ECSÉD

Ecsédi Polgármesteri Hivatal

naplózási eljárásrendje

Tartalomjegyzék

I. BEVEZETÉS

Az Ecsédi Polgármesteri Hivatal az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.), valamint annak végrehajtására kiadott rendeletekben foglalt elektronikus információbiztonsági feladatok elvégzésére irányuló felkészülést, illetve azok végrehajtását megkezdte.

Az Ibtv. 11. §-ának (1) bekezdés e) pontja és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet 3.3.12.1. pontjában meghatározottak szerint az Naplózási eljárásrendben a Hivatal mint érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül a szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a naplózási eljárásrendet, mely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;a naplózásra és elszámoltathatóságra vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a naplózási eljárásrendet.

Jelen dokumentum célja, hogy ismertesse a Hivatal naplózási eljárásrendjét.

II. NAPLÓZÁS

A rendszereket folyamatosan meg kell figyelni annak érdekében, hogy az előírtakat, illetve a normál működéshez képest minden eltérést észlelni és rögzíteni lehessen, hogy bizonyítékkal szolgálhassanak az esemény kivizsgálása, illetve az esetleges további eljárás során. A rendszermegfigyelés lehetővé teszi az alkalmazott védelmi intézkedések hatékonyságának ellenőrzését is.

Az informatikai rendszerekben történő naplózás – a jogszabályi megfelelés mellett - kettős célt szolgálhat. Az első, hogy „a naplózás információt nyújt az informatikai elemek általános állapotáról csakúgy, mint a biztonságilag fontos történésekről". A második, hogy a történések utólagos elemzése mellett a naplózás, ha csak nagyon korlátozott módon is, de annál fontosabb esetben jelenthet se-gítséget 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.

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.

2.1. A rendszerhasználat figyelése

Az információ-feldolgozó eszközök használatát, monitorozni kell. Az egyes eszközök esetében a megkívánt figyelési szintet a kockázatok elemzésével kell meghatározni.

A naplóellenőrzés magában foglalja a rendszerekre vonatkozó fenyegetések felismerését is. A rendszernaplók gyakran tartalmaznak nagy mennyiségben információt, amelynek nagy része nem biztonsági jellegű.

Meg kell fontolni, alkalmas rendszer segédprogramok vagy átvilágítási eszközök alkalmazását annak érdekében, hogy a biztonsági megfigyelés számára lényeges eseményekre azonosítani lehessen.

2.2.Naplóbejegyzések védelme

A naplóinformációkat védeni kell az illetéktelen hozzáféréstől, hogy megelőzzük az információk utólagos módosítását, törlését. A naplóinformációk biztonsági esemény esetén későbbi bizonyítékul szolgálhatnak, így védelmük fontos. A naplóinformációkat az információ feldolgozó eszközökön a jogosultságok megfelelő beállításával, illetve szükség esetén további titkosítási eljárásokkal kell védeni.

A megfelelő óvintézkedésekért az információbiztonsági felelős felel.

A naplóbejegyzéseket lehetőség szerint központilag kell gyűjteni, az elemzések megkönnyítése érdekében. A naplóbejegyzések integritását meg kell őrizni azáltal, hogy a naplófájlban szereplő adatok személy, vagy program által a későbbiekben ne

legyenek módosíthatók. A rendszerek lokális óráit szinkronizálni kell, a kézzel történő átállítást meg kell akadályozni.

2.3 Rendszergazda és operátor naplók

Az informatikai rendszerben végrehajtott műveleteket, objektumokhoz történő hozzáférést a kockázatokkal arányosan kell naplózni mind alkalmazás, mind operációs rendszer, mind adatbázis rendszer szinten. Az alkalmazott naplózásnak és a kapcsolódó kiegészítő adminisztrációnak olyan részletezettségűnek kell lennie, hogy abból az esemény érdemi értékelése elvégezhető, az egyértelmű személyes felelősség megállapítható legyen.

Az informatikai rendszer naplózási rendszerében biztosítani kell az informatikai rendszer legfontosabb elemeinek (eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosítását.

Gondoskodni kell olyan biztonsági környezetről, amely az informatikai rendszer működése szempontjából kritikus folyamatok eseményeit naplózza.

A fentiek szerint naplózás rendszeres és érdemi értékelésről gondoskodni kell.

Minden naplózást lehetőség szerint úgy kell beállítani, hogy a felhasználó éles adathoz naplózási lehetőségek megkerülésével ne férhessen hozzá.

2.4 Hiba naplózás

Az informatikai rendszer biztonsági és egyéb meghibásodását vagy rendellenes működését szóban vagy e-mail-en keresztül kell bejelenteni az üzemeltetőnek. Felelős: a meghibásodást vagy rendellenes működést észlelő személy.

A bejelentett hibákat a hibát fogadó személy a hiba naplóba rögzíteni köteles.

Minden bejelentett biztonsági eseményt jelenteni kell az információbiztonsági felelősnek.

A hiba kijavítását követően a hiba elhárításáról a hibát bejelentő személyt értesíteni kell. Felelős: az elhárítást végző, illetve külső támogató cég közreműködése esetén az azt felügyelő üzemeltető munkatárs.

2.5.Naplózási eljárásrend

Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül a szabályozásában meghatározott személyek vagy szerepkörök számára kihirdeti a naplózási eljárásrendet, mely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő; a naplózásra és elszámoltathatóságra vonatkozó eljárásrendben vagy más belső szabályozásában meghatározott gyakorisággal felülvizsgálja, és frissíti a naplózási eljárásrendet.

A Hivatal mint szervezet informatikai rendszereinek tervezésekor rögzített naplózási szabályokat kell alkalmazni. Ennek során az alábbi alapelveknek kell megfelelni:

- A Szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

- Az egyedi elszámoltathatóság érdekében a naplózási funkciókat lehetőleg úgy kell beállítani, hogy a felhasználói tevékenységek személyre szólóan nyomon követhetők legyenek.

- Az események és problémák azonosítása érdekében a napló tartalmazza a problémák megoldásához szükséges adatokat.

- A visszaélések felderítése érdekében a jogosult felhasználói tevékenységek és jogosulatlan tevékenységekre irányuló kísérletek naplózásra kerülnek.

- A Szervezet minden rendszerében megbízható módon védeni kell az ott keletkezett naplóállományokat a jogosulatlan felfedés, módosítás és törlés ellen.

- A naplóállományok ellenőrzését a rendszergazda végzi. Az ellenőrzéseknek rendszeresen, legalább kéthetente kell megtörténnie. Az ellenőrzések hatékonyságának növelésére automata ellenőrzőszoftvert is lehet alkalmazni, amennyiben ez az adott rendszeren technológiailag lehetséges.

- A munkaállomások naplóállományainak elemzése biztonsági incidensek esetén, de legalább a tervezett karbantartás során kötelező.

A rendszergazdán túl a naplóállományok adattartalmába betekinthet: információbiztonsági felelős.

Az előző pontban felsoroltak valamelyike által írásban felhatalmazott (akár külsős) szakember.

Az elektronikus információs rendszer:

- belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához,
- időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz – úgynevezett UTC – vagy a Greenwichi középidőhöz – úgynevezett GMT – rendelhető módon, megfelelve a szervezet által meghatározott időmérési pontosságnak, amely a „másodperc pontosság".
- a rendszerórákat a szervezet saját NTP-hez szinkronizálja, amely pedig a time.nist.gov szerverrel szinkronizál.

2.6. Naplózható események

Az érintett szervezet meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét; egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását; megvizsgálja, hogy a naplózható események megfelelőnek

tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.

Az alábbi felsorolás tartalmazza azon események körét, amelyek naplógyűjtő rendszerbe történő bevonását mindenképpen érdemes megfontolni:

- 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, antivírus program, stb.),
- naplózási rendszer adatai,
- monitoring rendszerek jelzései (szerverek teljesítmény adatai, szolgáltatások adatai, stb.)
- rendszer és felhasználó – biztonsági vonatkozású - tevékenységei,
- adatbázisokban zajló tevékenységek,
- 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).

2.7. Naplóbejegyzések tartalma

Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.

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.

2.8. Napló tárkapacitás

Az érintett szervezet a naplózásra elegendő méretű tárkapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével.

2.9. Naplózási hiba kezelése

Az elektronikus információs rendszer naplózási hiba esetén riasztást küld a meghatározott személyeknek vagy szerepköröknek; elvégzi a meghatározott végrehajtandó tevékenységeket, így például a rendszer leállítását, a legrégebbi naplóbejegyzések felülírását, a naplózási folyamat leállítását.

2.10. Naplóvizsgálat és jelentéskészítés

Az érintett szervezet rendszeresen felülvizsgálja és elemzi a naplóbejegyzéseket nem megfelelő vagy szokatlan működésre utaló jelek keresése céljából; jelenti ezeket a meghatározott személyeknek vagy szerepköröknek.

2.11. Időbélyegek

Az elektronikus információs rendszer belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához; időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a

Greenwichi középidőhöz - úgynevezett GMT - rendelhető módon, megfelelve az érintett szervezet által meghatározott időmérési pontosságnak.

2.12. Szinkronizálás

Az elektronikus információs rendszer meghatározott gyakorisággal összehasonlítja a belső rendszerórákat egy hiteles külső időforrással, és ha az időeltérés nagyobb, mint a meghatározott időtartam, szinkronizálja a belső rendszerórákat a hiteles külső időforrással.

2.13. A naplóbejegyzések megőrzése

Az érintett szervezet a naplóbejegyzéseket meghatározott - a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

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.

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.

2.14. Naplógenerálás

Az elektronikus információs rendszer biztosítja a naplóbejegyzés generálási lehetőségét a BM rendelet 3.3.12.2. pontjában meghatározott naplózható eseményekre; lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az

elektronikus információs rendszer egyes elemeire; naplóbejegyzéseket állít elő a BM rendelet 3.3.12.2. pontja szerinti eseményekre a 3.3.12.3. pontjában meghatározott tartalommal.

III. ZÁRÓ RENDELKEZÉSEK

Jelen szabályzat 2017. július 3. napján lép hatályba és visszavonásig érvényes.

Ecséd, 2017. július „3.".

ECSÉDI POLGÁRMESTERI HIVATAL Jegyző Ecséd

Nagy Lászlóné

jegyző