Póserné Oláh Valéria
Budapesti Műszaki Főiskola NIK,
poserne.valeria@nik.bmf.hu

IT KOCKÁZATOK, ELEMZÉSÜK, KEZELÉSÜK

Absztrakt

Napjainkban már a legtöbb szervezet működése elképzelhetetlen informatikai és telekommunikációs eszközök támogatása nélkül, de az információs technológia (IT) alkalmazása nagymértékben növeli a szervezeti működés kockázatát. További nehézséget okoz, hogy ahány szervezet, annyiféle kockázat profil különböztethető meg, ezért nem lehet minden szervezetre érvényes, az IT kockázatok kezelésére vonatkozó konkrét útmutatót kidolgozni. A cikk csoportosítja az IT kockázatokat a szervezetre gyakorolt hatásuk szerint, általános iránymutatást fogalmaz meg azok kezelésére, melyet a konkrét szervezet sajátosságainak figyelembevételével kell megvalósítani.

Nowadays the everyday work of most of the organization is unimaginable without the support of the informatics and telecommunication utilities, but the usage of information technologies (IT) increases enormously the threat of the organizational work. It does cause even more hardness that every organization has its own threat profile, that is why a concrete guide for handling IT threats cannot be carried out. This article groups the IT threats according to their effects on the organizations and shows a common orientation for the handling of them which has to be used by focusing on the unique points of the organization.

Kulcsszavak: *kockázat, információs technológia, IT kockázat, kockázatmenedzsment, kockázatelemzés, kockázatkezelés.*

BEVEZETÉS

Az elmúlt két évtizedben az informatikai rendszerek mindennapi életünk szerves részévé váltak. Jelen vannak mind a magán, az állami, a védelmi és üzleti szférában, és egyre több területen jutnak kulcsfontosságú szerephez. Napjainkban szinte minden szervezet szerves részét képezik az informatikai és telekommunikációs eszközök, a legtöbb szervezet tevékenysége pedig el sem képzelhető ezek alkalmazása nélkül. Az információs technológia (IT) kritikus tényezővé válása komoly veszélyeket rejt magában, mivel e rendszerek rendkívül sok fenyegetésnek vannak kitéve, a működésük során felmerülő hibák pedig igen súlyos veszteségeket okozhatnak a szervezetek életében. Éppen ezért az IT kockázatok kezelése egyre több időt és odafigyelést igényel a vezetés részéről. A megfelelő védelem kidolgozásával a kockázatmenedzsment foglalkozik, melynek célja a lehetséges kockázatok felderítése, elemzése, és a lehetséges veszteségek minimalizálása.

A Symantec közreadott egy tanulmányt melyben 2005 októberétől 2006 októberéig tartó felmérésének eredményeiről ad számot. A felmérésben különböző országokban, eltérő nagyságú szervezeteknél, különféle pozíciókban tevékenykedő, 37 ipari szegmens mintegy 500 IT szervezetének dolgozói szolgáltatták az adatokat az IT kockázatkezelésről. A

tanulmány felvázol egy ötlépéses folyamatot is a szervezetek számára, amely segítséget nyújt a kockázatok besorolásával és feltérképezésével az IT kockázatok kezelésében, a szervezetek szemléletének formálásában és a problémák elkerülésében. Segít megtartani a kockázatkezelési célkitűzéseket, valamint folyamatosan mérni az IT kockázatkezelési hatékonyságot. [1]

Mivel a különböző tevékenységeket végző szervezeteknek különböző típusú kockázattal kell szembenézniük, minden szervezetnek saját egyedülálló IT kockázat profilja van. Például egy szórakoztató vállalatnak nem okoz nagy gondot, ha rövid ideig honlapjuk nem elérhető, de jelentős mértékben kell a kereskedelmi- és tervinformációit védeni. Egy nagy pénzügyi vagy egy védelmi célú szervezet esetében azonban jelentős károkat okozhat, ha sérül az elérhetőség és rendelkezésre állás követelménye. Így tehát nem adható minden szervezetre érvényes, a kockázatok kezelésére vonatkozó konkrét útmutató, de, mint a Symantec tanulmánya is, általános iránymutatást meg lehet fogalmazni, melyet a konkrét szervezet sajátosságainak figyelembevételével kell implementálni.

A cikk általánosságban tárgyalja, csoportosítja a szervezetre gyakorolt hatásuk szerint a bekövetkezhető kockázatokat, és általános iránymutatást ad az IT kockázatok kezelésére vonatkozóan.

1. A KOCKÁZAT

Az üzleti kockázatok köre a mindennapi működésbeli hibáktól a ritkán előforduló kataklizmaszerű kudarcokig terjednek. Az elmúlt évtizedben az IT rendszerek kritikus fontosságúvá válása, a tőlük való függőség jelentős fokozódása eredményeként az IT kockázat, amely korábban kis szeletét képezte a működési kockázatnak, fő veszélyforrássá vált a szervezetek számára, melyet azonosítani és kezelni kell.

A kockázat egyrészt valamilyen veszélyforrás által okozott nemkívánatos következmények lehetősége, valószínűsége, másrészt a következmények természete és súlyossága.

Az informatikai rendszereket érintő veszélyek komoly hányadát teszik ki a teljes vállalati kockázathalmaznak, a felmerülő kockázatok több mint 50%-át jelenthetik.

Az IT rendszereket veszélyeztető kritikus tényezők négy alapvető csoportra oszthatók, mint ahogy az 1. ábrán látható:

1. ábra: IT kockázatok csoportosítása a szervezetre gyakorolt hatás szerint [1]

1. Adatbiztonság (Security): Az információ megváltozása, elvesztése, illetéktelen kezekbe való kerülése valamilyen rosszindulatú cselekmény (hozzáférés) következtében.

2. Rendelkezésre állás (Availability): Az információk vagy szolgáltatások elérési idejének megnövekedése, esetleg azok teljes vagy részleges elérhetetlenné válása rendszerhiba, vagy valamilyen külső behatás, pl. természeti katasztrófa következtében.

3. Teljesítmény (Performance): A rendszer egészének vagy valamely összetevőjének teljesítményromlása, nem optimális működése.

4. Szabályozóknak való megfelelés (Compliance): A rendszer nem felel meg a kitűzött normáknak, szabályoknak, előírásoknak.

Az IT rendszereket ért nemkívánatos események lehetséges következményei:

- Az információ megváltozása vagy elvesztése;
- Az információ (beleértve minősített adatokat is) illetéktelen (akár terrorista) kezekbe kerülése;
- Életfontosságú berendezéseket (vízellátás, áramellátás stb.) működtető rendszerek átmeneti, vagy végleges működésképtelenné válása;
- Politikai személyek vagy csoportok jó hírének károsodása;
- Bizalomvesztés, kétség a hatóságok eredményességét illetően;
- Vagyoni veszteség;
- A nemzetbiztonság veszélyeztetése.

2. IT KOCKÁZATMENEDZSMENT

Az informatikai eszközök alkalmazásának széles körű elterjedése magával vonta az IT kockázatok kiemelkedő megnövekedését a teljes működési kockázat összetevőjeként. Az IT kockázatok ma már többet jelentenek, mint csupán a működési kockázatmenedzsment egy speciális területe. Önálló területté nőtte ki magát a mai szervezetekben, amely szakosodott tudást, készségeket igényel.

A kockázatmenedzsment feladata a rendszert fenyegető veszélyek felmérése, és a megfelelő védelmi stratégia kidolgozása. Fontos, hogy a védelem megtervezése minden részletre kiterjedjen, ajánlott a komplex, átfogó stratégiák alkalmazása, így kiküszöbölhetők a rendszerben maradt gyenge láncszemek által okozott további fenyegetések. A felmerülő kockázatok egyedi kezelése helyett törekedni kell egy egyenszilárdságú rendszer kiépítésére, mely minden pontján egyforma erősségű védelmet nyújt, így a teljes rendszer hatékonysága nagyban növelhető.

Alapvető igény, hogy a védelem hatékony és optimális legyen, ehhez azonban szükséges a kockázatok, és a lehetséges veszteségek pontos ismerete. Ezen adatok számszerűsítése, vagy pénzbeli kifejezése azonban nagyon nehézkes feladat, legfőképp az informatikai rendszerek vizsgálatánál.

A védelemre fordítandó költség meghatározása hasonlóan nehéz feladat, de általában érvényes az a szabály, hogy a védelemre fordított energia és tőkebefektetés ne haladja meg a lehetséges kár által okozott veszteséget.

Ezen stratégiai lépések meghozatalához a vezetés, és a megfelelő szakemberek magas fokú együttműködése szükséges, a problémakör megfelelő átlátására van szükség a helyes döntések meghozatalához. A kockázatkezelést nagyban segítik a különböző komplex kockázatbecslési, kockázatkezelési és szimulációs stratégiák (pl., CRAMM, Monte-Carlo szimuláció), melyek megkönnyítik az optimális védelmi tervek kidolgozását. A szervezetek általában belső munkatársak segítségével végzik a kockázatkezelést és elhárítást, azonban legtöbbször nem áll rendelkezésre megfelelő szaktudás a szervezeten belül, ezért egy külső, kockázatkezelésre szakosodott cég megbízása nagyobb hatékonyságot eredményezne.
A kockázatmenedzsment ajánlott lépései:

- Veszélyforrások felmérése
- Kockázatelemzés, becslés
- A lehetséges védelmi intézkedések számbavétele
- Kockázatok kezelése

2.1 Veszélyforrások felmérése

A kockázatkezelés első lépése minden esetben a jelenlegi rendszer elemzése, gyenge pontjainak feltárása, a lehetséges fenyegetettségek megismerése.. Egy általános informatikai rendszernél ez a folyamat a következő tevékenységeket foglalja magában:

- hálózat, hálózati eszközök értékelése;
- hardware elemek értékelése;
- használt operációs rendszerek értékelése;
- adattárak, adatbázisok értékelése;
- alkalmazások értékelése;
- internetes, és kapcsolt szolgáltatások elemzése;
- üzemeltetési eljárások értékelése;
- kapcsolódó rendszerek értékelése. [2]

A kiértékelés során hozzávetőleges kép nyerhető a rendszer egyes összetevőit fenyegető tényezőkről, azok mennyiségéről és milyenségéről.
Az értékelés történhet személyes szemlét követően, dokumentációk elemzésével, interjúkkal, így mind a jelenlegi helyzet, mind a múltbeli tapasztalatok figyelembe vehetők.

A veszélyforrások tipikus csoportjai az alábbiak:

- szervezési gyengeségek (szervezési hiányosságokból eredő veszélyek, nem megfelelő erőforrás és kapacitástervezés),

- természeti veszélyforrások (pl. tűz, csőtörés, árvíz, villám, földrengés),
- fizikai veszélyek (pl. betörés, lopás, rongálás),
- logikai fenyegetések (pl. informatikai csalás, hálózati betörés, lehallgatás),
- humán veszélyforrások (belső munkatársak gondatlansága, visszaélések, szándékos rongálás). [3]

2.2. Kockázatelemzés, becslés

A kockázatkezelés második lépése a lehetséges kockázatok felmérése és a nemkívánatos események bekövetkezésekor keletkező kár becslése. Ez igen komoly feladatot jelent minden esetben, de az informatikai rendszereknél ezen adatok számszerűsítése szinte lehetetlen feladat. A legtöbb kockázatkezelési módszertan nem is vállalkozik a vagyoni ráfordításban való kifejezésre. Ennek legfőbb oka, hogy az informatikai rendszereket ért károk általában nem közvetlenül fejtik ki hatásukat, hanem a velük kapcsolatban álló rendszerelemeken keresztül az egész szervezet működésére befolyással lehetnek. Például egy adattároló meghibásodása, amelynek javítása vagy cseréje önmagában nem jelent nagy költséget, azonban az információvesztés, és az emiatt történő kiesés komoly kockázatokkal járhat. Az informatikai rendszerben bekövetkezett károsodás nem megfelelő védekezés mellett könnyen fennakadást okozhat a vele kapcsolatban álló munkafolyamatokban, ezzel áttételesen akár a szervezet alaptevékenységét is veszélyeztetheti. Ez pedig akár a vevők, üzleti folyamatok szintjét is befolyásolhatja, ami könnyen komoly bevételkieséshez, az ügyfelek elpártolásához, imázscsökkenéshez vezethet.

A kockázatbecslés legtöbbször a korábbi statisztikai és tapasztalati értékeken alapul. Egyes esetekben nem állnak rendelkezésre ezek az adatok, ilyenkor csak a bekövetkezett kár hatásmechanizmusainak teljes feltérképezésével lehet megközelítő kockázati becslést adni.

Sok esetben a statisztikai módszerekkel történő szimuláció is kiváló eredményekre vezet. Például a Monte-Carlo szimuláció a kockázatelemzés egyik alternatív módszere, amikor is a rendszer megfelelő modellezése után számítógépes szimulációk futtathatók a rendszernek megfelelő véletlen értékekkel. Ez a módszer megfelelő nagyságú minta alkalmazásával rendkívül előnyös a felmerülő kockázatok vizsgálatára, azonban hátránya is van, mégpedig a rendkívül nagy számítási kapacitásigény, mely viszonylag költségessé teszi a módszer alkalmazását. De mivel a szimuláció nem csak egyszerű véletlen értékgenerálást tartalmaz, hanem különböző hatékonyságnövelő eljárásokkal pontosítja a becslést, így viszonylag kisebb minta alkalmazásával is megközelítő pontosságú becslés érhető el vele. [4]

A kár hatása általában három szinten vizsgálható:

- **Elsődleges kár**: az adott rendszerben okozott tényleges kár mértéke, a helyreállítás költsége (pl. számítógép javítása, adatok pótlása).
- **Másodlagos** és **harmadlagos kár**: a különböző kölcsönhatásokon keresztül, a teljes szervezetben realizálódott veszteség mértéke.

Az elsődleges kár meghatározása általában egyszerű feladat, míg a másodlagos és harmadlagos veszteségek pontos feltérképezése csak nehezen, vagy egyáltalán nem oldható meg.

Mivel a bekövetkezési valószínűségek, és az okozott veszteségek számszerűsítése nehéz feladat, ezért a legtöbb módszertan kategóriákat állít fel ezek becslésére. A kategóriákba sorolással lehetőség nyílik a becsült értékek nagyságrendbeli összehasonlítására. A kockázatbecslés során három alapvető kategóriacsoport állítható fel:

- **Kár kategóriák:** kis összegű elsődleges kártól, a szervezet létét fenyegető veszélyforrásokig. A kategóriákba sorolásnál figyelembe kell venni az okozott kár természetét, illetve, hogy a rendszer milyen tulajdonsága sérült. (Pl. bizalmasság, sértetlenség, rendelkezésre állás.)

- **A bekövetkezési valószínűségek kategóriái:** az évente többször előforduló, bármikor bekövetkezhető veszélyforrásoktól a minimális eséllyel rendelkező fenyegetettségekig. A kategóriákba sorolásnál a valószínűség meghatározása a tapasztalati tényezőkön vagy szimuláción alapulhat. Támadás elemzése esetén fontos szempontot játszik a rendszer gyengeségének kihasználásához szükséges támadási potenciál, szaktudás megállapítása.

- **Kockázatok kategóriái:** a kockázatokra fordítandó relatív vagyon és energia befektetés kategóriái.

A kategóriák száma csoportonként erősen függ attól, hogy milyen és mekkora az elemzett rendszer, de általánosságban 4-7 kategória definiálása célszerű csoportonként.

Az előzetesen már felderített kockázati tényezők kategóriákhoz rendelése után megkezdődhet az egyes fenyegetések kockázatának elemzése. Ez általában matematikai módszerrel történik, az egyes fenyegetések előfordulási valószínűségének és az okozott kár nagyságának összevetésével.

A kockázatok bizonyos csoportjára külön figyelmet kell fordítani, mivel néhány, általában nagyon alacsony valószínűségű veszélyforrás a szervezet életére erős mértékben hathat, akár veszélyeztetheti is annak fennmaradását. Ezek az elviselhetetlen kockázatok, amelyek elleni védekezésre történő anyagi ráfordítás esetenként a valószínűség mértékéhez képest indokolatlanul magas lehet, azonban hosszútávon számolni kell velük, a felkészülés mindenképp szükséges.

2.3. A lehetséges védelmi intézkedések számbavétele

A rendszert fenyegető veszélyek elemzése után megkezdődhet a kockázatok kezelésére történő tervek kidolgozása. Ennek első lépése a lehetséges védelmi intézkedések számbavétele. A legfontosabb szempont természetesen az egyes veszélyforrások csökkentésére fordított anyagi ráfordítás és az elért hatás. Az egyes védelmi intézkedések hatással lehetnek egymásra, de hatásuk nem feltétlenül adódik össze. A cél, olyan kombinációt találni az adott lehetőségek közül, mely a teljes rendszer védelmét a lehető legnagyobb mértékben lefedi, és minden elviselhetetlen mértékű kockázatot legalább elviselhető mértékűre csökkent, valamint lehetőség szerint költséghatékony is.

2.4. Kockázatok kezelése

Öt alapvető kockázatkezelési stratégia különböztethető meg:

1. A veszélyforrás megszüntetése.

2. Bekövetkezési valószínűség csökkentése.

3. Okozott kár csökkentése.

4. Kockázat áthárítása.

5. Tudatos kockázatvállalás.

A veszélyforrás megszüntetése

Kétségkívül ez lenne a leghatékonyabb stratégia, azonban a kockázat teljes kiküszöbölésére csak elméletben van lehetőség. Bizonyos kockázatokat körültekintő, alaposan átgondolt, teljes körű felmérésen, elemzésen alapuló intézkedésekkel, befektetésekkel ki tudunk ugyan küszöbölni, de tökéletesen biztonságosan üzemeltethető rendszer nincs. Mindig történhetnek előre nem látható, váratlan események, melyekre a legnagyobb körültekintés mellett sem gondolhatunk előre.

A bekövetkezési valószínűség és az okozott kár csökkentése

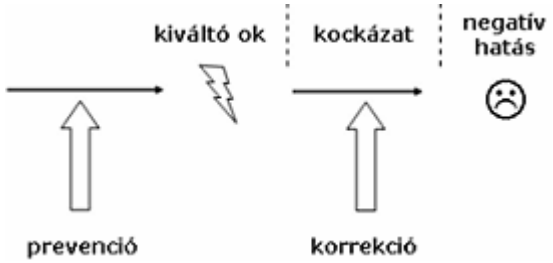
A gyakorlatban legtöbbször ennek a két stratégiának valamely kombinációja jelenti az optimális megoldást a felmerülő kockázatok kezelésére.

Kockázatkezelésre alkalmazhatók technológiai és folyamat alapú kontrollok. Általában ezek együttes kombinációja adja a legnagyobb hatékonyságot. A Symantec felmérése szerint azok a cégek, melyek nagyobb hangsúlyt fektetnek a folyamat és technológiai kontrollok együttes alkalmazására, nagyobb hatékonyságú, komplex védelemmel rendelkeznek az IT rendszereket illetően, mint a kevesebb, főként technológiai kontrollt alkalmazó társaik.

A gyakorlatban az egyik legelterjedtebb módszer az úgynevezett PreDeCO kontrollok alkalmazása. Ez a módszer három védelmi mechanizmus együttes használatát javasolja:

- **Pre**ventive: megelőző, kivédő kontrollok alkalmazása a bekövetkezési valószínűség csökkentésére.
- **De**tective: felismerő kontrollok a nem kívánt esemény bekövetkeztének detektálásához.
- **Co**rrective: elhárító, helyreállító kontrollok a felmerülő problémák orvoslására és a keletkező kár minimalizálására. [3]

A preventív és a korrektív védelmi mechanizmus alkalmazását a 2. ábra szemlélteti.



2. ábra: A preventív és korrektív kockázatkezelés [5]

A kockázat áthárítása

Bizonyos esetekben lehetőség van egyes kockázati terhek átruházására a partnerekkel, vevőkkel történő szerződéskötés során. Erre jó példák a különböző e-boltok weblapjai,

melyek a legtöbb esetben a lehető legkörültekintőbben járnak el adataink (pl. bankkártya adatok) védelmében, azonban semmilyen felelősséget nem vállalnak az adatlopásból eredő károkért.

Egy másik lehetőség a kockázat áthárítására a biztosítás. Ez a módszer a legtöbb esetben nem tűnik kifizetődőnek, hiszen a biztosítási összeg rendszerint meghaladja az esetleg keletkező károk mértékét, azonban biztosítás kötésével elkerülhetők a hirtelen bekövetkező, nagy arányú anyagi veszteségek, így a kockázatkezelés kontrollálhatóvá válik.

Tudatos kockázatvállalás

Egyes esetekben a védekezésre fordítandó összeg olyan mértékben meghaladja a lehetséges maximális veszteséget, hogy megéri meghozni a döntést a kockázat tudatos vállalásáról. Ilyenkor azonban teljesen tisztában kell lenni a lehetséges következményekkel, a veszteség másodlagos és harmadlagos hatásmechanizmusaival.

3. ÖSSZEGZŐ MEGÁLLAPÍTÁSOK

A Symantec felmérése szerint a vállalati vezetők 60 százaléka legalább egy komolyabb IT incidensre számít évente, valamint 5 évente legalább egy súlyos adatvesztéssel járó káreseménnyel kalkulál. Ezek a számok jól tükrözik a valós adatokat is, így érthető az IT szektorban felmerülő veszélyek megfelelő kezelésének fontossága. Az IT rendszerek központi szerepe és sérülékenysége miatt napjainkban **elengedhetetlen az informatikai rendszereket fenyegető veszélyek feltérképezése, és a kockázatok megfelelő kezelése, menedzselése**.

A kockázatelemzés eredményeként képet kapunk a rendszert fenyegető veszélyforrásokról, a káresemények lehetséges értékéről és bekövetkezési valószínűségéről. Ezen adatok ismeretében **kidolgozhatók a megfelelő védelemhez szükséges kockázatkezelési stratégiák**, a rendszer biztonsága hatékonyan fokozható.

Az IT kockázatmenedzsment programok kialakítása során **figyelembe kell venni a szervezet speciális kockázatprofilját**, üzleti céljait, az újabb kockázat létrehozásának elkerülése érdekében.

Az IT szakértők hatékonyabbak a technológia kontrolok alkalmazásában, mint a folyamat kontrolok alkalmazásában, ami aggodalomra ad okot, hiszen ezeknek a területeknek nagy szerepük van az IT kockázatok és működési költségek kontrollálásában.

Gondot okoz az IT kockázatok proaktív kezelésében kritikus fontosságú területek problémái, mint eszköz-befektetés, osztályozás és menedzsment valamint a kezelési kontrolok konfigurálása és cseréje.

A kockázatmenedzsment elveket helyesen alkalmazó szervezetek kevesebb incidensre számíthatnak, – még akkor is, ha magasabb kockázati szinttel rendelkeznek –, mint a kevésbé hatékony szervezetek. Egy **átfogó szemléletmód kialakítása szoros összefüggésben van a hatékonysággal**, illetve az incidensek alacsony számával. A kockázatkezelési befektetések megtérülése érdekében az IT szervezeteknek összhangba kell kerülniük egymással, illetve a szervezet teljes egészével. Az IT irányítás és a szervezetirányítás közötti IT kockázatokra vonatkozó eltérő álláspontok további problémát idézhetnek elő a gyenge koordináció miatt, mely az ellenőrzés területén túlzott, vagy nem elégséges befektetéseket

eredményez, az erőforrások pazarlásához vezet, és nem hatékony IT kockázatkezelési programokat eredményez.

FELHASZNÁLT IRODALOM

[1] Symantec Corporation: IT Risk Management Report 2007, http://www.symantec.com/enterprise/theme.jsp?themeid=itrisk_report, 2007.04.02.

[2] Metacom: Itaudit - IT technológiák biztonsági vizsgálata: www.itbiztonsag.hu, 2007.06.01.

[3] Biztostu.hu: Kockázatelemzés, http://www.biztostu.hu/mod/resource/view.php?id=121, 2007.05.30.

[4] James R. Conrad: Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations, http://infosecon.net/workshop/pdf/13.pdf, 2007.04.02.

[5] Wikipedia: Kockázat, http://hu.wikipedia.org/wiki/Kock%C3%A1zat, 2007.06.01.