HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Kassai Károly
kassai.karoly@hm.gov.hu

A KATONAI ELEKTRONIKUS ADATKEZELŐ KÉPESSÉGEK INCIDENSKEZELÉSÉRE VONATKOZÓ ÁLTALÁNOS KÖVETELMÉNYEK

Absztrakt

Az elektronikus adatkezelés fontos és egyben sérülékeny szolgáltatás a katonai üzemeltetési környezetben. A különböző formában jelentkező információs fenyegetések, mint a vírusok vagy rosszindulatú programok általi fertőzés, jogosulatlan rendszer vagy szolgáltatás hozzáférés, hoax fenyegetés, kiegészítve fizikai támadással, rendszer hibával vagy a nélkül, egyre hatékonyabb korlátozó hatásai vannak az információfüggő rendszerekre. A negatív hatások ellensúlyozás érdekében az IT üzemeltető szervezeteknek célszerű egy incidenskezelési keretrendszert kialakítani a kialakított folyamatok irányítására.

The electronic information handling is a very important and vulnerable service in military operational environment. The different information threats as a virus or malicious code infection, unauthorised system or service access, hoax, with or without physical attack, system error have more and more effective limitation impact of information dependent systems. To counterbalance this negative impacts the IT operating organisation should implement an incident handling framework for the control of established processes.

Kulcsszavak: *adat, információtechnológia, biztonság ~ data, IT, security*

BEVEZETÉS

Az elektronikus adatkezelő szolgáltatásokat fel kell készíteni az információs fenyegetések, meghibásodások ellensúlyozására. A gyakran csak statikusnak tekintett védelmi rendszabályokat úgy kell kialakítani, hogy a biztonság sérülése esetén is álljon rendelkezésre egy olyan eljárásrend, ami segíti a problémák érzékelését, a helyzet értékelését, a megfelelő reagálást.

A pontos értelmezés érdekében célszerű az alapvető kifejezések tisztázása a vonatkozó szabványnak megfelelően. E szerint:

- Információbiztonsági esemény (information security event): egy rendszer, egy szolgáltatás vagy egy hálózat állapotának azonosított előfordulása, amely az információbiztonsági szabályzat megszegését vagy a biztonsági ellenintézkedés hibáját, vagy egy addig nem ismert helyzetet jelez, amely biztonság vonzatú.
- Információbiztonsági incidens (information security incident): egyetlen, vagy egy sorozat nem kívánt vagy nem várt olyan információbiztonsági esemény, amely bekövetkezésének jelentős az üzleti műveleteket veszélyeztető és az információbiztonságot fenyegető valószínűsége van. [1]

A NEMZETI ÉS MÁS STRATÉGIAI SZINTŰ KÖVETELMÉNYEK

A minősített adat védelméről szóló jogszabályok szerint a minősített adat biztonságának sérülése esetén a biztonsági vezető feladata a kár felmérése, enyhítése, és lehetőség szerint a jogszerű állapot helyreállítása. A minősítő a Nemzet Biztonsági Felügyeletet tájékoztatja az esetről [2].

Elektronikus minősített adatkezelés esetén a rendszerbiztonsági felügyelet feladata a „hardver védelmét” rendszeresen ellenőrizni, és rendellenesség esetén annak kivizsgálása és a biztonság helyreállítása. A kivizsgálás támogatása érdekében a kormányrendelet naplózási kötelezettséget határoz meg, a naplófájlok időszakonként történő, dokumentált ellenőrzését rendeli el; a naplózási adatokról biztonsági mentéseket kell készíteni és azokat meg kell őrizni [3].

A Nemzet Biztonsági Felügyelet a vonatkozó törvény alapján kivizsgálja a minősített adatok védelmét érintő bejelentéseket és a biztonság megsértésével kapcsolatos eseményeket [4.].

A fentiek mellett az idézett jogszabályok a minősített adat biztonsága érdekében csak általános követelményeket határoznak meg, így megállapítható, hogy incidenskezelésre vonatkozó részletes módszertan, eljárásrend a minősített adatkezelés területén nem azonosítható.

Az elektronikus kormányzati gerinchálózat, illetve a csatlakozó hálózatok biztonságát szabályozó jogszabály szerint a „biztonsági események kezelése” és az „incidens menedzsment” címszavak gyakorlatilag azonos feladatokat tartalmaznak. E szerint:

- az észlelés történhet a hálózatfelügyelet észlelése, vagy felhasználói bejelentés alapján;
- rögzíteni kell az összes beérkező adatot és meg kell kezdeni az elemzést, az elemzési eredményeket öt évig meg kel őrizni;
- dönteni kell a beavatkozásról és tervet kell készíteni;
- a kialakított tervet végre kell hajtani és folyamatosan ellenőrizni kell, hogy nem keletkeznek-e újabb események.

Az incidens menedzselésnél ezek mellett szerepel még az a követelmény, hogy az üzemeltető incidens követő rendszerének képesnek kell lennie az incidensek életciklusának nyomon követésére, a korábbi incidensek közötti keresés támogatására [5]. A másik kormányzati szintű rendszer – az egységes digitális rendszer (EDR) – szabályozására vonatkozó kormányrendelet az előbbiekkel megegyező követelményeket tartalmaz, és sajnálatosan nem világítja meg még azt sem, hogy a címben szereplő „esemény" és „rendkívüli esemény" között mi a különbség [6].

A fentiek alapján megállapítható, hogy jogszabályok az incidenskezeléssel kapcsolatosan csak általános követelményeket határoznak meg, még a rendszer-specifikus kormányrendeletek sem tartalmaznak pontos eljárásokat.

A katonai szervezetek adatkezelésére vonatkozó incidenskezelési eljárások meghatározásának szükségességét a következő rövid stratégiai szintű áttekintés szemlélteti.

A Nemzeti Biztonsági Stratégia megállapítja, hogy a rendszerek sebezhetősége olyan kockázati tényező, amelynek jellegzetessége, hogy kis erőösszpontosítás nagy távolságból is rendkívüli kárt képes okozni. A technológia rohamos fejlődésének korában új feladatként jelentkezik a korszerű, biztonságos informatikai infrastruktúra kialakítása és a kormányzati információs rendszerek védelme. A kormányzati információs rendszert fel kell készíteni a kibernetikai támadások megelőzésére és kivédésére [7].

A Nemzeti Katonai Stratégia szerint a Magyar Köztársaság biztonsági környezetében biztonsági kockázatot jelenthetnek a kritikus infrastruktúra elleni támadások [8].

Az EU Biztonsági Stratégia megállapítja, hogy a kereskedelem, a befektetések, a technikai fejlődés erősítik Európa függőségét – így sebezhetőségét – az összekapcsolt szállítási, energetikai, információs és egyéb infrastruktúrákon keresztül [9].

Az új NATO Stratégiai Koncepció szerint a cyber-támadások egyre gyakoribbá, szervezettebbé vállnak és egyre nagyobb károkat okoznak a közigazgatásban, az üzleti életben és gazdaságnak, veszélyeztethetik a szállítást és az energia rendszereket és egyé kritikus infrastruktúrákat. A támadások elérték azt a küszöböt, amikor már a nemzeti és Euro-Atlanti jólétet, biztonságot és stabilitást fenyegetik [10.].

A stratégiai szintű megfogalmazások jó összegzik a fenyegetések és sebezhetőség szintjének emelkedését, az információs függőséget, illetve a kritikus infrastruktúra védelem (crtical infrastructure protection; CIP, magyarul: KIV) területén belül a kritikus információs infrastruktúra védelem fontosságát, ami kellő alapot kell, hogy adjon a kormányzati és alacsonyabb szintű szabályozásoknak.

A katonai szervezetek növekvő információfüggősége és az egyre veszélyesebb információs fenyegetések miatt célszerűnek látszik a honvédelmi tárca szervezetei számára az elektronikus adatkezelő képességek incidenskezelésére egy olyan általános követelmény kialakítása, ami szakmailag megfelelően támogatja a rendszer-specifikus szabályozások kialakítását.

AZ ÁLTALÁNOS INCINENSKEZELÉS KIDOLGOZÁSÁT TÁMOGATÓ FORRÁSOK

A nemzetközi és nemzeti információbiztonsági menedzsment szabványok [11][12] alapján készült nemzeti ajánlás [13] gyakorlatilag a szabványok ajánlásait tartalmazza, magyarázatokkal bővíti. Ezen kívül az informatikai szolgáltatás nyújtására vonatkozó szabvány nyújt segítséget a feladatok áttekintéséhez [14][14].

Az informatikai irányítás ellenőrzését célzó COBIT módszertan vonatkozó részeit szintén érdemes figyelembe venni, mert a kormányzati ellenőrzést végző szervezetek e módszertant követik [14]. A nemzetközi ajánlások, szabványok mellett más nemzeti vagy egyéb szakmai ajánlások adják a forrást, melynek feldolgozása képezi az incidenskezelés fontosabb feladatait [16][17].

Egy MH szintű szabályozásnak szükségszerűen keret-rendszerűnek kell lennie, így a cikk a helyi hálózatok, eszközök, valamint egy országos hálózat incidenskezeléséhez szükséges feladatok nem minősített adatokkal történő támogatását célozza az említett követelmények, ajánlások feldolgozásával, és nem helyezi előtérbe a központi szolgáltatások kérdését, melyet más formában célszerű rendszer-specifikusan kidolgozni.

AZ ESEMÉNYEK ÉS BIZTONSÁGI HIÁNYOSSÁGOK JELENTÉSE

A jelentésre kötelezett adatok formáját, tartalmát, a jelentési határidőket rendszerenként úgy kell meghatározni, hogy teljesüljenek a jogszabályokban és az állami irányítás egyéb jogi eszközeiben megfogalmazott követelmények. A jelentések rendjét a következő általános elvek szerint kell kialakítani:

- Helyi hálózat, vagy önálló telepítésű eszköz esetében alap biztonsági osztály esetében a rendszergazdát, vagy kijelölt szervezeti elemet kell értesíteni. MH szintű hálózat esetében a hálózatgazdát és az információvédelmi szakfelügyeletet végző szervezetet kell értesíteni.
- Minősített adat elektronikus kezelésére feljogosított rendszer esetében az incidenseket – beleértve a rejtjeltevékenység körébe tartozó incidenseket is – a honvédelmi szervezet biztonsági vezetőjének az információvédelmi szakirányítást végző HM szerv felé kell jelentenie.

Jelentési kötelezettség alá tartoznak minimum az alábbi esetek:

- felismert, vagy felismerni vélt biztonsági események vagy védelmi gyengeségek, biztonsági rések;
- a rendszer hibás működése (hardver, szoftverhiba), vagy engedély nélküli konfigurációváltozás, esetleges emberi hibák;
- a szabályzatoknak nem megfelelő működés, vagy hiányos, pontatlan szabályozás;
- a fizikai védelmi rendszabályok sérülése;
- engedély nélküli rendszerhez vagy adatokhoz való hozzáférés.

A kezdeti jelentésekben a következő adatokat kell jelenteni:

- jelentő személy, szervezet megnevezése;
- érintett rendszer, vagy önálló telepítésű eszköz megnevezése, helye;
- az incidens bekövetkezésének/észlelésének ideje;
- az incidens során: megtörtént/kísérlet történt rá/nem történt meg: bizalmasság, sértetlenség rendelkezésre állás elvesztése;
- az incidens hatásaként: zavart keletkezett a szervezet működésében, személyiségi jogok sérültek, pénzügyi/gazdasági veszteség keletkezett, minősített adat bizalmassága sérült (minősítési szint és kezelési utasítás és adatforma azonosításával);
- az érintett rendszer/hardverelem jellemzői;
- az incidens oka: katasztrófa/egyéb károsodás, hacker vagy egyéb külső behatolás, fizikai behatolás; rendellenes működés vagy technikai hiba, rosszindulatú szoftver, nem szabályos használat, személyi hiba vagy egyéb más ok;
- milyen művelet során derült ki az esemény;

- egyéb fontosnak tartott adatok.

A felhasználókat a jelentési kötelezettség megtételében formanyomtatványokkal, a segítségül hívható személyek nevének, telefonszámának azonosításával, help desk szolgáltatással kell támogatni.

A fenti eljárásrend ugyanígy vonatkozik a rendszer üzemeltető állományára is, tehát az ügyeletes adminisztrátor, technikus által érzékelt technikai paraméterek, riasztási jelzések ugyanezen rendben kell, hogy jelentésre kerüljenek.

A kezdeti jelentéseket nyílt formában kell megtenni, a szükséges védelmi intézkedések megtétele, együttműködő partnerek értesítése, illetékes hatóságok felé történő időbeni jelentés érdekében. A jelentési kötelezettséget nem lehet helyi kivizsgálás indokával késleltetni. Újabb tények felszínre kerülése esetén a kezdeti jelentések után további pontosítások, kiegészítések tehetők.

Az incidensekre történő reagálás rendszabályait, és azzal kapcsolatos egyéni feladatokat az információs rendszer sajátosságainak megfelelően rendszeresen, minimum évente oktatni kell a következő szempontok figyelembe vételével:

- ismertetni kell a helyes viselkedés szabályai az incidens bekövetkezésekor, vagy annak észlelésekor: minden lényeges adat feljegyzése (megsértett szabály, az előforduló rendellenes működés, képernyő üzenet);
- incidens észlelése esetén az egyéni beavatkozások tilalma, a jelentési, értesítési, valamint esetleges bizonyítékszolgáltatásra vonatkozó kötelezettségek.

Az oktatáson esettanulmányok, szimulált esetek feldolgozásával célszerű az incidens helyzetekre történő reagálás hatékonyságát növelni, a krízishelyzetek megoldását támogatni.

A rendszeradminisztrátorok, biztonsági felelősök és egyéb technikai feladatokat ellátó személyek esetében MH rendszerek és minősített adatkezelő rendszerek esetében automatizált mechanizmusokkal, valósághoz közeli tréning környezet biztosításával kell a hatékonyságot növelni.

AZ INCINDENSEK MEGOLDÁSÁNAK TÁMOGATÁSA

E cikkben részletes megoldási javaslatok nem dolgozhatók ki, így a továbbiakban csak a bejelentés (vagy automatikus jelzés) alapján történő megoldás fontosabb tényezőinek áttekintése történik.

A rendszerek üzemeltetői és biztonsági állományából azonosítani kell azokat a személyeket, szervezeti elemeket, akiknek feladata a bejelentett esemény vizsgálata (beleértve a kiegészítő adatok gyűjtését) és javaslattétel az incidensé nyilvánításra, valamint azt a felelős vezetőt, akinek feladata az incidenskezelés elrendelése, szükség esetén a működésfolytonossági tevékenységek beindítása.

A rendszerek sajátosságainak és a rendelkezésre álló erőforrások figyelembe vételével a kezelendő incidenseket fontosságuk szerint be kell sorolni, és azonosítani kell az elhárításhoz (megoldáshoz) szükséges előre látható lépéseket. Az esetek fontosságával arányosan azonosítani kell azokat a szervezeti elemeket, amelyek megerősítésül bevonhatók a feladatok megoldásába, beleértve a más szervezetektől kapott erő, eszköz lehetőségét, szakmai támogatást.

A rendszer-specifikus jellemzők szerint az üzemeltető állomány tevékenységének könnyítése, illetve a szubjektív hibák kizárása, a vezetői döntésekkel járó időveszteség elkerülése érdekében beavatkozási sablonokat kell kialakítani, tesztelni és jóváhagyatni. Így az egyedi döntésekre csak abban az esetben van szükség, ha a megoldás a sablonoktól való eltérést igényli.

A tapasztalatok értékelése és hasznosítása érdekében az incidensekről szóló jelentéseket meghatározott időszakonként összesíteni kell. A tapasztalatok gyűjtése, értelmezése és elemezése alapján az üzemeltetési és védelmi rendszabályokat, eljárásrendet pontosítani, szükség szerint fejleszteni kell. A rendszabályok pontosítása az adott tapasztalatnak megfelelően lehet a rendszerhez kötött technikai vagy adminisztratív jellegű változtatás, de az előfordulás súlyosságának és gyakoriságának függvényében magasabb szintű szabályozási változás sem zárható ki (információbiztonság politika, jogszabály).

Az incidens reagálásra irányuló képességeket a hatékonyság felmérése érdekében teszt, gyakorlások formájában időszakonként, a rendszer-specifikus sajátosságoknak megfelelően, dokumentálva kell ellenőrizni. A tesztek és ellenőrzések – mint kötelező jellegű, nem népszerű események – természetesen csak akkor érhetik el céljukat, ha a sematikus felszínes ismétlés, vagy ugyanazon mozzanatok sorozatos gyakorlása helyett az üzemeltető és biztonsági menedzsment pontosan kidolgozza és fejleszti a gyakorlásokat, a valósághoz közeli teszt feladatokat, gyakorlási lehetőségeket alakít ki, monitorozza az egyéni teljesítményeket, pótfoglalkozásokat szervez a hiányzóknak, gyakoroltatja a külső és belső szervezetek közötti együttműködési feladatokat is.

A későbbi visszakereshetőség, elemzés és feldolgozás érdekében az incidensekre vonatkozó adatokat, valamint a vizsgálati eredményeket rendszerenként, a biztonsági dokumentumokkal együtt kell tárolni.

Az MH szintű adatkezelő rendszerek külső csatlakozásainak, illetve rendszer belső védelmének emelt szintű biztonsága érdekében a detektálás, elemzés, értékelés, reagálás és bizonyítékszolgáltatás céljait szolgáló központi eseménykezelő rendszert a nemzetközi szabványok, és NATO ajánlások szerint kell kialakítani. A központi eseménykezelő rendszer felépítését, szervezeti kapcsolatait, működési rendjét egyedileg kell meghatározni.

A napjainkban egyre népszerűbb – de nemzetenként és szervezetenként egyedileg definiált – cyber-védelmi képesség nemzeti szintű kialakítása remélhetően nem sokáig várat magára. A központi követelmények mindenféleképpen hatással lesznek a fentiekben meghatározott általános követelményekre, de a katonai adatkezelő képességek egyedisége, specialitásai miatt mindenféleképpen szükség van a katonai sajátosságoknak megfelelő specializált eljárások kialakítására.

ÖSSZEFOGLALÁS

A fenti általános feladatok a helyi vagy rendszer-specifikus sajátosságok (adatkezelési jellemzők, minősítési szint, prioritások) alapján az incidens kezelés feladatai egyedileg kidolgozhatók, vagy a felhasznált irodalom alapján tovább bővíthetők. A NATO vagy EU minősített adatok kezelésére vonatkozó rendszabályokkal az incidenskezelés ugyanígy specializálható.

Az elektronikus adatkezelés egyre bonyolultabbá válása megalapozza azt a következtetést, hogy már a helyi rendszerek esetében sem lehet elégséges az emberi erőre támaszkodás. A hálózatok üzemeltetése közben normál esetben is hatalmas mennyiségű adat keletkezik, egy-egy esemény többszörös, különböző szempontú adatokat generál. Az e mellett megjelenő hálózati forgalmi vagy tűzfal adatok még elméletileg sem kezelhetők kézzel.

A napló adatok kezelése, mentése egyre bonyolultabbá válik, illetve az adatok szűrése, elemzése és a szükséges követelmények levonása további alkalmazásokat igényel, speciális szakértelmet követel. Az országos méretű hálózatoknál ezek a jellegzetességek nagyságrendekkel bonyolultabb helyzeteket okoznak.

E sajátosságok miatt a honvédelmi tárcánál szükség van a hálózati biztonsági kérdések erőteljes támogatására, és incidenskezelés esetén is a korszerű informatikai megoldások rendszerbe állítására. Ezt a szükségszerű igényt alátámasztja napjaink eseményei alapján az a

nemzetközi szinten is egyre többet hangoztatott jelenség, hogy a hálózatokat nem elégséges csak a külső támadásokra felkészíteni, azok belülről is sebezhetők. Nyilvánvaló, hogy a felügyelt pontok, a szenzorok számának növekedése az incidenskezelést is bonyolultabbá teszi.

A cikk alapján kijelenthető, hogy a tárca szintű információ biztonságpolitika általános követelményrendszere is bővíthető az incidenskezelésre vonatkozó irányelvek rögzítésével, ami az ellenőrizhetőséget erősítheti az üzemeltető katonai szervezeteknél.

Ugyanígy fontos annak megállapítása is, hogy a nemzeti és nemzetközi összekapcsolások miatt szükség van információbiztonság területén a menedzsment és a technikai szintű együttműködési megállapodásokra, melyek lehetővé teszik a korai előjelzést, segítséget nyújthatnak az incidensek felderítésben és az okozott károk helyreállításában, illetve a bizonyítékok összegyűjtésében és benyújtásában.

Felhasznált irodalom

[1] MSZ ISO/IEC TR 18044 Informatika. Biztonságtechnika. Az információbiztonsági incidensek kezelése, 3.2. p. és 3. 3. p.

[2] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről, 60. §. 1-2. bekezdés OK

[3] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól, 1. §. 22. p. és 58-59.§.

[4] 2009. évi CLV. törvény a minősített adat védelméről, 20. §. (2) j-k) p.

[5] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról, 3. sz. melléklet, Az elektronikus kormányzati gerinchálózat informatikai biztonsági szabályzata, 2. 5. 8. p. OK

[6] 109/2007. (V. 15.) Korm. rendelet az egységes digitális rádió-távközlő rendszerről, 2. sz. melléklet Az EDR használati szabályzata, 2. 2. 3. p. események és rendkívüli események jelentése, kezelése

[7] 2073/2004. (III. 31.) Korm. határozat, a Magyar Köztársaság nemzeti biztonsági stratégiája, II. 1. 6. és III. 3. 7. p.

[8] 1009/2009. (I. 30.) kormányhatározat a Magyar Köztársaság Nemzeti Katonai Stratégiájáról, I. fejezet

[9] A Secure Europe in a Better World, European Security Strategy 2003, „The global challenges" fejezet

[10] Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation, 2010

[11] MSZ ISO/IEC 27001:2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, „A" melléklet, A 14. 1 – 14. 1. 5. p.

[12] ISO/IEC 17799: 2006. Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002:2006), 14. 1.1 – 14. 1. 5. p.

[13] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v. 1.1. 2008, 14. fejezet

[14] Informatika. Szolgáltatásirányítás 1. rész: Előírás (MSZ ISO/IEC 20000-1: 2007), 6. 3. fejezet

[15] Információra és a kapcsolatos technológiára vonatkozó kontroll célkitűzések (COBIT 4.1) DS-6, DS-8, és DS-10. fejezetek

[16] A Chief Information Officer kézikönyve, 2003, Management Kiadó Kft. ISBN 963 86190 9 0; 3/3. 1. 2.

[17] Computer Security Incident Handling Guide (SP-61 revision 1), 3- 8. fejezet