Sector expertise

Industriële ondernemingen gewilde prooi voor cybercriminelen

ABN·AMRO

20 juni 2025

De maak- en voedselindustrie is door de vergaande procesautomatisering en vele digitale koppelingen binnen de keten kwetsbaar voor cyberaanvallen. Stilvallende productielijnen en gestolen IP-adressen kunnen enorme gevolgen hebben.

De druk binnen de toeleverketen, de groeiende digitalisering, 'slimme' machines, het uitvoeren van tijdige updates en het delen van data met partijen buiten de fabriek zijn stuk voor stuk risicofactoren die digitale criminelen kunnen aantrekken. Hoewel nieuwe technologieën zoals AI de beveiligingsmaatregelen kunnen versterken, brengen ze tegelijkertijd nieuwe risico's met zich mee. Het is dan ook van essentieel belang dat bedrijven in deze sector hun digitale weerbaarheid verbeteren om ervoor te zorgen dat hun processen ongestoord doorgang kunnen vinden.

Recente aanvallen in de sector

- In april 2023 is Nexperia, een chipfabrikant uit Nijmegen, slachtoffer geworden van ransomware. De hackers dreigden waardevolle informatie, zoals chipontwerpen en klantdata, openbaar te maken als het bedrijf geen losgeld zou betalen.
- In 2023 werd het Rotterdamse chemiebedrijf Chemours doelwit van een phishing-aanval, waarna het te maken kreeg met ransomware. Hackers stuurden e-mails die schijnbaar afkomstig waren van vertrouwde interne bronnen binnen de organisatie. De stilgelegde productielijnen leidden tot aanzienlijke financiële verliezen.
- VDL-groep is in 2023 slachtoffer geworden van een phishing-aanval. Valse interne portalen van het bedrijf werden gebruikt om aan inloggegevens van werknemers te komen. Hierdoor verkregen de hackers toegang tot gevoelige informatie, die zij gebruikten om losgeld te eisen.
- Op 3 februari 2025 werd het Nederlandse productiebedrijf Tosaf aangevallen door ransomware. Dit resulteerde in stilvallende productielijnen, wat de operationele bedrijfsvoering zwaar onder druk zette.
- In maart 2024 viel hackerscollectief Stormous Group de Belgische brouwer Duvel Moortgat aan, bekend van bieren als Duvel, La Chouffe en De Koninck. Ze claimden veel gegevens te hebben gestolen en dreigden deze te onthullen. De brouwer gaf geen details vanwege het onderzoek, maar dankzij voldoende voorraad kwamen leveringen niet in gevaar en werd de productie van alle labels snel hervat.
- De Belgische koffieproducent Koffie Beyers is in maart 2024 getroffen door ransomware. Het bedrijf produceert jaarlijks circa 35.000 ton koffiebonen en verwerkt deze tot diverse producten voor grote afnemers zoals HEMA en LIDL. De omvang van de schade is niet bekend.

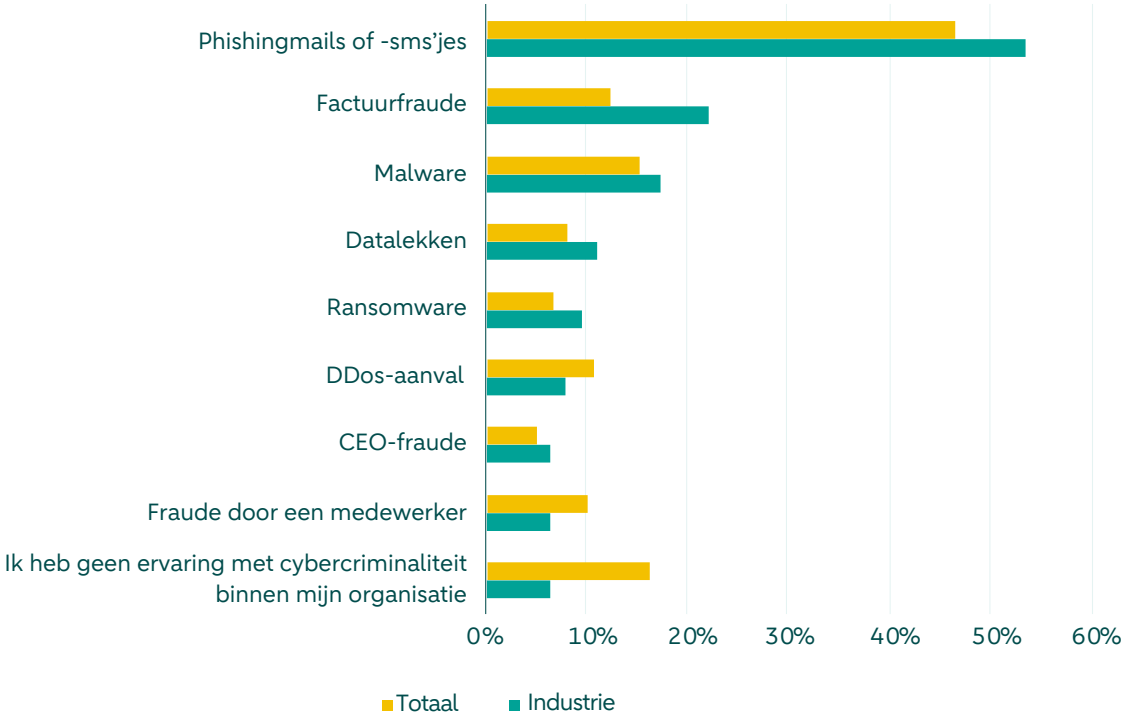
Cyberveiligheid in de sector

Uit onderzoek van de ABN AMRO blijkt dat 85 procent van de industriële bedrijven cybercriminaliteit ziet als risico binnen hun organisatie. Van de respondenten geeft één op de tien aan operationele verstoringen te hebben ervaren door cyberaanvallen. Vooral phishingmails, factuurfraude en malware zijn veelvoorkomende vormen van cybercriminaliteit.

Hetzelfde onderzoek toont aan dat industriële bedrijven actief investeren in cyberveiligheid. Van de respondenten geeft 48 procent aan meer te hebben uitgegeven in 2024, waarbij de helft aangeeft dat hun investeringen ongeveer gelijk zijn gebleven ten opzichte van 2023. De voornaamste reden voor de toename in uitgaven is de groeiende dreiging van cyberaanvallen en de noodzaak om te voldoen aan wettelijke vereisten zoals de NIS2-richtlijn en de Algemene Verordening Gegevensbescherming (AVG).

Cyberdreiging voor de industrie: bovengemiddeld, met accent op phishingmails en factuurfraude

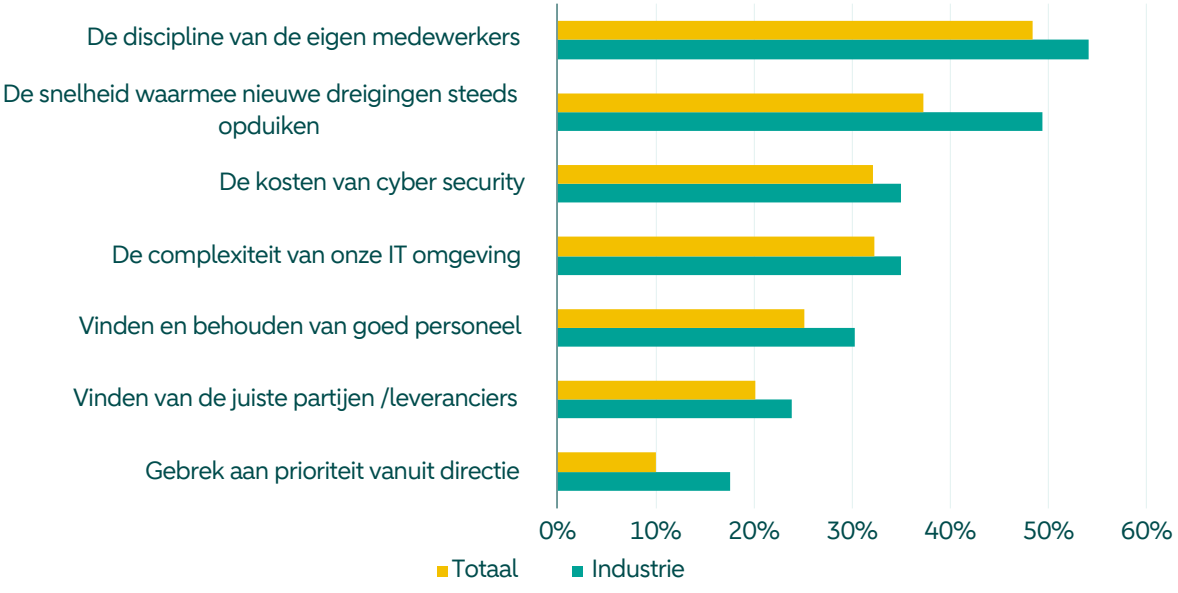
Hieronder ziet u de vormen van cybercriminaliteit waarmee uw organisatie wel eens te maken heeft gehad. Wat heeft in de afgelopen 12 maanden plaatsgevonden?



De uitdagingen binnen de sector liggen vooral bij de snelle opkomst van nieuwe dreigingen, de discipline van medewerkers en de kosten. Een meerderheid van de ondernemingen (61 procent) ziet AI als kans om de cyberveiligheid te versterken. AI kan bijvoorbeeld enorme hoeveelheden data analyseren om verdachte activiteiten te identificeren, zodat organisaties aanvallen kunnen voorkomen. Tegelijkertijd ziet 57 procent AI als mogelijke bedreiging voor hun organisatie. Zo gebruiken hackers AI om hun aanvallen te verfijnen. Dit maakt de aanvallen sneller, efficiënter en moeilijker te detecteren.

De grootste uitdaging voor de sector ligt bij snelle opkomst van nieuwe dreigingen

Wat zijn de grootste uitdagingen om cybersecurity goed op orde te krijgen en te houden?



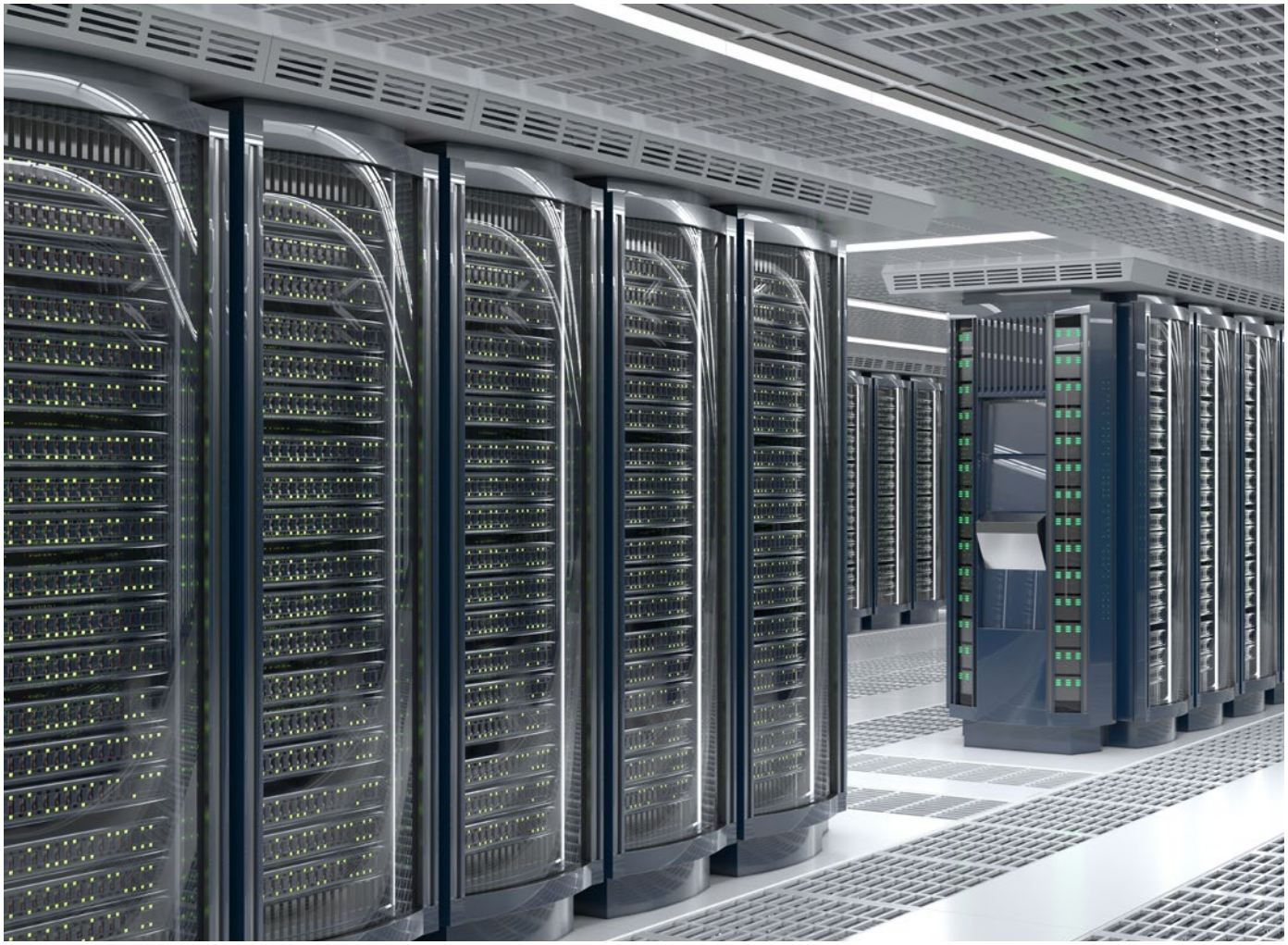
NIS2: nieuwe Europese wetgeving moet cyberweerbaarheid verbeteren

De NIS2, de opvolger van de Network and Information Security Directive (NIS), is per oktober 2024 in de Europese Unie van kracht. Deze richtlijn van de Europese Unie (EU) is bedoeld om de cyberbeveiliging van belangrijke diensten in lidstaten te verbeteren. Het is Nederland niet gelukt om de EU-richtlijnen binnen de gestelde termijn om te zetten in nationale wetten. Echter, de nationale wetgeving, bestaande uit de Cyberbeveiligingswet (Cbw/NIS2) en de Wet weerbaarheid kritieke entiteiten (Wwke/CER), is in aantocht. De verwachting is dat deze wetten in het derde kwartaal van 2025 van kracht zijn.

Uit onderzoek van ABN AMRO blijkt 48 procent van industriële bedrijven niet bekend is met de NIS2-verplichtingen. Tegelijk geeft 35 procent aan volledig te kunnen voldoen aan de verplichtingen van NIS2. Wanneer niet aan de NIS2-verplichtingen wordt voldaan, bestaat het risico op forse boetes. Deze boetes kunnen oplopen tot 10 miljoen euro of 2 procent van de wereldwijde jaaromzet.

Meer informatie

Benieuwd of uw organisatie onder de NIS2-richtlijn valt? Lees ons rapport: ‘Cyberweerbaarheid ondernemers blijft achter bij realiteit’, of vul de Zelfevaluatie NIS2 van het Nationaal Cyber Security Centrum in.



Verhoog de cyberveiligheid van uw organisatie

Steeds meer organisaties worden slachtoffer van cybercriminaliteit – criminelen hebben maar een kleine ingang nodig. Mogelijk loopt u nu al risico. Daarom is het belangrijk om passende maatregelen op het gebied van cyberveiligheid te nemen. Om u en uw mensen daarbij te helpen, zetten we verschillende oplossingen en downloads op een rij.

Cyberveiliger in 3 stappen

1 Maak een risico-analyse

Breng de 'kroonjuwelen' van uw organisatie in kaart. Welke zaken zijn cruciaal voor uw bedrijf of dienstverlening? Denk aan klantgegevens, productiemethoden of intellectueel eigendom. Identificeer vervolgens welke dreigingen deze kroonjuwelen in gevaar kunnen brengen: bijvoorbeeld een kwetsbaarheid in software of een medewerker die op een malafide link klikt. Nu kunt u de risico's analyseren. Wat is het gevolg van deze risico's, hoe waarschijnlijk zijn ze en wat doet u al om ze te beperken?

2 Neem adequate maatregelen

Uw risico-analyse bepaalt welke maatregelen de juiste zijn. De basismaatregelen van het Nationaal Cyber Security Centrum en de basisprincipes van het Digital Trust Center vormen in ieder geval een goed startpunt. Daarnaast kunt u:

- veilig gedrag van uw medewerkers stimuleren;
- bepalen en vastleggen wie de eigenaar van bepaalde gegevens is;
- risico's met uw partners en leveranciers bespreken.

Een cybersecurity-specialist kan u helpen om de juiste maatregelen te bepalen en te nemen.

3 Stel een Cyber Response Plan op

Ten slotte is het essentieel om procedures te ontwikkelen waarmee u cyberincidenten detecteert en afhandelt. Deze legt u vast in een Cyber Response Plan.

Whitepaper over Employee Awareness (Download onze Whitepaper)
Cybercriminelen komen vaak via medewerkers binnen in uw digitale systemen. Houd uw medewerkers scherp en maak hen bewust van de risico's van cybercrime – gebruik hiervoor onze whitepaper.

Third-Party Risk Management Checklist (Bekijk de checklist)
Als u met partners en leveranciers samenwerkt, kunnen er veiligheidsrisico's optreden.
Met Third-Party Risk Management brengt u deze in kaart.

- Identificeer mogelijke cyberrisico's
- Deel de checklist met uw klanten en leve- ranciers voor meer veiligheid

Cyber Response Plan (Maak uw Cyber Response Plan)
Een Cyber Response Plan helpt u om cybercrime-incidenten op te sporen, af te handelen en eventuele schade te herstellen.

- Stel uw eigen Cyber Response Plan op
- Bereid uw bedrijf en medewerkers voor op een cyberaanval

NIS2 praktijkgids (Check onze NIS2 praktijkgids)
Elke sector kent verschillende cyberrisico's. In de industrie sector is vaak de productie het doelwit van cybercriminelen, terwijl zij in de gezondheidszorg uit zijn op patiëntgegevens. Benieuwd naar de risico's en dreigingen in uw sector?

Zo helpt ABN AMRO u

Cyber Veilig & Zeker van MMOX

Voor midden- en grootbedrijf dat zoekt naar ontzorging in cyberveiligheid

- 24/7 proactief beschermd tegen cyberdreigingen
- Helpdesk voor cyberveiligheidsvragen

Bekijk Cyber Veilig & Zeker

Cyberverzekering

Voor zakelijke klanten die zich willen indekken tegen cyberschade

- Bescherming via onze cyberverzekering
- Uitgebreide dekking
- 24/7 hulp van onze specialisten

Ontdek onze cyberverzekering

Vrijblijvend cybergesprek

IVoor ondernemers die willen weten hoe zij ervoor staan op het gebied van cyberveiligheid

- Informatie over tools en oplossingen
- Samen logische vervolgstappen bepalen

Plan vrijblijvend een gesprek in

Op de hoogte blijven van de laatste ontwikkelingen en artikelen? Meld u aan voor onze nieuwsbrief