

Nincs biztonság kockázat nélkül



Ha lassan is, de a hazai nagyvállalatok körében is egyre inkább terjed az informatikai biztonság kockázat alapú kezelése, s ehhez ma már nemcsak kidolgozott metodológiák, hanem a kockázatkezelést támogató szoftverek is rendelkezésre állnak.

A magyar nagyvállalatok, illetve állami szervezetek a legutóbbi időszakban kezdenek ráébredni arra, hogy az informatikai biztonságot a korlátozott erőforrások miatt kockázat alapon kell kezelni, vagyis kockázatkezelési módszertanokat, illetve eszközöket kell és érdemes segítségül hívni, mivel ennek révén meg tudják védeni az informatikai rendszerek legkritikusabb pontjait a behatolástól vagy éppen egy katasztrófától. A kockázatkezelési módszertan, illetve az ehhez szükséges eszközöket a hazai piacon elsősorban a nagyvállalatok, illetve az államigazgatási szervezetek engedhetik meg maguknak. – A piac hajtóerejét elsősorban mégsem az üzleti érdekek jelentik, hanem a törvényi előírások, így például a Pénzügyi Szervezetek Állami Felügyeletének kockázatkezeléssel kapcsolatos előírásai. Emellett néhány multinacionális vállalat, ahol már foglalkoznak az informatikai biztonsági kockázatkezeléssel, hazai leányvállalatainál is hasonló metodoló-

giát, illetve szoftvert vezet be – magyarázta Kiss István, a Stratis vezető tanácsadója.

– Az informatikai biztonsággal kapcsolatos kockázatkezeléshez egyrészt informatikai tanácsadás ajánlott, másrészt egy olyan kockázatkezelő szoftvert, amellyel követni és menedzselni lehet az informatikai biztonsági problémákat – tette hozzá Vécsei László, az Abesse Rt. munkatársa. Az informatikai biztonságot a legtöbb magyarországi cég ma még szálítóoldaltól közelíti meg, azaz jellemzően tűzfal, vírusvédelmi vagy más biztonsági szoftvereket vásárol, de nem optimalizálja rendszereit és nem gondolkodik rendszerszinten.

Az előbbiektől eltérő szemléletet képviselnek a vállalati kockázatmenedzsment rendszerek. A kisméretű hazai piacot két magyar fejlesztésű termék uralja: az egyik az Abesse által fejlesztett Carisma (Corporate RiSk Management System), a másik a Humansoft UFO szoftvere; ezen kívül még néhány helyen működik a német

Strohl System rendszere. A szoftver – amely mintegy 100 projekt tapasztalata alapján született – referenciái között megtalálható többek között a Pannon, Malév, T-Online Magyarország és a Fővárosi Vízművek is.

A Carisma vállalati kockázatmenedzsment rendszerrel kapcsolatban Vécsei Lászlótól megtudtuk: a rendszer támogatja a kockázatmenedzsmentet mind az informatikai rendszerek, mind az üzleti rendszerek területén, a működési kockázatok feltárásától kezdve egészen a kvalitatív és kvantitatív kockázati értékek meghatározásáig bezárólag. A Carisma funkcionalitása a Security Management Methodology (SMM) eljárásaira épül, amely az informatikai folyamatok területén megfelel a Cobit4, a BS 7799 (ISO 17799), a TCSEC és a CC (ISO 15408) szabvány részét képező Common Evaluation Methodology ajánlásainak és szabványoknak, míg az üzleti folyamatok területén a MABISZ-szabványoknak.

A rendszer alkalmas vállalatok vagy cégcsoportok szervezeti egységeinek kockázatmenedzsmentjének, valamint az ahhoz kapcsolódó szabályozási dokumentumok előállításának és kezelésének támogatására, így az első lépés a vállalat vagy cégcsoport szervezeti, folyamat- és erőforráskapcsolatainak meghatározása. Majd az egyes szervezeti egységek kockázati területeinek meghatározása után a tipikus hazai veszélyforrásokat tartalmazó tudásbázis segítségével meghatározhatók a vállalati kockázatok szervezeti egysé-

genként és üzleti folyamatokként. A tudásbázis másik felhasználása a kockázatok csökkentésére kialakított vállalati védelmi intézkedések és azok hatásának minősítése az iparági átlagok alapján. A vállalati kockázatok és a védelmi intézkedések minősítése alapján határozza meg a rendszer a kvantitatív és kvalitatív kockázati értékeket. Így a teljes vállalat működési modellje leképezhető egy kockázati térképen, amelyet mind kvantitatív, mind kvalitatív módszerekkel ábrázolhatunk.

Az üzemeltetési szabályzatok, katasztrófatervék és az üzletmenet-folytonossági tervek védelmi akcióiból a rendszer projekteket generál, amelyeket a riportotokat készítő modul egy RO-SI (Return on Security Investment) modell szerint prioritási sorrendbe és grafikusán megjelenítve ábrázol a döntéshozóknak. Külső rendszerekkel összekapcsolva akár online módon követheti a vállalat a kockázati értékeinek változását. Az összekapcsolás jelenleg a HP Openview és IBM Tivoli rendszerekkel megoldott és tesztelt. A programcsalád használata támogatja a felhasználókat abban, hogy

ne csak statikus dokumentumokat készítsenek, hanem egy organikus, folyamatosan frissíthető dokumentumrendszer birtokába is jussanak. A csomag funkciói lehetőséget adnak arra, hogy az elkészült dokumentumokat a vállalat folyamatosan a változó szervezeti felépítéséhez, átalakuló üzleti folyamataihoz alakítsa. ■



Vécsei László
Carisma
termékmenedzser,
Abesse



Kiss István
vezető tanácsadó,
Stratis



KONFERENCIA

Karizmatikus kockázatkezelés

A vonatkozó ajánlások és törvények – például a Bazel II és a Sarbanes-Oxley – miatt a nagyobb szervezetek számára nem kérdés, hogy az IT kockázatkezelő és katasztrófaelhárító alkalmazás bevezetése szükséges. A kisebb vállalatok pedig adatvagyonuk értékét mérlegelve juthatnak hasonló következtetésre – hangzott el az I. Carisma Partneri Konferencián.

A rendezvény aktualitását a működési kockázatkezelést támogató Carisma legújabb, 3.0-s verziójának bejelentése adta. Az Abesse Informatikai Tanácsadó Zrt. fejlesztői a három modulból felépülő alkalmazás két modulját kibővített funkcionalitással Windows .NET alapokra helyezték.

Az egész napos konferencia kiváló alkalmat adott arra is, hogy az Abesse partnerei a Stratis Vezetői és Informatikai Tanácsadó Kft. tanácsadóinak előadásain keresztül megismerkedjenek a kockázatkezelő és katasztrófaelhárító megoldások piacát formáló legújabb trendekkel, majd aktívan bekapcsolódnak a párbeszédbe, amely a megvalósított projektek tapasztalatait elemző, délutáni műhelymunkát jellemezte.

A Carisma pozicionálása

A kockázatkezelő alkalmazást továbbfejlesztő Abesse két éve vásárolta meg a Carismát az Insurance Technology Kft.-től. Az IT-biztonság területén nyújtott tanácsadói szolgáltatásokat segítő, azok eszközéül szolgáló Carismát az Itech eredetileg saját projektjei során használta szakértői rendszerként. Az ügyfelek azonban beleszerettek az esz-



Kiss István, Rónai Balázs és Vécsi László

közbe, amely dobozos termékként a kockázatkezelés, a folytonos üzletmenet, a katasztrófaelhárítás tervezése, valamint az audittámogatás területén segíti a szervezeteket.

– A technológiai megújulással párhuzamosan új üzleti modellt állítottunk a Carisma mögé – mondta a konferencia résztvevőit köszöntve *Rónai Balázs*, az Abesse vezérigazgatója. –

Ebben egyrészt a zöldmezős szoftverfejlesztések, az ügyféligenyek lefedése, a szabványokra épülő megoldások kivitelezése terén szerzett tapasztalatainkra támaszkodtunk. Másrészt kialakítottuk partnerhálózatunkat, amelynek képviselői, az AlphaNet, az E-Comp, az Icon, a Proteus és a Stratis kiemelkedő kompetenciával bírnak az üzleti tanácsadás területén. Nem utolsósorban bővítettük ügyfélkörünket. Mára az Aegon Magyarország Általános Biztosító Zrt.-től a Budapest Airport Zrt.-n, a Giro Bankkártya Zrt.-n és a Mol Nyrt.-n át a T-Online Magyarország Internet Szolgáltató Zrt.-ig számos ágazatban vannak felhasználóink, referenciaértékű projektekkel. A Carisma korszerű technológiai alapokra helyezett új verziójával együtt mindez jó alap ahhoz, hogy megragadjuk a lehetőséget, amelyet a mintegy 60 milliárd forintos szoftver- és 300 milliárd forintos szolgáltatási piac kínál számunkra Magyarországon.

Microsoft .NET alapokon

A Carisma most bejelentett, 3.0-s verziójában az alkalmazás három modulja közül kettő – a BCP és a DRP – már Microsoft .NET alapokra épül.

– Az üzletmenet-folytonosság-tervező (BCP) és katasztrófaelhárítás-tervező (DRP) modul mögött levő módszertan lényegét tekintve maradt a régi – mondta *Vécsi László*, a Carisma termékmenedzserre. – Szoftverergonómiai szempontból és

funkcionalitását tekintve azonban annál többet fejlődött a Carisma 3.0. Jogosultságkezelő rendszere megújult, az új metaadatbázis pedig teljes mértékben testre szabhatóvá teszi a rendszert, jelentősen kibővítve a riportkészítési lehetőségek tárházát. Kiemelt szerepet kapott a tesztelés, az auditok és az éles helyzetben való reagálás támogatása. Az Importer funkció szorosabb

integrációt, zökkenőmentesebb adatkommunikációt tesz lehetővé a szervezet meglévő alkalmazásaival, például ERP-rendszerével, folyamatkezelő és menedzsment szoftverével. Ez az XML alapú integráció a CA, a HP, az IBM és a Microsoft rendszerfelügyeleti megoldásával egyaránt kialakítható. *Schultz Péter*, az Alphanet vezető tanácsadója egy ilyen, HP OpenView Service Deskkel kialakított integrációt mutatott be előadásában.



Az I. Carisma Partneri Konferencia résztvevői

A Carisma harmadik, kockázatkezelő modulja, a RiskMan hasonló technológiai megújulása a jövő év elején várható.

Tanácsadás az IT-biztonság terén

A Bell Research több mint 520 hazai vállalat részvételével készített felmérése szerint a tíznél több PC-t használó vállalatok zöme, 77 százaléka már átélte valamilyen IT-biztonsággal összefüggő incidenst. Az ötven PC-nél többel rendelkező cégek 73, és a száznál több számítógépet használó szervezetek 84 százaléka ugyanerről számolt be. A tíznél kevesebb PC-ből álló gépparkot üzemeltető cégek 52 százaléka szintén számot adott IT-biztonságot érintő eseményről – de az alacsonyabb arány valószínűleg annak tudható be, hogy a vállalatok egy része hosszabb időn keresztül sem szerez tudomást az üzleti adatait veszélyeztető kockázatokról és körülményekről.

– A felmérés arra is fényt derített, hogy a hazai vállalatok alig több mint felének, 52–56 százalékának van IT-biztonsági és üzemeltetési szabályzata – mondta *Kiss István*, a Stratis IT-biztonsági üzletágvezetője. – Katasztrófaelhárítási és üzletmenet-folytonossági tervet pedig még ennél is kevesebb szervezet dolgozott ki, a megkérdezett cégek mindössze 16, illetve 15 százaléka. A Carisma előnye, hogy ennek rö-

vid idő alatt történő elkészítését valamennyi vállalatméret számára lehetővé teszi. Dobozos termékként a nagyobb szervezeteknek ad megoldást az IT-biztonsági kockázatok feltérképezésére és a kezelésüket célzó stratégiák kidolgozására, gyakorlati alkalmazására. Szakértői rendszerként pedig azok a tanácsadó cégek használhatják eredménytel, amelyek mindezt szolgáltatás keretében biztosítják a kis- és középvállalatok számára.

Tim Zoltán, a Stratis vezető tanácsadója előadásában arról beszélt, hogy a Carisma miként segíti a tanácsadók munkáját:

– Ugyanazt az előnyt adja számunkra, mint az ügyfeleinknek, az előzetes felméréstől az elemzésen, a tervezésen és az implementáláson át a karbantartásig végigvezet bennünket mindazon a feladatokon, amelyeket egy projekt során el kell végeznünk az üzletmenet folytonosságát jól szolgáló, strukturált adattárolás kialakítása érdekében.

Ez segít megalapozni a szervezet információbiztonsági stratégiáját, a vele kapcsolatos dokumentum- és jogszabálykezelését, tudásbázisát és szabályzatát, gyakorlati működését, a későbbiekben pedig mindez az állandó változással jellemezhető, dinamikus IT-környezetben is eredményesen eredményre juttatható.

A partnertalálkozón az is elhangzott, hogy az Abesse az idei ITBN Informatikai Biztonság Napja rendezvényén külön standdal lesz jelen. A szeptember 26-án a MOM Parkban megrendezendő konferencia közönsége a helyszínen közelebbről is megismerkedhet azokkal az újdonságokkal, amelyekkel a Carisma 3.0 működési kockázatkezelés, üzletmenetfolytonosság-biztosítás, katasztrófaelhárítás és audittámogatás terén szolgál. ■