



WHITEPAPER

Food-industrie op weg naar NIS2

*Hoe borg je de cybersecurity in je OT- en IT-omgeving
en de supply chain?*

Actemium Veghel, 2023

Inhoud whitepaper



De aanleiding	3
Wat is NIS en waarom is het nodig?	3
Wat komt er af op bedrijven die onder NIS2 vallen?	4
Een goede voorbereiding is het halve werk	5
Een cybersecuritypartner die weet wat er speelt	5
De Actemium-aanpak: stapsgewijs en gestructureerd	7
Cybersecurity in thrillervorm	8
Verdiep je kennis!	8

De aanleiding

Produceren jullie diervoeder of voedingsmiddelen? Dan moeten jullie uiterlijk in oktober 2024 voldoen aan de strenge cybersecurity-eisen uit de Europese NIS2-richtlijn. In deze paper behandelen we de scope en het belang van deze richtlijn en leggen we uit hoe Actemium kan helpen met het compliant maken van jullie plant(s).

Wat is NIS en waarom is het nodig?

In een snel digitaliserende wereld wordt het risico op economische en/of maatschappelijke schade als gevolg van cyberaanvallen steeds groter. De Europese Unie heeft de afgelopen jaren hard gewerkt aan beleid voor het beveiligen van de digitale omgeving



Met de richtlijn over de beveiliging van Netwerk- en Informatie-systemen (NIS) werd in 2018 voor het eerst Europese wetgeving van kracht op het gebied van cyberbeveiliging. De huidige NIS1-richtlijn is van toepassing op 'essentiële sectoren' die beschikken over vitale infrastructuur. Denk aan de drinkwater- en energiesector. Uitval of verstoring van processen in deze sectoren kunnen leiden tot maatschappelijke ontwrichting en vormen een bedreiging voor de nationale veiligheid.

Op 16 januari 2023 is de NIS2-richtlijn in werking getreden. De opvolger van NIS1 scherpt de cybersecurity-eisen verder aan en heeft een groter toepassingsgebied. Naast 'essentiële sectoren' moeten ook 'belangrijke entiteiten' aan deze nieuwe richtlijn gaan voldoen. Producenten van diervoeder en voedingsmiddelen vallen hieronder.

Om compliant te zijn, dienen deze bedrijven onder meer maatregelen te nemen voor back-upbeheer, noodherstel, risicoanalyse, het beveiligen van de toeleveringsketen en het rapporteren van cyberincidenten. Het niet naleven van de vereisten kan tot fikse boetes leiden.

De invoering van NIS2 heeft als doel de cyberbeveiligingsveerkracht binnen de EU verder te versterken. Lidstaten hebben tot 17 oktober 2024 de tijd om NIS2 om te zetten in nationaal recht. In Nederland zal dit gebeuren via de aanpassing van de Wet bescherming netwerk- en informatiesystemen (Wbni).

”

Lidstaten hebben tot 17 oktober 2024 de tijd om NIS2 om te zetten in nationaal recht.

Wat komt er af op bedrijven die onder NIS2 vallen?

Cyberbeveiliging van OT en supply chain

Bedrijven in de food- en feed-industrie voorzien in een primaire behoefte: voeding voor mens en dier. Verstoring van hun productieprocessen verzwakt niet alleen hun concurrentiepositie, maar brengt bovendien de voedselzekerheid in gevaar. De operationele technologie (OT) van deze bedrijven moet dan ook feilloos functioneren. Door de voortschrijdende integratie van de OT- en IT-omgeving neemt het risico op cyberincidenten toe. OT-beveiliging conform de IEC 62443 is dan ook een speerpunt van de NIS2-richtlijn.

”

Naast hoge boetes kunnen juridische en strategische sancties worden opgelegd, waaronder het intrekken van vergunningen.

Cybersecurity gaat echter verder dan alleen het beveiligen van de eigen fabrieksomgeving. Productiebedrijven zijn een schakel in de keten. Een cyberincident bij een van hun leveranciers kan ook gevolgen hebben voor hun eigen organisatie. NIS2 focust daarom ook op de cyberveiligheid van de supply chain. Van producenten wordt verwacht dat zij samen met hun toeleveranciers potentiële risico's in de keten inventariseren en beheersbaar maken. Dit wordt onder meer mogelijk door het opnemen van security-eisen in contracten met leveranciers. Wanneer iedereen zijn eigen cyberbeveiliging aantoonbaar borgt is er helderheid over aansprakelijkheid bij onverhoopte incidenten en is de businesscontinuïteit in de keten geborgd.

Zorgplicht en meldplicht

Organisaties die onder de NIS2-richtlijn vallen, hebben een zorgplicht en een meldplicht. Onder zorgplicht wordt verstaan dat zij de voorgeschreven maatregelen implementeren om cyberincidenten te voorkomen, cyberdreigingen snel te detecteren en op adequate wijze te reageren. Denk aan het toepassen van cryptografie en versleuteling en het opstellen van een plan voor crisismanagementplan. De meldplicht houdt in dat organisaties gedetecteerde cyberincidenten binnen 24 uur moeten melden bij de toezichthouder, gevolgd door een gedetailleerd eindrapport uiterlijk één maand later. Met als doel het delen van informatie over incidenten tussen de Europese lidstaten te verbeteren en zo verdere verspreiding van cyberaanvallen te voorkomen.

Toezicht en sancties

Het is van cruciaal belang dat directies, managers, Chief Information Security Officers (CISO's) en IT/OT-verantwoordelijken binnen je organisatie de eisen uit de NIS2-richtlijn goed begrijpen. Er zal immers streng gecontroleerd worden op governance. Het niet (correct) implementeren van de vereiste maatregelen zal grote gevolgen hebben. Zo kunnen bestuurders van organisaties die hun cybersecurity niet aantoonbaar op orde hebben persoonlijk aansprakelijk worden gesteld voor de gevolgen van een cyberincident. Naast hoge boetes kunnen juridische en strategische sancties worden opgelegd, waaronder het intrekken van vergunningen.

Een goede voorbereiding is het halve werk

Nederland heeft tot 17 oktober 2024 de tijd om de Europese NIS2-richtlijn om te zetten in nationaal recht. Dit zal gebeuren via de aanpassing van de Wet bescherming netwerk- en informatiesystemen (Wbni). Met nog maximaal anderhalf jaar te gaan, zijn veel spelers in de food en feed-industrie zich al aan het voorbereiden. Zijn jullie hier nog niet meer bezig? Bedenk dan dat er weinig tijd te verliezen is. Jullie zullen naast technische wellicht ook organisatorische en operationele maatregelen moeten nemen om te voldoen aan de vereisten uit de richtlijn. Denk alleen al aan het verplicht rapporteren van cyberincidenten. Dit is in veel productiebedrijven nog geen onderdeel van de dagelijkse security-routines.

Hulp van deskundigen

De voorbereiding op NIS2 is een kennisintensief traject waarvoor je wellicht externe deskundigen zult moeten inschakelen. Daaronder juristen die gespecialiseerd zijn in cybersecurity en kunnen helpen met het aanpassen van inkoopcontracten, maar ook OT-specialisten met kennis van IT én cyberveiligheid. Dergelijke experts zijn schaars en momenteel zeer gewild. Bovendien kost het tijd om de voorgescreven maatregelen en procedures correct te implementeren en het cybersecurity-bewustzijn stevig te verankeren in je bedrijfscultuur. Dit traject kan meerdere maanden duren. Voor productiebedrijven met vestigingen in meerdere Europese lidstaten is de uitdaging nog complexer. Informeer je dus tijdig over de stappen die jouw bedrijf moet zetten en laat je begeleiden bij de omzetting hiervan. In het volgende hoofdstuk lees je hoe Actemium hierbij kan helpen.

Een cybersecuritypartner die weet wat er speelt

Op IT-gebied zullen jullie de cybersecurity wellicht al op orde hebben. Maar hoe zit het met de beveiliging van je productieomgeving? Welke OT-systemen zitten er op jullie procesnetwerk en wat is hun beveiligingsstatus? Een vraag die veel productiebedrijven maar moeilijk kunnen beantwoorden.

Overzicht creëren

In de meeste fabrieksomgevingen wordt het netwerk in de loop der jaren steeds verder uitgebreid en is sprake van organische groei van systemen. Mogelijk zijn jullie het overzicht enigszins kwijt omdat specifieke kennis over jullie OT-systemen is afgevloeid en er geen actuele tekeningen van het netwerk meer zijn. Gebrek aan inzicht in de assets op je netwerk betekent echter ook dat je potentiële cyber-risico's niet in beeld hebt.

Zijn de firewalls tussen jullie IT- en OT-omgeving nog goed ingericht? Hebben jullie standaardwachtwoorden in de loop van de jaren veranderd? Zijn de OT-systemen consequent gepatcht en de remote access punten in je netwerk goed beveiligd?

Risico's aanpakken

Een IT-netwerk moet in de eerste plaats flexibel en veilig zijn. Om dit te borgen, worden IT-systemen consequent en geforceerd gepatcht. Beschikbaarheid speelt een minder belangrijke rol. Het is meestal geen ramp dat een e-mail ietsje later wordt verzonden omdat er een update wordt geïnstalleerd. Daarentegen moeten OT-netwerken wél hoog beschikbaar zijn. Productiecontinuïteit is key. Daarom is het consequent patchen van OT-systemen lang geen vanzelfsprekendheid. Dit kan immers leiden tot productieverstoringen. Vaak ontbreekt het aan draagvlak, budget en beleid om de OT optimaal te beveiligen. Juist dit wordt door NIS2 verplicht, op straffe van hoge boetes en het verliezen van vergunningen.

De juiste partner

Wie schakel je in om je te helpen jouw OT-omgeving cybersecure te maken? Kies voor een partner die weet wat er speelt in jullie sector, die kennis heeft van jullie OT, IT én de technologie om deze te beveiligen. **Actemium heeft als system integrator tientallen jaren ervaring met het automatiseren van fabrieken in de food- en feed-sector.** Wij hebben talloze fabrieken letterlijk mee ontworpen, opgebouwd en in de loop van de jaren verder uitgebreid en gemoderniseerd. Als geen ander kennen wij jullie processen, machines en systemen. Wij hebben een team van cyberspecialisten in huis. Samen met jou zorgen we ervoor dat je organisatie NIS2-compliant wordt én blijft.

Basisstappen ter voorbereiding van NIS2

- 1 *Breng risico's in kaart en inventariseer wat prioriteit heeft.*
- 2 *Implementeer beleid en technologie om cyberincidenten nu en in de toekomst te detecteren en voorkomen.*
- 3 *Maak een plan voor de omgang met (onverhoopte) cyberincidenten.*
- 4 *Veranker cybersecurity in je bedrijfscultuur: iedereen moet weten hoe belangrijk dit is.*
- 5 *Ga met toeleveranciers in gesprek over de beveiliging van je supply chain.*
- 6 *Evalueer regelmatig de effectiviteit van je cybersecuritybeleid.*

De Actemium-aanpak: stapsgewijs en gestructureerd

Het voorbereiden van je plant(s) op NIS2 doen we in nauwe samenwerking met jouw organisatie. We pakken dit gestructureerd aan. Je mag van ons advies verwachten over technische maatregelen die je moet nemen, en wij kunnen deze ook voor je implementeren. Wij zijn als onafhankelijk system integrator niet gebonden aan bepaalde merken en hebben ervaring met de oplossingen van diverse leveranciers. Jij bepaalt welke technologie het beste bij jouw organisatie past. Uiteraard kunnen we je hierin ondersteunen.

Risico's inventariseren en prioriteren



Optimale cyberbeveiliging begint bij overzicht. Onze consultants brengen samen met jullie in kaart met welke systemen jullie werken en wat hun beveiligingsstatus is. Hieruit ontstaat een lijst van cyber-risico's die jullie lopen. Omdat niet elk risico even relevant is, stellen we een prioriteitenlijst op. Je weet nu in welke volgorde je potentiële risico's gaat mitigeren.

Doorkijken naar oplossingen



Het dichten van cybersecurity-gaps kan op verschillende manieren gebeuren. Van het updaten van bestaande systemen tot de implementatie van bijkomende technologie om je netwerk te beveiligen en te monitoren. Onze consultants verstrekken in principe altijd een merkonafhankelijk advies en kunnen je helpen de beste keuze te maken. Naast technologische oplossingen kunnen wij vanuit onze ervaring met bedrijven in de food- en feed-industrie ook tips geven over het mitigeren van risico's met behulp van organisatorische of operationele maatregelen. Ons brede netwerk omvat specialisten die je op deze terreinen kunnen helpen.

Implementatie van technische maatregelen



Eenmaal de technologische keuzes gemaakt zijn, kun je zelf aan de slag met de inkoop, engineering en implementatie van nieuwe producten en systemen. Je kunt dit echter ook aan ons overlaten. Onze consultants zullen je dan in contact brengen met onze engineers die het vervolgtraject begeleiden tot en met de inbedrijfstelling. Hun kennis en ervaring is voor jou een garantie dat alles snel wordt opgeleverd en in één keer goed werkt.

Service en onderhoud



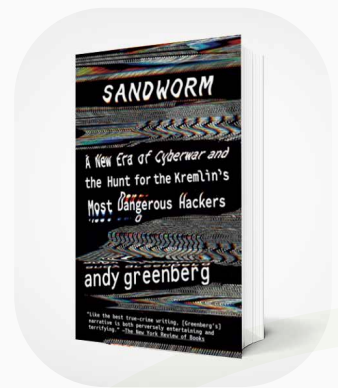
Het borgen van je cybersecurity is een continu proces. De technologische ontwikkelingen gaan razendsnel en ook hackers zitten niet stil. Jouw systemen moeten continu up-to-date worden gehouden zodat je blijft voldoen aan de vereisten uit de NIS2-richtlijn. Dit traject kun je door ons laten verzorgen.

Actie: Cybersecurity in thrillervorm

Maak [hier](#) een afspraak met een van onze consultants voor een advies over de cyberbeveiliging van jouw plant en ontvang het boek **Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers**. Een razend spannende inkijk in de wijze waarop hackers in staat zijn om cruciale voorzieningen te ontwrichten en vernietigen. Leest als een thriller en is ook voor niet-techneuten heel toegankelijk!

Sandworm brengt verschillende hacking-aanvallen in kaart die Rusland de afgelopen succesvol heeft uitgevoerd in Europa en de Verenigde Staten. Het boek geeft een goede inkijk in de cyberstrategie van het Kremlin en laat zien hoe grote mogelijkheden hacking al inzetten als een tactisch wapen.

De Amerikaanse onderzoeksjournalist Andy Greenberg volgde een groep hackers met de naam Sandworm. Hij zag hun activiteiten evolueren van pesterijen (zoals het platleggen van een netwerk via een DDOS-aanval) tot zeer geavanceerde aanvallen waarbij slachtoffers vielen. Greenberg neemt je onder andere mee naar de Oekraïne, waar de afgelopen jaren diverse grote hacks hebben plaatsgevonden. Op banken, websites van overheidsorganen en vitale infrastructuur zoals water- en elektriciteitscentrales. De technieken van deze aanvallen werden ook gebruikt bij enkele wereldwijde bekende hacks die miljarden aan schade veroorzaakten. Een voorbeeld is WannaCry.



Verdiep je kennis!

Als technologiepartner voor de food- en feed-industrie organiseren wij regelmatig kennisevenementen rond thema's die ertoe doen voor de sector. [Kijk voor meer informatie op onze eventpagina.](#)

TIP!

Naast kennisevenementen delen we ook kennis via onder andere whitepapers en webinars. Op onze website bieden we deze whitepapers en webinars aan om te downloaden. Het downloaden hiervan is eenvoudig. Bezoek onze website, bekijk de beschikbare materialen en kies degene die het beste aansluit bij jouw interesses. Klik erop en vraag de download aan. Mis deze kans niet om jouw kennis op het gebied van cybersecurity te vergroten. **Samen werken we aan een veiligere digitale toekomst!**

[Klik hier om webinars terug te kijken](#)

[Voor al onze whitepapers en andere downloads, klik hier](#)