Cyberveiligheid in de maak- en voedingsindustrie

Operationele technologie vormt aantrekkelijk doelwit

Stilvallende productielijnen en gegijzelde werkprocessen: de industrie – ook die voor levensmiddelen – is door haar vele in- en externe afhankelijkheden kwetsbaar voor cyberaanvallen. Tijdsdruk in de toeleverketen, digitalisering, machines die 'smart' worden, achterstallige updates en data die met partijen buiten de fabrieksmuren wordt gedeeld: het zijn stuk voor stuk beruchte buitenkansen voor digitale dieven en afpersers.

Risico's op een rij

Machines, robots en magazijnsystemen communiceren continu met elkaar. Doel: optimale efficiency. Daarnaast digitaliseert de werkvloer, kan apparatuur steeds vaker op afstand worden bediend en is er veel externe data-uitwisseling – bijvoorbeeld over software-updates en machineonderhoud. De digitale verbondenheid tussen schakels in complexe, internationale toeleverketens (vooral bij elektronica, auto's en hightechmachines) bespaart kosten, maar is ook risicovol. En dan is er nog de transitie van het industriële verdienmodel (productie en verkoop) naar 'servitization' ('as-a-service'-proposities). Online datadeling tussen gebruiker en fabrikant neemt hierdoor enorm toe. Dit is een potentiële poort voor hackers en een achilleshiel die de industrie geliefd maken bij cybercriminelen.

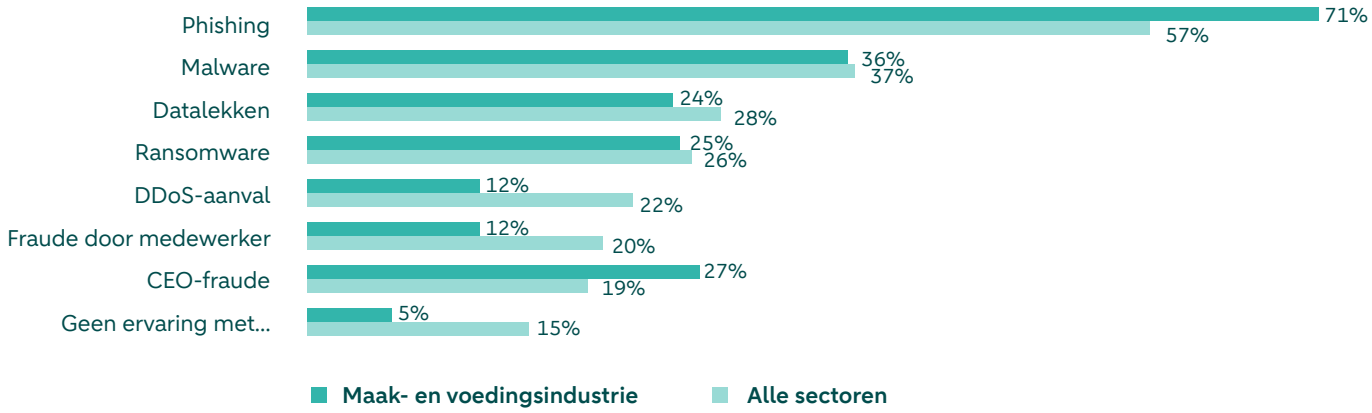
Recente cyberaanvallen in de sector

- In augustus 2023 sluit Kendrion, fabrikant van elektromagnetische actuatoren, aan in de rij van honderden slachtoffers van hackerscollectief Lockbit. Zodra de ransomware werd ontdekt, zijn alle systemen uitgezet om meer schade te voorkomen. Gevolg: tijdelijk ouderwets handwerk. Wat er is ontvreemd, welke eisen de daders hadden en de omvang van de schade is niet bekendgemaakt. Uiteraard zijn er experts ingezet om de oorzaak te vinden.
- Een 'heterdaadje' gebeurt niet vaak, maar het lukte voedingsmiddelenproducent Royal Smilde begin 2022. Via phishing achterhaalden hackers het wachtwoord van een medewerker waarmee zij op de server kon. Nét toen ze hun ransomware wilden installeren, werden de criminelen betrapt door het alerte crisisteam en gealarmeerde cybersecuritybedrijf. Zo bleef de schade beperkt: sommige bestanden werd geïnfecteerd en één fabriek moest even dicht.
- In maart van dit jaar had hackerscollectief Stormous Group het gemunt op het Belgische Duvel Moortgat: producent van bekende bieren, waaronder Duvel, La Chouffe en De Koninck. De hackers – ook bekend van aanvallen op Coca-Cola en Epic Games (Fortnite) – claimden veel gegevens te hebben buitgemaakt die ze dreigden te onthullen. In het belang van het ingestelde onderzoek gaf de brouwer hierover geen details. Mede dankzij genoeg voorraad kwamen leveringen niet in gevaar. Ook werd de productie van alle labels vrij snel weer hervat.

ABN·AMRO

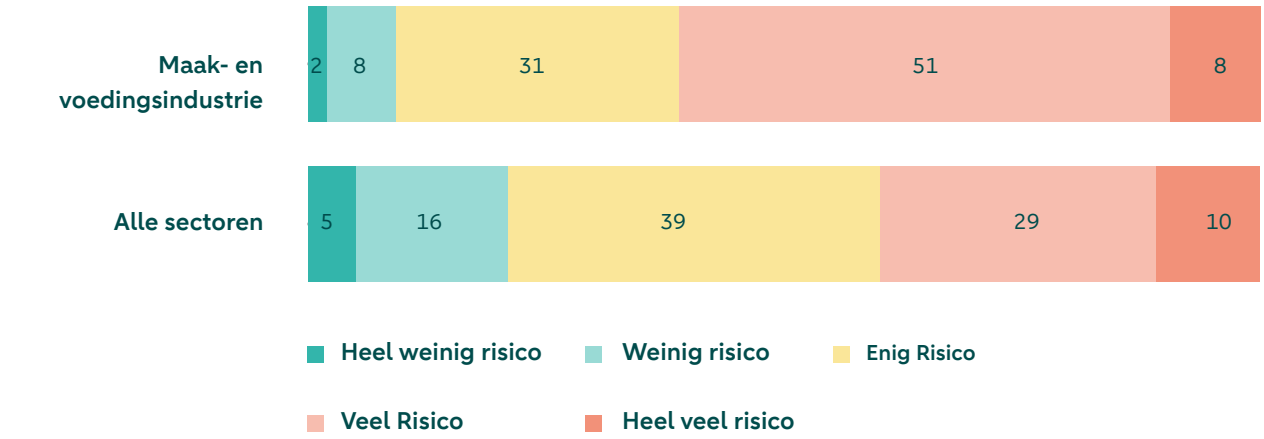
Bedrijven in de maak- en voedingsindustrie bovengemiddeld getroffen door cyberaanvallen

*Met welke van de volgende vormen van cybercriminaliteit heeft u binnen uw organisatie weleens te maken gehad?**



Realisme heerst in de sector: we lopen relatief veel risico

*In welke mate denkt u dat cybercriminaliteit een risico is voor uw organisatie?**



* Bron: enquête van ABN AMRO en MWM2 onder 895 Nederlandse organisaties, maart 2024

NIS2: Nieuwe Europese wetgeving moet cyberweerbaarheid van ketens versterken

Om de cyberveiligheid in Europa te verbeteren, gaat in oktober 2024 een nieuwe wet in: NIS2, de opvolger van de Network and Information Security Directive (NIS). Dit geldt voor bedrijven met minimaal vijftig werknemers of een jaaromzet en balanstotaal van meer dan € 10 miljoen. Organisaties in de voedingsmiddelen & industrie krijgen zowel direct als indirect met de nieuwe wet te maken. De nieuwe NIS2-richtlijn verplicht essentiële en belangrijke organisaties om maatregelen te nemen om te zorgen voor de beveiliging van de keten waar zij deel van uitmaken.

- Cybersecurity was vrijwillig en wordt nu verplicht
- Focus op het inzichtelijk maken van en handelen op risico's
- Samenwerking met leveranciers om de keten te beveiligen

Benieuwd of uw organisatie onder de NIS2-richtlijn valt?
Lees ons rapport: **Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker,**
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 drie 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 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 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 uw digitale systemen binnen. Houd uw medewerkers scherp en maak ze bewust van de risico's van cybercrime. U leest er alles over in ons whitepaper.

Checklist: Third-Party Risk Management (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 leveranciers 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

Cyberveiligheidsrapport (Lees het complete rapport)
Afgelopen jaar kreeg bijna driekwart van de Nederlandse bedrijven te maken met een cyberaanval. Lees alle feiten en ontwikkelingen in het jaarlijkse rapport 'Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker'.

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

Zo helpt ABN AMRO

Cyber Veilig & Zeker van MMOX
Voor een 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
Voor ondernemers die willen weten hoe ze 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