ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel


**Incidens-menedzsment, BCP, DRP integráció**

**A biztonság eseménykezelés, és illeszkedése a működésfolytonosság tervezéshez, és az informatikai szolgáltatásfolytonosság tervezéshez**

**Horváth Gergely Krisztián, CISA CISM**

Nemzeti Közszolgálati Egyetem

**Budapest, 2014**

# Tartalomjegyzék

# 1 Bevezetés

## 1.1 Háttér

A megfelelő információbiztonsági rendszer kialakítása és fenntartása egyik kulcsfontosságú tevékenysége a rendkívüli eseménykezelés tevékenység, mely a felkészülés és tervezés révén megelőző kontrollok megvalósításával, illetve a reagálási képesség megvalósításával helyesbítő kontrollok lehetővé tételével növeli a szervezet biztonságát.

Az információbiztonsági eseménykezelés kiemelten fontos vezetői felelőssége egy információbiztonsági felelősnek, mivel az eseményekre adott nem szakszerű reakciók adott esetben nem csak, hogy nem csökkentik a kockázatokat, de akár nagyságrendekkel növelhetik a hatásukat.

A tárgy oktatásának célja, hogy az elektronikus információs rendszer biztonságáért felelős személyek (IBV) legyenek tisztában a munkájuk során, az információbiztonsági események kezelésére való felkészülés, az események elhárítása, és a működés visszaállítása során felmerülő jogi – igazgatási – biztonsági – minőségi – vezetési alapokkal.

## 1.2 Jegyzet célja, felépítése

Jelen jegyzet a Nemzeti Közszolgálati Egyetem (NKE) Elektronikus Információbiztonsági Vezető (EIV) szakirányú továbbképzésen, az Információbiztonsági események kezelése nevű tárgy keretében elsajátítandó ismereteket foglalja össze. A képzés során az elektronikus információs rendszer biztonságáért felelős személyek magabiztos szakmai tudást szerezhetnek az információbiztonsági eseménykezelés nemzetközi szabványairól és bevált gyakorlatairól, és a hazai közigazgatás környezetére való alkalmazásáról.

Az IBV-k a tárgy tananyagának elsajátítását követően képesek lesznek elvégezni a biztonsági események felismerését, kockázatértékelését és osztályozását, és képesek lesznek irányítani a biztonsági események kezelésére felkészülés tevékenységeit, és az események elhárítását, illeszkedve a szervezet működésfolytonossági és informatikai szolgáltatásfolytonossági tevékenységeihez.

A biztonsági eseménykezelés irányításához kapcsolódó biztonságtudatos gondolkodásmód kialakításához a kapcsolódó alapelvek és alapismeretek megismerése

eredményeképpen a szervezet céljaihoz illeszkedő legmegfelelőbb eseménykezelési stratégia, megelőzési intézkedések, és cselekvési képesség kialakítására válik képessé az IBV.

A jegyzet felépítése a következő főbb fejezeteket követi:

- Definíciók és rövidítések (Glossary)
    - kulcsfogalmak és rövidítések, melyek ismerete elengedhetetlen a tananyag megértéséhez.
- Az információbiztonsági eseménykezelés (Incidensmenedzsment) módszerei (Incident management methods)
    - a szakterület nemzetközileg elterjedt bevált gyakorlatait foglalja össze a fejezet, amelyek elemei felhasználhatóak egy adott szervezet belső szabályozásának kialakításához.
- Az információbiztonsági eseménykezelés (incidensmenedzsment) folyamatai (Incident management process)
    - a tananyag bemutatja azokat a folyamatokat, amelyek a sikeres információbiztonsági eseménykezeléshez általában szükségesek, és amelyek végrehajtásának eredményeképpen a jogszabályi megfelelőség biztosítható,
- Az információbiztonsági események osztályozásának módszerei (Incident classification)
    - különféle osztályozási módszereket mutat be a fejezet, amelyek használatával az események priorizálása elvégezhető.
- Az információbiztonsági események cselekvési terve (Incident response plan)
    - Az események kezelésével kapcsolatos feladatvégzés dokumentálására szolgáló terv kidolgozását és alkalmazását foglalja össze a fejezet.
- Az információbiztonsági események nyomainak rögzítése (Incident forensics)
    - Bizonyítékok rögzítésének és értékelésének szükségessége, eljárásai ismerhető meg a fejezetből.
- Az információbiztonsági eseménykezelő szakemberek eszköztára (Incident management tools)
    - A tananyagban ismertetett tevékenységek elvégzését támogató szoftvereszközök ingyenes változataira néhány példa.

A tananyag ezen túlmenően további hivatkozásokat is biztosít külső információforrásokhoz: szabványokhoz, módszerekhez, és más kiadványokhoz. Helyenként statisztikák, grafikonok, táblázatok és folyamatábrák segítik a megértést.

A tananyag készítésénél szempont volt a lényeges információk összegyűjtése, és azok strukturált, és közérthető formában való tálalása lehetőleg kézzel fogható gyakorlati példákkal szemléltetve.

# 2 Definíciók és rövidítések

## 2.1 Definíciók

A tananyag definíciós részében elsősorban az elektronikus információs rendszerek működtetését végző szakemberek által leginkább ismert módszertan, az ITIL, és a hatályos jogszabályok vonatkozó fogalmait ismertetjük, és kísérletet teszünk ezen fogalmak egymáshoz való viszonyának bemutatására.

ITIL v3 módszertanban[1] használt meghatározás szerint, ha egy szolgáltatás nem az elvárt követelmények szerint működik most, vagy a jövőben az incidensnek tekintendő, pontosabban:

- *incidens (incident)*: Egy IT szolgáltatás be nem tervezett megszakadása, vagy az IT szolgáltatás minőségének csökkenése. Egy konfigurációelem meghibásodása, amely még nincs hatással semmilyen szolgáltatásra, szintén incidensnek tekintendő – például a tükrözést végző diszkek közül az egyik meghibásodása.

Az, hogy hogyan jutunk egy incidens deklarálásáig szintén fontos. Az ITIL szerint az incidensre vonatkozó információ eredhet automatizált észlelésből (detection), felhasználói hívásból (call), felhasználói bejelentés (user logging) beleértve a rendszergazda általi bejelentést is.

- *észlelés* (detection): A kiterjesztett incidenséletciklus egy szakaszs. Az észlelés hatására az incidens ismertté válik a szolgáltató számára. Az észlelés lehet automatikus, vagy lehet annak az eredménye, hogy egy felhasználó bejelenti az incidenst.
- A *bejelentés* (logging) fogalma nincs külön definiálva, azonban értik alatta a hívást, és a hibakezelő rendszerben való rögzítést is, és nem különböztetik meg a felhasználókat, így idetartozhat az IT üzemeltetők általi bejelentés is.
- *hívás (call)*: Telefonhívás a felhasználótól az ügyfélszolgálatra. Egy hívás incidens vagy szolgáltatáskérés rögzítését eredményezi.

[1] ITIL_2011_Hungarian_Glossary_v1.0.pdf (ITIL® magyar szakkifejezés-gyűjtemény v1.0, 2011. október 16. a v1.0-ös, 2011. július 29-i angol szakkifejezés-gyűjtemény alapján)

Azonban nem minden hiba (error), meghibásodás (failure), vagy (rendszer) esemény (event) lesz szükségszerűen incidens is. Például ha nem érinti az IT-szolgáltatások minőségét, és az üzemeltetők képesek megoldani, akkor nem incidens.

- *esemény (event)*: Olyan állapotváltozás, amelynek jelentősége van egy konfigurációs elem, vagy IT szolgáltatás menedzsmentjében. A kifejezést bármilyen IT-szolgáltatás, konfigurációs elem vagy megfigyelő eszköz által keltett riasztásra vagy értesítésre is használják. Az események általában az IT-üzemeltető személyzet beavatkozását igénylik, és gyakran vezetnek naplózandó incidensekre.
- *hiba (error / fault):* Tervezési hiányosság vagy helytelen működés, amely meghibásodást okoz egy vagy több konfigurációelemben vagy IT-szolgáltatásban. Emberi tévedés, vagy hibás folyamat, amely valamilyen konfigurációelemre, vagy IT-szolgáltatásra hatással van szintén hiba.
- *meghibásodás (failure):* Annak a képességnek az elvesztése, hogy előírás szerint működjön, vagy, hogy a kívánt eredmény előálljon. A kifejezést az IT-szolgáltatások, folyamatok, tevékenységek, konfigurációelemek s a többi esetében lehet használni. A meghibásodás gyakran incidenst okoz.

Az incidenskezelés folyamatában az elsődleges cél a szolgáltatás helyreállítása (restoration), amely történhet ismert hiba (known error) esetén megkerülő megoldás (workaround) alkalmazásával, vagy megoldással (resolution). Tehát nem a hibát javítjuk, hanem a felhasználó számára minél rövidebb időn belül a szolgáltatás igénybevételének képességét adjuk vissza.

- *ismert hiba (known error):* Olyan probléma, amelynek van dokumentált eredendő oka és megkerülő megoldása. Az ismert hibákat a problémamenedzsment hozza létre, és kezeli végig az élettörténetükön keresztül. Ismert hibákat a fejlesztők, vagy a szállítók is azonosíthatnak.
- *szolgáltatás helyreállítása (restoration of service):* Intézkedés egy IT-szolgáltatás javítás és visszaállítás utáni visszaadásáról a felhasználóknak. Ez az incidensmenedzsment fő célja.
- *workaround (megkerülő megoldás):* Olyan incidens, vagy probléma hatásának csökkentése vagy kiküszöbölése, amelyre teljes megoldás még nincs – például egy meghibásodott konfigurációelem újraindítása. A problémák megkerüléseit ismert hiba rekordokban dokumentálják. Azon incidensek megkerülő megoldásait,

amelyeknek nincs kapcsolódó problémarekordjuk, az incidensrekordban dokumentálják.

- *megoldás (resolution):* Intézkedés egy incidens, vagy probléma eredendő okának kijavítására, vagy egy megkerülő megoldás megvalósítására.
- *eredendő ok (root cause)*: Egy incidens, vagy probléma mögöttes vagy eredeti oka.

Az incidenskezelés kulcsfogalmainak ismertetése rátérünk, hogy a biztonság fogalma hogyan jelenik meg az incidens definíciójában közvetlenül, közvetve mégis szerepel benne a szolgáltatás minőség fogalma, amelynek része a biztonságos szolgáltatás képessége is. Továbbá az ITIL felhívja a figyelmet arra, hogy az incidensmenedzsment folyamatnak az információbiztonság-menedzsment folyamattal kapcsolódnia kell.

- *minőség (quality)*: Egy termék, szolgáltatás vagy folyamat képessége arra, hogy a tervezett értéket nyújtsa. Például egy hardverkomponenst jó minőségűnek kell tekinteni, ha az elvárások szerint működik, és nyújtja az elvárt megbízhatóságot. A folyamatminőség szintén megköveteli a képességet az eredményesség és hatékonyság megfigyelésére, és ha szükséges a javítására.
- információbiztonság-menedzsment (information security management): Ez a folyamat felelős azért, hogy egy szervezet eszközeinek, információinak, adatainak és IT-szolgáltatásainak bizalmassága, integritása, és rendelkezésre állása megfeleljen a megállapodott üzleti igényeknek. Az információbiztonság-menedzsment támogatja az üzlet-biztonságot, és szélesebb a hatóköre, mint az IT-szolgáltatóénak, mivel olyan dolgokra is kiterjed, mint a papírdokumentumok, az épületbe való bejutás, a telefonhívások stb. kezelése az egész szervezetben.
- *biztonságmenedzsment információs rendszere (security management information system)*: Azon segédeszközök, adatok és információk összessége, amelyet az információbiztonság-menedzsment támogatására használnak. A biztonságmenedzsment információs rendszere a része az információbiztonság menedzsmentrendszerének.

A magyar jogszabályok nem a szolgáltatás minőség, hanem a biztonság fogalmának elemei alapján - a 2013. L. törvényben - határozzák meg egy (informatikai) incidens, azaz itt *biztonsági esemény* fogalmát, a következőképpen:

- *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;

- *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;

Egy KIM rendelet (26/2013. (X. 21.) KIM rendelet) szinonimaként határozza meg a biztonsági események kezelése és az incidenskezelés fogalmakat (6. § *d)), amely egyébként jelen képzésre vonatkozik.*

Nem egységes egyébként a hazai joganyag az incidenskezelés fogalomhasználatában. Megjelenik még egy szélesebb körben - létfontosságú rendszerek és létesítmények szabályozásáról szóló 2012. évi CLXVI. tv – az esemény fogalma, a biztonságot veszélyeztető, vagy sértő esemény értelmében külön definíció nélkül („rendkívüli esemény", a „hálózatbiztonsággal kapcsolatos események"). Ugyanakkor több helyen megjelenik az incidens szó is, szintén definíció nélkül (pl. 83/2012. (IV. 21.) Korm. rendeletben „biztonsági incidens" szerepel, 309/2011. (XII. 23.) Korm. rendeletben „felhasználói incidens" szerepel, és a 301/2013. (VII. 29.) Korm. rendeletben „incidens-kezelési munkacsoport" szerepel). Korábban egyébként használta már a jogalkotó az incidens fogalmát biztonsági eseményként, különösen a légiközlekedés biztonságát szabályozó joganyagban (pl. 86/1997. (V. 28.) Korm. rendelet), továbbá megtalálható még banki területen (23/2013. (XI. 6.) MNB rendelet) és honvédelemben (16/2013. (VIII. 30.) HM rendelet).

A katasztrófa olyan hirtelen, nem tervezett, szerencsétlen esemény, amely jelentős kárt vagy veszteséget okoz. Ez akkor jelentkezik, ha a szervezet egy előre meghatározott időn belül nem képes a kritikus folyamatait működtetni. Katasztrófát felelős vezetőnek kell deklarálni.

Az üzletmenet-folytonosság menedzsment (Business Continuity Management - BCM) az a folyamat, melynek során egy szervezet felkészül a kritikus üzleti folyamatok megszakadása, vagy kiesése esetén a folyamatok visszaállítására. Cél a kritikus szolgáltatások

minimálisan szükséges szintjének fenntartása krízishelyzet esetén, és a folyamatok mielőbbi visszaállítása a normál üzemre.

Működésfolytonossági Terv (MFT) – (angolul: Business Continiuty Plan, BCP) azoknak az információknak és eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes váratlan káreseményekre hatékonyan reagálni és kritikus üzleti folyamatait egy elfogadható szinten fenntartani. MFT-nek nevezik azt a keretrendszert, amely átfogja a működésfolytonosság tervezési, megvalósítási és ellenőrzési fázisait. Ugyanakkor a normál működés megszakadása esetén alkalmazandó, az egyes kulcsfolyamatokhoz, szolgáltatásokhoz kapcsolódó konkrét tevékenységeket is MFT-nek hívják.

Katasztrófa-elhárítási Terv (angolul: Disaster Recovery Plan, DRP) azoknak az eljárásoknak a gyűjteménye, amelyek alapján egy szervezet képes a káresemények következtében kiesett szolgáltatásait a normál működési szintre visszaállítani. Működésfolytonossági terv készítése esetén a katasztrófa-elhárítási terv az előbbi szerves részeként jelenik meg.

Üzleti hatáselemzés – (angolul: Business Impact Analysis, BIA) eljárás, amely során a szervezet meghatározza a kritikus üzleti folyamatok megszakadásának következményeit és a normál működési állapotra való visszaállás elvárásait.

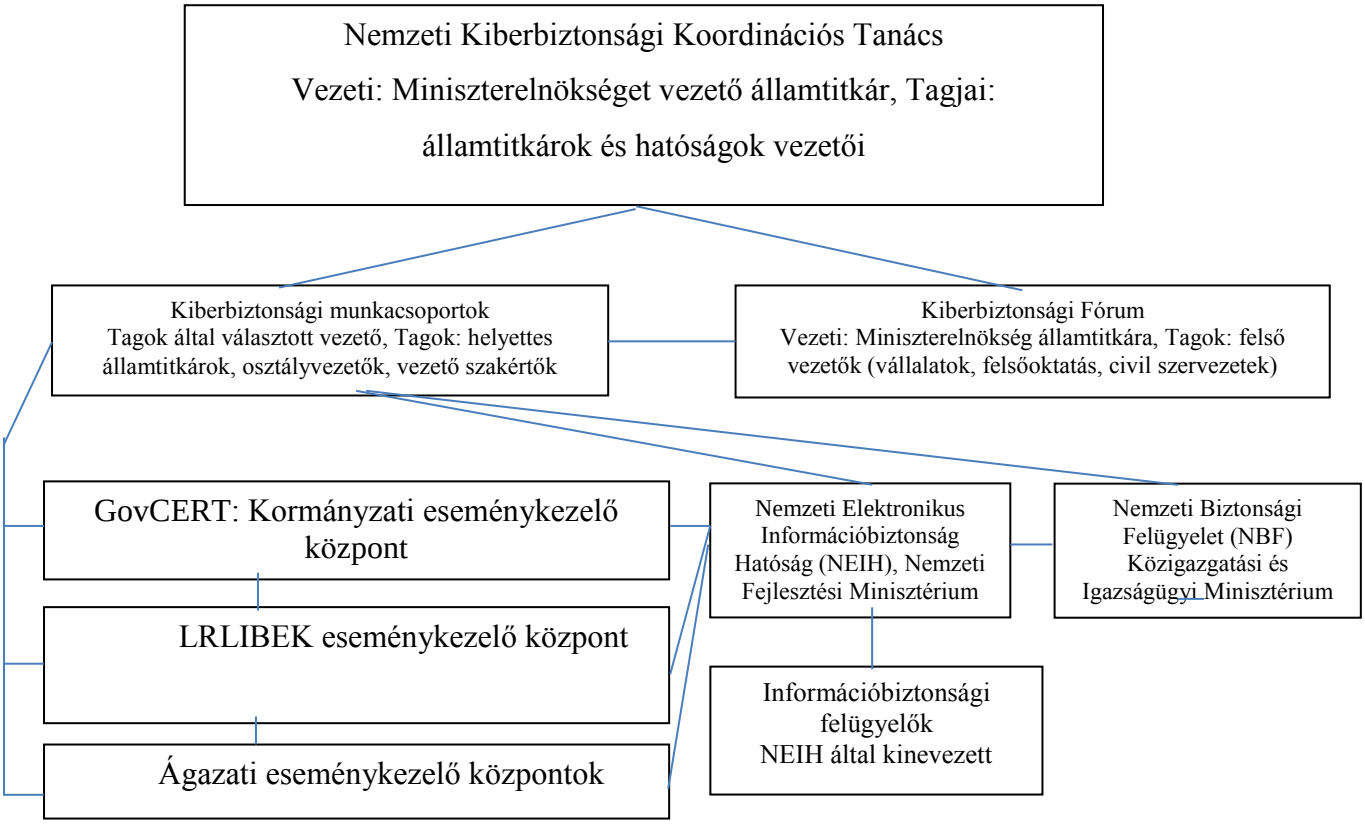
## 2.2 Rövidítések

A tananyagban a következő rövidítéseket használjuk:

- BCM – Működés-folytonosság menedzsment (Business Continuity Management)
- CI - Konfigurációs elem (Configuration Item)
- CISM - tanúsított információbiztonsági vezető cím (Certified information security manager), melyet az ISACA szakmai vizsga és a tanúsítási feltételek teljesítése esetén, folyamatos továbbképzés, a szakmai és etikai szabályok betartása mellett viselheti a tanúsított személy.
- CISSP – tanúsított informatikai biztonsági szakértő (Certified information systems security professional), az ISC2 szakmai szervezet tanúsítványa,
- DRP – Informatikai katasztrófa helyreállítási terv (disaster recovery plan)
- Ibtv – 2013. évi L törvény
- IBV – információbiztonsági vezető Az Ibtv szerinti személyek, akik az elektronikus információs rendszer biztonságáért felelősek.
- ISACA – Nemzetközi informatikai kontroll szakmai szervezet, a rövidítést nem oldják fel.
- ITSCM – Informatikai szolgáltatás-folytonosság menedzsment (IT service continuity management)
- NKE – Nemzeti Közszolgálati Egyetem
- NIST – National Institute of Standards and Technology, azaz az amerikai Nemzeti Szabvány- és Technológiaügyi Intézet
- SLA – szolgáltatási megállapodás (Service Level Agreement)
- SZEÜSZ – szabályozott elektronikus ügyintézési szolgáltatás

## 2.3 Szervezeti intézményrendszer

Az állami és önkormányzati elektronikus információbiztonsági törvény a kiberbiztonság koordinálását a Miniszterelnökség feladatává tette, melynek felelőse a Miniszterelnökséget vezető államtitkár.




**1. ábra** ***A kiberbiztonság intézményrendszere Magyarországon***

Szervezetek:

- Nemzeti Kiberbiztonsági Koordinációs Tanács, Kiberbiztonsági Fórum, Kiberbiztonsági munkacsoportok (URL: nincs) 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szabályozza a feladatait. A Tanács feladata a Magyarország Nemzeti Kiberbiztonsági Stratégiájában meghatározott cselekvési területeken a kormányzati tevékenység koordinációjának elősegítése és a végrehajtás figyelemmel kísérése. A Forum javaslatokat fogalmaz meg és véleményt formál, a Kiberbiztonsági Munkacsoportok döntés-előkészítő feladatot látnak el.

- Kormányzati eseménykezelő központ, GovCERT (URL: http://www.cert-hungary.hu/) az incidenskezelés optimalizálása, illetve az internetes hálózatbiztonsági incidensek időzóna függetlensége miatt nonstop (0/24 órás) ügyeleti rendszert működtet. Kiemelt szerepet játszik a nemzetgazdaság és az állami működőképesség szempontjából létfontosságú informatikai rendszerek védelmében, ezzel összefüggésben a nemzetközi szervezeteknél Magyarország képviseletében, és a hálózatbiztonsági tudatosításában egyaránt.
- Nemzeti Elektronikus Információbiztonság Hatóság, NEIH (URL: http://neih.gov.hu/), főbb feladatai az Ibtv. szerint: nyilvántartás vezetése a hozzá érkezett bejelentésekről, jogszabályban meghatározott követelmények teljesülésének ellenőrzése; az ellenőrzés során a feltárt vagy tudomására jutott biztonsági hiányosságok elhárításának elrendelése, és eredményességének ellenőrzése; a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálása, továbbá az információs társadalom biztonságtudatosságának elősegítésen és támogatása. Ezen túlmenően kapcsolatot tart az érintett kormányzati szervekkel, javaslatokat fogalmaz meg, és tájékoztatja a Kormányt a kibervédelem helyzetével kapcsolatban.
- Nemzeti Biztonsági Felügyelet, NBF (URL: http://nbf.hu/) az állami, önkormányzati és létfontosságú infrastruktúrák információs rendszerei esetén elősegíti, hogy az állampolgárok adatai, a nemzeti adatvagyon, az állami működésre vonatkozó információk megfelelő védelemben részesülhessenek a nem papír alapú adatkezelés esetén is.

Kapcsolódó szervezetek:

- Nemzeti Adatvédelem és Információszabadság Hatóság (URL: http://naih.hu/) feladata a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülésének ellenőrzése és elősegítése.
- Elektronikus Ügyintézési Felügyelet (URL: https://euf.kim.gov.hu/) biztosítja a 2011. évi CLXXIV törvény (Ket.) színvonalát, minőségét, és biztonságát, annak alkalmazása során. A Felügyelet működése nem csak az állami szolgáltatókra terjed ki, hanem a magánszektorra is, így teljes körűen képes biztosítani a szabályozott szolgáltatások (SZEÜSZ) egységességét, mely előremutató az interoperabilitás szempontjából is.

# 3 A biztonsági eseménykezelés bevált gyakorlatai

## 3.1 Biztonsági eseménykezelés bevált gyakorlatai

A jegyzet ismerteti a témakörhöz kapcsolódó lényegesebb módszereket, de részletesen nem mutatja be őket, mert meghaladja jelen tananyag kereteit, egyéni feladat a szakirodalom feldolgozása.

## 3.2 ITIL incidenskezelési folyamat és a biztonsági eseménykezelés

Az informatikai szolgáltatásokkal kapcsolatos bevált gyakorlatok gyűjteményét, az ITIL-t (IT Infrastructure Library – IT Infrastruktúra Könyvtár) a brit kormányzat közigazgatás területéről elindulva, nemzetközi IT szolgáltatóvállalatok által felkarolva vált irányadóvá világszerte, majd nemzetközi szabvánnyá. Magyarországon az MSZ ISO/IEC 20000 szabvány érhető el magyar nyelven, a nemzetközi módszertanból az ITIL v2011 a legfrissebb.

Az ITIL Szolgáltatástámogatás szakterület egyik fő folyamata az incidenskezelés, melyhez kapcsolódik az IT szolgáltatás-folytonosság, és az információbiztonság-menedzsment.

Az Ibtv biztonsági esemény fogalmától eltérően az ITIL incidens alatt az IT szolgáltatás minőségének csökkenését érti, amely nagyobb halmazt jelent. Ugyanakkor a módszertan jól használható az informatikai üzemeltetési területen, illesztve a kapcsolódó jogszabályi követelményeknek való megfelelés más módszereivel. Ehhez segítséget adnak interneten elérhető elemzések, mint például az „ITIL V3 and Information Security”[2], amelynek B függeléke az ITIL v3 és az ISO/IEC 27000 szabványcsalád elemei közötti kapcsolatot mutatja be.

## 3.3 Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) anyagai

Annak érdekében, hogy a lehető legnagyobb biztonságot garantálja a felhasználók számára, az Európai Unió (EU) létrehozta az ENISA-t, amely tanácsot ad a Bizottságnak és az EU-tagállamoknak, valamint koordinálja az általuk végrehajtott olyan intézkedéseket, amelyek hálózataik és információs rendszereik biztosítását szolgálják.

[2] http://www.axelos.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf

Éves incidenskezelési jelentést ad ki, amelyből az Unióra vonatkozó jellemző incidensek megismerhetőek. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

Az Eseménykezelő Központokban (CERT/CSIRT) a biztonsági eseménykezelés megvalósítását, illetve működtetését és fejlesztését segíti az ENISA Biztonsági eseménykezelési útmutatói. URL: https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide-in-hungarian/at_download/fullReport

URL: https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport

Példák is találhatóak gyakorlatok megvalósítására. URL: https://www.enisa.europa.eu/activities/cert/support/exercise

További az incidenskezelés különféle feladatait támogató szoftvereszközök ismertetése is elérhető az ENISA honlapjáról. URL: https://www.enisa.europa.eu/activities/cert/support/chiht

## 3.4 ISACA

Az ISACA egy független, nonprofit, nemzetközi szervezet, amely az információs rendszerekre vonatkozó iparági és nemzetközi tudás, és bevált gyakorlatok kifejlesztésében, és alkalmazásában működik közre. 80 országban több, mint 110.000 tagja van.

Az információbiztonsághoz és a biztonsági eseménykezeléshez kapcsolódóan több kiadvány jelent meg.

A „Cobit 5 for Information Security” egy átfogó keretrendszer az informatikai irányítási keretrendszerbe illeszkedően az információbiztonság holisztikus megvalósítására. (Pénzért hozzáférhető tartalom)

ISACA informatikai ellenőrzési szakemberek részére elkészítette a biztonsági-eseménykezelés vizsgálati programját, mely részletes kérdéseket és szempontokat tartalmaz egy szervezet biztonsági eseménykezelési tevékenységének a felméréséhez és értékeléséhez. (Pénzért hozzáférhető tartalom)

Az információbiztonsági rendkívüli eseménykezelés a CISM vizsga négy fő területeinek egyike, mely kimondja, hogy a szervezetet érő károk csökkentése érdekében tervezett módon kell az információbiztonsági eseményeket és következményeik helyreállítását kezelni. A vizsgára felkészítő CISM Review Manual (2013, 200.o.) szerinti információbiztonsági eseménykezelés a következőt jelenti: „annak a képessége, hogy

eredményesen kezeljünk a váratlan rendkívüli eseményeket azzal a céllal, hogy hatásukat minimalizáljuk, és fenntartsuk vagy helyreállítsuk a normál működést az elvárt határidőkön belül." A biztonsági eseményekre tett válaszintézkedéseket így határozza meg: „a biztonsági eseménykezelésnek olyan gyakorlati képessége, amely a biztonsági események azonosítását, kezelésükre való felkészülést és válaszintézkedések megtételét jelenti a bekövetkezésük okozta kár csökkentése és kontrolálása érdekében; amely jelenti a nyomok rögzítésének és kivizsgálásának képességét; és amely jelenti még a szolgáltatási megállapodásokban (SLA) rögzített normál működés fenntartását, visszaállítását és helyreállítását."

## 3.5 Nemzetbiztonsági Minisztérium, USA

Az USA Nemzetbiztonsági Minisztériuma az általa lényegesnek tartott, biztonsági eseménykezelésre vonatkozó szakmai ajánlásokat, és útmutatókat egy oldalon összegyűjtötte (2013). URL: https://buildsecurityin.us-cert.gov/articles/best-practices/incident-management/incident-management

## 3.6 NIST, USA

Az USA Nemzeti Szabvány és Technológiai Intézete széles körben ad ki információbiztonsággal kapcsolatos kiadványokat. Két anyaga szorosan kapcsolódik jelen tananyag hatóköréhez:

SP800-61 Rev.2.: Számítógépes biztonsági eseménykezelési útmutató, 2012

URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

SP 800-86: Biztonsági eseményekre tett válaszintézkedések során az igazságügyi szakértői módszerek integrálására útmutató, 2006

URL: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

## 3.7 ISO/IEC 27000 szabványcsalád

Az ISO/IEC 27001 szabványcsalád kidolgozása során is felmerült az igény az információbiztonsági eseménykezelésre vonatkozó tevékenység szabványosítására. Ennek eredményeként készült el az információbiztonsági irányítási rendszerbe illeszkedően az ISO/IEC 27035:2011 szabvány a biztonsági eseménykezelésről.

A szabvány mintegy 80 oldalban foglalja össze a biztonsági eseménykezelés nemzetközi szabvánnyá emelt gyakorlatait, kiegészítésképpen az ISO/IEC 27002-ben meghatározott kontrollokhoz.

URL: http://webstore.iec.ch/preview/info_isoiec27035%7Bed1.0%7Den.pdf (tartalomjegyzék)

## 3.8 KIB 25. ajánlássorozat - Magyar Informatikai Biztonsági Ajánlások

A Magyar Informatikai Biztonsági Ajánlás a Közigazgatási Informatikai Bizottság 25. számú ajánlássorozata, mely az Informatikai Tárcaközi Bizottság korábbi 8, 12 és 16 számú ajánlásait váltja ki. Az ajánlások a 2008-ban hatályos elektronikus közigazgatásra vonatkozó követelményrendszert követték (mely azóta többször lényegesen megváltozott) és nemzetközi bevált gyakorlatok honosítása során a magyar közszféra korlátait is figyelembe vették. Az ajánlások szabályzatok, eljárásrendek, és a kapcsolódó dokumentációk elkészítését teszik lehetővé, azonban figyelemmel kell lennünk arra, hogy azóta változtak a jogszabályok.

URL: http://www.ekk.gov.hu/hu/kib/ajanlasok

## 3.9 KIB 28. ajánlássorozat – eKözigazgatási keretrendszer

Az E-Közigazgatási Keretrendszer projekt eredményeként állt elő 2008-ban a KIB 28. számú ajánlása, mely az elektronikus közigazgatás fejlesztéséhez szükséges teljes eszköztárat tartalmazza. Azaz az informatikai biztonsági követelményeken túlmenően a funkcionális és a módszertani követelményeket egyaránt. Az eszköztár kidolgozása során kiemelt cél volt, hogy az önállóan megvalósuló szakágazati és önkormányzati rendszerek között az együttműködés (interoperabilitás) képessége biztosított legyen.

Egyik kötete az INCIDENSMENEDZSMENT AJÁNLÁS, jól alkalmazható a biztonsági eseménykezelés megvalósítása során is, noha alapvetően szolgáltatás menedzsment szemléletű, így ki kell egészíteni biztonsági vonatkozásokkal.

URL: http://www.ekk.gov.hu/hu/kib/ajanlasok

## 3.10 Cert.hu

Egy kilenc lépésből álló egy oldalas útmutató tettek közzé informatikai rendszerek működtetői részére: Incidens kezelés lépésről lépésre.

## 3.11 Brit kormányzati szabvány - Public Services Network projekt

A Brit Cabinet Office adott ki 2013-ban egy nyilvános kormányzati szabványt a brit közhálóra vonatkozó biztonsági eseménykezelés témájában: Common Standard for Protective Monitoring, Security Incident Management and Situation Awareness

Az anyag leírja a követendő folyamatot, és tartalmaz jelentés sablont, illetve válaszintézkedési terv sablont is.

URL:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/136009/PMSIMSA-Std-v1-0.pdf

## 3.12 OWASP

Az OWASP szoftverbiztonsággal foglalkozó nonprofit szervezet, mely az alkalmazás biztonságra vonatkozó útmutatókat tesz közzé, többek között a biztonság tesztelése, a programkód felülvizsgálat, vagy a biztonságos webfejlesztés területén. Folyamatban van egy projekt a biztonsági eseményre adandó válaszintézkedésekre vonatkozó útmutató elkészítésére.

URL: http://www.owasp.org/

## 3.13 SANS Intézet

A SANS Intézet számos útmutatót készít információbiztonsági témákban. A biztonsági eseménykezelés területén jól használható a KKV számára készített útmutató: An Incident Handling Process for Small and Medium Businesses.

URL: http://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791

# 4 Az információbiztonsági eseménykezelés folyamata

## 4.1 A biztonsági eseményekre tett válaszintézkedések célja

A biztonsági események kezelési képességének megteremtése és eredményes kezelésük az információbiztonsági vezetők kiemelt feladatai közé tartoznak. A biztonsági események kezelése (incidensmenedzsment) során az IBV elsődleges célja a szervezet működése szempontjából legfontosabb informatikai szolgáltatások működésének legalább a minimálisan szükséges szolgáltatási szinten való fenntartása ITIL módszertan szerint.

Tehát sikeres lehet az a biztonsági eseménykezelési tevékenység, amely során az informatikai szolgáltatások nyolcvan százaléka kiesik, és akár még a legfontosabb szolgáltatások minősége is romlik, akkor, ha minden, a szervezet vezetője által meghatározott szolgáltatás legalább a minimálisan elvárt szolgáltatási szinten, a visszaállítási időablakon belül működnek.

Ezt úgy oldják meg, hogy akár ideiglenes úgynevezett áthidaló megoldásokat léptetnek életbe a kritikus szolgáltatások minden körülmények közötti biztosítása érdekében. Adott esetben egy kiesett optikai hálózati kapcsolatot egy alternatív kapcsolattal, például mikrohullámú hálózaton pótolnak, ameddig nem sikerül helyreállítani.

Fontos kiemelni, hogy nem a biztonsági események kezelése során nem az összes szolgáltatás teljes helyreállítása a cél. Nem cél a felmerült hiba gyors javítása, adott esetben napokkal, vagy hetekkel később kerül sor a hiba teljes javításra.

A szervezetek céljaikat akkor képesek elérni, ha biztosított folyamatos működésük, vagy legalábbis a működést akadályozó, vagy megszakító rendkívüli helyzetekből való mielőbbi visszaállítás, majd helyreállítás. A biztonsági eseménykezelés, továbbá a folyamatos működés fenntartására vonatkozó (BCM, ITSCM) módszerek ehhez biztosítják a szükséges szervezési hátteret.

Ha egy ügyfélkapcsolat-tartást támogató önkormányzati szolgáltatást működtető szerver számítógép alaplapja a hónap első hetében meghibásodik, és kikapcsol, a szolgáltatást előre kidolgozott eljárások szerint, a tartalék eszközök és mentések felhasználásával 10 perc alatt átállítják egy tartalék szerverre, ami kisebb kapacitású, de teljes funkcionalitással pótolni tudja a kiesett szerver számítógépet. A kiesés ideje (10 perc) bőven benne van a vállalt 99,5 százalékos rendelkezésre állás időben, a kapacitás csökkenés csak a hónap végén várhatóan megemelkedő kérelem beadások idején okozna szolgáltatási szint megsértését, így ekkor a

szolgáltatónak van két hete megjavíttatni a hibás alaplapot, vagy pótolni a szervert egy hasonló kapacitású másik géppel.

Fontos kihangsúlyozni, hogy a tehát felhasználók által érzékelhető szolgáltatási szint visszaállítása az incidens-menedzsment folyamat célja, ami nem egyezik meg azzal az informatikai megközelítéssel, mely szerint az incidens-menedzsment folyamat célja a dolgok (például a konfigurációs elemek) működésének a visszaállítása. A fenti példából is látszik, hogy nem feltétlen az elromlott eszközt kellett mielőbb működésre bírni. (Hasonlóan a problémakezelés folyamat célja az incidensek kiváltó okainak megszűntetése, nem dolgok ismételt elromlásának megakadályozása.)

Az informatikai szolgáltatásmenedzsment bevált gyakorlatok szerinti incidensmenedzsment (rendkívüli események kezelése) tevékenység nem feltétlen vezet a biztonság szintjének növeléséhez. A szolgáltatás képességének minden áron való mielőbbi visszaállítása könnyen vezethet adatvesztéshez, kevésbé védett kiszolgálók ideiglenes használatához. Akkor járunk el felelősen, ha az üzleti igények és a kockázatok mérlegelése alapján hozzuk meg a döntésünket IBV-ként.

Az Ibtv. definíciójából kiindulva, mely szerint a biztonsági esemény kezelése alatt *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*et kell érteni, a biztonsági eseménykezelés az ITIL definíciójánál bővebb, a biztonsági események következményeinek (hatása) felszámolását célozza és hangsúlyos elem a jövőbeni előfordulás megakadályozása.

Az Ibtv. követelményeinek való megfelelés azonban nem ellentétes az ITIL elvárásaival, és szakmailag is akkor képzelhető el a biztonsági eseménykezelés folyamatának eredményes és hatékony megvalósítása, ha az illeszkedik az informatikai incidenskezelési folyamathoz, és a szakmai, és biztonsági követelményeket egyidejűleg teljesíti.

Összefoglalva azt mondhatjuk, hogy dokumentált módon szükséges a rendkívüli események kezelését megvalósítani, a következményük felszámolása során a szakmai és a biztonsági szempontokat egyaránt érvényesítve. Szintén fontos, hogy a biztonsági eseményeknél hangsúlyt kell helyezni az események nyomainak rögzítésére a felelősségek meghatározásához.

## 4.2 Az IBV biztonsági eseménykezelési képessége

Az ISACA CISM Review Manual (2013) anyagának készítői háromévente felmérik, és összefoglalják az IBV-k biztonsági eseménykezeléssel kapcsolatos szükséges szaktudását (tudás megállapítás), és végzendő tevékenységeit (feladatmegállapítás). Ezeknek az elsajátítása, illetve megvalósítási képességének megteremtésével válik az IBV képessé a biztonsági események kezelésére.

*Tudás megállapítások* (eredeti nyelven):

KS4.1 Knowledge of the components of an incident response plan

KS4.2 Knowledge of incident management concepts and practices

KS4.3 Knowledge of business continuity planning (BCP) and disaster recovery planning (DRP) and their relationship to the incident response plan

KS4.4 Knowledge of incident classification methods

KS4.5 Knowledge of damage containment methods

KS4.6 Knowledge of notification and escalation processes

KS4.7 Knowledge of the roles and responsibilities in identifying and managing information security incidents

KS4.8 Knowledge of the types and sources of tools and equipment required to adequately equip incident response teams

KS4.9 Knowledge of forensic requirements and capabilities for collecting, preserving and presenting evidence (for example, admissibility, quality and completeness of evidence, chain of custody)

KS4.10 Knowledge of internal and external incident reporting requirements and procedures

KS4.11 Knowledge of postincident review practices and investigative methods to identify root causes and determine corrective actions

KS4.12 Knowledge of techniques to quantify damages, costs and other business impacts arising from information security incidents

KS4.13 Knowledge of technologies and processes that detect, log and analyze information security events

KS4.14 Knowledge of internal and external resources available to investigate information security incidents

*Feladat megállapítások* (eredeti nyelven):

T4.1 Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate identification of and response to incidents.

T4.2 Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.

T4.3 Develop and implement processes to ensure the timely identification of information security incidents.

T4.4 Establish and maintain processes to investigate and document information security incidents to be able to respond appropriately and determine their causes while adhering to legal, regulatory and organizational requirements.

T4.5 Establish and maintain incident escalation and notification processes to ensure that the appropriate stakeholders are involved in incident response management.

T4.6 Organize, train and equip teams to effectively respond to information security incidents in a timely manner.

T4.7 Test and review the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.

T4.8 Establish and maintain communication plans and processes to manage communication with internal and external entities.

T4.9 Conduct postincident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.

T4.10 Establish and maintain integration among the incident response plan, disaster recovery plan and business continuity plan.

## 4.3 Felkészülés a biztonsági események kezelésére

A rendkívüli események *megelőzés*ét nem lehet elvégezni kizárólag szabályzatok és tervek kiadásával. Szintén kevés, ha csak az informatikai biztonsági és informatikai üzemeltetési szakembereket felkészítjük. A rendkívüli események kezelése a teljes szervezetet érintő feladat, mely során minden munkatársát fel kell készíteni, és a saját felelősségi körüket tudatosíttatni kell velük. Ilyen felkészítési feladat lehet például, hogy mi a teendője tűz-, csőtörés vagy vészjelzők megszólalása esetén, illetve hogy hogyan kell az alternatív feldolgozási folyamatokat elindítani.

Évente legalább egy alkalommal célszerű képzést tartani erről az alkalmazottaknak, illetve minden olyan esetben, amikor ezek a szabályzatok jelentős módon megváltoztak. A

képzésnek ki kell terjednie a jogszerű számítógép használat határaira, a Btk. vonatkozó paragrafusainak összefoglalására. Szintén fontos tájékoztatni a munkatársakat, hogy beosztásuktól függően mire terjed ki a felelősségünk. Ezek folyamatosan változnak, de a belső hálózatokon biztosítható egy naprakész tájékoztató a munkatársak számára.

A biztonsági eseménykezelésben részt vevő munkatársak részére pedig gyakrabban kell képzéseket szervezni, és mérni kell felkészültségüket. A felkészítés mellett rendszeresen gyakorlatoztatni is kell a munkatársakat, hogy a rendkívüli események bekövetkezésekor szükséges minden lépés rutinszerűen rögzüljön minden munkatársban. Ha szervezeten kívüli, azaz külsős felhasználói is vannak a szervezetnek, akkor őket is tájékoztatni kell arról, hogy mit tegyenek rendkívüli helyzetben a szervezet telephelyein. Ezek segítik őket a nem várt helyzetekben a megfelelő döntések meghozatalában, és az eredményes problémamegoldásban.

A biztonsági események megelőzésének másik fontos tevékenysége *a biztonsági eseménykezelési képesség kialakítása és fenntartása*.

Napjainkban az informatikai biztonsági események kezelése már sokkal több műszaki biztonsági kérdéseknél, holisztikusan, a kapcsolódó kockázatot átfogó kezelésével lehetünk képesek megelőzni, illetve elhárítani. Ennek az oka az, hogy már nem lehet egy hibás vagy kártevő tevékenységre utaló adatjellemzők alapján azonosítani a veszélyeket. Ezért már az egész rendszernek a védelmi mechanizmus részét kell képeznie, ugyanakkor rugalmasnak is kell lennie, hogy akár a rendszer tervezésekor nem is várt támadások ellen is képes legyen eredményesen védekezni biztosítva a védelmet a rendszer minden elemén keresztül.

## 4.4 Biztonsági események megelőzése: visszaélések megelőzése

Mindenki csak azzal él(het) vissza, amivel tud. De általában az emberek nem azon gondolkoznak naphosszat, hogy visszaéljenek valamivel. Ha mégis visszaélésen törik a fejüket, akkor többnyire azt mérlegelik, hogy megéri-e a várható haszon a tett következtében vállalt kockázatot… Megjegyezzük, hogy jellemző még az is, hogy az emberek túlértékelik a képességeiket, és biztosak benne, hogy az ő visszaélésükre nem derül fény, vagy ha napvilágra is kerül, akkor sem fogják feltárni, hogy ők követték el.

Milyen számítógépes visszaélésekre gondolhatunk? Az informatikai szakértő közreműködését is igénylő nyomozások esetében a bűncselekmény elkövetése során az informatikai eszköz a megvalósítás tárgyi környezete vagy segédeszköze. A milliárdos adócsalók számítógépen leveleznek, a pénzhamisítók digitalizálják a pénzjegyet, majd kinyomtatják, de még az orgazdák is használnak számítógépet: azon vezetik a

nyilvántartásukat. Ezekben az esetekben a bűnözők informatikai felkészültsége változó, de általában nincsenek tisztában azzal, hogy milyen nyomokat hagynak maguk után az informatikai rendszerekben. Itthon a visszaélések kisebb része az, amikor magasan képzett informatikai szakemberek, a szaktudásuk felhasználásával követnek el bűncselekményeket. Ide tartozik például a bankkártya hamisítás, vállalati adatok jogosulatlan lemásolása.

A számítógépes visszaélések megelőzésének első lépése, hogy a visszaélési lehetőségek vizsgálata során meghatározzuk, hogy melyek azok a kontroll hiányosságok, amelyek visszaélésre adnak lehetőséget, és ezek közül melyek kihasználása járhat a legnagyobb előnnyel egy csaló számára. Majd a rendelkezésre álló forrásokat figyelembe véve új kontrollokat, illetve kiegészítő kontrollokat léptetünk életbe annak érdekében, hogy növeljük a kontroll rendszer eredményességét. Ahol nem lehetséges, vagy nem gazdaságos új megelőző kontrollokat kialakítani ott kiegészítő monitoring kontrollokat alkalmazunk, melyek időben feltárják a visszaéléseket, hogy a hatásuk minél kisebb legyen.

A visszaélések megelőzését a Deloitte 2010-es belső ellenőrzési felmérése szerint leginkább az erre a célra rendelkezésre álló források szűkössége a legnagyobb probléma: pénz nélkül nem képesek megtartani, vagy felvenni tapasztalt szakembereket, és nem képesek korszerű speciális szoftvereszközöket alkalmazni, vagy a jelenlegi rendszereikhez csalás megelőzést segítő funkciókat kifejleszteni.

PÉLDA:

Egyik nagy kereskedelmi bankunk jelentős nagyságrendű veszteségeket szenvedett el az elmúlt 5 évben és ennek hatására fejlesztették a visszaélés megelőzés módszereit, növelték a visszaélés kivizsgáló csoport létszámát és különböző automatizmusokat építettek be az információs rendszerekbe, hogy a gyanús eseményeket feltárják.

Ha a kontroll rendszer felülvizsgálata során ezekre a kockázatokra megfelelő figyelmet szenteltek volna korábban, akkor milliárdos veszteségeket részben megelőzhették volna.

## 4.5 Eseménykezelési életciklus folyamatai

Az ITIL az eseménykezelési életciklust a következő lépésekre bontja fel.

- A szolgáltatás minőségi mutatóinak meghatározása rendkívüli helyzet esetére,
- a szolgáltatások rangsorolása (üzleti hatás alapján),
- a szolgáltatás elemei közötti függőségek azonosítása (nem kritikus szolgáltatás, de nélküle nem megy egy kritikus szolgáltatás akkor ez is kell),

- a rendkívüli események azonosítása / a rendkívüli eseményekre vonatkozó bejelentések fogadása,
- a rendkívüli események hatásának figyelemmel kísérése (amíg a hiba javítható anélkül, hogy sérülne a szolgáltatási szint, nem léptetik életbe a katasztrófa tervet),
- Katasztrófa terv alapján beindul az alternatív hibakezelés, a helyzet megoldásának felelőssége általában egy másik vezetőhöz kerül (eszkaláció), aki irányítja az együttműködést a szolgáltatást biztosító szervezetekkel, szakértőkkel és párhuzamosan az ügyfelekkel és más érintettekkel, esetleg felügyeleti szervekkel / hatóságokkal.
- folyamatosan rögzítik a hibára vonatkozó információkat, és a hibakezelési tevékenységeket a hibakezelő rendszerben.
- Párhuzamosan zajlik az érintettek tájékoztatása, lehetőség szerint előre kidolgozott kommunikációs tervek, sablonok felhasználásával.
- A szolgáltatási szint visszaállításával és a visszaállítás dokumentálásával lezárul a rendkívüli eseménykezelési folyamat.
- Amennyiben nem történt meg a teljes helyreállítás beindul a problémakezelési folyamat.
- A lezárást követően kerülhet sor az ex-post jellegű, utólagos vizsgálatra, amely a tanulságok levonására szolgál.

## 4.6 Eseménykezelés és működésfolytonosság menedzsment integráció

Ha egy szervezet hosszabb vagy rövidebb ideig nem tudja feldolgozni, előhívni vagy megvédeni elektronikusan kezelt információit, miközben működési folyamataiban jelentős mértékben alkalmaz elektronikus rendszereket, akkor a szervezeti feladatok ellátásában problémák léphetnek fel. A problémák mértéke az adott szervezet feladataitól és folyamataik automatizáltságának mértékétől függően eltérőek lehetnek.

Amennyiben a szervezet tolerálni képes az informatikai szolgáltatások hiányát akár több napig, akkor az informatikai szolgáltatásfolytonosságra kisebb hangsúlyt lehet helyezni. Ha az adott szervezet valamely tevékenységéhez az informatikai támogatás elengedhetetlen, akkor folyamatosan biztosítani kell a szolgáltatást, így a súlyosabb biztonsági események kezelésére a megfelelő mentési rendszer alkalmazásán túlmenően, akár alternatív működési helyet is ki kell kialakítani. Erre a következő fejezet tér ki.

A működésfolytonosságot eredményesen és gazdaságosan biztosító megoldások akár működési folyamatok, telephelyek, érintett munkatársak vagy más szempont szerint is lényegesen különbözőek lehetnek.

Például, ha egy Citrix szerver meghibásodik, az számos felhasználói csoportot, és működési folyamatot érint általában. Ezek közül egyesek tudják folytatni a munkát a saját Windows rendszerükből közvetlenül, megkerülve a Citrix-et. Mások számára alternatív folyamatokat kell életbe léptetni. De olyanok is lehetnek, amelyek egyáltalán nem működtethetőek ilyen esetben. A szakterületek vezetői által meghatározott prioritások, és a műszaki lehetőségek alapján határozható meg a megfelelő megoldás.

A szükséges működésfolytonossági kontrollok megvalósításához az alábbi lényeges feladatokat kell végrehajtani:

1. Működésfolytonosság-irányítási rendszer kialakítása és szabályzatba foglalása.
2. A lényeges és érzékeny informatikai folyamatok értékelése, valamint az ezeket támogató erőforrások azonosítása.
3. Intézkedések foganatosítása a potenciális károk és üzemszünetek minimalizálására.
4. Átfogó működésfolytonossági tervek kidolgozása, és oktatása.
5. A működésfolytonossági terv rendszeres tesztelése és aktualizálása.
6. A működésfolytonossági tervek életbe léptetése

A működésfolytonossági tervek kialakításakor a szervezetnek fel kell mérni a kritikus üzleti folyamatokat, azok üzleti és informatikai területeinek kapcsolatait, a kiszolgáló informatikai erőforrásokat. A folyamat végén pedig ki kell alakítani az úgynevezett helyettesítő folyamatokat, amelyek a gyakorlatban is alkalmazhatóak. A tervek minőségének és használhatóságuknak a mérése általában azok megvalósíthatóságával tesztelhetőek. Ez utóbbi megállapítás igaz a működésfolytonossági (BCP) és katasztrófa (DRP) tervekre is. Egy tervnél tehát az a leglényegesebb, hogy az mennyire használható, mennyire naprakész és mennyire ismert a felhasználók körében

Ezekkel párhuzamosan létre kell, hozni a BCM szervezetet és keretrendszerét, amely koordinációs szerepet tölt be a korábban meghatározott helyettesítő folyamatok menedzselésében.

A kritikus folyamatok azonosításával és osztályozásával összhangban meg kell határozni, hogy a bekövetkezett üzemzavar vagy katasztrófa esetén milyenek legyen a folyamatok visszaállításának prioritásai. Egyértelműen meg kell határozni a visszaállítási feladatok pontos sorrendjét, a feladatok felelős végrehajtóit, valamint a végrehajtáshoz szükséges eszközöket illetve minden egyéb erőforrást.

A fenti felmérési folyamat alkotja a működésfolytonossági alapját, illetve biztosítja, hogy egy rendkívüli, vagy katasztrófa helyzetben is a lehető leghatékonyabban használják fel

a rendelkezésre álló informatikai erőforrásokat. A prioritások megállapításába szintén be kell vonni mind a felhasználókat, mind az informatikai vezetést.

Megkülönböztetjük a BCM-ben a visszaállítást (resumption), amely legalább a szükséges vészhelyzeti minimális szolgáltatási szint biztosítását jelenti, a helyreállítástól (recovery), amely a teljes normál üzemi szolgáltatási szintet jelenti.

A működés folyamatossága kritikus kérdés – szervezet mérettől és iparágtól függetlenül. A szigorú jogszabályok, az éles verseny, valamint az ügyfelek és tulajdonosok elvárásai is ez irányba mutatnak.

Az üzletfolytonossági terv (BCP) készítése és karbantartása komplex feladat, gyakran jelentős külső erőforrást vesz igénybe és talán sosem lesz rá szükség. De amikor baj történik, és nincs kéznél használható BCP, az az igazi katasztrófa.

Az üzletmenet-folytonosság menedzsment sikertényezői a következők:

- Naprakész BCP tervek
- Az erőforrások naprakész listája a visszaállításhoz
- A szükséges vállalkozók listája, naprakész elérhetőségekkel
- Alapos tesztelés
- Az alternatív helyszíni működés szabályainak meghatározása

Elsődleges telephelyre való visszatérés eljárásainak meghatározása.

## 4.7 Eseménykezelés és informatikai szolgáltatás-folytonosság integráció

Az informatikai szolgáltatás folytonosság (ITIL: ITSCM), vagy informatikai katasztrófa-tervezés (DRP) az informatikai üzemeltetési tevékenység egy kritikus eleme. Az informatikai rendszerek tervezése során törekszenek a várható emberi, illetve műszaki hibák és események hatásának csökkentésére, a rendszerbe például tartalék kapacitást és párhuzamos feldolgozási képességet (redundanciát) építenek be, illetve az adatok rendszeres mentésével biztosítják a minél kisebb adatvesztést.

A szervezet informatikai szakterületének a működésfolytonossági tervhez illeszkedően kell kidolgoznia az informatikai szolgáltatás-folyamatossági keretrendszert, amely meghatározza a feladatokat és felelősségi köröket, az alkalmazandó kockázat alapú megközelítési módszert, valamint az informatikai szolgáltatás-folyamatossági terv dokumentálására és jóváhagyására vonatkozó szabályokat és struktúrákat. Nem csak egyszer kell a terveket kidolgozni, hanem megfelelő eljárásokat kell kidolgozni a változtatások terveken való átvezetésére annak érdekében, hogy naprakész maradjon és igazodjon a szakmai és informatikai elvárásokhoz.

A Működésfolytonossági Terv (DRP) célja, hogy pontosan meghatározza az informatika működésének folyamatosságát biztosító elveket, feladatokat és meghatározza a tervezéshez, a végrehajtáshoz és az ellenőrzéshez kapcsolódó felelősségi köröket és kötelességeket. A Működésfolytonossági Terv megadja a keretét annak a tevékenységnek, amely során az informatikai szolgáltatások rendelkezésre állását folyamatosan javítani lehet, és tartalmazza a jelenleg érvényes konkrét intézkedéseket.

A Működésfolytonossági Terv gazdája az informatikai biztonsági felelős. Feladata a Terv elkészítése, tárolása és elérhetővé tétele, a Terv átvizsgálásának kezdeményezése és a szükséges módosítások átvezetése. E feladata során szorosan együttműködik az informatikai és üzemeltetési főosztályvezetővel. A Működésfolytonossági Tervet évente, illetve lényeges változások bekövetkezésekor át kell vizsgálni annak biztosítására, hogy továbbra is alkalmas, helytálló és hatékony maradjon.

A rendszerek visszaállításának részletes leírását biztosító úgynevezett DRP tervek segítik a visszaállítást. A DRP, vagy informatikai katasztrófa tervek lépésről lépésre tartalmazzák azokat a tevékenységeket, amelyeket elvégezve egy informatikai szolgáltatás újraindítható az éles vagy a tartalék üzemi környezetben. A terveket tesztelni, és oktatni szükséges, és minden az érintett rendszerben való változtatást követően felül kell vizsgálni. Az informatikai szolgáltatás folytonosság a DRP terveken túlmenően azok kialakításához, karbantartásához és működtetés szükséges folyamatokat, és tevékenységeket határozza meg.

PÉLDA

IT Szolgáltatás-folytonossági politika (alapelvek)

1.1. A Szervezet informatikai osztálya kiemelten fontosnak tartja, hogy magas színvonalon folyamatosan ki tudja szolgáltatni az informatikai szolgáltatásokat saját szervezete, ügyfelei és partnerei részére. Ennek biztosítására IT Szolgáltatás-folytonossági Tervet készít és működtet, amellyel megvalósítja a következő célokat:

1.2. Folyamatos IT szolgáltatás biztosítása a nem várt rendkívüli események bekövetkezése esetén is.

1.3. A folyamatos IT szolgáltatás megszakadása esetén (például súlyos biztonsági esemény következtében) az elfogadott visszaállítási időn belül történő visszaállás a normál működésre.

1.4. Az IT szolgáltatás-folytonossági Terv kockázatfelmérésre és hatáselemzésre épül, amely meghatározza a működés és az ügyfelek kiszolgálása szempontjából létfontosságú működési folyamatokat, valamint a támogató erőforrásokat. A támogató

erőforrások működési zavarainak kezelésére is tervek készülnek, amelyek biztosítják a szolgáltatások rendelkezésre állását.

1.5 A rendkívüli események bekövetkezése esetére a feladatok és felelősségek előre meghatározottak.

1.6 Az IT-szolgáltatásfolytonossági Terv karbantartása rendszeresen végzett tevékenyég.

## 4.8 Biztonsági események kommunikációja

Jelentős kárt okozhat egy szervezet számára a bekövetkezett rendkívüli esemény közvetlen hatásán túlmenően, ha a szervezet vezetése, illetve a szervezet szolgáltatásainak biztosításában érintett felek nem készültek fel a krízishelyzetben való belső és külső kommunikációra.

Egyrészt a krízishelyzet elhárítása során az elhárítást végző embereknek el kell tudniuk időben érni egymást, és pontos információkat kell eljuttatniuk egymásnak. Ehhez ismerniük kell egymás nevét, szerepét, és elérhetőségét, és rendelkezniük kell alternatív kommunikációs eszközökkel, amennyiben a mobiltelefon rendszer nem elérhető. Indokolt lehet például CB rádió, vagy műholdas telefon biztosítása a rendkívüli események elhárításában részt vevő vezetőknek.

Másrészt a hatóságok, az állam és a média megfelelő, szakszerű tájékoztatása emberi életeket menthet meg, illetve megelőzheti későbbi kártérítési pereket. A külső felekkel való kommunikációra fel kell készíteni a szervezet minden tagját (ki, milyen témában nyilatkozhat) és különösen az elhárításban részt vevő vezetőket, és kommunikációs szakembereket. Sokat segít a kommunikációs eljárások szabályozása, minta sajtóközlemények előzetes kialakítása.

PÉLDA:

A kolontári iszapkatasztrófa vizsgálata feltárta, hogy a tározó sérüléséről a MAL ügyeletes vezetője elmulasztotta értesíteni a hatóságokat közel egy órán keresztül, ami jelentős anyagi és emberi élet és egészségbeli veszteséggel járt.

Jelenleg az eset kapcsán büntetőügy van folyamatban és ez a vezető a vádlottak padján ül. Védekezésében azt adta elő, hogy úgy gondolta a társaság első számú vezetője értesíti a hatóságokat.

# 5 Az információbiztonsági események osztályozásának módszerei

## 5.1 Biztonsági események forrása

Az informatikai veszélyforrások csoportosítása (megegyeztethetőek a Cobit-ban használt erőforrás kategóriákkal):

- infrastruktúra
- alkalmazások
- adatok
- emberek
- egyéb.

A kockázatok bekövetkezését a biztonság fő tényezői valamelyikének, vagy mindegyikének sérülése jelenti, például:

- ha sérül a bizalmasság - az információ nyilvánosságra kerülhet,
- ha sérül a sértetlenség – az információt kitörölhetik, módosíthatják,
- ha sérül a rendelkezésre állás – az információ esetleg nem elérhető, amikor szükséges.

A veszélyforrások típusai és hatása az iparágtól, a szervezet típusától és méretétől, a földrajzi elhelyezkedéstől, a kultúrától, és más jellemző tényezőktől függően jelentősen eltérhetnek. Egy lehetséges csoportosításuk:

- infrastruktúrából eredő fenyegetések: az infrastruktúra valamely elemének hibájából fakadó. Fontos megjegyezni, hogy egy hálózati útválasztó, vagy akár egy hálózati nyomtató is egy vagy több számítógépet tartalmaz akár saját háttértárral.
    - üzleti folyamatok megszakadása,
- logikai hozzáférési fenyegetések: jogosulatlan használat, nyilvánosságra hozás, vagy módosítás. Például:
    - minősített adat / üzleti titok sérülése (például információ elküldése elektronikus levélben titkosítás nélkül),
    - felhasználó bizalmának elvesztése,
- külső környezetből fakadó fenyegetések: extrém környezeti hatások
    - árvíz / belvíz elönti az alagsorban levő géptermet.
- humán fenyegetések: emberi hiba, vagy tevékenység hatása,
    - gyenge jelszavat használ a rendszergazda, ezért könnyen feltörik a szervert.

- fizikai tényezők: az ingatlan emberi tevékenység, és környezeti tényezők elleni védelme nem megfelelő,
    - eszközök eltulajdoníthatóak az épületből.

## 5.2 Biztonsági események azonosítása

A biztonsági események azonosítása több információforrásból történhet. Amennyiben az eseménynek emberek által tapasztalható hatása van, akkor ezt, az általában negatív hatást (szolgáltatás degradáció) felismerve *bejelentést* tesznek az ügyfélszolgálaton, illetve a szolgáltatásért felelős szervezeti egységnek, amelyek rögzítik a hívást.

Az elektronikus információszolgáltatásokat működtető szervezetek / szervezeti egységek esetében elterjedt gyakorlat a szolgáltatások kulcsjellemzőinek felügyeleti rendszerben való figyelemmel kísérése. A felügyeleti rendszerek képesek észlelni, és az előre meghatározott módon automatikus *hibaeseménnyel* értesíteni a szolgáltatás minőségének romlásáról a szolgáltatás működtetőjét, illetve más megadott értesítendő felet. Ezek az értesítések becsatornázhatóak hibajegy-kezelő rendszerbe, így biztosítható, hogy automatikusan felelőshöz rendelve kivizsgálandó feladatként jelenik meg egy rendkívüli esemény.

Amennyiben számottevő észlelhető hatással nem jár egy biztonsági esemény, és a felügyeleti rendszerekben beállított ellenőrzések során sem kerül feltárásra, akkor gyakran közvetett módon merül fel a gyanúja, hogy biztonsági esemény történt: például adatok szivárognak ki, amelyet jogosulatlanul használnak fel. Ilyenkor a *naplóesemények felülvizsgálatával* tárható fel, hogy van-e nyoma valamilyen rendellenességnek, vagy jogosulatlan rendszerműveletnek.

## 5.3 Biztonsági események osztályozásának módszerei

A rögzített eseményeket osztályozni szükséges az adott szervezet által meghatározott jellemzők szerint. Itt derül ki például, hogy biztonság eseménynek tekintendő-e.

Több féle osztályozása ismert a biztonsági eseményeknek: például az eseményeket kiváltó ok, az események által érintett erőforrás szerint.

A kiváltó okok alapján véletlen események, illetve szándékos károkozás eredményei.

Az események által érintett erőforrás alapján: ember, informatikai erőforrás, létesítmények, adatok.

## 5.4 Biztonsági események súlyossági szintjei

A következő lépés a biztonsági események priorizálása, amikor az események egymáshoz való fontosságát, illetve az esemény súlyosságát meghatározzák az érintett rendszerek jellege és száma, illetve az érintett felhasználók jellege és száma alapján.

| Csoport | Súlyosság | Példák |
|---|---|---|
| VÖRÖS | nagyon súlyos | DDoS, adathalászat |
| SÁRGA | súlyos | Trojai, jogosulatlan adatmódosítás |
| NARANCS | normál | Spam, szerzői jogsértés |

**2. ábra *ENISA egyszerűsített priorizálási táblázat súlyosság szerint***

| Csoport | Közigazgatási ügyfél | SLA-s ügyfél | Egyebek |
|---|---|---|---|
| VÖRÖS | 1 | 1 | 2 |
| SÁRGA | 2 | 1 | 3 |
| NARANCS | 3 | 2 | 3 |

**3. ábra *ENISA egyszerűsített priorizálási táblázat érintettek szerint***

Az informatikai szolgáltatásmenedzsment módszertanok megkülönböztetik a rendkívüli eseményeket a hatásuk mértékétől függően. Általában a rendkívüli esemény: csekély hatás (normál eljárásrend) – jelentős hatás (vészhelyzet) – kritikus hatás (katasztrófa helyzet). Nem kizárólag a szolgáltatásműködésre gyakorolt hatás alapján minősül egy esemény biztonsági eseménynek így ez egy másfajta kategorizálást jelent.

Hazai módszertanok is foglalkoznak a biztonsági események súlyosságának meghatározásával. A következmények alapján történő osztályozást tartalmazza a KIB25 ajánlás.

# 6 Az információbiztonsági események cselekvési terve

## 6.1 Eseménykezelő csoport (Incident response team) és kiemelt szerepkörök

Szükséges a következő szerepkörök kijelölése és megvalósítása (Ibtv és rendeletei szerint) a jogszabály által előírt feladatok végrehajtásához:

- Elektronikus információs rendszer biztonságért felelő személy (feladatait az Ibtv. 13. § tartalmazza)
- működtetésért felelős személy
- adatkezelésért felelős személy
- (Kirendelés esetén az Információbiztonsági felügyelő)
- Az elektronikus információs rendszer felett felügyeletet gyakorló személy (77/2013. Nfm. rendelet)
- A rendszert szállító, fejlesztő és karbantartó személyek, valamint ezek tekintetében illetékes kapcsolattartó személyek
- az egyes elemek adminisztrálásáért felelős személyek
- (fizikai) biztonsági személyek
- karbantartó személyek
- privilegizált fiókkal rendelkező személyek
- az információbiztonsággal összefüggő egyéb szerepkörök

Javasolt a következő szerepkörök megvalósítása, szervezeten belül, illetve külső erőforrásból (KIB 28 alapján):

„Incidensmenedzser feladatai:

a) az incidensmenedzsment folyamatának kidolgozása,

b) az incidensek kezelését végző munkatársak (elsődleges és másodszintű támogatás) munkájának megszervezése és irányítása,

c) a jelentős incidensek kezelése,

d) az incidensmenedzsment hatékonyságának és eredményességének elősegítése,

e) információk szolgáltatása a menedzsment részére.

Elsődleges támogatás: Az elsődleges támogatást az ügyfelek részére az IT ügyfélszolgálat munkatársai adják. Ahogy maga az ügyfélszolgálat, így az elsődleges támogatás megvalósítása is kötelező a központi rendszerhez csatlakozó és elektronikus

ügyintézést nyújtó szervezeteknek. Az ügyfélszolgálat által ellátott feladatokat az IT ügyfélszolgálatról szóló rész taglalja.

Másodszintű támogatás: Másodszintű támogatás nyújtása javasolt azon elektronikus közigazgatási szolgáltatások esetében, ahol az incidensek magas száma, a szolgáltatás bonyolultsága vagy egyéb okok miatt az ügyfélszolgálat nem tudja hatékonyan kezelni az ügyfelek igényeit.

A másodszintű támogatást nyújtó munkatársak nagyobb, de még mindig általános technikai tudással rendelkeznek, és nem állnak közvetlenül kapcsolatban az ügyfelekkel. Feladatuk azon incidensek megoldása, amit az ügyfélszolgálat munkatársai már nem tudnak megoldani, de még nem szükséges hozzájuk a harmadszintű támogatás speciális szaktudása.

Harmadszintű támogatás: A harmadszintű támogatás megvalósítása többek között a következőket foglalja magában:

a) hálózati támogatás,
b) szerver támogatás,
c) adatbázis támogatás,
d) desktop támogatás,
e) alkalmazásmenedzsment,
f) hardverek karbantartása.

Összességében, a szükséges képességeket biztosító, felhatalmazott biztonsági eseménykezelő csapat lehet képes az elvárásoknak megfelelően végrehajtani a válaszintézkedéseket.

## 6.2 Biztonsági események válaszintézkedései

A válaszintézkedés egy biztonsági esemény azonosítását követően megtett intézkedések sorozata. Az ENISA szerint a válaszintézkedéseket úgynevezett Válaszintézkedési Tervben (response plan) kell meghatározni, legalább a következők szerint:

- Az eseménykezelő csoport felépítése, tagjai, felelősségi körük,
- Az eseménykezelő csoport gyülekezési helye, döntéshozatali folyamata,
- Létesítmény kiürítési eljárástrend, vagy óvóhely kialakítása a telephelyen eljárásrend,
- Evakuált munkatársak biztonságos telephelyre juttatása eljárásrend,
- Kapcsolattartás a vészhelyzeti szolgáltatokkal eljárásrend,

- Közvetlenül a biztonsági esemény bekövetkezését követően a helyzet stabilizálására vonatkozó eljárásrend,
- Tájékoztatás a biztonsági esemény által érintett emberek felé eljárásrend,
- Elsősegély, munkavédelmi, és evakuálást segítő csoport mozgósítása eljárásrend,
- A telephelyen, vagy közvetlen közelükben levők létszámának megállapítására eljárásrend,
- Biztonságos telephely megtalálása és bejutáshoz szükséges részletek eljárásrend,
- Eseménykezelő Helyiség helyzete és bejutáshoz szükséges részletek eljárásrend,
- Hatóságokkal és szolgálatokkal való kapcsolattartás eljárásrend,
- Személyzet, az információ és a fizikai létesítmények védelme eljárásrend,
- Helyzetértékelési eljárásrend

A tárgy gyakorlati óráján kerül részletes bemutatásra a válaszintézkedések köre, illetve a tervek típusai.

## 6.3 Biztonsági események bejelentése az eseménykezelő központnak

Az IBV-t egyes jogszabályok (pl. 2013. L. tv.) kötelezik arra, hogy a jogszabály hatálya alá tartozó bármely felügyelete alá tartozó rendszert érintő biztonsági eseményről nyilvántartást kell vezetnie, és tájékoztatni köteles a jogszabályban meghatározott szervett.

A 2013. L. tv szerint az IBV alapesetben a NEIH hatóságot és a Kormányzati eseménykezelő központot (GovCert, Nemzetbiztonsági Szakszolgálat) tájékoztatja a biztonsági eseményről a vonatkozó összes információ megadásával. A bejelentések megküldésére elektronikus levélben, illetve és elektronikus ÁNYK űrlapon van lehetőség. Más ágazatokban ágazati eseménykezelő központ működhet, akkor oda kell a bejelentést megtenni. Például a honvédségi, rendvédelmi, diplomáciai szervek, NAV, Információs Hivatal és NMHH.

A biztonsági események nyilvántartásának az esemény kapcsán tett intézkedéseket, és azok eredményét is tartalmazni kell.

Nem kell bejelenteni a hatóság felé azokat a biztonsági eseményeket, amelyeket az érintett szervezet el tudott hárítani, és amelyek kárt vagy működésbeli kiesést nem okoztak.

## 6.4 Kormányzati Eseménykezelő Központ tevékenysége

A Kormányzati Eseménykezelő Központ a bejelentett biztonsági eseményeket haladéktalanul megvizsgálja, és intézkedéseket hoz és tájékoztatja az illetékes más hatóságokat.

A szakhatósági feladatokat a Nemzeti Biztonsági Felügyelet végzi, így például a biztonsági események adatainak műszaki vizsgálatát elvégzik, és ez alapján javaslatot tesznek a biztonsági esemény által okozott kár elhárítására.

# 7 Az információbiztonsági események nyomainak rögzítése

## 7.1 Biztonsági események figyelemmel kísérése

A hálózati forgalom, virtualizációs környezetek, operációs rendszerek, alkalmazások, adatbázisok, és más elektronikus eszközök működésére és használatára vonatkozó információ segíthet események rekonstruálásban, és ezáltal hatásuk csökkentésében és a felelősök számonkérésében.

Számos módszer létezik az elektronikus információs rendszerek működésének figyelésére. Általánosan elterjedt a rendszerek működésének és a felhasználók által végzett műveletek naplózása helyi vagy központi naplógyűjtéssel (például: syslog-ng), majd ezen naplóesemények meghatározott szempontok szerinti szűrése, korrelálása és jelentések készítése. Használatos továbbá a felügyeleti eszközökkel való valós idejű tevékenységfelügyelet megvalósítása (például: NAGIOS, Microsoft Network Monitor).

Vállalatok esetén különösen fokozottan védendő adatok kezelése esetén egyre inkább foglalkoznak a kiemelt (*privilegizált) felhasználók tevékenységének naplózásá*val, illetve az *adatszivárgás megelőzésével*. Adatszivárgás megelőzésére DLP (data loss/leak prevention) szoftverrendszereket alkalmaznak, melyek minden lehetséges adatszivárgási ponton figyelik a felhasználók tevékenységét, és a beállított szabályok szerint korlátozzák, illetve kísérik figyelemmel a tevékenységeket.

Paradigmaváltás következett be az elmúlt években a számítógéppel támogatott ellenőrzés területén. Komplex ellenőrzések valós idejű folyamatos végrehajtását lehetővé tevő megoldásokkal elérte a szakma azt, hogy alacsony fajlagos költség mellett szinte a teljes bizonyosságot el lehet érni. Azonban a fajlagosan alacsony költség még mindig jelentős beruházást jelent egy közigazgatási szervezet részére, így széles körben nem terjedhetett még el. A folyamatos kontroll monitoringot a tranzakciós rendszerekbe épített monitoring funkciót, illetve monitoring céljára épített adattárházakhoz kapcsolódó jelentés rendszerek támogatják.

## 7.2 Bizonyítékok, összegyűjtésük és megőrzésük

Bűncselekmény gyanúja esetén a nyomozás célja a bűncselekmény helyszínén maradt nyomok begyűjtése, valamint a bizonyítékok összegyűjtése és megőrzése. Nyomozati szakaszban az ügyész felkutatja a bűncselekménnyel kapcsolatos valamennyi bizonyítékot, és

dönt arról, hogy vádat emel-e. Ennek részeként az ügyész megkísérli megállapítani a bűncselekmény elkövetőjének személyazonosságát, és megtalálni a bizonyítékokat. A vádemelési szakaszban az ügyész az összegyűjtött bizonyítékok alapján eldönti, hogy szükséges-e további nyomozás, vagy vádat emel, illetve meg is szüntetheti az eljárást. Ezt követően az elsőfokú bíróság: a bíróság lefolytatja a bizonyítási eljárást (meghallgatja és szembesíti egymással a tanúkat s a többi), majd határoz arról, hogy a vádlott bűnös–e a bűncselekmény elkövetésében. Ezt követhetik a fellebbezések, eljárási hiba esetén az eljárás ismételt lefolytatása.

Ahhoz, hogy bírósági szakaszba eljuthasson egy informatikai biztonsági esemény felelőseinek bűnügye, illetve polgári peres ügye arra van szükség, hogy kétséget kizáróan bizonyítható legyen az esemény és az eseményben való közreműködés.

A bűnjel (11/2003. (V. 8.) IM-BM-PM együttes rendelet szerint az a lefoglalt dolog, amely az eljárás során a bizonyítás eszközéül szolgál, valamint, amelyet az eljárás során azonosítani, megvizsgálni, valamint megtekinteni szükséges) egy tárgyi bizonyítási eszköz lehet, amely az eljárásban, a szakvélemény, az okiratok a tanúvallomások és a terhelt vallomása mellett bizonyítékká válhat. Bűnjel lehet elektronikus úton rögzített adat, amelyet szakértő bevonásával ment le a hatóság.

Ezért fontos a bűnjelek szakszerű begyűjtése, csomagolása, és a felügyeleti lánc megtartása, majd az igazságügyi szakértő személye, illetve felkért eseti szakértő által készített szakvélemény.

A bizonyíték elfogadhatóságának alapelvei a következők:

- elfogadható (jogszabályoknak megfelelő)
- hiteles (kapcsolódik az eseményhez)
- teljes (minden nézőpont szerint gyűjtött)
- megbízható (begyűjtési és elemzés során megmaradt a hitelessége)
- hihető (könnyen érthető és világos)

Az igazságügyi szakértők feladata a bíróság, az ügyészség, a rendőrség, illetve a jogszabályokban meghatározott más hatóságok kirendelése, illetve más megrendelők megbízás alapján, a tudomány és a műszaki fejlődés eredményeinek felhasználásával készített szakvéleménnyel segítse a tényállás megállapítását, a faladataként meghatározott szakkérdés eldöntését.

Jelenleg is ismert igazságügyi szakértői rendszert a 29/1964. Korm. számú rendelet alapozta meg, majd sokáig a 4/1976. MT. rendelet határozta meg. Jelenleg az igazságügyi

tevékenységről szóló 2005. évi XLVII. törvény a hatályos, mely lefekteti a tevékenység alapvető szabályait. A törvény az alábbi informatikával kapcsolatos szakterületeket különbözteti meg:

- informatikai berendezések, számítógépek, perifériák és helyi hálózatok (hardver),
- informatikai biztonság,
- informatikai rendszerek tervezése, szervezése,
- stúdiótechnika, multimédia területtel összefüggő informatikai tevékenység,
- számítástechnikai adatbázis, adatstruktúrák,
- szoftverek.

A fenti szakterület csoportosítás nem enged lehetőséget a pontos szakterületek megadására (például szoftver specifikus tudás). Indokolt lenne a területek további alábontása.

Nincs azonban egységes szabályozás arra vonatkozóan, hogy pontosan hogyan kell a szakértői munkát elvégezni. Jelenleg minden igazságügyi szakértő a saját legjobb tudása alapján dolgozik. Indokolt lenne minimális követelményeket megfogalmazni példának okáért az adathordozók hiteles másolásának menetéről. Igazságügyi szakértővé válásnak több feltétele van. Egyrészt a büntetlen előélet, másrészt rendelkezni kell az igazságügyi szakértői tevékenység folytatásához meghatározott képesítéssel a bejegyezni kért szakterületen (legalább ötéves szakirányú szakmai gyakorlattal), továbbá többnyire tagjának kell lennie a szakterületén működő szakmai kamarának. Emellett kötelezettséget kell vállalnia arra, hogy a hatósági kirendelésnek is eleget tesz.

Ha igazságügyi szakértőt akarunk igénybe venni az igazságügyi szakértői névjegyzékben indokolt ellenőrizni, hogy a felkért szakértő személy, vagy cég jogosan végez szakértői tevékenységet. URL: https://szakertok.kim.gov.hu/szakertok.

A névjegyzékben nem szerepelnek az igazságügyi szakértői tevékenység folytatására külön jogszabályban feljogosított állami szervek, intézmények, szervezetek. Ezen túlmenően, ha egy speciális kérdésben nincsen igazságügyi szakértő, akkor kirendelhetőek a témában jártas természetes személyek vagy szervezetek, de ők csak eseti jelleggel adhatnak szakvéleményt.

Az informatikai igazságügyi szakértők speciális eszköztárral rendelkeznek a digitális bizonyítékok megszerzésétől kezdve a bizonyítékok elemzésén a bizonyítékok értékeléséig.

PÉLDA:

Amennyiben egy nagy értékű informatikai rendszer bevezetési projekt nem hozza meg a kívánt eredményt, vagy teljesen sikertelen lesz, akkor jogvita alakulhat ki a

Megrendelő és a Vállalkozó között. Ha nem sikerül megállapodniuk, és perre viszik a vitát, igazságügyi informatikai szakértő kirendelésére kerül sor. Az igazságügyi szakértő szakvéleménye független szakmai vélemény a bíró részére, mely segíti őt a megalapozott döntés meghozatalában.

Továbbá a Felek felkérhetnek további igazságügyi szakértőket az álláspontjuk független megerősítésére, amennyiben úgy látják, hogy a kirendelt igazságügyi szakértő nem megalapozott véleményt fogalmazott meg. Azonban a szakértői vélemények nem kötelezik a bírót arra, hogy eszerint is döntsön.

## 7.3 Károkozás, visszaélések, csalások típusai

Az elektronikus információs szolgáltatások használatából eredően különbözőképpen szenvedhet kárt egy szervezet. A kár lehet környezeti hatás, és gondatlan, vagy szándékos emberi tevékenység eredménye.

Gondatlan károkozás lehet például egy állomány törlése, abban az esetben, ha nem állítható a szükséges időben vissza. Ezt meg lehet előzni többféleképpen is: az állomány tulajdonságainál csak olvashatóra állítjuk, esetleg használjuk az operációs rendszer lomtár funkcióját, vagy rendszeres mentéseket készítünk. A nem megfelelően képzett munkavállalóink is jelentős károkat tudnak okozni, kárt tehetnek eszközökben, vagy adatvesztéseket illetve rendszer leállásokat okozhatnak. A gondatlan károkozást leginkább a munkatársak képzésével, a felkészültségük rendszeres ellenőrzésével lehet megelőzni.

PÉLDA:

Klasszikus példa, amely inkább humoros, hogy a hajlékony lemezek idején egyes kollegák félbehajtották lemezeket, hogy ingzsebükben elférjen és csodálkoztak, hogy használhatatlanná vált. A CD megjelenésével voltak olyan munkatársak, akik kávésbögre tartónak használták a CD lejátszó tálcáját. De okoztak álmatlan éjszakát olyan takarítók is, akik egy kisvállalatnál az irodai szervert működtető konnektort találták a legalkalmasabbnak a porszívó működtetésére is, és a nem megfelelő leállítás miatt helyre kellett állítani a szervert a mentésekből.

A szándékos károkozással a számítógépes bűncselekmények kategóriájához jutottunk. Ezeknek kétféle fő típusa van, az első a számítógépek felhasználásával elkövetett bűncselekmény, ami a bűncselekmények széles körét jelentheti, itthon leginkább az internetes hirdetéseket használják fel visszaélésre, de ide tartozhat az olyan adócsalás, ahol a hamis számlákat számítógéppel állítják ki.

A másik fő típus a számítógépes rendszerek ellen elkövetett bűncselekmények csoportja. Ezt hívják a médiában számítógépes betörésnek, vagy hekkelésnek. Gyakori formája az internetes honlapok tartalmának jogosulatlan megváltoztatása (deface), vagy más postaládájának jogosulatlan olvasása (postafiók feltörése).

Szándékos károkozásoknak sokféle altípusa van. Megkülönböztethetjük a szándék típusa szerint (például károkozás, előnyszerzés), a károkozó(k) személye szerint (például belső, külső, ismeretlen, csoportos, s a többi), vagy akár a jogi minősítésük alapján (például szabálysértés, bűncselekmény, s a többi).

Kik is a számítógépes bűnözők (avagy fekete kalapos hekkerek)? Ezek az emberek általában magasan képzett informatikus szakemberek, akik képességeiket jogszabályellenes tevékenységekre használják fel anyagi vagy más haszonszerzés érdekében, vagy csak figyelemfelkeltésért, esetleg egy ideológia érdekében, vagy mert kényszerítik őket rá, de arra is volt példa, hogy megtévesztették őket. Céljaik nem feltétlen ártó szándékúak. A számítástechnika hőskorából származó romantika lengi be a hekkerek világát, valamifajta demokratikus, modern kori Robin Hood-ként írnak róluk, akik nem ismerik a világukat. De az igazi számítógépes bűnözők egy világméretű iparág szakmunkásai, jól felépített értéklánc különböző pontján dolgoznak: megtervezik a visszaéléseket, adatlopó vírusokat írnak, hitelkártya adatokkal kereskednek, ipari titkokat szereznek meg védett rendszerekből.

A belső támadók legnagyobb csoportját a sértett munkavállalók alkotják. Esetenként a munkavállalók vélt, vagy valós sérelmeiket a munkaadóikon az informatikai rendszereket érő támadással igyekeznek megtorolni. Volt már példa többek között éles rendszerek elérhetetlenné tételére, ügyféladatok eltulajdonítására, vezetők rendszerből való kitiltására. Gyakori példa az ügyféladatbázis részleges, vagy teljes eltulajdonítása is jellemzően a munkahelyváltást megelőzően.

A jogi szabályozás sajátosságaiból adódóan mindig utólag követi az élet eseményeit, a műszaki fejlődést. Napjainkra a számítógépes, és számítógépek segítségével elkövetett visszaélések és bűncselekmény bekerültek a Büntető Törvénykönyvbe:

- Zártörés (287)
- Terrorcselekmény (314)
- Információs rendszer felhasználásával elkövetett csalás (375)
- Védelmet biztosító műszaki intézkedés kijátszása (386)
- Pénzhamisítás elősegítése (390)
- Készpénz-helyettesítő fizetési eszköz hamisításának elősegítése (394)
- Tiltott adatszerzés (422)

- Információs rendszer vagy adat megsértése (423)
- Információs rendszer védelmét biztosító technikai intézkedés kijátszása (424)
  (URL: http://njt.hu/cgi_bin/njt_doc.cgi?docid=152383.262832)

## 7.4 Informatikai nyomozás, vizsgálati módszerek

Folyamatban van a rendőrség átalakítása ezen a szakterületen. Általában kiemelt ügyekben a Nemzeti Nyomozó Iroda vizsgálódik, de a TEK-nél (Terror Elhárító Központ) is létrehoztak a közelmúltban kiberbiztonsággal foglalkozó részleget. A nemzetbiztonságot érintő ügyekben a szakszolgálatok végzik a nyomozást. A 2012-es budapesti nemzetközi Kibertér konferencián elhangzott, hogy nemzetközi szinten is erősen korlátozott a kiberbűnözés felderítésében jártas bűnüldözési kapacitás. Gyakran az ügyek már ott elbuknak, hogy az ilyen bűncselekményekre vonatkozó nyomok rögzítése sem történik meg olyan módon, hogy bizonyítékként felhasználható legyen a bíróság előtt. Az országok bűnüldöző szervei közötti kooperációt a kiberbűnözés területén is az Europol, illetve az Interpol koordinálja. Nagy erőfeszítéseket tesznek ezek a szervezetek a koordináció fejlesztésére, és a számítógépes bűncselekmények elleni fellépés képességének javítására.

Magyarországon, ahogy a világon máshol is, terjed a kiberbűnözés. Legutóbb egy nemzetközi bankkártya csalást végző hálózat tagjai használtak hamisított kártyákat nagy összegű pénzfelvételre. A kiberbűnözés elleni hatósági fellépés, ahogy a világon máshol is, jelentősen lemaradva követi a bűnözés technikáinak feltárását.

PÉLDA

Többek között a bűnözők egymás közötti kapcsolattartására is a mobiltelefonokat, majd az internetes csevegő programokat, fórumokat és internet telefonokat használják. A hagyományos telefonlehallgatás így már nem tud segítséget adni az ilyen jellegű ügyek teljes körű felderítéséhez.

A bűnüldöző szerveknek is naprakész műszaki szakmai tudásra van szükségük. A rendőrök többsége azonban csak általános számítógépes ismeretekkel rendelkezik, ami az ilyen munkához nem elégséges, és a rendőrség korlátozott képességekkel rendelkezik a kiberbűnözés elleni harcban megfelelő eszközök és szakemberek hiányában.

Az informatikai nyomozás (computer forensics) célja a különböző informatikai eszközökkel, illetve műszaki megoldások felhasználásával elkövetett bűncselekmények felderítése, modellezése, rekonstruálása, az egyes tevékenységek időbeliségének megállapítása, valamint a bizonyítékok felkutatása, és strukturált formában való

összegyűjtése. Napjainkban már a bűnügyi tudományok egy elismert ágának tekinthető, ez a széleskörű szakismeretet igénylő szakma. Ehhez igazságügyi informatikai szakértőket, vagy eseti szakértőket vesznek igénybe a hatóságok.

PÉLDA:

A rendőrség leggyakrabban a nyomozások során a házkutatásnál talált, illetve a lefoglalt műszaki eszközök adattartalmának elemzésére vesz igénybe igazságügyi szakértőt hazánkban. Gyakori kérés a megadott kulcsszavakat tartalmazó dokumentumok azonosítása. Itt a merevlemezek tartalmának elemzésekor a szakmai feladat az, hogy a vizsgálandó adatokból a feltett kérdéseknek megfelelő lekérdezést állítson össze a szakértő. Másik tipikus megbízás a nem jogtiszta szoftverek azonosítása a lefoglalt adathordozókon.

## 7.5 Biztonsági események vizsgálatára vonatkozó jelentés

A súlyos biztonsági eseményeket az IBV-nek ki kell vizsgálnia. A vizsgálatáról vizsgálati jelentést kell készíteni, mely a vizsgálat során feltárt lényeges megállapítások rangsorolt rögzítését tartalmazza, és a megállapításokból eredő kockázatokat. A jelentések akkor segítik igazán biztonsági események ismételt bekövetkezésének megelőzését, amennyiben a feltárt kockázatok kezelésére vonatkozó, bevált gyakorlatokon alapuló javaslatokat is beépítik.

A súlyos biztonsági események vizsgálatáról vizsgálati jelentést készít az IBV. A jelentésben az ellenőrzés a megállapításokat elegendő, megbízható, érdemi és hasznos bizonyítékokkal kell alátámasztani, és azok kockázatait bemutatni. A megállapításokat, következtetéseket és javaslatokat lényegre törően és világosan kell megfogalmazni.

A vizsgálatok során értékelni kell a rendelkezésre bocsátott minden információt és véleményt. A vélemények azonban nem befolyásolhatják a tényeken alapuló megállapításokat, következtetéseket.

A vizsgálati jelentés megállapításai alapján intézkedési tervet kell készíteni, melyben az intézkedések végrehajtásának ütemezése a végrehajtásáért felelősök személye, és a vonatkozó határidők kerülnek megjelölésre.

# 8 Az információbiztonsági eseménykezelő szakemberek eszköztára

## 8.1 Események megelőzésének támogatása

Az *UTM eszközök*ben megtalálható minden olyan védelmi funkció (Tűzfal, IPS, kéretlen levélszűrő, tartalomszűrő, magánhálózat, terhelés-elosztó, adatszivárgás megelőző), amely megvédi az információs rendszereinket az eszközbe kötött hálózat (általában Internet) felől érkező fenyegetésektől.

Ingyenesen elérhető eszközök:

- Endian (URL: http://www.endian.com/en/community/efw-30)
- PfSense (URL: https://www.pfsense.org/about-pfsense/features.html)
- Zorp (URL: http://www.balabit.com/network-security/zorp-gpl/features)

A naplózás, a *naplóelemzés* központi helyet elfoglaló védelmi megoldás a biztonság szakemberek eszköztárában, feltáró kontroll. Újabban *SIEM megoldások*nak nevezik azokat az eszközöket, amelyek különböző forrásokból biztonság specifikus információt gyűjtenek össze, elemeznek és mutatnak meg a biztonsági szakemberek részére.

Ingyenesen elérhető eszközök:

- iView (URL: http://sourceforge.net/projects/cyberoam-iview/)
- LOGAlyze (URL: http://www.logalyze.com/product/major-features)
- OSSIM (URL: http://www.alienvault.com/open-threat-exchange/projects)
- Syslog-ng (URL: http://www.balabit.com/hu/network-security/syslog-ng/opensource-logging-system)

## 8.2 Eseménykezelő központ működésének támogatása

Szükségesek szoftver eszközök és nyilvántartások annak érdekében, hogy megfelelően felvértezzük egy eseménykezelő központban dolgozó, illetve a reagáló csapatokat:

A hibajegy-kezelő rendszerek főbb funkciói: hibajegyek megnyitása, frissítése, és lezárása, továbbá a hibajegyekben keresés, eszkaláció, és a hibajegyek adminisztrációja. Célszerű még, ha kimutatások készíthetőek belőle az SLA paraméterek szerint. Ilyen például:

- SZTAKI ITAK szolgáltatás URL: http://itak.sztaki.hu/hu/termekek/hibajegykezelo.html (nem ingyenes)
- SpiceWorks, URL: http://www.spiceworks.com/free-help-desk-software/?utm_campaign=Listly&utm_medium=list&utm_source=listly
- Mantis, URL: http://www.mantisbt.org/
- JIRA, URL: https://www.atlassian.com/software/jira

Naprakész címjegyzék, és tudásbázisok (GYIK, útmutatók, s a többi) segíthetik a gyors reagálást. Ezek tárolhatóak egy egyszerű táblázatkezelőben, vagy adatbázisban is, de hatékonyabb a helpdesk rendszerrel integráltan alkalmazni. Ilyen például:

- Spiceworks, URL: http://www.spiceworks.com/free-it-knowledge-base-software/

## 8.3 Nyomok rögzítésének és elemzésének támogatása

A digitális bizonyítékok rögzítése, elemzése és értékelése az igazságügyi szakértő feladata. Munkája során minden szakértő megválaszthatja, hogy milyen eszközöket használ. Ezek általában adatrögzítő és másolós eszközök, adat elemző eszközök és kis célszoftverek (például: rejtjel fejtő szoftver)

Ingyenes nyomrögzítést, illetve elemzést támogató eszközök:

- SANS SIFT (URL: http://digital-forensics.sans.org/community/downloads) – többfunkciós eszköz
- CAINE (URL: http://www.caine-live.net/) – többfunkciós eszköz
- PST viewer (URL: http://www.nucleustechnologies.com/pst-viewer.html) levelezés elemzése
- Wireshark (URL: http://en.wikipedia.org/wiki/Wireshark) – hálózat elemzés
- Volatililty (URL: https://code.google.com/p/volatility/) – memória elemzés
- Dc3DD (URL: http://sourceforge.net/projects/dc3dd/) – lemezmásolat
- McAfee Forensic Toolkit v2.0 (URL: http://www.mcafee.com/us/downloads/free-tools/forensic-toolkit.aspx)

# 9 Hivatkozások

## 9.1 Könyvek

COBIT 5 for Information Security Task Force, ISACA, 2012

COBIT 5 for Information Security

ISBN 978-1-60420-255-7

Susan Snedaker, Elsevier, 2007

Business Continuity and Disaster Recovery Planning for IT Professionals

ISBN 13: 978-1-59749-172-3

## 9.2 Szakfolyóiratok

Haris Hamidovic, ISACA JOURNAL VOLUME 6, 2011, p1-7

An Introduction to Information Security Incident Management Based on ISO/IEC TR 18044:2004

## 9.3 Internetes és egyéb források idézése

Mason Pokladnik, SANS Institute, 2007

An Incident Handling Process for Small and Medium Businesses

URL: http://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791

Jim Clinch, AXELOS, 2009

ITIL V3 and Information Security

URL:

http://www.axelos.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf

Szádeczky Tamás, PhD értekezés, Pécs, 2011

Szabályozott biztonság, Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan

URL:

http://doktori-iskola.ajk.pte.hu/files/tiny_mce/File/Vedes/szadeczky/ertekezes_szadeczky_nyilv.pdf

# 10 Mellékletek

## 10.1 Windows 7 eseménynaplók[3]

A Windows 7 eseménynapló beállításait rendszergazdaként lehet módosítani. Felhasználók csak a felhasználói fiókra érvényes beállításokat szerkeszthetik. Az Eseménynapló Start gomb - Vezérlőpult - Rendszer és biztonság lapon a Felügyeleti eszközökön belül az Eseménynapló parancsra kattintva érhetőek el. Itt a bal oldali táblában egy eseménynaplóra, majd azon belül egy eseményre duplán kattintva tekinthetőek meg az események részletei.

Az eseménynaplók olyan speciális fájlok, amelyek a számítógépen történő jelentős eseményeket rögzítik, például egy felhasználó belépését a számítógépre, vagy azt, ha egy program hibát okoz. Minden esetben, ha egy ilyen esemény történik, a Windows rendszer rögzíti az eseményt egy eseménynaplóba, amelyet az Eseménynapló alkalmazással lehet megtekinteni. Az információbiztonsági szakértők az egyes naplók részleteit a Windows és más programok hibáinak azonosítása, illetve a biztonsági események nyomainak feltárására és elemzésére használhatják.

A Windows 7 eseménynaplói a következőket tartalmazzák:

- Alkalmazás (program) események. Az események osztályozása lehet hiba, figyelmeztetés vagy információ, az esemény fontosságától függően. A hiba általában egy jelentős probléma, például adatvesztés. A figyelmeztetés nem feltétlenül jelentős, de jelezhet egy lehetséges, jövőbeli hibát. Az információ esemény egy programmal, illesztő-programmal vagy szolgáltatással végrehajtott sikeres műveletet jelöl.

- Biztonsággal kapcsolatos események. Az ilyen esemény neve naplózás, és az eseménytől függően lehet sikeres vagy sikertelen, amilyen például az, hogy egy felhasználó bejelentkezése a Windows rendszerbe sikeres volt-e.

- A telepítés eseményei. A tartományvezérlőként konfigurált számítógépek a következő naplóbejegyzésekkel rendelkeznek.

[3] forrás: Windows támogatás - http://windows.microsoft.com/hu-hu/windows/what-information-event-logs-event-viewer#1TC=windows-7, http://windows.microsoft.com/hu-hu/windows7/monitor-attempts-to-access-and-change-settings-on-your-computer

- Rendszeresemények. A rendszereseményeket a Windows rendszer vagy a Windows rendszerszolgáltatás eszköz naplózza, ezek osztályozása lehet hiba, figyelmeztetés vagy információ.

- Továbbított események: Ezeket az eseményeket más számítógépek továbbítják ebbe a naplóba.

Az alkalmazások és a szolgáltatások naplói eltérnek a fent részletezett naplóktól. Az alkalmazás naplók különböző naplóbejegyzéseket rögzítenek a számítógépen futó egy-egy programról, és a szolgáltatás naplók részletesebb bejegyzéseket tartalmaznak az egyes Windows szolgáltatásokról. A Windows 7 számítógép biztonsági naplójából megállapítható, ha valaki bejelentkezett a számítógépre, létrehozott egy új felhasználói fiókot, biztonsági házirendet módosított vagy megnyitott egy dokumentumot. Biztonsági események főbb típusai:

- Fiókkezelési műveletek: Mikor történt egy fiók nevének módosítása, fiókok engedélyezése vagy letiltása, létrehozása vagy törlése, jelszó módosítása vagy felhasználói csoportok megváltoztatása.

- Bejelentkezés: A bejelentkezés vagy kijelentkezés a számítógépről (akár közvetlenül, akár a hálózaton keresztül).

- Címtárszolgáltatás elérése: Ki fér hozzá a saját rendszerszintű hozzáférés-szabályozási listával rendelkező AD objektumokhoz.

- Objektum-hozzáférés: Ki használt egy fájlt, mappát, nyomtatót vagy más objektumot. Lehetőség van a beállításkulcsok naplózására is.

- Házirendkezelés: A helyi biztonsági házirendek módosítására tett kísérletek, valamint a felhasználói jogok kiosztásának, és a naplózási vagy a megbízhatósági házirendeknek a megváltoztatása.

- Használati jog: Ki hajt végre a számítógépen egy olyan feladatot, amihez engedéllyel rendelkezik.

- Folyamatok nyomon követése: Észlelhető, ha egy esemény (például programaktiválás vagy folyamatmegszakadás) bekövetkezik.

- Rendszeresemények: Észlelhető, ha a valaki leállította vagy újraindította a számítógépet, vagy amikor a folyamat vagy program olyan műveletet próbál meg végrehajtani, amihez nincs engedélye.

A szolgáltatások és alkalmazások működése még biztonságosabbá tehetőek úgy, hogy a rajta történő eseményeket figyelemmel kísérik (naplóelemzés). A naplóelemzés nem akadályozza meg azt, hogy illetéktelen személyek módosításokat hajtsanak végre, de időben értesítést küldhet változtatásokról.

A naplófájlok törlése az Eseménykezelő Műveletek ablakában, a Napló törlése parancs használatával végezhető.

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.