FERM Rotterdam Port Cyber Resilience

Voorbereiden op belangrijke wetswijziging

NIS2: WAT MOET IK ERMEE?

De tijd van afwachten is voorbij: 2024 wordt met de komst van nieuwe wetgeving een absoluut DOEN-jaar voor cyber. In deze special kijken we daarom naar de Europese NIS-2-richtlijn (en de daaruit volgende Nederlandse regels en wetten) én natuurlijk wat dat voor jou betekent.

De Europese NIS2-richtlijn en de aanstaande vertaling naar Nederlandse wetgeving is een onderwerp dat veel organisaties bezighoudt. Er is nog veel onduidelijk, maar dat het impact gaat hebben is zeker.

Laten we bij het begin beginnen.

NIS2: WAT IS HET?

De Europese NIS richtlijn is de Security richtlijn voor netwerk- en informatiesystemen. In Europa is nu nog de NIS-richtlijn van kracht, specifiek voor aanbieders van essentiële diensten zoals drinkwater- en telecom. De NIS2 richtlijn is de opvolger van NIS. NIS2 is geldig voor een breder scala aan bedrijven dan NIS1 en de eisen zijn flink aangescherpt. Het doel is het gemeenschappelijk Europees niveau op het gebied van cyberweerbaarheid te verhogen. Deze richtlijn wordt nu vertaald naar Nederlandse wetgeving, die naar verwachting in januari 2024 als voorstel bekend gemaakt wordt. In oktober 2024 wordt deze nieuwe wet van kracht.

FERM gaat in de zogenoemde ‘consultatieronde’ – na januari 2024 – feedback geven op de voorgestelde wet met input van de bij ons aangesloten organisaties.

WAT VERANDERT ER?

Een paar honderd – vitale – bedrijven in Nederland zijn in scope van de NIS, die vertaald is naar de Wet beveiliging netwerk en informatiesystemen (Wbni). Deze scope wordt in de wet die op basis van NIS2 opgesteld gaat worden flink uitgebreid, naar verwachting zullen dit duizenden organisaties zijn. Ook zal de impact van de wetgeving steviger zijn. In de huidige Wbni staat een zorgplicht en een meldplicht: zorgen dat er passende maatregelen genomen te worden om hoge risico’s te voorkomen en melden als er iets gebeurt bij speciaal aangewezen instanties. De NIS2 heeft de zorgplicht uitgebreid, de meldplicht aangescherpt en introduceert een registratieplicht en toezicht.

Onder de zorgplicht valt nu niet alleen dat er passende maatregelen genomen moeten worden, maar deze moeten aantoonbaar voortkomen uit een risicoanalyse waarbij het bestuur van de organisatie deze analyse moet goedkeuren en op implementatie van de maatregelen moet toezien. Het bestuur moet daarvoor jaarlijkse getraind worden en zijn aansprakelijk als de wetgeving niet wordt nageleefd.

De meldplicht is aangescherpt; incidenten moeten nu binnen 24 uur gemeld worden.
Nieuw is de registratieplicht: de overheid zal geen bedrijven aanwijzen, maar levert een lijst op van type organisaties in scope en de organisatie is verplicht zichzelf te registreren als NIS2 plichtig. Ten slotte eist de NIS2 richtlijn ook dat er formeel toezicht wordt ingericht door onze overheid. Deze verplichtingen komen met een toezichthouder en mogelijke boetes voor organisaties die hier niet aan voldoen – de Europese richtlijn noemt 2% van de wereldwijde jaaromzet of € 10.000.000.

VAL IK ERONDER?

Enkele kaders om te controleren of je er onder valt: heb je meer dan 50 FTE óf een jaaromzet van meer dan 10 miljoen of een balanstotaal van meer dan 43 miljoen en ben je actief in een van de volgende 18 sectoren? Dan mag je ervan uitgaan dat je eronder valt.

18 sectoren

1. Energie
   a) elektriciteit
   b) stadsverwarming en -koeling
   c) aardolie
   d) aardgas
   e) waterstof
2. Transport
   a) lucht
   b) spoor
   c) water
   d) weg
3. Bankwezen
4. Infrastructuur voor de financiële markt
5. Gezondheidszorg
6. Drinkwater
7. Afvalwater
8. Digitale infrastructuur
9. Beheer van ICT-diensten (B2B)
10. Overheidsdiensten
11. Ruimtevaart
12. Post- en koeriersdiensten
13. Afvalstoffenbeheer
14. Chemische stoffen
15. Levensmiddelen
16. Vervaardiging / Manufacturing
    a) van medische hulpmiddelen en voor in-vitrodiagnostiek
    b) informaticaproducten en elektronische en optische producten
    c) elektrische apparatuur
    d) machines, apparaten en werktuigen, n.e.g.
    e) motorvoertuigen, aanhangers en opleggers
    f) andere transportmiddelen
17. Digitale aanbieders
18. Onderzoek

‘ESSENTIEEL’ EN ‘BELANGRIJK’

Er wordt voor de toepasselijkheid van de NIS2 een onderscheid gemaakt tussen ‘essentiële’ en ‘belangrijke’ bedrijven, en tussen ‘middelgroot’ (tussen de 50-250 medewerkers en een jaaromzet van 10-50 miljoen) en ‘groot’ (alles daarboven of een jaarlijks balanstotaal van meer dan 43 miljoen). Valt een bedrijf onder de sectoren 1 tot en met 11 en is er sprake van een grote entiteit, dan is het een essentieel bedrijf. De middelgrote entiteiten zijn ‘belangrijk’. Is sector 12 tot en met 18 van toepassing, dan vallen zowel groot als middelgroot onder belangrijk.

Van essentiële entiteiten wordt over het algemeen aangenomen dat de uitval van hun diensten veel meer ontwrichtende impact heeft op de economie en samenleving, dan uitval bij belangrijke entiteiten. Essentiële entiteiten vallen daarom onder een intensiever regime van toezicht, waarin zowel voor- als achteraf toezicht wordt gehouden op de naleving van de verplichtingen.

Voor een meer preciezere duiding – er zijn ook tal van uitzonderingen – heeft onze partner Digital Trust Center een tool gelanceerd: regelhulpenvoorbedrijven.nl/NIS-2-NL

NIS2: SERIEUZE GAMECHANGER IN CYBERSECURITY

De komst van de nieuwe wet gebaseerd op NIS2 is een gamechanger op drie gebieden:

1) De huidige wetgeving had bij introductie in de gehele Mainport Rotterdam slechts betrekking op 1 havenbedrijf (Havenbedrijf Rotterdam), waarna later ook een handjevol multinationals werd toegevoegd. De aangepaste wetgeving zal naar schatting betrekking hebben op zo’n 150-450 bedrijven in de Mainport Rotterdam. Uiteraard is het aantal bedrijven in de gehele Europoort regio én de Nederlandse economie nog groter.
2) De NIS2 behelst niet alleen de voorwaarde dat je je eigen cyberweerbaarheid onder controle hebt, maar bevat ook verplichtingen omtrent rapportage en richting je keten en leveranciers.

Bedrijven kunnen verantwoordelijk worden gehouden bij incidenten, waarbij bestuurders aansprakelijke gesteld kunnen worden als geconstateerd wordt dat een organisatie niet voldoet aan de wet.

Wat zijn de risicobeheersmaatregelen?

De verplichting tot het nemen van risicobeheersmaatregelen op het gebied van cyberbeveiliging, inclusief beveiliging van de toeleveringsketen. Dat levert een praktische lijst op die je op de volgende pagina's kunt koppelen aan de dienstverlening van FERM en haar netwerk.

i. beleid inzake risicoanalyse en beveiliging van informatiesystemen;
ii. incidentenbehandeling;
iii. bedrijfscontinuïteit, zoals back-upbeheer, noodvoorzieningen en crisisbeheer;
iv. de beveiliging van de toeleveringsketen;
v. beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
vi. de effectiviteit van maatregelen tegen cyberbeveiligingsrisico’s te kunnen beoordelen;
vii. basispraktijken op het gebied van cyberhygiëne en opleiding;
viii. beleid en procedures inzake het gebruik van cryptografie en/of encryptie;
ix. beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
x. multifactor-authenticatie- of beveiligde communicatie binnen de entiteit.

Wat houdt de rapportageverplichting in?

Een meldplicht bij significante incidenten:

- binnen 24 uur een waarschuwing
- binnen 72 uur een melding
- binnen 1 maand na de melding een eindverslag indienen

WAT ZIJN MOGELIJK OPGELEGDE GELDBOETES EN SANCTIES?

Er wordt voor de mogelijk opgelegde geldboetes en sancties een verschil gemaakt tussen ‘essentiële’ en ‘belangrijke’ bedrijven. Voor ‘essentiële’ bedrijven geldt voor het niet opvolgen van de zorgplicht of meldplicht een administratieve geldboete met een maximumbedrag van ten minste € 10.000.000 óf ten minste 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de essentiële entiteit behoort (afhankelijk van wel bedrag hoger is). Indien de door de handhaver gevraagde actie niet binnen de gestelde termijn wordt ondernomen, krijgt de bevoegde autoriteit de bevoegdheid om al dan niet via de rechter een vergunning tijdelijk op te schorten, en een natuurlijk persoon (algemeen directeur of wettelijke vertegenwoordiger) tijdelijk te verbieden deze rol uit te voeren. Voor ‘belangrijke’ bedrijven is de boete minder hoog, namelijk 1,4% van de wereldwijde omzet of maximaal 7 miljoen euro. Daar geldt opschorting van de bevoegdheid en uit functie zetten van een natuurlijk persoon niet.

WAT KUN JE ALS BEDRIJF DOEN?

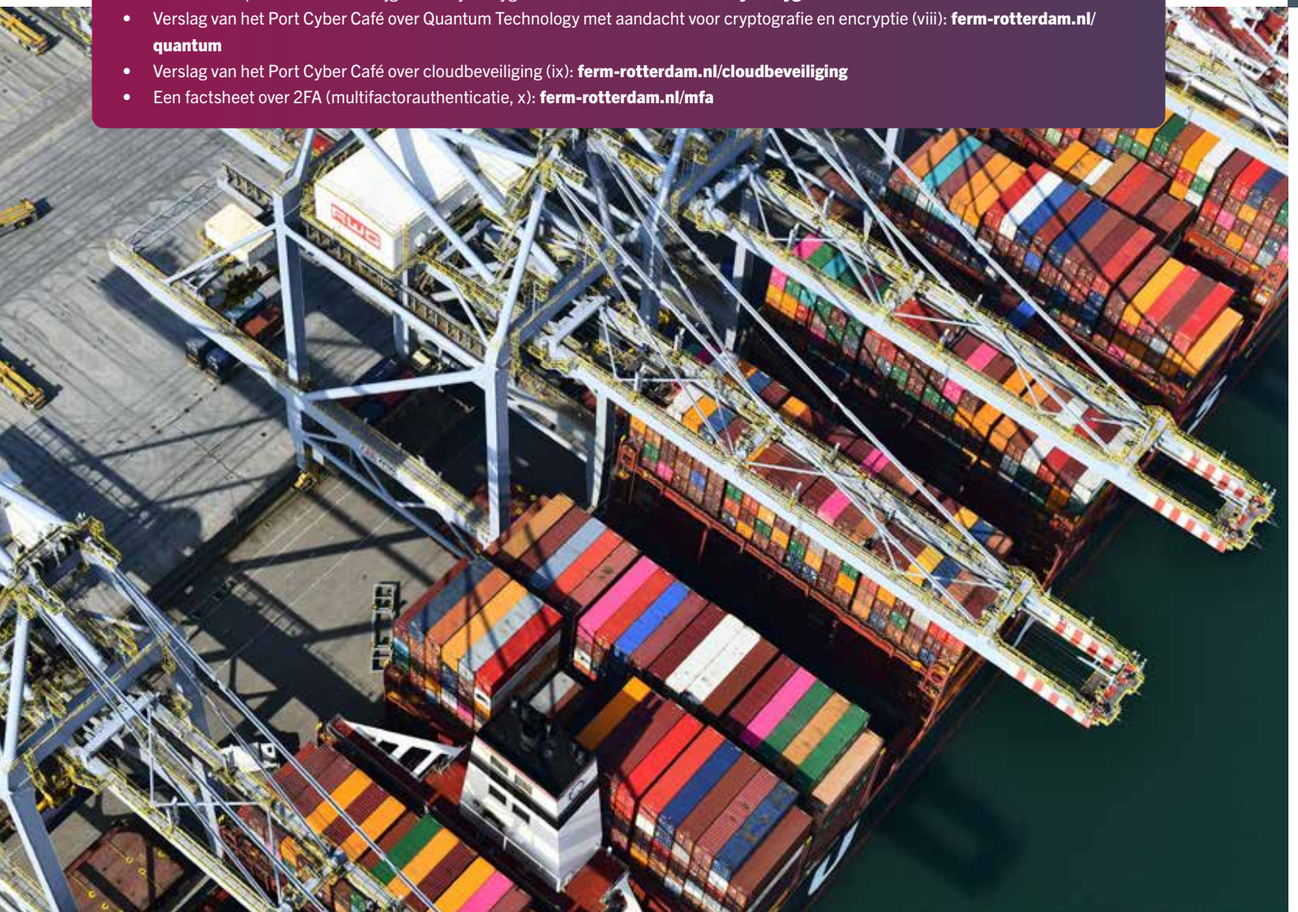
START VROEG, MAAR PAS OP VOOR COWBOYS
Het is verstandig om NU al een eerste analyse te maken: vallen wij onder de NIS2, wat heb ik al geregeld en wat nog niet? Waar moet je je op voorbereiden?

Er zijn enorm veel mogelijkheden en nieuwe consultancy organisaties en tooling ontstaan om je te helpen. Let daarbij op het volgende!

1. Per sector kunnen er accentverschillen gelegd gaan worden. Er komen waarschijnlijk verschillende toezichthouders, wat er helaas voor zorgt dat je niet een set maatregelen van andere bedrijven kunt “kopiëren” – elk bedrijf moet zijn eigen analyse maken gebaseerd op risico’s voor dat specifieke bedrijf.
2. De verplichtingen gaan verder dan alleen de techniek. Het omvat ook training van het bestuur en de medewerkers, toegangsbeleid en omgaan met je leveranciers – inkoopbeleid – en mogelijk zelfs aanpassing van bestaande contracten.
3. Er zijn naast serieuze aanbieders ook cowboys op de markt. Elke tool of oplossing die je nú al kan beloven dat je “NIS2-compliant” wordt, moet een rode vlag opleveren – immers ís de Nederlandse wet er nu nog niet.

Wat kan ‘iedereen’ bij ons vinden?

- Samenvatting van de NIS2: **ferm-rotterdam.nl/samenvatting-nis2**
- Een Incident Respons Plan met specifieke havenmeldpunten, geschikt als basis voor ‘incidentafhandeling’ (ii, v): **ferm-rotterdam.nl/irp**
- Een bijdrage van SANS over goed backupbeheer (iii): **ferm-rotterdam.nl/backup**
- Praktische tips voor het orde krijgen van cyberhygiëne (vii): **ferm-rotterdam.nl/cyberhygiene**
- Verslag van het Port Cyber Café over Quantum Technology met aandacht voor cryptografie en encryptie (viii): **ferm-rotterdam.nl/quantum**
- Verslag van het Port Cyber Café over cloudbeveiliging (ix): **ferm-rotterdam.nl/cloudbeveiliging**
- Een factsheet over 2FA (multifactorauthenticatie, x): **ferm-rotterdam.nl/mfa**



Wat we doen in vertrouwelijkheid, voor onze participanten?

- Leren van een collega wat al in scope is van de Wbni (NIS-richtlijn)
- Tijdige, actuele en relevante dreigingsinformatie met zogenoemd ‘handelingsperspectief’ vanuit onze rol als OKTT: **ferm-rotterdam.nl/oktt**
- Nulmeting (of FERM Cyberweerbaarheidsscan) voor inzicht in de huidige situatie, gericht op beleid rond risicoanalyse/beveiliging (i): **ferm-rotterdam.nl/nulmeting**
- Toegang tot CYRA, een tool waarmee je de cyberweerbaarheid van – en naar - leveranciers en klanten aantoonbaar kunt maken (iv): **ferm-rotterdam.nl/cyra**
- Besloten oefeningen en trainingen (vi, vii), waaronder Cybernautics FERM, diverse cybersecuritytrainingen zoals Introduction to Cybersecurity Management, en onze periodieke NIS2-bijeenkomsten

Onze participanten bieden we via het FERM-portal diensten van aangesloten partners aan. Via **ferm-rotterdam.nl/portfolio** vind je een geselecteerd overzicht, waaronder;

- Short Cyber Resilience & Incident Preparedness Test, waarbij twee specialisten in één werkdag de resultaten met je doornemen. Aan de hand van deze resultaten gaan zij met jou en je collega's sparren over realistische aanvalsscenario’s, bescherming van de kroonjuwelen van de organisatie en hoe te reageren op een digitaal incident.
- NIS2 GAP analyse (op basis van de Europese richtlijn): deze analyse wordt uitgevoerd door middel van interviews, document reviews en systeem reviews, die in een heldere rapportage worden verwerkt met handvatten en acties.
- [Binnenkort]: on-boarding training en online cursusportfolio.

SAMEN STAAN WE FERM?
“Cyber – daar hebben we FERM toch voor?”

FERM zet zich in voor digitale veiligheid van bedrijven. Cyberweerbaarheid is én blijft de verantwoordelijkheid van bedrijven zelf, maar FERM kan je ondersteunen om de taken die hierbij horen te vervullen. Wat we ‘voor iedereen’ kunnen, doen we ‘voor iedereen’ en wat in vertrouwelijkheid moet, doen we in vertrouwelijkheid, met bedrijven die in FERM participeren. FERM deelnemers hebben elkaar om de NIS2 richtlijn te begrijpen en passende maatregelen bij bepaalde risico’s te definieren. Ook krijgen FERM participanten vouchers (waardebonnen) waarmee ze cybersecuritydiensten kunnen inkopen als onderdeel van de gedefinieerde set maatregelen.

In de nu volgende kaders vind je de ondersteuning vanuit FERM respectievelijk voor ‘iedereen’ (onder andere vanuit onze openbare website) en voor onze participanten vanuit onze dienstverlening. De Romeinse cijfers tussen haakjes (i tot en met x) corresponderen met het overzicht van **risicobeheersmaatregelen** op de vorige pagina's.

In januari gaan we gezamenlijk feedback geven op de wetgeving. Wil je daaraan nog meedoen, kun je je nu nog aansluiten bij FERM. Help jouw organisatie en laat je horen, want SAMEN staan we FERM en hebben we ook een FERMere stem in Den Haag.

WWW.FERM-ROTTERDAM.NL/LID-WORDEN