

NIS2-richtlijn: beveilig uw geconnecteerde productie

09 april 2025, 09:47

Thierry Coutelier
Olivier Gramaccia

Bent u klaar om te voldoen aan de nieuwe cyberbeveiligingsverplichtingen opgelegd door de NIS2-richtlijn?

Geconnecteerde sensoren, intelligente machines, cobots... Het Internet of Things (IoT) brengt een ware revolutie teweeg voor de industriële productie. Processen worden efficiënter, de productiviteit gaat omhoog en het concurrentievermogen neemt toe. Tegelijkertijd stelt deze technologische revolutie uw bedrijf echter bloot aan nieuwe cyberrisico's. De NIS2-richtlijn helpt u om uw cyberbeveiliging op te krikken.

De Europese NIS2-richtlijn is sinds 18 oktober 2024 in België van kracht. Ze verplicht bedrijven in kritieke sectoren – zoals productiebedrijven – om hun cyberweerbaarheid te versterken.

NIS2: een wettelijke verplichting en een strategische uitdaging

Als uw bedrijf geconnecteerde apparatuur (IoT) gebruikt voor productie, opslag of logistiek, dan is de NIS2-richtlijn mogelijk ook op u van toepassing. En dat geldt niet alleen vanuit technisch oogpunt: bij niet-naleving kunnen bedrijfsleiders aansprakelijk worden gesteld. Daarom moet u weten op welk niveau uw bedrijf geclassificeerd is om uw verplichtingen te begrijpen.

NIS2 negeren? Dat houdt drie grote risico's in:

- **Verstoring van de activiteiten:** een cyberaanval kan uw productielijnen lamleggen, wat tot financiële verliezen en vertraagde leveringen kan leiden.
- **Lekken van gevoelige gegevens:** de vertrouwelijke informatie over uw producten, klanten, processen of financiën kan in gevaar komen.
- **Reputatieschade:** een beveiligingslek kan het vertrouwen van uw klanten en partners schaden.

Bezoek deze webpagina van het CCB om uw NIS2-niveau te bepalen:

Bepaal uw NIS2-niveau

CyberFundamentals: de conformiteitsmethode van het CCB

Om bedrijven te helpen, heeft het Centrum voor Cybersecurity België (CCB) het zogeheten ‘CyberFundamentals Framework’ opgezet. Dat kader stelt concrete maatregelen voor, afgestemd op de omvang en het risicoprofiel van elke organisatie. CyberFundamentals onderscheidt vier verzekeringsniveaus: ‘Small’, ‘Basis’, ‘Belangrijk’ en ‘Essentieel’. Andere certificeringen, zoals ISO 27001, kunnen de naleving van NIS2 vergemakkelijken. De geïmplementeerde cyberbeveiligingsmaatregelen moeten in verhouding staan tot de risico's die het bedrijf loopt.

Heeft uw bedrijf meer dan 50 VTE's of een omzet van meer dan € 10 miljoen, dan bent u ten minste onderworpen aan het niveau ‘Belangrijk’ van NIS2. En zelfs als dat niet het geval is, kunt u uw systemen doeltreffend beveiligen en de verwachtingen van uw klanten inlossen door de aanbevelingen van het ‘Basis’-niveau op te volgen.

‘Basis’-niveau: de fundamenten om uw geconnecteerde objecten te beschermen

Het ‘Basis’-niveau heeft het niet expliciet over het IoT, maar verschillende maatregelen zijn direct van toepassing op deze systemen. Hier volgt een selectie, onderverdeeld in vijf categorieën: Identificeren:

Identificeren:

- **ID.AM-1:** Hierbij wordt een inventaris van fysieke apparaten opgesteld, inclusief alle geconnecteerde objecten (IoT) die verbonden zijn met het netwerk van de organisatie.
- **ID.AM-2:** Net als ID.AM-1 richt deze maatregel zich op de inventarisering van softwareplatformen en -toepassingen. Daarom is het ook noodzakelijk om een lijst te maken van de specifieke software en toepassingen die door IoT-apparaten worden gebruikt.
- **ID.AM-3:** Deze maatregel legt de nadruk op het documenteren van de organisatorische communicatie en gegevensstromen. In de context van het IoT is het belangrijk deze stromen

in kaart te brengen: waar komen IoT-gegevens vandaan, waar gaan ze naartoe en hoe circuleren ze?
- **ID.RA-1:** Identificeert de bedreigingen en kwetsbaarheden van uw IoT-apparaten. Zo kunt u het risico zo nauwkeurig mogelijk inschatten en dienovereenkomstig handelen.

Plannen:

- **PR.AC-1:** Beheer de identificatie van geconnecteerde objecten (IoT) op de juiste manier: vermijd standaardwachtwoorden, pas sterke regels toe en deel ze niet.
- **PR.AC-3 (belangrijke maatregel):** Beveilig de externe toegang tot IoT-apparaten met een sterke identificatie (zoals MFA). Isoleer apparaten indien mogelijk ook van het hoofdnetwerk (zie PR.AC-5).
- **PR.AC-4 (belangrijke maatregel):** Hanteer het principe van minimale rechten voor IoT-apparaten: geef gebruikers of systemen alleen de toegang die ze nodig hebben.
- **PR.AC-5:** Segmenteer het netwerk om geconnecteerde objecten te isoleren en het risico van verspreiding in het geval van een aanval te beperken.
- **PR.DS-1:** Versleutel gegevens die zijn opgeslagen op IoT-apparaten, en indien mogelijk, ook gegevens die onderweg zijn (PR.DS-2).
- **PR.IP-4 (belangrijke maatregel):** Maak regelmatig back-ups van gegevens en configuraties van IoT-apparaten en test deze.
- **PR.MA-1 (belangrijke maatregel):** Houd apparaten up-to-date met de nieuwste patches en beveiligingsupdates.
- **PR.PT-1 (belangrijke maatregel):** Maak en test regelmatig back-ups van gegevens en configuraties van IoT-apparaten. Dat maakt het mogelijk om apparaten en gegevens na incidenten te herstellen naar de toestand van vóór het incident.
- **PR.PT-4:** Onderhoud IoT-apparaten om hun beveiliging te garanderen. Installeer patches en beveiligingsupdates voor de besturingssystemen en software die door IoT-apparaten worden gebruikt.

Detecteren:

- **DE.CM-1:** Controleer het netwerk op verdachte activiteiten van IoT-apparaten en gebruik tools om afwijkingen te detecteren.
- **DE.CM-4 (belangrijke maatregel):** Spoor malware op om IoT-apparaten te beschermen. Gebruik anti-malwareoplossingen om infecties te blokkeren die tegen deze apparaten zijn gericht.

Beantwoorden:

- **RS.RP-1:** Voorzie een responsplan om te reageren op IoT-incidenten, inclusief detectie, analyse, insluiting, verwijdering en herstel van aangetaste IoT-apparaten.

Herstellen:

- **RC.RP-1:** Stel een herstelplan op voor IoT-apparaten en bijbehorende services na een beveiligingsincident. Dat plan moet procedures bevatten om gegevens te herstellen, apparaten te herconfigureren en de dienstverlening te hervatten.

Goed om te weten: deze lijst is niet volledig. Naargelang de context en de specifieke behoeften van de organisatie kunnen ook andere maatregelen relevant zijn voor de beveiliging van IoT-apparaten.

De cyberbeveiligingsmaatregelen van het ‘Basis’-niveau hebben een aanzienlijke invloed op de beveiliging van geconnecteerde objecten (IoT). Door deze maatregelen te implementeren op het niveau van de organisatie, versterkt u uw gegevensproductie, verlaagt u het risico op cyberaanvallen en vergroot u uw cyberweerbaarheid in een omgeving waar het IoT steeds meer aanwezig is.

Raadpleeg de volledige handleiding voor het ‘Basis’-niveau:

CyberFundamentals - 'Basis'-niveau (PDF)

Niveau ‘Belangrijk’: voor middelgrote en grote bedrijven

Middelgrote en grote organisaties moeten verder gaan. Het niveau ‘Belangrijk’ bevat de volgende aanvullende maatregelen:

- Afhankelijkheden en kritieke functies identificeren (ID.BE-4)
- Veerkrachtvereisten vaststellen (ID.BE-5)
- De risico’s van de toeleveringsketen evalueren (ID.SC)
- De configuratie van apparatuur beveiligen (PR.IP-1)
- Het gebruik van verwisselbare media beperken (PR.RT-2)
- Het principe van de minste functionaliteit toepassen (PR.PT-3)
- De faciliteiten fysiek controleren (DE.CM-2)
- Kwetsbaarheden analyseren (DE.CM-8)

Door deze maatregelen toe te passen, voldoet uw kmo aan de wet en beschermt ze haar activiteiten, gegevens en reputatie. Door uw IoT-apparaten en het beheer ervan te beveiligen, versterkt u de weerbaarheid van uw bedrijf tegen cyberbedreigingen en verzekert u een voorspoedige toekomst.

In een notendop

- NIS2 is sinds 18 oktober 2024 in België van kracht.
- Deze regeling geldt voor tal van industriële kmo's die het IoT gebruiken.
- Het ‘Basis’-niveau van het CCB vormt een solide basis om uw apparatuur te beveiligen.
- Sirris kan u helpen om conformiteit te bereiken.

Sirris kan u helpen compliance te bereiken

Om de NIS2-richtlijn te implementeren hebt u nood aan een duidelijke strategie en een goed inzicht in de industriële uitdagingen.

Sirris kan u helpen om:

- Uw IoT-risico's in te schatten.
- Uw NIS2-niveau te bepalen.
- De beste praktijken te implementeren.
- De opleiding van uw teams te versterken.

Onderneem nu actie!

Bescherm uw geconnecteerde objecten. Beveilig uw productie. Bereid u voor op de toekomst.

Neem contact op met een Sirris-expert:

Thierry COUTELIER

Raadpleeg de richtlijn CyberFundamentals – 'Basis'-niveau (PDF)

Zie ook

- De officiële NIS2-pagina – CCB
- De gratis CyberActive-opleidingen (project mede gefinancierd door de FOD Economie en de Europese Unie)

Artikel geschreven in het kader van de Normen-Antennes, met de steun van de FOD Economie.

Auteurs



Thierry Coutelier



Olivier Gramaccia