

Kockázatelemzés, kockázatkezelés

Jelen cikkemben arra az egyszerű tényre szeretnék rávilágítani, hogy az információbiztonsági kockázatelemzés kapcsán nem létez(het)nek sablonos megoldások.

Alapok - Kockázatelemzés

Amennyiben egy adott vállalatnak, szervezetnek nincs semmiféle információbiztonsági kockázatelemzése, de valamilyen oknál fogva (ISO 27001-es szabvány bevezetése, SOX, CoBit bevezetés stb.) elérkezettnek látja az időt, hogy elkészítse azt, akkor bátran kijelenthetjük, hogy nincs könnyű helyzetben.

Minden egyes vállalat esetében – attól függően, hogy melyek az adott vállalat tevékenységi körei, földrajzilag hol helyezkedik el, és mekkora az alkalmazotti létszám – sok olyan szempontot kell figyelembe venni, amely megköveteli, hogy minden egyes kockázatelemzés kapcsán egyedileg kialakított értékelési rendszert alkalmazzon a kockázatelemzés végző csapat.

Fenti állítás alátámasztására nézzünk néhány egyszerű példát, amely megmutatja, hogy egy-egy kockázati tényező mellett, hogy valamennyi – a példákban megemlített – vállalkozásnál jelen van, mégsem esik egyforma megítélés alá.

Fontos látni, mint ahogy fentebb már említettem, hogy egy-egy fenyegetés, mint kockázati tényező megítélése nagymértékben függ az adott szervezet tevékenységétől, földrajzi elhelyezkedésétől, alkalmazottainak számától, a tevékenység típusától stb. Az alábbi példákon jól szemléltethető, hogy egy-egy kockázati tényező megítélése mennyire egyedi lehet.

A különböző fenyegetések, mint kockázati tényezők értékelése viszonylag bonyolult folyamat. Az értékelés során – a fent említettek túl – fontos figyelembe venni az esemény bekövetkeztéből eredő lehetséges kár(ok) mértékét, a kár típusát (pénzügyi, erkölcsi, emberi élet stb.), valamint a kockázat (lehetséges kár) csökkentésére bevezetett meglévő intézkedések (biztosítás, oktatás, technológiai folyamatok, eljárásrendek, szabályzatok stb.) meglétét, gyakorlatát, hatékonyságát.

Tipikus példa, hogy egy-egy kockázati tényező önmagában rendkívül nagy kockázatot jelentene, de az adott vállalat a kockázati tényezővel kapcsolatos valamennyi folyamatot, eljárást oly mértékben szabályozta és ellenőrzi, hogy a kockázat mértéke közepesre vagy alacsonyra redukálódik.



Kiss Péter

Információbiztonsági szakértő, tanácsadó. Rendszeresen tart szervezett képzéseket nagyvállalati környezetben, információbiztonsági témában. Független szakértőként nemzetközi és hazai nagyvállalatoknál segít az információbiztonsági rendszerek kialakításában, felülvizsgálatában, működtetésében. Nemzetközi szintű projektvezetői tapasztalattal rendelkezik. ISO 27001-es szabvány bevezetésében, kialakításában több mint öt éves szakmai múlttal rendelkezik. Információbiztonsági auditor, nemzetközi szakmai szervezetek tagja. Szakmai tapasztalatát többek között ipari, banki, biztonsági szektorban szerezte.

Számtalan esetben találkoztam már ennek a fordítottjával is, amikor a kockázati tényező, például egy munkafolyamat önmagában alacsony vagy közepes kockázatot jelentene, de mivel az adott vállalat egyáltalán nem szabályozta és ellenőrizte a munkafolyamatot, ezért a kockázat mértéke elérte a magas kockázati szintet.

Fenyegetés típusa	TERRORFENYEGETÉS		
	Kockázati szint		
Szervezet típus	Magas	Közepes	Alacsony
Pénzügyi (pl. Bank)	×		
Iskola			×
Szkipar (pl. Kőműves)			×
Orvos			×
Étterem			×
Informatikai		×	

Fenyegetés típusa	SZALMONELLAFERTŐZÉS		
	Kockázati szint		
Szervezet típus	Magas	Közepes	Alacsony
Pénzügyi (pl. Bank)		×	
Iskola	×		
Szkipar (pl. Kőműves)			×
Orvos			×
Étterem	×		
Informatikai			×

Fenyegetés típusa	BETŐRÉS		
	Kockázati szint		
Szervezet típus	Magas	Közepes	Alacsony
Pénzügyi (pl. Bank)		×	
Iskola		×	
Szkipar (pl. Kőműves)	×		
Orvos	×		
Étterem	×		
Informatikai		×	

Fenyegetés típusa	ADATVÉDELMI FENYEGETETTSÉG		
	Kockázati szint		
Szervezet típus	Magas	Közepes	Alacsony
Pénzügyi (pl. Bank)	×		
Iskola		×	
Szkipar (pl. Kőműves)			×
Orvos	×		
Étterem			×
Informatikai	×		

Fenyegetés típusa	HAVÁRIA ESEMÉNY		
	Kockázati szint		
	Magas	Közepes	Alacsony
Pénzügyi (pl. Bank)		×	
Iskola		×	
Szakipar (pl. Kőműves)		×	
Orvos		×	
Étterem		×	
Informatikai		×	

Fenyegetés típusa	ÁRAMSZÜNET		
	Kockázati szint		
	Magas	Közepes	Alacsony
Pénzügyi (pl. Bank)		×	
Iskola			×
Szakipar (pl. Kőműves)			×
Orvos		×	
Étterem		×	
Informatikai	×		

Jelen - Kockázatkezelés

Amennyiben egy vállalat túl van a kezdeti lépéseken, azaz elkészült a kockázatok felméréssel és elemzésével, utána sem pihenhet a babérajain. Ahhoz, hogy az elvégzett kockázatelemzés megfelelően szolgálja az információbiztonságot, folyamatosan nyomon kell követni a kockázatok változását, alakulását. A vállalat tevékenységéből, a piaci magatartásból eredő változásokat – kockázati szempontból – követni kell, és az újabb kockázatokat szintén számításba kell venni. Ez a folyamat a kockázatkezelés. A kockázatkezelés során a meghatározott feltevérendszer szerint a kockázatok rendszeresen felülvizsgálatra kerülnek. Ennek keretében egyes kockázatok mértéke változhat, egyes kockázatok eltűnhetnek (megszűnhetnek), míg

újabb kockázatok kerülhetnek előtérbe. A megfelelően végzett kockázatkezelési tevékenység képes garantálni a vállalatok számára, hogy az elvárt információbiztonsági szintet képesek legyenek tartani, illetve, hogy az esetleges veszélyhelyzetekre a megfelelő hatékonysággal legyenek képesek reagálni. Érdekes tény, hogy a vállalatok többsége egy-egy minősítés, tanúsítvány megszerzése után (például ISO 27001) gyakran elhanyagolja a folyamatos kockázatelemzést, amellyel gyakorlatilag kockára teszi (kockázati tényező [1]) a megszerzett minősítést és az elért információbiztonsági eredményeket.

Jövő - Még mindig Kockázatkezelés

A megfelelően kialakított és bevezetett kockázatkezelési eljárások során nem csak a meg-

lévő kockázatokkal kell foglalkozni, hanem a lehetséges kockázatokot is elemezni kell. Egyes nagyvállalatoknál, ahol a vállalat tevékenysége megköveteli (kutató cégek, elektronikai fejlesztő cégek, vegyipar stb.), egy-egy üzleti döntésbe az információbiztonsági szakértőt is bevonják annak érdekében, hogy előre megpróbálják felmérni egy-egy jövőbeni üzleti döntés lehetséges kockázatait, mind a vállalatra, mind az adott termékre vonatkozóan. Szintén fontos szerep jut a kockázatelemzésnek technológiaváltásoknál, illetve újabb technológiák bevezetése során annak eldöntése érdekében, hogy a bevezetendő technológia vajon nem rejt-e arányosan nagyobb kockázatot (bármilyen szempontból), mint a megvalósítástól remélt haszna.