Dr. Magyar Sándor[94]*:* **A kockázatelemzés szerepe az adatvédelem erősítése érdekében**

Az adatvédelem területén rendkívül fontos, hogy a felelősségi körünkbe tartozó személyes adatokat megfelelő biztonságban tudhassuk az általunk menedzselt informatikai rendszerben.
Véleményem szerint elengedhetetlen, hogy az információbiztonság tekintetében rendelkezésre álló erőforrásokat úgy használjuk fel, hogy annak mértéke optimális legyen. Ennek meghatározására egyik módszer a kockázatelemzés lehet.
Kockázatelemzés végrehajtásával, a veszélyek, a sérülékenységek számbavételével csökkenthető a hamis biztonságérzet kialakulása, amely sokszor félrevezető lehet. Példaként említem: ha azt hisszük, hogy védett vonalon beszélünk, amely megóvja az átviteli úton a beszédkommunikációnkat az aktív és a passzív felderítéstől, azonban a titkosítási eljárás gyenge, esetleg vannak olyan nyílt hálózatokhoz illeszkedő külső csatlakozási pontok a rendszerben, melyek irányából fenyegetettség adódhat, amivel mi nem vagyunk tisztában, akkor a hamis biztonságérzet miatt olyan információkat mondhatunk el, melyeknek súlyos következménye lehet. A kockázatelemzés feladata többek között ezeknek a hiányosságoknak a feltárása is.

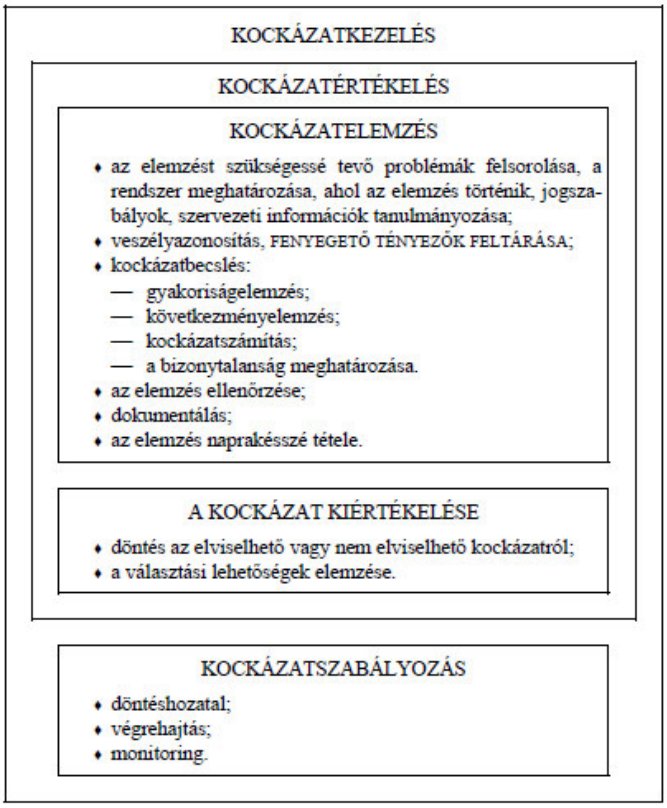
A rendszerek fejlesztésénél kiemelt szerepet kell kapjon a PDCA ciklus, mely az alábbi összetevőkből épül fel:

- tervezés (plan);
- cselekvés (do);
- ellenőrzés (check);
- beavatkozás (act).

Lényege a folyamatos körforgás. A tervezés után kivitelezett rendszert ellenőrizzük, elemezzük, a feltárt hiányosságoknak megfelelően beavatkozunk. Amennyiben az eredményeknek, elvárásoknak megfelelően működik a rendszer, abban az esetben az SDCA ciklus kezdődhet el, ahol az „S" a szabványosítás (standardize) szóból ered. Fontos elem, hogy az ellenőrzés minden esetben nagy szerepet játszik, mely meghatározza, hogy újratervezési vagy szabványosítási funkcióval kezdődjön a következő kör újból.

Az információtechnológia fejlődésével jelentősen megnövekednek a kibertérből érkező kockázati tényezők is a rendszerben, ott ahol mindig, minden esetben biztosítani kell a folyamatos elérést a jogosultságoknak megfelelően. Ezek alapján, a cél a biztonság, amelynek elérését a veszélyek, kockázati tényezők gátolják. Ezeket a kockázati tényezőket azonosítani szükséges, meg kell tenni a megelőző intézkedéseket.
Mint ahogy az, az 1. számú ábrán is látható, a kockázatkezelés része a kockázatértékelés és a kockázatszabályozás is. Azonban előadásomban a legismertebb résszel, a kockázatelemzéssel foglalkozom. A kockázatszabályozásra és a kockázat kiértékelésre nem térek ki.

[94] Óbudai Egyetem, Biztonságtudományi Doktori Iskola



1. ábra: A kockázatkezelés rendszere Forrás: Schutzbach Mártonné [95]

A kockázatelemzés céljának ismertetése, szerepének kiemelése

A kockázatok a szervezetek életében mindenhol jelen vannak, azonban nem mindenhol hasonló súllyal. Egy nem banki környezetben kiszolgált IT rendszer üzemeltetésénél például nem kell számolnunk akkora reputációs kockázattal, mint amekkora a működési kockázata a rendszernek. Például teljesen más típusú kockázatokkal kell számolni a nemzetbiztonsági szolgálatoknál keletkezett minősített adatok kezelésénél, mint egy közműszolgáltatónál.

A szervezetek eredményességében az információs rendszer hatékonysága egyre nagyobb szerepet játszik. Ahhoz, hogy a rendelkezésre állás megfelelő szintű legyen, számba kell venni azokat az információkat – hívjuk ebben az esetben adatvagyonnak –, amelyek hatással vannak az üzletmenetre, a szervezeti célok elérésére, így biztosítani kell azok bizalmasságát, sértetlenségét.

Az az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) értelmezésében a kockázat: „a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye”. Az elektronikus információs rendszerek esetében mindenképpen biztosítani kell a kockázatokkal arányos védelmet.

Ahhoz, hogy az arányos védelmet biztosítani tudjuk, szükség van informatikai rendszerünk lehető legpontosabb ismeretére, továbbá be kell azonosítani a rendszert befolyásoló fenyegetettségeket. Az Ibtv. ezért kihangsúlyozza az elektronikus rendszer számára elvárt biztonsági intézkedések szintjét,

[95] Schutzbach Mártonné: Az informatikai biztonságot fenyegető tényezők, Nemzetvédelmi Egyetemi Közlemények, 7. évfolyam, 2. szám, 2003.

amelyhez az adatokat osztályba kell sorolni. Bár a törvény a kormányzati, államigazgatási, létfontosságú rendszerek[96] védelmére vonatkozik, azonban az alapelv érvényes a piaci szektor esetére is, különösen ott, ahol az információ érteke magasabb.
A kockázatelemzést két módon lehet végrehajtani. Az első a kvantitatív kockázatelemzés, amely számszerűleg mérhető módon közelíti meg a feladatot, melyet egy előre definiált skálán jelenít meg. Az informatikai rendszer sérülékenységeit elsősorban mennyiségi paraméterek alapján állítja be. A második, a kvalitatív kockázatelemzés, mely során minőségi paraméterek alapján állítja be az üzletmenetre gyakorolt hatását. A kvalitatív módszer eredményei kevésbé erőforrás igényesek és komplexebb rendszer esetében kevésbé megbízhatóak.

ISO/IEC 27005:2008 az információbiztonsági kockázatmenedzsment
A szabvány leírja, hogy azonosítani kell:

- a vagyontárgyakat;
- a fenyegetéseket;
- sérülékenységeket.

A 27005-ös szabvány szerint a tipikus fenyegetettségek az alábbiak lehetnek:

- fizikai károk;
- természeti csapás;
- alapvető szolgáltatások kimaradása;
- sugárzás okozta károk;
- adatok kompromittálódása;
- technikai meghibásodás;
- engedély nélküli műveletek;
- funkciók veszélyeztetése.

A fenyegetések felméréséhez a nemzetközi szabvány segítséget ad, melyek az alábbiak lehetnek[97]:

- hardver (pl: nem hatékony karbantartás; porra-, páratartalomra-, elektromágneses sugárzásra-, hőmérsékletingadozásra-, áramingadozásra érzékenység; stb.);
- szoftver (pl: tesztelés hiánya; kijelentkezés nélküli kilépés lehetősége; azonosítási, hitelesítési hiányosságok, gyenge jelszó szabályrendszer, mentés hiánya, stb.);
- hálózat (pl: védelem nélküli kommunikációs vonala, forgalmak; rossz kábelcsatlakozások; küldő vagy fogadó nem megfelelő azonosítása, hitelesítése; nem megfelelően védett nyilvános hálózati csatlakozás, stb.);
- személy (pl: nem megfelelő biztonsági oktatás, biztonságtudatosság hiánya, stb.);
- helyszín (pl: beléptetés szabályozatlansága, nem stabil áramellátás, épület nem megfelelő fizikai védelme, stb.);
- szervezet (pl: felhasználói jogosultságot szabályozó eljárások-, felügyeleti tevékenység-, a kockázatok azonosítására és felmérésére vonatkozó eljárások hiányossága stb.).

ISO 31000:2009 kockázatmenedzsment
Míg az ISO 27005-ös szabvány a hagyományos kontrol rendszerű elgondolást használja, addig az ISO 31000 új alapokra helyezi a gondolkodást.
A ISO 31000 szabvány szerint:

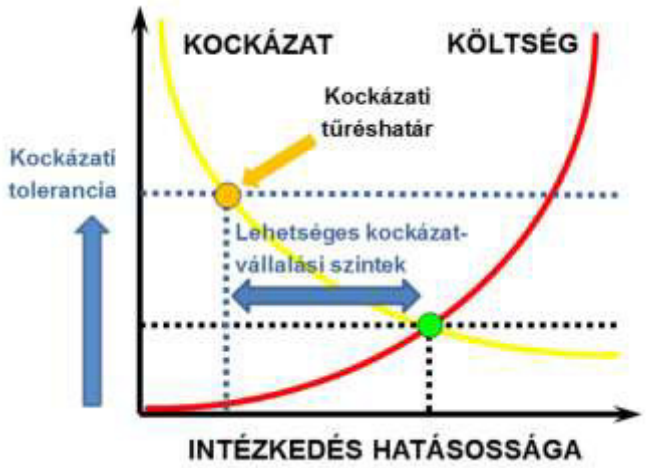
- a kockázatelemzés nem önálló tevékenység, amely külön áll a szervezet fő tevékenységétől, hanem szerves része a vállalati folyamatoknak. A kockázatkezelésnek segítenie szükséges a döntéshozókat a megalapozott döntések meghozásához, a

[96] létfontosságú rendszerek alatt a kritikus infrastruktúra elemeit értem
[97] ISO/IEC 27005: 2011, az információbiztonsági kockázatmenedzsment, C melléklet, p. 42 - 43.

lehetőségek fontossági sorrendbe állításával, alternatív cselekvési megoldásokat nyújtásával.

- A kockázatelemzés során meg kell fontolni a kockázatok okait és forrásait, azok kedvező és kedvezőtlen következményeit, a következmények előfordulásának valószínűségét.
- A kockázatelemzés magában foglalja kockázatok fejlődését és megértését. A kockázatelemzés adatokat szolgáltat a kockázatértékeléshez és döntések meghozatalához, melyik kockázat kezelendő és melyek a leginkább megfelelő kockázatkezelési stratégiák és módszerek.
- A kockázatelemzés során figyelembe kell venni a kockázati források okait és eredetét, azok pozitív és negatív következményeit, valamint azok előfordulási valószínűségét.

Az ISO 31000 megnöveli a valószínűségét a célkitűzések elérésének a lehetőségek, fenyegetettségek azonosításával, az erőforrások hatékony allokálásával, melyet a 2. számú ábra szemléltet.



2. ábra: Hatékonysági megfontolások a kockázatkezelés költségeinek vonatkozásában
Forrás: Ivanyos János [98]

Összefoglalás, következtetések

A kockázatelemzés szükségességét a jogszabályi háttér is kiemeli. Számos új veszély azonosítható, amennyiben tisztában vagyunk a kockázatelemzés szükségességével. Már a kockázatelemzés elmaradása is egyfajta veszélyforrás lehet, mivel a fel nem tárt veszélyforrások miatt kialakult hamis biztonságérzet sok esetben félrevezető lehet.

Azáltal, hogy a kockázatelemzés feltárja informatikai rendszerünk fenyegetettségét, a hiányosságokat, a lehetséges sérülékenységeket, erősödik az informatikai rendszer biztonsága, ezáltal az adatvédelem szintje is.

A kockázatelemzés segíthet a vállalati adatvédelem hatékonyabb megvalósításában, az erőforrások optimalizálásában a szükséges minimális szint meghatározása által.

A kockázatelemzés fő célkitűzése nem a kockázatok számának, hanem azok hatásainak csökkentése kell, hogy legyen.

A kockázat, amely hatással van a szervezet célkitűzéseinek eléréséhez, lehet negatív és pozitív kockázat is. A pozitív kockázatok előnyt jelentenek.

[98] Ivanyos János: Az ISO 31000 szabvány alkalmazása az államháztartási belső kontroll standardok kockázatkezelési ajánlásai vonatkozásában, Trusted Business Partners Kft. http://www.trusted.hu/attachments/article/81/Az%20ISO%2031000%20szabv%C3%A1ny%20alkalmaz%C3%A1sa%20az%20%C3%A1llamh%C3%A1ztart%C3%A1si%20bels%C5%91%20kontroll%20standardok%20kock%C3%A1zatkezel%C3%A9si%20aj%C3%A1nl%C3%A1sai%20vonatkoz%C3%A1s%C3%A1ban.pdf

Felhasznált irodalom

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
- COBIT 5 for Information Security, ISACA, ISBN 978-1-60420-255-7.
- ISO/IEC 27005: 2011, az információbiztonsági kockázatmenedzsment
- ISO 31000 : 2009 Risk Management - Principles and Guidelines
- Ivanyos János: Az ISO 31000 szabvány alkalmazása az államháztartási belső kontroll standardok kockázatkezelési ajánlásai vonatkozásában, Trusted Business Partners Kft. http://www.trusted.hu/attachments/article/81/Az%20ISO%2031000%20szabv%C3%A1ny%20alkalmaz%C3%A1sa%20az%20%C3%A1llamh%C3%A1ztart%C3%A1si%20bels%C5%91%20kontroll%20standardok%20kock%C3%A1zatkezel%C3%A9si%20aj%C3%A1nl%C3%A1sai%20vonatkoz%C3%A1s%C3%A1ban.pdf
- Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2013. évi tevékenységéről.
- Schutzbach Mártonné: Az informatikai biztonságot fenyegető tényezők, Nemzetvédelmi Egyetemi Közlemények, 7. évfolyam, 2. szám, 2003.
- F. Szlivka, I. Molnar: Measured and non-free vortex design results of axial flow fans, Journal of Mechanical Science and Technology 22:(10) pp. 1902-1907, 2008
- Dr. Ferenc Szlivka, Dr. Péter Kajtár, Dr. Ildikó Molnár, Dr. Gábor Telekes: CFX Simulation by Twin Wind Turbine, International Conference on Electrical and Control Engineering (ICECE), Wuha, China, pp. 5780-5783