



## Korai Figyelmeztető Rendszer (EWS) – Szolgáltatási Szabályzat





Verziószám:	1.0
Hatályba lépés dátuma	2022.11.01.
Dokumentum besorolása:	nyilvános

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
1.0	2022.10.11.	Kiinduló változat			



## Tartalomjegyzék

1. Bevezetés.....	3
1.1. Általános információk.....	3
1.2. Az EWS előnyei .....	3
1.3. Az EWS-hez történő csatlakozás menete .....	4
2. EWS csatlakozás műszaki követelményei .....	5
2.1. A hálózati forgalom átadása .....	5
2.2. A titkosítás feloldása.....	6
2.3. Hogyan alakítsam ki a kritikus hálózati csomópontokat? .....	6
2.4. A naplókezelés minimumkövetelményei .....	7
3. EWS csatlakozás kialakításához kapcsolódó feladatok.....	8
3.1. EWS csatlakozási terv készítése.....	8
3.2. Műszaki feltételek megvalósítása.....	8
3.3. Oktatáson való részvétel .....	9
3.4. Csatlakozás próbaüzemének támogatása .....	9
3.5. Adatvédelem megfelelőségének fenntartása .....	9
3.6. Belső szabályozás felülvizsgálata.....	10
4. EWS csatlakozás fenntartásához kapcsolódó feladatok.....	11
4.1. EWS üzemeltetési feladatok támogatása.....	11
4.2. Változáskezelés.....	11
4.3. Felhasználó kezelés, tokenek .....	11
5. EWS csatlakozás hatékonyságnövelő ajánlások.....	12
5.1. Naplókezelés (log management) .....	12
5.2. Hálózathasználati házirendek.....	14
5.3. Határvédelmi eszközök beállítása .....	14
6. Mellékletek .....	15
6.1. Védendő intézmény adatlap (minta).....	15
6.2. Védendő rendszer adatlap (minta) .....	17

## 1. Bevezetés

### 1.1. Általános információk

Jelen dokumentum a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NKI) Korai Figyelmeztető Rendszer (early warning system, továbbiakban: **EWS**) Szolgáltatási Szabályzata, amely az EWS által nyújtott szolgáltatásokra vonatkozik.

A rendszerrel kapcsolatos részletszabályokat az elektronikus információbiztonsági korai figyelmeztető rendszerről szóló **214/2020. (V. 18.)** kormányrendelet tartalmazza.

Az NKI jogszabályi felhatalmazás alapján **egy informatikai biztonsági korai figyelmeztetőrendszert** valósított meg és üzemeltet. Az EWS az egyes vele egyirányúan összekapcsolt védendő elektronikus információs rendszerek hálózati forgalmának **szenzorokkal** történő passzív elemzésével automatizált módon azonosít kockázatokat, valamint támadásra, visszaélésre vagy ezek kísérletére utaló eseményt. Az EWS jelzéseket, adatokat és ezekre épülő szolgáltatásokat nyújt az egyes védendő rendszerekre vonatkozóan azok fenntartó intézményeinek kijelölt munkatársai és az NKI számára.

Az EWS rendszer a KÖFOP-2.2.2-VEKOP-16-2016-00001. számú projekt keretében valósult meg, a rendszerek csatlakoztatására ütemezetten van lehetőség.

### 1.2. Az EWS előnyei

Az EWS rendszer szolgáltatásai a 2013. évi L. törvény (**lbtv.**) illetve az annak végrehajtásáról szóló 41/2015. (VII. 15.) BM rendelet (továbbiakban: **BMr.**) által előírtan az intézmény által önállóan megvalósításra kerülő védelmi intézkedések nyújtotta biztonságon felüli **kiegészítő szolgáltatásként** javítja a csatlakozó intézmény észlelési, felügyeleti, és megfelelőség ellenőrzési képességét, és ezeken keresztül integritását.

Az EWS segítségével az intézmény számára **hamarabb és nagyobb mértékben válhatnak láthatóvá**, illetve ezáltal kezelhetővé a rendszert érintő támadások (pl. hálózati betörési kísérlet, adatlopás, weboldal rongálás), visszaélések, korrupciós cselekmények (pl. adatszivárogtatás, zsarolási kísérlet) és kockázatok (pl. sérülékeny vagy illetéktelen eszközök és szolgáltatások, lappangó kártevők).

Az EWS csatlakozással az intézménynek csökkennek az incidens kivizsgáláshoz kapcsolódó adminisztratív terhei, mivel (1) a tipikusan átadandó adatok egy része már eleve **elektronikus formában a csatlakozást követően** az NKI rendelkezésére fog állni; valamint (2) az NKI ezen adatok előzetes elemzésével és a védendő rendszer felépítésének ismeretében **célzottabb**



**javaslatot** tud tenni a még szükséges műszaki adatok begyűjtésére illetve az indokolt védelmi intézkedésekre vonatkozóan.

Az EWS-hwz történő csatlakozás feltétele, hogy az intézmény legalább egy fő IT munkatársat és egy fő integritási tanácsadót jelöljön ki, akiknek az NKI szakmai és integritás-tanácsadói képzést biztosít térítésmentesen.. Ezen szakmai továbbképzés, biztonság tudatos és anti-korrupciós szemléletformálás eredményeként a munkatársak jobban hozzá tudnak járulni a védendő rendszerek által kezelt adatvagyon illetve nyújtott szolgáltatások biztonságához, az informatikai biztonsági incidensek kezeléséhez, és a korrupció kockázatának csökkentéséhez.

### 1.3. Az EWS-hez történő csatlakozás menete

Az egyes rendszerek fenntartó intézményeinek a csatlakozásra vonatkozó döntést követően általánosságban a következő feladatok végrehajtásáról szükséges intézkedniük:

- a csatlakozási pontok tervét, műszaki/méretezési adatait az NKI-val **jóváhagyni**;
- a csatlakozás műszaki feltételeit **megteremteni**, illetve a rendszer életciklusa alatt **fenntartani**;
- a műszaki feltételek ellenőrzését, az esetlegesen szükséges EWS eszköz telepítést, illetve az EWS-hez csatlakoztatást az NKI számára lehetővé tenni a rendszer életciklusához igazodva, előre egyeztetetten;
- IT illetve integritás-tanácsadó munkatársakat az EWS-hez kapcsolódóan ütemezetten meghirdetendő oktatásokra **delegálni**;
- a rendszer életciklusa alatt bekövetkező változásokat (próbaüzem indulás, élesítés, bővítés, migráció, tulajdonoscsere, kivezetés, stb.) az NKI felé jelezni, valamint azok EWS-t érintő kezelésében (csatlakozási kapacitás bővítés/szűkítés, konfiguráció, stb.) az NKI-val **együtműködni**.

Az EWS rendszerhez való kapcsolódás a legegyszerűbben a NISZ-KAK (Kormányzati Adatközpont) felhőjében lévő rendszerek és szolgáltatások vonatkozásában valósítható meg, ott minden szükséges technikai eszköz (forgalomkicsatoló, ssl terminálás, szenzor) rendelkezésre áll. A NISZ-KAK elhelyezés esetén mindenképpen szükséges az SSL terminálás a KAK tűzfalon, valamint a tanúsítvány átadása a NISZ-nek. Az EWS rendszert lehetőség van egyéb helyszínen (on-premise) is telepíteni, ez azonban összetettebb folyamat, mely mindenképpen személyes, szakmai egyeztetést igényel. Utóbbi esetben jelentős előny, hogy a szolgáltatást az igénybevevő nagyon kedvező pénzügyi feltételek mellett tudja igényelni. Az intézmény a kiegészítő biztonsági szolgáltatások előnyeit már a csatlakozás kiépítésétől élvezheti a nap 24 órájában.

## 2. EWS csatlakozás műszaki követelményei

Az EWS csatlakozás alapvető műszaki feltétele, hogy az intézmény az NKI-val **egyeztetve** oly módon alakítsa ki, illetve szervezze át a védendő rendszerét, hogy annak legalább az internet felőli biztonsága szempontjából kritikus **hálózati csomópontokon** áthaladó **forgalom** másolata 1 helyen, a lehető legkevesebb, de legfeljebb 2 (nagy rendelkezésreállású rendszerek esetében legfeljebb 4) szabványos hálózati porton titkosítatlanul **átadásra kerüljön**, valamint az azt elemző EWS **szenzorok elhelyezése**; és a NISZ adatközpontbeli EWS központi alrendszerrel való **összeköttetése** biztosított legyen.

Az EWS jelzései alapján az intézménynek képesnek kell lennie az esetek **kivizsgálására** (incidenskezelés), a jelzésbeli technikai azonosítók (timestamp, IP, port, domain, URL, stb.) alapján az érintett eszközök, szolgáltatások, felhasználók **beazonosítására** legalább **2 hónapra** visszamenőleg megfelelő szervezési illetve **naplókezelési** megoldások kialakításával.

### 2.1. A hálózati forgalom átadása

Az EWS rendszernek a hálózati forgalom másolatát szükséges átadni szabványos hálózati interfészekon (réz: I00BASE-TX, I000BASE-T, réz/optika: 1GbE, önállóan vagy LACP aggregálással). A másolás történhet dedikált, lehetőleg valódi passzív vagy fail-open TAP eszközzel<sup>1</sup>, vagy indokolt esetben szoftveresen (pl. SSL proxy inspection portja, fizikai/virtuális router/switch monitor portja).

Az EWS rendszer több **NISZ telephelyen** rendelkezik közvetlen csatlakozási pontokkal, így a forgalom átadása ezen adatközpontokban elérhető portok esetében fizikai vagy virtuális összeköttetéssel történik (patchelés, konfigurálás).

A **többi esetben** a védendő rendszerek és/vagy portok esetében az NKI-val előzetesen egyeztetendő egyedi kialakítás szükséges, mind az EWS eszközeinek elhelyezésére, mind azok EWS központi rendszerrel való hálózati összeköttetésére vonatkozóan.

Ha az elemezhető forgalom titkosított (pl. HTTPS, SMTPS, VPN), akkor a titkosítás feloldására és a feloldott forgalom elemezhetővé tételére **kiegészítő megoldás** szükséges.

---

<sup>1</sup> az EWS projekt keretében TAP eszközök korlátozott számban rendelkezésre állnak



## 2.2. A titkosítás feloldása

Célszerű az end-to-end titkosított csatornák, terminál eszközt, megoldások alkalmazása, mint például:

- saját VPN esetén: a VPN-t végződtesse külön eszközön, a VPN csatornába terelt forgalmat tükrözze ki<sup>2</sup>
- saját HTTPS/SMTS/IMAPS vagy más SSL/TLS-sel védett szolgáltatás esetén:
  - o az SSL/TLS csatorna kiszolgálón történő végződtetése helyett alkalmazzon **SSL/TLS-képes reverse proxy**-t, így a DMZ-ben már nincs szükség titkosításra, a proxy és a szerver közötti titkosítatlan forgalom TAP-pel elemzés céljára duplikálható<sup>3</sup>
  - o amennyiben a kiszolgálón kívüli végződtetés nem megvalósítható, de rendelkezésre áll a szerver titkos kulcsa úgy megfelelő beállítások mellett egy **SSL/TLS decryption** eszköz elő tudja állítani egy TAP által készített titkos forgalom másolata alapján a titkosítatlan forgalmat
- végponti böngészés esetén: alkalmazzon webproxy-ként **SSL/TLS elemzésre és tükrözésre alkalmas új-generációs tűzfalat**<sup>4</sup>, ezzel nemcsak az EWS-hez csatlakozást teszi lehetővé, de lényegesen több lehetősége nyílik a böngészés biztonságának növelésére, valamint az internethasználatra vonatkozó házirendek kikényszerítésére<sup>5</sup>

A csatlakozási tervben nyilatkozzon azon titkosított csatornákról, ahol objektív okból nem lehetséges a titkosítás feloldása.

## 2.3. Hogyan alakítsam ki a kritikus hálózati csomópontokat?

A hozzáférési pontok számának minimalizálása [BMr. 3.3.13.6.2] érdekében biztonsági érzékenység szerint ossza zónákra a rendszerelemeket és erőforrásokat, mint például (a bizalom szintje szerint növekvően):

- internet zóna
- külső DMZ (pl. web/email szerverek/átjárók, távoli elérés)
- intézményi zóna (pl. munkaállomások)
- külső rendszerek zóna (extranet: harmadik fél rendszereivel való kapcsolatok)
- belső DMZ (alkalmazáserverek)

---

<sup>2</sup> ha a VPN csatorna nem dedikált eszközön kerül végződtetésre, akkor akadályba ütközhet minden a csatornába terelt forgalom elemzése, mint pl. a localhost irányú csomagoké

<sup>3</sup> ilyenek pl. a Varnish, nginx, stunnel

<sup>4</sup> ilyenek pl. a ClearTunnel, McAfee Web Gateway, BlueCoat ProxySG, Palo Alto Networks PA-3000/5000/7000, FS BIG-IP Local Traffic Manager

<sup>5</sup> az EWS projekt keretében korlátozott számban rendelkezésre állnak ilyen eszközök, jelezze igényét



- korlátozott zóna (pl. kritikus vagy sok adatot kezelő rendszerek, identity management)
- menedzsment zóna (pl. jump hostok, konfiguráció- és naplómenedzsment)

Minden zónának egy meghatározott belépési pontja legyen, amit forgalomelemző tűzfal felügyel (monitoroz és szűr) [BMr. 3.3.13.6.3]. Csak az alapfeladathoz szükséges forgalom léphessen ki vagy be a zónákból [BMr. 3.3.13.6.3.1.2] [BMr. 3.3.13.6.4]. A (titkosított) alkalmazásrétegbeli kommunikáció közvetlenül ne, csak átjárókon, lehetőleg alkalmazásrétegbeli proxy szervereken keresztül valósuljon meg [BMr. 3.3.10.4, 3.3.13.6.6] [SP800-53r4 AC-7] például a web, e-mail, DNS, RDP esetében; ahol ez nem kívánatos, ott indokolt a jump hostok használata pl. SSH, DB, IPMI eléréshez.

Ilyen kialakítás mellett az EWS szempontjából leginkább kritikus hálózati csomópontok az internet zónát és külső DMZ-t, valamint az extranet zónát és a belső DMZ-t határoló tűzfalak „belső” oldalai.

## 2.4. A naplókezelés minimumkövetelményei

Az EWS által észlelt gyanús események védendő rendszeren belüli kivizsgálhatósága érdekeit figyelembe véve szükséges kialakítani a naplózásba bevont eszközök körét, a naplóbejegyzések információtartalmát és a naplók megőrzési idejét. [BMr. 3.3.12]

A naplózásba minimálisan **bevonandó eszközök** a

- host védelmi eszközök;
- behatolás jelző- és megelőző rendszerek (IDS/IPS);
- VPN vagy más távoli hozzáférés;
- proxy szerverek (web, email, stb.);
- sérülékenység menedzsment eszközök;
- hitelesítő szerverek;
- tűzfalak, vagy engedélyezési listákat kezelő más hálózati eszközök.

A minimális **megőrzési idő** biztonsági naplók esetében legalább 2 hónap.

Minden naplóbejegyzésnek tartalmaznia kell **időbélyeget**. A naplózó fizikai/virtuális eszközök rendszeróráit feltétlenül szinkronizálni kell (NTP, lehetőleg NISZ pontos idő szolgáltatás), az idő szinkronizáció sikeressége szintén **monitorozandó**. Azon rendszerek esetében, ahol az időzóna automatikus átállítása (tipikusan CET és CEST között) nem lehetséges ott javasolt az UTC használata.

A naplózás sikerességét folyamatosan **monitorozni** kell.





A monitorozás alatt olyan folyamat értendő, mely proaktív automatikus észlelés alapján olyan jelzést ad, amelyről a probléma elhárítása érdekében intézkedésre kijelölt személy értesül.

### 3. EWS csatlakozás kialakításához kapcsolódó feladatok

#### 3.1. EWS csatlakozási terv készítése

Az EWS-hez csatlakozó intézmény az NKI-nak jóváhagyásra megküldi a csatlakoztatandó rendszereire vonatkozóan az EWS csatlakozási tervet, mely tartalmazza az alábbiakat:

- az intézmény és a rendszer(ek) kitöltött biztonsági adatlapjait [6.1, 6.2], benne a csatlakozás megvalósításának tervezett módját
- kritikus hálózati csomópontok
- kivezetők típusai
- **[BMr. 3.3.1.3.1.2]** azonosítsa a rendszer **interfészeit**, határozza meg az interfészek paramétereit (pl. fizikai médium, protokoll, maximális/maximálisan engedélyezett sávszélesség)
  - o az átvitt adatok jellegét (protokollok, adattartalom, tartalmaz-e személyes adatot, tipikus sávszélesség)
- **[BMr. 3.2.5.1.1] [SP800-53r4 SA-17]** adja meg a rendszer **infobiztonsági architektúra** fejlesztői leírását:
  - o a biztonsági követelmények alapján szükséges **biztonsági funkcionalitás**, valamint a funkciók **fizikai és logikai eszközökhöz** rendelése
  - o a biztonsági követelményeknek való megfelelés kimutatása a biztonsági funkciók, **eljárások** és **szolgáltatások** egymásra épülésének bemutatásával
- az EWS csatlakozás folyamatának egykapus kommunikációja érdekében az intézmény által kijelölt operatív kapcsolattartó (pl. vagy a 187 /2015. (VII. 13.) Korm. rendelet 8. § szerinti projekt vezetője) elérhetőségeit.

Az egyes pontokhoz benyújtható bármely meglévő, illetve hivatkozható bármely korábban az NKI-hoz benyújtott dokumentum (pl. NEIH OVI űrlap, rendszerterv).

#### 3.2. Műszaki feltételek megvalósítása

A védendő rendszernek az előkészítő tervezés során meghatározott külső vagy zónák közötti interfészekén áthaladó forgalom másolatát az az előkészítő tervezés során meghatározott helyen és módon elérhetővé kell tennie az EWS rendszer szenzorjai számára.

- forgalommásoló funkció megvalósítása
  - o span/TAP /decryption/proxy csatlakoztatása illetve létesítése, konfigurálása
- hálózati összeköttetés
  - o az EWS szenzorok bemeneti interfészeire való kapcsolódás kialakításának támogatása
- nem NISZ telephely esetén felhordó-hálózat és fix sáv szélesség biztosítása az EWS szenzorok menedzsment interfészei számára

### 3.3. Oktatáson való részvétel

Az EWS –hez történő csatlakozás feltétele az ingyenes oktatásokon való részvétel

- o védendő rendszer technikai személyzete, mint EWS felhasználó
- o védendő intézmény integritás-tanácsadói állománya, mint EWS hasznélvező.

### 3.4. Csatlakozás próbaüzemének támogatása

A csatlakozást követően próbaüzemre kerül sor, amelynek során a védendő rendszer személyzete együttműködik az NKI munkatársaival a kivezetők és szenzorok finomhangolásában

- o nem kivezetendő/vizsgálandó forgalmak azonosítása
- o irreleváns elemzési módok (protokollok) azonosítása
- o jelzési/riasztási szintek hangolása
- intézményi felhasználói felület használatba vétele
  - a jogosult személyek regisztrációja
  - EWS bevezetésével kapcsolatos esetleges belső szabályozási feladatok végrehajtása o szabályzók, szerződések felülvizsgálata

### 3.5. Adatvédelem megfelelőségének fenntartása

Az EWS csatlakozáskor különös tekintettel kell lenni az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.) rendelkezéseinek való megfelelésre, különös tekintettel a rendszerek rendeltetéséből (pl. állampolgárok adatainak nyilvántartása), vagy az intézmény munkáltatói jellegéből (pl. dolgozók bejelentkeztetése) adódóan megjelenő **személyes adatok** - mint például természetes személy neve, azonosítója - védelmére.

A közigazgatási szervek törvényi **feladata elektronikus információs rendszereinek védelme**, nevezetesen gondoskodni az elektronikus információs rendszer eseményeinek nyomon



követhetőségéről [Ibtv. 11. § (1) bek.], mely jogalapot teremt az adatkezelő intézménynek a rendszereken tárolt és továbbított személyes adatok biztonsági eseménykezelési célú felhasználására. Az EWS ezen célhoz kötötten támogatja a biztonsági események nyomon követését a műszaki adatok feldolgozásával, de nem az adatok kezelésével - az EWS rendszerben kizárt a személyes adatok felvétele, megváltoztatása, de általában nem biztosított még a személyes adatok beazonosíthatósága sem.

Az **NKI jogosult** az állami és önkormányzati szerveket érintő informatikai biztonsági eseményekhez kapcsolódó, valamint a központosított informatikai és elektronikus hírközlési szolgáltatótól átvett **műszaki, technikai adatok kezelésére** [Ibtv. 19-20. §, 271/2018. (XII. 20.) Korm. rendelet 16-18. §], mely adatok tartalmazhatnak az Infotv. szerint személyes adatnak minősülő adatokat is. Az EWS rendeltetésének nem része, ugyanakkor a felépítésből adódóan elkerülhetetlen a hálózati forgalomban esetlegesen megjelenő személyes adatok feldolgozása, az ebből adódó kockázatok minimalizálására a csatlakozás kialakításakor hálózati csomópontonként az intézmény által jelzett kockázatokkal arányos egyedi **helyettesítő biztonsági intézkedések** [Infotv. 7. §, BMr. 2. szakasz] kerülnek alkalmazásra, mint pl. a feldolgozandó forgalom automatizált előszűrése, kitakarása, potenciálisan személyes adatot tartalmazó naplók megőrzési idejének csökkentése.

Amennyiben az intézmény adatkezelést végez, úgy az EWS szolgáltatásai igénybevételének feltétele lehet az EWS üzemeltetőjének adatfeldolgozói szerződés keretében történő megbízása [Infotv. 10. §], valamint erről az érintettek tájékoztatása.

### 3.6. Belső szabályozás felülvizsgálata

Az EWS-hez csatlakozás, illetve annak előkészítésére megtett intézkedések indokoltá tehetik egyes szabályzók felülvizsgálatát, különösen:

- Biztonsági eseménykezelési eljárásrend [BMr. 3.1.5.1.]
- Biztonságelemzési eljárásrend [BMr. 3.3.4.1]
- Konfigurációkezelési eljárásrend [BMr. 3.3.6.1]
- Naplózási eljárásrend [BMr. 3.3.12.1]
- Rendszer- és kommunikáció védelmi eljárásrend [BMr. 3.3.13.1]
- belső adatvédelmi és adatbiztonsági szabályzatok [Infotv. 24. §]

## 4. EWS csatlakozás fenntartásához kapcsolódó feladatok

### 4.1. EWS üzemeltetési feladatok támogatása

- várható, illetve váratlanul bekövetkezett üzemi események (pl. áramszünet, védendő rendszer leállása) jelzése
- amennyiben EWS rendszer részét képező eszköz van az intézmény fizikai felügyelete alatt (pl. saját telephely esetén), akkor az NKI megbízottjai előre egyeztetett belépésének lehetővé tétele

### 4.2. Változáskezelés

A védendő rendszer felépítését, szolgáltatásait, használatát, kapacitását a fenntartó intézményt, a kapcsolattartást érintő tervezett vagy várható egyedi vagy tartós változásait **jeljeze** az NKI felé az EWS erre a célra kialakított EWS ügyfélkapcsolati felületén keresztül, vagy az NKI felé tett egyéb bejelentéssel összevontan.

Nem várt, vagy akár az NKI által észlelt/jelzett változás esetén **működjön közre** a változás okának és lehetséges következményeinek azonosításában.

Amennyiben egy változás lényegesen érinti az EWS csatlakozást (pl. annak újratervezését teszi szükségessé), úgy **vonja be** az NKI-t a változás tervezésébe, végrehajtásába - ugyanúgy, mint a csatlakozás kialakításakor.

### 4.3. Felhasználó kezelés, tokenek

A felhasználók az EWS-be kéttényezős hitelesítést követően (tudás és birtoklás alapú – jelszó és token) tudnak bejelentkezni. A tokenek kiosztása a védendő rendszer vezetőjének kijelölése alapján, az EWS oktatáson és vizsgán átesett munkatársaknak történik meg. Szerepkör csere esetén a token visszavételre kerül, az új munkatárs számára új token kerül kiadásra. A felhasználói fiók három hónap inaktivitás után felfüggesztésre kerül. A felhasználói fiókokat minden év márciusában megújítani szükséges. Amennyiben ez nem történik meg a fiók felfüggesztésre kerül.



## 5. EWS csatlakozás hatékonyságnövelő ajánlások

### 5.1. Naplókezelés (log management)

Naplókezelés alatt az alkalmazások, operációs rendszerek, szerverek, hálózati és határvédelmi eszközök stb. által előállított eseménynaplók beállítását, gyűjtését, tárolását, elemzését és végül megsemmisítését értjük

A naplókezelés általános célja, hogy az eseményekkel kapcsolatos információk kellő ideig rendelkezésre álljanak a visszaélések, biztonsági incidensek, vagy üzemzavarok észlelése és kivizsgálása érdekében.

A teljes szervezetre vonatkozóan a naplók (logok) fizikailag elkülönített gyűjtése és archiválása csökkenti a logok véletlen megsemmisülésének illetve rosszindulatú manipulálásának lehetőségét. A folyamatos esemény naplózást egy folyamatos mentési eljárásba javasolt illeszteni. A helyi naplók kisebb időszakra, míg az archivált naplók lehetőleg minél nagyobb, akár a teljes mindenkori működés időszakára terjedjenek ki.

Naplózás sikerességét folyamatosan monitorozni kell, bizonyos szolgáltatások letiltása is indokolt lehet a naplózás helyreállításáig.

A **naplózandó események** körét a napló előállítója szerint csoportosítottuk, kiemelve a minden csoportra érvényeseket:

- Általános
  - o Indulás és leállítás
  - o Biztonsági beállítások változása
  - o Felhasználói fiókok illetve csoportok létrehozása/módosítása/törlése
  - o Sikeres és sikertelen bejelentkezési kísérletek, kijelentkezések
  - o Biztonsági események (pl. limit-túllépés, elégtelen jogosultságok, malware észlelés)
  - o Induláskor a naplózó verziója (pl. alkalmazás verzió, OS kernel build, firmware verzió)
- Operációs rendszer
  - o Szolgáltatások indítási kísérlete, indulása és leállása
  - o Eszközök/adathordozók csatlakoztatása és eltávolítása
  - o Rendszeróra változása
- Alkalmazás
  - o Felhasználó által kezdeményezett tranzakciók (pl. űrlap kitöltés, e-mail küldés, HTTP kérés) és azok sikeressége



- o Üzletmenet szempontjából kritikus elemhez történő hozzáférés
- o Kivételek, abnormális leállítás
- Hálózati eszközök (router, switch)
  - o Biztonsági szűrők által megakadályozott forgalom (pl. fw rule, ARP spoof)
  - o Csatlakoztatott eszközök (link-state, switchport, MAC)
  - o Cím kiosztás és -fordítás (DHCP, NAT)
- Határvédelmi eszközök (firewall, IDS/IPS)
  - o Biztonsági szűrők által megakadályozott forgalom (pl. fw rule, IP /domain blacklist)
  - o Ismeretlen gyanús forgalom (pl. port-scan, graylist, SQLi)
  - o Kiugróan magas forgalom (burst, DDoS)
- Egyéb elemek
  - o Biztonsági vonatkozásaik mérlegelése alapján a log-kezelésbe indokolt lehet bevonni további elemeket is:
    - o Hálózati ki-/beviteli eszközök (pl. nyomtatók, kamerák)
    - o Hálózati üzembiztonsági eszközök (pl. UPS, PDU, AC)
    - o Távfelügyeleti interfészek (pl. IPMI/iLO /DRAC/AMT, IP-KVM, VNC)
    - o Fizikai biztonsági rendszerek (pl. beléptető, átlépési pontok, mozgásérzékelők)

További naplókezelési tanácsokat talál az alábbi hivatkozásokon:

- NIST

Guide to Computer Security Log Management (Spedal Publication 800-92)

<http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf>

- Microsoft TechNet

Biztonsági események naplózása - gyakorlati tanácsok

<http://technet.microsoft.com/hu-hu/library/cc778162.aspx>

- Cisco

Network Security Policy: Best Practices White Paper

<http://www.cisco.com/en/US/support/docs/availability/high-availability/13601-secpol.html>



## 5.2. Hálózathasználati házirendek

Nemcsak a rendszer biztonságát növeli, de a kezelendő fals jelzések számát is csökkenti a forgalomáramlási szabályok kialakítása [BMr. 3.3.13.6.3] a nemkívánatos hálózati forgalom csökkentése érdekében, mint például:

- alapfeladattal, közszolgálattal össze nem egyeztethető célú felhasználás korlátozása
  - o fájlcsereelő;
  - o videómegosztók, streaming szolgáltatások;
  - o agresszív, szexuális, illegális tartalmak;
  - o nem-intézményi VPN;
- magáncélú felhasználás szabályozása (ellenjavallat, korlátozás)

Hasonlóan előnyös a felügyelni kívánt forgalom meg nem figyelt csatornákon keresztüli áramlásának korlátozása, elsősorban adminisztratív intézkedésekkel:

- mobilnet, WiFi korlátozása;
- mobil eszközök (pl. pendrive) okostelefon, laptop) csatlakoztatásának szabályozása;
- felhasználói VPN, külső proxy szerverek) és anonimizáló szolgáltatások (pl. TOR) használatának korlátozása.

## 5.3. Határvédelmi eszközök beállítása

A határvédelmi eszközök irányába menő, potenciálisan kártékonyként azonosított hálózati csomagok olyan EWS jelzést eredményezhetnek, amelyek nem jelentenek veszélyt, ha a határvédelmi eszköz azokat nem továbbítja. A továbbítás tényére vonatkozó információ nem feltétlenül áll rendelkezésre (pl. egy a határvédelmi eszköz másik oldalán található felügyelt csomópont forgalmának elemzésével), és így feleslegesen vezethet kivizsgálás kezdeményezéséhez.

Amennyiben a kivezető tűzfal mögött kerül elhelyezésre, úgy a tűzfal lehetőleg a megfelelő ICMP válaszcsoporttal jelezze az elutasított forgalmat a későbbi elemzések támogatása, hamis pozitív jelzések azonosítása érdekében.

## 6. Mellékletek

### 6.1. Védendő intézmény adatlap (minta)

Kategória	Megnevezés	Adat	Megjegyzés
Alapadatok	Intézmény neve	<i>Pelda Hatterintezmeny</i>	
	jogelőd vagy korábbi nevek	<i>Előd Közalapítvány</i>	<i>jogutódlással megszűnt</i>
	felügyelő minisztérium	<i>PM</i>	
Informatikai biztonságért felelős személy (IBF/CISO)	neve	<i>Biztos Ferenc</i>	
	telefon	<i>+36 1 555-5555</i>	
	mobil	<i>+36 1 555-5555</i>	
	email	<i>ibf@pelda.gov.hu</i>	
Biztonsági besorolás	lbtv. hatálya alá esik	<i>igen</i>	<i>biztonsági szint: 3</i>
	nb. védelem alá esik	<i>igen</i>	
	európai vagy nemzeti létfontosságú rendszerelem (KIV)	<i>nem</i>	
	alapvető szolgáltatást nyújtó szolgáltató	<i>nem</i>	
	bejelentésköteles szolgáltató	<i>nem</i>	
	központosított informatikai és elektronikus hírközlési szolgáltató	<i>nem</i>	
Saját online jelenlét	hivatalos honlap(ok)	<i>www.pelda.gov.hu, www.projekt.hu</i>	
	allokált publikus domainnevek	<i>pelda.gov.huy *.pelda.gov.hu, elod.gov.hu, projekt.hu</i>	
	allokált publikus fix IP címek/címtartományok	<i>84.206.1.64/27, 195.10.20.30</i>	





	<b>Internet, email, DNS, VPN, VoIP, stb. szolgáltatók</b>	<i>NISZ, Telekom</i>	<i>Telekom csak másodlagos DNS</i>
--	---	----------------------	--

## 6.2. Védendő rendszer adatlap (minta)

Kategória	Megnevezés	Adat	Megjegyzés
Alapadatok	rendszer neve	<i>Üveggolyó Nyilvántartó (UNy)</i>	
	KÖFOP azonosító (ha KÖFOP projekt)		
	jogszabály(ok)	<i>42/2042. (V/35) PM rendelet</i>	
	fejlesztő cég	<i>Fejlesztő Kft</i>	
	fejlesztés rövid célja	<i>Az üveggolyók hatékony nyilvántartása, API biztosítása az üveggolyó gyárak részére</i>	
	készre jelentés várható ideje	<i>2019.12.31</i>	
	a rendszer a kormányzati adatközponti szolgáltatások igénybevételére vagy igénybevételének vizsgálatára kötelezett	<i>igen</i>	
	KAK felhőben található?	<i>nem</i>	
Ha a KAK felhőben található	SSL terminálás a KAK tűzfalon valósul meg?		
	rendelkezik a rendszer önálló NISZ-nek átadható (nem wildcard) tanúsítvánnyal?		
Ha NEM a KAK	ha nem? hol?	<i>Pelda Hatterintezmény telephelye</i>	<i>a rendszert az intézmény fogja</i>



Kategória	Megnevezés	Adat	Megjegyzés
felhőben található			<i>hostolni a saját telephelyén</i>
	lehetséges-e tűzfal előtti forgalom kicsatolás?	<i>igen</i>	
	a kicsatoláshoz szükséges külön eszköz?	<i>igen</i>	<i>a hálózati eszközök nem alkalmasak port mirroringra</i>
	lehetséges a titkosítás nélküli kicsatolás (pl tűzfal SSL terminálással stb.)?	<i>nem</i>	<i>az SSL terminálás a célszerveren történik, hálózati eszköz erre nem alkalmas</i>
	rendelkezik a rendszer önálló (nem wildcard) tanúsítvánnyal?	<i>igen</i>	
Biztonság osztály	bizalmasság	<i>3</i>	<i>jelenleg: 2</i>
	sértetlenség	<i>3</i>	<i>jelenleg: 1</i>
	rendelkezésre állás	<i>3</i>	<i>elérve : 2015.</i>
IT felelős	neve	<i>Szaki Szabolcs</i>	
	telefon	<i>+36 1 555-5555</i>	
	mobil	<i>+36 1 555-5555</i>	
	email	<i>it@pelda.gov.hu</i>	
Internet kapcsolat	publikusan elérhető felületek	<i>https://www.pelda.gov.hu/uny 84.206.1.65:8081(API) 84.206.1.66:2222(SSH)</i>	
	kijáratok	<i>84.206.1.66:10001-65000</i>	<i>szerverek frissítésére szolgáló kijárat {NAT}</i>



Kategória	Megnevezés	Adat	Megjegyzés
	fizikai interfész és előfizetett sávszélesség	84.206.1.64/27: 1GbE/30 Mbps	kihelyezett NISZ CE routeren, nem redundáns
	átlagos és csúcsterhelés	0.5Mbps>12Mbps	2015. május hónap alapján
	titkosítás aránya	SSL/TLS: 60%, SSH: <1 %	
	különleges és személyes (esetleg minősített) adatok gyakorisága	A bejelentkezésnél, adatmódosításnál személyes adat jelenik meg a hálózaton, tehát gyakori.	
Külső rendszer kapcsolatok	függőségek	NJSZ NJSZ KAÜ	DNS,
	összeköttetések	MÁK KSzR (feltöltés/letöltés)	
Elsődleges kritikus hálózati csomópont	összekötött zónák	az Internet-zónabeli SSL/TLS terheléelosztó és a DMZ-beli webszerverek között	
	fizikai interfészek	2 x 1 GbE [LACP trónk)	
	átlagos és csúcsterhelés	0.4Mbps/10Mbps	
	EWS kivezető típusa	fizikaj TAP	
Másodlagos kritikus hálózati csomópont	összekötött zónák	a DMZ-beli szerverek és az Internet- zónabeli NAT-oló router	
	fizikai interfészek	1 GbE	
	átlagos és csúcsterhelés	0.2Mbps/10Mbps	
	EWS kivezető típusa	SSL/TLS proxy	