HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Kuris Zoltán
zoltan.kuris@bm.gov.hu

Faggyas Zoltán
zoltan.faggyas@bm.gov.hu

MINŐSÍTETT ADATOKAT KEZELŐ INFORMATIKAI RENDSZEREK KOCKÁZATÉRTÉKELÉSE ÉS KOCKÁZATMENEDZSMENTJE

Absztrakt

A minősített adatokat kezelő informatikai rendszerekben kezelt minősített adat bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása komplex védelmi intézkedéseket igényel a rendszer teljes életciklusában. Ezen intézkedések csak akkor lehetnek kellően hatékonyak, költségek szempontjából is optimalizáltak, ha azokat a biztonsági kockázatokkal arányosan tervezik és implementálják. Jelen cikkben a szerzők ismertetik a hazai nemzeti és külföldi minősített adatokat kezelő informatikai rendszerek kockázatértékelésére és kockázatmenedzsmentjére vonatkozó követelményeket, a megvalósításukkal kapcsolatos dilemmákat, valamint javaslatokat fogalmaznak meg a még nem szabályozott területein elveiket, módszereiket és eszközeiket illetően.

Providing for the confidentiality, integrity and availability of classified information that are handled in information systems dealing with classified information requires complex protective measures during the entire life-cycle of the system. Such measures can be efficient and cost-efficient only when they are designed and implemented with respect to the security risks. In this current article the authors demonstrate the requirements regarding risk assessment and risk management for information systems that handle national and international classified data, the dilemmas about their implementation, and they form recommendations about their principles, methods and instruments for the unregulated areas.

Kulcsszavak: *kockázatértékelés, kockázatmenedzsment, minősített adat, informatikai rendszerek, INFOSEC ~ risk assessment, risk management, classified information, information systems*

BEVEZETÉS

Korunkat globális fejlettsége alapján információs társadalomként szokás jellemezni. Az elmúlt évtizedek információtechnológiai fejlődése az információ előállításának, terjesztésének, használatának és kezelésének elveit, módszereit és eszközeit forradalmian átalakította, döntő hatást gyakorolva a társadalom gazdasági, politikai és kulturális működésére. Az információ érték, tudás, hatalom, az információvagyon szerepe folyamatosan felértékelődik, napjainkban egyre több területen legfontosabb erőforrássá válik. A magánszektor és a kormányzati szektor szereplőinek hatékony működéséhez, ügyfeleik kiszolgálásához egyaránt fontos, hogy a kellő információ, a megfelelő helyen és időben, a szükséges formában és minőségben könnyen hozzáférhető legyen, melynek érdekében informatikai rendszereiket és infrastruktúráikat folyamatosan fejlesztik, szolgáltatásaikat bővítik. Társadalmunk ezzel egyidejűleg egyre jobban függ ezek működésétől és szolgáltatásaitól, meghibásodásuk, megsemmisülésük, információik kiszivárgása üzemeltetőik és ügyfeleik számára is súlyos károkat okozhatnak. „Az információs társadalom szorosan kapcsolódik és függ a funkcionális információs infrastruktúráktól (pl. távközlő hálózatok, számítógép-hálózatok, távvezérlő rendszerek), melyek tevékenysége viszont nem lehetséges a támogató infrastruktúrák (pl. villamos energiaellátó rendszerek) hatékony működése nélkül.”[1]

Az informatikai rendszerek és infrastruktúrák biztonságának kritikusságát a vállalkozások, állami szervek és intézmények egyre nagyobb mértékben felismerik, a véletlen események (melynek hátterében legtöbbször nem megfelelő rezsimintézkedések vagy emberi mulasztások állnak) és szándékos támadások (adatlopás, kibertámadás, kémkedés, szabotázs, rombolás) bekövetkezési valószínűségének és hatásainak minimalizálására komplex védelmi intézkedések rendszerét alkalmazzák, amely személyi, fizikai, adminisztratív és elektronika biztonsági intézkedések alrendszereiből épül fel.

A komplex védelmi intézkedések rendszerének megvalósítását nemzetközi szabványok (az információbiztonság területén vezető ISO 2700x szabványcsalád), ajánlások (hazai viszonylatban legfontosabb a Közigazgatási Informatikai Bizottság 25. számú ajánlása) támogatják.[2]

Ahhoz hogy a komplex védelmi intézkedések kellően hatékonyak és költségek szempontjából is optimalizáltak legyenek, - a hatékony projektszervezet kialakításán túl - szükséges az alapos és körültekintő kockázatértékelés és jól működő kockázatmenedzsment a rendszerek teljes életciklusában. A kockázatértékelés egy olyan eljárásrendszer, amely azonosítja az informatikai rendszerek biztonsági kockázatait, azaz fenyegetettségüket és sebezhetőségeiket. Meghatározza nagyságukat és, hogy mely területeken szükséges a biztonság megerősítése vagy ellenintézkedés foganatosítása. A biztonsági kockázatmenedzsment pedig az a teljes folyamat, amely azonosítja, kontrollálja és minimalizálja a bizonytalan események lehetőségét, melyek a rendszer erőforrásaira kihatással lehetnek.

A KOCKÁZATÉRTÉKELÉS ÉS KOCKÁZATMENEDZSMENT JELENTŐSÉGE

Azt, hogy milyen gazdasági és politikai hatásokat okozhatnak informatikai rendszereket ért véletlen események (pl. természeti katasztrófa), illetve célzott támadások az alábbi néhány példa jól szemlélteti.

„A Katrina hurrikán 2005 augusztusában mind a vállalati vezetőket, mind az informatika felelőseit megdöbbentette. Ez a természeti katasztrófa súlyos csapást mért az USA déli

államainak informatikai struktúrájára és hálózati rendszereire, jószerével rendet vágott számos szervezet elsődleges és tartalék informatikai rendszerei között."[3]

A közelmúltban a Sony 70 millió felhasználójának adatait szerezték meg hackerek, személyes adatok mellett, bankkártya adatokat is, mely dollármilliárdos kárt okozott a cégnek, jelentősen megingatva piaci jó hírét és pozícióját.

Az USA egyik legnagyobb hadipari cége a Lockheed Martin május végén jelentette be, hogy kibertámadást kíséreltek meg ellene, a támadásnál a távoli elérést biztosító RSA SecurID hardverkulccsal támogatott authentikáció EMC által márciusban közzétett sebezhetőségét használták ki, a támadás sikerességével kapcsolatos hírek ma még ellentmondásosak.[4]

Irán elismerte, hogy jelentős károkat okozott nukleáris erőműveiben a Stuxnet féreg vagy vírustámadás, mely az iráni atomprogramban kulcsszerepet játszó urándúsító centrifugák vezérlését támadta, a hírek szerint a Stuxnet tevékenysége kapcsán az urándúsító centrifugák több mit 20%-a megsemmisült, melynek hatására a többi működését is leállították. A New York Times egy cikke és az iráni kormányzat szerint is a Stuxnet féreg az amerikai és izraeli titkosszolgálat közös fejlesztése.

Szakértők egyenesen orosz-észt kiberháborúként jellemezték a 2007-ben észt informatikai infrastruktúra fontos informatikai pontjait célzó támadást, mely az észt kormánynak egy szovjet hősi emlékmű áthelyezését érintő döntése után indult, internetes kibertámadások összehangolt sorozata volt. E mellett az interneten és mobiltelefon-üzeneteken keresztül folytatódtak, az intenzív propagandatámadások. Az internetes támadások megpróbálták megbénítani a különböző észt honlapok működését, súlyosságát jelzi, hogy az észt hálózaton az adatforgalom sokszor órákon át a normális ezerszerese volt. Az észt miniszterelnök kiberháborúról, külügyminiszterük orosz kormányszervek számítógépeiről érkező internetes terrortámadásokról beszélt.[5]

A Wikileaks nemzetközi nonprofit szervezet weboldalán tesz folyamatosan közzé minősített adatokat tartalmazó anyagokat, legnagyobb számban amerikai diplomáciai jelentéseket, iraki és afganisztáni katonai műveletekkel kapcsolatos dokumentumokat. A nyomozás megállapította, hogy az egyik legnagyobb kiszivárogtatás (köztük 250 ezer diplomáciai jelentés) elkövetője egyetlen személy volt, az amerikai hadsereg volt hírszerző elemzője Bradley E. Manning őrvezető, aki Irakban szolgált a 10. hegyi hadosztálynál és hozzáférése volt az amerikai külügy és hadügy közös SIPRNet[1] hálózatához, melyet „Titkos!" minősítési szintű adatok kezelésére is alkalmaznak.

A fent említett esetek jól példázzák, hogy még tőkeerős vállalatok, nemzetek fő prioritást élvező információs infrastruktúrái is sérülékenyek. A kockázati események bekövetkeztének valószínűsége, és hatásai gyakran alulértékeltek, legyen szó akár emberi mulasztásról, akár természeti katasztrófáról, vagy gazdasági és politikai érdekből vezérelt támadásról.

Az államok az információs infrastruktúráikat ért támadások megelőzésére egyre határozottabb elrettentő intézkedéseket is hoznak, 2011. május 31-ei cikkében a New York Times írta, hogy az USA új katonai stratégiája a kritikus infrastruktúráit ért kibertámadásokat egyenértékűnek fogja tekinti a hagyományos háborús cselekményekkel, és arra katonai csapással is válaszolhat.[6]

[1] Secret Internet Protocol Router Network

MINŐSÍTETT ADATOT KEZELŐ INFORMATIKAI RENDSZEREK KOCKÁZATÉRTÉKELÉSÉT ÉS KOCKÁZATMENEDZSMENTJÉT MEGHATÁROZÓ HAZAI SZABÁLYOZÁS

Felismerve azt, hogy a minősített adatok kezelésénél különösen fontos az egységes szabályozás és követelményrendszer, a külföldi minősített adatok védelme mellett a hazai minősített adatok védelme sem lehet másodlagos. A 2010. április 1-én hatályba lépett, a minősített adat védelméről szóló 2009. évi CLV. törvény (továbbiakban Mavtv.) és végrehajtási rendeletei a NATO és EU minősített adatok védelmével összhangban határozta meg a hazai minősített adatok védelmének rendszerét. A Mavtv. megalkotásának alapját az Alkotmány vonatkozó rendelkezései, az Alkotmánybíróság 34/1994. (VI. 24.) AB határozata, valamint az EU minősített adatok védelmére vonatkozó - az EU tagállamokban kötelező érvényű (a Tanács 2001/264/EK határozat a Tanács biztonsági szabályzatának elfogadásáról), továbbá a NATO minősített adatok védelmére vonatkozó - a NATO tagországokban kötelező érvényű (C-M (2002)49 NATO biztonsági politika) - normák és az euro-atlanti térségben általánosan elfogadott nemzetközi gyakorlat képezi.

A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010. (III. 26.) Korm. rendelet és a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet a hazai és külföldi minősített adatok védelmének személyi, fizikai, adminisztratív biztonsági szabályaira valamint minősített adatokat kezelő rendszerek elektronikus biztonságára egységes követelményeket határozott meg.

A korábban NATO és az EU minősített adatok védelméért és szakmai felügyeletért felelős Közigazgatási és Igazságügyi Minisztérium szervezeti keretében működő Nemzeti Biztonsági Felügyeletet feladata lett a minősített adat védelmének hatósági felügyelete, a minősített adatok kezelésének hatósági engedélyezése és felügyelete, valamint a nemzeti iparbiztonsági hatósági feladatok ellátása. A Mavtv. értelmében a minősített adat védelmi feltételeinek kialakításáért a minősített adatot kezelő szervek vezetője felelős, ezzel kapcsolatos feladatok végrehajtását és koordinálását a biztonsági vezetőnek kell végezni, ahol nagyobb mennyiségű minősített adatot kezelnek, ott a biztonsági vezető vezetésével külön szervezeti egységként helyi biztonsági felügyeletet is kijelölhető.[7]

A 161/2010. Korm. rendelet rendelkezik arról, hogy minősített adatot elektronikus rendszeren kezelő szerveknél szükséges kijelölni az üzemeltetett rendszer elektronikus biztonságáért felelős személyeket: rendszerbiztonsági felügyelőt, rejtjelfelügyelőt illetve rendszeradminisztrátort (rendszerbiztonsági felügyelet és rejtjelfelügyelet létrehozható, ha a minősített adatok mennyisége indokolja). Az elektronikus biztonságra vonatkozó definíciója „a rendszerekben alkalmazott biztonsági intézkedések - a személyi-, a fizikai-, az adminisztratív-, valamint a rendszer-, a kommunikáció- és a rejtjelbiztonság - összessége, amelyek biztosítják az elektronikusan kezelt minősített adat bizalmasságát, sérthetetlenségét és rendelkezésre állását”, utóbbi három fogalmat a Mavtv. Alapelvek alfejezetében2 definiálja.[8]

Minősített adatot a jogszabályok szerint csak NBF által kiállított adatkezelési engedély birtokában lehet („Korlátozott terjesztésű!” kivételével), elektronikus kezelésükhöz

2 2. § …(3) Bizalmasság elve: minősített adat illetéktelen személy számára nem válhat hozzáférhetővé vagy megismerhetővé.
(4) Sérthetetlenség elve: a minősített adatot kizárólag az arra jogosult személy módosíthatja vagy semmisítheti meg.
(5) Rendelkezésre állás elve: annak biztosítása, hogy a minősített adat az arra jogosult személy számára szükség szerint elérhető és felhasználható legyen.

rendszerengedély szükséges, melyet a kérelmező biztonsági vezetőnek kell hitelesítenie és büntetőjogi felelőssége tudatában kell nyilatkoznia arról, hogy a kérdőíveikben szereplő adatok a valóságnak megfelelőek. Az engedélyek kiadása előtt azt az NBF helyszíni bejárás keretében ellenőrizheti, illetve a már akkreditált rendszert is ellenőrizheti. (A törvény hatályba lépése előtt már működő minősített adat kezelések esetében a követelményeknek történő megfelelésre 2011. december 31., az engedélyek megszerzésére 2012. december 31. a törvény által előírt határidő.)

Minősített adatok elektronikus kezelése esetén követelmény a biztonsági dokumentáció elkészítése, amely a rendszerbiztonsági követelmények („Bizalmas!" és magasabb minősítési szintű adatot kezelő rendszer esetében, valamint internetre vagy más nyilvános hálózathoz kapcsolódó „Korlátozott terjesztésű!" minősítési szintű adatot kezelő rendszer esetében) és az üzemeltetés-biztonsági szabályzat, továbbá - ha a minősített adatot elektronikus rendszeren kezelő szerv rejtjeltevékenységet folytat – a rejtjelszabályzat, a működtetési szabályzat és a kezelési utasítás.

Kockázatértékeléssel és kockázatmenedzsmenttel kapcsolatosan a 161/2010. Korm. rendelet 58. § (2) bekezdése rendelkezik arról, hogy „a biztonsági vezető a rendszer életciklusának kezdeti szakaszában megkezdi a biztonsági dokumentáció kidolgozását, és a rendszer megvalósítása során, valamint a rendszer életciklusának további szakaszaiban, kockázatelemzés és kockázatértékelés alapján a szükséges mértékben kiegészíti vagy módosítja", továbbá R2 4. § (1) d) alpontja hogy az NBF d) „útmutatást ad és konzultációt folytat a biztonsági kockázatelemzéssel, kockázatkezeléssel és az elfogadható kockázattal kapcsolatos kérdésekben".

A nemzeti és külföldi minősített adat személyi, fizikai és adminisztratív biztonságával kapcsolatos követelményeket a hazai jogszabályok teljes körűen szabályozzák, ugyanakkor az elektronikai biztonság tekintetében a nemzeti minősített adatokra vonatkozó követelmények közül csak a kisugárzás biztonság (TEMPEST) követelményei lettek az NBF által kiadott dokumentumban meghatározva.

A jelenlegi gyakorlat szerint az elektronikus biztonság többi területén – az NBF állásfoglalására való tekintettel - a NATO követelményeknek való megfelelés az elvárt. A külföldi minősített adatok hazánkban elsődlegesen EU illetve NATO minősített adatok, melyekre vonatkozóan irányadó az EU-s illetve különösen a NATO-s szabályozás, amelyek lényegesen részletesebb szabályozást tartalmaznak az elektronikai biztonság tekintetében. A fentiekben kifejtett anomáliák indokolják, hogy a cikk következő fejezetében a kockázatértékelés és kockázatmenedzsment EU-s és NATO-s irányelveit átfogóan bemutassuk.

KOCKÁZATÉRTÉKELÉS ÉS KOCKÁZATMENEDZSMENT EU ÉS NATO IRÁNYELVEI

Az EU minősített adatok kezelésére friss jogszabály a Tanács 2011. március 31-i 2011/292/EU határozata az EU-minősített adatok védelmét szolgáló biztonsági szabályokról, amely 2011. május 27-én lépett hatályba, hatályon kívül helyezte a Tanács biztonsági szabályzatának elfogadásáról szóló 2001. március 19-i 2001/264/EK tanácsi határozatot. Az új szabályozás a korábbinál is hangsúlyosabban kezeli a biztonsági kockázatértékelést. A korábbi szabályozás is tartalmazta azt, hogy EU minősített adatokat kezelő kommunikációs és információs rendszerek rendszerbiztonsági követelményeit megállapító dokumentumnak (SSRS), mely „EU Bizalmas!" és magasabb minősítésű rendszerek akkreditációjához követelmény, a Tanács biztonságpolitikáján és kockázatértékelésen kell alapulnia, az SSRS-sel kapcsolatban számos követelményt meghatározott, ugyanakkor a kockázatértékelés folyamatát nem részletezte.

Az új szabályozás előírja, hogy Az EU-minősített adatokat fenyegető kockázatokat folyamatként kell kezelni. A folyamat célja az ismert biztonsági kockázatok feltárása, az ilyen kockázatok elfogadható szintre történő csökkentésére irányuló biztonsági intézkedések meghatározása a határozat alapelveivel és minimumszabályaival összhangban, a benne meghatározott elveknek megfelelően. Ezen túl kimondja, hogy ezen intézkedések hatékonyságát folyamatosan értékelni kell. Az EU-minősített adatok teljes életciklusuk alatti védelmét szolgáló biztonsági intézkedéseknek arányban kell állniuk különösen az adatok biztonsági minősítésével, az adat vagy anyag formájával és mennyiségével, az EU-minősített adatok tárolására használt létesítmények elhelyezkedésével és felépítésével, valamint a szándékos károkozás és/vagy bűncselekményekből - a kémkedést, a szabotázst és a terrorizmust is ideértve - eredően helyi szinten fennálló fenyegetéssel. A biztonsági kockázatkezelés a kommunikációs és információs rendszer (CIS) meghatározásának, kialakításának, működtetésének és fenntartásának szerves részét képezi. A kockázatkezelést (értékelés, tulajdonképpeni kezelés, elfogadás, kommunikáció) ismétlődő folyamatként kell elvégezni, a rendszertulajdonosok, projekthatóságok, működtető hatóságok és biztonsági jóváhagyó hatóságok képviselőivel közösen, egy kipróbált, átlátható és teljes mértékben érthető kockázatértékelési folyamat alkalmazásával.

A CIS alkalmazási körét és eszközeit a kockázatkezelési folyamat kezdetekor egyértelműen meg kell határozni. Az illetékes hatóságoknak át kell tekinteniük a CIS-t fenyegető potenciális veszélyeket, valamint naprakész és pontos, az aktuális működési környezetet tükröző fenyegetésértékeléssel kell rendelkezniük. A változó információtechnológiai környezettel való lépéstartás érdekében folyamatosan frissíteniük kell a sebezhetőségi kérdésekkel kapcsolatos ismereteiket, és rendszeresen felül kell vizsgálniuk a sebezhetőségi értékeléseket. A biztonsági kockázatkezelés célja olyan biztonsági intézkedések alkalmazása, melyek eredményeképpen kielégítő egyensúly teremthető a felhasználók igényei, a költségek és a fennmaradó biztonsági kockázatok között. Egy adott CIS akkreditálásának vonatkozásában a megfelelő biztonsági akkreditációs hatóság által meghatározott különös követelményeknek, nagyságrendnek és részletességnek arányban kell állnia a valamennyi vonatkozó tényező figyelembe vételével - a CIS-ben kezelt EU-minősített adatok minősítési szintjét is beleértve - megállapított kockázattal. Az akkreditáció magában foglalja a fennmaradó kockázat hivatalos megállapítását és a fennmaradó kockázatnak a felelős hatóság általi elfogadását.

A CIS-t fenyegető veszélyek enyhítése érdekében mélységi védelem szükséges, amely technikai és nem technikai biztonsági intézkedések végrehajtását jelenti. Szigorúságuk mértékét kockázatfelmérés alapján kell meghatározni, melyek többszörös biztonsági réteget (elrettentés, megelőzés, észlelés, ellenálló képesség, helyreállítás) alkotnak. Meghatározza továbbá, hogy a Főtitkárságnak és a tagállamoknak együtt kell működniük a CIS-en kezelt EU-minősített adatok védelmére vonatkozó legjobb gyakorlat kialakítása érdekében. A legjobb gyakorlatra vonatkozó iránymutatások tartalmazzák a CIS-szel kapcsolatos, az adott fenyegetésekkel és sebezhetőségekkel szemben bizonyítottan hatékony technikai, fizikai, szervezeti és eljárási biztonsági intézkedéseket. A CIS-ben kezelt EU-minősített adatok védelme az információvédelemben részt vevő - az EU-n belüli és kívüli - szervezetek által levont tanulságokra épül.[9]

A NATO Biztonsági politikája (CM(2002)49) B (Alapelvek és minimális biztonsági előírások) és F (INFOSEC) mellékletében rögzíti, hogy civil és katonai szerveinél ahol minősített adatot kezelő rendszereket üzemeltetnek, azokat kockázatértékelésnek és kockázatelemzésnek kell alávetni a biztonságpolitika támogató irányelveinek követelményei szerint. Összhangban az INFOSEC elsődleges irányelvei, INFOSEC menedzsment irányelvei, valamint műszaki és kivitelezési irányelvek követelményeivel a biztonsági kockázatmenedzsment elveit és módszereit akkor is alkalmazni kell, ha NATO

kommunikációs és információs rendszert kapcsolunk más CIS-hez (beleértve az internetet vagy más hasonló nyilvános hálózatot). A biztonsági kockázatmenedzsment elveit és módszereit szintén befogadhatják a nemzeti biztonságot jóváhagyó hatóságok.[10]

A NATO AC/35-D/2004-REV2 (Iránymutatás CIS-ek biztonsági jóváhagyására vagy biztonsági akkreditációjára) dokumentum a biztonsági jóváhagyás/engedélyezés első elemeként nevesíti a kockázatértékelési eljárás felülvizsgálatát és az ebből származó információkat, továbbá vizsgálja a biztonsági dokumentációban rögzített rendszer teljes életciklusára kiterjedő biztonsági intézkedések részeként a kockázatmenedzsmentet és az azonosított fennmaradó kockázatokat.[11]

A NATO kommunikációs és információs rendszerek (CIS) biztonsági kockázatértékelésére és kockázatmenedzsmentjével kapcsolatos iránymutatások, általános irányelveit illetően megállapítható, hogy a kockázatértékelés és a kockázatmenedzsment szerepét kiemeli, a minősített adatot kezelő informatikai rendszerek teljes életciklusára kiterjedő folyamatok, feladatok részletes szabályozását várja el. Kockázatértékelési módszertan választását illetően nem tartalmaz megkötéseket, ugyanakkor megalapozott módszertant vár el, illetve automatizált kockázatértékelő szoftver alkalmazását javasolja.

Az automatizált kockázatértékelő szoftverek előnyei:

- könnyű rögzítés, módosítás és hozzáférés az adatbázisokban tárolt összeállított kockázatértékelő információkhoz;
- képes szemléltetni azokat a hatásokat, melyek tárgyi eszközök vagy információvagyon elvesztéséből erednek, ellenintézkedések kombinációinál;
- segítségükkel gyorsan bevihetünk változásokat a kockázati környezetbe és azonosíthatók a változások a szervezet kockázati pozíciójában.

A fenti munkához nyújt támogatást a NATO AC/35-D-1020 (Áttekintés a CIS-ek fenyegetéseinek jellegéről és mértékéről és CIS-ek sebezhetőségéről) dokumentum. Figyelemmel arra, hogy ez NATO „Korlátozott terjesztésű!”, nyílt publikációban nem elemezhető.

KOCKÁZATÉRTÉKELÉS ÉS KOCKÁZATMENEDZSMENT FOLYAMATAI

Minősített adatot kezelő kommunikációs és információs rendszerek kockázatértékelés és kockázatmenedzsment végrehajtásához a legjobb alapokat a NATO biztonsági politika, irányelvek és útmutatások adják, melyek a nemzeti és EU minősített adatok komplex védelmét biztosító intézkedések kialakítására is jól alkalmazhatók. A NATO INFOSEC menedzsment irányelve rögzíti, hogy a kockázatértékelési és a kockázatmenedzselési eljárásokat közösen kell végezniük a CIS elektronikus információbiztonságát tervező és kivitelezéséért felelős (ök) nek, a működtetéséért felelős(ök)kel, a biztonsági felügyelettel, valamint a projekt tagokkal és a biztonságot jóváhagyó hatósággal/hatóságokkal.

A kockázatértékelési és kockázatmenedzselési eljárásoknak követnie kell a strukturált megközelítést (kivitelezhető mind manuálisan, mind automatizált eszközökkel) és tartalmaznia kell a következő szakaszokat:

- a kockázatértékelés hatókörének és célkitűzéseinek meghatározása;
- a tárgyi eszközök és az információvagyon azonosítása;
- a tárgyi eszközök és az információvagyon értékének meghatározása;
- a meglévő ellenintézkedések azonosítása;
- a szükséges ellenintézkedések meghatározása, összehasonlítása a meglévő intézkedésekkel;
- a kockázatot és a javasolt ellenintézkedések felülvizsgálata;

- kockázatkezelési (kockázatmenedzselési) jelentés elkészítése, mely tartalmazza a végrehajtandó ellenintézkedések leírását és a fennmaradó kockázat leírását. [6.]

A kezdeti kockázatértékelésből származó információkat meg kell őrizni és alapul kell használni a jövőbeli frissítésekhez, az újraértékelések követelményeinek összhangban kell lennie a biztonságot jóváhagyó hatóság/hatóságok követelményeivel, vagy amint az egyeztetve lett a biztonsági jóváhagyó vagy akkreditáló eljárásban.

Kockázatértékelési eljárás

A kockázatértékelés az eljárás azonosítja a CIS-ek biztonsági kockázatait, azaz fenyegetettségüket és sebezhetőségeiket, meghatározza nagyságukat és meghatározza, hogy mely területeken szükséges a biztosítás megerősítése vagy ellenintézkedés. A kockázatértékelés hozzájárul ahhoz a döntéshez, hogy mely biztonsági intézkedéseket kell megkövetelni, és hogy ezek technikai vagy más biztonsági intézkedések egyensúlyával hogyan valósíthatók meg, és elfogulatlanul értékeli a fennmaradó kockázatot. A kockázatértékelésből származó haszon a fokozott/megnövekedett biztonsági tudatosság, amelynek nyilvánvalónak kell lennie minden szervezeti szinten a felső vezetéstől a működtetésen át a kisegítő személyzetig bezáróan. Mivel azok a biztonsági intézkedések, amelyeket a CIS rendszer bevezetésekor határoznak meg bizonyítottan hatékonyabbak, mint azok, amiket később hoznak meg, a kezdeti kockázatértékelést végre kell hajtani a projekt kezdeti tervezési szakaszában és nagyobb részletességgel ki kell terjeszteni, amikor a követelmény meghatározások szövegezésre kerülnek.

A kockázatértékelés, mint feladat nem zárható le véglegesen egy rendszer bevezetésekor. Időszakosan végre kell hajtani azon követelmények szerint, melyeket a biztonsági jóváhagyás vagy akkreditációs eljárás során elfogadásra kerültek, annak érdekében, hogy naprakészen viszonyuljon a változó fenyegetettséghez és sebezhetőségekhez, valamint a szervezet küldetéséhez, információvagyonához, létesítményeihez és eszközeihez. Fő erőforrása az idő és a képzett munkaerő, valamint lehetőség szerint egy automatizált kockázatértékelő eszköz (szoftver) mely megalapozott módszertant alkalmaz. Gyakorlati tapasztalataink alapján a projektek vagy szervezetek első kockázatértékelése igényli a legtöbb erőforrást. Megállapítható, hogy a kockázatértékelésre fordítható erőforrásoknak arányosnak kell lennie a célokkal.

A NATO irányelvek szerint a kockázatértékelés sikere nagyban függ a felső vezetés szerepétől az eljárásban. Vezetői egyetértésnek kell lennie a kockázatértékelés céljaira és hatókörére vonatkozóan, kinyilvánítva, hogy azt a szervezeten belül minden szinten támogatja, ezen túl a vezetésnek felül kell vizsgálnia és jóvá kell hagynia a kockázatértékelés eredményeit.

A kockázatmenedzsment

A kockázatmenedzsment foglalkozik a kockázat kezelésének lehetőségeivel, amely lehet a csökkentés, az áthárítás, a megszüntetés, az elkerülés és az elfogadás. A kockázatot csökkenti a jól szervezett rendszer architektúra, ahol hatásosak a fizikai biztonsági, személyi biztonsági, információbiztonsági és INFOSEC intézkedések. A kockázatmenedzsment magába foglalja a tervezését, szervezését, irányítását és felügyeletét az erőforrásoknak, biztosítva hogy optimális költségeknél a fennmaradó kockázat elfogadható mértékű legyen. A kockázatmenedzsment olyan együttműködési folyamat, amelyet a különböző érdekcsoportok képviselői közösen dolgoznak ki, megértve és mérlegelve a követelményeket és a lehetőségeket. Meggyőződésünk, hogy az így kialakuló fokozott tudatosság erősíteni fogja a biztonságot és jobban megfelel a felhasználói igényeknek.

Irányadó szakemberek szerint és álláspontunk szerint is, a CIS rendszerek kockázatmenedzsmentjénél különös nehézséget jelent a kockázati tényezők dinamikus jellege

és a gyors technológiai fejlődés. Ha a biztonsági kockázatok hibásan nem a megfelelő módon és időben kerülnek felismerésre, szükségtelen, hatástalan költséges intézkedéseket eredményezhetnek.

A kockázatértékelési eljárás kimenete (eredménye) tartalmazza azokat a részleteket, amelyeket bele kell foglalni a biztonsági dokumentációba, amely megkövetelt a biztonsági védelmi intézkedések jóváhagyási vagy akkreditációs eljárásnál (pl. a rendszer specifikus rendszerbiztonsági követelmények szövegezése egy konkrét CIS-re).

Kockázatértékelés és kockázatmenedzselés a CIS-ek életciklusában

A CIS tervezés során kell a kockázatértékelési követelményeket és az alkalmazandó kockázatértékelési és kockázatmenedzselési módszertant meghatározni (felelős szerve – biztonsági felügyelet, koordinálva a CIS tervező szervvel és projekt munkatársakkal.) Majd meg kell kezdeni a kezdeti kockázatértékelést a biztonsági felügyelet követelményei szerint (felelős szerv – CIS tervező szerv/projektcsapat (az INFOSEC technikai és kivitelezési szempontjaiért), koordinálva a biztonsági felügyelettel). Ezt követi a kezdeti kockázatértékelés eredményének jóváhagyása (felelős szerv – biztonsági felügyelet.

A CIS tervezés és beszerzés során aktualizálni kell a kockázatértékelést a biztonsági felügyelet követelményei szerint (felelős szerv – CIS tervező szerv/projektcsapat, kapcsolatot tartva a biztonsági felügyelettel), következő lépcső a finomított kockázatértékelés eredményének jóváhagyása (felelős szerv – biztonsági felügyelet).

A CIS kivitelezés és biztonsági jóváhagyás/biztonsági akkreditáció során kell meghatározni és megegyezi az elfogadható maradék kockázatokról (felelős szerve – biztonsági felügyelet, kapcsolatot tartva a CIS üzemeltetéséért felelős szervvel), a folyamatos kockázatmenedzsment eljárásairól (felelős szerve – biztonsági felügyelet, kapcsolatot tartva a CIS üzemeltetéséért felelős szervvel).

A CIS működtetés során végre kell hajtani a folyamatos kockázatmenedzsment eljárásait (felelős üzemeltetéséért felelős szerv, kapcsolatot tartva a biztonsági felügyelettel).

A CIS bővítésekor pontosítani kell a kockázatértékelést a biztonsági felügyelet követelményei szerint (felelős szerv – CIS tervező szerv/projektcsapat, kapcsolatot tartva a CIS működtető szervvel és a biztonsági felügyelettel), következő lépcső a finomított kockázatértékelés eredményének jóváhagyása (felelős szerv – biztonsági felügyelet) követ. Felül kell vizsgálni és meg kell egyezni az elfogadott maradvány kockázatról (felelős szerv – biztonsági felügyelet, kapcsolatot tartva a CIS üzemeltető szervvel), valamint a folyamatos kockázatmenedzsment eljárásairól (felelős szerv – biztonsági felügyelet, kapcsolatot tartva a CIS működtető szervvel).

A kockázatértékelés menedzsmentje

A kockázatértékelés sikeressége nagyban függ a felső vezetés projektben betöltött szerepétől, ezért szükséges hogy:

- a felső vezetés kinyilvánítsa a projekt támogatását a szervezet minden szintjén;
- a felső vezetés egyetértsen a kockázatértékelés célkitűzéseivel és hatókörével;
- a felső vezetés szakértői kockázatértékelés és kockázatmenedzselés felügyeleti munkacsoportot hozzon léte hivatalos megbízással a hatáskörére és a felelősségére;
- a felső vezetés felügyelje és hagyja jóvá a megállapításait a kockázatértékelő munkacsoportnak és a felügyeleti munkacsoportnak.

A kockázatértékelés tervet úgy kell kialakítani, hogy minimálisan az alábbi szempontokat tartalmazza:

- a CIS rendszer bemutatását;
- a kockázatértékelés hatókörét és célkitűzéseit;

- a kockázatértékelésnél alkalmazott módszertant;
- a kockázatértékelés menedzsmentjét, beleértve a kockázatértékelő munkacsoport és a felügyeleti munkacsoport létrehozását, a jelentések követelményeit.

A kockázatértékelési tervet a CIS tervező és kivitelező szervnek/CIS működtető szervnek/projektcsapatnak kell szövegbe foglalnia, jóváhagyni a biztonsági felügyeletnek kell.

A kockázatértékelő munkacsoport és a vezetés felülvizsgálati munkacsoportja

A kockázatértékelő munkacsoportot személyi, fizikai, adminisztratív és elektronikai biztonságért felelős szakterületeket képviselő szakemberekből szükséges összeállítani, akik saját szakterületük komplex védelemre gyakorolt hatását illetően is felkészültek. A NATO irányelvei szerint a munkacsoport vezetőjét és tagjait a kockázatértékelés végrehajtása alatt teljes munkaidőben e feladatra kell foglalkoztatni. Külső szolgáltatók bevonhatók a kockázatelemzésbe a hatékony erőforrás felhasználás érdekében, ugyanakkor a szervezeteknek maguknak is tisztában kell lennie a kockázatértékelés folyamataival. A kockázatértékelés időigényes folyamat, amit nem szabad siettetni, korábbi tapasztalatok, illetve korábbi kockázatértékelésből származó információk nagyban támogatják a kockázatértékelés eredményeit. Tapasztalati tény, hogy sokszor a munkacsoport tagjaira nyomást gyakorol az őket delegáló szervezeti egység, sietteti őket, hogy térjenek vissza napi munkafolyamataikhoz, ezért súlyponti kérdés az, hogy a kockázatértékelésre fordított erőforrásokat gondosan tervezzük.

A vezetés felülvizsgálati munkacsoportjának hatásköre és felelőssége mind a kezdeti mind a finomított kockázatértékelés eredményének (kimentének) felülvizsgálata és jóváhagyása. Annak észszerűségét, szervezeti információbiztonsági politikához és szervezethez igazodását szükséges felülvizsgálnia. A felülvizsgálati munkacsoport felelős a végső jelentés szövegezésért és elfogadásáért, mely a szervezet felső vezetése és a biztonságot jóváhagyó hatóság számára szükséges előállítani.

A kockázatértékelési eljárás

A kockázatértékelési eljárás egy adatgyűjtő és értékelő gyakorlati eljárás, amely két alapvető kérdéssel foglalkozik:

- mi az értéke a kockázatértékelés tárgyának;
- mi valószínűsége a hatásnak vagy következménynek, mely azonosított fenyegetések bekövetkeztéből ered.

Célja tehát meghatározni egy CIS biztonsági profilját, a kockázatokkal arányosan. A kimenete a kockázatértékelésnek egy biztonsági stratégia mely gondoskodik a CIS elemeinek (értékek) megfelelő védelméről.

A kockázatértékelési eljárás tartalmi elemeit illetően az alábbi lépésekre bontható:

- meghatározni a hatáskörét és célját a kockázatelemzésnek, a céljáról egyeztetni kell a CIS INFOSEC tervező és végrehajtó szervnek/ CIS működtető szervnek/ biztonsági menedzsmenttel/projekttagoknak és a biztonsági felügyeletnek
- Meghatározni a tárgyi eszközöket és információvagyont, melyek hozzájárulnak egy CIS feladatának teljesítéséhez vagy egy szervezeti küldetés teljesítéséhez.
- Meghatározni az értékét a tárgyi eszközöknek, beleértve a hardvert, szoftvert, a környezetben alkalmazott berendezéseket és kapcsolódó dokumentációt.
- Meghatározni az értékét az információvagyonnak a következő hatásokra: közzétételük, módosulásuk, elérhetetlenségük, megsemmisülésük.

- Azonosítani a fenyegetéseket és sebezhetőségeket a kockázati környezetben, és azok szintjét
- Azonosítani a létező ellenintézkedéseket.
- Meghatározni a szükséges ellenintézkedéseket és összehasonlítani a meglévő ellenintézkedésekkel, azonosítani a már meglévő ellenintézkedéseket, meghatározni a javasolt ellenintézkedéseket.
- Felülvizsgálni a kockázatot és az javasolt ellenintézkedéseket, figyelembe véve a következő lehetőségeket, megfelelve a szabványos védelem minimumkövetelményeinek:
  - kockázat megszüntetése: a cél teljesen kiküszöbölni a valós vagy potenciális sebezhetőségeket, teljes körű ellenintézkedések végrehajtásával;
  - tárgyi eszközök és információvagyon káreseményeinek elhárítása: a cél olyan ellenintézkedések bevezetése, melyek megelőzik a kárt amennyire csak lehetséges;
  - tárgyi eszközök és információvagyon káreseményének minimalizálása: a cél olyan ellenintézkedések bevezetése melyek a káresemények hatásait elfogadható szintre csökkentik;
  - tárgyi eszközök és információvagyon káresemény kockázatának elfogadása: lehet olyan döntés, ami elfogad egy kockázatot és következményeit, például ha a káreseménynek a költsége/hatása nem jelentős, vagy a káresemény kockázata elég kicsinek ítélt, vagy az ellenintézkedések költsége sokkal magasabb, nem arányos a káresemény költségével/hatásával.
- Kockázatmenedzsment jelentés elkészítése, amely tartalmazza a megvalósított ellenintézkedések leírását és a fennmaradó kockázat leírását.

Elsőként a kockázati környezet meghatározásánál meg kell szerezni a rajzokat és vázlatokat az adott esthez kapcsolódó szervezeti létesítmények fizikai elrendezéséről. Emellett rajzot kell készíteni az elektromos hálózat, fűtés, szellőztetés és légkondicionálás berendezéseiről. Sokat ezek közül csak egyszer a kezdeti kockázatelemzéskor kell elkészíteni, és a későbbiek során lehet, hogy kevésbé kell aktualizálni. A kockázati környezetben minden fizikai eszközt és információvagyont azonosítani kell és fel kell jegyezni.

Ezt követi az információvagyon értékének megállapítása. A tárgyi eszközök (hardver, szoftver, környezetben alkalmazott berendezések és kapcsolódó dokumentációik) értéke azok cseréjének vagy helyreállításának költsége. Az információvagyon értékét az adatgazdával, vagy az információvagyont ismerő meghatalmazott illetékesekkel, folytatott interjú alapján lehet megállapítani. Az érték megállapításának, mely lehet minőségi tényező is (például alacsony, közepes vagy nagy), az adatgazdától vagy képviselőjétől kapott tájékoztatásból kell származnia, értékelve az információvagyont ért alábbi, legrosszabb forgatókönyv bekövetkezte esetén ért, hatásokat:

- megsemmisülése;
- elérhetetlensége;
- illetéktelken személy általi megismerése;
- illetéktelken személy általi módosítása.

Következő lépésben a kockázatértékelő munkacsoportnak kezdeti konzultációt célszerű folytatnia az illetékes biztonsági jóváhagyóval (biztonsági vezetővel) vagy akkreditációs hatósággal, hogy naprakészre frissítsék ismereteiket a kockázatértékelésben, és szerezzenek

egy átfogó listát a lehetséges sebezhetőségekről. Ezen felül más helyi kockázatértékelése megszerzése a megfelelő hatóságoktól szintén előnyös lehet a kockázatértékelő munkacsoport számára. A kockázatértékelésnek foglalkoznia kell a szándékos fizikai és elektronikai támadási fenyegetettségekkel, és tartalmazniuk kell a természeti katasztrófák fenyegetettségeit is, például tűz, árvíz, villámkár, vihar, földrengés (NATO minősített adatok esetén ehhez már a AC/35D1020 dokumentum alkalmazása is követelmény.) A potenciális sebezhetőségek átfogó listájának, minden elemével kell foglalkoznia az adott kockázati környezetben, és értékelést kell készíteni a potenciális sebezhetőségek bekövetkeztének valószínűségéről. Ez végrehajtható a létesítmény tényeges felmérése alapján vagy a megfelelő személyekkel folytatott interjúkkal.

Ezt követően azonosítani és dokumentálni kell a létező ellenintézkedéseket (személybiztonság, fizikai biztonság, információbiztonság, iparbiztonság, INFOSEC területén levő).

Miután meghatározásra (azonosításra) került a kockázati környezet minden tárgyi eszköze, teljes információvagyona és azok értéke, a következő lépés meghatároznia a javasolt ellenintézkedéseket. Ezt történhet úgy, hogy megvizsgálunk minden egyes tárgyi eszközt, és az információvagyon elemeket vagy csoportosíthatjuk is ezeket, tanulmányozva a fenyegetéseket és sebezhetőségeket, valamint meghatározni az ellenintézkedés (eke)t. Vagy fordítva úgy, hogy azonosítunk minden egyes fenyegetést és sebezhetőséget és azokhoz rendeljük azokat a tárgyi eszközöket és információvagyon elemeket, melyeket érinthet, és utána meghatározzuk a biztonsági ellenintézkedést. Meg kell azonban jegyezni, hogy csak azon fenyegetéseknek van jelentősége, melyeket érintően van olyan sebezhetőség, amelyet kihasználhat egy csapás (szándékos vagy természeti). Fordítva, egy sebezhetőség csak akkor válik jelentőssé, ha van olyan fenyegetettség, ami kihasználhatja azt a sebezhetőséget.

Az ellenintézkedések meghatározásához figyelembe kell venni, hogy a minimális szabványelőírások hazai és külföldi minősített adatok kezelésénél is meghatározottak. A Mavtv. rendelkezik arról, hogy a minősített adatok nyilvánosságra hozatalának, jogosulatlan megszerzésének, módosításának vagy felhasználásának, illetéktelen személy részére hozzáférhetőségének, valamint az arra jogosult részére hozzáférhetetlenné tételének kárértéke alapján kell a minősítési szintet („Korlátozott terjesztésű!”, „Bizalmas!”, „Titkos!”, „Szigorúan titkos!”) megállapítani. A „Szigorúan titkos!” minősítési szintű, minősített adatok bizalmasságának, sértetlenségének és rendelkezésre állásának kompromittálódása súlyosan veszélyeztetheti többek között a nemzet biztonságát, jelentős érdekeit vagy nagyszámú emberéletet.

A folyamat eredménye ként képződik egy lista a biztonsági ellenintézkedésekről melyet összehasonlítunk a meglévő ellenintézkedésekkel és ebből származtatjuk a javasolt ellenintézkedések halmazát. A folyamat utolsó szakaszaként felül kell vizsgálni a kockázatokat és a javasolt ellenintézkedéseket. Ezt a műveletet közösen kell végeznie a projekttagoknak, az adatgazdáknak, a CIS működtető szervnek és a biztonsági felügyeletnek vagy az akkreditáló hatóságnak.

Amikor a kockázatértékelés befejeződik és egyezség születik a végső ellenintézkedések halmazáról, a kockázatértékelés eredményét és a kockázatértékelési eljárás végrehajtásából származó lényeges információkat bele kell foglalni a biztonsággal kapcsolatos dokumentációba (pl. rendszer specifikus biztonsági követelmények ismertetése dokumentum, rendszer-összekapcsolások biztonsági követelményeinek ismertetése)

Kockázatkezelési jelentés

A kockázatértékelés befejezéséhez egy kockázatkezelési (kockázatmenedzsment) jelentést kell készíteni, a következő szempontok szerint:

- kockázatértékelés célja és hatóköre;

- a kockázat értékelési módszertan és a terv;
- az azonosított eszközállomány (tárgyi eszközök és információvagyon), hatások, fenyegetések és sebezhetőségek
- a minimumkövetelményeknek való megfelelésre;
- az elfogadott fennmaradó kockázatokat;
- a folyamatos lévő kockázatmenedzselési folyamatokat.

A kockázatértékelési eszközöknél körültekintően kell ellenőrizni, azt hogy alkalmasak-e a tervezett feladatra, a kockázatértékelő eljárásban levő végleges használatuknak vezetői döntés tárgyának kell lennie.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Napjainkban egyre több területen válik az információ a legfontosabb és legértékesebb erőforrássá, az alkalmazásukat támogató informatikai rendszerek és infrastruktúrák szolgáltatásaitól egyre jobban függ a társadalom, ezzel egyidejűleg ezek emberi mulasztásból, környezeti katasztrófából, vagy szándékos támadásból eredő kárai egyre súlyosabbak mértékűek lehetnek, melyeket általános és minősített adatok kezeléséhez kapcsolódó példákkal szemléltettünk. Ezek megelőzése érdekében komplex – személyi, fizikai, adminisztratív és elektronikai – védelmi intézkedések alkalmazása szükséges, amely hazai és külföldi minősített adatok informatikai rendszeren történő kezelésénél követelmény, és jogszabályokban van meghatározva.

Megállapítató, hogy mind a nemzeti és külföldi minősített adatok kezelésére vonatkozó jogszabályok is kötelező elemként határozzák meg a kockázatértékelést, fontos elemét képzik a CIS-ek biztonsági követelményeinek, a biztonsági dokumentáció részeként szövegbe foglaltan előírtak.

Kijelenthető, hogy a NATO a minősített adatokat kezelő rendszerek komplex védelmének érdekében a kockázatértékelés és kockázatmenedzsment szerepét súlyának megfelelően kezeli, szigorú követelmények határoz meg, azok megvalósítását biztonsági politikája, irányelvei, útmutatásai kellő mértékben segítik.

Az EU minősített adatok védelmét szolgáló új szabályozásában a leghangsúlyosabb új elemek a kockázatértékeléshez kapcsolódnak, követelményeit kellő mértékben részletezi, ugyanakkor folyamataira nem ad olyan részletes útmutatást, mint a NATO-s biztonságpolitika, és az azt támogató számos irányelv és iránymutatás.

Tekintettel arra, hogy a kockázatértékelés és kockázatmenedzsment NATO-ban alkalmazott gyakorlata összhangban van a hazai és EU-s követelményrendszerrel is, a cikk súlyponti részét képezően ezt ismertettük legrészletesebben. Megállapítható, hogy az alkalmazott eljárásrend, amely NATO minősített adatok vonatkozásában most is kötelező, a nemzeti és EU minősített adatokra vonatkozó követelmények teljesítéséhez is jól alkalmazható, az a gyakorlatban is megvalósítható. E munka sikeressége nagyban függ a felső vezetés elkötelezettségétől, ezért a szakterületi vezetők fontos feladata, hogy jelentőségét kellően tudatosítsák. Végrehajtása a személyi, fizikai, adminisztratív és elektronikai biztonsággal foglalkozó szakemberek munkacsoportban történő együttműködését igényli.

A megfelelő anyagi erőforrások biztosításán túl fontos, hogy erre a védendő rendszer fontosságával és kritikusságával arányos kellő időkeret legyen biztosítva. Ennek eredménye ként kielégítő egyensúly teremthető a felhasználók igényei, a költségek és a maradvány biztonsági kockázatok között. Fontos, hogy a megvalósítandó ellenintézkedések nyomán fennmaradó biztonsági maradványkockázatokról a felső vezetés pontos információkat kapjon, és az ellenintézkedések megvalósulása a biztonságot akkreditáló hatóság által elfogadott követelmények alapján folyamatos kockázatmenedzsmentben biztosítva legyen.

A szükséges és elégséges mértékű befektetett anyagi erőforrásokon túl, a kockázatértékelési munkába befektetett erőfeszítések és szakértelem jelentőségét nem szabad lebecsülni, mert az pozitív hatással van a projekt eredményességére, a teljes beruházási költségekre és az időkeretre is.

Felhasznált irodalom

[1] Haig Zsolt: Az információbiztonság komplex értelmezése. Hadmérnök különszám, Robothadviselés 6. tudományos szakmai konferencia 2006. november 22. http://hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.html

[2] Közigazgatási és Informatikai Bizottság 25. számú ajánlása. Magyar Informatikai Biztonsági Ajánlások, http://www.ekk.gov.hu/hu/kib/ajanlasok

[3] Fekete Gizella: A katasztrófa utáni helyreállítási stratégia újragondolása. Business Online, 2008. február 24., http://bonline.hu/cikk/65920/

[4] Dajkó Pál: Támadás érte az USA hadiipari beszállítóinak biztonsági rendszereit. IT Café, 2011. május 28. http://itcafe.hu/hir/usa_lockheed_martin_emc_rsa_securid_hacker_cracker.html

[5] Muha Lajos: Kiberháború az orosz-észt viszony kapcsán. Hacktivity konferencia, 2007. 09. 22-23.

[6] David E. SANGER, Elisabeth BUMILLER: Pentagon to Consider Cyberattacks Acts of War. New York Times, 2011. május 31. http://www.nytimes.com/2011/06/01/us/politics/01cyber.html?_r=1

[7] 2009. évi CLV. törvény a minősített adat védelméről

[8] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[9] A Tanács határozata (2011. március 31.) az EU-minősített adatok védelmét szolgáló biztonsági szabályokról (2011/292/EU)

[10] Security Within The North Atlantic Treaty Organisation (NATO) (C-M(2002)-49). North Atlantic Council, http://www.nbf.hu/anyagok/jogszabaly/C-M(2002)49.pdf

[11] Primary Directive on INFOSEC (AC/35-D/2004-REV2), NATO Security Committee