Naplózás e-kormányzati rendszerekben

1 Bevezetés

Az informatikai rendszerek biztonságának egyik legfontosabb alapköve a megfelelő naplózás, azaz az infrastruktúrában történt események rögzítése. A naplózás információt nyújt az informatikai elemek általános állapotáról csakúgy, mint a biztonságilag fontos történésekről. Ez a műszaki megoldás nélkülözhetetlen a szabálysértések azonnali érzékeléséhez és akár a hónapokkal későbbi kivizsgáláshoz, esetleg bűnügyi nyomozáshoz is. A jelenleg fejlesztés alatt álló elektronikus kormányzati rendszerek összetettsége miatt azonban nehezen meghatározható, hogy a naplózás pontosan milyen eseményeket, tartalmat, részletezettséget, forrást, célt, protokollt, stb. jelent. Jelen tanulmány célja erre a kérdésre kielégítő választ adni, olyan összefoglalást megjeleníteni, mely elméleti ismeretek és gyakorlati tapasztalatok alapján hasznos útmutató lehet a magyar e-közigazgatási rendszerek fejlesztői számára.

Az első rész bemutatja azokat a jogszabályokat, melyek alapján a naplózás minden elektronikus közszolgáltatást nyújtó szervezet számára elvárásként jelenik meg. Kitekintésként bemutatásra kerül más területek jogszabályi kötelezettsége is, hiszen itt már több éves gyakorlat áll rendelkezésre. Szintén elemzésre kerülnek a vonatkozó információbiztonsági szabványok követelményei is.

A második részben egy tipikus elektronikus közszolgáltatást nyújtó közigazgatási rendszer architektúrája kerül felvázolásra, mely a korszerű fejlesztéseknél megszokott web service megoldásokat használja. Itt azonosítani lehet minden naplóforrást, valamint be lehet mutatni, mely források bevonása szükséges a törvényi kötelezettségek teljesítéséhez.

A harmadik rész a kitűzött céloknak megfelelő loggyűjtési, archiválási és elemzési lehetőségeket tárgyalja meg. Mivel a naplózó infrastruktúrának jelentős terheléssel kell megbirkóznia, olyan paraméterek meghatározása válik szükségessé, melynek segítségével hosszú távon is jól működő rendszer tervezhető. Itt kerül ismertetésre a lehetséges naplózási protokollok köre is.

Az architekturális kérdések után ki kell térni a naplózás tartalmi kérdéseire is. A negyedik rész a szabványok és jógyakorlatok alapján bemutatja, hogy mik azok az események, amelyeket biztonsági szempontból gyűjteni és vizsgálni szükséges, valamint azokat az eseményekhez kapcsolódó további információkat is, melyek alapján a pontos nyomon követés lehetséges.

Az ötödik részben kerülnek ismertetésre a naplózással kapcsolatos adminisztratív eljárások. Ez lefedi az azonnali cselekvés, incidenskezelés szükséges lépéseit, a naplóállományok, mint bizonyítékok felhasználásának lehetőségeit, valamint a felelősségi körök meghatározását.

Ez az öt lépés egységesen szükséges ahhoz, hogy egy szervezet a gyakorlatban is jól működő naplózási eljárást alakítson ki. Magyarországon ilyen eljárásrendet és rendszert nagyon kevés helyen működtetnek sikeresen, holott a példa adott: az USA-ban és Nyugat-Európában igen sikeres tapasztalatokkal bírnak, és magának a naplózásnak is több évtizedes múltja van. A tanulmány egy apró lépéssel kíván hozzájárulni a magyar kormányzati informatika biztonságának megerősítéséhez e tapasztalatok összefoglalásával.

2 Jogszabályok, szabványok

2.1 Közigazgatási követelmények

Az informatikai rendszerek naplózással kapcsolatos követelményei régóta részei a magyar jogi környezetnek. Az elektronikus közigazgatás kialakulása ezeket a követelményeket annyira hangsúlyossá tette, hogy a területet szabályozó kormányrendeletek külön paragrafusokat szántak a logolásnak. Jelenleg a 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról 15. §-a tárgyalja részletesen a területet.

„(1) A szolgáltatást nyújtó szervezet az általa működtetett rendszerben vagy annak környezetében vagy mindkettőben gondoskodik a rendszer működése szempontjából meghatározó folyamatok valamennyi kritikus eseményének naplózásáról.

(2) A szolgáltatást nyújtó szervezet a naplózandó események körét, a napló adattartalmának megőrzési idejét - a vonatkozó jogi szabályozás alapján, az adott eljárási cselekmény biztonsági jellegére, érzékenységére tekintettel - határozza meg. A megőrzési időn belül a megbízhatóság megítéléséhez szükséges mértékben valamennyi, az eljárási cselekménnyel kapcsolatos eseménynek rekonstruálhatónak kell lennie. Naplózni kell minden személyes adat továbbítását.

(3) A naplóállomány bejegyzéseit védeni kell az arra jogosulatlan személy általi hozzáféréstől, módosítástól, törléstől, illetve biztosítani kell, hogy a napló tartalma a megőrzési időn belül a jogosult számára megismerhető és értelmezhető maradjon.

(4) A naplóállományokat a 16-17. §-ban szabályozott mentési rendnek megfelelően, a maradandó értékű dokumentumokra vonatkozó szabályok szerint kell tárolni, hogy egy esetleges lokális károsodás ne tegye lehetetlenné a bizonyítást.

(5) A naplóállományok megőrzési idejét - a (2) bekezdésben foglaltak figyelembevételével - a vonatkozó iratkezelési szabályzatok részeként kell meghatározni. A működtető a vonatkozó jogszabály, illetve iratkezelési szabályzat rendelkezésétől függően, a megőrzési határidő lejártával gondoskodik a naplóállományok adathordozóinak levéltári őrizetbe adásáról vagy az adatállományok dokumentált, visszaállítást kizáró megsemmisítéséről.”

Ezeket a magas szinten megfogalmazott követelményeket segít pontosítani a kormányrendelet 1. mellékletének 7.10. alfejezete, mely a Központi Elektronikus Szolgáltató Rendszer, hétköznapi nevén az Ügyfélkapu és a mögötte álló kiszolgáló rendszerek naplózási előírásait tartalmazza. Ezek szerint figyelemmel kell kísérni a jogosult és illetéktelen rendszerhasználatot, jelezni kell a jogosulatlan használatot, meg kell oldani a naplóállományok biztonságos tárolását, kiemelten kell foglalkozni az adminisztrátori tevékenységekkel, gyűjteni kell a rendszer hibás működésével kapcsolatos logokat, valamint az összes rendszert egyetlen időforráshoz kell szinkronizálni.

A magyar szabályozás hiányossága, hogy a kormányrendelet csak az elektronikus közszolgáltatásokkal foglalkozik, mely a 2009. évi LX törvény 3. § (1) szerint „... törvényben elektronikus úton nyújtott szolgáltatások biztosítására kötelezettek, illetőleg elektronikus úton szolgáltatást nyújtó egyéb szervezetek hatósági vagy egyéb tevékenységének, hatósági nyilvántartásból történő adatszolgáltatásának, a központi elektronikus szolgáltató rendszer (a továbbiakban: központi rendszer) igénybevételével, elektronikus úton történő végzése.”. Hatálya tehát nem terjed ki azokra a szakrendszerekre, melyek egy-egy közigazgatási szerv belső működését támogatják, holott a hibák, visszaélések felderítésére ezekben is fokozottan

szükség van. Itt a rendszereket beszerző közigazgatási intézmény feladata a követelmények meghatározása. Ebben segíti őket a Közigazgatási Informatikai Bizottság (továbbiakban KIB) 28. számú ajánlása, melynek „IT biztonsági műszaki követelmények” című kötete foglalkozik a naplózással.

A KIB 28. ajánlás három eltérő biztonsági szintet határoz meg a közigazgatási rendszerek területén. Az alacsony, fokozott és kiemelt kihatású szint megállapításához az ajánlás szerinti kockázatelemzést kell elvégezni, melynek bizalmassági, sértetlenségi és rendelkezésre állási paraméterei alapján lehet a döntést meghozni. A három szinten egyre komolyabb naplózási tevékenységeket kell a rendszernek és az üzemeltető szervezetnek folytatnia.

Minden esetben el kell készíteni egy olyan naplózási szabályzatot, mely a teljes eljárásrenddel foglalkozik, így kielégítően teljesíti a kormányrendeletben előírtakat is. Az első komoly próbatétel a naplózandó események körének meghatározása. Egyetlen rendelet vagy ajánlás sem határozza meg ezt a halmazt, nem is teheti, hiszen minden rendszer máshogy működik. A tanulmány későbbi részében a Common Criteria szabvány segítségével kerül bemutatásra egy általános közigazgatási rendszer által előállítandó logok listája. Annyi bizonyos, hogy minden bejegyzésnek tartalmaznia kell az esemény dátumát és időpontját, a rendszer megfelelő összetevőjét (pl. szoftver összetevő, hardver összetevő) az esemény keletkezésének helyét, az esemény típusát, a felhasználó azonosítóját és az esemény kimenetelét (siker vagy hiba). A KIB 28. ajánlás még támpontot ad, hogy kiemelt szinten központi naplózást kell megvalósítani.

Komoly kihívás az ajánlásban előírt tárkapacitás megbecslése is. Erre vonatkozó becsléseket a tervezési fázisban lehet tenni, de a gyakorlat ettől általában jelentősen el szokott térni. A szükséges és rendelkezése álló erőforrások tehát folyamatosan értékelendők. Kiemelt szinten a tárhely beteléséről automatikus riasztást kell küldeni az üzemeltetőknek. Amennyiben nem áll rendelkezésre elegendő tároló kapacitás, a legoptimálisabb megoldás a rendszer leállítása, vagy olyan működés fenntartása, mely minimális új bejegyzést generál. Minden más megoldásnál figyelembe kell venni, hogy biztonsági esemény nem maradhat naplózatlanul!

Fokozott és kiemelt szinten meg gondoskodni kell a naplóelemzésről is, azaz olyan eszközt kell biztosítani, mellyel az összegyűjtött naplóállományok bizonyos paraméterek alapján szűrhetők és aggregálhatók. Ezt akár egyedi lekérdezés során, akár rendszeres időközönként történő automatikus előállítással is meg lehessen tenni.

A bejegyzéseket bizonyos esetekben bizonyítékként is fel kell használni. Ehhez elengedhetetlenül fontos az időbeliség biztosítása, azaz minden logforrásnak ugyanazt az időinformációt kell felhasználnia. Fokozott és kiemelt szinten nem elég egy belső NTP szervert beüzemelni, hanem ezt valamilyen megbízható, külső, rádiós időszolgáltatóhoz kell szinkronizálni. Minden körülmények között biztosítani kell a jogosulatlan hozzáféréssel szembeni védelmet, opcionálisan akár WORM eszköz felhasználásával is. Szintén lehetséges a bejegyzésekben a letagadhatatlanság megvalósítása is, pl. az egyes kritikus események digitális aláírásával, de ez nem kötelező. A naplóbejegyzéseket a belső iratkezelési szabályok és a jogszabályok szerint kell megőrizni.

2.2 Más iparágak követelményei

A közigazgatáson belül egyes részterületek rendelkeznek még naplózásra vonatkozó szabályokkal. Ezek az iratkezelés köré csoportosulnak, hiszen az általános és minősített

iratkezelés, az elektronikus aláírás, a digitális archiválás azok a területek, melyeknél a logolás törvényi követelményként jelenik meg.

A közigazgatás mellett a pénzintézeti terület rendelkezik jól kialakított naplózási követelményekkel. A hitelintézetek, pénzügyi vállalkozók, magánnyugdíjpénztárak, befektetési vállalkozások, árutőzsdei szolgáltatók és az Önkéntes Kölcsönös Biztosító Pénztárak működésére vonatkozó jogszabályok mind kitérnek erre a területre. A Pénzügyi Szervezetek Állami Felügyeletének 1/2007. számú módszertani útmutatója a pénzügyi szervezetek informatikai rendszerének védelméről értelmezi a törvények vonatkozó paragrafusait, és ad eligazítást a megvalósításhoz.

2.3 Szabványból eredő követelmények

A naplózási követelmény minden információbiztonsággal foglalkozó szabvány része. Magyarországon ezen a területen általában két ajánlásra szoktak hivatkozni. Az egyik az Information Systems Audit and Control Association (ISACA) által kiadott Control Objectives for Information and related Technology (COBIT), a másik az ISO/IEC 27002:2005 Code of practice for information security management szabvány, mely az információbiztonság megvalósítását segíti. A két dokumentum között szoros összefüggés fedezhető fel. Míg a COBIT magas szinten határoz meg irányítási és kontroll elveket, az ISO 27002 konkrét útmutatókat tartalmaz, melyek jól összerendelhetők. Ezt tette meg az ISACA a „Mapping of ISO/IEC 17799:2005 With COBIT® 4.0" című tanulmányában, melyből jelen fejezet építkezik.

A COBIT elsősorban a DS 5 folyamatban foglalkozik a logolással, emellett azonban több közvetlen vagy közvetett utalás is történik erre a biztonsági kontrollra. Az ISO 27002 részletesen a 10.10. fejezetében ír a naplózással kapcsolatos követelményekről, 6 csoportba foglalva ezeket, részletesen kifejtve a megvalósítás lehetőségeit is:

- 10.10.1 Audit naplózás: Az audit naplóknak, melyek a felhasználói tevékenységeket, kivételeket és információbiztonsági eseményeket tartalmazzák, olyan módon kell előállítani és egy előre meghatározott ideig megtartani, hogy azok felhasználhatók legyenek egy későbbi kivizsgálásban vagy hozzáférési ellenőrzésben.
- 10.10.2 Rendszerhasználat figyelése: Olyan eljárásokat kell kialakítani, melyek figyelik az információfeldolgozó eszközök használatát, és ezek eredményét rendszeresen felül kell vizsgálni.
- 10.10.3 Naplóinformáció védelme: A naplózó infrastruktúrát és a naplóállományokat védeni kell a nem jogosult hozzáféréstől és módosítástól.
- 10.10.4 Adminisztrátori és operátori naplók: A rendszeradminisztrátorok és rendszeroperátorok tevékenységét naplózni kell.
- 10.10.5 Hibanaplózás: A hibákat naplózni és elemezni kell, és a szükséges javító intézkedéseket meg kell tenni.
- 10.10.6 Óraszinkronizáció: Minden szervezeten vagy biztonsági területen belül levő fontos információfeldolgozó rendszer óráját egy egyezményes, pontos időforráshoz kell szinkronizálni.

A COBIT ezeket rendeli az egyes folyamatok teljesítéséhez az alábbiak szerint.

AI2.3 Alkalmazás kontroll és auditálhatóság: Üzleti kontrollokat, ahol az értelmes, automatizált alkalmazási kontrollok formájában kell megvalósítani, oly módon, hogy az

adatfeldolgozás pontos, teljes, időszerű, engedélyezett és auditálható legyen. Ez többek között a 10.10.1 Audit naplózás és a 10.10.5 Hibanaplózás ISO 27002 követelményekkel teljesíthető.

DS5.5 Biztonság tesztelése, felügyelete és figyelemmel kísérése: Az informatikai biztonság megvalósítását aktívan és kezdeményezően kell tesztelni és nyomon követni. Az informatikai biztonságot idejekorán, ismételten kell bevizsgálni annak biztosítása érdekében, hogy a vállalat jóváhagyott alap informatikai biztonsági szintjét fenntartsák. Egy naplózási és egy figyelemmel kísérési funkciónak kell lehetővé tennie az olyan szokatlan, és/vagy abnormális tevékenységek korai megelőzését, és/vagy észlelését és azt követően időben történő jelentését, amelyekkel lehet, hogy foglalkozni kell. Ez többek között a 10.10.2 Rendszerhasználat figyelése, a 10.10.3 Naplóinformáció védelme és a 10.10.4 Adminisztrátori és operátori naplók követelményekkel fedhető le.

DS5.7 Biztonsági technológiák védelme: A biztonsággal kapcsolatos technológiát úgy kell megvalósítani, hogy az ellent tudjon állni az engedély nélküli módosításnak, és a biztonsági dokumentációt nem szabad szükségtelenül nyilvánosságra hozni. Ez többek között a 10.10.1 Audit naplózás, 10.10.3 Naplóinformáció védelme, a 10.10.4 Adminisztrátori és operátori naplók, a 10.10.5 Hibanaplózás és a 10.10.6 Óraszinkronizáció követelményekkel oldható meg.

ME1.2 Figyelemmel kísérési adatok meghatározása és gyűjtése: Együtt kell működni az üzleti területekkel a teljesítmény célok egy kiegyensúlyozott csoportjának meghatározásában, és annak az üzleti és az egyéb érintett érdekelt felek jóvá kell hagyatni. Ipari normákból a mérési alapokat kell meg határozni a célokkal való összehasonlításhoz, és a célok mérése érdekében begyűjtendő rendelkezésre álló adatokat azonosítni kell. Az adatok időben és pontosan történő begyűjtését szolgáló folyamatok kell bevezetni a célokhoz képesti előrehaladás jelentése érdekében. Teljesítéséhez a 10.10.2 Rendszerhasználat figyelése fejezet szükséges.

ME2.2 Ellenőrző felülvizsgálat: A belső informatikai vezetői felülvizsgálati kontrollok hatékonyságát és eredményességét figyelemmel kell kísérni és értékelni kell. A folyamat többek között a 10.10.2 Rendszerhasználat figyelése és a 10.10.4 Adminisztrátori és operátori naplók követelményekkel kivitelezhető.

ME2.5 A belső irányítási és ellenőrzési rendszer értékelése: Szükség esetén be kell szerezni a belső kontrollok teljességére és eredményességére vonatkozó további garanciát a külső felek által készített felülvizsgálatokon keresztül. A folyamat sikeréhez szintén többek között a 10.10.2 Rendszerhasználat figyelése és a 10.10.4 Adminisztrátori és operátori naplók ISO 27002 fejezetek teljesítése szükséges.

ME4.7 Független bizonyosság nyújtás: Független bizonyosság nyújtást (belső, illetve külső) kell beszerezni az informatika vonatkozó törvényeknek és szabályozásoknak való megfelelőségéről; a szervezet irányelveiről, szabványairól és eljárásairól; az általánosan elfogadott gyakorlatokról; és az informatika eredményességéről és hatékonyságáról. Ez többek között a 10.10.2 Rendszerhasználat figyelése alkalmazásával lehetséges.

3 Naplóforrások e-közigazgatási környezetben

3.1 Általános e-közigazgatási szolgáltatást nyújtó infrastruktúra

A KIB 28. ajánlás „A magyar e-közigazgatási architektúra” című részdokumentuma megadja azokat a fő irányvonalakat, melyek mentén egy általános e-közszolgáltatási infrastruktúra felépíthető. Általánosan elterjedté vált a szolgáltatás-orientált architektúra (SOA), mely elosztott, egymással webes technológiák útján kommunikáló modulokból álló rendszereket eredményez.

Azok az alkalmazások, melyeket köztisztviselők és állampolgárok tízezrei használnak majd az interneten keresztül, egészen más biztonsági környezetben alakulhatnak ki, mint azok, melyeket csak néhány száz felhasználó láthat szeparált, lokális hálózatról. Éppen ezért a már korábban említett három védelmi szintet a gyakorlatban úgy határozhatjuk meg – teljesítve a KIB 25. és 28. számú ajánlásában leírt három szintet –, mint az államtitkot feldolgozó rendszerek (kiemelt), a belső használatú, bizalmas információkat kezelő rendszerek (fokozott), valamint a széles körben, interneten keresztüli hozzáférést biztosító rendszerek (alap).

A három szint azonban a legtöbbször hasonló architektúrára épül. Középpontjában a SOA architektúrát megvalósítani képes eszközök állnak (.NET 3.0, OpenESB, Oracle SOA Suite, IBM Websphere, stb.). Ezek valamilyen portálfelületen keresztül érhetők el a felhasználók számára. A háttérben komoly adatbázisrendszerek szolgálják ki az infrastruktúrát. Általában foglalkozni kell a szervezeten belül működő öröklött rendszerek integrációjával, valamint csatlakozni kell más szervezetek szakrendszereihez is. Elektronikus közszolgáltatás esetén ehhez még hozzájön az Ügyfélkapu vagy Hivatali Kapu kapcsolat. A fejlesztők tehát egy igen heterogén, kiterjedt, bizonyos részeiben interoperábilis, szabványok szerint működő, más részeiben viszont saját protokollokon működő rendszerhez próbálnak az előírások szerinti alkalmazást létrehozni.

3.2 Naplóforrások az infrastruktúrában

Az előző fejezetben meghatározott infrastruktúra a legtöbbször valamilyen piaci termékre épül (operációs rendszer, adatbázis, alkalmazásszerver, tűzfal, IDM, stb.), melyek általában rendelkeznek valamilyen szintű Common Criteria tanúsítvánnyal, így viszonylag egyszerűen kideríthető, hogy ezek a naplóforrások milyen bejegyzéseket képesek létrehozni. Az alábbi példák bemutatják az elterjedt megoldásokat, a Common Criteria szerinti Biztonsági Előirányzatukat, illetve ezekben a naplózási követelményekkel foglalkozó oldalszámokat.

- Operációs rendszerek:
    - Windows Server 2003, http://www.commoncriteriaportal.org/files/epfiles/20080303_st_vid10184-st.pdf, 42-44. oldal
    - Windows Server 2008, http://www.commoncriteriaportal.org/files/epfiles/st_vid10291-st.pdf, 40-42. oldal
    - HP-UX 11i v3, http://www.commoncriteriaportal.org/files/epfiles/lfl_t257-hp_st_v1.6.pdf, 18-20. oldal

- Red Hat Enterprise Linux Version 5.1, http://www.commoncriteriaportal.org/files/epfiles/st_vid10286-st.pdf, 33-38. oldal

- Adatbázis-kezelők:
  - Oracle Database 11g Enterprise Edition, http://www.commoncriteriaportal.org/files/epfiles/0588b_pdf.pdf, 20. oldal
  - IBM DB2 Version 9.7, http://www.commoncriteriaportal.org/files/epfiles/st_vid10336-st.pdf, 23. oldal
  - Microsoft SQL Server 2008 Enterprise Edition, http://www.commoncriteriaportal.org/files/epfiles/0520b.pdf, 49. oldal
- Határvédelmi eszközök:
  - Cisco termékek verziókövetéssel, http://www.commoncriteriaportal.org/files/epfiles/st_vid6016-st.pdf, 15. oldal
  - Check Point termékek verziókövetéssel, http://www.commoncriteriaportal.org/files/epfiles/CheckPoint%20FP1%20ST.pdf,
- Hálózati eszközök:
  - Cisco termékek verziókövetéssel, http://www.commoncriteriaportal.org/files/epfiles/st_vid10313-st.pdf, 19. oldal

Ezek mellett természetesen számtalan egyéb eszköz is a tervezők rendelkezésére áll. Amennyiben a rendszer felépítéséhez Common Criteria tanúsított termékeket használnak, a naplózási követelmények meghatározása egyértelműbb, mint más esetekben.

4 Naplózó infrastruktúrák

4.1 Gyűjtés, elemzés és archiválás

A rendszeradminisztrátorok egyik feladata a belső szabványban leírt naplózási folyamatok végrehajtása. Ebbe beletartozik a naplóforrások beállítása, a naplóelemzés, a reagálás az azonosított eseményekre, valamint a naplóbejegyzések hosszútávú megőrzése.

4.1.1 Naplóforrások beállítása

A naplóforrásokat úgy kell beállítani, hogy a bejegyzések mindig a megfelelő tartalommal, a megfelelő helyen keletkezzenek és a szükséges ideig legyenek megtartva. Ez általában igen komplex feladat. Először azonosítani kell, mely forrásoknak kötelező és melyeknek ajánlott naplóbejegyzéseket létrehozni. Sokszor több forrás egyetlen helyre naplóz (pl. Windows event-ek), ebben az esetben azt is meg kell határozni, hogy ebből az egyetlen naplóállományból milyen események érdekesek.

Log generálás

Feltételezve, hogy a logforrás lehetőséget ad a naplózás finomhangolására, a kezdeti beállításokat kellő körültekintéssel kell megtenni. Előfordulhat ugyanis az, hogy egyetlen forrás olyan mennyiségű adatot generál, amit a felállított infrastruktúra nem tud kezelni. Ez adatvesztéshez vezethet, lelassíthatja, vagy akár teljesen elérhetetlenné teszi a naplózó szolgáltatást, szélsőséges esetben akár a teljes hálózat átviteli sebességére is hathat.

A fenti problémák megelőzése érdekében a naplózást először nem produktív környezetben kell kipróbálni, különösen a leggyakoribb források és a legkritikusabb szolgáltatások esetén. Az egyes gyártók általában tudnak információt adni a naplózással kapcsolatban.

Logtárolás és megsemmisítés

A belső szabványokban el kell dönteni, hogy az egyes logforrások hol tárolják a bejegyzéseiket. Ezt elsősorban a naplózásra és az iratkezelésre vonatkozó belső szabályzat határozza meg, előírva például azt, hogy milyen naplóadatokat kell a központi logtárban gyűjteni. Ha explicit nincsen meghatározva ilyen szabály, az adminisztrátoroknak rugalmas választási lehetőségeik vannak.

- Nincs tárolás: A bejegyzéseknek nincs vagy nem nagy az értékük, ezért nem kell tárolni. Ilyenek lehetnek azok a hibaüzenetek, melyeket csak a szoftver gyártója ért meg, vagy azok a bejegyzések, melyek nem tartalmaznak részletes leírást az eseményről, ezért használhatatlanok.
- Rendszerszintű tárolás: A bejegyzéseknek van információértéke, de általában csak az adott rendszer adminisztrátorának, ezért nem érdemes a központi tárba továbbítani. Ezek az információk kiegészíthetik a központi elemzés során feltárt eseményeket, vagy segíthetnek a rendszeradminisztrátornak az általa felügyelt infrastruktúra trendjeinek megértésében és ez alapján az üzemeltetés finomhangolásában.
- Rendszer és infrastruktúra szintű tárolás: Azok az események tartoznak ide, melyek elég érdekesek ahhoz, hogy mind a keletkezés helyén, mind a központi tárban megőrizzék azokat. Jó indok lehet erre a kettős tárolásra az, hogy ha akár a logforrás, akár a központi infrastruktúra sérül, a másikon még megtalálhatók a bejegyzések, vagy ha egy támadás során a támadó megpróbálja eltűntetni a nyomait a naplóállományból, a másik helyen még megtalálhatók a nyomok.
- Infrastruktúra szintű tárolás: Általában indokolt legalább két helyen tartani a naplóállományokat, de amennyiben ez nem megoldható, mert pl. a logforrás tárolókapacitása kicsi, akkor elégséges csak egy központi helyen tárolni.

Előre meg kell határozni a logrotálás paramétereit is. Ez azt jelenti, hogy a felgyűlt bejegyzéseket csak egy előre meghatározott méretig vagy ideig kell egy naplóállományban gyűjteni, utána ezt archiválni kell. Így garantálható, hogy mindig lesz szabad tárolókapacitás a naplózáshoz. Amennyiben ez nem lehetséges, el kell dönteni, hogy mi történjen a naplózó tárhely betelésénél.

- Naplózás leállítása: ez nem javasolt megoldás, hiszen a rendszer naplózás nélkül működik tovább, így fontos eseményekről nem értesül az üzemeltető. A naplóállomány betelítése ráadásul külső támadások során könnyen elérhető.

- Legrégibb állományok felülírása: Ez elfogadható megoldás kisebb prioritású rendszereknél, vagy ahol a régebbi állományokat már archiválták vagy továbbították a központi tárhelyre. Ha a logrotálás nem megoldható, ez az elfogadható megoldás.
- A logforrás leállítása: Kritikus rendszereket úgy kell konfigurálni, hogy ha nem tudnak naplózni, akkor működésüket fel kell függeszteni, vagy minimális üzemeltetői szinten folytathatják csak működésüket.

A legtöbb naplóforrás riasztja az üzemeltetőt, ha a logtára kezd betelni. Ezeket a riasztásokat komolyan kell venni, az üzemeltetésért felelősnek be kell avatkozni, pl. a logállományokat archiválnia kell. Amennyiben olyan naplóállományok vannak a rendszeren, aminek a megtartási ideje lejárt, azt le kell törölni a rendszerről.

Logok biztonsága

A kockázatok ismeretében fontos lehet a naplóállományok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása. Ezen a téren az alábbi javaslatokat kell megfontolni:

- A naplóállományokhoz történő hozzáférések szabályozása: Az átlagos jogú felhasználók nem férhetnek hozzá a naplóállományokhoz.
- Az érzékeny adatok naplózása: Az érzékeny vagy személyes adatok naplózása nem megengedett. Minden logforrást elemezni kell, hogy tartalmazhatnak-e olyan adatot, mely ebbe a kategóriába tartozik. Személyes adatok naplózásánál a belső adatvédelmi szabályzatnak tartalmaznia kell ezt a tényt is.
- Archivált logállományok védelme: Ebbe tartozik az archivált bejegyzések védelme digitális aláírással, lenyomattal, titkosítással vagy megfelelő fizikai védelemmel.
- Naplóbejegyzések létrehozásának biztonságos módja: Nem jogosult személyek ne manipulálhassák a naplózási folyamatot.
- Biztonságos adatátviteli csatornák használata: Amennyiben lehetséges, mind technikailag, mind terhelési szempontból, a naplóállományokat biztonságos csatornán, pl. SSL megoldással kell eljuttatni a logforrásból a központi infrastruktúrába.

4.1.2 Reagálás az azonosított eseményekre

A naplóelemzés célja, hogy olyan eseményekre derüljön fény, amik egyébként rejtve maradnának. Amikor az elemzéssel megbízott személy valamilyen visszaélésre vagy hibára derít fényt, az incidenskezelési eljárási szabályzat szerint kell intézkednie. Ehhez olyan képzést és eszközöket kell kapniuk, melyek segítik a hatékony reagálást. Az adminisztrátoroknak nem feltétlenül feladata a reagálás koordinálása, de mindenképpen részt kell venniük benne. Az incidenskezelésre a későbbiekben még visszatérünk.

4.1.3 Hosszútávú megőrzés

A naplóállományok hosszútávú megőrzését elsősorban a belső előírások (pl. iratkezelési szabályzat) határozzák meg. Amennyiben központi naplózó infrastruktúra működik, a logforrásokon nem szükséges hosszú ideig tárolni a bejegyzéseket. A központi infrastruktúra logjait azonban akár évekig is meg kell őrizni. Ebben az esetben az alábbi szempontokat érdemes figyelembe venni.

- Az archiválási formátum megfelelő kiválasztása: Lehetséges valamilyen általános formátumban történő tárolása, vagy a logforrás saját formátumban történő archiválás. Az általános formátumot a későbbiekben könnyebben lehet feldolgozni, de a saját formátumban biztosan nincsen konverzió miatti adatvesztés.
- A logadatok archiválása: El kell dönteni, hogy milyen médián történik a tárolás (DVD, szalag, SAN, stb.). Ehhez figyelembe kell venni, hogy mennyi ideig kell megoldani az archiválást. Nem mindegy ugyanis, hogy egy gyártó meddig vállalja az adatok megőrzését a médián, illetve az, hogy rendelkezésre fog-e állni olyan berendezés az évek múltán, amivel a médiát ki lehet olvasni.
- A logok integritásának folyamatos ellenőrzése: A hosszútávú megőrzés egyik kulcskérdése a bejegyzések sértetlenségének biztosítása. Ez megvalósítható lenyomatokkal vagy digitális aláírással.
- A tárolómédia biztonságos tárolása: Ahogy minden archiválási média esetén, gondoskodni kell arról, hogy az archívumhoz csak az arra jogosult személyek férhetnek hozzá, illetve megfelelő fizikai környezetben történik a tárolás.

4.1.4 Tesztelés és validálás

A szervezetnek rendszeresen ellenőriznie kell, hogy a naplózási szabályzatok és eljárások megfelelnek-e az elvárásoknak, hatékonyan csökkentik-e a kockázatokat, valamint az üzemeltetés betartja-e a leírtakat. A logmenedzsment auditok segítenek a hiányosságok feltárásában. A leggyakoribb technikák a következők:

- Passzív: Az auditorok áttekintik a naplózási beállításokat, a rendszerlogokat, az infrastruktúralogokat, az archívumokat, így egy reprezentatív mintát kapnak a szabályok teljesüléséről.
- Aktív: Az auditorok olyan biztonsági eseményeket végeznek a rendszerekben, amik naplózást váltanak ki, így jutnak reprezentatív mintához a naplózás hatékonyságáról.

Leggyakrabban a passzív mintavételezést szokták alkalmazni. Az aktív mintavételezés ugyan hatékonyabb, de sokkal több erőforrást igényel, valamint megvan annak a kockázata, hogy pl. egy behatolási tesztelés esetén a rendszerben fennakadások lesznek.

4.2 Tervezési peremfeltételek

A szervezetnek meg kell határoznia azokat a követelményeket és célokat, melyekkel eleget tud tenni a belső elvárásoknak, szabályzatoknak, valamint a hatályos jogszabályoknak. A célokat a kockázatokhoz kell mérni, azaz éppen annyi erőforrást kell felhasználni a logmenedzsment kialakítására, amennyi érdemben, hatékonyan tudja csökkenteni az azonosított kockázatokat. A szabályzatoknak tartalmaznia kell a kötelező elvárásokat és az ajánlott célokat is. Ezt a szabályzatot összhangba kell hozni a szervezet más szabályzataival is.

A következő információkat javasolt a szabályzatban rögzíteni:

- Naplóállomány létrehozása
    - Mely hosztoknak kötelező és melyeknek ajánlott naplóbejegyzéseket létrehozni?
    - Mely rendszerkomponenseknek (pl. operációs rendszer, szolgáltatás, stb.) kötelező vagy ajánlott naplózni?

- Milyen eseménytípusokat (pl. biztonsági események, hálózati események, stb.) kötelező vagy ajánlott naplózni?
- Milyen tartalmat kell naplózni (pl. felhasználónév, forrás IP cím, stb.)?
- Milyen gyakorisággal kell a naplóbejegyzést létrehozni (pl. minden bekövetkezésnél, percenként x alkalommal)?

- Naplóbejegyzések továbbítása
  - Mely forrásoknak kell a központi naplózó infrastruktúrába továbbítania a bejegyzéseket?
  - Milyen típusú bejegyzéseket kell a központi naplózó infrastruktúrába továbbítani?
  - Milyen módon kell a bejegyzéseket továbbítani (pl. milyen protokollon), és mi a teendő nem hálózatba kötött rendszereknél?
  - Milyen gyakran kell a központi egységbe továbbítani a naplóállományokat (pl. real-time, 5 percenként)?
  - Hogyan lehet gondoskodni a továbbítás sértetlenségéről, bizalmasságáról és rendelkezésre állásáról?

- Naplóállományok tárolása és törlése
  - Milyen gyakran kell a naplóállományokat rotálni?
  - Hogyan lehet a naplóállományok bizalmasságáról, sértetlenségéről és rendelkezésre állásáról gondoskodni a tárolás alatt?
  - Mennyi ideig kell egy naplóbejegyzést megőrizni (a logforráson és a központi infrastruktúrában)?
  - Hogyan kell a már szükségtelen naplóállományokat megsemmisíteni?
  - Hogyan kell kezelni a logokat tároló háttértár szabad kapacitását?
  - Hogyan lehet megoldani a bejegyzések bizonyító erejét?

- Logelemzés
  - Milyen gyakran kell a logelemzést elvégezni?
  - Kinek van joga hozzáférni a naplóadatokhoz és ezt a hozzáférést milyen módon kell naplózni?
  - Mit kell tenni azonosított vagy gyanított esemény esetén?
  - Hogyan lehet a logelemzés eredményének bizalmasságát, sértetlenségét és rendelkezésre állását biztosítani?
  - Hogyan lehet az érzékeny adatokat, mint pl. e-mail tartalmakat a naplóbejegyzésekben rögzíteni?

Példa lehet a szabályzatban foglaltakra az alábbi táblázat.

Kategória	Alacsony kockázatú rendszerek	Közepes kockázatú rendszerek	Nagy kockázatú rendszerek
Meddig kell megőrizni a naplóállományokat?	1-2 hét	1-3 hónap	3-12 hónap
Mikor lehet a	Opcionális (ha	Legalább 6-24	Legalább 15-60

logokat rotálni?	kell, legalább hetente vagy legalább 25 MB-onként)	óránként, legalább 2-5 MB-onként	percenként, legalább 0,5-1 MB-onként
Mikor kell a logokat a központi naplózóba küldeni?	Legalább 3-24 óránként	Legalább 15-60 percenként	Legalább 5 percenként
Milyen sűrűn kell a bejegyzéseket elemezni?	Legalább 1-7 naponta	Legalább 12-24 óránként	Legalább naponta hatszor
Szükséges a naplóállományok sértetlenségét ellenőrizni?	Opcionális	Igen	Igen
A rotált állománykat kell titkosítani?	Opcionális	Opcionális	Igen
Titkosított csatornán kell az állományokat a központi infrastruktúrába küldeni?	Opcionális	Igen, ha lehetséges	Igen

A naplózási szabályzatnak meg kell felelnie a törvényeknek. Egyrészt teljesítenie kell az elektronikus közigazgatási rendszerekre vonatkozó követelményeket, másrészt azonban figyelembe kell venni az adatvédelmi törvényt is. Ez a két jogszabályhalmaz erős határokat szab a naplózás tartalmára vonatkozóan. A pontos naplótartalom meghatározása tehát nem csak műszaki, hanem jogi kérdés is.

A digitális nyomrögzítés egyik alapkérdése az, hogy egy cselekményt bizonyító bejegyzések elégségesek-e a központi naplótárban vagy meg kell-e őrizni azokat a keletkezésük helyén is. Amennyiben a logokra, mint bíróság előtt megálló bizonyítékokra gondolunk, fontos azokat a keletkezés helyén is megőrizni, vagy legalábbis azok pontos másolatát kell bemutatni. A logok feldolgozott formájukban információt szolgáltatnak a belső ellenőrzéshez, de nem állják meg a helyüket a bíróság előtt. Amennyiben az eredeti állományok megőrzése igény, ezekre külön szabályzatot kell kidolgozni, mely tartalmazza például a letagadhatatlan tárolás folyamatát (digitális aláírással vagy WORM médián).

4.3 Protokollok

A naplók formája rendszerenként eltérő lehet, kerülhetnek fájlba vagy adatbázisba, lokálisan vagy hálózaton keresztül, de van néhány olyan gyakori protokoll szabvány, amikre építve egységes naplózási rendszer tervezhető. A három leggyakoribb naplózási protokoll a syslog, a Windows Event Log és az SNMP.

A syslog elsősorban naplóüzenetek továbbítására használatos IP hálózatokban, ezért kliens-szerver felépítésű. az 1980-as évek óta használják, elsősorban *nix alapú rendszerekben és hálózati eszközökben. A syslog kliens kicsi, kb. 1 kB méretű üzeneteket küld a syslog szerver részére, melyet syslogd-nek vagy syslog daemonnak neveznek. Az üzenet tartalmára minimális megkötések vannak, ezért rugalmas, de éppen ezért nehezen feldolgozható heterogén környezetben. Az üzenet hagyományosan UDP protokollon közlekedik, de az újabb szabványok lehetőséget adnak a TCP feletti küldésre is. A tartalom nem titkosított, ezért kritikus bizalmasságú esetekben SSL felett szokták továbbítani. Jelenleg az RFC 5424 szabvány határozza meg a működését.

A Windows Event Log a Microsoft által használt naplózási formátum, melyet 1993-ban, a Windows NT-ben vezettek be először. Alapvetően három forrásból származhatnak a bejegyzések: a rendszerből (System), az alkalmazásoktól (Application) és a biztonsággal kapcsolatos szolgáltatásoktól (Security). Az aktuális változata XML formátumú naplókat hoz létre, melyek megkönnyítik a gépi feldolgozást. Az egyes operációs rendszerből származó események egyedi azonosítót kapnak. Elsősorban helyi naplózásra alkalmas, a hálózaton keresztüli begyűjtésre azonban számos eszköz áll rendelkezésre.

A Simple Network Management Protocol (SNMP) nem elsősorban naplózási protokoll, de olyan információkat tartalmaz, melyek segítik a rendszer biztonságos működésének figyelését, így fontos része a naplózási infrastruktúrának. UDP alapú protokoll, leggyakrabban a hálózati eszközök működésének megfigyelésére használják. Jelenleg az RFC 3411-3418 közötti szabványok határozzák meg a működését, ez az SNMPv3. Megtalálható benne az üzenetek integritásvédelme, az authentikáció és a titkosítás is.

5 Alkalmazásnaplók

5.1 Common Criteria követelmények

A Common Criteria szabvány kitűnő forrás lehet egy termék vagy rendszer biztonsági naplózási követelményeinek összeállításához. Egy teljes ún. család foglalkozik a naplózással kapcsolatos funkcionális követelményekkel, emellett minden egyes biztonsági funkcióhoz meghatározza a naplózandó eseményeket, melyek rugalmasan választhatók ki.

A FAU osztály, melynek címe a szabvány magyar fordításában Biztonsági átvilágítás, összesen 6 területre osztja a logolással kapcsolatos tevékenységeket:

- Automatikus válaszadás: milyen eseményeket kell megtenni akkor, amikor lehetséges biztonsági szabálysértést észlel a rendszer. Egyfajta IDS működést ír elő.
- Naplóadatok létrehozása: meghatározza, hogy milyen típusú tevékenységeket kell rögzíteni, milyen minimális információtartalommal, hogy az jól használható legyen. Ez a funkció hozza létre a naplóbejegyzéseket.
- Biztonsági naplóelemzés: olyan automatikus tevékenységek felsorolása, melyek segítenek a rendszer tevékenységéből és naplóadataiból kiszűrni a vélt vagy valós biztonsági tevékenységeket.
- Biztonsági naplóadatok áttekintése: annak meghatározása, hogy milyen módon lehet a jogosult felhasználónak lehetővé tenni a naplóadatok megtekintését. Praktikusan a naplóbejegyzések felhasználói felületére vonatkozó követelmények tartoznak ide.

- Naplóesemények kiválasztása: azon lehetőségek felsorolása, melynek segítségével a logok halmazából egy adott tulajdonsággal rendelkező eseményeket ki lehet választani. Gyakorlatilag a riportkészítés követelménye.
- Események tárolása: a logállományok létrehozásának és tárolásának feltételeivel foglalkozó követelmény.

Az egyes biztonsági funkciók naplózási szintjét minimális, alap, részletes és nem meghatározott szinten lehet előírni. Minden egyes Common Criteria 2. kötetben meghatározott biztonsági funkcióhoz leírták, hogy ezen a három szinten mit kell naplózni. A FIA_SOS.1 komponens esetén, mely például a megfelelően erős jelszavak kikényszerítéséért felelős biztonsági funkciót írja le, minimálisan naplózni kell a visszautasított jelszógenerálási kísérleteket, alap szinten az elfogadott kísérleteket is, részletes szinten pedig ezek mellett a jelszóerősségi beállításokhoz képest történő minden változtatást is.

5.2 Minimális naplózási követelmények alkalmazásokban

Általában nehézséget okoz az e-közigazgatási rendszerek biztonsági naplózásának meghatározása. A Common Criteria követelményrendszerének figyelembevételével azonban pontosan leírható, hogy az alkalmazás fejlesztőjének minimálisan mit kell teljesítenie. A közigazgatási ajánlások és a jogszabályi követelmények is általában ebből indulnak ki.

- Az alkalmazásnak naplóznia kell (FAU_GEN.1.1):
  - A naplózási funkció elindulását és leállítását,
  - A rendszer biztonsági besorolástól függően minimális, alap vagy részletes szinten a kiválasztott biztonsági funkcióknál meghatározott eseményeket
- A naplóbejegyzésnek tartalmaznia kell (FAU_GEN.1.2):
  - Az esemény dátumát és idejét, típusát, a kiváltó felhasználói azonosítót és az esemény kimenetét.
- Amennyiben az alkalmazás teszi lehetővé a naplóadatok megtekintését, gondoskodni kell arról, hogy csak megfelelő jogosultsággal rendelkező felhasználók férjenek hozzá az adatokhoz (FAU_SAR.1.1).
- A bejegyzéseket felhasználó által is olvasható módon kell megjeleníteni (FAU_SAR.1.2).
- Lehetővé kell tenni, hogy az eseményeket szűrni lehessen a felhasználónév, host név és esemény típus alapján (FAU_SEL.1.1).
- A naplóállományokat meg kell védeni a nem jogosult törlési kísérletekkel szemben (FAU_STG.1.1).
- A naplóállományokat meg kell védeni a nem jogosult módosítástól is (FAU_STG.1.2).
- Amennyiben a naplózásra szánt tárterület 90%-ban betelt, azonnali riasztásokat kell küldeni az operátoroknak. Amennyiben a tárterület 95%-a betelt minden operatív modult automatikusan le kell állítani, hogy csak minimális naplózás tevékenység történjen (FAU_STG.3.1).

6 Adminisztratív eljárások

6.1 Üzemeltetési eljárások

A logkezelési eljárás részeként meg kell határozni azokat a szerepköröket és felelősségeket, amiket a folyamatban érintett személyeknek és csoportoknak be kell töltenie. Általában a következő szerepköröket kell kiosztani:

- Rendszer és hálózati adminisztrátorok, akiknek be kell állítaniuk a naplózást az egyedi rendszereken és hálózati eszközökön, valamint ezeket a logokat át kell nézniük, és jelenteniük kell ennek eredményét. Emellett rendszeresen karban kell tartaniuk a naplóállományokat és a naplózó szoftvert.
- Biztonsági adminisztrátorok, akik a logmenedzsment infrastruktúra kezeléséért és konfigurálásáért felelősek, ők állítják be a biztonsági infrastruktúra elemeinek (pl. tűzfal, IDS, antivírus szerver) naplózását, jelentik a tevékenységük eredményeit, valamint támogatják a többi szerepkört a naplózás beállításában.
- Biztonsági incidenseket kezelő csoport (CSIRT, Computer Security Incident Response Team), akik a naplóállományokat a felfedezett incidensek kezelésében használják fel.
- Alkalmazásfejlesztők, akiknek úgy kell az alkalmazásokat létrehozni és személyre szabni, hogy a naplózás megfeleljen a leírt követelményeknek és ajánlásoknak.
- IT biztonsági felelős, aki felügyeli a naplózó infrastruktúra működését.
- IT vezető, aki felelős az összes IT erőforrásért, ami naplóbejegyzést hoz létre, továbbít vagy tárol.
- Auditorok, akik az auditok során használják fel a naplóállományokat.
- Beszerzési felelősök, akik olyan dobozos szoftverek beszerzéséért felelnek, melyek biztonságilag releváns naplóbejegyzéseket hoznak létre.

Ezeknek a szerepköröknek az összevonása attól függ, hogy mennyire lehet központosítani a naplózási folyamatot. Amennyiben nincs lehetőség központi logmenedzsment bevezetésére, általában a hálózati, biztonsági és rendszeradminisztrátorok felelősek a rájuk bízott rendszer teljes logmenedzsment folyamatának elvégzéséért a szabályzatokban leírtaknak megfelelően. A centralizált működési modellben az egyes egyedi rendszerek üzemeltetőire sokkal kisebb felelősség hárul.

Ilyenkor a biztonsági adminisztrátorok feladata elsősorban az infrastruktúra üzemeltetése a következő felelősségi körökkel:

- Együttműködés a logforrásként működő rendszerek üzemeltetőivel egy-egy esemény megértésében, valamint kivizsgálásában.
- A logforrásban szükséges változtatások azonosítása (pl. milyen adatokat, milyen formában, milyen adattartalommal küldjön), és a rendszeradminisztrátorok értesítése ezekről a változásokról.
- Beavatkozás kezdeményezése egy-egy azonosított biztonsági eseménnyel kapcsolatban.
- Gondoskodás a logok archiválásáról valamint a tárolási idő leteltével biztonságos megsemmisítéséről.
- Együttműködés az auditorokkal, nyomozó hatóságokkal, és más érintett vizsgáló szervekkel.

- A logmenedzsment infrastruktúra megfelelő működésének folyamatos ellenőrzése és szükség esetén a javítások kezdeményezése.
- Az infrastruktúra elemeihez kiadott frissítések tesztelése és implementálása.
- A naplózó rendszer biztonságának folyamatos biztosítása.

További fontos feladat a logmenedzsment infrastruktúra adminisztrátorának az egyes logforrás rendszerek adminisztrátorainak ellenőrzése. Amikor megszületik a döntés a naplózásért felelős szerepkör létrehozásáról, az elszámoltathatóság kérdése is felmerül. Például egy biztonsági adminisztrátor meg tud róla győződni, hogy a logforrás rendszergazdája valóban beállította-e a naplózást a szabályoknak megfelelően. A szerepkörök ilyen szétválasztása – bár plusz erőforrást jelenthet – a biztonsági szintet jelentősen növeli. Ebben az esetben is a kockázatarányos védelmet javasolt tehát választani, azaz át kell tekinteni az egyes rendszerek által kezelt információk értékét, és a legfontosabb elemek esetében mindenképpen javasolt különválasztani az üzemeltető és az ellenőrző szerepköröket.

Annak érdekében, hogy a naplókezelés az egész szervezeten belül azonos hatékonysággal működjön, az egyes rendszeradminisztrátoroknak hozzá kell jutni a szükséges információkhoz. Általában a következő lépések szükségesek ehhez:

- A naplózással kapcsolatos információk hozzáférhetővé tétele és oktatások tartása a logforrásként működő rendszerek adminisztrátorainak.
- Olyan személy kijelölése, aki választ tud adni a naplózással kapcsolatos kérdésekre.
- Az adminisztrátorok véleményének, tapasztalatainak meghallgatása, pl. belső levelezőlistán.
- Olyan rendszerspecifikus technikai ajánlások rendelkezésre bocsátása, melyek leírják az adott rendszer integrációjának módját.
- Meg kell fontolni egy teszt naplózó rendszer felépítését is, ahol a különböző rendszereket különböző beállítások mellett lehet kipróbálni, és így hatékonyabbá tenni a logmenedzsment infrastruktúrát.
- A naplózást segítő eszközök (pl. logrotáló szkriptek, elemző alkalmazások) hozzáférhetővé tétele a dokumentációkkal együtt.

6.2 Incidenskezelés

A biztonsági incidensek kezelése fontos, de Magyarországon kevéssé ismert területe az informatikai biztonságnak. A biztonságilag fontos fenyegetések nem csak számban, hanem a károkozás nagyságában is egyre jelentősebbek. Napról napra újabb fenyegetések jelennek meg, melyekre nem feltétlenül van meg a szervezetnél a megfelelő megelőző védelem. Az incidenskezelési eljárás segítségével azonban a nem kivédhető támadások, esetleges csalások észlelése és a károk minimalizálása és a működés mielőbbi visszaállítása hatékonyan támogatható.

A folyamat bevezetése nem egyszerű, komplex tervezést igényel, valamint új erőforrásokat is. Használata feltételezi a működő naplózási és naplóelemzési folyamatok meglétét. Bevezetésének a folyamat a következő.

- Az incidenskezelési képesség megteremtése
    - Incidenskezelési szabályzatok és eljárások kidolgozása
    - Incidenskezelési csapat felállítása, akár outsource-olt erőforrások bevonásával

    - A csapatot támogató belső erőforrások kijelölése
- Általános incidenskezelési eljárás kidolgozása az előkészületektől az incidens elhárítása utáni értékelésig és büntetőfeljelentésig.
- Speciális események kezelésének leírása
    - Túlterheléses támadások (Denial of Service – DoS)
    - Kártékony kódok
    - Nem jogosult hozzáférés
    - Nem megfelelő használat
    - Összetett támadások elhárítása

A formális incidenskezelési képesség kialakításában segítséget nyújthat a Cert-Hungary Központ, mely a közigazgatáson belül látja el ezt a feladatot. A velük való formális együttműködés az elektronikus közigazgatási szolgáltatást nyújtó szervezeteknek több, mint ajánlott.

6.3 Büntetőeljárás (1 oldal)

A magyar jogrend már évek óta foglalkozik az elektronikus úton keletkezett bizonyítékok kezelésének szabályaival, a gyakorlatban azonban mégsem alakult ki az az egyértelmű műszaki megoldás, aminek segítségével a naplóállományok bizonyítékként fel lehetne használni. A 1998. évi XIX. törvény a büntetőeljárásról 115. § (1) szerint „Tárgyi bizonyítási eszköz minden olyan tárgy (dolog), amely a bizonyítandó tény bizonyítására alkalmas, így különösen az, amely a bűncselekmény elkövetésének vagy a bűncselekmény elkövetésével összefüggésben az elkövető nyomait hordozza, vagy a bűncselekmény elkövetése útján jött létre, amelyet a bűncselekmény elkövetéséhez eszközül használtak, vagy amelyre a bűncselekményt elkövették. A (2) szerint „E törvény alkalmazásában tárgyi bizonyítási eszköz az irat, a rajz és minden olyan tárgy, amely műszaki, vegyi vagy más eljárással adatokat rögzít. Ahol e törvény iratról rendelkezik, ezen az adatot rögzítő tárgyat is érteni kell.” Ennek tehát megfelel az elektronikus formában keletkezett naplóállomány.

Problémát jelent azonban, hogy milyen módon lehet ennek a naplóbejegyzésnek a sértetlenségét biztosítani. Ugyanennek a törvénynek a 158/A. §-a foglalkozik a számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezésről. Ennek (3) szerint „A megőrzésre kötelezett a határozat vele történő közlésének időpontjától köteles a határozatban megjelölt számítástechnikai rendszer útján rögzített adatot változatlanul megőrizni, és - szükség esetén más adatállománytól elkülönítve - biztosítani annak biztonságos tárolását. A megőrzésre kötelezett köteles a számítástechnikai rendszer útján rögzített adat megváltoztatását, törlését, megsemmisülését, valamint annak továbbítását, másolat jogosulatlan készítését, illetőleg az adathoz való jogosulatlan hozzáférést megakadályozni.” A (4) szerint „A megőrzésre kötelezést elrendelő a megőrzéssel érintett adatot fokozott biztonságú elektronikus aláírással láthatja el. Ha az adat eredeti helyen történő megőrzése az érintettnek az adat feldolgozásával, kezelésével, tárolásával vagy továbbításával kapcsolatos tevékenységét jelentősen akadályozná, az elrendelő engedélyével az adat megőrzéséről annak más adathordozóra vagy más számítástechnikai rendszerbe történő átmásolásával gondoskodhat. Az átmásolást követően az elrendelő az

eredeti adatot tartalmazó adathordozóra és számítástechnikai rendszerre a korlátozásokat részlegesen vagy teljesen feloldhatja."

Bár ez a paragrafus nem konkrétan a tanulmány elsődleges tárgyával foglalkozik, mégis útmutatást ad arra, hogy milyen körülmények között kell a naplóállományokat tárolni, hogy azok bizonyítékként felhasználhatók legyenek. Az elsődleges feladat nyilvánvalóan a sértetlenség biztosítása, melyre javasolt a fokozott biztonságú elektronikus aláírás használata. Ez praktikusan azt jelenti, hogy minden logrotálásnál a rotált fájlt elektronikusan alá kell írni és lehetőleg időbélyegezni kell. További lehetőségeket mutat be a 2/2002. (IV. 26.) MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről 63. pontja, mely szerint „A naplóadatok sértetlenségének védelme érdekében a megbízható rendszereknek gondoskodniuk kell olyan eszközről és eljárásról (így különösen elektronikus aláírás, kulcsolt lenyomatfüggvény, hitelesítési kód), mely a napló, illetve naplóbejegyzések módosításának kimutatására alkalmas."

Önmagukban természetesen a naplóállományok sem mindig lehetnek kizárólagos bizonyítóeszközök, ám a megfelelően zárt és a sértetlenséget megoldó rendszerekben készült bejegyzések erős támogatást nyújthatnak egy bírósági tárgyalás során.

7 Összefoglalás

A megfelelő naplózás kialakítása számos feltétel együttes teljesítésétől függ, nem lehet pusztán technológiára alapozni. A helyes megközelítés szerint az adminisztratív és műszaki intézkedések harmóniáját kell elérni, mely minden más információbiztonsági intézkedéshez hasonlóan kockázatarányosan alakul ki. A piacon elérhető naplózási keretrendszereket az adott szervezetre kell szabni, azok önmagukban nem csökkentik a biztonsági kockázatokat.

Az elektronikus közigazgatási rendszerekben ez fokozottan igaz. Az egymással sok esetben szervezeten belül és kívül is együttműködő szakrendszerek olyan bonyolult infrastruktúrát alkotnak, melyekben a támadások, visszaélések vagy működési hibák könnyen észrevétlenek maradhatnak. Egy ilyen incidens viszont a közigazgatáson belül nagy kiterjedésű zavarhoz vezethet. A naplózás csak egy, de igen fontos eleme az informatikai eredetű hibák megelőzésének, felfedezésének és javításának.

8 Idézett forrásmunkák

Common Criteria Development Board. (2009., július). Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1.

International Organization for Standardization. (2008., április 22.). ISO/IEC 27002:2005 Code of practice for information security management.

IT Governance Institute. (2007). *Control Objectives for Information and related Technology (COBIT®).* Rolling Meadows, IL 60008 USA: IT Governance Institute.

IT Governance Institute. (2007., február 20.). Mapping of ISO/IEC 17799:2005 With COBIT® 4.0. Rolling Meadows, Illinois, USA.

Közigazgatási Informatikai Bizottság. (2009., március 24.). E-Közigazgatási Követelménytár. Budapest.

National Institute of Standards and Technology. (2006., szeptember). Guide to Computer Security Log Management, Special Publication 800-92. Gaithersburg, Maryland, USA.

Pénzügyi Szervezetek Állami Felügyelete. (2007, október). 1/2007. számú módszertani útmutató a pénzügyi szervezetek informatikai rendszerének védelméről. Budapest.