalizáljunk, meghozzunk hosszú ideje halogatott döntéseket, még ha néha fájdalmas is a számunkra.

> „És igazán itt van az a pont, amikor eldől minden.

És igazán itt van az a pont, amikor eldől minden. Mert ha egy tulajdonos hallani sem akar arról, hogy azon gondolkozzon: megérett-e már a cége, illetve a helyzet ahhoz, hogy az addigi befektetéseit egy nagyobb egység részévé tegye, ragaszkodik és kapaszkodik a tulajdonába, ami a döntésképtelensége vagy a nem-döntése következtében elkezd értéktelenedni, szétesni. Mert ha egy ügyvezető képtelen levezényelni azokat a változásokat, amelyek szükségesek a katasztrófa elhárításához, a túléléshez, ha a menedzsment nem tud azonosulni a megváltozott helyzettel és ellenfeszül a döntéseknek, bizton állítom, hogy az a szervezet elindul a széthullás irányába.

Cégvezetőként és tulajdonosként 20 évvel a hátam mögött sok tapasztalatot szereztem. Hoztam én is rossz döntéseket, de ma már biztonsággal tudom, hogy hosszú távon csak azok maradhatnak életben, akik:

- a kitűzött cél érdekében kitartóan, elkötelezetten dolgoznak, pozitívan gondolkoznak,
- akik képesek a folyamatos változásokhoz folyamatosan és rugalmasan hozzáállni és megújulni,
- akik hosszú távú kapcsolatokra törekszenek az etikus piaci hozzáállásukkal és munkatársaik megbecsülésével,
- akik kellő "alázattal", empátiával és diplomáciai képességgel vannak megáldva,
- akik képesek dönteni, a döntéseiket felvállalni és végre is hajtani, és végül
- akik nem az oktalan spórolásban, hanem az észszerű befektetésekben látják a fejlődés útját.

És e dolgokhoz semmi köze nincs a válságnak, a politikának, a kormánynak... stb. Ehhez nekünk, cégtulajdonosoknak, cégvezetőknek van közünk, akik mintát vagyunk, példát mutatunk a jövő generációnak.

Mutassunk hát jó példákat, hogy ne szegje kedvüket a panaszáradat, az elégedetlenség és a problémák. Mindezekben lehetőségeket, megoldásra váró feladatokat és előrelátó problémaelhárítást, megelőzést lássanak!

És hogy én hogy vagyok? Köszönöm, jól! Mert szerencsés vagyok, hogy a fenti értékekkel élhettem, mert olyan menedzsmentem volt, amely támogatott, és most az új céljaimhoz is remek fiatal csapattal dolgozhatok, akik ezekkel az értékekkel építkeznek majd utánam is!

ARCHITEK-TÚRA

Szerver-odüsszeia

Tizennyolc ország harminc városát érintő bemutató körútján Budapesten állomásozott a HP teherautója, rakterében a szerverarchitektúrák egyesítésére indított Odyssey-projekt első fejlesztéseivel. /Írta: Kis Endre

A HP bő másfél éve azzal a céllal indította a programot, hogy az Intel Itanium és x86-os szerverarchitektúrákat közös felügyelet alá vonja, és az üzletileg kritikus alkalmazásokhoz szükséges, magas rendelkezésre állás, nagy teljesítmény és méretezhetőség mellett a választás lehetőségét is nyújtsa egyetlen platformon.

– Az informatika területét formáló négy erő, a felhő, a mobilitás, a közösségi és a nagyadat-alkalmazások az eddiginél is nagyobb elvárásokat támasztanak az infrastruktúrával szemben, az ebből eredő kihívásokkal a következő 5-7 év folyamán minden IT-vezető szembesülni fog – mondta *Birnbauer Péter*, a HP Magyarország üzletileg kritikus rendszerekért felelős vezetője a budapesti bemutató alkalmával. – Jóllehet, az említett technológiákkal összefüggő fejlesztésekre a vállalatok jelenleg az IT-költségvetés mindössze 20 százalékát költik, ez az arány a következő években 90 százalékra fog nőni.

A mind magasabb szolgáltatási szinteket a szervezeteknek ráadásul úgy kell tartaniuk, hogy az ehhez szükséges informatikai fejlesztésekre a pénzügyi keret szűkre szabott. A HP szerint az egymással látszólag szembemenő elvárások is teljesíthetők olyan platform bevezetésével, amely a Unix rendszerek magas rendelkezésre állását, meghibásodásokkal szembeni ellenálló képességét a költséghatékonyabb, széles körben hozzáférhető technológiát képviselő ipari szabványos szerverekre is kiterjeszti.

Az Odyssey-projekt keretében a HP a moduláris BladeSystem architektúrára építve egységes szerverplatformot fejleszt, amelyen a vállalatok Intel Itanium és Xeon processzorokkal működő kiszolgálókat is használhatnak üzletileg kritikus alkalmazásaikhoz.

DragonHawk kódnéven a HP például olyan, Intel Xeon processzorokkal szerelhető pengeszervereken dolgozik, amelyek a HP Superdome 2 szerverkeretébe illeszkednek. Az egységes felügyeletet lehetővé tevő technológiákkal a felhasználók az Itanium-alapú blade-eken, HP-UX operációs rendszeren futó, üzletkritikus alkalmazásaik mellett Linux és Windows-alapú alkalmazásaikat is ugyanabban a szerverkeretben működtethetik majd.

Az üzletileg kritikus, konvergens infrastruktúra kiterjesztésével a Unix világában már bizonyított technológiák egy része Linux és Windows-alapú, x86-os rendszereken is elérhetővé válik. A 32 processzorfoglalatos DragonHawk-pengék például több száz processzormagig méretezhetők, a szintén x86-os, 2-8 foglalatos, HydraLynx kódnéven fejlesztett pengék a HP BladeSystem robusztus, c-kategóriájú szerverkeretében virtualizációval növelik a rendelkezésre állást, míg az nPartitions (nPars) technológiával az erőforrások megbízható módon oszthatók fel az alkalmazások között.

> „A megoldás fürtözött környezetben automatikusan átmozgatja a szolgáltatáscsomagokat a szerverek között.

Már elérhető Linuxhoz a HP Serviceguard, amelyet Unix környezetben Magyarországon is számos vállalat használ. A megoldás fürtözött környezetben automatikusan átmozgatja a szolgáltatáscsomagokat a szerverek között. Ha erre valamely hardverelem meghibásodása miatt kerül sor, az alkalmazás átlagosan 1-2 percen belül újraindul egy másik kiszolgálón. A megoldás a szerverek működés közben történő karbantartását is megkönnyíti. A Serviceguard linuxos változatának első hazai felhasználói bankok és iparvállalatok közül kerültek ki.

A konvergens infrastruktúra felügyeletét a keretrendszerbe ágyazott HP Analysis Engine x86-os változata rendszerdiagnosztikával és összetett hibák másodperceken belüli, automatikus elhárításával segíti.

Az Odyssey-projekt fejlesztései a HP legmagasabb rendelkezésre állást biztosító NonStop szervereit is érintik, amelyek szintén helyet kaptak a túrakamion fedélzetén, a gyártó nagyadat-alkalmazásokhoz szánt készülékeivel, az SAP HANA és a Microsoft Parallel Warehouse appliance-ekkel együtt.

A HP túrakamionja Budapesten: Intel-architektúrák a raktérben

Az SAP adatközpontja a Walldorf melletti St. Leon-Rotban

Üzleti alkalmazások a HANA-felhőből

Az SAP memóriaalapú vállalatirányítási, ügyfélkapcsolatkezelő- és adattárház-megoldásait felhőszolgáltatásként is kínálja új HANA Enterprise Cloud platformján.

/Írta: Kis Endre

> Az SAP HANA Enterprise Cloud platform leszámol az előítélettel, amely szerint a felhő nem alkalmas összetett, tranzakciós rendszerek futtatására.

Orlandóban megtartott Sapphire Now 2013 konferenciáján az SAP bejelentette, hogy a memóriában futó adatbázis mellett fejlesztőeszközöket és integrációs szolgáltatásokat tartalmazó HANA Enterprise Cloud platformon fogja egységesíteni felhő alapú megoldásainak teljes portfólióját.

Az SAP a konferenciát megelőző napokban mutatta be a HANA Enterprise Cloud platformot, amelyen elsőként az SAP Business Suite nagyvállalati alkalmazáscsomag és Business Warehouse adattárház-megoldás érhető el felhőszolgáltatásként – ezeket a szoftvereket a szervezetek az eddigiekben jellemzően házon belül, saját adatközpontjaikban vezették be.

A 2011-ben bejelentett HANA in-memory adatplatformot – amely eredetileg az analitikai alkalmazásokat támogatta – az SAP rövid időn belül a tranzakciós alkalmazások futtatására is felkészítette: Business One kis- és középvállalati ERP rendszere után idén januárban Business Suite nagyvállalati alkalmazáscsomagját is portolta HANA-ra.

A lépés akkor nagy visszhangot keltett, mivel az in-memory technológia teljesítménye mind a jelentéskészítést, a lekérdezéseket és az összetett elemzéseket nagyon nagy adatmennyiségen is valós idejűvé teszi. Merevlemezeket használó adatbázis-kezelők esetében az eredmények perceket, órákat is váratnak magukra. Az azonnaliság olyan távlatokat nyit a szervezetek előtt, amelyekért már érdemes lehet HANA-ra cserélni az üzleti alkalmazás alatt futó Oracle vagy Microsoft adatbázist.

Az SAP januárban és a mostani bejelentéskor is hangsúlyozta, hogy a választás lehetőségét kívánja biztosítani, és hosszú távon támogatni fogja a többi adatbázis-technológiát is, de HANA melletti elkötelezettsége egyértelmű, és ez érezhető hatással lehet még az adatbázispiacra.

A HANA az eladásokat tekintve már jelenleg is az SAP legsikeresebb termékének számít, amelytől a cég idén mintegy 700 millió euró bevételt vár. Ez az összeg megközelítőleg akkora, mint a legutóbbi negyedév teljes szoftverárbevétele.

Hasso Plattner, az SAP társalapítója és elnöke szerint a felhőplatform még jobban fel fogja gyorsítani a HANA-eladásokat. A vállalatoknak nem kell heteket várniuk a HANA készülékek megérkezésére, projektjeiket órákon belül megkezdhetik. A szolgáltatást elsőként élesben használó Florida Crystals SAP ERP és Business Warehouse alkalmazásait két hónap alatt migrálta a felhőbe. Másrészt az SAP felhőszolgáltatásait használó, több mint 6 ezer szervezet eleve könnyebben léphet a HANA Enterprise Cloud platform irányába. Jelenleg a cég 60 ügyfele dolgozik ilyen projekteken.

Hozd a saját licenced

Az SAP HANA Enterprise Cloud platform leszámol az előítélettel, amely szerint a felhő nem alkalmas összetett, tranzakciós rendszerek futtatására – mondta *Vishal Sikka,* a vállalat technológiai igazgatója a bejelentéskor.

Nem ez az egyedüli dolog, amiben a HANA Enterprise Cloud eltér a többi felhőkörnyezettől. Az in-memory platform ugyanis az adatközpontban nem virtuális gépeken, hanem a vason fut.

Az SAP adatközpontjaiban több száz terabájt memóriát és nagy sebességű hálózati elemeket tartalmazó szerverkonfigurációkat állított össze, és saját fejlesztésű felügyeleti rendszer, a Cloud Frame Monitor eszközeivel grafikus kezelőfelületről biztosítja a felhőkörnyezetekre jellemző, rugalmas erőforrás-kezelést. A szolgáltatást használó ügyfelek nem virtuális gépeket, hanem dedikált tárhelyet, hálózati és feldolgozási kapacitást kapnak HANA-n futó alkalmazásaikhoz.

A szolgáltatás használatának előfeltétele, hogy a szervezet rendelkezzen a HANA és a felhőben futtatni kívánt alkalmazás, például a Business Suite licencével. Az SAP tanácsadói segítenek meghatározni, hogy mely alkalmazások felhőbe vitele járna a legnagyobb előnnyel, majd a költözést is migrációs szolgáltatásokkal támogatják.

Az ügyfél ezt követően havi díjat fizet a menedzselt felhőszolgáltatás használatáért az alkalmazás méretének, adatintenzitásának függvényében. Az idő majd megmutatja, hogy ezt a „hozd a saját licenced"-konstrukciót minden, felhő iránt érdeklődő vállalat kellően rugalmasnak fogja-e találni.

Mobilmenedzsment a felhőből

A termékfejlesztés mellett az SAP a közelmúltban cégfelvásárlások útján is bővítette felhőalapú megoldásainak portfólióját. A SuccessFactors HR szolgáltatásai a munkaerő-toborzás, a képzés és a bérszámfejtés folyamatait támogatják, az Arriba megoldásai pedig a beszerzést, a beszállítók kiválasztását segítik többek között analitikai és közösségi eszközökkel.

Ezen alkalmazásokat az SAP a jövőben szintén a HANA Enterprise Cloud platformra fogja átültetni, miként saját fejlesztésű szolgáltatásait is, amelyeket a stratégia jegyében már átnevezett: a Financials OnDemand mostantól Cloud for Financials, a Travel OnDemand pedig Cloud for Travel néven lesz ismert.

A SuccessFactors felvásárlásával az SAP portfóliójába került, felhőalapú Jam vállalati közösségi kollaborációs alkalmazás funkciói a továbbiakban szintén megjelennek majd ezekben a szolgáltatásokban. Az Arriba Spend Analytics költségelemző szoftvere már HANA platformon fut, a többi alkalmazás a következő hónapokban követheti, de a portolás pontos ütemterve egyelőre nem ismert.

Az SAP a HANA Enterprise Cloud platformon elérhető fejlesztőkörnyezetet is bemutatott Orlandóban, amellyel a független szoftvercégek és az induló vállalkozások a felhőben futó in-memory adatplatformra készíthetnek alkalmazásokat. További bejelentés, hogy a Business Suite HANA-n futó változata a januártól mostanáig tartó, bevezetési időszak után immár világszerte elérhető, 25 iparág számára készült kiterjesztéseivel együtt.

Hasso Plattner, az SAP elnöke

A Sapphire Now 2013 konferencián debütált az SAP Mobile Secure menedzsmentmegoldása is, amellyel a nagyvállalatok mobileszközeiket, alkalmazásaikat és tartalmaikat felügyelhetik minden elterjedt mobilplatformon. A megoldás az SAP Afaria felhőszolgáltatásként elérhető változatát is tartalmazza, amelyet a szervezetek felhasználónként havi egy euróért használhatnak a mobileszközök menedzselésére.

SAP Fiori néven egy app-gyűjtemény is készült – első kiadása 25 alkalmazást tartalmaz, amely a cég üzleti szoftvereinek leggyakrabban használt funkcióit teszi elérhetővé mobileszközökön, hangsúlyozottan felhasználóbarát kezelőfelületen keresztül.

Megjelent az SAP Business One 9.0 verziója is, melynek HANA platformon futó változata egyelőre korlátozottan érhető el. A kis- és középvállalati ERP megoldást az SAP az Arriba hálózatával integrálta, így a felhasználók számos folyamaton keresztül automatizálhatják beszállítókkal és vásárlókkal kialakított kapcsolataikat a felhőben.

IRÁNYÍTÓKÖZPONT IT-PROJEKTEKHEZ

Az SAP HANA Enterprise Cloud platformot a vállalat a világ több pontján kialakított adatközpontjaiban működteti, de a jövőben a hosztingpartnerek is kínálhatják majd a szolgáltatást.
Az adatközpontok egyike a németországi Walldorfban, az SAP székhelyén található, ahonnét az európai újságírókkal együtt telepresence kapcsolaton keresztül követtük a Sapphire Now konferencia eseményeit.
A walldorfi adatközpontot három, földrajzilag elkülönített létesítmény alkotja, amelyek között az SAP a teljes környezetet replikálja. Az SAP 6 fő adatközpontja világszerte több mint 20 ezer fizikai és 45 ezer virtuális szervert, 14 ezer alkalmazást működtetnek, a biztonsági mentések mérete meghaladja a napi 400 terabájtot.
Ugyancsak Walldorfban működik az április végén bejelentett Mission Control Center létesítmények egyike. Az SAP Active Global Support szervezethez tartozó támogató központok többek között az SAP HANA platform, a felhőalapú és a mobil megoldások bevezetését és működtetését segítik a cég ügyfeleinél kialakított Innovation Control és Operation Control központokkal együttműködve, a megoldások teljes életciklusán keresztül. A Mission Control Center támogatását az SAP MaxAttention és ActiveEmbedded szolgáltatásait használó vállalatok meglévő szerződésük részeként megkapják.
További MCC-k jelenleg Kínában és az Egyesült Államokban működnek, de az SAP további központokat fog nyitni Brazíliában és Mexikóban is.

ADATKÖZPONTI SZOLGÁLTATÁSOK

Centrális vonzások és taszítások

Öt évre szóló előrejelzése szerint a virtuálisszerverbérlet-szolgáltatás nő majd legnagyobb ütemben, a kolokáció pedig mindössze évi 2 százalékkal bővül – a piackutató IDC egy regionális kutatás eredményeiről adott tájékoztatást lapunknak.

KIS ENDRE

Közép-Európában a vállalatok negyede még mindig az irodában, úgyszólván az íróasztal mellett tartja szervereit – derült ki az International Data Corporation (IDC) felméréséből (IDC IT Buyers Pulse, 2012). Az informatikai beruházásokkal kapcsolatos terveket feltérképező piacelemző 291 végfelhasználó vállalatot kérdezett meg a múlt év végén Csehországban, Magyarországon és Lengyelországban többek között arról, hogy hol tárolják elsődleges szervereiket (lásd az 1. ábrát). A válaszadók közel fele külön szerverszobát hozott létre az iroda területén, míg valamivel több mint ötöde saját adatközponttal is rendelkezik. A külső adatközponti szolgáltatást használó szervezetek aránya a 8 százalékot sem éri el.

– Magyarországon ennél kedvezőbb a helyzet, a külső adatközponti szolgáltatást használó vállalatok aránya a KKV-k között eléri a 16 százalékot, ami a régiós átlag kétszeresének felel meg. A nagyvállalatok körében (100 fő felett) ugyanakkor a saját adatközpont-használat felé tolódnak az arányok – mondta *Balicza Gábor,* az IDC Hungary vezető elemzője. – A legnépszerűbb szolgáltatások közé a szerverelhelyezés és a hozzá kapcsolódó monitoring, illetve felügyeleti szolgáltatások tartoznak, a hardver- és virtuálisszerver-bérlet még kevéssé terjedt el, ám az adatok egyértelműen az adatközponti szolgáltatások iránti nagyobb nyitottságot tükrözik.

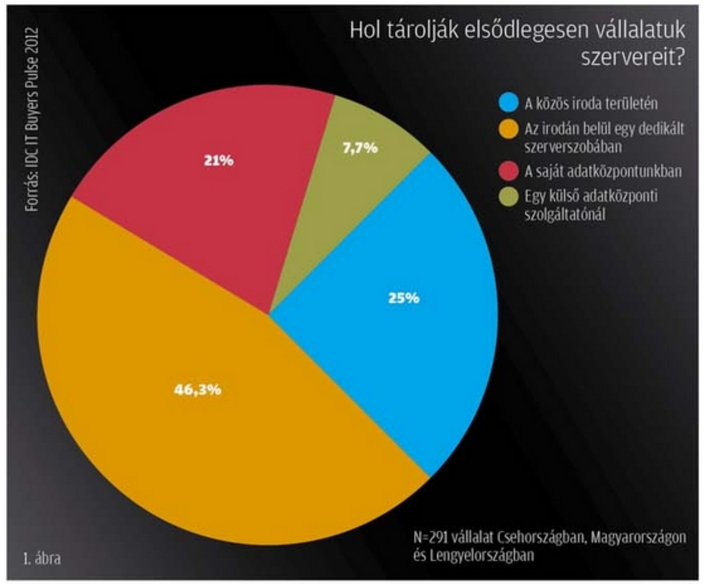
A felmérésben részt vevő, adatközpontot használó 82 vállalat több mint fele a következő egy évben nem tervez különösebb fejlesztéseket e téren (lásd a 2. ábrát), Magyarországon azonban kétharmaduk nyilatkozott hasonlóan. A vállalatok negyede készül új adatközpont építésére vagy a meglévő bővítésére, de Magyarországon ez az arány is csupán 10 százalék körüli. Régiós szinten a megkérdezett vállalatok mindössze 11,1 százaléka mondta azt, hogy alapterület bérlésére készül külső adatközponti szolgáltatónál.

Fogyasztás alapú elszámolás

Az IDC a kapacitásbiztosítással és üzemeltetéssel összefüggő szolgáltatásokat sorolja az adatközponti szolgáltatások közé. Ezt fontos megjegyezni, az adatközpontok építése és működtetése ugyanis az IT-piac szinte valamennyi szegmensét érinti – ezek teljesítményét a piacelemző külön-külön méri. Adatközponti szolgáltatások alatt ezért a továbbiakban a kolokációt, a hosztingot, valamint a hardver- és a virtuálisszerver-bérletet értjük.

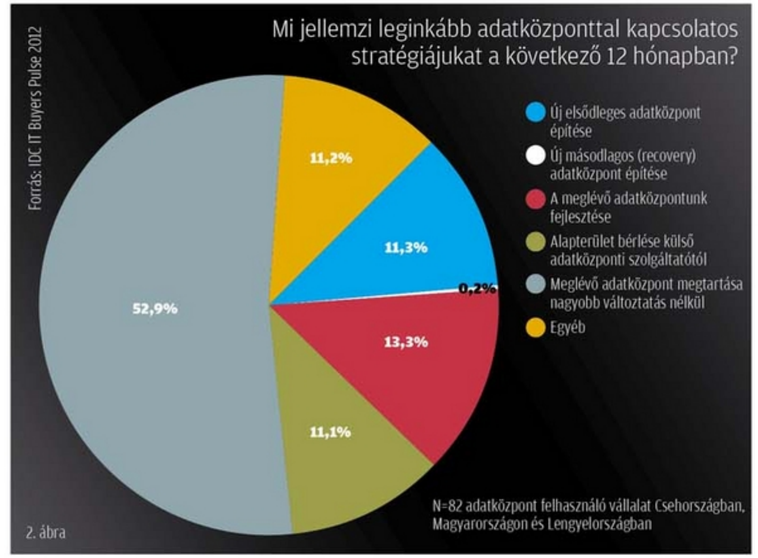
Némi egyszerűsítéssel a szolgáltatókat szintén e három kategóriába sorolhatjuk: a kolokációs szolgáltatók alapterületet, áramellátást, hűtést és fizikai védelmet kínálnak a szerverek elhelyezéséhez. A szerverek és alkalmazások üzemeltetésére szakosodott hosztingszolgáltatók többnyire maguk is kolokációs szolgáltatásokat vesznek igénybe. A hardver- és virtuálisszerver-bérletet is kínáló szolgáltatók esetében ez gyakran egy sokkal átfogóbb szolgáltatáscsomag részét, annak infrastrukturális alapját képezi.

A kolokációs szolgáltatók az eddigiekben négyzetméter alapján számolták a bérleti díjat. A technológia gyors ütemű fejlődése azonban mind nagyobb teljesítménysűrűség elérését teszi lehetővé egy négyzetméteren, amit nagyobb hűtésigény kísér, másrészt az infrastruktúra mind kisebb részegységeinek energiafogyasztása is jól mérhetővé válik, ezért mindinkább előtérbe kerül az energiafogyasztás alapján történő díjelszámolás.



1. ábra

Nagyban hozzájárult a teljesítménysűrűség növekedése ahhoz is, hogy a távközlési cégek megerősödtek az adatközponti szolgáltatások területén, a magyar piac legnagyobb szereplői közülük, illetve leányvállalataik és partnereik közül kerülnek ki. Itt jegyezzük meg, hogy a távközlési cégek felhőinfrastruktúrán, több-bérlős – úgynevezett multi-tenant környezetben – is kínálnak szolgáltatásokat, de ezeket az IDC nem az adatközponti szolgáltatások, hanem a cloud-piac részeként méri.



2. ábra

Virtuális bérlés

Az IDC adatai szerint Magyarországon a kolokáció – a szerverek polcos, illetve rackszekrényben történő elhelyezése – adja az adatközponti szolgáltatások piacának mintegy 33 százalékát kitevő szeletét. Az infrastruktúra-hoszting – a hardver- és virtuálisszerver-bérlettel, valamint menedzsmentszolgáltatásokkal együtt – a piac 40 százalékát, míg az alkalmazáshoszting körülbelül a 25 százalékát teszi ki.

– A kolokációs szolgáltatások piaci részesedése azonban egyre kisebb – mondta Balicza Gábor. – E területen már 2011-ben is 10 százalékos csökkenést regisztráltunk az azt megelőző évhez képest, és előzetes adataink alapján a kolokáció 2012-t is hasonló eredménnyel zárta. Végleges számokat nyárra elkészülő jelentésünkben adunk majd közre. A kolokációs piac csökkenéséhez a teljesítménysűrűség említett növekedésénél is nagyobb mértékben járul hozzá a multinacionális cégeknél zajló adatközpont-konszolidáció. Az utóbbi két évben több meghatározó ügyfél is elvitte adatközpontját Magyarországról, érezhetően csökkentve a kolokációs szolgáltatásokból származó bevételeket. Észak-Európában például több olyan, nagyon nagy méretű adatközpont is épült, amely a helyben termelt energia és a hűtést segítő, hidegebb éghajlat folytán versenyképesebb szolgáltatásokat kínál, és elcsábítja az ügyfeleket más térségekből.

A szerverek vállalaton kívüli elhelyezésében a kolokáció az adatközponti szolgáltatások belépő szintjét képviseli, ha úgy tetszik, ez a szállás reggelivel. A spektrum másik végén a virtuálisszerver-bérlet felel meg az elnöki lakosztálynak.

> A szerverek és alkalmazások üzemeltetésére szakosodott hosztingszolgáltatók többnyire maguk is kolokációs szolgáltatásokat használnak.

– E szegmensben a szolgáltatói bevételek gyorsabban nőnek a magyar piacon, mint amilyen ütemben a kolokáció részesedése csökken – mondta az elemző. – Az erős kétszámjegyű növekedés ellenére a virtuálisszerver-bérlet szegmense egyelőre a piac mindössze 1-2 százalékát adja. Tekintve, hogy a virtualizáció korántsem idegen a hazai vállalatoktól, ez első látásra meglepően alacsony aránynak tűnhet. A 2005 körül indult szervervirtualizáció azonban mostanáig a vállalati adatközpont falain belül zajlott. A tesztkörnyezetek virtualizálása után a szervezetek 2008-2009-től kezdték élesben is használni a technológiát, és mára terjedt el a szolgáltatásközpontú szemlélet, amely az erőforrások szabad mozgatását, bérlését és összekapcsolását is elfogadja. A virtuálisszerver-bérlet térhódításának feltételei napjainkra értek be. Hozzátenném azonban, hogy míg régiónkban a virtualizált szerverek aránya eléri a 25 százalékot, addig Magyarországon közelebb állunk a 20 százalékhoz, e téren van még hová fejlődnünk.

Virtuális szervert elsősorban kis- és középvállalatok bérelnek, a házon belüli korlátozott IT-erőforrások miatt kézenfekvő számukra, hogy külső szolgáltatásokat vesznek igénybe. A nagyvállalatok először saját adatközpontjukat virtualizálják, ezért náluk csak később merül fel, hogy a további virtuális szervereket már béreljék.

– A kolokációs szolgáltatások szegmense a következő öt évben átlagosan 2 százalékkal nőhet Magyarországon, idén azonban inkább stagnálást várhatunk – adott előrejelzést Balicza Gábor. – A piac alakulását azonban erősen befolyásolhatja, ha újabb multinacionális cégek döntenek adatközpontjuk elviteléről vagy idehozataláról. Az infrastruktúra-hoszting szegmensében mind a polcos és a rackes szerverelhelyezés, mind a hardverbérlet terén visszafogott, 5 százalék körüli éves növekedésre számítunk ebben az időszakban, míg a virtuálisszerver-bérlet évi 10 százalékot meghaladó mértékben nőhet a következő öt évben is. A tisztán kolokációs szolgáltatásokat kínáló piaci szereplőknek ezért előbb-utóbb lépniük kell, vagy elmozdulnak a nagyobb hozzáadott értéket hordozó hosztingszolgáltatások irányába, vagy amire már látunk példát, magánfelhő-környezeteket fogadnak be létesítményeikbe.

ILLÉS MÁRTON

technológiai igazgató
BalaBit IT Security

Teszt a kezdet, avagy a TDD természetrajza

Szoftvert fejleszteni nem könnyű, különösen nem megfelelő minőségben, a kívánt funkciókkal, határidőre és a kitűzött költségkereten belül maradva. Legyen szó egy egyszeri projektről, vagy akár egy dobozos termék következő verziójáról.

> ...először tesztelünk, majd fejlesztünk, aztán amikor ezzel is készen vagyunk, akkor megtervezzük, vagy inkább újratervezzük az egészet. Elsőre meredeknek hangzik, nem?

Aki már csinálta, tudja, hogy mindennek megfelelni szinte lehetetlen, nagy a nyomás az ügyfél, a menedzsment és természetesen a fejlesztők oldaláról is. Mondhatjuk persze, hogy megfelelő előkészítéssel, tervezéssel és egy jó csapattal azért megoldható. Ám tegyük egy pillanatra a kezünket a szívünkre, fordult-e már elő, hogy mindezek ellenére valami mégis közbejött, pár dolog megcsúszott, kidőlt egy csontváz a szekrényből, megváltoztak az igények menet közben? Valószínűleg a válasz igen, sőt lehet, hogy ez nem csak egyszer, elvétve fordult elő, hanem többször, egymás után, vagy akár szinte mindig.

Aztán ha csúszunk, akkor jönnek az egyszerűsítések: nem kell ez a feature, a másikat elég lesz egyszerűbben is megcsinálni, itt-ott egy-két ideiglenes megoldás, automata tesztek helyett elég lesz csak kézzel kipróbálni, vagy majd az ügyfélnél teszteljük... Ezek után, amikor jön a továbbfejlesztés, a csontvázak már előre be vannak építve a rendszerbe, persze lehet majd refaktorálni, rendet rakni, csak ki lesz az, aki hozzá mer nyúlni a kódhoz? Hiszen ami most van, az legalább működik, ne próbáljuk megjavítani azt, ami nincs eltörve, nem?

A legtöbb esetben a probléma nem akkor jelentkezik, amikor valaki megír egy kódot, hanem amikor valaki más – vagy akár az eredeti szerző később – hozzányúl, belejavít, kiegészíti. Ilyenkor kezd el a kód minősége romlani, főleg ha jönnek az új funkciók, az új elvárások és persze az időnyomás, ezek pedig általában mindig kikerülhetetlenek.

Ilyen esetekben a szokásos első reakció, hogy megpróbálunk még részletesebben tervezni, felkészülni még aprólékosabban és még több lehetőségre. Megszorozzuk a fejlesztői becsléseket kettővel, hárommal, ízlés és tapasztalat szerint. A tervezésre, előkészítésre szánt idő tovább nyúlik, a fejlesztés lassul, a határidő csúszik, a végén pedig újra jön az egyszerűsítés – és jó, ha egyáltalán valami működőt lehet az ügyfélnek leszállítani.

Sajnos, végeredményben – legyünk akár megrendelők vagy szállítók – itt a probléma. Megrendelőként persze kiköthetünk kötbért, de a csúszás akkor is fáj, a továbbfejlesztés lassabb és drágább, azaz nehezebben tudunk reagálni a változó üzleti igényekre, hátrányba kerülhetünk a versenytársakkal szemben, és csak reménykedhetünk, hogy náluk sem jobb a helyzet.

Nehéz ebből az ördögi körből kitörni – aki már átélte, tudja, aki éppen benne van, az keresi a kiutat.

Szerencsére nem vagyunk egyedül, a probléma megoldásán már sokan gondolkoznak és több különböző válasz is született vagy éppen jelenleg is formálódik. Ennek eredményeként jött létre több agilis módszertan: SCRUM, Kanban, eXtream Programing, Pair programing, stb. A lista hosszú. Nem lehet kijelenteni, hogy ezek közül valamelyik a legjobb vagy legbiztosabb, hiszen a szervezetek különbözőek, mint ahogy a feladatok és az elvárások is, nincs csodafegyver, érdemes kipróbálni többet és kiválasztani a leginkább testhez állót. Egy a fontos: nyitottnak és agilisnak kell lenni.

Mi is végigjártuk a magunk útját, még most is járjuk, sőt talán a legfontosabb felismerés az, hogy ennek az útnak soha sincs vége. Nincs egy cél, ahol megpihenhetünk és hátradőlhetünk, hanem folyamatosan fejlesztenünk kell magunkat, a kollégákat, a módszereket. Rémisztő? Szerintem inkább inspiráló!

Ezen az úton mi is eljutottunk egy módszertaning, amely megtetszett nekünk és jelenleg is alkalmazzuk. Nem csodafegyver ez sem, bár a talpáról a tetejére állított sok mindent a fejlesztésen és a fejekben. Ez a módszertan vagy inkább megközelítés a Test Driven Development (TDD), avagy a tesztelésvezérelt fejlesztés. Hadd meséljek kicsit erről és a mi tapasztalatainkról.

Az iskolában megtanultuk, hogy a szoftverfejlesztésnek három nagyon fontos fázisa van: az első a tervezés, a második a fejlesztés, a harmadik pedig a tesztelés. A TDD gyakorlatilag megfordítja ezt: először tesztelünk, majd fejlesztünk, aztán amikor ezzel is készen vagyunk, akkor megtervezzük, vagy inkább újratervezzük az egészet. Elsőre meredeknek hangzik, nem? Nézzük meg gyorsan, hogyan működik ez a gyakorlatban!

Lényege a TDD-nek, hogy a tesztelés-fejlesztés iterációk gyorsan pörögjenek. Első lépésként az elvárásoknak megfelelően elkészül az első tesztet, amely természetesen egyből hibázik. A fejlesztés részeként pedig egy a cél, kipipálni a tesztesetet, azaz éppen csak annyit fejleszteni, amennyi a tesztesethez szükséges. Ha ez megvan, akkor jöhet a második teszteset, majd az ahhoz tartozó fejlesztés, ahol viszont az első teszteset biztosítja, hogy ne rontsunk el semmit, ami már egyszer működött. Ilyen kis lépésekkel jut el a fejlesztés oda, hogy elkészüljön az alkalmazás az összes elvárásnak és funkciónak megfelelően.

Az biztos, hogy e módszerrel nem fordulhat elő, hogy a tesztesetek lemaradnak a fejlesztés végén, de joggal kérdezheti bárki, hogy hol marad az architektúra megtervezése, illetve nem lesz-e teljesen szedett-vedett a kód? A kérdés jogos, és e ponton jutunk el a tervezés fázishoz. Miután megvannak a tesztesetek és a kód is kész, jöhet a refaktorizáció, avagy a kód és az architektúra rendberakása. A lényegi különbség a TDD esetében, hogy a fejlesztők bármilyen módosítás után a tesztesetekkel egyből ellenőrizhetik, hogy nem törtek-e el valamit, azaz kis kockázattal lehet nagyobb kódmódosításokat is elvégezni. A refaktorizáció a TDD esetében nem egy külön – nagy kockázatú – projekt, hanem a fejlesztés egy folyamatos eszköze, ez garantálja, hogy a kód ne kezdjen el romlani, hanem a folyamatos változások után is megőrizze minőségét.

Amint funkcionálisan elkészül valami és a teszteset működik, egyből jön a kód rendberakása, ezáltal az architektúra folyamatosan közelít az ideálishoz. Nem kell esetleges jövőbeli funkciókra már előre felkészülni, nincs szükség nagy átalakítási projektekre, amikor új igények merülnek fel, és nincsenek feleslegesen előre lefejlesztett modulok, amelyek esetleg majd jók lesznek valamire. Az készül el, amire szükség van, más nem. Cserébe – az igények menet közbeni változtatása esetén – csak a teszteseteket kell módosítani vagy kibővíteni, és a fejlesztés részeként javítani őket. Az architektúrát pedig szintén könnyebb később ehhez hozzáigazítani. A folyamatos refaktorizáció, rendrakás a kulcs a TDD működőképessége szempontjából, gondoskodni kell arról, hogy ez ne maradjon el, tényleg beépüljön az alaprutinba.

A tesztesetek előre való elkészítésének a másik fontos előnye az, hogy a fejlesztőknek már a fejlesztés kezdetén meg kell érteniük a követelményeket. Azzal, hogy tesztelést első helyre helyezzük, egyenrangúvá válik a fejlesztéssel, ez segít csökkenteni a fejlesztő és a tesztelő közötti távolságot, sőt jobban kényszeríti a fejlesztőket a tesztelésre. Nagyon fontos, hogy ezek után az automata tesztek minősége kritikus, azokat úgy kell kezelni, mint a termék saját kódjait.

Nem csodafegyver a TDD, nem old meg minden problémát, de új szemléletet képvisel a fejlesztésben. A változás főleg a napi rutinokban és a fejekben nem megy egyik napról a másikra, a meglévő kódokat is csak lassan lehet megtisztítani, az automatatesteseteket elkészíteni – az elején befektetést igényel, ami csak a később térül meg. A TDD-nek is megvannak a maga hibái, buktatói, amelyek odafigyelést és energiát igényelnek. A menedzsmentnek és a megrendelőnek is meg kell értenie a módszert, támogatnia kell és nem utolsó sorban kihasználnia a TDD adta lehetőségeket.

Vállalati jóhírnév: az informatikán áll vagy bukik

Biztonság, üzletmenet-folytonosság, technikai támogatás – a topvezetők szerint a legtöbb cégnél e három területen jelentkezik a vállalati reputációt leginkább fenyegető kockázat.

Ha a cég hírneve csorbát szenved, nem biztos, hogy a vállalati PR-os fogja megoldani a gondjainkat – ez az IBM csaknem félezer vezető megkérdezésével végzett Risk & IT felmérésének egyik fontos tanulsága. A kutatás, melyben észak-amerikai, európai és ázsiai vezetők – közel felearányban topmenedzserek – vettek részt, a vállalati reputáció és az informatikai zavarokból fakadó problémák összefüggéseit vizsgálta.

A vezetők válaszaiból kiderül, hogy a vállalatok egyre komolyabban veszik az informatikai rendszer működéséből fakadó hibák és zavarok kezelését, hiszen azok a hírnév alappilléreit, az üzemszerű működést, az ügyfélkapcsolatot és a bizalmat veszélyeztetik. Az ügyvezetők az informatikai és pénzügyi vezetőkkel egyetértésben az adatlopást tekintik a legnagyobb reputációs kockázatnak, amit az adatvesztés és a rendszerhiba követ, de komoly rizikónak tűnik a céges weboldal kiesése is. A marketingvezetők azt mondják, a technikai támogatás zavarai olyan sebeket ejtenek a vállalat imázsán, melyek csak egy, vagy rosszabb esetben két év múlva gyógyulnak. A reputáció szempontjából tehát egyre inkább a biztonság, az üzletmenet-folytonosság és a technikai támogatás a legnagyobb odafigyelést igénylő területek.

Ha informatikai probléma adódik, az IT-felelősök szerint a kommunikációnak gyorsnak, pontosnak és brutálisan őszintének kell lennie, de érdemes hosszú távon is átgondolni a jóhírnév védelmében meghozható intézkedéseket. Ilyen lehet például a vállalati kockázatkezelési stratégia fejlesztése. Fontos, hogy az informatikai vezetők rendszeresen konzultáljanak profi kockázatkezelési szakértőkkel, és készítsenek átfogó hírnévvesztési kockázati profilt a vállalat számára. Fontos a forgatókönyv-elemzés, különösen az újonnan bevezetett technológiák esetében, így a váratlan események is könnyebben elkerülhetők. Számtalan esettanulmány létezik, amely a „mi lenne, ha" típusú tervezés alapját képezheti, megéri rendszeresen olvasgatni őket. Érdemes kockázatbecslést készíteni az egész ellátási láncra vonatkozóan: egy távoli beszállítónál jelentkező hiba éppúgy végzetes lehet, mint egy belső probléma. Ráadásul a kockázatfelügyeletet a kulcsfontosságú szereplők összehangoltan végezhetik.

Ahogy az IBM kutatásából kiderül, a vezetők többsége tisztában van a digitális környezetből fakadó kommunikációs kockázatokkal, és egyre jobban ügyel az informatikai rendszer megbízható működtetésére. Ha szükséges, arra is hajlandók, hogy új befektetésekkel erősítsék meg a védvonalaikat, amelyek a vállalat IT-biztonsága mellett a cég jóhírnevét is őrzik. ■

TERVKERETREND

James Bond és az üzletfolytonosság

A vállalatoknak manapság ahhoz, hogy működni tudjanak, hozzá kell férniük az adataikhoz, különben igen rövid idő alatt teljesen megbénulhatnak. Ennek ellenére a cégek jelentős részének nincsen rá terve, hogy mihez kezd, ha előáll egy vészhelyzet. A megoldást az üzleti folytonosság tervezése és menedzsmentje (BCM) adhatja. Összeszedtük hozzá a legfontosabb elemeket.

/Írta: Meixner Zoltán

A brit titkosszolgálat, az MI5 a következőt írta a miniszterelnöki kabinetirodának egy terrorelhárításról szóló 2005-ös jelentésében: „Minden évben majdnem minden ötödik vállalkozás jelentős működési zavart szenved el, és széles körben úgy gondolják, hogy e zavarokkal foglalkozni jó üzleti érzék kérdése. A hatékony üzleti folytonosság tervezése kritikus abból a szempontból, hogy a szervezetek alapvető funkciói tovább működhessenek vészhelyzet esetén is."

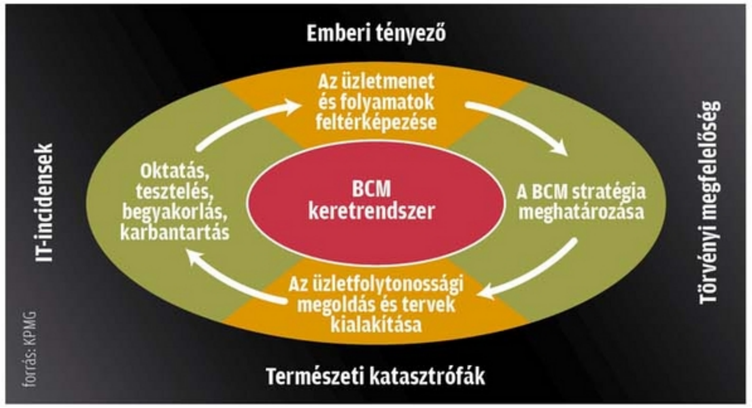
A vészhelyzetek megoldásához James Bondot is ki lehet hívni, de talán jobb észben tartani, hogy minden terv annyit ér, amennyit megvalósítanak belőle. Úgy is mondhatnánk, hogy megfelelő menedzsment nélkül az alapfunkciók működésének fenntartása vagy gyors helyreállítása elképzelhetetlen. A működési zavarok (közöttük a természeti katasztrófák, a kulcsemberek elveszítése, a szervezet elleni rosszindulatú támadások vagy éppen a véletlen balesetek) kivédésére csak akkor van esély, ha ezzel folyamatosan és rendezett keretek között foglalkoznak. E tevékenységben vannak olyan kulcsfontosságú tényezők, amelyekre újra és újra vissza kell térni. Így rendszeresen vizsgálni kell, hogy a működéshez nélkülözhetetlen funkciók leállásának milyen hatása van az üzletre. Hasonló rendszerességgel kell értékelni a fenyegető kockázatokat. Ha új kockázatok jelennek meg, akkor azt is vizsgálni kell, hogy a kialakított védekezési és helyreállítási eljárások megfelelő választ tudnak-e adni ezekre, s ha nem, úgy mit kell megváltoztatni. A kockázatokról és fenyegetésekről folyamatosan kommunikálni kell, az alkalmazottak gyakorlatozásai során kell kipróbálni a védekezési eljárásokat, illetve rendszeresen tesztelni és auditáltatni kell a terveket. Ez így együtt elég macerásnak hangzik.

Talán ez volt az oka, hogy a KPMG 2011-es BCM-felmérése idején a magyar vállalatok több mint kétharmadának még nem volt kész és működőképes üzletfolytonossági modellje. Egy év alatt azonban nagyot javult a helyzet. A tanácsadó cég 2012 végén publikált jelentése szerint a vizsgált cégek kétharmadának volt már működőképes BCM-keretrendszere. Nagyon örülni azonban még nem érdemes, mert e rendszereket csak ritkán tanúsítják BCM-specifikus szabványok (például az ISO 22301:2012) szerint, elvétve találkozni dedikált BCM-költségvetéssel, továbbá a BCM-keretrendszert kiépítők 60 százaléka szkeptikus annak működőképességét illetően. A bizonytalanságot részben az okozza, hogy a válaszadók fele még nem kényszerült a tervei használatára, így nem tudni, hogy azok jók-e, de a terveket nem is auditáltatták, ezért független szakértői vélemény sincs a birtokukban.

A tervek minősége valóban felvet kérdéseket, hiszen a KPMG szerint azoknak a cégeknek a negyede, amelyeknek van üzletfolytonossági keretrendszerük, nem készítette el üzletihatás-elemzést (BIA) sem. Nem világos tehát, hogy mire alapozták terveiket, mégis 41 százalékuk szerint stabil és működőképes a BCM-jük.

Ha a reményeket meghaladják a kétségek, érdemes pár ellenőrző kérdést feltenni. A legfontosabbak a következők: a BCP átesett felülvizsgálaton vagy teszten az elmúlt egy évben? Van a BCP-ben egy olyan jelzőérték, amelynek a túllépése aktiválja a tervet? Részt vesz-e a stáb rendszeres tréningeken, ahol a terv végrehajtását gyakorolja? Van olyan felsővezető, aki elkötelezett a BCM mellett? Van kijelölt BCM-vezető a cégnél? A terv jól dokumentált és könnyen elérhető azon munkatársak számára, akik érintetté válnak az aktiválódásakor?

Az Európai Unió hálózati és információbiztonsági ügynöksége, az ENISA meghatározta, hogy miféle tényezők hatásai miatt kell elsősorban vigyázni, és üzletfolytonossági menedzsmentet alkalmazni. Először is azoknak a vállalatoknak kell ébernek lenniük, amelyek jogi és szabályozási oldalról vannak kitéve veszélyeknek. Ezek a szervezetek ugyanis olyan bizalmas, illetve személyes ügyfél-információkat tartanak, amelyeknek a kezelésére kötelező törvényi előírások vonatkoznak. Az adatok elvesztése vagy megsemmisítése miatt a szabályozó testületek jelentős bírságot szabhatnak ki. Illetve ha az ügyfelek nem férnek hozzá ezekhez az adatokhoz az előírt szinten és ez üzleti veszteséget okoz a számukra, az perek forrása lehet.



A termelékenység is fontos tényező. A szolgáltatások és a működési folyamatok nagymértékben függenek az információs rendszerektől, az alkalmazásoktól és a külső szolgáltatásoktól. Ha megszakadnak ezek a szolgáltatások vagy működési folyamatok, az elviselhetetlen termelékenységcsökkenést eredményezhet. Emiatt pedig jelentős költségek és erőfeszítések szükségesek az üzleti tevékenység helyreállításához és a piaci veszteség eltüntetéséhez – mondja az ENISA.

A szervezet szerint a pénzügyi stabilitás veszélyeztetésére is figyelni kell, mert ha nem lehet elérni egy cég termékeit vagy szolgáltatásait, az kevesebb, mint egy nap alatt jelentős egyszeri pénzügyi veszteséghez vezet, ami nem tolerálható. A vállalatok egy része ma már folyamatosan online szolgáltatásokat nyújt, vagy az interneten kereskedik. Ha elvész az online jelenlét, annak közvetlen pénzügyi veszteség a vége. De hatalmas bírságot vonhat maga után, ha a cégek nem tartják be a jogi és szabályozási követelményeket, s ez szintén elviselhetetlen pénzügyi veszteséget okozhat.

Az ENISA végül felhívja a figyelmet, hogy bajba kerülhetnek azok a társaságok is, amelyek a hírneve sérül, és vele együtt oda lesz a fogyasztói bizalom is. Ha egy szolgáltatás nem működik, az közvetlen hatást gyakorol a cég reputációjára, ami pedig kevesebb termék és szolgáltatás megvásárlását eredményezi.

TÍZ FONTOS LÉPÉS

Az Attainium amerikai szakcég szerint a következő tíz lépéssel el lehet jutni a megfelelő üzletfolytonossági terv felállításához.

1. lépés: Meg kell szerezni a felsővezetők támogatását, és elfogadtatni velük, hogy szükség van az üzletfolytonossági tervre. Illetve rá kell venni a vezetőket, hogy erről győzzenek meg mindenkit a szervezet minden szintjén.

2. lépés: A kulcspontok azonosítása és számszerűsítése nélkül nem lehet elkezdeni a folyamatot. Ezért a vezetőknek fel kell tenniük a kérdést, hogy melyek a szervezet legfontosabb üzleti funkciói, és ezek közül melyek nélkülözhetetlenek a működés fenntartásában. A különböző részlegek irányítóinak a saját fennhatóságuk alatt lévő területen azonosítaniuk kell e funkciókat, amelyeket a lehető leghamarabb újra kell indítani, helyre kell állítani, s arra kell tervet készíteni, hogy ezt miként lehet elérni a lehető leghamarabb.

3. lépés: Aktív kockázatkezelésre van szükség, amely a cég létesítményeit fenyegető potenciális veszélyek felmérésével, azonosításával kezdődik. A vezetőknek ezért át kell gondolniuk az épületek elhelyezkedését. A kockázat nagyságát a valószínűség és a várható behatások mértékének szorzata adja. Ezzel az egyenlettel közelebb lehet jutni azokhoz a katasztrófákhoz és fenyegetésekhez, amelyekkel az üzletfolytonossági tervnek foglalkoznia kell.

4. lépés: Ha nyakunkon a baj, az első teendők listája leegyszerűsödik, mert csak egyetlen fókusz marad – az emberek és az egészségük védelme, illetve szükség esetén kimentése.

5. lépés: Világos parancsnoki struktúra kialakítására van szükség, hogy mindenki ismerje az intézkedésre feljogosított személyeket. Ez a feltétele, hogy a helyreállítási műveleteket gyorsan és hatékonyan végre lehessen hajtani. A professzionális katasztrófa-elhárításnál a parancsnoki lánc általában hat ember mélységű, amely a legfőbb irányítótól az elhárítás frontvonalában lévőkig tart.

6. lépés: A gyakorlatozás a siker záloga. Ezzel lehet elérni, hogy a munkatársak emlékezzenek a teendőikre a katasztrófa bekövetkezésekor, vagy más váratlan, működési zavarokat okozó helyzetekben, illetve az irányítók vészhelyzetben a megfelelő intézkedéseket hozzák meg.

7. lépés: A fenyegetettség tudatosítása a vezetők feladata, mert ennek révén ösztönözhetők a munkatársak a nagyobb figyelemre, és a szervezet működésének szempontjából legfontosabb részlegekkel való együttműködésre a veszélyek megelőzésében.

8. lépés: Az üzletfolytonossági tervet karban kell tartani és a szükséges pontosításokat, változtatásokat ismertetni kell a szervezet tagjaival. A vezetőknek meg kell győződniük, hogy a terv helyesen reflektál a három kritikus elemre, azaz hatékonyan kezeli a változásokat a létesítmények és berendezések, az IT és az emberi erőforrások esetében is.

9. lépés: Minden rendellenesség és működési zavar után ellenőrizni kell, hogy a terv hogyan működött. Ehhez ki kell kérdezni az érintett munkatársakat és vezetőket, felül kell vizsgálni a folyamatokat és el kell végezni a szükséges módosításokat. A zavarok alatt szerzett tapasztalatok elemzésével el lehet dönteni, hogy egyszeri eseményről vagy valamiféle tendenciáról van-e szó, azaz miféle intézkedések szükségesek.

10. lépés: Mindenképpen el kell kerülni a pánikot. A pánik ugyanis – bármilyen jó az üzletfolytonossági terv és bármilyen sok munka és gyakorlatozás áll a hatékony végrehajtása mögött – lerombolhatja a gondosan elrendezett eljárásokat. Ez pedig egyet jelent a szükségesnél nagyobb, vagy sokkal nagyobb veszteségekkel és a normális üzletmenethez való lassúbb visszatéréssel.

GÖNCZY LÁSZLÓ
kutatómérnök
BME MIT Hibatűrő Rendszerek csoport

Informatika nélkül megállhat az élet

A katasztrófaelhárítási terv elkészítésénél az informatikai szakembereknek és a vállalat üzleti vezetőinek együtt kell dolgozni.

/Írta: Mallász Judit

Kétségtelen tény, hogy az informatikai rendszerek működésének egyaránt kiszolgáltatottak a szolgáltatók és a fogyasztók. Az IT-eszközöket és -alkalmazásokat használó cégeknél egy áramszünet, az internetkapcsolat megszakadása vagy egy adatvesztés ugyanúgy katasztrófát jelenthet, mint egy természeti csapás. Egyes kritikus szervezetek (például bankok, biztosítók) számára jogi előírás a katasztrófaelhárítási terv megléte. Számos olyan területen, ahol ugyan nincs ilyen követelmény, szintén legalább az elvárható gondos gyakorlat szintjén indokolt a felkészülés, ezt a de facto szabványok (például ITIL) is támogatják. Mindenekelőtt tehát azt kell felmérni, hogy mik azok a váratlan események, amik az adott cég működését veszélyeztetik. Ezt követi a megoldást jelentő tervek elkészítése.

„A problémakör fő nehézsége, hogy vannak ugyan általános érvényű előírások, ám minden felborul, ha azokat megpróbálják átültetni a gyakorlatba. A tervek, tartalmukat tekintve jellemzően modellekből és táblázatokból állnak, amelyekben az szerepel, hogy az adott cég mit gondol a saját rendszeréről. A valós rendszer azonban sokszor különbözik az elképzelt modelltől. Szerencsére az utóbbi években számos olyan technológia jelent meg, melyek segítségével naprakész képet lehet kapni arról, hogy egy cég hogyan is működik valójában informatikai szempontból" – mutat rá *Gönczy László*, a Műegyetem Méréstechnika és Információs Rendszerek Tanszék Hibatűrő Rendszerek csoportjának kutatómérnöke.

LOGELEMZÉS

Az informatikai rendszerek működésük közben rengeteg adatot termelnek, amelyek tanulságosak lehetnek. A logokból következtetések vonhatók le például a rendszer működéséről, a kiesésekről. Érdemes tehát elgondolkozni azon, hogy miként lehet a logokat figyelni, hasznosítani.

Előnyös a felhő

A felmérésnél kétféle metodikát célszerű követni: lentről fölfelé, valamint föntről lefelé közelíteni a kérdést. Az informatikusok általában szeretnek a konkrét, megfogható számítástechnikai eszközök felől elindulni. Ezt a módszert segítheti, ha az adott cégnek van egy úgynevezett konfigurációmenedzsment-adatbázisa (CMDB), ami lényegében egy leltár, a cég informatikai erőforrásainak automatikusan készített és karbantartott leltára, amely egyben élő képet ad a rendszerről.

A másik, föntről lefelé haladó felmérés jelenti általában a nagyobb kihívást. Ennek során azt kell meghatározni, hogy az adott cég szempontjából melyek azok a funkciók, amelyeknek a kiesése kritikus. Ezen megközelítés alapja a cég üzleti folyamatainak definiálása, akár folyamatmodellek, akár szöveges leírások szintjén. A feladat nem kicsi, hiszen az üzletmenethez kapcsolódó folyamatok száma egy közepes méretű magyar cégnél is több százra rúghat.

Ezután – az üzleti szakterület bevonásával – kockázatelemzéssel meg kell határozni a legfontosabb folyamatokat.

DRP ÉS BLP

A katasztrófahelyzetek megfelelő kezelésére alapvetően kétfajta terv létezik: a katasztrófaelhárítási terv (disaster recovery plan, DRP) és az üzletmenet-folytonossági terv (business continuity plan, BCP). Míg a DRP szorosan nézve a helyreállítással foglalkozik, addig a BCP arra is kitér, hogy miként lehet már a helyreállítás közben is valamilyen – akár csökkent értékű – szolgáltatást nyújtani az ügyfeleknek.

A választásnál több szempontot célszerű figyelembe venni. Az első helyen a pénzügyi szempontok állnak, de fontosak lehetnek a jogi, valamint az adott cég belső szabályozásából adódó szempontok is. Jellemzően azt vizsgálják, hogy egy relatív skálán egy adott időtartamra vonatkoztatva milyen súlyosságú egy rendszer kiesése.

A következő lépésben a kiválasztott folyamatokat össze kell rendelni a cégnél használt erőforrásokkal. Így megmondható, hogy katasztrófa esetén mit kell helyreállítani, illetve minek az alapszintű működése elengedhetetlen. „Ez már egy közepes méretű cégnél is komoly kihívás, hiszen az adott folyamatok gyakorlati megvalósítása gyakran eltér a dokumentációkban foglaltaktól. Sokszor a különböző automatizált és manuális módszerek segítségével történő felderítésnek nincs alternatívája a kritikusnak minősített üzleti folyamatok meghatározására, ami a helyreállítási terv alapja. Fontos, hogy a helyreállítási terv ne csak az informatikai jellegű lépéseket tartalmazza, hanem az ezekhez szükséges szervezeti hátteret is. A szerepkörök definiálásával rögzíteni kell, hogy a cégen belül kik képesek a szükséges helyreállítási lépéseket megtenni, illetve ha házon belül nincs ilyen szakember, akkor milyen tudású, képesítésű külső szakembert kell a feladat elvégzéséhez igénybe venni. A katasztrófaelhárítási terv tehát számos, az informatikán túlmutató elemet is tartalmazhat, ugyanakkor elkészítése önmagában is 'rendet' csinál" – hangsúlyozza a szakember.

Technológiai oldalról nézve a probléma megoldását, a katasztrófaelhárítás folyamatát nagymértékben segíthetik a felhőalapú szolgáltatások, amikor is a cég nem maga üzemelteti az informatikát, vagy ha mégis, akkor is fenntarthat a távolban egy meleg vagy forró tartalékot, amire akár kiesés nélkül átállhat.

Nem szabad megfeledkezni a frissítésről

A katasztrófaelhárítás szempontjából kényes kérdés az informatikai rendszer változásainak időről időre történő nyomon követése. Mivel az ITIL szabványnak része a változáskezelés, azon szervezetek, amelyek az ITIL szerint próbálnak meg működni, könnyebb helyzetben vannak. Itt a katasztrófaelhárítási terv frissítését célszerű lehet akár a változáskezelési folyamat részévé tenni.

A kisebb cégeknél, illetve ott, ahol nem rendelkeznek ITIL jellegű működési kézikönyvvel, legalább a nagyobb hardveres és szoftveres változások után érdemes a tervet frissíteni. Ezen kívül évente legalább egyszer ajánlott ellenőrizni a feltételezéseket (a rendszerek megfelelnek-e a tervben foglaltaknak, a megnevezett munkatársak elérhetőek-e, a szerződések élnek-e stb.)

Hiányzik az emberi erőforrás

Magyarországon a cégeknél még nem általánosan elterjedt a katasztrófaelhárítási és/vagy üzletmenet-folytonossági terv készítése. Annak dacára ez a helyzet, hogy a tervek elkészítéséhez számtalan ingyenes (jellemzően angol nyelvű) forrás áll rendelkezésre. Szó sincs tehát arról, hogy feltétlenül költséges szoftverberuházásban kellene gondolkozni.

„Tapasztalatunk szerint a tervek elkészítésének legfőbb akadálya az emberi erőforrás hiánya. Egy megfelelő elhárítási tervvel számos, manapság igen gyakori rendszerleállást lehetne megelőzni. Ráadásul egy ilyen tervnek járulékos haszna is van. Alkalmazásával teljesebbé válik a rendszerrel kapcsolatos tudás, aminek birtokában akár a hibaokok is kiküszöbölhetők, azaz minimális beruházással megelőzhetők bizonyos katasztrófák. A katasztrófaelhárítási terv költsége természetesen függ a cég méretétől. Nagyságrendje összehasonlítható egy rendszerfelmérési projekt költségével" – tájékoztat Gönczy László.

A katasztrófaelhárítási tervvel egy cég nem csupán az esetleges kiesésekből származó veszteségeket csökkentheti, hanem erőforrásai pontos ismeretében olcsóbbá is teheti üzemeltetését.

Minden cégnek érdemes lehet felmérnie, hogy mivel jár, ha az informatika egy óráig/napig/hétig nem működik. Ha ezt szám-szerűsítik, valószínűleg átlagosnak mondható hazai cégméret esetén is érdemes a katasztrófelhárítással foglalkozni.

A szakember szerint tipikus hiba a katasztrófaelhárítási terv készítésének teljes folyamatát rábízni a rendszergazdára. Nem elég ugyanis a teljes informatikai rendszert feltérképezni, azt is pontosan fel kell mérni, hogy mindebből mire van igazán szükség a cégnél. Ez utóbbi feladatot csak olyasvalaki tudja elvégezni, akinek horizontális rálátása van a cég teljes működésére. (Esetleg több ember láthatja el ezt a feladatot.) Összességében a katasztrófaelhárítási terv elkészítésénél az informatikai szakembereknek – fejlesztőknek és üzemeltetőknek – a vállalat üzleti vezetőivel együtt kell dolgozni.

A területhez kapcsolódóan júniusban Budapesten rendezik meg a hibatűrő módszerek világkonferenciáját, az IEEE/IFIP Dependable Systems and Network Conference 43. kiadását.

FONTOS A DOKUMENTÁLÁS

A BME informatikusképzésének több szakirányán oktatnak katasztrófaelhárítással kapcsolatos ismereteket. Az elmélet gyakorlati alkalmazására vonatkozó ajánlások megismertetésén kívül azt a legfontosabb tudatosítani a szakemberekben, hogy egy informatikai infrastruktúra működtetése maga is üzleti érték, amihez bizonyos üzleti folyamatok tartoznak. Ebből következően elengedhetetlen az informatikai erőforrások pontos modellezése/dokumentálása.

A vállalati IT már nem mindentudó

A technológia folyamatos fejlődése miatt az informatikai osztályok helyzete és működése is folytonosan változik. Átalakul a kontrollingnak nevezett folyamat is, amely során meghatározzák, hogy a cégnek és egyes részlegeinek (köztük az IT-nak) milyen költségkeretek mellett, milyen eszközökkel, miféle és mekkora célokat kell elérni. /Írta: Meixner Zoltán

Mind az IT kontrollingja, mind a kontrolling IT-ja egyre inkább a felhasználókat helyezi a középpontba. *Drótos György*gyel, az IFUA Horváth & Partners partnerével, a Corvinus Egyetem tanszékvezetőjével tekintettük át a változásokat.

Az IT kontrollingja

Az előbbi egyre kevésbé a nagy központi keretek valamilyen racionális szétosztását vagy a nagy központi projektek megvalósításának nyomon követését jelenti. Inkább arra fókuszál, hogy az IT üzemeltetési és fejlesztési költségei hogyan finanszírozhatók meg a felhasználóknak nyújtott szolgáltatások „kiterhelésén" keresztül. Azaz a felhasználóknak olyan mértékben kell hozzájárulniuk az informatikai kiadások fedezéséhez, amennyi rájuk jut az általuk igénybevett IT-szolgáltatások költségei alapján. Ám kiderült, hogy azok a kulcsok, amelyekkel e költségeket eleinte szétosztották, nem igazságosak. Hatalmas különbségek alakulnak ki, ha csak a fejkvóta alapján folyik a szétosztás, vagy ha csak a licenc-költségeket nézik, de nem veszik figyelembe a mögöttük lévő további járulékos kiadásokat. Ha e tételeket végigkövetik, és az alkalmazáshoz nyújtott szakértői támogatást (például helpdesk), a fejlesztőeszközt, az adatbázis-kezelőt, a szervert, a hálózatot is nézik a költségeikkel együtt, akkor a tényleges, okozathű eredmény 30-50 százalékkal is eltérhet az egyszerű kulcsok alapján mechanikusan számított értékektől. Ha az okozathű allokáció megtörtént, kiderült, hogy valójában mi mennyibe került, és a szolgáltatási szintekről szóló megállapodásokat is figyelembe vették, akkor lehet tiszta képről beszélni – fejtette ki Drótos György.

A szolgáltatási listák és az SLA-k (service level agreement – a szolgáltatási szintről szóló megállapodás) kialakítása korábban az IT-kontrollingtól független volt. Jellemzően az IT outsourcing-szolgáltatóknak volt ez a kötelezően elvégzendő feladatuk. Aztán a belső informatika is átvette ezt a gyakorlatot. Ám nem is annyira a felhasználók, hanem a maga védelmére, főleg a felhasználók egyedi, adhoc-jellegű informatikai igényeinek ellensúlyozására. A szolgáltatáslistákkal és az egyes szolgáltatási elemekhez tartozó SLA-kkal azt akarták elérni, hogy rendszerezetten érkezzenek az IT-részleghez a szolgáltatási igények. De akkor még nem volt szó a költségekről.

Csakhogy a kettő összetalálkozott néhány évvel ezelőtt. A hatékonyabb működés érdekében egyre nőtt a nyomás, hogy a tényleges igénybevétel arányában a felhasználókra terheljék az üzemeltetési költségeket. A tervezhető igénybevétel pedig az SLA-k és a szolgáltatási listák alapján jelenik meg, azaz hogy ki, milyen listából, mit és milyen szolgáltatási szinten vesz igénybe. E tételeket már elég jól lehet kalkulálni, s az a felhasználói kör, amelynek van IT-ra fordítható költségvetése, ezek alapján már elég jól tud tervezni. Például eldöntheti, hogy kell-e neki tíz SAP munkaállomás vagy elég nyolc, melyik modulhoz akar hozzáférést, és melyikre nincs szüksége stb.

Drótos György emlékeztet: az lenne az ideális, ha a felhasználói kör mérlegelhetné, hogy bizonyos kapacitásokat esetleg a cégen kívülről rendeljen-e meg, ha az egyébként olcsóbb, a céloknak jobban megfelelő, vagy gyorsabban rendelkezésre áll. Természetesen ennek megvannak a korlátai, hiszen ha mindenki szabadon vásárolna külső szolgáltatásokat, az valószínűleg zűrzavart okozna, részben pedig megkérdőjelezné a korábbi IT-beruházások értelmét. A cégen belüli szolgáltatások ugyanis nagyon megdrágulnának, mert a fix kiadások (például a szerverpark üzemeltetési költségei) kevesebb helyre oszlanának el. Ennek következtében ha szóba is kerül külső informatikai cég igénybevétele, a megrendelés jellemzően csak a belső IT-szolgáltató jóváhagyásával, sőt akár azon keresztül történhet meg.

> A hardver- és szoftverfejlesztések abba az irányba mutatnak, hogy a komoly BI-számításokat nagy teljesítmény- és időszükséglet nélkül is képesek elvégezni.

DRÓTOS GYÖRGY
partner, IFUA Horváth & Partners
tanszékvezető, Corvinus Egyetem

Egy ilyen rendszert jellemzően körülbelül 100 felhasználó felett érdemes kidolgozni. De a kisebb vállalatoknál is szükséges, hogy a felhasználók kontrollszerepbe kerüljenek, ám a szolgáltatási listák, a szolgáltatási szintek, továbbá a költségszámítással előálló árcédulák alkalmazása már bizonyos vállalati méretet tételez fel – állítja a szakértő.

A kontrolling IT-ja

A kontrolling IT-ját vizsgálva kitűnik, hogy a felhasználó nemcsak belső vagy külső erőforrásokat vásárolhat, hanem esetenként dönthet úgy is, hogy a számára szükséges kapacitást maga hozza létre. A különböző alkalmazási területek közül talán itt mutatkozik meg leginkább, hogy a felhasználó külső segítség és tulajdonosi szoftverek igénybevétele nélkül is kialakíthat egy teljes szolgáltatási csomagot. A kritikus tranzakció-feldolgozó rendszereket, például ERP-rendszereket nem lehet egy főosztályon laikusok által üzemeltetni. Hasonlóképpen egy bérügyviteli rendszert – hiába nagyon jók a területen dolgozó szakemberek – sem lehet külső fejlesztők, állandó támogatás, a jogszabályi változások követése nélkül működtetni. Azaz ilyen esetekben az IT nem kerülhető meg. De amikor a meglévő tranzakcionális adatokra akarnak építeni egy tervezési vagy beszámolási rendszert – mert már vannak ilyen eszközök –, a vállalati kontrollerek egyre inkább maguk is elboldogulnak vele. Szokták ezt a tevékenységet önkiszolgáló BI-nak (üzleti intelligenciának) is nevezni.

Ez a helyzet azért áll elő, mert a központi IT-nak se kapacitása, se pénze nincs az egyes részlegek helyben felmerülő igényeinek kielégítésére. Ám ha rendelkezésre állnának a források, e fejlesztéseket akkor is besorolnák a többi közé, ami növelné a várakozás idejét. A felsővezetők azonban kikényszerítik az alájuk tartozó részlegekből azokat a jelentéseket, szimulációkat, amelyeket nekik is prezentálniuk kell. Így a kontrollerek nem feltétlenül várják meg például a sokára esedékes Cognos-fejlesztést, hanem elkezdenek kísérletezni olyan szabad forráskódú eszközökkel (mondjuk a Palóval), amelyekkel fel tudnak építeni egy modellt. Ha nagyon nagy adatállományokat kéne mozgatniuk, amihez a vállalati szerverekre is szükség volna, akkor inkább valamilyen felhőmegoldással élnek. Továbbá támaszkodhatnak a memóriaalapú műveletekre is, amelyeket már a nagyobb teljesítményű notebookok, illetve egyes adatbázis-technológiák (pl. SAP HANA) is támogatnak. A hardver- és szoftverfejlesztések egyaránt abba az irányba mutatnak, hogy a komoly BI-számításokat, az aggregált adatok előállítását nagy teljesítmény- és időszükséglet nélkül is képesek elvégezni. A nagy adatállományból pedig mindig éppen annyit töltenek le a felhőből, amennyire szükség van, és komoly nagyságrendű adatbázisokban is képesek elboldogulni. Ráadásul ezekben a BI-eszközökben a modellalkotás elég felhasználóbarát ahhoz, hogy egy olyan gazdasági szakember is megtudja tanulni, akinek nincsenek különösebben elmélyült informatikain ismeretei.

Mobilitás és vizualizáció

Az összképre a mobilitás is hatott. Ha a kontroller önkiszolgáló módon előállította a vezetői jelentéseket, akkor a mobileszközökön igen produktív munkát tud végezni a felsővezetőjével. A tableteken ugyanis könnyű közösen elemezni a jelentéseket. Szó szerint összedughatják felette a fejüket néhányan. Ilyen körülmények között hatékonyan működhet az áttekintést és a változások megértését szolgáló vizualizáció. Ez nem olyan egyszerű dashboardok, műszerfalak használatában merül ki, amelyek színes ábrákon összegzik az eredményeket. A technológiai áttörés abban van, hogy az egyes mutatókat meg lehet változtatni, és az új beállításokkal valós idejű szimulációkat lehet lefuttatni, ami nagyon megkönnyíti és felgyorsítja a döntéshozatalt.

Amíg nem voltak ilyen eszközök, addig a „mi lenne, ha" típusú feladatokkal csak lassan boldogultak, mert a megváltoztatott paraméterrel hazament a kontroller, leképezte az összefüggéseket, és másnap visszatért az eredménnyel. Ha az nem felelt meg a várakozásoknak, akkor jószerivel elfecséreltek egy napot. És kezdhettek valami máshoz, aminek a kimenetele szintén bizonytalan volt. Egy másik lehetséges út az volna, ha egy bonyolult rendszerben a kontrollerek és döntéshozók együtt írnák át az adatsorokat. De ez az út sem igazán kényelmes vagy járható. Az új típusú vizualizáció viszont rendkívül hatékony, igen erős döntéstámogató eszköz. És ez nagy lökést ad a BI felhasználásának a kontrollingmunka segítésében. Az önkiszolgáló BI-ban is fontossá válik e képesség, mert a vizualizáció a folyamat tartalmi szempontjává válik, s a felsővezetők alkalmasint akár a kontroller nélkül is kipróbálhatják az egyes mutatók megváltoztatásának hatásait.

Az új fejlemények az IT-szállítók és a belső IT-szervezetek szerepére is visszahatnak, mert ha a felhasználók szabad forráskódú szoftvereket szereznek be, azokat a saját PC-jükre telepítik, és önkiszolgáló módon eljutnak egészen az adatok elemzéséig, akkor nagy kérdés, hogy a professzionális szolgáltatók mit kínáljanak a jövőben. Természetesen az IT-infrastruktúra és a nagy tranzakciófeldolgozó rendszerek professzionális működését továbbra is felkészült IT-szakemberekkel és egységesen kell megoldani. Egyre inkább látszik azonban annak az évtizedeken keresztül stabilan álló modellnek a tarthatatlansága, amelyben feltételezték, hogy az IT mindent tud, az összes szükséges kompetencia a rendelkezésére áll, mindent kontrollál és mindent központilag irányít. Mivel azonban a szabad forráskódú eszközök teljesen elfogadottá váltak az üzletben, s a felhasználók már rengeteg dolgot maguktól el tudnak végezni, nincsenek már központilag allokált IT-források, és bebizonyosodott, hogy ha központilag akarnak irányítani mindent, azzal nem feltétlenül jutnak jobb eredményre, új helyzet állt elő. Ezért a szélsőségesen hierarchikus IT-modellt a nagy gazdálkodó szervezetek egyre inkább feladják – vélekedik Drótos György.

> ...e funkciók már jóval túlmutatnak az egyszerű vírusvédelmen, és olyan szolgáltatásokat adnak, melyekkel megelőzhetjük, hogy adataink illetéktelen kezekbe kerüljenek...

Hordozható kockázat

Új veszélyek forrásaivá válnak a mobilvilág népszerű eszközei, amikor a felhasználók vállalati környezetben kezdenek működni. Megjelennek rajtuk a rosszindulatú programok, olykor alkalmazásnak látszó szoftverek bőrébe bújva.

SEBŐK NÁNDOR
CISSP
RENDSZERMÉRNÖK
NOREG KFT.

A mobiltelefon és az internet közötti adatáramlás a vonalkapcsolt 9600 bps-os modemmel vette kezdetét. Ekkor a telefon még csupán egyszerű modemként működött, veszély a modemhez kapcsolódó számítógépet fenyegethette. Nem sokkal később a GPRS kezdeti verzióival csomagkapcsoltan is lehetséges volt az internet elérése, azonban akkoriban a telefonok még nem futtattak teljes értékű webböngészőt, így továbbra is a rácsatlakoztatott eszköz volt veszélyeztetett.

1997-ben megszületett a WAP, majd 2002-ben a WAP 2.0, azonban mindkét protokollverzió saját „nyelven" készült weboldalakat támogatott csak (WML és XHTML Mobil Profil), így a mobilplatform még mindig nem került a károkozó programok kereszttüzébe. Nagyjából még igaz maradt ez az okostelefonok előtti időszakban is, hiszen nagyon sokféle készülék volt forgalomban, hasonló mennyiségű beépített (zárt forráskódú) böngészővel. Emellett nagyon kevesen használtak csak internetelérést a telefonjukon, így az esetleges támadások hatásossága sem lehetett volna túl nagy.

A változást a Google által bemutatott mobil operációs rendszer, az Android hozta el. Nyílt forráskódjával megadja a lehetőséget a fejlesztőknek a készülék minél jobb kihasználására – ugyanakkor alkalmat ad a hackereknek az új típusú támadásokhoz.

Android mindenhol

Az Androidot futtató eszközök eladási számai hihetetlen mértékben nőttek, mára egyértelműen az Android vezeti az eladási listákat.

A fenti adatokat megvizsgálva már nem az a kérdés, hogy ki lesz a harmadik nagy szereplő, hanem hogy lesz-e egyáltalán harmadik „nagy". Az Android és az iOS együttes piaci részesedése ugyanis egy év alatt 75%-ról 90% közelébe került, így a harmadik helyezett mozgástere drasztikusan csökkent.

Android és a biztonság

A Google nemrégiben bevezette a Google Play-re feltöltött alkalmazások ellenőrzését. A Google Bouncer automatikusan ellenőrzi valamennyi feltöltött alkalmazást, kártékony viselkedésre utaló jeleket keresve a szoftverben. A 2011-es bevezetésekor a kártékony alkalmazások 40%-os csökkenését várták (Forrás: Scmagazine).

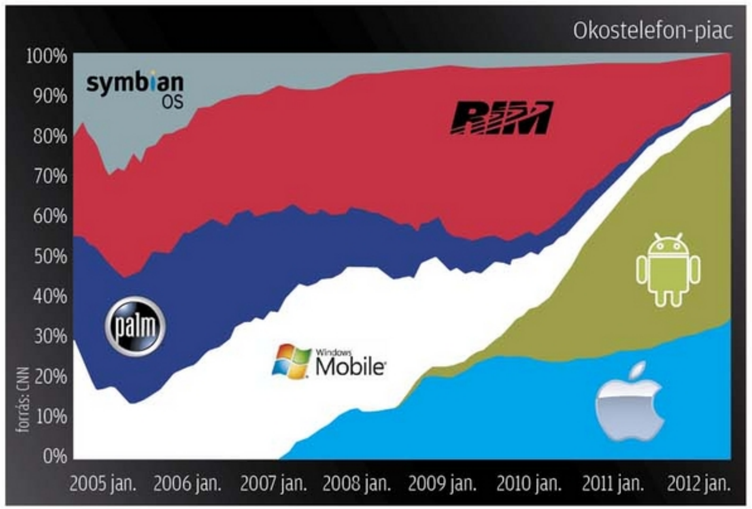
A TrustGo által végzett felmérés alapján azonban a kártékony alkalmazások számának növekedése nem állt meg. 2011. szeptember és 2012. szeptember között a kártékony alkalmazások száma 580%-kal növekedett. Ez a szám azonban 175 különböző marketplace vizsgálatából adódik, tehát nem csak a „hivatalos" Google Play adatait tartalmazza. A vizsgálat kimutatta továbbá, hogy 175 millió letöltés kapcsolódott olyan alkalmazásokhoz, melyek a hozzáférési jogokat megvizsgálva magas kockázatú besorolást kaptak. A kártékony minták száma egy év alatt 4 951-ről 28 707-re nőtt 2012 szeptemberére. Ez a trend tovább folyatódott a harmadik negyedévben is, itt már több mint 42 ezer mintát tartottak nyilván.

A fenti számok megismerése után tekintsük át azokat a legfőbb kockázatokat, amelyek androidos eszközünket fenyegetik, illetve megvizsgáljuk azt is, hogyan miként lehet ezek ellen védekezni.

Az eszköz elvesztése. Ez a legfőbb kockázat, amely valamennyi mobileszközt fenyeget. Egyértelmű azonban a megoldás, telepítsünk biztonsági mentésre szolgáló alkalmazást, amely vagy a saját számítógépünkre, vagy pedig valamely weben elérhető tárhelyre készít mentést az általunk kiválasztott adatokról. Lehetőségünk van még az elveszített mobileszközünket megtalálni, ha arra előtte telepítjük valamelyik erre a célra készült alkalmazást, például az ingyenes Where's MyDroid nevűt, amelynek segítségével sms-üzenettel felhangosíthatjuk a telefont, de akár a GPS koordinátáit is lekérhetjük.

Képernyőzár. A 2.2-es Android előtt nem volt más lehetőségünk telefonunk lezárására, mint egy 3×3-as mezőkön előzőleg megadott mintát rajzolni az ujjunkkal. Tisztában kell lennünk azonban azzal, hogy e megoldás nem biztosít elégséges védelmet. A védelem feltöréséhez elég egy jó minőségű fényképet készítenünk a telefon kijelzőjéről, és azt egy képszerkesztő programmal megfelelően manipulálni, így az esetek túlnyomó részében a fotó alapján a telefont ki tudjuk nyitni. Ezt elkerülhetjük, ha PIN kódot vagy jelszót állítunk be a záráshoz. A 2.2-es Androidnál régebbi rendszer esetén ajánlott külön alkalmazást telepíteni a záráshoz.

Adatvédelem. Hardveres titkosítási lehetőség az Android 3.0-tól elérhető, amit mindenképpen javasolt bekapcsolni, mind a telefon belső tárhelyére, mind pedig az esetleges SD kártyára. Ezt kiegészítendő egy távoli törlést is biztosító alkalmazással a telefon adatait elvesztés esetén távolról is megsemmisíthetjük. Ne felejtsük el azonban, hogy ehhez valamilyen módon el kell érni az eszközt (sms, e-mail).



Böngésző-sérülékenységek. Ahogy az Android operációs rendszer egyre népszerűbbé vált, úgy került egyre jobban fókuszba a böngészője, illetve annak biztonsága. A 2.0-ás és 2.1-es verziókban a WebKit böngészőmotor hibáját kihasználva a böngésző által olvasható valamennyi adat elérhetővé válhat. A 2.2-es verzióban egy böngészőhibát kihasználva az SD kártya tartalmához férhetünk hozzá. 2011 márciusában a Google javított egy cross-site scripting típusú hibát. Mindenképpen javasolt tehát telefonunkon ellenőrizni és telepíteni az elérhető biztonsági frissítéseket. Alternatív megoldásként használhatunk más böngészőt, azonban ekkor is figyeljünk oda a javítások rendszeres telepítésére.

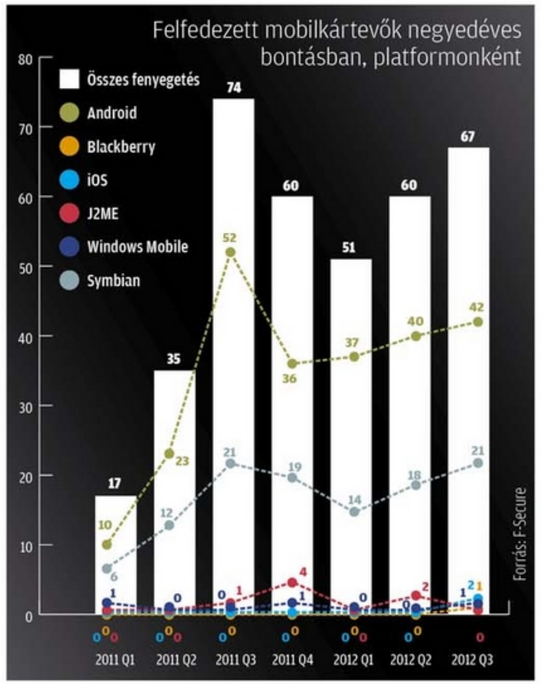
MI IS AZ AZ ANDROID?

Az Android a Google alapvetően okostelefonokra és tabletekre készített nyílt forráskódú operációs rendszere, amely Linux kernelre épül. Sikerének egyik titka, hogy bárki viszonylag egyszerűen fejlesztheti hozzá alkalmazást a szabadon elérhető fejlesztői eszközökkel. Az Android-alkalmazások gyűjtőhelyén, a Google Playen már több mint 800 ezer alkalmazás található.

Alkalmazások megbízhatósága és jogosultságai. Sajnos nem minden alkalmazás az, aminek mondja magát. Általánosságban elmondható, hogy találkozhatunk olyan alkalmazással, amely egy legális szoftver és egy androidos trójai program ötvözeteként veszélyezteti telefonunkat. Egy nemrégiben történt incidens során egy 09Droid nevű fejlesztő több mint 50 különböző „banki" alkalmazást készített az adott banknál vezetett számlánk eléréséhez. Az említett alkalmazásokat végül a bankok kérésére eltávolították. Az még mindig nem tisztázódott, hogy mi volt a készítő pontos célja, de azt valószínűsíthetjük, hogy nem a jó szándék vezette. Az alkalmazást letöltők és használók pedig könnyen számlájukon tartott pénzüket is elveszíthették. Az ilyen alkalmazásokat nagyobb eséllyel kerülhetjük, ha csak a Google Playből töltünk le szoftvereket. Különösen legyünk óvatosak a telefonunk biztonságát szolgáló alkalmazásokkal. Próbáljunk olyat választani, amely ismert gyártótól származik.

Az alkalmazások telepítésekor telefonunk jelzi, hogy az adott alkalmazásnak milyen jogosultságokra van szüksége. E listát mindenképpen nézzük át telepítés előtt, és ha olyan funkcióhoz kér engedélyt, amely nem függ össze a működésével (például egy szövegszerkesztő alkalmazás sms-küldési jogosultságot kér), akkor inkább ne telepítsük.

Kártékony programok. A mobil kártevők száma összességében még mindig igen alacsony az ismert összes kártékony programhoz viszonyítva. Ám a fent bemutatott Android-eladási számokat látva biztosak lehetünk benne, hogy a trend továbbra is az erős növekedés irányába



mutat. Ezért mindenképpen ajánlott valamely ismert vállalat vírusvédelmi szoftverének telepítése telefonunkra.

Rootolás. Android telefonunkon az alkalmazások kontrollált szoftverkörnyezetben egy úgynevezett sandboxban futnak, így biztosítva, hogy magához az Android rendszerhez ne férhessenek hozzá, csak a szükséges erőforrásokat használhassák. Amennyiben telefonunkat rootoljuk, e korlátozást oldjuk fel, azaz olyan alkalmazások futtatására is lehetőségünk van, amelyek operációs rendszer szintjén férnek hozzá erőforrásokhoz. A rootolás a Google által eltűrt lehetőség, hiszen a hivatalos Google Playben is találhatunk olyan alkalmazásokat, amelyek csak rootolt telefonon működnek. Legyünk azonban tisztában azzal, hogy e megoldással telefonunk biztonságát is kockáztatjuk.

Nagyvállalati megoldások

A fentiek alapján nyugodtan kijelenthetjük, hogy ma már nem lehet kérdés, szükséges-e megvédenünk okostelefonjainkat, illetve tabletjeinket. A helyzet súlyos, de nem reménytelen. Nézzük át, hogy melyek a lehetőségeink.

A nagyvállalatok biztonságára az egyik legnagyobb veszélyforrást még mindig a dolgozók jelentik. Valamennyi eszközt megfelelően védeni kell, azaz e környezetben már kötelezőnek tekinthető az üzleti célra használt okostelefonok, tabletek központi menedzselhetősége, ugyanis ezek az eszközök hozzáférhetnek a céges erőforrásokhoz, így ugyanolyan védelmi szint elérése szükséges, mint a hagyományos eszközök (például notebookok) esetén.

E rendszerekkel jellemzően a következő funkciók megvalósítása lehetséges:

- Telefonzár kikényszerítése
- Adott jelszóhossz és komplexitás kikényszerítése
- Alkalmazások felügyelete (tiltott, engedélyezett alkalmazások)
- Telefonfunkciók engedélyezése/tiltása
- Helymeghatározás
- Távoli zárolás és adatmegsemmisítés
- Tartalomszűrés előre definiált szabályrendszer alapján
- Privát eszközök menedzsmentje, privát és céges adatok elkülönítése (BYOD)

Ilyen – a Noreg Kft. által forgalmazott megoldás – például a Mobile Active Defense által készített Mobile Enterprise Compliance and Security Server, amellyel a fenti funkciók könnyedén bevezethetők nagyvállalati környezetben.

Megoldások privát eszközök esetében

Saját, nem vállalati eszközeink is jó eséllyel tartalmaznak olyan adatokat, amelyeket nem szívesen látnánk mások kezében. Gondoljunk csak például a bankok által küldött sms-ekre, amelyekben esetenként még a számlánk aktuális egyenlege is megtalálható. Hosszan lehetne sorolni még az érzékeny adatokat: telefonszámok, dokumentumok, jelszavak stb. Központi menedzsment híján saját magunknak kell gondoskodni az eszközök biztonságáról, nézzük meg, itt milyen lehetőségek adódnak:

Telefonzár. Használjuk az eszköz által kínált PIN kódos vagy jelszavas lezárást, természetesen megfelelő erősségű és hosszúságú jelszót/PIN kódot választva. Kerüljük a minta használatát a feloldáshoz.

Vírusvédelem. Mindenképpen javasolt egy vírusvédelmi szoftver beszerzése. Igyekezzünk ismert gyártót választani, valamint olvassuk el az alkalmazásról írt véleményeket is telepítés előtt. Találhatunk ingyenes verziókat, azonban a fizetős verziók sem kerülnek többe évi néhány ezer forintnál, amely egy 50-100 ezer forintos készülék esetén könnyen beleférhet a költségvetésünkbe. Nézzük át, hogy jellemzően milyen funkciókat kínálnak ezen alkalmazások:

- Rendszeres vírusminta-frissítések letöltése a készítőtől
- Memóriatartalom és alkalmazások ütemezett vírusellenőrzése
- Webhelyek biztonságosságának ellenőrzése
- Konfigurációs beállítások felügyelete
- Biztonsági mentés készítése és visszaállítás lehetősége
- Az eszköz távolról történő lezárása
- Az elveszített telefon/tablet helyzetének meghatározása
- Hangos riasztás távoli bekapcsolása (némított készülék esetén is)
- Az eszköz adatainak távolról történő teljes törlése

Láthatjuk, hogy e funkciók már jóval túlmutatnak az egyszerű vírusvédelmen, és olyan szolgáltatásokat adnak, amelyekkel megelőzhetjük, hogy adataink illetéktelen kezekbe kerüljenek, illetve hogy a telefonnal a számlánkra hívás- vagy sms-költséget generáljanak, és akár az elveszített eszköz megtalálására is lehetőséget adnak.

Titkosítás. Amennyiben telefonunkon olyan állományokat is tárolunk, amelyeket nem szeretnénk illetéktelen kezekben tudni, akkor érdemes telepítenünk egy titkosító alkalmazást is. Ahogy már láthattuk, az Android operációs rendszeren csak nemrégiben vált lehetővé hardveres titkosító alkalmazások fejlesztése, azonban a régebbi verziókkal is lehetőségünk van állományaink titkosítására.

Ilyen alkalmazások jellemzően néhány száz forinttól kaphatók, azonban ezek esetében is olvassuk el más vásárlók értékelését, esetleg nézzük meg, hogy próbaverzióban elérhető-e, így vásárlás előtt ki is próbálhatjuk, hogy megfelel-e az igényeinknek.

A fent bemutatott kockázatok alapján egyértelmű, hogy valóban elérkezett az idő, amikor telefonjaink/tabletjeink védelméről is gondoskodnunk kell, legyen az akár a sajátunk, akár vállalati eszköz. A megfelelő védelemhez szükséges eszközök már adottak, csak használnunk kell őket.

BANKOK, LÉGITÁRSASÁGOK, MOBILOPERÁTOROK ÉS KKV-K AZ INVITEL ADATKÖZPONTJAIBAN

Lemaradunk, vagy tartjuk a lépést a világgal?

Az Invitel több, mint 10 éve üzemeltet adatközpontokat, így az egyik legtapasztaltabb hazai szolgáltatónak számít ezen a területen. A vállalat négy fővárosi adatközpontját már több száz üzleti ügyfél választotta.

Az Invitel legújabb adatközpontja – a Kozma utcában található DataCenter – az egyik legbiztonságosabb megoldás üzleti adatok tárolására, vállalati informatikai rendszereket futtató szerverek üzemeltetésére. Ezt hónapról-hónapra egyre több cég, vállalkozás ismeri fel: a szolgáltató számos konstrukcióban kínál költséghatékony, biztonságos és rugalmas szervermegoldásokat. Legyen szó néhány szerverrel rendelkező kisvállalatról, nemzetközi óriás légitársaságról, bankcsoportról, mobiloperátorról vagy kórházról, az Invitel számos és sokféle partnernek nyújt testreszabott megoldásokat.

„A nemzetközi trendek azt mutatják, hogy a vállalati telephelyeken tárolt szerverek ideje lejárt. A hagyományos irodai szerverüzemeltetés sok tekintetben nem képes versenyezni a felhőből és adatközpontokból szolgáltatásként vásárolható szervermegoldásokkal" – mondta el *Béres András*, az Invitel vállalati szolgáltatásmenedzsment vezetője, akit nemrégiben választottak meg az Informatikai Távközlési és Elektronikai Vállalatok Szövetsége (IVSZ) Adatközpont és felhő munkacsoportjának vezetőjévé. Az Invitel szakembere szerint a következő években dől el, hogy képesek leszünk-e lépést tartani az informatikában és a technológia terén a fejlett világgal, vagy végérvényesen lemaradunk. Mint mondja, ebben kulcsszerepe lesz a szolgáltatásként vásárolható, előfizethető informatikai megoldásoknak és az adatközpontoknak is. „A gazdasági válság hatásai, a szűkülő vállalati beruházási keretek egyre inkább az előfizethető informatikai szolgáltatásokat helyezik előtérbe. Nem véletlen tehát, hogy a világban hódítanak a cloud- és a hosztingalapú megoldások. A szakember úgy fogalmazott: bizonyos szempontból az ország versenyképessége is múlik azon, hogy a hazai vállalatok képesek lesznek-e lépést tartani, vagy lemaradnak technológiában a világtrendektől. Béres András elmondta: „Van még mit tennünk, elsősorban nekünk, szolgáltatóknak a szakmai tájékoztatás, felvilágosítás terén. Noha az adatközpontok biztonság, megbízhatóság és költségek terén is – akár 30%-kal is – előnyösebb megoldásokat adnak, a hazai vállalatvezetők még nem ismerik eléggé ezeket a lehetőségeket" – tette hozzá a szakember. ■

INVITEL DATACENTER: MÉRLEGEN A VALÓSÁG

Jelentős hálózati kapacitás, több oldalról biztosított állandó elérés
- Kétoldali, független optikai betáplálás és mikrohullámú kapcsolat
- BIX2 csatlakozási lehetőség
- Közvetlen kapcsolatok a nagyobb internetcsomópontokhoz

Többszintű biztonság
- 99,999%-os rendelkezésre állás energiaellátás és hűtés tekintetében
- Redundáns megoldások
- Maximális fizikai védelem, 24x7 órás biztonsági szolgálat
- Elektromágneses védelem
- Modern légkezelő és szellőztető berendezések
- Korai reagálású füstérzékelő rendszer
- Környezetbarát gázos oltórendszer

Személyre szabható szervermegoldások
- Szerverelhelyezés (terület alapú bérlet, polcos és rackszekrényben történő elhelyezés)
- Bérelhető szerverek
- Virtualizált és felhő alapú szerver- és tárhelymegoldások

BÉRES ANDRÁS
vállalati szolgáltatásmenedzsment vezető
Invitel

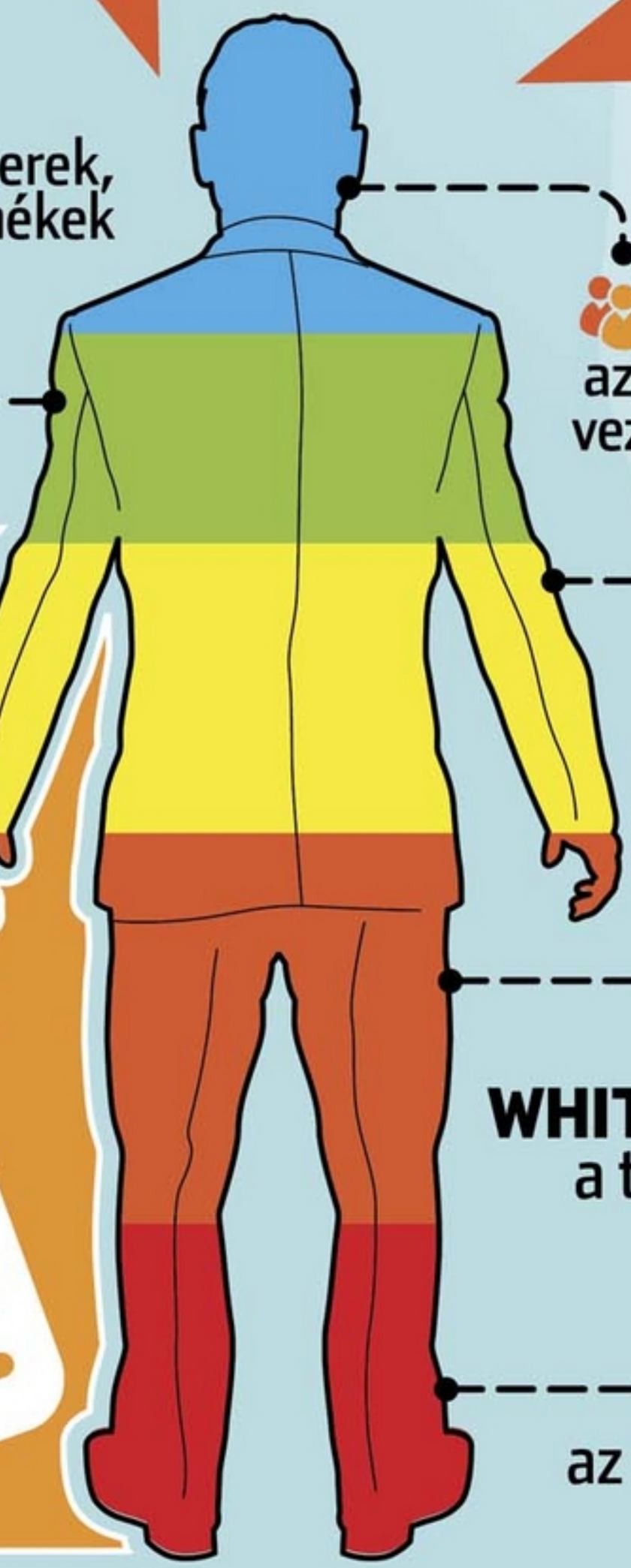
COMPUTERWORLD ONLINE

Olvassa el, ami történt

Tudja meg, ami történni fog

VIDEÓK: emberek, események, termékek

CIO.HU: az informatikai vezetők fóruma



HÍREK ÉS ESEMÉNYEK az IKT-piacról

WHITEPAPER: a tudásbázis

CÉGINFÓ: az IKT-adatbázis

Mobilon is!

www.facebook.com/computerworldhu

www.computerworld.hu