

— KIBERBIZTONSÁGI ÉS MEGFELELÉSI ÚTMUTATÓ

NIS2-megfelelés

Hogyan segít a ManageEngine az új EU-s követelmények teljesítésében

Gyakorlati útmutató a NIS2-nek megfelelő biztonsági ökoszisztéma kialakításához az Endpoint Central, a Log360, a PAM360, az ADManager Plus, az ADSelfService Plus és a további megoldások segítségével.

IRÁNYELV

EU
2022/2555

21. cikk – kockázatkezelési intézkedések. 23. cikk – incidensbejelentés.

Mit talál benne

Ez az útmutató végigveszi a NIS2 irányelv legfontosabb követelményeit, és termékenként bemutatja, hogyan felel meg nekik a ManageEngine portfóliója – anélkül, hogy azt sugallná, a szoftver önmagában megfelelést jelent.

01 Mit követel valójában a NIS2

02 23. cikk: hatékony incidensbejelentési képesség kialakítása

03 A 21. cikk megfeleltetése a portfóliónak

04 A legnagyobb hiba: a NIS2 egyetlen termék kérdéseként kezelése

05 A technikai terhet viselő termékek

06 Endpoint Central: Az információbiztonság tudatos alapja

07 Log360: biztonsági incidensek észlelése és kivizsgálása

08 PAM360: a privilegizált fiókok védelme

09 ADManager Plus és ADSelfService Plus: identitás és hitelesítés

10 Firewall Analyzer, ServiceDesk Plus, OpManager és RecoveryManager Plus

11 Miért az együttműködés számít, nem egyetlen termék

12 A megfelelés több, mint szoftvervásárlás

Az európai kiberbiztonsági környezet jelentősen megváltozott a NIS2 irányelv (EU 2022/2555) bevezetésével.

Az irányelv szigorítja a kritikus és fontos szektorokban működő szervezetek kiberbiztonsági követelményeit, és nagyobb felelősséget ró rájuk a kiberkockázatok azonosításáért, az incidensek megelőzéséért, a hatékony reagálásért, valamint annak bizonyításáért, hogy a megfelelő biztonsági kontrollok valóban működnek.

A NIS2 nem csupán IT-biztonsági követelmény. Az irányelv szélesebb kiberbiztonsági kockázatkezelési program felépítését írja elő, amely kiterjed az emberekre, a folyamatokra, a technológiára, az incidenskezelésre, az üzletmenet-folytonosságra, az ellátási lánc biztonságára, a hozzáférés-kezelésre, a sérülékenységkezelésre és a biztonsági felügyeletre. A lefedett terület széles, és éppen ezért sok szervezet alábecsüli, mit igényel valójában a megfelelés.

A jó hír az, hogy a követelmények teljesítésének megkezdéséhez a szervezeteknek nem kell teljesen új biztonsági platformot bevezetniük. A ManageEngine megoldásainak kombinációja számos olyan technikai kontrollt biztosít, amely támogatja a szervezet NIS2-megfelelési programját.

Egyetlen szoftvertermék sem teszi önmagában „NIS2-kompatibilissé” a szervezetet. A NIS2 a szervezeti szabályzatok, a vállalatirányítás, az emberek, a folyamatok és a technikai kontrollok együttes működését igényli – ugyanezt a kitélt maga a ManageEngine is megteszi a NIS2-ről szóló anyagaiban.

Mit követel valójában a NIS2

A Network and Information Security 2 irányelv az EU frissített kiberbiztonsági kerete, amelynek célja a kritikus vagy fontos szolgáltatásokat nyújtó szervezetek ellenállóképességének erősítése. Lényegesen kiterjeszti az eredeti NIS irányelv hatályát, és szigorúbb követelményeket állít a kiberbiztonsági kockázatok kezelésére és a jelentős incidensek bejelentésére.

A 21. cikk értelmében a szervezeteknek megfelelő és arányos kockázatkezelési intézkedéseket kell bevezetniük. A lista hosszú, és a legtöbb szervezetnél már megvannak egyes elemei. A probléma ritkán az, hogy semmi nincs – hanem az, hogy az egyes elemek nem kommunikálnak egymással.

A 21. CIKK KITERJED

Kockázatelemzés · incidenskezelés · üzletmenet-folytonosság · ellátási lánc biztonsága · sérülékenységkezelés · kiberbiztonsági szabályzatok és oktatás · kriptográfia · humánerőforrás-biztonság · hozzáférés-kezelés · eszközkezelés · többfaktoros hitelesítés

23. cikk: hatékony incidensbejelentési képesség kialakítása

A NIS2 szerint a szervezeteknek fel kell tudniuk ismerni, amikor egy kiberbiztonsági incidens súlyos üzleti eseménnyé válik, és cselekedniük kell, mielőtt a következmények eszkalálódna. A NIS2 összehangolt bejelentési képességet ír elő, amelyet megbízható információk, világos felelősségi körök és vezetői felügyelet támogat.

24 ó

Korai előrejelzés

72 ó

Incidensbejelentés

Zárás

Előrehaladási és záró jelentés

A GYAKORLATBAN A NIS2 20., 21. ÉS 23. CIKKÉNEK TELJESÍTÉSÉHEZ A SZERVEZETEKNEK KÉPESNEK KELL LENNIÜK:

- | | |
|---|--|
| <p>01 Meghatározni, hogyan azonosítják, értékelik és eszkalálják a jelentős incidenseket, figyelembe véve a szolgáltatáskiesést, a pénzügyi következményeket, valamint az ügyfelekre és más felekre gyakorolt hatást;</p> <p>02 Biztosítani a hatósági kommunikációt, ideértve a 24 órán belüli korai előrejelzést, a 72 órán belüli incidensbejelentést, valamint a szükséges további előrehaladási vagy záró jelentéseket (23. cikk);</p> <p>03 A vezetőség számára időszerű és megbízható incidensinformációt biztosítani (20. cikk), lehetővé téve az incidens, annak üzleti hatása és a megtett válaszingtezkedések megalapozott felügyeletét;</p> <p>04 Világos felelősségi köröket meghatározni az incidens értékelésére, a reagálásra és a bejelentésre (20. és 21. cikk), hogy az üzleti, biztonsági, IT- és egyéb érintettek a tisztázatlan felelősség miatti késedelem nélkül tudjanak cselekedni;</p> | <p>05 Auditálható incidensnyilvántartást és bizonyítékokat vezetni (21. cikk), köztük a biztonsági eseményeket, a rendszeraktivitást, a válasz- és javító intézkedéseket, amelyek a kivizsgáláshoz, a bejelentéshez és a folyamatos fejlesztéshez szükségesek;</p> <p>06 Fenntartani a kommunikációt az incidens teljes életciklusa alatt (23. cikk), beleértve a releváns előrehaladási tájékoztatásokat és a kiváltó ok, a hatás, a reagálás és a megelőző fejlesztések záró összegzését;</p> <p>07 Összekapcsolni az incidensbejelentést a szolgáltatás-visszaállítással és az ellenállóképességet célzó tevékenységekkel (21. cikk), biztosítva, hogy az érintett szolgáltatások biztonságosan álljanak helyre, a tanulságok pedig beépüljenek a jövőbeli biztonsági és folytonossági intézkedésekbe;</p> |
|---|--|

A ManageEngine megoldásai olyan technikai képességeket biztosítanak, amelyek támogatják a NIS2 20., 21. és 23. cikkének szervezeti megvalósítását.

A Log360 és a Firewall Analyzer betekintést ad a biztonsági eseményekbe, az OpManager segít felmérni az infrastruktúra- és szolgáltatáskiesést, míg az Endpoint Central, a PAM360, az ADManager Plus és az ADSelfService Plus a kártétel korlátozását és a hozzáférés védelmét támogatja. A ServiceDesk Plus koordinálhatja a válaszingtezkedéseket és vezetheti az incidensnyilvántartást, a RecoveryManager Plus pedig a védett Microsoft-környezetek helyreállítását támogatja.

A 21. cikk megfeleltetése a portfóliónak

Áttekintés arról, melyik követelményt melyik termék fedi le. A ManageEngine portfólióját közvetlenül a 21. és 23. cikk egyes követelményeihez rendeli; a technikai réteg azonban csak egy része annak, amit az egyes követelmények igényelnek.

A 21. CIKK KÖVETELMÉNYE	ELSŐDLEGES TERMÉK	MIT NYÚJT
Sérülékenység- és patchkezelés	Endpoint Central	Automatikus felmérés és patchtelepítés a végpontokon
Eszközkezelés	Endpoint Central	Központi hardver- és szoftverleltár, eszközkontroll
Incidensészlelés és -kezelés	Log360	SIEM, központi naplózás, korreláció, riasztás, kivizsgálás
Hozzáférés-kezelés	PAM360 · ADManager Plus	Privilegizált hozzáférés kezelése, hozzáférés-felügyelet, jogosultság-átvizsgálás
Többfaktoros hitelesítés	ADSelfService Plus	MFA, adaptív hitelesítés, jelszószabályzat kikényszerítése, SSO
Hálózatbiztonság	Firewall Analyzer · OpManager	Tűzfalnaplók elemzése, konfigurációs audit, rendelkezésre állás felügyelete
Üzletmenet-folytonosság és katasztrófa-helyreállítás	RecoveryManager Plus	Az Active Directory és a Microsoft 365 mentése és helyreállítása
Szabályzatok, folyamatok és auditbizonyítékok	ServiceDesk Plus	Dokumentált incidens-, változás- és problémafolyamatok nyilvántartással

A legnagyobb hiba: a NIS2 egyetlen termék kérdéseként kezelése

A patchelés önmagában nem jelent NIS2-megfelelést. A szervezetnek ennél jóval hosszabb kérdéslistára kell válaszolnia – folyamatosan és bizonyítékokkal.

Itt mutatkozik meg egy integrált ManageEngine biztonsági és IT-menedzsment környezet értéke: összekapcsolja ezeket a kérdéseket, ahelyett hogy mindegyiket külön, egymástól elszigetelt eszközre hagyná.

A probléma ritkán az, hogy semmi nincs. Hanem az, hogy az egyes elemek nem kommunikálnak egymással.

KÉRDÉSEK, AMELYEKET AZ AUDITOR FELTESZ

Milyen eszközök vannak?

Milyen sérülékenységek vannak?

Kinek van hozzáférése?

Kinek van privilegizált hozzáférése?

Mi történik a hálózaton?

Észlelik a gyanús tevékenységeket?

Kivizsgálják az incidenseket?

Biztonságosak a tűzfalkonfigurációk?

Megőrzik a naplókat?

Helyre tud állni a szervezet egy támadás után?

Bizonyítani tudja a megfelelést az auditorok előtt?

A technikai terhet viselő termékek

Néhány ManageEngine-termék együtt a NIS2 technikai követelményeinek jelentős részét lefedi, és mindegyik más elemért felel.

EC Endpoint Central

Végpontbiztonság, patchelés, sérülékenységi és eszköz kezelés, eszközkontroll

L36 Log360

SIEM, központi naplózás, fenyegetésészlelés, incidenskivizsgálás

PAM PAM360

Privilegizált hozzáférés kezelése és a privilegizált fiókok biztonsága

ADM ADManager Plus

Identitáskezelés, hozzáférés-felügyelet, Active Directory biztonsága

ADS ADSelfService Plus

MFA, jelszóbiztonság, identitásvédelem

FWA Firewall Analyzer

Tűzfalfelügyelet, konfigurációs audit, hálózatbiztonság

SDP ServiceDesk Plus

Incidens- és változáskezelés, ITSM-folyamatok, auditbizonyítékok

OPM OpManager

A hálózat és az infrastruktúra rendelkezésre állásának felügyelete

RMP RecoveryManager Plus

Microsoft-környezetek mentése és helyreállítása

EC

Endpoint Central: Az információbiztonság tudatos alapja

A modern támadások gyakran sérülékeny végpontokkal kezdődnek. Egy nem patchelt laptop, egy elavult alkalmazás vagy egy rosszul konfigurált munkaállomás belépési pontot adhat a támadónak a szervezetbe.

Az Endpoint Central erre automatikus patchkezeléssel, sérülékenységfelméréssel, alkalmazás és eszköz-kezeléssel, végpontkonfigurációval, USB és periféria-kontrollal, adatszivárgás-megelőzési képességekkel, titkosítás és jogosultságkezeléssel, végpontbiztonsággal, megfelelési jelentésekkel, valamint végpontkarantén és helyreállítás funkcióval válaszol.

Az üzleti eredmény jobb végpont-átláthatóság, gyorsabb hibajavítás és erősebb kiberhigiénia, érezhetően kevesebb kézi munkával az IT-csapatok részéről.

KOCKÁZAT → KONTROLL

Sérülékeny és nem patchelt végpontok	Automatikus sérülékenységfelmérés és patchtelepítés
Ismeretlen eszközök a környezetben	Központi átláthatóság a hardver- és szoftvertvagyon felett
Cserélhető adathordozók engedély nélküli használata	USB- és periféria-kontroll
Gyenge végpontbiztonsági konfiguráció	Központi konfiguráció- és megfeleléskezelés

L36

Log360: biztonsági incidensek észlelése és kivizsgálása

A NIS2 nem csak a támadások megelőzéséről szól; a szervezeteknek észlelniük, kezelniük és kivizsgálniuk is kell tudni a biztonsági incidenseket. A Log360 központi naplókezelést és SIEM-képességeket nyújt, amelyekkel biztonsági események gyűjthetők és elemezhetők az Active Directoryból, Windows-kiszolgálókról, hálózati eszközökről, tűzfalakról, alkalmazásokból, felhőkörnyezetekből, végpontokról, adatbázisokból és hitelesítési rendszerekből. A platform korrelálja az eseményeket, és riasztást ad a gyanús tevékenységre.

Központi felügyelet nélkül egy teljes támadási lánc rekonstruálása valóban nehéz. A Log360 összegyűjti és korrelálja ezeket az eseményeket, így a biztonsági csapat egyetlen központi platformról vizsgálhat – és olyan auditnyommal rendelkezik, amelyet kérésre valóban be tud mutatni.

EGY KOMPROMITTÁLT FIÓK, ÖT ESEMÉNY

- 01 Bejelentkezik az Active Directoryba
- 02 Jogosultság-emelést kísérel meg
- 03 Több kiszolgálóhoz hozzáfér
- 04 Gyanús fiókot hoz létre
- 05 Törli a biztonsági naplókat

PAM

PAM360: a privilegizált fiókok védelme

A túlzott privilegizált hozzáférés minden szervezetben az egyik legsúlyosabb kockázat. Az a támadó, aki megszerez egy tartományi rendszergazdai vagy más privilegizált fiókot, laterálisan mozoghat a hálózatban, és elérheti a kritikus rendszereket.

A PAM360 erre a privilegizált hozzáférés kezelésével válaszol: felderíti a privilegizált fiókokat, védi azok hitelesítő adatait, kontrollálja az adminisztratív hozzáférést, kezeli a privilegizált munkameneteket, szerep alapú hozzáférést alkalmaz, felügyeli a privilegizált tevékenységet, csökkenti az állandó jogosultságokat, és auditálja a privilegizált műveleteket.

A megfelelő személynek a megfelelő ideig kell megfelelő hozzáféréssel bírnia, ami csökkenti annak kockázatát, hogy kompromittált hitelesítő adatok széles körű kárt okozzanak.

AZ ÁLLANDÓ JELSZAVAKTÓL A KONTROLLÁLT HOZZÁFÉRÉSIG

Privilegizált hozzáférés kérése

Jóváhagyás

Kontrollált hozzáférés

Munkamenet-felügyelet

Jelszórotáció

Alapvetően erősebb biztonsági modell, mint állandó rendszergazdai hitelesítő adatokat kiosztani a kritikus kiszolgálókhoz.

ADManager Plus és ADSelfService Plus: identitás és hitelesítés

ADM ADManager Plus

Az identitásbiztonság a NIS2 másik alappillére. Az ADManager Plus segít az IT-csapatoknak a felhasználók, csoportok és számítógépek kezelésében, az adminisztratív feladatok delegálásában, a fiókkezelés automatizálásában, az inaktív fiókok azonosításában, auditjelentések készítésében, a jogosultságok kezelésében és az identitásfolyamatok egységesítésében.

Az identitás-életciklus kezelésének automatizálása és a jogosultságok rendszeres átvizsgálása csökkenti az identitáshoz kötődő kockázatot, és szilárd bizonyítékot ad arról, kinek van hozzáférése a kritikus rendszerekhez.

Volt munkatársak aktív fiókkal

Túlzott jogosultságok

Használaton kívüli fiókok

Rosszul kezelt csoportok

Követhetetlen hozzáférési jogok

ADS ADSelfService Plus

Az ADSelfService Plus ezt magának a hitelesítésnek az erősítésével egészíti ki: többfaktoros és adaptív hitelesítés, jelszószabályzat kikényszerítése, önkiszolgáló jelszó-visszaállítás, fiókfeloldás, SSO és jelszószinkronizáció.

Még ha a támadó megszerzi a felhasználó jelszavát, az MFA olyan réteget ad, amely lényegesen megnehezíti az illetéktelen hozzáférést.

Firewall Analyzer, ServiceDesk Plus, OpManager és RecoveryManager Plus

FWA Firewall Analyzer

A tűzfal önmagában nem elég; a szervezetnek tudnia kell, milyen forgalom halad át rajta, előfordulnak-e gyanús kapcsolatok, ki módosította a konfigurációt, és kivizsgálhatók-e a korábbi események. A Firewall Analyzer több gyártó eszközeihez nyújt tűzfalnapló-elemzést és konfigurációs auditot.

SDP ServiceDesk Plus

A kiberbiztonság folyamatkérdés is, nem csupán technikai. A ServiceDesk Plus dokumentált, auditálható munkafolyamatokat hoz az incidens-, változás-, probléma- és eszközkezelésbe.

Észlelve › Értékelve › Jóváhagyva › Javítva › Ellenőrizve ›

Dokumentálva

OPM OpManager

Az OpManager teljessé teszi az átláthatóságot: kiszolgálókat, switcheket, routereket, hálózati eszközöket és az infrastruktúra általános rendelkezésre állását felügyeli, és elég korán észleli a hibákat ahhoz, hogy megvédje az üzletmenet folytonosságát.

RMP RecoveryManager Plus

A Microsoft-környezetek óriási mennyiségű üzletkritikus adatot tárolnak az Active Directoryban, a Microsoft 365-ben, az Exchange Online-ban, a SharePoint Online-ban és a OneDrive-ban. A RecoveryManager Plus védi és helyreállítja ezeket az adatokat – ami kulcsfontosságú ransomware-forgatókönyvekben, ahol a nehéz nap és a működés végét jelentő esemény között az a különbség, hogy a helyreállítás egyáltalán lehetséges-e.

Miért az együttműködés számít, nem egyetlen termék

A legnagyobb előny nem egyetlen eszköz, hanem az, hogy összekapcsolt biztonsági és IT-menedzsment ökoszisztéma építhető belőlük – valódi kiberbiztonsági életciklus, amely szorosan illeszkedik a NIS2 mögötti kockázatkezelési szemlélethez.

AZONOSÍTÁS

Az Endpoint Central megtalálja és védi a végpontot

VÉDELEM

Az ADManager Plus és a PAM360 kezeli az identitásokat és a privilegizált hozzáférést

ÉSZLELÉS

A Log360 figyeli, mi történik; a Firewall Analyzer a hálózatot őrzi

REAGÁLÁS

A ServiceDesk Plus kezeli az incidenseket és a javítást

HELYREÁLLÍTÁS

A RecoveryManager Plus helyreállítja a kritikus rendszereket és adatokat

JELENTÉS

Irányítópultok, jelentések és változásnylvántartás az auditoroknak

ÜZLETI ELŐNYÖK

Jobb átláthatóság a végpontok, felhasználók, hálózatok, privilegizált fiókok és biztonsági események felett

Gyorsabb incidensészlelés és jobb kivizsgálás központi naplók és auditnyomok

Gyorsabb sérülékenységmentesítés automatikus felmérés és patchelés

Jobb üzletmenet-folytonosság mentés, helyreállítás és infrastruktúra-felügyelet révén

Erősebb identitásbiztonság MFA és hozzáférés-kontroll

Kisebb üzemeltetési komplexitás, mint elszigetelt ponteszközök kezelésénél

A megfelelés több, mint szoftvervásárlás

Az Endpoint Central, a Log360, a PAM360 vagy bármely más biztonsági termék megvásárlása nem teszi automatikusan NIS2-kompatibilissé a szervezetet. A NIS2 az emberek, a folyamatok és a technológia együttes működését igényli.

EMBEREK

Kiberbiztonsági tudatosság, világos felelősségi körök, vezetői elkötelezettség, munkavállalói oktatás

FOLYAMATOK

Kockázatértékelés, incidenskezelés, üzletmenet-folytonosság, sérülékenységkezelés, hozzáférés-átvizsgálás, beszállítói kockázatkezelés

TECHNOLÓGIA

Végpontbiztonság, SIEM, MFA, PAM, hálózatfelügyelet, sérülékenységkezelés, mentés és helyreállítás

A ManageEngine e technológiai réteg jelentős részét biztosíthatja, a körülötte lévő vállalatirányítást, szabályzatokat és folyamatokat azonban a szervezetnek magának kell felépítenie.

A NIS2 jelentős szemléletváltást jelent abban, ahogyan az európai szervezetek a kiberbiztonsághoz állnak. A cél már nem az, hogy vírusvédelmet vagy tűzfalat telepítsenek, és lezártnak tekintsék a témát – a szervezeteknek strukturált, kockázatalapú, folyamatosan felügyelt kiberbiztonsági programot kell felmutatniuk.

KÖVETKEZŐ LÉPÉS

Készen áll a NIS2-nek megfelelő biztonsági architektúra kialakítására?

Az MWT Solutions a ManageEngine disztribútora Baltikumban, Lengyelországban, Csehországban, Szlovákiában és Magyarországon. Beszéljünk arról, hogyan illeszthető a ManageEngine portfóliója a szervezete NIS2-követelményeihez.

mwtsolutions.eu