



NIS2-richtlijn: hoe kan de Belgische industrie zich verdedigen tegen cyberdreigingen?

28 maart 2025, 10:16

Thierry Coutelier

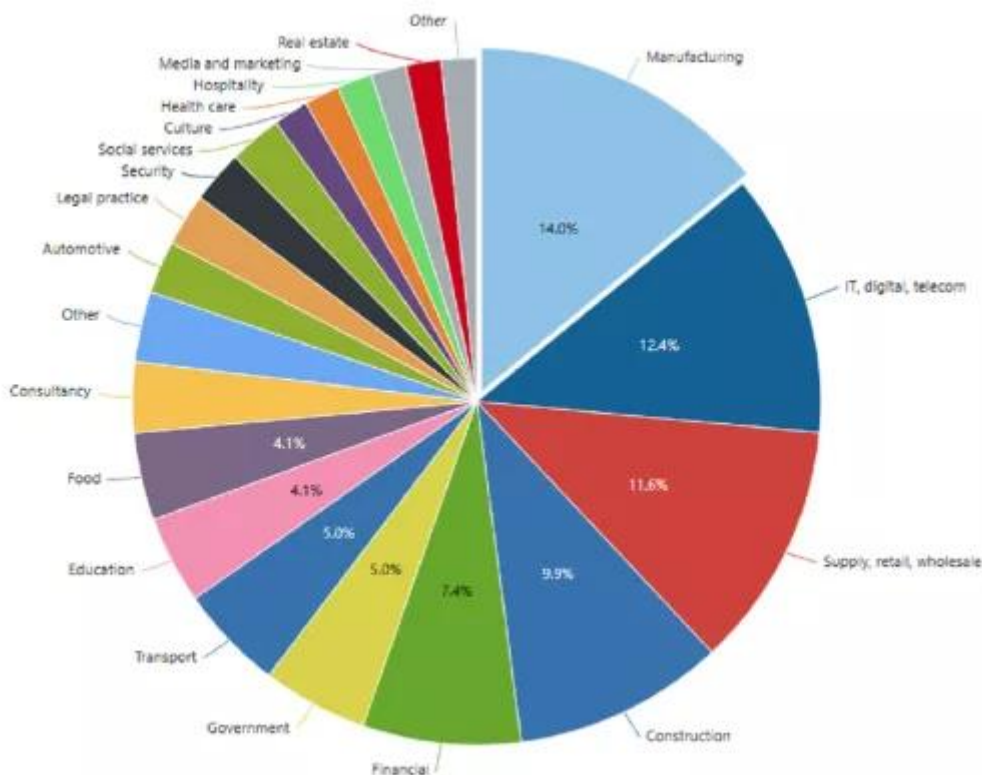
Nu de industrie haar digitale transformatie versnelt, zien we steeds meer cyberaanvallen die de veerkracht van productiebedrijven op de proef stellen. Met de recente invoering van de Europese NIS2-richtlijn in België, worden bedrijven verplicht hun cyberbeveiliging te versterken. Doen ze dat niet, dan volgen er sancties. Van wettelijke verplichtingen tot veelvoorkomende kwetsbaarheden en best practices, hier leest u hoe u kunt anticiperen en uw bedrijf doeltreffend kunt beschermen.

De digitale transformatie biedt industriële bedrijven nieuwe kansen: innovatie, procesoptimalisatie, kostenverlaging, nieuwe inkomstenbronnen... De digitale verschuiving gaat echter ook gepaard met een zorgwekkende toename van cyberaanvallen. Geen enkele industriële organisatie blijft er nog van gespaard, of het nu om een grote multinational of een lokale KMO gaat. Ransomware die de productielijnen lamlegt, massale diefstal van gevoelige gegevens, gerichte aanvallen op strategische leveranciers: het aantal incidenten stijgt exponentieel en ze worden steeds complexer.

Sinds de Europese NIS2-richtlijn (Network and Information Security) op 18 oktober 2024 werd ingevoerd in België, worden productiebedrijven aan strenge regels onderworpen om deze risico's af te wenden en hun cyberweerbaarheid te versterken.

Waarschuwing voor Belgische productiebedrijven

Diverse recente onderzoeken waarschuwen voor een toename van cyberbeveiligingsincidenten in de industriële sector. In 2023 en 2024 registreerde het Centre for Cybersecurity Belgium (CCB) 120 respectievelijk 109 ransomware-aanvallen tegen Belgische organisaties. Vooral de productie-sector is het doelwit van deze cyberaanvallen (zie infographic). Volgens Sirris, het collectief van Belgische ondernemingen, is de trend: industriële systemen worden steeds meer gekoppeld aan IT en zijn bijzonder



De gevolgen van een cyberaanval op industriële systemen kunnen dramatisch zijn: langdurige stilstand van productielijnen, aanzienlijke financiële verliezen, snelle reputatieschade in de ogen van klanten en partners. In extreme gevallen komt zelfs de veiligheid van werknemers in gevaar wanneer cybercriminelen kritieke systemen aanvallen. En dan hebben we het nog niet over lekken van gevoelige gegevens, zoals industriële geheimen of strategische informatie.

NIS2: nieuwe, aangescherpte verplichtingen

Met het oog op deze groeiende dreigingen neemt de Europese Unie een hardere houding aan met NIS2, de nieuwe richtlijn voor netwerk- en informatiebeveiliging. Die heeft als doel de veerkracht te versterken van sectoren die als belangrijk of essentieel worden beschouwd, waaronder de verwerkende industrie. Concreet legt NIS2 de Belgische bedrijven een aantal verplichte maatregelen op, waaronder:

- de regelmatige beoordeling van cyberrisico's om kwetsbaarheden te identificeren;
- de opstelling van incidentbestrijdingsplannen om snel te kunnen reageren bij een aanval;
- een strengere controle van leveranciers en onderaannemers;
- financiële sancties bij niet-naleving.

Bij Sirris merken we dat veel bedrijven de impact van niet-naleving van NIS2 nog steeds onderschatten. Toch kunnen de gevolgen ernstig zijn, zowel vanuit financieel oogpunt als qua reputatieschade. Meer nog dan een verplichting is cyberbeveiliging uitgegroeid tot een cruciale factor voor het concurrentievermogen en de industriële veerkracht van bedrijven.

Vijf vaak voorkomende gebreken inzake industriële cyberbeveiliging

Industriële bedrijven, waarvan de IT-systemen (informatica) en OT-systemen (operationele technologieën) nauw met elkaar verweven zijn, blijven bijzonder kwetsbaar. Dit zijn enkele van de meest voorkomende kwetsbaarheden in de industrie:

1. **Gebrek aan netwerksegmentatie**

Wanneer IT- en OT-systemen met elkaar verbonden zijn zonder duidelijke scheiding, volstaat één kwetsbaarheid om de hele infrastructuur in gevaar te brengen.

2. **Verouderde software**

Veel fabrieken gebruiken nog steeds besturingssystemen en software die tientallen jaren oud zijn, zonder updates. Dat maakt ze tot een gemakkelijk doelwit voor hackers.

3. **Phishing en social engineering**

Cybercriminelen maken gebruik van menselijke zwakheden: een eenvoudige frauduleuze e-mail kan al genoeg zijn om een systeem te infiltreren.

4. **Slecht toegangsbeheer**

Als werknemers te veel toegang hebben tot gevoelige systemen, kunnen cybercriminelen misbruik maken van beveiligde accounts om ze te infiltreren.

5. **Kwetsbaarheden in de toeleveringsketen**

Externe leveranciers en dienstverleners kunnen toegangspunten zijn voor cyberaanvallen die de hele industriële infrastructuur aantasten.

Die kwetsbaarheden, die welbekend zijn bij cybercriminelen, vereisen een constante waakzaamheid en strengere beveiligingsmaatregelen.

Vijf belangrijke maatregelen om uw beveiliging te versterken

Geen enkel bedrijf is volledig onkwetsbaar, maar enkele eenvoudige en doeltreffende maatregelen kunnen de risico's sterk terugdringen:

1. **IT- en OT-netwerken segmenteren**

Door de IT- en OT-omgevingen te scheiden, beperkt men de verspreiding van aanvallen en voorkomt men dat een probleem op een kantoorstelsel de productie lamlegt.

2. **Software up-to-date houden**

Beveiligingsupdates zijn essentieel om de kwetsbaarheden te corrigeren die door hackers worden uitgebuit. Een verouderd systeem is een gemakkelijk doelwit.

3. **Werknemers opleiden en hen bewust maken van cyberrisico's**

Werknemers vormen de eerste verdedigingslinie. Maak hen bewust van de gevaren van phishing-aanvallen en het belang van veilige wachtwoorden en goede cyberbeveiligingspraktijken.

4. **Het toegangsbeheer versterken**

De toegang tot kritieke systemen moet worden beperkt tot bevoegd personeel. Doeltreffende oplossingen daarvoor zijn multi-factorauthenticatie (MFA) en de toewijzing van toegangsrechten op basis van rollen.

5. **De toeleveringsketen beveiligen**

Leveranciers moeten voldoen aan strenge normen voor cyberbeveiliging. Controleer of ze

adequate controles toepassen om te voorkomen dat ze worden blootgesteld aan indirecte kwetsbaarheden.

Deze best practices zijn toegankelijk voor alle bedrijven en kunnen aanzienlijke financiële verliezen helpen te voorkomen. Bij Sirris geloven we dat kleine acties vandaag grote rampen in de toekomst kunnen voorkomen.

Anticiperen om beter weerstand te bieden

Cyberdreigingen evolueren snel en de sector kan de uitdagingen van cyberbeveiliging niet langer negeren. Hoewel de naleving van de NIS2-richtlijn een uitdaging is, geeft ze industriële bedrijven ook de kans om hun concurrentievermogen en veerkracht te versterken. Vandaag investeren in cyberbeveiliging verzekert de bedrijfscontinuïteit en beschermt de toekomst van de sector.

CyberActive, een initiatief waarvan Sirris partner is, helpt u uw weg te vinden in de wereld van cyberdreigingen, of u nu actief bent in de productie of digitale dienstverlening. Het voorziet opleidingen, educatief materiaal en videohandleidingen over alle aspecten van cyberbeveiliging.

[Ontdek het programma en schrijf u in](#)

CyberActive is een initiatief van Sirris, Howest, de Université catholique de Louvain en de Vrije Universiteit Brussel. Gefinancierd door de FOD Economie en de Europese Unie (Next Generation)

Auteurs



Thierry Coutelier