FŐ KÉPESSÉGEK

PROXEDO NETWORK SECURITY

- Biztonságos azonosítás és jogosultságkezelés
- Hálózati forgalom mélységi vizsgálata
- Örökségrendszer felügyelet és kontrol
- NIS2 megfelelés kikényszerítése
- Incidensbejelentési folyamatok támogatása

NIS2 MEGFELELÉS

Európai tűzfal EU szabályozásokhoz

- Kritikus infrastruktúra rendszerek szeparálása
- Hozzáféréskezelés bármilyen rendszerhez
- Részletes naplózás, felügyelet és audit
- Zero Trust hálózati architektúra
- Adatvédelem és titkosítás kikényszerítése
- Remote site üzemeltetés
- Központi konfiguráció management
- On-prem és virtualizáció támogatás

NIS2 kibervédelmi szabályozások

A Proxedo Network Security egy rugalmas, többfunkciós tűzfalmegoldás, mely lehetővé teszi vállalatok számára, hogy megerősítsék a kibervédelmi fenyegetésekkel szembeni rezilienciájukat és teljesítsék a NIS2 előírásait.

A Proxedo személyre szabható szabályrendszerének és folyamatosan fejlődő, kibervédelmi eszköztárának köszönhetően több, mint 20 éve biztosítja kritikus infrastruktúrák, pénzügyi szolgáltatók, egészségügy, telekommunikáció, államigazgatás és ipari szereplők hálózatbiztonságát.

NIS2 incidensbejelentési kötelezettségek

A PNS hálózatfelügyelet biztosítja az összes adat- és információs rendszer forgalmának teljes átláthatóságát. Testreszabható naplózási szabályaival segít a NIS2 által előírt incidensbejelentéshez szükséges információk összegyűjtésében, megjelölésében és a jelentések összeállításában.

Az idő fontos tényező, a NIS2 incidensjelentési követelmények esetében, mivel a vállalatoknak már 24 órával az incidens után korai figyelmeztetést kell adniuk. A PNS olyan eszközkészletet kínál, amely automatikusan összegyűjti és előkészíti az összes szükséges információt a küldéshez, biztosítva, hogy egyetlen incidens se maradjon észrevétlen, és minden jelentés hiánytalanul, valamint határidőkön belül kerüljön kiküldésre.

Rugalmas megoldás bármilyen rendszerhez

A Proxedo tűzfal Deep Packet Inspection technológiát alkalmaz, hogy teljeskörű betekintést adjon a védett rendszerek forgalmába, a Proxedo tartalom alapú szabályainak köszönhetően egy eszközzel kikényszeríthető a biztonság, teljesítmény és folyamatos felügyelet.

A 15+ IT és OT protokoll proxyjával és az egyedi proxyk létrehozására szolgáló eszközkészlettel bármilyen rendszer forgalmára kiterjeszthető felügyeletet kínál, legyen az modern-, egyedi-, vagy örökségrendszer.

BALASYS

info@balasys.hu
Balasys IT Zrt. Minden jog fenntartva.

NIS2 KIBERVÉDELEM ÉS AUTOMATIZÁLT INCIDENS JELENTÉSEK

NIS2 MEGFELELÉS

- **Kibervédelem és Törvényi megfelelés** egy megoldásban
- **Könnyű és gyors integráció** bármilyen rendszerrel
- **NIS2 incidens jelentése készítése** a hálózati forgalomból
- **Automatikus bejelentés** biztonságos csatornákon
- **Incidensbejelentési kötelezettség** teljesítése, büntetések nélkül
- **Gyorsabb NIS2 auditok** és folyamatos ellenőrzés

Ábra 1: *A Proxedo Network Security alkalmazása NIS2 incidensbejelentési kötelezettségek teljesítéséhez*

TECHNIKAI ELŐNYÖK

- 15+ protokoll proxy
- “Best-match” alapú szabály ellenőrzés
- LDAP/AD, Kerberos és RADIUS hozzáféréskezelés
- Erős authentikáció (S/Key, SecurID, X.509, …)
- License- és certificate management
- Titkosítás kikényszerítése TLS 1.3 támogatással
- IPSec és OpenVPN támogatás
- GeoIP, Blacklist, Whitelist
- WAF, AV, sandboxing és URL-szűrő
- IDS/IPS, DLP, MFA & SIEM integráció

Tudjon meg többet

Látogasson el balasys.hu oldalra további információkért a Proxedo megoldásokról

BALASYS

Zero Trust Architectúra és NIS2

A Proxedo Network Security a NIST Zero Trrust Architektúra alapelveit alkalmazza a támadási felületek minimalizálására, valamint a támadók laterális mozgásának megakadályozására és az incidensek által érintett rendszerek teljeskörű behatárolására.

A NIS2 irányelv is javasolja a Zero Trust elvek használatát az incidensek hatékony megelőzésének érdekében. A riasztások általi gyors reagálás, az incidens mihamarabbi izolálása és feltérképezése kulcsfontosságú szerepet játszik az üzletfolytonosság megőrzésében.

Híd az örökségrendszerek felügyeletéhez

A Proxedo képes alkalmazkodni széleskörű felhasználási területhez és erősen specializált környezetek működéséhez egyaránt, mely alól az örökségrendszerek sem képeznek kivételt.

Legyen szó akár kompatibilitási kérdésről, akár a kibervédelmi standardeknek való megfelelésről, a PNS rugalmas megoldást kínál a Biztonsági-, Üzemeltető- és Hálózatos csapatoknak egyaránt.

A PNS a kiszolgáló rendszer módosítása nélkül képes megoldani a kompatibilitási hibákat, kikényszeríteni biztonsági-, titkosítási- és naplózási szabályokat, valamint akár üzleti logikát is.

Bármilyen környezetben alkalmazható

A Proxedo Network Security a VM és hardveres hardveres környezetben egyaránt üzemeltethető, támogatott platformok széles választékával.

Terjessze ki a felügyeletet és modern kibervédelmet az irodai szerverszobától, a kihelyezett telephelyekig és ipari környezetekig.