FEHÉR JUDIT[1]

INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK KEZELÉSE EGY BELÜGYI SZERVNÉL

Absztrakt

Nem minden információbiztonsági esemény incidens. Hajlamosak vagyunk arra, hogy incidensként detektáljunk az információs rendszerünkben történő működésbeli elakadást. Holott, ha jól, megfelelően szabályozott környezetben kezelnénk, akkor a biztonsági eseményt okozó problémának a felfedéséből, kivizsgálásából egyértelműen kiderülne, hogy történt-e károkozás azaz olyan incidens, amit kezelni kell. Sok esetben csak elfedjük a probléma okozóját, „tűzoltással" helyre állítjuk a működést és nem veszünk tudomást az okokról. Ami ismételt biztonsági eseményt fog okozni később, mind addig amíg meg nem szüntetjük a probléma okát. Ezzel önmagunknak és a szervezetünknek még nagyobb kárt okozunk. Valószínűleg a probléma megoldásának és megszüntetésébe fektetett energia már az első jelenségnél kevesebb lenne, mint később a nagyobb, szélesebb károkozás megszűntetése.

Kulcsszavak: biztonsági esemény, incidens, probléma, kárelhárítás

Bevezetés

„Tökéletes biztonságot akkor tudunk elérni, ha beszüntetjük az összes tevékenység végzését, azaz nem csinálunk semmit. Belátható, hogy ez ritkán választható megoldás. Azonban a veszélyek és lehetőségek ismeretében eredményesen kezelhetjük a tevékenységek végzéséből fakadó kockázatokat a szükséges kontrollok kialakításával, és működtetésével. A belső kontroll rendszer kialakítása során különféle védelmi intézkedések kombinációjaként alakítják ki a biztonsági szakemberek azt a kontroll rendszert, amely a felső vezetés által felvállalt kockázat vállalási szintnek megfelelő védelmet biztosítja a szervezet számára.

Egy szervezetnél akkor jó a biztonsági kultúra, ha a munkatársak ismerik jogaikat és kötelezettségeiket, és érvényesítik is azokat. Azoknak a munkatársaknak, akik tudatlanságból, hanyagságból, vagy szándékosan nem biztonságtudatosan viselkednek, ismételt biztonságtudatossági oktatáson kell részt venniük, illetve el is marasztalhatják őket. A biztonsági kultúrát tehát az egyének biztonságtudatos magatartása alakítja ki, ahol kialakult, ott a munkatársak tudják, mi veszélyeztet(het)i a biztonságot, és ennek megfelelően cselekszenek is. „[1]

[1] doktorjelölt, Óbudai Egyetem, Biztonságtudományi Doktori Iskola

„Az információs rendszer szempontjából fenyegetésnek tekintünk minden olyan körülményt vagy eseményt, amely az adatok, vagy információs rendszerek biztonságát fenyegethetik. Ide soroljuk például a személyektől eredő támadásokat (pl. számítógépes betörés), és a külső behatásokat (pl. földrengés).”[1]

Egy belügyi szervnél minden esetben érzékeny kérdésként jelentkezik az információbiztonság területén a biztonsági események kezelése. Minden esetben az a cél, hogy minél kisebb területet érintsen, minél alacsonyabb kárértékkel, minél rövidebb időn belül megszűnjön a biztonsági esemény és helyre álljon az eredeti állapot.

Mindenkinek más és mást jelent a biztonsági esemény az információbiztonság világában. Mit is nevezünk biztonsági eseménynek? Sok szakember hajlamos a biztonsági eseményeket incidenséként vagy problémaként detektálni. Ez a három kifejezés, három különböző jelentéstartalommal bíró szakmai meghatározása az események kezelésének sorában. A fogalmak értelmezésében segítségül vannak a szakmát meghatározó útmutatók.

1. A biztonsági esemény az Ibvtv szerint

„*biztonsági esemény:* nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;” [2]

Ebből következik, hogy a biztonsági eseménynek még a gyanúját is komolyan kell venni, nem lehet eltekintetni tőle, ki kell vizsgálni.

Összegezve biztonsági eseménynek tekintjük az elektronikus információs rendszer biztonságában beállt olyan kedvezőtlen változást, melynek hatására az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült vagy megsérülhet.

2. Az incidenst az ITIL informatikai szolgáltatás módszertana az alábbiakban határozza meg:

„Incidens (Incident) – Olyan esemény, amely nem része az informatikaszolgáltatás normális működésének és a szolgáltatás kiesését vagy minőségének romlását eredményezi.”

Ebből az következik, hogy az események mögött általában valamilyen incidensek állnak. Az incidens lehet hiba egy kérdés vagy új kérés is, tehát valamilyen információval már rendelkezünk róla és kárt okozott.

Összegezve az incidens egy bekövetkezett biztonsági esemény, amely azonnali beavatkozást igényel.

3. A problémát az ITIL informatikai szolgáltatás módszertana az alábbiakban határozza meg:

„Probléma (Problem) - Az incidens(ek) valódi, még fel nem tárt oka. Ez lehet egy meghibásodott konfigurációs elem vagy ismeretlen hiba.”

Ebből az következik, hogy ez lehet ismert, amelyre létezik megkerülő vagy igazi megoldás, vagy ismeretlen, amelyre még nincs megoldás, ezért mindaddig fennállnak, amíg egy változtatással végleg meg nem oldjuk a problémát.

Összegezve a probléma egy incidens kiváltó oka, amelyet ha megoldunk, megszűnik az incidens, megkezdhetjük a károk elhárítását, minimalizálását, csökkentését és lezárásra kerül a biztonsági esemény.

A biztonsági esemény szabályozása

„A közigazgatási információs rendszerek működésében tapasztalt tipikus biztonsági kockázatok:

- egy új rendszer a beüzemelést követő néhány héten belül több napra megbénul;
- vezető munkatársak adathordozói illetéktelenek kezébe kerülnek a rajta levő személyes levelezéssel, nem nyilvános adatokkal;
- a munkájában el nem ismert rendszergazda az üzemeltetési feladatok naprakész pontos dokumentálása nélkül távozik;
- a munkatársak áthelyezésüket követően is hozzáférnek a korábbi szervezeti egységük anyagaihoz.

Mi okozza a biztonsági kockázatok növekedését:

- • az informatikai szolgáltatásoktól és az adatkapcsolat folyamatosságától való függés;
- • a szándékos károkozás megnövekedett motivációja;
- • a nagy informatikai beruházást is tartalmazó projektek kudarcai;
- • a hardver, illetve szoftver eszközök meghibásodása;
- • a virtuális vállalatok terjedése;
- • az időjárás változása.

Az információbiztonsági kockázatok kezelésének négy alapmódszere van:

- a tevékenységek beszüntetése (kockázat megszűnik);
- a tevékenység kockázataira biztosítás kötése (kockázatot áthárítottuk a biztosítóra);
- a felelős vezető a kockázatot megismeri és nem tart további intézkedést szükségesnek (kockázatot a szervezet felvállalta);
- a felelős vezető védelmi intézkedéseket (kontroll) valósít meg, vagy szüntet meg (kockázati válasz meghatározása és megvalósítása).”[1]

A biztonsági eseményt minden esetben kezelni kell. Még az Ibvtv is kiterjed erre a feladatra:

„A biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;”[3]

Hogyan is kezdjünk neki egy ilyen esemény kezelésének?

Célszerű egy szervezetnél eljárásrendet kidolgozni a biztonsági esemény kezelésére. Álláspontom szerint egy ilyen eljárásrendnek célja, hogy az adott szervezetnél az elektronikus információs rendszerei tekintetében egységes módon definiálja az alapelveket, rögzítse a keretrendszert és szabályozza azokat a munkafolyamatokat, amelyekkel a legkisebb kárértékkel elháríthatja a működést befolyásoló tényezőket. Az alábbiakban összegzem azokat a javaslatokat, amit egy belügyi szervezetnek feltétlenül rögzítenie kell egy biztonsági eseményt kezelő eljárásrendben.

Egy ilyen eljárásrendben meg kell határozni a szervezeti hatályát, hogy a szervezeten belül és kívül kik érintettek benne. Azaz a szervezettel más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (külső személy). A szervezeti hatályban feltétlenül meg kell határozni a hatály mértékét. Például a külső személyek tekintetében a velük kötött szerződésben rögzített mértékben, illetve a titoktartási nyilatkozat alapján kötelesek eljárni biztonsági eseménykor.

A szervezeti hatályt követően ki kell térni a területi hatály tekintetében. Meg kell határozni azon telephelyeket, egymástól elkülönülő épület egységeket, vagy alszervezetek objektumait, amelyek adott esetben akár földrajzilag is elkülönülnek a szervezettől, de szervesen részét képezik.

A következő szabályozandó terület a tárgyi hatálya. Itt javasolt meghatározni a szervezet általa üzemeltetett valamennyi meglévő és a jövőben fejlesztendő informatikai rendszert, illetve azok környezetét alkotó rendszerelemeket azok teljes életciklusában (az előkészítéstől a rendszerből történő kivonásig). A tárgyi hatálynál egy kormányzati szervnél megfontolandó a minősített adatokat rendszerek kérdésköre, és a vezeték nélküli Internet hozzáférés használatra és a nyilvános prezentáció megjelenítő rendszerek. Ezek viszont olyan speciális területeket fednek le, hogy javasolt őket külön szabályozni.

Egy biztonsági esemény kezelő eljárásrendnek álláspontom szerint feltétlenül figyelembe kell vennie és hivatkoznia, az alábbi normatívákra:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- A hivatkozások között mindenképpen meg kell említeni az adott szervezet Informatikai Biztonsági Szabályzatát.

A hivatkozásokat követően az alapfogalmak között definiálni kell a biztonsági eseményeket, hogy mit minősítünk annak, ezért javaslok néhányat az eddigi tapasztalataim alapján:

- a biztonság megsértésének lehetősége,
- a bizalmasság megsértésének lehetősége,
- a sérthetetlenség megsértésének lehetősége,
- a rendelkezésre állás megsértésének lehetősége,
- az adatokkal való visszaélés lehetősége,
- jogosulatlan hozzáférés az adatokhoz,
- jogosulatlan adatkezelés,
- jogosulatlan adatfeldolgozás,
- tudatos vagy gondatlan károkozás az informatikai rendszerben, a rendszerek által kezelt adatok körében,
- tudatos vagy gondatlan károkozás az informatikai eszközökben.

Az eljárásrendben meg kell határozni biztonsági események kezelésével kapcsolatos azon alapelveket, melyek a szervezet céljait szolgálják. Az alábbiak meghatározóak lehetnek egy belügyi szerv esetében:

- a normál szolgáltatásüzemeltetés mielőbbi helyreállításra kerüljön, és az események folyamatokra gyakorolt káros hatása a lehető legkisebbre legyen csökkenthető,
- bármilyen biztonsági esemény hatékonyan felderíthető és kezelhető legyen, különösen abban a tekintetben, hogy egy eseményt incidensként kell-e kezelni vagy sem,
- az azonosított incidensek kiértékelése és a rájuk adott válasz a legmegfelelőbb és leghatékonyabb módon történjen,
- a szolgáltatás lehető legjobb minőségi és elérhetőségi szintje valósulhasson meg,
- a biztonsági eseményekből és azok kezeléséből gyorsan levonhatók legyenek a megfelelő következtetések, hogy a jövőbeli biztonsági események megakadályozásának az esélyei növekedjenek.

A biztonsági eseményeket minősíteni kell, rangsorolni kell. A minősítésekor meg kell állapítani, hogy az eseményben érintett alkalmazások, eszközök, illetve szolgáltatások mennyire fontosak, fennáll-e szolgáltatás-kiesés. Ha van szolgáltatás-kiesés, az mekkora anyagi vagy egyéb kárt okoz, illetve fel kell mérni az érintett felhasználók számát, körét, összetételét.

A biztonsági esemény súlyozását a következő tényezők összességének figyelembe vételével kell meghatározni a szervezetnek:

- alkalmazás kritikussága
- az érintett felhasználók száma
- alkalmazás(ok)ban a hiba által érintett funkciók jellege
- érintett alkalmazások száma
- a szakrendszerek közti kommunikáció működése;
- rendészeti szerv érintettsége,

Tekintettel a fentiekre a biztonsági esemény súlyozása az alábbiak szerint alakulhat:

1. alacsony: az esemény gyanúja, kéretlen levél, kismennyiségű adathalász levél,
2. közepes: vírusfertőzés adatvesztés és adatkompromittálódás nélkül,
3. magas: működés biztonsági esemény, kis mennyiségű adat szivárgás, tudatos személyes adat kiszivárogtatás, bűncselekmény,
4. kritikus: nagy mennyiségű személyes adat szivárgás, az informatikai rendszerek kompromittálódása, az informatikai rendszer működésének megakadályozása, leállítása.

A biztonsági esemény kezelése során meg kell határozni az eljárásban érintettek körét, a felelőseket. Egy belügyi szervnél az alábbi felelős személyek lehetnek érintettek:

- A szervezet Információbiztonsági Felelőse (a továbbiakban: IBF), vagy helyettese,
- az üzemeltető szervezet Biztonsági Vezetője,
- az ügyben érintett külső személyek Biztonsági Vezetője
- az ügyben érintett szerv vagy szervezeti egység vezetője,
- az informatikai szakterület vezetője,
- a szervezet ellenőrzési szakterületének vezetője,
- a szervezet Adatvédelmi Felelőse,
- az érintett rendszer Adatgazdája.

Az eljárásrendben rögzíteni kell az értesítendő Hatóságok körét, melyeket az alábbiakban rendszereztem egy belügyi szervezet esetében:

- NEIH - Nemzeti Elektronikus Információbiztonsági Hatóság
- NAIH - Nemzeti Adatvédelmi és Információszabadság Hatóság
- NMHH - Nemzeti Média- és Hírközlési Hatóság
- Országos Informatikai és Hírközlési Főügyelet
- NKI - Nemzeti Kibervédelmi Intézet
- EÜF – Elektronikus Ügyintézési Felügyelet
- Nyomozó Hatóság
- Nemzetbiztonsági Szolgálatok

A definíciók rögzítését követően meg kell határozni a keretrendszerét az eljárásrendnek, ez azt jelenti, hogy számba kell venni a biztonsági esemény eseteit. Néhányat felsorolok, amelyek egy belügyi szerv esetében a szervezeti felépítéséből fakadóan előfordulhatnak:

I. Hatósági megkeresés alapján kezelendő biztonsági események
II. Házkutatási parancs alapján kezelendő biztonsági események
III. Vezetői megkeresés alapján kezelendő biztonsági események
IV. Biztonsági esemény észlelése az üzemeltetői szervezet által
V. A szervezet IBF megkeresése alapján végezendő feladatkör
VI. Az Iktató rendszerben történt biztonsági esemény kezelése
VII. A szervezet munkatársa által bejelentett biztonsági esemény kezelése

A szabályozásnak ki kell térnie az eseményt alátámasztó adatok kinyerésének módjára, és azok átadására az érintett hatóságok részére.

Az adatokat minden esetben úgy kell kinyerni az adott érintett elektronikus információs rendszerből vagy az azt monitorozó rendszerből, hogy a későbbiekben más eljárásban bizonyító erőként felhasználhatóak legyenek. Kiemelt figyelmet kell fordítani ezen adatok tárolására, a bizalmasság, sérthetetlenség és rendelkezésre állás szavatolására. Ennek megfelelően az alábbi követelmények elengedhetetlenek:

1. a mentéseket külső elektronikus adathordozóra kell másolni, amit biztosíthat a szervezet, vagy az érintett Hatóságis. Ha az adatok átadása online módon történik, a folyamatot alá kell támasztani igazoló log file-okkal, offline mód esetében az átadás-átvételt aláírással kell igazolni.
2. a sérthetetlenség garantálása érdekében minden egyes file-ról valamilyen fajta algoritmussal kell lenyomatokat készíteni,
3. nagy mennyiségű file-ok esetében a könyvtárak tartalmáról készült lenyomatokból egy összegző lenyomatot kell generálni,
4. a külső elektronikus adathordozó mellé kell tenni papír alapon a rögzített állományok listáját könyvtárszerkezettel, valamint a lenyomatokkal,
5. nagy mennyiségű file-ok esetén a kísérő lapon csak a főkönyvtárak listáját, azok leírásait, továbbá az összegző lenyomatot kell megjeleníteni,
6. az átadandó eszközöket és listákat lepecsételt zárt borítékban kell a Hatóság, illetve az igénylő számára átadni.

A biztonsági esemény kezelésének folyamata

A biztonsági események megjelenését két alapvető részre oszthatjuk.

- működés közben minőségi hiba történik
- hatósági megkeresés keretében keressük az esemény jelenlétét

Amennyiben az elektronikus információs rendszerek működése közben minőségi hiba történik, akkor az kihatással van a rendszerek üzemeltetésének céljára. Bekövetkezik egy úgy nevezett esemény. Az esemény egyszerűen egy külső vagy belső hatás, amely miatt az elektronikus információs rendszerek működésének minőségében változás történik.

Ezt a működés változást lehet emberi erőforrással ellenőrizni vagy monitorozni az elektronikus információs rendszerek működését. Az esemény detektálása akkor történik meg, amikor a normális aktivitást megváltozik. Ezt a változás érzékelheti maga a felhasználó, vagy üzemeltető egyaránt:

- megjelennek bizonyos jelenségek, az elektronikus monitorozás közben,
- egy adott időpontban többen hívták az üzemeltetőket ugyanazon eseménynek a megjelenésével,
- többen keresték a helpdesket szerteágazó működési fennakadással,
- izolált esemény történt egy felhasználónál.

Az események bekövetkezésekor a következő feladatokat kell végrehajtani:

1. Esemény észlelése. Ez a legfőbb cél, hogy egyáltalán észlelni tudjuk az eseményeket. Ezért fontos az elektronikus információs rendszerek monitorozása mind monitorozó alkalmazásokkal, mind emberi erőforrás segítségével.
2. Események csoportosítani tudjuk. Többnyire hatásfoka és rendszeressége szerint. Itt fontos megjegyeznem, hogy nem minden eseményből lesz incidens vagy probléma. Lehetnek olyan események is, amelyek csak a gyanúját vetik fel egy létező problémának, de még nem okoztak incidenst, csak biztonsági eseményként jelentek meg. Vannak események, amelyek csak informatív jellegűek, tudnunk kell róluk, de azonnali beavatkozást nem igényelnek. Be kell tudnunk sorolni az eseményt a szabályzóban meghatározottak szerint.
3. Meg kell tudni állapítani, hogy bekövetkezett-e a biztonsági esemény, azaz történt-e incidens és ha igen, az milyen fokú.
4. Előzetes diagnózist kell felállítani, hogy igényel-e az esemény beavatkozást. Ha nem akkor le kell zárni az esetet.
5. Ha igényel beavatkozást, akkor át kell tekintetni, hogy mekkora kört érint az esemény.
6. Meg kell vizsgálni, hogy mi lehetett az esemény kiváltó oka, a probléma.
7. Események közti összefüggések vizsgálatát kell lefolytatni. Meg kell keresni a probléma forrását.
8. Több alternatív intézkedést kell megfontolni, felsorakoztatni.
9. Meg kell kezdeni az intézkedést a probléma megszűntetésére.
10. Vissza kell térni az eredeti normális működési rendre.
11. Fel kell mérni a károkat, és intézkedéseket kell tenni a kárenyhítésre.
12. Az esemény észlelője felé ki kell dolgozni a válaszadási procedúrát, melyen keresztül meg kell történnie a visszacsatolásnak, hogy az esemény megszűnt.

13. Meg kell vizsgálni, hogy hogyan keletkezett a probléma, és megelőző intézkedéseket kell tenni az újbóli megjelenése előtt. Tehát okulni kell az esetből, le kell vonni a konzekvenciákat.

Az incidens kezelése

Az incidens kezeléséről szakmai egyeztetést folytattam a Belügyminisztérium Információbiztonsági szakterület vezetőivel, és mind az igazgatás, mind az ágazathoz tartozó szervek esetében megállapításra került, hogy sok helyen kapkodnak egy valóban megállapított incidens kezelése kapcsán. Megpróbálják minél előbb helyre állítani a működést, helyre állítani az adatokat. Legtöbb esetben figyelmen kívül hagyják az okozó problémát.

Ennek fényében az általuk elmondottak alapján, azokat összegezve felállítottam egy incidenskezelési modellt. Próbáltam olyan nagy adatfeldolgozó szervezeteket megkeresni, ahol az ilyen esetek kezelése mindennapos tevékenységnek minősült. Az alábbi modellt a KEKKH, a Belügyminisztérium és a Rendőrség gyakorlati elemeiből, továbbá a jogszabályok feldolgozásából építettem fel.

A megállapított incidens bejelentését fogadó elsődleges feladata az incidens hatása és sürgőssége alapján annak besorolása. Erre javasolt egy incidens kezelési rendszert létrehozni.

Az incidensek kezelésével kapcsolatos alapfeladatok

1. Felelősségek és eljárások: meg kell fogalmazni és dokumentálni kell a vezetői felelősségeket, valamint azokat az eljárásokat, amik révén biztosítható a gyors, hatásos és rendezett válaszadás az incidensekre.
2. Események jelentése: meg kell követelni, hogy az események, amilyen gyorsan csak lehet, jelentésre kerüljenek a megfelelő csatornákon keresztül.
3. Gyengeségek jelentése: meg kell követelni az elektronikus információs rendszerrel kapcsolatban álló valamennyi személytől – beleértve a felhasználókat, adminisztrátorokat, rendszergazdákat stb. – hogy jelentsék, ha bármilyen gyengeséget (biztonsági rést) észlelnek vagy gyanítanak az elektronikus információs rendszerekben vagy szolgáltatásokban, vagy a rendszerekhez, a rendszerek biztonságához kapcsolódó szabályzatokban, munkautasításokban.
4. Felmérés és döntéshozatal: a gyengeségeket és az eseményeket fel kell mérni, és el kell dönteni róluk, hogy incidensnek minősülnek-e.
5. Reagálás az incidensekre: a dokumentált eljárások szerint kell reagálni az incidensekre.
6. Tényekre vonatkozó adatok összegyűjtése: meg kell fogalmazni, dokumentálni és alkalmazni kell az incidensekkel kapcsolatos adatok azonosítására, gyűjtésére, beszerzésére és megőrzésére szolgáló eljárásokat.
7. Tanulás az incidensekből: az incidensek elemzéséből és megoldásából szerzett ismereteket fel kell használni arra, hogy csökkenjen a jövőbeni incidensek bekövetkezésének valószínűsége és hatása, illetve, hogy növekedjen az incidenskezelési rendszer hatékonysága.

Az incidenskezelési rendszerrel kapcsolatos használati feladatok

Ahhoz, hogy viszonylag gyorsan tudjuk kezelni az incidenseket, egy elektronikus információs rendszerrel érdemes a folyamatokat megtámogatni. Az incidenskezelési rendszerbe javaslom az alábbi alapadatokat és folyamatokat rögzíteni:

a. az események, incidensek észlelése és bejelentése (emberi és\vagy automatikus eszközök útján);
b. a bejelentéssel kapcsolatos információk összegyűjtése, majd kiértékelése annak megállapítására, hogy mely bejelentéseket kell incidensnek minősíteni;
c. az incidensek megválaszolása a tevékenységek időkorlátainak megfelelően:
   – azonnal, valós- vagy majdnem valós időben;
   – ahol az incidensek ellenőrzés alatt állnak, ott a nem sürgős tevékenységek levezetése;
   – ahol az incidensek nem állnak ellenőrzés alatt, akkor a krízis tevékenységek indítása – mint például a tűzoltóság kihívása vagy egy üzletmenet folytonossági terv (Business Continuity Plan, a továbbiakban: BCP) aktiválása;
   – az incidens kommunikálása a meghatározott belső és külső partnerek felé.
d. meghatározott minősítésű incidensek minőségügyi vizsgálata;
e. valamennyi tevékenység és döntés megfelelő naplózása a további elemzések számára;
f. az incidens döntéssel történő lezárása.[2]

Az incidenskezelési rendszerrel kapcsolatos felülvizsgálati feladatok

Ki kell alakítani az incidensek lezárását követő felülvizsgálati tevékenységeket, ennek keretében:

– a tevékenységek elemzéséből, a vizsgálatok eredményéből le kell vonni a tanulságokat
– meg kell határozni az intézkedésekkel kapcsolatos fejlesztéseket, függetlenül attól, hogy a tanulságokat egy vagy több incidensből vonták-e le
– meg kell határozni az incidenskezelési rendszer egészére vonatkozó fejlesztéseket.

Az incidenskezelési rendszerrel kapcsolatos fejlesztési feladatok

Az incidenskezeléshez kapcsolódó folyamatok fejlesztésének magában kell foglalnia a következőket:

– a szervezet kockázatelemzési és kockázatkezelés folyamatainak felülvizsgálata;
– az incidenskezelési rendszer és a kapcsolódó dokumentáció fejlesztése;
– az információbiztonságra vonatkozó fejlesztések kezdeményezése, amely magában foglalhatja új és/vagy javított biztonsági ellenintézkedések bevezetését is.

A probléma kezelése, az okok felderítése

Ha megvizsgáltuk a problémát, rádöbbenünk, hogy a probléma az incidens mögötti ok, amit egy incidensből nem is feltétlenül lehet kideríteni. Sok esetben az informatikai szolgáltatást nyújtó üzemeltető, a fellépő hibát javítja rögtön, de nem tudják garantálni, hogy máskor nem fog előfordulni. Ennek az az oka, hogy rögtön tűzoltási tevékenységeket kell, végezni, hogy a működés helyre álljon, de nincs idő kivizsgálni, hogy mi okozta az incidenst, tehát a problémát. És mivel nem sikerült feltárni az okát az incidensek, elfedik így az üzemeltetők a következményt, azaz kijavították a hibát, de lehet, másnap újra előjön. Ebből fakad, hogy egy adott probléma felderítéséhez nagyon sok körülményt kell ismerni, amit hiába is vizsgálunk ki közel sem biztos, hogy a probléma teljesen feltárható. Miért is ilyen nagyon fontos, hogy a problémát felfedjük? A problémák feltárásának van egy másodlagos

[2] A KEKKH nyomán

haszna is, létrejön egy adatbázis az ún. ismert hibákról, amelyek segítséget nyújthatnak az üzemeletetők számára, tehát ki lehet belőle alakítani egy incidens kezelési eljárást, ezzel az incidensekre még gyorsabb választ tudnak adni, és már ki is küszöbölhető a hiba. Ez a tapasztalat szerzés. Ha ezt a tudást az adott szerv üzemeltetői egy másik hasonló belügyi szerv üzemeltetőivel meg tudnák osztani, létre lehetne hozni egy közös „probléma adatbázist", annak érdekében, hogy az incidenseket elkerülhessék az üzemeletetők, vagy azonnal elháríthassák az azokat okozó problémákat. A probléma kezelését két fajta féle képen tehetjük meg:

- „Reactive (visszaható) Problem Management: amikor a rendelkezésre információk alapján utólag tárjuk fel és elemezzük a problémát.
- Proactive (kezdeményező) Problem Management: előzetes elemzése a lehetséges problémáknak."[4]

Mindkét megoldás következménye lehet a kárenyhítésnek.

Biztonsági Esemény Kezelési Eljárásrend általános rendelkezései

Az előző fejezetekben azt taglalgattam, hogy milyen sorra jelentkező feladatokat kell ellátni egy biztonsági esemény kapcsán. Ezeket a feladatokat eljárásokba rendszerezni, amelyek mindenkor minden körülmény felett betarthatóak. A fenti eljárások hogyan is jelennek meg a gyakorlatban? Lássunk rá egy általános példát:

1. Biztonsági esemény gyanúját vagy észlelését követően az észlelő szervezet vagy személy értesíti a szervezet IBF-ét,
2. a szervezet IBF megteszi az elsődleges intézkedéseket az esemény kivizsgálására,
3. a szervezet IBF-e felméri az esemény körülményeit, valamint súlyozza azt, valamint megállapítja, hogy történt- e incidens,
4. a súlyozási rend szerint magas és kritikus besorolású biztonsági eseménynél a szervezet IBF értesíti a szervezet vezetőjét és az ügyben érintett felelős személyeket,
5. a szervezet IBF intézkedéseket tesz a biztonsági esemény vagy adott esetben az incidens elhárítására,
6. a súlyozási rend szerint magas és kritikus besorolású biztonsági eseménynél a szervezet IBF értesíti a megfelelő Hatóságokat a biztonsági eseményről, annak körülményeiről és a megtett intézkedésekről,
7. a szervezet IBF együttműködik az eljárásban résztvevő hatósággal és képviseli szervezet érdekeit, adott esetben átadja az érintett adatállomány az arra illetékesek számára,
8. a szervezet IBF felméri a károkat, összegzi a károk enyhítésére teendő intézkedéseket,
9. a szervezet IBF kivizsgálja az esemény körülményeit és levonja a következtetéseket, melynek keretében megelőző intézkedéseket fogalmaz meg a hasonló biztonsági események elkerülése érdekében,
10. a súlyozási rend szerint magas és kritikus besorolású biztonsági eseményről az eljárás végén a szervezet IBF elkészíti a jelentést és átadja a szervezet vezetőjének,
11. a szervezet IBF minden hónap utolsó munkanapján összefoglaló jelentést készít az adott hónap biztonsági eseményeiről.

Az IBF feladatai a biztonsági esemény kezelése során

Amint az előzőekben is láttuk az IBF-nek rendkívül sok feladata van a szervezetnél, a szervezet képviselése során, és a biztonsági esemény kezelése során. Az alábbiakban rendszereztem ezen feladatokat:

- a nyilvántartásokból az érintett személy nevén lévő számítástechnikai eszközök listája,
- az érintett szerv postafiók (levelezés) mentése,
- az érintett számítógépben található adathordozók a mentése,
- mobil számítástechnikai eszközök mentése,
- mobil adathordozók mentése,
- a hálózati file szerver szervezeti közös meghajtójának a mentése,
- az érintett hálózati tárhelyeinek a mentése,
- az érintetthez köthető városi és szervezeti telefonszám híváslistája,
- az érintett szolgálati mobil telefon híváslistája,
- az érintett személy vagy szervezet, különböző rendszerekhez történő jogosultságainak feltalálása,
- az érintett személy által kezelt rendszerek naplói,
- az érintett személy által kezelt, iktatórendszerben rögzített irat állomány listája,
- és minden más, ami a biztonsági esemény vizsgálatához, illetve elhárításához szükséges.

Biztonsági esemény során a kárelhárítás, vagy intézkedés keretében az eljárásban érintett személy tekintetében az alábbi hozzáférések vagy jogosultságok felfüggesztéséről vagy megszüntetéséről gondoskodhat az IBF:

- hálózati hozzáférés,
- hálózati közös meghajtóhoz történő hozzáférés,
- levelezési postafiókhoz történő hozzáférés,
- különböző levelezési csoportokhoz történő hozzáférés,
- az érintett rendszerekhez történő hozzáférés,
- szolgálati mobiltelefon korlátozása,
- szervezeti és városi telefon korlátozása.

Az üzemeltető szervezet Biztonsági Vezetőjének feladatai az érintett szervezet IBF megkeresése alapján:

- a szervezet által biztosított felhasználói postafiók (levelezés) mentése és azok átadása, tiltása, felfüggesztése,
- az üzemeltett számítógép adathordozóinak a mentése és azok átadása,
- a szervezetileg nyilvántartott mobil számítástechnikai eszközök mentése és azok átadása,
- a szervezet által nyilvántartott mobil adathordozók mentése és azok átadása,
- a hálózati file szerver szervezeti közös meghajtójának a mentése és azok átadása,
- az érintett személy vagy szervezet hálózati tárhelyeinek a mentése és azok átadása, tiltása, felfüggesztése,

- az érintett személyhez köthető városi és a szervezeti telefonszám, szolgálati mobiltelefon híváslistájának elkészítése és azok átadása, az eszközök használatának tiltása, felfüggesztése,
- az érintett személy az üzemeltett különböző rendszerekhez történő jogosultságainak feltalálása és azok átadása,
- az üzemeltett rendszerek tekintetében, az érintett személy által kezelt rendszerek naplóinak mentése és azok átadása,
- minden elvégzett feladatról visszajelzés küldése,
- minden online vagy off line átadott adatállományhoz mellékelni kel valamely titkosított eljárással készített HASH lenyomatot.

Biztonsági Esemény Kezelése során az IBF-nek értesítenie kell az alábbi Hatóságokat

- NEIH - Nemzeti Elektronikus Információbiztonsági Hatóság
- NAIH - Nemzeti Adatvédelmi és Információszabadság Hatóság
- NKI - Nemzeti Kibervédelmi Intézet

Összefoglalva, a fenti elemzésben sorra vettem, hogy mit tekinthetünk biztonsági eseménynek, incidensnek és problémának. E három fogalom egymásból következtek. Ezen kifejezéseket próbáltam körülhatárolni, meghatározni.

Egyértelműen kitűnt az elemzésekből, hogy nem minden biztonsági esemény incidens. Bizonyos biztonsági események az általunk végzett vizsgálatok alapján lehetnek megvalósult incidensek, amelyek minden esetben intézkedést igényelnek, továbbá a legtöbb esetben károkozással járnak, vagy problémák, amelyek eseményt váltanak ki. Viszont azt is sikerült megállapítani, hogy minden incidenst valamilyen probléma okozza. A probléma egy vagy több incidens eredő oka is lehet.

Ha az incidenst okozó problémát megtaláltuk, akkor azt kezelni is kell. „A problémakezelés fő célja az incidensek hatásának minimalizálása. Reaktív módon a hiba okának megkeresésével foglalkozik és megelőző, proaktív módon az incidensek jövőbeni előfordulásának megakadályozását végzi.”[4] Tehát, egyértelművé vált, hogy az incidens és a probléma nem azonos fogalmak, egymásból következnek és igen szoros a kapcsolat közöttük. A problémának a feltárása és megoldása maga után vonzza azt a tényt is, hogy az incidenst megszüntettük, azaz a biztonsági eseményt kezeltük.

Annak érdekében, hogy a probléma többször ne jelenjen meg szervezetünknél és okozzon biztonsági eseményt létre kell hozni, a saját, illetve más szervezetek tapasztalásaiból egy tudásbázist, egy adattárat, melyben modellezzük a biztonsági esemény megjelenésétől a probléma megoldásán át a kárenyhítésig a teljes folyamatot. Így lehetőséget adunk saját magunk és azon szervezetek számára, akikkel ezen tudást megosztjuk, hogy időben észlelhessük és el is háríthassuk a fenyegető veszélyeket.

Felhasznált Irodalom

[1] Horváth Gergely Krisztián, CISA CISM: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, KIFÜ, Széchényi terv, Budapest, 2013, 1-2.

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 9. pont

[3] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 10. pont

[4] ITIL - az informatikaszolgáltatás módszertana KFKI Számítástechnikai Rt Verzió: 3.1 2002. Széchenyi-terv, 10-15

Feldolgozott irodalom

– 2003. évi C. törvény az elektronikus hírközlésről
– 2010. évi CXLVII. törvény egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról
– 222/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás működtetéséről
– 276/2006. (XII. 23.) Korm. rendelet a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala létrehozásáról, feladatairól és hatásköréről
– 30/2011. (IX. 22.) BM rendelet a Rendőrség szolgálati szabályzatáról
– 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról Köteles Bernadett (összeállította): A kormányzati intézmények informatikai stratégiájának készítése - A Közigazgatási Informatikai Bizottság 22/1. számú (2.0 verzió) ajánlása – 2009.
– Sebestyén Attila: Stációk és determinánsok a rendvédelmi szervek informatikai működésének fejlődésében - doktori (PhD) értekezés (28. oldal) - Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest - 2009.- p.17-28.
– Rajnai Zoltán - Mógor Tamásné: Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása - Bolyai Szemle XXIII. évfolyam, 2014/2. szám - Nemzeti Közszolgálati Egyetem - ISSN 1416-1443 - p.43-59.
– Pándi Erik: A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-katonai-, és közigazgatási kommunikációs rendszerek megszervezésére és irányítására - doktori (PhD) értekezés - Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi

Könyvtár, Budapest - 2005. - p. 21-68.

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) Az Európai Unió Hivatalos Lapja, 2016.5.4., L 119/1-88pp.
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
- 2000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről,
- 2011. évi CXII. tv az információs önrendelkezési jogról és az információszabadságról,
- 2003. évi C. tv. az elektronikus hírközlésről,
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,
- a 301/2013. (VII. 29.) Korm. rendelet „a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról”,
- 233/2013. (VI. 30.) Korm. rendelet „az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről,
- 36/2013. (VII. 17.) BM rendelet „a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról”,
- 77/2013. (XII. 19.) NFM rendelet az „állami és önkormányzati szervek elektronikus

információbiztonságáról szóló 2013. évi L. törvényben, illetve a módosításáról szóló 2015. évi CXXX. törvényben, meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről.

- 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról,
- 21/2011. BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról,
- 94/2009. HM utasítása a honvédelmi tárca információbiztonság politikájáról,
- 23/2013. (V.17.) ORFK utasítást a belső adatvédelmi és adatbiztonsági szabályzatról,
- 45/2013. (XI.15.) ORFK utasítást az internethálózat működtetéséről, valamint az Internet és elektronikus levelezési rendszer Rendőrségi igénybevételének szabályairól.
- 25. számú Ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA),
- 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK),
- 25/1-3. kötet Az Informatikai Biztonság Irányításának Vizsgálata (IBIV),
- 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR),
- 25/2. Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS).
- ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványok,
- ISO/IEC 27001:2005,
- ISO/IEC 27001:2013.
- a 185/2015. (VII. 13.) Korm. rendelet „a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól”