NIS2 beszállítói adatlap

Az OPEREX üzemeltetési adatot kezel folytonos üzemű, veszélyes létesítményekben. Ha Önök a NIS2 (2024. évi LXIX. tv.) hatálya alá tartoznak, a 21. cikk (2) d) pontja szerint a beszállítóik biztonságáért is felelnek. Ez a lap azt írja le, MIT tesz az OPEREX az egyes intézkedés-csoportokban — megfelelési minősítést szándékosan nem állítunk, azt Önök és a hatóság ítélik meg.

10/10
a 21. cikk (2) intézkedése leképezve

≤24 óra
incidens-értesítés Ön felé

EU
elsődleges adattárolás, titkosított köteten

117/117
bérlői tábla adatbázis-szintű izolációval

Értesítés biztonsági eseményről

- ✓ Biztonsági esemény vagy adatvédelmi incidens észlelésétől számított legfeljebb 24 órán belül értesítjük Önöket — e-mailben, visszaigazolást kérve.
- ✓ Részleges információval is szólunk: nem várjuk meg a kivizsgálás lezárását, és megadjuk a következő tájékoztatás várható idejét.
- ✓ Miért 24 óra: ha Önöket bejelentési kötelezettség terheli, a korai előrejelzést 24 órán belül kell megtenniük — a beszállítói értesítésnek ezt kell kiszolgálnia.
- ✓ A hatósági bejelentés Önöket terheli; mi a kivizsgáláshoz szükséges tényadatot szolgáltatjuk.

Amit NEM állítunk

- — Nincs ISO 27001 tanúsítványunk. Ami van: írott szabályzatok, adatfeldolgozási megállapodás a 32. cikk szerinti intézkedésekkel, és mérhető technikai kontrollok.
- — Külső penetrációs teszt még nem volt — az első enterprise-bevezetés elé ütemezve.
- — Nincs automatikus átállás (failover). A védelmet a 6 óránkénti, próbával igazolt mentés adja.
- — Az off-szerver mentést a tárolószolgáltató titkosítja a saját kulcsaival; a saját kulcsú titkosítás bevezetés alatt.
- — A biztonságért ma egy fő felel, kijelölt második vészhozzáférővel és írott folytonossági tervvel. Enterprise-megbízásnál forráskód-letét vagy on-premise átadás megállapodható.

Ez a lap technikai tényeket rögzít, nem jogi minősítést. Részletes biztonsági áttekintésért és kérdőív-kitöltéshez keressen minket.

A 21. CIKK (2) INTÉZKEDÉSEI ÉS AZ OPEREX

a) Kockázatelemzés, infobiztonsági szabályzatok

Azonosítóval követett gap-nyilvántartás és üzemeltetési szabályzatok (incidenskezelés, hozzáférés-kezelés, offboarding); a formális kockázati nyilvántartás és a rendszeres felülvizsgálati ciklus kialakítás alatt.

b) Incidenskezelés

Írott incidensterv súlyossági osztályokkal, bizonyíték-megőrzési lépéssel és ügyfél-értesítési sablonnal. Észlelés: mély állapot-ellenőrzés, log-figyelő és push-értesítéses ébresztő-csatorna, külső elérhetőség-figyelés. A logokról napi másolat készül a szerveren kívülre (90 nap), így a gépen törölt helyi nyom után is marad mit elemezni.

c) Üzletmenet-folytonosság, mentés

6 óránkénti, önellenőrző off-szerver mentés (SHA-256 visszaolvasás), kb. 6 órás helyreállítási ponttal; EU-joghatóságú tárolóba, 90 napos hosszútávú réteggel. A visszaállítást próbával igazoljuk, nem feltételezzük.

d) Ellátási lánc biztonsága

Nyilvántartott alfeldolgozói lista a jogi dokumentumokban, 30 napos előzetes értesítéssel új alfeldolgozó bevonása előtt. A szoftver-ellátási lánc zárolt függőségekkel, automatikus sebezhetőség-figyeléssel és titok-szivárgás elleni kapuval épül. Kilépéskor teljes adatátadás (minden adattábla gépi olvasható és táblázatkezelős formában, fájl-leltárral és ellenőrzőösszeggel), majd kérésre igazolt törlés.

e) Beszerzés, fejlesztés, sérülékenység-kezelés

Minden változás automatikus ellenőrzéseken megy át (bérlő-izolációs tesztek, biztonsági vizsgálat, titok-kapu), és a kiadás csak zöld ellenőrzés után indulhat. Sérülékenység-bejelentés fogadása RFC 9116 szerinti csatornán.

f) A hatékonyság értékelése

A kontrollokat gépi kapuk őrzik, amelyeket szándékos rontással is megmérünk — így bizonyított, hogy a kapu tényleg fog. Független kód-auditok rendszeresen; külső penetrációs teszt ütemezve.

g) Kiberhigiénia, képzés

Dokumentált üzemeltetési eljárások és hozzáférés-nyilvántartás; a terméket használó szervezet felé a Súgó és a Tudástár ad használati útmutatást.

h) Kriptográfia, titkosítás

TLS minden forgalomra HSTS-sel; az éles kiszolgálón az adatbázis, a fájltár és a helyi mentések titkosított köteten; jelszó-hash és külön titkosított kétfaktor-kulcsok.

i) Hozzáférés-kezelés, eszközkezelés

Kizárólag meghívásos fióklétrehozás, szerep-alapú jogosultság, adatbázis-szinten kikényszerített bérlő-izoláció és append-only auditnyom, amelynek átírását és törlését az adatbázis MINDEN szerepkörnek megtagadja. Nyilvántartott eszköz- és hozzáférés-lista, negyedéves felülvizsgálattal.

j) Többtényezős hitelesítés

A platform-adminisztrátori hozzáféréshez kötelező TOTP-alapú kétfaktoros hitelesítés; bérlői adminisztrátorokra szervezetenként kikényszeríthető. Az üzemeltetői oldalon minden külső szolgáltatói konzolon aktív.