Az informatikai rendszerek naplózása

Sági Gábor[10]

Absztrakt: Az informatikai rendszerek működése során a rendszerekben zajló eseményekről nap, mint nap rengeteg naplóbejegyzés készül, amelyek gyűjtés, elemzése a jogszabályi megfelelés mellett hatékony segítséget nyújt a szervezet informatikai rendszerét ért sikeres támadás feltárásához, az események rekonstruálásához, de támogatást adhat folyamatban lévő támadás azonosításához is. Ugyanakkor sem az államigazgatásban, sem piaci környezetben nem alakult ki egységes gyakorlat a naplózási funkció működtetésével kapcsolatban, így az állami szervezetek sok esetben ma még csak a jogszabályi elvárás teljesítése érdekében működtetnek naplógyűjtő, elemző rendszert. A szerző jelen cikkében bemutatja az informatikai rendszerekben zajló tevékenységek naplózásával kapcsolatos nemzetközi és hazai jogszabályokban, valamint szabványokban megfogalmazott elvárásokat. Továbbá javaslatot tesz a naplózásba bevonandó rendszerek körére, bemutatja, hogyan lehet megállapítani, hogy egy szervezet milyen érettségi szinten van informatikai rendszereinek naplózásával kapcsolatban, illetve milyen kérdésekre kell választ adnia a naplózási képesség kialakítása során. Bemutatásra kerül továbbá, hogy egy rendszerben keletkező naplóbejegyzés, miként kerülhetnek feldolgozásra, egy eseményből milyen módon lesz információbiztonsági incidens.

Kulcsszavak: naplógyűjtés, naplóelemzés, naplózás

Abstract: During the operation of IT systems in systems taking place every day a lot of logs made to the collection, analysis, in addition to the legal requirements is the only way the organization's IT system has successfully attack detection, and large can help to identification an ongoing attack.Neither the state administration nor the market environment is no common practice in the operation of the logging function. And there is no established best practice to uniformly used, in many cases the organizations operate only log collection, analysis system in order to meet the legal requirements.
The author of this article presents international and national legislation and standards related expectations of logging functions of information systems activities. The author proposes a range of systems which should be involve in the logging systems, and demonstrates that an organization's logging maturity level related to the IT systems and what kind of questions to be answered in the development of the logging function. Also on display will be that generated a system log entry, how it is processed the way in which it becomes an information security incident.

Keywords: log collection, log analyses, logging

[10] *NKE doktorandusza, e-mail: gabor.sagi@yahoo.com, ORCID azonosító: 0000-0002-4473-0895*

Bevezetés

Az informatikai rendszereket üzemeltető, használó vállalatoknak két információbiztonsági érintettségű kihívást kell teljesíteniük. Az első a szervezet tevékenységtől függő jogszabályi megfelelés, amely hivatott bizonyítani, hogy a szervezet a tőle elvárható módon mindent megtesz az informatikai rendszereinek biztonságos üzemeltetése érdekében. A második – és talán sokkal nagyobb – kihívást az informatikai rendszerek gyakorlati napi védelme jelenti. Ezen két kihívás – bár szorosan kapcsolódnak egymáshoz – sok esetben teljesen más megközelítést igényelnek.

Az elektronikus információs rendszerek biztonságával kapcsolatos jogszabályi megfelelés biztosítása során számos előre meghatározott követelménynek kell megfelelni, amelyeket a vállaltok jelentős mértékű erőforrás befektetéssel törekednek is biztosítani. Az információbiztonsági követelményeknek történő megfelelés az alapja, hogy a szervezet információbiztonság felügyeletét ellátó hatóságok engedjék a tevékenység indítását, folytatását, így egy esetleges nem megfelelés komoly büntetést vagy akár a tevékenység megszűnését is jelentheti. A jogszabályi megfelelés mellett, számos – elsősorban - nagyvállalat az informatikai biztonsági tevékenység átláthatóságának érdekében irányítási rendszert működtet, amely a gyakorlati hasznon túl, marketing erővel is bír.

Ugyanakkor az elmúlt időszakban informatikai rendszerek ellen végrehajtott sikeres támadások, legyen szó akár pénzügyi rendszerek, akár ipari irányító rendszerek, vagy egyéb széleskörben használt szolgáltatások elleniről, bebizonyították, hogy a jogszabályi megfelelés önmagában nem elegendő az informatikai rendszerek sikeres megvédéséhez. A tapasztalatok azt is mutatják, hogy az informatikai rendszerek hatékony védelme szinte megoldhatatlan feladat elé állítja az infrastruktúra üzemeltetőket, köszönhetően az emberi tényezőnek, az informatikai rendszerek hibáinak, valamint a védelmi rendszerek sok esetben nem elég hatékony működésének, működtetésének.

Széles szakmai körben egyre elfogadottabbá kezdenek válni azok az elhíresült mondatok, amelyek a vállalatok áldozattá válását jósolják. John Chambers (CISCO vezérigazgató) szerint „Két fajta vállalat létezik: akit már sikeresen megtámadtak, és akit még nem,”[11] ami egyben azt is jelenti, hogy véleménye szerint nem az az igazi kérdés, hogy meg fogják-e a vállalatot sikeresen támadni, hanem az, hogy mikor.

Az úgynevezett APT[12] jellegű támadások elemzése kapcsán egy másik kérdés is felmerülhet: tudjuk-e egyáltalán, hogy sikeres támadást hajtottak végre

[11] *Joseph MUNIZ, Gary MCINTYRE, Nadhem ALFARDAN: Security Operations Center: Building, Operating, and Maintaining your SOC p. 24. CISCO PRESS 2015 ISBN-10: 0-13-405201-3*

[12] *APT: APT (Advanced Persistent Threat) olyan támadássorozat, melynek célja nem a károkozás, hanem a folyamatosan fenntartott rejtett jelenlét és információszerzés*

vállaltunk ellen. Könnyen meglehet, hogy a védelemre szánt rendszerek nem ismerték fel sem a behatolást, sem a támadó folyamatban lévő tevékenységét, így a támadás tényéről csak késve, a sikeres támadás publikálása után vagy egy zsarolás jellegű megkeresés után értesülünk. Az információszerzésre szakosodott támadásoknál a támadás feltételezett kezdete és annak észlelése között általában hosszú idő telik el, azaz ennyi ideig áll fenn az információszivárgás. A sok esetben, hónapokban, sőt években mérhető.[13]

Mind a jogszabályi megfelelés, mind egy támadás felismerésének és a biztonsági események utólagos vizsgálatának elengedhetetlen feltétele, hogy az informatikai rendszerekben történt eseményekről naplóbejegyzések készüljenek, amelyeket helyben vagy az informatikai rendszertől távol (központi helyen) kerülhet eltárolásra, feldolgozásra.

Egy támadás során a támadó végig haladva a támadás láncon számos nyomot hagy az informatikai rendszerekben. Ezen nyomok egy része akár alkalmas is lehet a támadás felfedésére, ha a támadáskor mutatott viselkedés, vagy a támadásra használt kód ismert a védelmi rendszer számára. Ugyanakkor a fejlett támadások során alkalmazott technikák, kódok a korszerű védelmi rendszerek számára is láthatatlanok maradhatnak, ám egy nyomozás során, amikor célirányosan keresünk, ezek a naplóadatok is jól felhasználhatók. A támadás felfedezése utáni elemzési fázisban az egyes rendszerekben keletkezett bejegyzések ugyanis nagymértékben hozzájárulhatnak a támadás karakterisztikájának megismerésében, a károk megállapításában, valamint ebből következően a védelem felkészítésében hasonló támadások megelőzésére. Ahhoz azonban, hogy a védelemnek valóban hatékony része legyen a naplózási képesség, számos feltételnek kell teljesülnie, mind szervezeti, folyamati mind technikai oldalon.

Nemzetközi kitekintés

Az egyes nemzetközi szabványok, előírások eltérő részletezettséggel foglalkoznak az informatikai rendszerekben zajló tevékenységek naplózásával, a naplótartalmak elemzéséve, az elemzés során feltárt incidensek kezelésével.

Jelen cikkben a számos nemzetközi szabványból az MSZ ISO/IEC 27001: 2014,[14] mint hazánkban legelterjedtebb információbiztonsági tanúsítási szabvány, valamint a NIST által kiadott Security and Privacy Controls for Federal In-

(Forrás: http://www.t-systems.hu/megoldasok/infrastruktura/felugyelt-es-biztonsagos/apt-vedelmi-megoldasok.)

[13] KOVÁCS Zoltán: Információgyűjtés – A kibertér felhasználása. In: A nemzetbiztonság technikai kihívásai a 21. században Szerk.: BODA József – DOBÁK Imre. Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet. Budapest 2015. pp. 123-135. ISBN: 978-615-5527-74-6

[14] MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika Információbiztonság-irányítási rendszerek Követelmények

formation Systems and Organizations SP 800-53r4,[15] mint a hazai szabályozás forrása kerül részletesebben bemutatásra.

Az ISO 27001 szabvány egy követelményszabvány, mely az információbiztonsági irányítási rendszer (ISMS 7) kialakításához, megvalósításához, működtetéséhez, figyelemmel kíséréséhez, átvizsgálásához, fenntartásához és fejlesztéséhez szükséges követelményeket írja le.[16] A szabvány A.12.4 „Naplózás és megfigyelés" pontja 4 követelményt fogalmaz meg a naplózással kapcsolatban:

- eseménynaplózás (event logging): amely előírás szerint a felhasználói tevékenységekről, kivételekről, hibákról és információbiztonsági eseményekről kell naplóbejegyzést készíteni, és megtartani,
- naplóinformációk védelme (protection of log information): mely előírás szerint a naplózó eszközt valamint a napló állományokat meg kell védeni a jogosulatlan módosítás, illetve a hozzáféréssel szemben,
- adminisztrátori és operátori naplók (administrator and operator logs): az előírás szerint a két kiemelt szerepkörben végzett műveleteket naplózni kell és a naplóállományokat időszakosan felül kell vizsgálni,
- Óraszinkronizálás (clock synchronisation): egy időszolgáltatóhoz kell szinkronizálni valamennyi infrastruktúra és védelmi rendszerelemet, így a naplózást is.

A szabvány közvetlenül nem fogalmaz meg követelményt a központi, vagy dedikált biztonsági naplózás, a naplóelemzési tevékenység végzésére, illetve a naplótartalmak vonatkozásában, ugyanakkor az incidenskezelésről szóló fejezetben (16. pont) elvárásként jelenik meg az incidensek felismerése, megismerése és a tapasztalatok beépítése a hatékonyabb információbiztonság megteremtése érdekében. A 16. pontban megfogalmazott követelményeknek történő megfelelés viszont nem képzelhető el hatékony naplóelemzés nélkül.

A NIST SP 800-53r4. Audit and accountability, (ellenőrzés és megfelelőség) (AU) fejezete foglalkozik részletesen, a naplózás megvalósításának kérdésével. A fejezet különböző biztonsági szinten lévő rendszerekre eltérő követelményeket határoz meg

- a naplózási eljárásrenddel,
- a naplóbejegyzések tartalmával,
- a tárolókapacitás kezelésével,
- a naplózási képesség hibájának kezelésével,

---

[15] *NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations http://nvlpubs.nist.gov/ nist-pubs/SpecialPublications/NIST.SP.800-53r4.pdf (leöltve: 2016.09.20)*

[16] *Dr. Haig Zsolt: Az információbiztonság szabályozói és szervezeti kerete http://hadmernok.hu/kulonszamok/robothadviseles7/haig_rw7.pdf (leöltve: 2016.09.21)*

- a naplóbejegyzések áttekintésével, elemzésével és jelentések készítésével,
- a naplóbejegyzések összevonásával és jelentés generálásával,
- a naplóbejegyzések időbélyeggel történő ellátásával,
- a naplóbejegyzések védelmével,
- a naplóbejegyzések letagadhatatlanságával, illetve
- az naplóbejegyzések megőrzésével kapcsolatban.

A naplózási tevékenység megértésére, naplózási képesség kialakításához, fenntartásához a NIST 2006-ban kiadta a NIST SP 800-92-es számú Guide to Computer Security Log Management[17] című publikációját. A dokumentum technikai és folyamati oldalról közelíti meg a naplómenedzsmentet. Részletesen bemutatja a

- a naplózás menedzsment infrastruktúrát (architektúrát, syslog alapú központnaplózás kezelést, SIEM rendszereket)
- a naplózás menedzsmenttervezést (szabályokat, felelősségeket, megadja azon kérdéseket, amelyek segíthetnek a naplózási és működési szabályok kialakításában)
- a naplózás menedzsment működési folyamatait (források konfigurálását, naplóállományokgenerálását, a tárolással feldolgozással kapcsolatos folyamatokat)

A NIST SP 800-53r4 H. melléklete tartalmaz, több összehasonlító táblázatot, melynek célja a NIST SP 800-53r4. kontrollok, valamint az ISO/IEC 27001, illetve az ISO/IEC 15408 (Common Criteria)[18] követelmények egymásnak történő megfeleltetése, ami hasznos segítséget nyújthat az információbiztonsági megfelelés hatékony megvalósításában.

Hazai szabályozás

A NIST SP 800-53r4. alapján készült állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény[19] (továbbiakban: Ibtv.) hatálya alá tartozó szervezetek esetében a törvény végrehajtására kiadott

[17] *Special Publication 800-92 Guide to Computer Security Log Management http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf (letöltve: 2016.09.20)*

[18] *ISO/IEC 15408 (Common Criteria): Information technology - Security techniques - Evaluation criteria for IT security*

[19] *2013. évi L. törvényaz állami és önkormányzati szervek elektronikus információbiztonságáról http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV (letöltve: 2016.09.20)*

41/2013. számú BM rendelet[20] (továbbiakban: Vhr.) 3. számú mellékletében külön csoportban (3.3.12) vannak meghatározva azon naplózással kapcsolatos követelmények, amelyeket a szervezetnek, rendszernek – biztonsági osztálytól függően más szinten – teljesíteni kell.

A rendelet nem határoz meg konkrét műszaki elvárásokat, az alkalmazóra bízza azt, hogy az elvárt követelmény teljesítését miként valósítja meg. A rendszer biztonsági osztálytól függetlenül elvárásként jelenik meg

- naplózási eljárásrend alkalmazása,
- naplózandó események meghatározása (megfelelő tartalommal, időbélyeggel),
- a naplótartalom védelme,
- a naplóbejegyzések megőrzése a különféle jogszabályokban meghatározottak szerint,
- naplózási képesség kialakítása.

Magasabb biztonsági osztályba sorolt rendszerek esetén további követelmények jelennek meg, többek között hibakezeléssel, riasztással, jelentési képességgel, napló tartalom védelemével, a naplóbejegyzések időbélyeggel történő ellátásával, illetve a fizikai belépés naplózásával kapcsolatban.

A Vhr. két konkrét esetet nevesít 4-es és 5-ös biztonsági osztályba sorolt rendszereknél, mint naplózandó eseményt:

- felhasználói fiókokkal kapcsolatos tevékenységek naplózása,
- privilégizált felhasználói tevékenység naplózása.

Az Ibtv. hatálya alá nem tartozó szervezetek esetén ágazatspecifikus szabályozás fogalmazhat meg a rendszer, naplózási funkcióival szemben teljesítendő követelményt. Az ágazati szereplőkre vonatkozó jogszabályok az Vhr.-ben megfogalmazott elvárásokat pontosítva, azt kiegészítve további követelményeket határozhatnak meg. Pénzügyi szolgáltatók esetén az MNB ajánlás az Vhr.-nél lényegesen magasabb szinten fogalmazza meg az elvárásokat, de a szabályozás konkrét naplózandó tevékenységeket is meghatároz, illetve az üzletmenet folytonosság szempontjából kritikus rendszereknél előírja az azonnali riasztásra történő reagálási képesség kialakítását, ami az Vhr.-ben csak az 5-ös biztonsági osztályba sorolt rendszerek esetében elvárás.

A naplózás célja

Az informatikai rendszerekben történő naplózás – a jogszabályi megfelelés mellett - kettős célt szolgálhat. Az első, hogy *„a naplózás információt nyújt az infor-*

[20] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm (letöltve: 2016.09.20)

matikai elemek általános állapotáról csakúgy, mint a biztonságilag fontos történésekről"[21]. A második, hogy a történések utólagos elemzése mellett a naplózás, ha csak nagyon korlátozottmódon is, de annál fontosabb esetben jelenthet segítséget egy folyamatban lévő támadás felismerésében. A támadások detektálása, megakadályozása elsősorban olyan védelmi eszközök feladata, mint a host oldali végpontvédelmi rendszerek, vírusvédelmi rendszerek, tűzfalak, IDS/IPS-ek, és az informatikai rendszerelemeket folyamatosan figyelő egyéb monitoring rendszerek. A naplógyűjtés és elemzés a hosszabb ideig tartó, fejlett támadások (APT) felderítésében játszhat szerepet, mivel e támadás típusokat jellemzően a védelmi eszközök önmagukban általában nem képesek detektálni, a felismeréshez szükséges lehet hosszabb időintervallumban keletkezet naplóbejegyzések vizsgálatára, illetve az különböző rendszerekben keletkezett naplóbejegyzések korrelált elemzése.

Ahhoz, hogy a két cél hatékonyan megvalósuljon, számos feltételnek kell teljesülnie, amelyek közül a legfontosabbak:

- valamennyi biztonsági szempontból releváns informatikai eszközben keletkezzenek megfelelő tartalmú naplóbejegyzések a rendszerben zajló tevékenységekről,
- a biztonsági szempontból releváns naplóbejegyzések jussanak el az elemzőhöz, legyen szó automatikus elemző rendszerről vagy emberi erőforrásról,
- legyen meg az elemzési képesség, azaz kerüljön kialakításra olyan feltételrendszer (erőforrás), amely biztosítja a káros esemény feltárását,
- valós idejű riasztás esetén biztosítva legyen a válaszadáshoz szükséges képesség, mind folyamati, mind technikai, mind személyi, szervezeti oldalról.

A naplóbejegyzések forrásai

Az Ibtv. hatálya alá tartozó rendszerek esetében a naplózási képesség megléte alapkövetelményként jelenik meg a legalacsonyabb biztonsági osztályba sorolt rendszerek esetében is. A rendszer és ezen keresztül a szervezet pillanatnyi biztonsági állapotának méréséhez, illetve az utólagos incidens vizsgálathoz elengedhetetlenül fontos, hogy ezen rendszerekben zajló eseményekről naplóbejegyzés készüljön.

A régóta működő egyedi fejlesztések kivételével napjainkban már nem találkozhatunk olyan informatikai rendszerekkel, amelyek ne rendelkeznének naplógenerálási képességgel, legyen szó alkalmazásról, operációs rendszerről, adatbázis-kezelőről, vagy az informatikai biztonságot segítő rendszerről.

[21] *KRASZNAY Csaba: Naplózás e-kormányzati rendszerekben p 1. http://krasznay.hu/presentation/nws2010_krasznay.pdf (letöltve: 2016.09.20)*

Az üzleti folyamatot kiszolgáló rendszerek, a hálózati és védelmi eszközök teljes körű bevonása nélkül könnyen előfordulhat, hogy egy incidens rejtve marad, illetve egy utólagos vizsgálat során nem deríthető fel, hogy egy támadást milyen módon hajtottak végre és mely rendszerekből, milyen adatok kompromittálódtak. A nem megfelelő vizsgálati eredmény következtében könnyen elképzelhető a korábban sikeresen végrehajtott támadáshoz hasonló újabb sikeres támadások végrehajtása a szervezet informatikai rendszerei ellen. Éppen ezért, a fentiek miatt a naplóforrások meghatározása a jogszabályi elvárásokon túl, kockázatelemzési folyamat eredményeként állhat elő.

Az alábbi felsorolás tartalmazza azon események körét, amelyek naplógyűjtő rendszerbe történő bevonását mindenképpen érdemes megfontolni:[22,23,24,25,26]

- hálózati adatok (netflow és packet adatok, DNS[27] információk, stb.),
- hálózati védelmi eszközök jelzései (IPS/IDS,[28] tűzfal, spamszűrő, stb.),
- adatszivárgás megelőző eszközök (DLP[29]) jelzései (végponti, hálózati),
- végpontvédelmi eszközök jelzései (végponti behatolás detektáló eszközök, antivirus program, stb.),
- naplózási rendszer adatai,
- monitoring rendszerek jelzései (szerverek teljesítmény adatai, szolgáltatások adatai, stb.)
- rendszer és felhasználó – biztonsági vonatkozású - tevékenységei,
- adatbázisokban zajló tevékenységek,

---

[22] Building a World-Class Security Operations Center: A Roadmap https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907 (letöltve: 2016.09.20)

[23] Rajat MOHANTY: Upgrade your SOC with Security Analytics and Orchestration http://paladion.net/upgrade-your-soc/ (letöltve: 2016.09.20)

[24] Oliver ROCHFORD, Neil MACDONALD: The Five Characteristics of an Intelligence-Driven Security Operations Center Gartner report http://www.ciosummits.com/Online_Assets_Intel_Security_Gartner.pdf (letöltve: 2016.09.20)

[25] Kenneth HO: The Definitive Guide to Building A World Class Security Operations Center http://docplayer.net/13444776-The-definitive-guide-to-building-a-world-class-security-operations-center-table-of-contents.html (letöltve: 2016.09.20)

[26] Intel Security: Creating and Maintaining a SOC http://www.mcafee.com/ca/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf (letöltve: 2016.09.20)

[27] DNS: Domain Name System egy hierarchikus decentralizált tartománynévrendszer számítógépes rendszerek, szolgáltatások és egyéb internetre vagy privát hálózatra kapcsolat eszközök számára (https://hu.wikipedia.org/wiki/Domain_Name_System)

[28] IDS/IPS (Intrusion detection system/intrusion prevention system): informatikai rendszer behatolás jelző rendszer/behatolás megelőző rendszer

[29] DLP (Data Lost Prevention): adatvesztést megelőző rendszer

- fizikai biztonsági elemek (beléptető eszközök, nyomkövető rendszerek) adatai,
- folyamatoknál, kontrolloknál használt rendszerek (supervisory control and data acquisition (SCADA), distributed control system (DCS)) jelzései
- alkalmazás fehérlista, fájlintegritás ellenőrzés eredményei,
- sérülékenység értékelés és monitoring adatok.

A naplózási kapacitás függvényében születhet olyan döntés, hogy egy rendszercsoport csak bizonyos kiemelt kockázatú elemei kerülnek kiválasztásra (pl.: vezetői, rendszergazdai számítógépek), vagy a naplók begyűjtése mintavételezés szerűen történik (pl.: hálózati forgalmi adatok).

A naplózási szint meghatározása

A rendszerek jelentős részénél lehetőség van többszintű és eseménycsoporthoz rendelt naplózás beállítására, ami a rendszer indításától valamennyi esemény naplózásáig terjedhet.

Egyedi fejlesztésű rendszerek esetén a tervezési fázisban dől el, hogy mely tevékenységek lesznek naplózva, illetve lesz-e és, ha igen, akkor milyen szintű naplózás. A nem megfelelő tervezés esetén a naplózási képesség módosítása nehézkes és költségigényes lehet.

A naplózási szint, illetve a rendszer, naplózási képessége nagymértékben meghatározza, hogy mely eseményekről készül naplóbejegyzés. A Vhr. néhány magas kockázatú esemény kivételével nem határozza meg konkréten, hogy mely eseményekről, illetve milyen szinten kell naplóbejegyzést készíteni, a naplózandó események körét az üzemeltetőre bízza. Ugyanakkor például pénzügyi szervezetek vonatkozásában a vonatkozó szabályzat például előírja, hogy valamennyi üzleti és biztonsággal kapcsolatos tranzakciót naplózni kell.

A naplózási szint és ezzel együtt a naplózandó események körét alapvetően az alábbi tulajdonságok határozzák meg:

1. informatikai biztonsági szempontból mennyire kockázatos a rendszer (milyen biztonsági osztályba van besorolva), és a rendszer, naplózási képessége
2. informatikai rendszerek esetén a rendszer, naplózási képessége,
3. rendelkezésre álló tárolási és feldolgozási kapacitás,
4. a szervezet biztonságtudatossága,
5. korábbi informatikai biztonsági incidens tapasztatok.

A naplózás fejlesztésénél, beállításánál különösen oda kell figyelni, hogy a keletkezett naplóbejegyzések tárolhatók és feldolgozhatók legyenek. A túl sok és nem releváns naplóbejegyzések gyűjtése és a feldolgozás során keletkező események olyan terhelést jelenthetnek a szervezet számára, amelyet már nem képes elviselni, és aminek következtében – a naplózás háttérbe szorulása miatt –

pont az elérni kívánt cél nem lesz teljesíthető. A releváns naplóbejegyzések hiánya pedig ellehetetleníthet a hatékony vizsgálatot.

A naplóbejegyzés tartalma

A naplózási célok teljesülését nagymértékben befolyásolja a naplóbejegyzések tartalma. Amennyiben lehetőség van a naplóállományok tartalmának az összeállítására, akkor törekedni kell arra, hogy bejegyzésben minden olyan információ szerepeljen, amely a naplózás céljainak megvalósításához szükséges, és ne tartalmazzon olyan információkat, amely később nem kerül felhasználásra. A minimálisan a naplóbejegyzésnek tartalmaznia kell az esemény időpontját, a naplóállomány forrásaként szereplő rendszert, az eseményt, valamint az esemény sikerességét.

Az eszköz funkciójától függően további információknak kell a naplóbejegyzésben minimálisan szerepelnie:

- hálózati eszközök esetében minimálisan a forgalmi adatok (forrás, cél, protokoll, port, stb.), amennyiben lehetőség van rá, akkor hálózati csomag adatok, tartalom,
- informatikai rendszerek esetében az esemény adatai, jellemzői, érintett felhasználó/rendszer, stb.,
- egyéb infrastruktúra elemek esetében a tevékenységet végző felhasználó, a tevékenység leírása,
- üzleti alkalmazás esetében az érintett üzleti terület által meghatározott események felismeréséhez szükséges információk.

A naplóbejegyzések tartalmának meghatározása során különös figyelmet kell fordítani arra, hogy a naplóbejegyzések lehetőség szerint ne tartalmazzanak jogszabállyal védett (személyes, különleges) adatokat, csak abban az esetben, ha azt jogszabály előírja.

A naplóbejegyzések tárolása, megőrzése

A naplóbejegyzések tárolása történhet a naplóállományok keletkezésének helyén, vagy egy központi naplógyűjtő eszközön. A központ helyen történő tárolást a Vhr. csak a legmagasabb biztonsági osztályba sorolt rendszereknél ír elő, ugyanakkor számos alacsonyabb besorolású rendszer esetén teljesítendő követelmény teljesítését jelentősen megkönnyíti egy központi naplótároló és elemző rendszer kialakítása.

A központi naplótárolásnak és elemzésnek számos előnye van a helyi tárolással szemben, többek között:

- előre meghatározott események figyelése könnyebben megvalósítható,
- lehetőséget biztosít különféle rendszerekben keletkezett naplóbejegyzések közötti összefüggőségek vizsgálatára (korrelációk),
- hatékonyan támogatja a teljes támadási folyamat felderítését,

- hatékony támogatást nyújt a biztonsági esemény kiterjedtségének felderítésében,
- hatékonyabb monitoring tevékenységet tesz lehetővé,
- egységes infrastruktúrán, egységes módon kezelhetők a naplóbejegyzések,
- megnehezíti a támadók által hagyott nyomok eltüntetését,
- általában hosszabb idejű naplómegőrzést tesz lehetővé.

Másrészről a központi naplózó rendszer fenntartása erőforrást igényel a szervezettől, mind üzemeltetési, mind a felügyeleti tevékenység esetén. Amennyiben nincs szükség a naplóbejegyzések hosszabb idejű tárolására, úgy a régebbi, vagy a kevésbé fontos bejegyzéseket célszerű meghatározott időközönként törölni.

Amennyiben jogszabály alapján kerül meghatározásra a személyes adat megőrzésének ideje, úgy a előírás szerinti ideig a naplóbejegyzés megőrzendő. Ugyanakkor önkéntes hozzájáruláson alapuló adatkezelés esetén a hozzájárulás megszűnésekor – néhány esetet kivéve –, megszűnik az adatkezelés jogszerűsége, azaz az érintett személyes adatait is törölni kell, beleértve a naplóbejegyzésekben megtalálható adatokat. Egy naplóállományból néhány adat törlésének jelenleg nincs kialakult technikai gyakorlata, jellemzően az adatkezelők vállalják a jogi kockázatot. Jogszabályi megfelelés vagy üzleti okok miatt sok esetben szükséges a rendszerben végrehajtott naplóbejegyzések hosszú távú megőrzése, oly módon, hogy egy esetleges későbbi hatósági eljárás során bizonyítékként felhasználható legyen az adatállomány. Ahhoz, hogy egy naplóbejegyzés bizonyítékként felhasználható legyen, a keletkezéstől a felhasználásig biztosítani kell a naplóbejegyzés sértetlenségét. A sértetlenség bizonyítása történhet elektronikus aláírással, vagy olyan meghajtó használatával, amely nem engedi az utólagos módosítást. Az Vhr. előírása alapján sértetlenség szempontjából 5-ös szintre besorolt rendszerek esetén kriptográfiai eszközöket kell alkalmazni a naplóinformációk, és a naplókezelő eszköz sértetlenségének védelmére.

A naplóállományok tárolása (és feldolgozása) során különös figyelmet kell fordítani a tartalom bizalmasságának és sértetlenségének a megőrzésére is. A szervezetnek meg kell határoznia, hogy milyen naplóbejegyzésekhez, ki és milyen módon férhet hozzá.

Egy szervezet naplókezelési szintjének meghatározása

A különféle rendszerekben keletkezett naplóbejegyzések vizsgálata az adott szervezet között nagyon eltérő lehet. Az eltérés okai részben szervezet nagyságában, érettségében, részben a jogszabályi háttérben keresendők.

A naplóbejegyzések gyűjtésének és feldolgozásának érettségére vonatkozóan többféle besorolási módszer létezik. A hagyományos módszer szerint megha-

tározott érettség modell[30] a naplózási folyamat szempontjából határozza meg a naplózás fejlettségét, míg Raffael Marty által bemutatott modell[31] a fejlettséget működtetett funkciókhoz köti. Tapasztalatom szerint a folyamati érettség együtt jár a naplókezelési funkciók meglétével, és emiatt e kettő tényező együttese tudja meghatározni a szervezet érettségi szintjét:

- Ad-hoc szint: kevésbé tudatos, illetve nem magas kockázatú rendszereket üzemeltető szervezetek esetén – amennyiben a naplóbejegyzések tárolásra kerülnek - a naplóbejegyzések vizsgálata eseti jellegű, csak konkrét incidens esetén utólagosan történik, az incidensek kezelésére nincs kialakult folyamat. A biztonsági incidensek felismerése esetleges. A naplóforrások meghatározása szintén esetleges jellegű, jellemzően nincs központi naplógyűjtés és elemzés. Nincsenek dedikált biztonsági munkatársak, szervezet hiányában jellemzően az informatikai üzemeltetési terület végzi a naplóbejegyzések vizsgálatát.
- Fejlődés alatti szint: magasabb érettségi szinten lévő szervezetek esetén a naplóelemzés napi folyamatba építve, akár automatizált eszközökkel támogatva valósul meg. Ezen fejlettségi szinten már feltárásra kerülhetnek folyamatban lévő incidensek, illetve informálisan kialakulhatnak azon folyamatok, amelyek az incidens kezelés során működésbe lépnek. A szervezetben már van informatikai biztonsággal foglalkozó szervezet vagy olyan üzemeltető, aki magáénak érzi az informatikai biztonság képviseletét, megvalósult a központi naplógyűjtés, jellemzően már van az elemzést támogató eszköz is;
- Fejlett szint: dedikált naplóelemző szervezeti egység és naplógyűjtő és elemző rendszer megléte esetén lehetőség van számos olyan tevékenység végzésre, amely magasabb védelmi szintet biztosít a szervezet számára:
    - a különböző rendszerekből érkező naplóbejegyzések közötti összefüggés (korreláció) vizsgálata, riasztáshoz szükséges szabályok beállítása,
    - fejlett incidenskezelési és reagálási folyamat,
    - kockázat alapú prioritások meghatározása,
    - tudatosan, szabályozott módon szabályok beállítása, amelyek a szervezet működéséhez igazodva képesek egy bekövetkezett incidenst jelezni,

[30] *Security Logging in the Utility Sector: Roadmap to Improved Maturity https://www.bromberger.com/files/SecurityLoggingCMM1.0.pdf (letöltve: 2016.09.20)*

[31] *Maturity Scale for Log Management and Analysis http://raffy.ch/blog /2010/06/07/maturity-scale-for-log-management-and-analysis (letöltve: 2016.09.20)*

- az incidens vizsgálatok során feltárt hiányosságok elemzési eredményeinek beépítése a védelmi rendszerbe,
- külső forrásból származó, információbiztonsági fenyegetésekkel kapcsolatos információszerzés (CTI) és belső incidensekről információ megosztás,
- korábban nem ismert támadások felismerési képessége,
- nagy mennyiségű adatfeldolgozás fejlett modellekkel (matematikai, big data),
- szakképzett és motivált személyzet.

A szervezet érettségi szintje önmagában nem terjed ki a bevont rendszerek körére, de tapasztalatok alapján magas érettségi szinten lévő szervezetek esetében a naplózásba bevont rendszerek száma, illetve a begyűjtött naplók minősége megfelelő a hatékony naplóelemzési folyamatok végrehajtásához.

A központi naplógyűjtés és elemzés folyamata

A központi naplógyűjtő rendszerbe push vagy pull módban érkezhetnek a naplóforrásokból a naplóbejegyzések.

A forrásrendszerekből többféle protokoll[32] [33] használatával juthat el a naplóbejegyzés a központi naplóbejegyzés-gyűjtő rendszerbe. Az átviteli protokollt a küldő és a fogadó rendszer képességei határozzák meg.

Az előfeldolgozás során kiválasztott bejegyzések kerülnek be a központi naplógyűjtő rendszerbe, ahol megtörténik a naplóbejegyzés tárolása és normalizálása. A normalizálás során a naplóbejegyzések „kiválogatása", egységes formátumra hozása és letárolása valósul meg. A naplógyűjtő rendszerek általában a legelterjedtebb informatikai rendszerekhez „gyári" előfeldolgozást/normalizálást biztosítanak, ugyanakkor egyedi alkalmazások esetén a normalizáláshoz szükséges modult le kell fejleszteni.

Az események feldolgozása célszerűen a szervezet által meghatározott prioritás alapján történik. A normalizált naplóbejegyzések elemzése történhet automatikusan, illetve manuálisan. Manuális elemzés esetén az elemző dönti el, hogy mely naplóbejegyzéseket, tevékenység sorozatot vizsgál meg alaposabban. Az irányt az elemző számára rendelkezésre álló információ vagy sejtés határozza meg, de nagymértékben függ az elemzést végző tudásától, tapasztalatától is. Ugyanakkor sok esetben (pl. új támadási vektor vagy APT) a manuális elemzés az egyetlen út egy biztonsági incidens felderítéséhez, az események feltárásához.

---

[32] *Joseph MUNIZ, Gary MCINTYRE, Nadhem ALFARDAN: Security Operations Center: Building, Operating, and Maintaining your SOC CISCO PRESS 2015 ISBN-10: 0-13-405201-3*

[33] *KRASZNAY Csaba: Naplózás e-kormányzati rendszerekben p 12. http://krasznay.hu/presentation/nws2010_krasznay.pdf (letöltve: 2016.09.20)*

Az automatikus elemzés a már ismert információk alapján történő incidens megállapításban jelentős. Az automatikus elemzés során előre meghatározott feltételek alapján történik valós vagy közel valós időben a beérkező naplóbejegyzések vizsgálata. Amennyiben a vizsgálat során a naplóbejegyzésekből az előre beállított szabályokkal és információkból automatikusan megállapítható a feltételezett biztonsági esemény, úgy a rendszer automatikus riasztást küld a felügyeletet ellátó szakemberek részére.

Az incidens jelzéséhez szükséges információkat előre meg kell adni, de az eseményjelzéshez szükséges információk érkezhetnek több forrásrendszerből is (korreláció). Az információk érkezhetnek a szervezet által működtetett védelmi rendszerekből (IPS, DLP, stb.), de érkezhetnek külső, fenyegetettségeket jelző forrásokból származó információgyűjtésből (cyber threat intelligence - CTI). Automatikus feldolgozás esetén – elsősorban a külső, nem mindig pontos információk alapján – számos esetben keletkezhet olyan jelzés, amely nem valós incidenst (false positive) takarnak. Ezen események kiszűrése manuális úton tud megtörténni, további külső információforrások felhasználásával. A hagyományos – szignatúra alapú – védelmi rendszerek jelzései nagy biztonsággal valós jelzések lesznek, ugyanakkor a viselkedéselemzésen alapúló rendszerek esetében nagyszámú false positive riasztás keletkezhet, ami akár el is lehetetlenítheti az elemző tevékenységét. Ugyanakkor a false positive riasztások száma jelentősen csökkenthető a korábbi hasonló események feldolgozási eredményeinek visszatáplálásával és automatikus szűrésének kialakításával.

A naplóelemző rendszerek általában rendelkeznek olyan képességgel (enrichment), hogy a naplóbejegyzésben lévő információkat kiegészíthetik az elemzés és a jelentés készítés során hasznos információkkal, mint pl.: IP cím alapján hely vagy fertőzési adatokkal, domain névvel, whois[34] információkkal, fájl HASH információk.

Az naplóbejegyzések feldolgozása során keletkező riasztások kezelése szintén a szervezet által meghatározott prioritás alapján történik.

A naplóelemzési tevékenység eredményét a rendszer által automatikusan vagy manuálisan készített időszakos vagy eseti jelentések segítségével lehet bemutatni.

Szervezeten kívüli naplógyűjtés, naplóelemzés

Amennyiben a szervezet nem rendelkezik megfelelő erőforrással vagy nem kíván naplóelemzéssel foglalkozni, lehetősége van az elemzési tevékenységet kiszer-

[34] *whois jelentése: WHOIS egy TPC- alapú tranzakciós orientált kérés/válasz protokoll, amely széles körű információt szolgáltat az internet használóknak (https://tools.ietf.org/html/rfc3912) (letöltés ideje?)*

vezni, szolgáltatásként külső szolgáltatótól igénybe venni. A kiszervezés több szinten valósulhat meg:

- elemzési funkció kiszervezése: a szervezet hozzáférést biztosít a szervezet által üzemeltetett naplóelemző rendszerhez a naplóelemzést végző partner számára. Ebben az esetben a külső partner részben vagy egészben hozzáfér a naplóállományokhoz. A naplóállományok nem hagyják el a szervezet határait, tevékenysége jól nyomon követhető;
- naplógyűjtési funkció kiszervezés: a naplóállományokat a szerződéses partner részben vagy teljes egészében megkapja és az elemzési tevékenységet saját infrastruktúráján végzi el;
- publikus felhő alapú szolgáltató igénybevétele: a szervezet a keletkezett naplóbejegyzések vagy azok egy részének elemzéséhez felhő alapú infrastruktúrát vesz igénybe;

Külső szolgáltatók hatékony eszközökkel rendelkeznek a nagyobb informatikai szállítók által szállított rendszerek elemzésének képességével, ugyanakkor egyedi alkalmazásokból származó naplóállományok elemzése problémát és jelentős többletköltséget okozhat.

Külső szolgáltató igénybevételének számos szakmai és pénzügyi előnye lehet, ugyanakkor bizonyos informatikai rendszerek esetén az információbiztonsági kockázatok jelentős mértéke miatt a szervezet számára nem jelent megoldást. A magyar állami és önkormányzati szférában a hazai szigorú szabályozás miatt a teljes és a felhő alapú megoldások nem igazán tudnak elterjedni.

A jogszabályi környezet megteremtése után a hazai állami és önkormányzati szervezetek számára külső naplóelemzési szolgáltatás igénybevételéhez jelentős segítséget nyújthatna egy független bizalmi szolgáltató, ahol rendelkezésre állnának azon infrastruktúra elemek, szervezeti, személyi feltételek, amelyek lehetőséget biztosítanának az egyes csatlakozott szervezetek fenyegetettségeinek kezelésére, az egyes szervezetek rendszereihez kapcsolódó fenyegetettségi információ megosztására.

Összegzés

Az informatikai rendszerekben zajló eseményekről készülő naplóbejegyzések gyűjtése, elemzése a jogszabályi megfelelés mellett jelentős mértékben hozzájárulhat a szervezet biztonsági szintjének növeléséhez. A szervezet érettségi szintjétől függően lehetőség van korábban lezajlott incidens feltárására vagy fejlettebb szinten lévőszervezet esetén akár egy folyamatban lévő incidens felfedezésére is.

A nemzetközi és hazai szabványok, jogszabályok adnak iránymutatást naplózási elvárásokkal kapcsolatban, ugyanakkor ezen elvárások kevés kivételtől eltekintve nem határoznak meg konkrét elvárásokat, sem a naplózandó események

körére, sem az események feldolgozására. A szervezetre bízzák, hogy az elvárt követelményt miként teljesítik.

A szervezet működését biztosító informatikai rendszerek szerepétől, valamint a szervezet kockázat elemzésétől függően kell meghatározni azon rendszerek körét, amelyeket be kell vonni a (központi) naplózási körbe.

A naplózásba bevont rendszerek esetén nagyon fontos, hogy a releváns biztonsági eseményekről készüljön megfelelő tartalmú naplóbejegyzés, amelyet a jogszabályokban vagy a belső szabályzókban meghatározott ideig meg kell őrizni, de gondoskodni kell a törlendő naplóbejegyzések törléséről is.

Tekintettel arra, hogy az Ibtv. hatálya alatt álló szervezetek naplózási gyakorlata jelentősen eltér, javasolt lenne egy naplózási képesség kialakítását támogató dokumentumot kidolgozni, ezzel segítve az egyenszilárdságú védelem kialakítását. A dokumentumnak – megítélésem szerint – ki kell térni a naplózási, naplóelemzési tevékenység nyújtásával kapcsolatos elvárásokra, követelményekre is.

Felhasznált irodalom:

- 2013. évi L. törvényaz állami és önkormányzati szervek elektronikus információbiztonságáról http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300050.TV
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1500041.bm
- Building a World-Class Security Operations Center: A Roadmap https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907
- DR. HAIG Zsolt: Az információbiztonság szabályozói és szervezeti kerete http://hadmernok.hu/kulonszamok/robothadviseles7/haig_rw7.pdf
- ERNST & YOUNG: Third-generation Security Operations Centers http://www.ey.com/Publication/vwLUAssets/ey-third-generation-security-operations-centers-2015/$FILE/ey-third-generation-security-operations-centers-2015.pdf
- Intel Security: Creating and Maintaining a SOC http://www.mcafee.com/ca/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf
- Joseph MUNIZ, Gary MCINTYRE, Nadhem ALFARDAN: Security Operations Center: Building, Operating, and Maintaining your SOC CISCO PRESS 2015 ISBN-10: 0-13-405201-3

- Kenneth HO: The Definitive Guide to Building A World Class Security Operations Center http://docplayer.net/13444776-The-definitive-guide-to-building-a-world-class-security-operations-center-table-of-contents.html
- KOVÁCS Zoltán: Információgyűjtés – A kibertér felhasználása. In: A nemzetbiztonság technikai kihívásai a 21. században. Szerk.: BODA József – DOBÁK Imre. Nemzeti közszolgálati Egyetem Nemzetbiztonsági Intézet. Budapest 2015. ISBN: 978-615-5527-74-6
- KRASZNAY Csaba: Naplózás e-kormányzati rendszerekben http://krasznay.hu/presentation/nws2010_krasznay.pdf
- Maturity Scale for Log Management and Analysis http://raffy.ch/blog/2010/06/07/maturity-scale-for-log-management-and-analysis
- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények
- NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- Oliver ROCHFORD, Neil MACDONALD: The Five Characteristics of an Intelligence-Driven Security Operations Center Gartner report http://www.ciosummits.com/Online_Assets_Intel_Security_Gartner.pdf
- Rajat MOHANTY: Upgrade your SOC with Security Analytics and Orchestration http://paladion.net/upgrade-your-soc/
- Security Logging in the Utility Sector: Roadmap to Improved Maturity https://www.bromberger.com/files/SecurityLoggingCMM1.0.pdf
- Special Publication 800-92 Guide to Computer Security Log Management http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf