Szabadszállási Polgármesteri Hivatal

KOCKÁZATELEMZÉS

2015. július 1.

Storchné Somogyi Eszter
jegyző

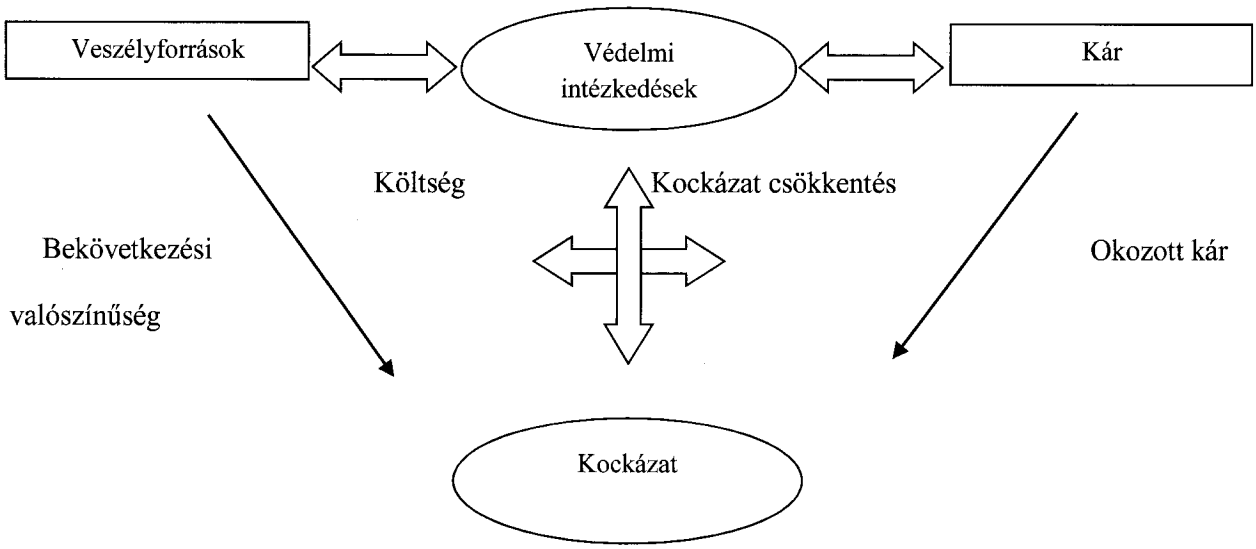
Bevezetés

Az informatikai rendszereket fenyegető veszélyforrások által jelentett kockázatokat nehéz megbecsülni, a védelem költségeit meghatározni. Egyrészt ebben a folyamatosan változó világban a veszélyforrások bekövetkezésének gyakoriságára nincsenek jó statisztikák, másrészt a ténylegesen okozott károk pénzben kifejezett mértéke sem határozható meg, sokszor még nagyságrendileg sem. Annak ellenére, hogy számszerű közelítő eredményt nem remélhetünk legalább elvi síkon célszerű tisztában lenni a veszélyforrások, illetve károk hatásmechanizmusával.

Kockázatbecslési modell

Rendszerelemek	Alkamazói szoftver	Ügyviteli folyamatok
Szerverek	Pénzügyi rendszer	Stratégiai tervezés
Központi adattár	Szociális segélyezési rendszer	Operatív irányítás
Munkaállomások	Ügyiratkezelő rendszer	Pénzügyi menedzsment
Hálózat	Helyi adók nyilvántartása	Beszerzés
Operációs rendszerek	Banki utaló rendszer	Számlázás
	Népesség nyilvántartó rendszer	
	Kataszter	
	Ebek nyilvántartása	

1. ábra kockázat becslési modell



2. ábra Kár keletkezésének hatásmechanizmusai

3.) Kockázat metamatikai definiciója

A kockázat kiszámításához a független fenyegető tényezők közel teljes körű feltárásával lehet eljutni. A közel teljes körű feltárás azt jelenti, hogy a fenyegető tényezők halmaza általában nem fedi le a teljes eseményteret, de arra kell törekedni, hogy ezeket a tényezőket mind teljesebben írjuk le. A teljes valószínűség tételét alkalmazva kapjuk a kockázat becslését:

P =P(A1)P(K|A1)+P(A2)P(K|A2)+ ... +P(An)P(K|An) =

£ P(A)P(K\Ax) (3)

i=i

ahol: P(Ai) * 0 ; ie N+;

P — a kockázat valószínűsége;

P(Ai) — az i. fenyegető tényező bekövetkezésének a valószínűsége; P(K|Ai) — az i. fenyegető tényező bekövetkezésekor keletkező kár feltételes valószínűsége. A kockázat ilyen módon való meghatározásának nagy előnye a szilárd elméleti alap és a jól definiált fogalmak, de a gyakorlatban több probléma is felmerülhet:

- a teljes eseményrendszer megadásának a nehézsége;

- a képletben szereplő valószínűségek meghatározásához nem áll rendelkezésre elég statisztikai, tapasztalati érték;

- sok valószínűséget kell meghatározni és megadni;

- valamilyen változás esetén az értékeket újra meg kell határozni;

- a keletkezett károk becslése is problémát jelenthet.

Egy informatikai rendszerben elsődleges, másodlagos stb. kárról is beszélnünk kell. Tehát fel kell tárni az áttételes hatásokat, meg kell becsülni az elsődleges, másodlagos, n-edleges károk nagyságát.

4.) Kockázati paraméterek becslése

Egy informatikai rendszer esetében azért van különösen nehéz feladatunk a kockázat mértékének pontos meghatározásakor, mert a fenti képlet egyetlen paraméterét sem tudjuk jól megbecsülni. A veszélyforrások listája sem lehet teljes; sok esetben a bekövetkezési valószínűség becsléséhez nem áll rendelkezésre korábbi statisztikai, tapasztalati érték; a keletkezett kár pedig egy informatikai rendszerben komplex, áttételes hatásmechanizmuson keresztül realizálódik, amely hatásmechanizmus feltérképezése, és a kár pénzben kifejezett meghatározása sem magától értetődő.

Informatikai rendszerek esetén a veszélyforrások általában konkrét rendszerelemeket támadnak, majd az egyes rendszerelemek sérülése hat a velük kapcsolatban lévő alkalmazásokra, amelyeken keresztül a munkafolyamatokban - mind az alaptevékenységben, mind az operatív, taktikai és stratégiai irányításban is - fennakadások lehetnek. Amennyiben a kár hatását nem sikerül jól kezelni, a fennakadás az ügyfelek, partnerek, üzleti folyamatok szintjén is érzékelhető lehet és ez szélsőséges esetben piaci hatásokhoz is vezethet (imázs romlás, ügyfelek elpártolása, piacvesztés). A hatás továbbterjedésének megfelelően szokás ezért úgynevezett *elsődleges, másodlagos, harmadlagos* stb. kárról beszélni.

Egy informatikai rendszer esetében a másodlagos, harmadlagos károk nagyságrendekkel nagyobbak az elsődleges, károknál, ezért rendkívül fontos minden veszélyforrás esetén egyenként elbírálni, hogy az esetlegesen bekövetkező hatás meddig terjedhet ki.

Például egy egyszerű merevlemez meghibásodása okozhatja, hogy nagy mennyiségű adat visszaállíthatatlanul megsemmisül. Ilyenkor az elsődleges kár, a merevlemez megjavításának költsége eltörpül az áttételesen okozott károkhoz viszonyulva. Az elveszett adatok pótlásának költségei, a visszaállítás ideje alatt

fennakadt üzleti folyamatok és még rosszabb esetben az ennek hatására elmaradt üzleti haszon hatalmasak lehetnek a bekövetkezés konkrét okától függetlenül.

Tekintve, hogy informatikai rendszerekben a veszélyek, károk, illetve kockázati tényezők hatásmechanizmusa ennyire összetett, gyakorlatilag egyetlen komoly módszertan sem vállalkozik arra, hogy a kockázat pénzügyi nagyságát közvetlenül megbecsülje, forintosítsa.

5.) Kockázat menedzsment

A legtöbb, gyakorlatban alkalmazott kockázatbecslési módszertan a kategorizálás módszerét alkalmazza, azaz csak nagy nagyságrendben határozza meg a bekövetkezés valószínűségét és a kár nagyságát. Ez ugyan nem teszi lehetővé, hogy a biztosításokhoz hasonlóan, számszerű kockázati értéket határozzunk meg egy veszélyforráshoz, de már jó kiinduló pontot ad. Az *egyes kockázati tényezőket egymáshoz hasonlítva* határozzuk meg a gyenge láncszemeket, azokat a pontokat, ahol a legcélszerűbb védekezni. Ezt a folyamatot nevezzük kockázatelemzésnek vagy kockázatmenedzselésnek, nevében is megkülönböztetve a kockázatbecsléstől.

6.) Kockázati veszélyforrások

	Veszélyforrás	Bekövetkezés valószínűsége	Kár			Kockázat	Védelmi intézkedés
		P	C	I	A	R	
Fizikai Vf. 1	Áramszünet	magas		X	X	nagy	Szünetmentesítés
Fizikai Vf. 1	HW meghibásodás	közepes		X	X	közepes	Redundáns rendszerfelépítés
Fizikai Vf. 3	Adathordozó meghibásodása	közepes		X	X	közepes	Biztonsági mentések
Humán vf. 1	Betöréses lopás	alacsony	X	X	X	magas	Riasztó és betörésvédelmi rendszerek
Logikai vf. 1	Lehallgatás	alacsony	X			alacsony	Lehalgatásvédelmi eszközök
Logikai vf. 2	Jogosulatlan módosítás	alacsony	X	X		alacsony	Rendezett jogosultsági rendszerfelépítés
Logikai vf. 3	Megszemélyesítés	alacsony	X	X		alacsony	Rendezett jogosultsági rendszerfelépítés
Logikai vf. 4	Számítógépes betörés	alacsony	X	X		közepes	Tűzfal telepítés
Logikai vf. 5	Vírusfertőzés	közepes	X	X		közepes	Vírusvédelmi rendszer telepítés

7.) Kockázat kezelésének módszerei

A kockázatelemzés eredményeként képet kapunk egy rendszert fenyegető veszélyforrásokról, a bekövetkezési valószínűségeken és becsült kár értékeken keresztül pedig a fellépő kockázat egymáshoz viszonyított nagyságáról. A kockázatmenedzsment célja ennek ismeretében a kockázat hatékony csökkentése, ezáltal a biztonság növelése.

Egy kockázati tényező kezelésére alapvetően három eszköz áll rendelkezésünkre:

- a kockázat csökkentése megfelelő szintű védekezéssel,
- a kockázat áthárítása,
- a tudatos kockázatvállalás.

8.) Védekezés

A kockázatot a bekövetkezési valószínűségek és az okozott károk szorzatainak összegeként definiáljuk, így csökkentése ezen tényezők csökkentésével valósulhat meg. A kockázatcsökkentés alapmódszerei tehát:

- a bekövetkezési valószínűség csökkentése,
- a veszélyforrás kiküszöbölése,
- az okozott kár nagyságának korlátozása, csökkentése.

A megfelelő szintű védekezési módszerek tervezésére általánosan elfogadott és a gyakorlatban is rendkívül jól alkalmazható szemlélet az úgy nevezett PreDeCo kontrollok rendszere alkalmazható. A név a három fő mechanizmus angol nevének kezdetéből áll:

- Preventive: megelőző, kivédő kontrollok
- Detective: felismerő kontrollok
- Corrective: elhárító, helyreállító kontrollok

A PreDeCo szemlélet szerint egy kontroll cél (control objective) biztosítására tett védelmi intézkedések e három, alapvetően más működésű védelmi mechanizmus ötvözéséből tevődnek össze:

A *bekövetkezési valószínűség csökkenthető* erősebb védelmi mechanizmus (megelőző intézkedések) alkalmazásával.

A *veszélyforrások kiküszöbölése* tulajdonképpen tekinthető a bekövetkezési valószínűség csökkentés speciális esetének is, azzal a lényeges kitétellel, hogy ez a valószínűség itt közel nullára csökken. Sajnos a veszélyforrások kiküszöbölése védekezéssel általában nem valósítható meg. Bizonyos ritka esetekben nyílik csak erre lehetőség (pl. megfelelő villámvédelemmel a villámcsapás hatása gyakorlatilag kivédhető). A teljes kiküszöbölés a legtöbb esetben csak megfelelő *architekturális átszervezéssel* oldható meg (új operációs rendszerek telepítésétől a manuális

visszaellenőrzésekig), amelyek kivitelezése csak nagyon ritkán jelent reális alternatívát.

A kockázat csökkentésének fontos eszköze a keletkező *kár nagyságának csökkentése.* Általában azonban csak a kár mértékének korlátozásáról beszélünk. A másodlagos, harmadlagos, egyre nagyobb kárt okozó hatásmechanizmust úgy kezelhetjük, ha az elsődleges károknál, illetve a lehető legalacsonyabb szinten "megakadályozzuk" a kár továbbterjedését. Ehhez minél előbb felismerni (detekció) és minél gyorsabban orvosolni (korrekció) kell a problémát. A károk továbbterjedési mechanizmusának feltérképezése után megfelelő átszervezéssel és a megszüntethető függőségek felszámolásával tovább korlátozható a kár terjedése.

A különösen nagy kárt okozó veszélyhelyzetek lekezelésére célszerű külön felkészülni, úgynevezett katasztrófa-elhárítási tervek készítésével, illetve természetszerűleg az ilyen helyzetekre számító felkészülési tevékenységek végzésével (például biztonsági mentések készítésével).

9.) Kockázat áthárítás

Ha a kár bekövetkezését megakadályozni már nem tudjuk, akkor a kockázat és ezzel a károk áthárítása sok esetben még enyhítheti, orvosolhatja a problémát.

A kockázat-áthárítás elvét követve, például a beszállítókkal, illetve az ügyfelekkel olyan szerződést köthetünk, hogy bizonyos veszélyforrások következményeit ők viseljék. Például bankkártyáknál, ha a PIN-kód illetéktelen kezekbe kerül, akkor a jogosulatlan pénzfelvételért nem a bankot, hanem a kártya birtokosát terhelik az ebből származó veszteségek.

Az áthárítás másik módja *biztosítás* kötése. A biztosítás a bekövetkezett károk pénzügyi kezelését könnyíti. A biztosítási összeggel azonban meg kell fizetni a biztosító kockázatát és költségeit is, így a biztosításként kifizetendő összeg minden esetben meg haladja a kiküszöbölni szándékozott kockázatot. Bár a biztosítás a károk és a kiadások összegének várható értékét nem csökkenti, azaz célszerűtlennek látszik ezt a védelmet alkalmazni, sok esetben mégis érdemes, mert megvédi a céget a kirívóan nagy veszteségektől, amelyek további sokkal nehezebben kezelhető és nagyobb veszteségeket jelentő károkat indukálhatnak. Informatikai kockázatok tekintetében a biztosítási lehetőségek sajnos még eléggé szűkösek.

10.) Tudatos kockázatvállalás

A megfelelő biztonságérzet kialakítása nem más, mint tudatos kockázatvállalás. Mint láttuk, bizonyos veszélyforrások ellen csak célszerűtlenül nagy költségekkel lehet védekezni. Ilyen esetekben a veszélyforrás által jelentett kockázat vállalható, azonban e kockázatokkal feltétlenül tisztában kell lenni. A kockázat vállalására irányuló döntést minden esetben a felső vezetésnek kell meghoznia, illetve jóváhagynia.

Lehetséges védelmi intézkedések számbavétele

A védekezési lehetőségeket célszerű külön dokumentumban, táblázatban összegyűjteni. Az egyes lehetőségekhez fel kell mérni a beruházás és az üzemeltetés nagyságrendi költségeit, valamint az általuk kielégített követelményeket. A könnyebb áttekinthetőség, hivatkozhatóság érdekében a védekezési lehetőségekhez hasonlóan a veszélyforrásokhoz azonosító rendelhető. A kockázatelemzési táblázatba ugyanis már csak a javasolt védekezési lehetőségek azonosítói kerülnek.

A kockázatmenedzselés elve szerint a megfelelő védelmi intézkedéseket úgy lenne célszerű kiválasztani, hogy felírjuk az összes elképzelhető védelmi intézkedést, mindegyiknél megadjuk, hogy milyen hatása van, majd az összes lehetséges kombináció értékelésével megkaphatjuk, hogy melyeket kell kiválasztani ahhoz, hogy az összes elviselhetetlen veszélyforrást megfelelően lefedjük, valamint a maradvány kockázat és a védelmi költségek összege a lehető legkisebb legyen.

A gyakorlatban azonban egy szakember hozzávetőlegesen meg tudja adni, hogy az adott esetben mely védelmi intézkedések alkalmazása jöhet szóba. Ezen alternatívák közötti választásban nyújt segítséget a kockázatelemzés.

Az egyes védelmi intézkedések közötti választás legfontosabb szempontja az ár és az elért hatás. Költségek tekintetében célszerű megkülönböztetni az egyszeri beruházási költségeket az éves fenntartási költségektől. Egy adott módszer kiválasztásánál a rövid- és hosszú távú pénzügyi célok jól elkülöníthetőek.

Védelmi intézkedések		
ID	**Védelmi intézkedés**	**Hatás**
V1	Szünetmentes táp	Az okozott kár és a bekövetkezés valószínűségének csökkenése
V2	Áramfejlesztő generátor	Veszélyforrás kiküszöbölése
V3	Hidegtartalékolás (redundancia)	Okozott kár csökkentése
V4	Duplikálás	Bekövetkezés valószínűségének komoly csökkenése
V5	Hibatűrő rendszerek	Bekövetkezés valószínűségének komoly csökkenése
V6	Biztonsági mentések	Okozott kár csökkenése
V7	Riasztó rendszerek	Okozott kár csökkenése
V8	Biztosítás	Okozott kár csökkenése
V9	Adatkommunikáció rejtjelezés	Veszélyforrás kiküszöbölése
V10	Hozzáférés védelem	Bekövetkezési valószínűség csökkenése
V11	Digitális aláírás	Veszélyforrás kiküszöbölése
V12	Vírusirtó	Okozott kár csökkenése
V13	Aktív vírusvédelem	Bekövetkezési valószínűség csökkenése

11.) Infomatikai rendszerek kockázati besorolása

Az elektronikus információs rendszerek osztályba sorolása															
Sorszám	Az elektronikus információs rendszer megnevezése	Szolgáltatás-menedzser neve	A rendszer különleges személyes adatokat kezelő rendszer?	A rendszer nemzeti adatvagyont kezelő rendszer?	A rendszer létfontosságú információs rendszerelem?	Bizalmasság			Sértetlenség			Rendelkezésre állás			A rendszer biz. sért .rend. áll. szerinti"általános" osztálya (a maximum értékből számolva)
						Az elektronikus információs rendszer bizalmasságának sérülése esetén, a lehetségesen bekövetkező káresemény mértéke	A beállított bizalmasságot érintő káresemény bekövetkezésének gyakorisága	A rendszer besorolás szerinti bizalmassági osztálya	Az elektronikus információs rendszer sértetlenségének sérülése esetén, a lehetségesen bekövetkező káresemény mértéke	A beállított sértetlenséget érintő káresemény bekövetkezésének gyakorisága	A rendszer sértetlenség szerinti bizalmassági osztálya	Az elektronikus információs rendszer rendelkezésre állásának sérülése esetén, a lehetségesen bekövetkező káresemény mértéke	A beállított rendelkezésre állást érintő káresemény bekövetkezésének gyakorisága	A rendszer rendelkezésre állás szerinti bizalmassági osztálya	
1.	TITÁN rendszer	Pénzügyi Iroda vezető	NEM	NEM	NEM	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2
2.	Szociális segélyezési rendszer	Jegyző	NEM	NEM	NEM	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2

3.	Ügyiratkezelő rendszer	Jegyző	NEM	NEM	NEM	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2
4.	Önkadó	Költségvetési csoport vezető	NEM	NEM	NEM	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2
5.	OTP Elektra	Költségvetési csoport vezető	NEM	NEM	NEM	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2
6.	Visual Regiszter	Jegyző	NEM	NEM	NEM	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2
10.	Ebinfo	Jegyző	NEM	NEM	NEM	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2. Csekély káresemény következhet be.	évente	2	2
11.															
12.															

13.															
14.															
15.															
16.															
17.															
18.															

A kockázatelemzés tartalmát megismertem:

.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....