SecuPi

NIS2-megfelelés
a SecuPi adatbiztonsági platformmal

Az érzékeny adatokhoz való kiemelt hozzáférés biztosítása és kezelése

Mi az a NIS2 irányelv?

A NIS2 irányelv az Európai Unió egészére kiterjedő kiberbiztonsági jogszabály, amely jogi eszközökkel törekszik a kiberbiztonság általános szintjének növelésére az EU-ban.

A 2016-ban bevezetett uniós kiberbiztonsági szabályokat a 2023-ban hatályba lépett NIS2 irányelv frissítette. A NIS2 modernizálta a meglévő jogi kereteket, hogy lépést tartson a fokozódó digitalizációval és a folyamatosan fejlődő kiberbiztonsági fenyegetésekkel. A kiberbiztonsági szabályok új szektorokra és entitásokra való kiterjesztésével az irányelv tovább javítja a köz- és magánszféra szereplőinek, az illetékes hatóságoknak és az EU egészének ellenállóképességét és incidenskezelési kapacitásait.

A tagállamok által az említett ágazatokban alapvető szolgáltatásokat nyújtó szereplőkként azonosított vállalkozásoknak megfelelő biztonsági intézkedéseket kell tenniük, és értesíteniük kell az érintett nemzeti hatóságokat a súlyos incidensekről.

Az uniós tagállamoknak 2024. október 18-ig kellett beépíteniük az új irányelvet nemzeti jogrendszerükbe. Ettől az időponttól kezdve minden érintett szervezetnek gondoskodnia kell arról, hogy biztonsági és monitorozási képességei kellően robusztusak legyenek a bírságok és a reputációs károk elkerülése érdekében.

Hasonlóan ahhoz, ahogyan az EU az adatvédelem kérdését a GDPR-ral, a pénzügyi szektort pedig a DORA-val szabályozza, a NIS2 a kiberbiztonsági intézkedések harmonizálására törekszik egy kockázatalapú megközelítés alkalmazásával annak érdekében, hogy kezelje a tagállamokat érintő növekvő kiberfenyegetéseket.

A NIS2 egy olyan keretrendszert biztosít, amely előírások sorát fogalmazza meg az EU-s entitások számára:

1. **Legjobb gyakorlatok:** A biztonsági megközelítés szabványosítása a tagállamokban.
2. **Szabályérvényesítés:** Az irányelv követelményeinek betartatása szigorú büntetések alkalmazásával.
3. **Kötelező incidensjelentés:** Szigorú előírások az incidensek bejelentésére vonatkozóan.

A NIS2 továbbá ösztönzi az EU-tagállamok közötti együttműködést az ellenállóképesség növelése érdekében.

SecuPi – Copyright 2025

A NIS2 irányelv hatálya

Az irányelv 21. cikke a következőképpen foglalja össze a szabályok hatókörét:
„A tagállamok biztosítják, hogy az alapvető és fontos entitások megfelelő és arányos műszaki, üzemeltetési és szervezeti intézkedéseket tegyenek az általuk a tevékenységük során vagy szolgáltatásaik nyújtásához használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelésére, valamint az incidenseknek a szolgáltatásaik igénybevevőire és más szolgáltatásokra gyakorolt hatásának megelőzésére vagy minimalizálására.”

- **A NIS1 hatályának kiterjesztése:** A NIS2 több iparági szektorra és digitális szolgáltatóra terjed ki, beleértve olyan szervezeteket is, amelyek az eredeti NIS1 hatálya alá még nem tartoztak.
- **Új bírságok és büntetések:** A NIS2-re kötelezett, ám azoknak meg nem felelő entitások akár 10 millió euróig vagy a vállalat éves forgalmának 2%-áig terjedő közigazgatási bírsággal sújthatók attól függően, melyik a magasabb összeg.
- **A menedzsment új felelőssége:** Ha egy vállalat nem felel meg a NIS2-nek, a felsővezetők (C-level döntéshozók) személyesen is felelősségre vonhatók súlyos gondatlanságért.
- **Vállalati besorolások frissítése:** A NIS2 „alapvető” (essential) és „fontos” (important) kategóriákba sorolja a szervezeteket a korábbi OES (alapvető szolgáltatást nyújtó szereplő) és DSP (digitális szolgáltató) megnevezések helyett.

Konkrétan a NIS2 követelményei a kockázatok csökkentése érdekében az alábbiakat tartalmazzák:

- Kockázatelemzési és IT-biztonsági szabályok
- Incidenskezelés
- Üzletmenet-folytonosság
- Ellátási lánc biztonsága a beszállítói ökoszisztémában
- Sérülékenységkezelés és nyilvánosságra hozatal
- A kiberkockázat-kezelés hatékonyságának értékelése
- IT-higiéniai gyakorlatok és biztonsági tudatossági képzés
- Kriptográfia és titkosítás
- Humánerőforrás-biztonság, hozzáférés-kezelési szabályok és eszközmenedzsment
- Többtényezős hitelesítés (MFA) és folyamatos hitelesítés alkalmazása

SecuPi – Copyright 2025

Az egyes szervezetek pontos besorolása a társadalomban és a gazdaságban betöltött szerepüktől, valamint más ágazatok tőlük való függőségétől függ. Általánosságban a NIS2 így határozza meg az alapvető és fontos szervezeteket:

Több, mint 250 alkalmazottal rendelkeznek, éves forgalmuk eléri az 50 millió eurót (vagy a mérlegfőösszegük legalább 43 millió euró). Az alapvető szervezeteket proaktívan monitorozzák a NIS2 jogszabályoknak való megfelelés ellenőrzése érdekében.

Kiemelten kritikus ágazatok

Szervezet (entitás)	NIS1 hatálya alatt	NIS2 hatálya alatt
Energia	Némileg	Igen
Távfűtés és távhűtés	Nem	Igen
Olaj és gáz	Igen	Igen
Hidrogén	Nem	Igen
Közlekedés (légi, vasúti, vízi, közúti)	Igen	Igen
Bankszektor	Igen	Igen
Pénzügyi piaci infrastruktúrák	Igen	Igen
Egészségügy	Némileg	Igen
Egészségügyi szolgáltatók	Igen	Igen
EU referencia-laboratóriumok	Nem	Igen
Gyógyszerészeti kutatás és fejlesztés	Nem	Igen
Alapvető gyógyszerészeti termékek és készítmények	Nem	Igen
Orvostechnikai eszközök (vészhelyzeti)	Nem	Igen
Ivóvíz	Igen	Igen
Szennyvíz	Nem	Igen
Digitális infrastruktúra	Igen	Igen
IKT-szolgáltatások	Nem	Igen
Közigazgatás	Nem	Igen
Világűr	Nem	Igen

Kritikus ágazatok

Szervezet (entitás)	NIS1 hatálya alatt	NIS2 hatálya alatt
Postai és futárszolgálatok	Nem	Igen
Hulladékgazdálkodás	Nem	Igen
Vegyszerek gyártása, előállítása, forgalmazása	Nem	Igen
Élelmiszer-termelés, -feldolgozás és -forgalmazás	Nem	Igen
Orvostechnikai eszközök gyártása	Nem	Igen
Számítógépek, elektronikai és optikai termékek gyártása	Nem	Igen
Villamos berendezések gyártása	Nem	Igen
Gépek és berendezések gyártása	Nem	Igen
Gépjármű-, pótkocsi- és félpótkocsi-gyártás	Nem	Igen
Egyéb szállítóeszközök gyártása	Nem	Igen
Digitális szolgáltatók	Némileg	Igen
Online piacterek	Igen	Igen
Keresőprogramok	Igen	Igen
Közösségi média platformok	Nem	Igen
Kutatóintézetek	Nem	Igen

Forrás: Stibbe

SecuPi – Copyright 2025

NIS2 irányelv – Auditok és büntetések

A büntetéseket és szankciókat az Európai Unió NIS2 irányelve határozza meg, a felügyeletet és a jogérvényesítést pedig az alapvető és fontos entitásokat ellenőrző hatóságok végzik.

A hatósági felügyeleti tevékenységek közé tartoznak:

- Rendszeres és célzott auditok.
- Helyszíni és távoli (off-site) ellenőrzések.
- Adatszolgáltatási kérelmek.
- Hozzáférés dokumentumokhoz vagy bizonyítékokhoz.

Büntetések

Az irányelv jelentős büntetéseket ír elő a megfelelés elmulasztása esetén. A szankciók mértéke attól függ, hogy a szervezet „alapvető” vagy „fontos” besorolású-e.

- **Alapvető (Essential) entitások:** A maximális bírság összege 10 000 000 euró, vagy az előző pénzügyi év teljes világszintű éves forgalmának 2%-a attól függően, melyik a magasabb.
- **Fontos (Important) entitások:** A maximális bírság összege 7 000 000 euró, vagy az előző pénzügyi év teljes világszintű éves forgalmának legalább 1,4%-a attól függően, melyik a magasabb.

SecuPi – Copyright 2025

Megfelelés a NIS2 irányelvnek a SecuPi adat fókuszú biztonsági platformjával

A NIS2 irányelvben meghatározott követelmények széles körű kontroll- és érvényesítési képességek bevezetését igénylik, amelyeket szelektíven kell alkalmazni a helyszíni (on-premise), a „federált” és a felhők közötti adatműveletek során.

Főbb megfigyelések arról, miként kezeli a SecuPi a NIS2 technikai biztonsági követelményeit:

1. **Központosított felügyelet:** A SecuPi biztosítja a NIS2 által megkövetelt központi vezérlési képességeket a szervezet teljes adat-ökoszisztémájára kiterjedő, egységes felületű („single pane-of-glass”) megközelítésével.

2. **Közvetlen technikai megfelelés:** A platform közvetlenül válaszol több NIS2 technikai követelményre, beleértve az alábbiakat:

    a Többtényezős hitelesítés (MFA)

    b Titkosítás és kriptográfia

    c Hozzáférés-szabályozási irányelvek

    d Kockázatkezelés

    e Ellátási lánc biztonsága

3. **Incidensjelentés támogatása:** A SecuPi valós idejű monitorozási képességei támogatják a NIS2 által előírt kötelező incidensjelentési követelményeket.

4. **„Zero-code” megközelítés:** A platform kódolást nem igénylő architektúrája segít a szervezeteknek a NIS2 által megkövetelt kontrollok bevezetésében, jelentős fejlesztési költségek nélkül.

5. **Hibrid és multicloud támogatás:** A SecuPi azon képessége, hogy helyi, „federált” és felhőkörnyezetekben is egyaránt működik, különösen alkalmassá teszi a NIS2 által szorgalmazott, határokon átnyúló, átfogó védelmi megközelítés megvalósítására.

SecuPi funkciók a NIS2 viszonylatában

Az alábbi összefoglaló táblázat bemutatja, miként válaszolnak a SecuPi adatbiztonsági platform (DSP) képességei a NIS2 technikai biztonsági követelményeire.

NIS2 követelmény	SecuPi funkciók	Leírás
Kockázatelemzés és IT-biztonsági szabályzatok	Valós idejű láthatóság és monitorozás, adatosztályozás, dinamikus biztonsági szabályok, nulla állandó jogosultság (Zero-standing Privileges)	A SecuPi teljes körű betekintést nyújt minden adathozzáférési és adatkezelési tranzakcióba, biztosítva a végfelhasználói kontextust, az osztályozást és a „forenzikus” elemzést.
Incidenskezelés	Központosított vezérlés, felhasználói viselkedéselemzés (UBA), automatizált riasztások	A szervezet teljes ökoszisztémáját lefedő „single-pane-of-glass” felület lehetővé teszi az adatbiztonsági incidensek gyors észlelését, kivizsgálását és a válaszadást.
Ellátási lánc biztonsága	Kockázatalapú, részletes hozzáférés-szabályozás, érzékeny adatok deidentifikációja (anonimizálása)	A SecuPi attribútumalapú hozzáférés-szabályozással (ABAC), adatosztályozással és többféle anonimizálási módszerrel biztosítja a harmadik felek hozzáférését, kezelve a beszállítói ökoszisztéma kockázatait.
Kiberkockázat-kezelés értékelése	Végponttól végpontig terjedő láthatóság, UBA, valós idejű riasztások	A felhasználói adathozzáférések teljes körű monitorozása minden adattároló és feldolgozó eszköz felett lehetővé teszi a folyamatos kockázatértékelést.
Számítógépes higiénia és biztonsági tudatosság	Kiemelt hozzáférések közvetítése (Privileged Access Brokering)	A SecuPi szigorú kontrollok és láthatóság mellett kezeli a kiemelt jogosultságú felhasználók hozzáférését, biztosítva, hogy az érzékeny adatokhoz csak a „need-to-know” elve alapján lehessen hozzáférni.
Kriptográfia és titkosítás	Végpontok közötti titkosítás és tokenizáció, formátummegőrző titkosítás (FPE), kliensoldali titkosítás, kulcsszétválasztás (HYOK)	A kliensoldali titkosítás az adatbeviteltől a felhasználásig, a kulcsok elkülönítésével együtt garantálja, hogy illetéktelen felhasználók ne férhessenek hozzá az adatokhoz.
HR-biztonság és hozzáférés-szabályozás	Többszempontú ABAC, kiemelt hozzáférések közvetítése, dinamikus szabályok, MFA/SSO	Kontextusfüggő adathozzáférés-szabályozás több attribútum (felhasználó, munkamenet, adathalmaz, IP, osztályozás, helyszín stb.) alapján.
Többtényezős hitelesítés (MFA)	MFA/ SSO integráció	A SecuPi támogatja a többtényezős hitelesítést a kiemelt jogosultságú felhasználók hozzáféréseihez.

A SecuPi **adat fókuszú biztonsági megközelítése** lehetővé teszi a szervezetek számára a **NIS2 előírásainak** hatékony teljesítését. **Valós idejű monitorozással, automatizált szabályérvényesítéssel és dinamikus hozzáférés-szabályozással** a SecuPi garantálja a megfelelést, miközben védi az érzékeny adatokat **mind a helyi (on-premise), mind a felhőkörnyezetekben.** Az egységes felügyeleti felületnek **(„single-pane-of-glass")** és a házirend-alapú érvényesítésnek köszönhetően a SecuPi **ideális megoldás** a NIS2 megfelelőséget célzó szervezetek számára.

A SecuPi-ról

A SecuPi képessé teszi a szervezeteket az adatok biztonságos, szabályos és felelősségteljes felhasználására. A SecuPi díjnyertes megoldása és módszertana újgenerációs adatbiztonsági platformot és adatvédelmi megfelelést kínál a legacy, helyi rendszerektől kezdve a hibrid felhőkörnyezetekig.
A központilag menedzselt, konzisztensen alkalmazott és transzparens, adatvezérelt biztonsági megoldás, amely magában foglalja az attribútumalapú hozzáférés-szabályozást (ABAC), a folyamatos monitorozást, a felhasználói viselkedéselemzést (UBA) és a szabályérvényesítést, a világ legnagyobb pénzügyi szolgáltatói, biztosítói, távközlési vállalatai és kiskereskedői körében használatos.
További információkért látogasson el hozzánk: www.relnet.hu
Értékesítési kérdésekben keresse csapatunkat: sales@relnet.hu