Elektronikus információbiztonsági korai figyelmeztető rendszer (EWS) csatlakozás

Ügyféltájékoztató

NEMZETI KIBERBIZTONSÁGI INTÉZET

Vezetői összefoglaló

Az EWS egy központosított hálózati behatolásészlelő/figyelmeztető rendszer (IDS + hálózati forgalomelemzési képességek), amelyet az NBSZ üzemeltet. Célja, hogy a csatlakozó intézmények internet felé nyitott szolgáltatásainak forgalmát szenzorokon keresztül vizsgálva korai észlelést és célzott támogatást nyújtson incidensek esetén. **Kötelező csatlakozni** azoknak, akik a NISZ – Kormányzati Adatközpont (KAK) felhőjében üzemeltetnek rendszereket, illetve akikre a vonatkozó kormányrendeletek ezt előírják; **on-premise csatlakozás** lehetséges és ajánlott, de **opcionális**, és érdemi eszköz- és projektköltséggel jár. Fő műszaki feltétel a hálózati forgalom titkosítatlan átadása a szenzor(ok) felé (KAK-ban jellemzően a tűzfalon SSL-terminálással), valamint a naplózás és időszinkron rendben tartása. A csatlakozás lépései: csatlakozási terv → műszaki kiépítés → kötelező oktatás → próbaüzem → adatvédelmi megfelelés és belső szabályozás frissítése. A csatlakozás tényét alátámasztó vagy kizáró dokumentumot a **fejlesztett alkalmazás üzembe helyezéséhez kapcsolódó szakmai beszámoló** keretében be kell nyújtani.

Jogszabályi háttér, jogosultak és kötelezettek

- **214/2020. (V. 18.) Korm. rendelet** a korai figyelmeztető rendszerről – igénybevételre jogosultak köre (pl. – a honvédelmi létfontosságú rendszerelemek kivételével – az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt üzemeltetők), valamint együttműködési megállapodással bővíthető lehetőség.
- **EWS rendelet 3. § (2)**: a korai figyelmeztető szolgáltatás igénybevétele **kötelező** a Kormányzati Adatközpont (KAK) szolgáltatásait igénybe venni köteles, illetve igénybevételének vizsgálatára kötelezett felhasználók számára.
- **467/2017. (XII. 28.) Korm. rendelet** – a Kormányzati Adatközpont működésére és szolgáltatásaira vonatkozó előírások.

Összefoglalva

- **Kötelező**: NISZ-KAK felhőben üzemeltetett rendszerek (és a jogszabály alapján kötelezettek).
- **Opcionális, de ajánlott**: on-premise üzemeltetők számára; ugyanakkor számolni kell a magas eszköz- és kialakítási költségekkel.

Szolgáltatás rövid leírása (mit nyújt az EWS?)

- Központi szenzorhálózat, **szabály- és eseménykezelés** az NKI és az intézmény együttműködésében.
- **Nyers hálózati forgalom, NetFlow** és Alert logok gyűjtése a törvényben meghatározott ideig incidenskezelési célból; hálózati monitoring, korai észlelés és célzott támogatás.
- Csatlakozás **KAK-ban** külön szenzor elhelyezése nélkül megoldható (elérhető forgalomkicsatolás, SSL terminálás, szenzor-kapacitás). **On-premise** telepítés is lehetséges, de személyes/technikai egyeztetést és tervezést és hátteret igényel.
- Napi hálózatbiztonsági riportok készítése, amennyiben az intézmény részéről van igény egy jól kereshető, a portálok forgalmára optimalizált és az azokra érkező veszélyes forgalmak kimutatására készült technikai összefoglalóra.

Csatlakozási modellek

KAK felhő

- A hálózati forgalom kicsatolása és **SSL terminálás** a KAK tűzfalon történik; a szükséges **tanúsítványt** át kell adni a NISZ részére.
- Javasolt csak az érintett (al)domain(ek)re szóló tanúsítványt használni; a **wildcard** tanúsítvány kerülendő.
- A forgalom a tűzfal és az alkalmazásszerver között jellemzően **dedikált VLAN-ban**, **titkosítatlanul** jut el az elemzési pontig.

On-premise

- Lehetséges, de **opcionális**; **jelentős költséggel** jár (tap/forgalomkicsatoló, decryption/proxy, szenzor, hálózati eszközök, felhordó kapcsolat, üzemeltetés).
- Irányadó eszközigény: a kialakítástól függően **~50 M Ft** nagyságrend (szenzor, switch, router, PBS, felhordás stb.); pontos költség egyedi tervezést igényel.
- Tipikusan a **nyílt internet felé publikált** szolgáltatások forgalmának bevonásával valósul meg.

Műszaki követelmények (kivonat)

Hálózati forgalom átadása

- A kritikus perem-pontokon áthaladó forgalom **másolata** szükséges; a szenzorok felé **titkosítatlan** formában.
- Titkosított forgalom esetén szükséges a **feloldás**: KAK-ban tűzfalon végződő SSL; on-premise esetében reverse proxy/decryption megoldás, vagy dedikált TAP+kulcsmegosztás.

Kritikus hálózati csomópontok

- Internet ↔ DMZ, Extranet ↔ Belső DMZ határain elhelyezett eszközök „belső" oldalai különösen relevánsak.

Naplózás és időszinkron

- Naplózó eszközök köre: végpont- és határvédelmi eszközök, VPN, proxy, hitelesítő szerverek stb.
- **Minimális megőrzés**: legalább **2 hónap**; rendszerórák **NTP**-vel szinkronizálandók (javasolt: UTC).
- **Hozzáférés-szabályozás:** szerepkör alapú (RBAC), naplómegőrzés.

Adatvédelem

A hálózati adatáramlásban **személyes adatok** megjelenhetnek; az EWS adatkezelése célhoz kötött, kockázatcsökkentő intézkedésekkel (előszűrés, kitakarás, rövidebb megőrzés) biztosítandó. Szükség esetén **adatfeldolgozói szerződés**.

Csatlakozás lépései és felelősségek

1) **EWS csatlakozási terv** (NKI jóváhagyással): intézményi/rendszer adatlapok, kritikus csomópontok, interfészparaméterek, infobiztonsági architektúra kivonat, operatív kapcsolattartó megjelölése.
2) **Műszaki feltételek megvalósítása**: forgalommásolás (SPAN/ TAP/ proxy/ decryption), hálózati összeköttetés a szenzorokig, KAK-ban SSL terminálás és tanúsítvány átadás.
3) **Oktatás (kötelező)**: az EWS-hez kapcsolódó **ingyenes** képzés(ek)en a kijelölt IT-szakemberek (és integritás-tanácsadók) részvétele; cél az EWS működésének, felületének és jelzéseinek szakszerű kezelése.
4) **Próbaüzem támogatása**: finomhangolás (nem kivezetendő forgalmak, irreleváns protokollok, riasztási szintek), jogosultak regisztrációja a felületen.
5) **Adatvédelmi megfelelés fenntartása**: tájékoztatás, helyettesítő biztonsági intézkedések alkalmazása, naplómegőrzési idők.
6) **Belső szabályozás felülvizsgálata**: eseménykezelés, konfiguráció- és naplókezelés, rendszer- és kommunikációvédelem, adatvédelmi szabályzatok frissítése.

Oktatás (kötelező követelmény)

- **Cél**: az EWS használatának és jelzéseinek értelmezése, incidenskezelési folyamatba illesztés, jó gyakorlatok megismerése.
- **Résztvevők**: legalább **1–2 kijelölt szakértő** (IT-üzemeltetés/IBF, szükség szerint integritás-tanácsadó).
- **Bizonyítás**: részvételi igazolás/oktatási tanúsítvány csatolása a szakmai beszámolóhoz.

Dokumentációs követelmény

- Az **EWS igénybevételének vizsgálatát** (214/2020. Korm. r.) az **NBSZ NKI** szakterület bevonásával szükséges elvégezni.
- A csatlakozás **tényét alátámasztó vagy kizáró dokumentumot** a **fejlesztett alkalmazás üzembe helyezéséhez kapcsolódó szakmai beszámoló** keretében be kell nyújtani.

Minimális megfelelés és ajánlások

Minimális (kötelező a kötelezetteknek)

- **Csatlakozási terv és jóváhagyás;** forgalom titkosítatlan átadása azonosított pontokon; naplózás+NTP rendben; kötelező oktatás; próbaüzem; adatvédelmi megfelelés; dokumentum benyújtása.

Ajánlott (best practice, on-prem esetén erősen javasolt)

- Proxy/decryption kialakítás a fedettség növelésére; fals pozitív szűrés finomhangolása; házirendek (forgalomáramlási szabályok) szigorítása; határvédelmi eszközök visszajelző konfigurációja (ICMP reject); napló-SIEM integráció.

Gyakori kérdések (GYIK)

Kötelező az EWS csatlakozás?

Kötelező a NISZ–KAK felhőben üzemeltetett rendszerekre (és a jogszabályban meghatározott kötelezetteknek). On-premise esetén lehetséges és ajánlott, de opcionális.

Csak internet felé nyitott szolgáltatásokat vizsgál az EWS?

A csatlakozás elsődlegesen a publikusan elérhető szolgáltatások forgalmára terjed ki (internet/DMZ és extranet/belső DMZ határpontok).

Szükséges az SSL titkosítás feloldása?

Igen. KAK-ban a tűzfalon történik (NISZ üzemeltetésében). On-premise esetben reverse proxy/decryption/TAP megoldással biztosítható.

Át kell adnunk tanúsítványt? Használhatunk wildcardot?

KAK esetén a szükséges tanúsítványt át kell adni a NISZ részére. Javasolt nem wildcard, csak az érintett (al)domain(ek)re szóló tanúsítvány.

Keletkezik-e személyes adat az EWS működése során?

A hálózati forgalomban megjelenhet személyes adat, de az EWS célhoz kötötten, kockázatcsökkentő intézkedésekkel működik; szükség esetén adatfeldolgozói szerződés készül.

Milyen naplómegőrzési minimumra számítsunk?

Legalább 2 hónap biztonsági naplók esetében; az időszinkron kötelező (NTP/UTC javasolt).

Mennyibe kerül az on-prem csatlakozás?

A kialakítástól függ; jellemzően jelentős eszköz- és projektköltség, irányadóan ~50 M Ft eszközpark (szenzor, switch, router, PBS, felhordás stb.). Pontosítás tervezéskor.

Milyen humánerőforrás-igénnyel jár?

Projektvezetés/architekt (kapcsolattartás), hálózat- és rendszermérnök (kicsatolás, titkosítás), IBF/CISO (szabályozás), üzemeltetés (monitorozás, riasztások kezelése).

Mi a minimális határidő?

Tipikusan: előkészítés 2–4 hét, kialakítás 4–8 hét, próbaüzem 2–4 hét; a tényleges ütemezés az intézményi környezettől függ.

A rendszer átalakítása hatással van a csatlakozásra?

Igen. A védett intézmény a korai figyelmeztető szolgáltatás igénybevétele során köteles a rendszer-üzemeltető számára valamennyi olyan, a rendszerei felépítésével és a

rendszerein nyújtott szolgáltatásokkal kapcsolatos információt és az azokban bekövetkezett változást bejelenteni, amely a szolgáltatás nyújtását korlátozza, kizárja, vagy más módon ellehetetleníti. A védett intézmény nem végezhet olyan rendszer-, illetve szolgáltatásfejlesztést, valamint nem hajthat végre olyan szervezeti átalakítást, amely a szolgáltatás nyújtását korlátozza, kizárja, vagy más módon ellehetetleníti.

Kapcsolat és egyeztetés

Kérjük, jelöljék ki a technikai és üzemeltetési kapcsolattartókat (név, e-mail, telefon), és az EWS csatlakozási terv véglegesítése előtt egyeztessenek az NKI-val.

Kérdés esetén keressen minket az alábbi elérhetőségeink egyikén!

Általános kérdések esetén:
titkarsag@nki.gov.hu

Hatósági kérdések esetén:
hatosag@nki.gov.hu

Incidensbejelentéssel kapcsolatos kérdések esetén:
csirt@nki.gov.hu

Csatlakozással kapcsolatos kérdések esetén:
edt@nki.gov.hu

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERBIZTONSÁGI INTÉZET