Ploum
Rotterdam Law Firm

Cybersecurity risico's in de logistiek (NDL)

NIS2, cybersecuritywet en -regels in de praktijk

15 juni 2023

Hugo van Aardenne

Wrap-up presentatie Ploum / Stappenplan

- **NIS2 betekent:**
  - **=> forse uitbreiding van sectoren**
  - **=> forse uitbreiding van verplichtingen**
  - **=> forse uitbreiding consequenties bij schending verplichtingen**

- **STAP 1: beoordeel of het bedrijf onder de NIS2 valt**
  - Onderscheid zeer kritieke sectoren en andere kritieke sectoren;
  - Onderscheid tussen essentiële en belangrijke entiteiten;
  - De omvang van een bedrijf is niet doorslaggevend en het gaat om waar de bedrijfsactiviteiten worden ontplooid;

- **STAP 2: indien het bedrijf niet onder de NIS2 valt**
  - Houdt de juridische ontwikkelingen bij, er kunnen mogelijk toch verplichtingen vanuit het nationale recht ontstaan. Beoordeel tevens of aanvullende maatregelen (toch) wenselijk zijn in het kader van de cyberresilience, en om schade en claims te voorkomen.
  - Beoordeel of leveranciers of dienstverleners onder de NIS2 vallen;

- **STAP 3: indien het bedrijf onder de NIS2 valt**
  - Maak budget vrij;
  - Laat de juridische verplichtingen inventariseren en beoordeel wat deze betekenen voor uw bedrijf. Denk hierbij aan:
    - Het treffen van maatregelen op het gebied van resilience (minimumverplichtingen + maatregelen afgestemd op specifieke risico's);
    - (opleidings)Verplichtingen voor de board en personeel;
    - (meldings)Verplichtingen bij incidenten;
    - Verplichtingen m.b.t. het vastleggen van beleid en maatregelen;
    - Verplichtingen die zien op het kennen van de resilience van leveranciers/afnemers en partners;
    - Gevolgen voor de contracten met leveranciers/afnemers en partners;
  - Zet het budget in om de geïnventariseerde verplichtingen te implementeren;

- **STAP 4: indien het bedrijf niet, maar leveranciers/dienstverleners wel onder de NIS2 vallen**
  - Breng de gevolgen in kaart:
    - Welke gevolgen heeft de NIS2 voor die leveranciers/dienstverleners en hun services?
    - Welke aanvullende maatregelen verlangen zij eventueel van uw bedrijf?
    - Maak indien nodig budget vrij om de verlangde maatregelen te implementeren;

Cybercrime & Cybersecurity

- **Cybercrime:** Wat gebeurt er?
  - Hacken
  - Ransomware
  - DDoS
  - Spionage
  - Sabotage
- **Cybersecurity:** Wat is er aan te doen?
  - **P**revent
  - **D**etect
  - **R**esponse

NIS2 Wet-en regelgeving

Wat betekent het in de praktijk?

- Van **7** sectoren naar **18 s**ectoren
- Veel **m**eer **b**eveiligingseisen op het gebied van **p**revent, **d**etect & **r**epsonse
- **S**upply **c**hain beveiligen
- **M**eldingsplichten bij incidenten
- **C**ompliance, **g**overnance en **s**choling
- **A**ansprakelijkheid, handhaving, hoge boetes
- **P**raktische Tips

Sectoren

- NIS2-richtlijn tót oktober 2024 voor de implementatie.

- Vitale sectoren die moeten voldoen aan eisen van cybersecurity:

Zeer kritieke sectoren

- Energie, **vervoer**, bankwezen, infrastructuur financiële markt, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, openbaar bestuur en ruimtevaart.

Andere kritieke sectoren

- Post- en koeriersdiensten, afvalbeheer, vervaardiging, productie en distributie van chemische stoffen, voedingsproductie, -verwerking en –distributie, verwerkende industrie, digitale aanbieders en onderzoek

Vervoersectoren in de NIS2

Transportsectoren		
Sector	Subsector	Soort entiteit
Vervoer	**L**ucht	Luchtvaartmaatschappijen (definitie)
		Luchthavenbeheerders (definitie)
		Exploitanten op het gebied van verkeersbeheer en -controle die luchtverkeersleidingsdiensten (definitie)
	Spoor	Infrastructuurbeheerders (definitie)
		Spoorwegondernemingen (definitie)
	Water	Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht (definitie)
		Beheerders van havens én entiteiten die werken en uitrusting in havens beheren (definitie)
		Exploitanten van verkeersbegeleidingssystemen (definitie)
	Weg	Wegenautoriteiten (definitie)
		Exploitanten van intelligente vervoerssystemen (definitie)

Post- en koeriersdiensten

Post- en koeriersdiensten		
Sector	Subsector	Soort entiteit
Post- en koeriersdiensten		Aanbieders van postdiensten (definitie), met inbegrip van aanbieders van koeriersdiensten

Vervaardiging, productie en distributie van chemische stoffen

Vervaardiging, productie en distributie van chemische stoffen		
Sector	Subsector	Soort entiteit
Vervaardiging, productie **en distributie** van chemische stoffen		Ondernemingen die stoffen vervaardigen en stoffen of mengsels **distribueren** (definitie)

Productie, verwerking en distributie van levensmiddelen

Productie, verwerking en distributie van levensmiddelen		
Sector	Subsector	Soort entiteit
Productie, verwerking **en distributie van levensmiddelen**		Levensmiddelenbedrijven (definitie) die zich bezighouden met groothandel en industriële productie en verwerking

Sectoren, autoriteiten & toezichthouders nu

AED-sectoren	Bevoegde autoriteit	Toezichthouder dienst
Energie	Minister van Economische Zaken en Klimaat	Agentschap Telecom
Digitale infrastructuur	Minister van Economische Zaken en Klimaat	Agentschap Telecom
Bankwezen	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Infrastructuur voor de financiële markt	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Vervoer	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport
Levering en distributie van drinkwater	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport
Gezondheidszorg	Minister voor Medische zorg en Sport	Inspectie Gezondheidszorg en Jeugd

Toepassing

- Meer dan **250 fte en 50 miljoen euro omzet** dan zijn de bedrijven uit de zeer kritieke sectoren essentiële entiteiten. (Artikel 3 lid 1 sub a NIS2)
- Meer dan **50 fte en 10 miljoen euro** omzet voor bedrijven uit zeer kritieke sectoren of andere kritieke sectoren zijn belangrijke entiteiten (Artikel 3 lid 2 NIS2).
- Bedrijven *kunnen* worden aangewezen als kritieke of belangrijke entiteiten (artikel 3 lid 1 sub e en lid 2 NIS2)
- En dan wordt gekeken naar artikel 2 lid 2 sub b t/m e NIS2:

b) de entiteit in een lidstaat de enige aanbieder is van een dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten;

c) verstoring van de door de entiteit verleende dienst aanzienlijke gevolgen kan hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;

d) verstoring van de door de entiteit verleende dienst een aanzienlijk systeemrisico met zich kan brengen, met name voor sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;

e) de entiteit kritiek is vanwege het specifieke belang ervan op nationaal of regionaal niveau voor de specifieke sector of het specifieke type dienst, of voor andere onderling afhankelijke sectoren in de lidstaat;

Beveiligingseisen 1/2

- De lidstaten zorgen ervoor dat essentiële en belangrijke **entiteiten passende en evenredige technische, operationele en organisatorische maatregelen** nemen om de **risico's** voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het **verlenen van hun diensten** gebruiken, te **beheren en om incidenten te voorkomen of de gevolgen van incidenten** voor de afnemers van hun diensten en voor andere diensten te **beperken**.

- Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met **de uitvoeringskosten**, zorgen de in de eerste alinea bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is **afgestemd op de risico's die zich voordoen**. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen

Beveiligingseisen 2/2

- a) **beleid inzake risicoanalyse** en beveiliging van informatiesystemen;
- b) **incidentenbehandeling**;
- c) **bedrijfscontinuïteit**, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;
- d) de **beveiliging van de toeleveringsketen**, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties **tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners**;
- e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
- f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
- g) basispraktijken op het gebied van **cyberhygiëne en opleiding** op het gebied van cyberbeveiliging;
- h) beleid en procedures inzake het gebruik van **cryptografie** en, in voorkomend geval, **encryptie**;
- i) beveiligingsaspecten ten aanzien van **personeel, toegangsbeleid en beheer van activa**;
- j) wanneer gepast, het gebruik van **multifactor-authenticatie**- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Toeleveringsketen

- De lidstaten zorgen ervoor dat de entiteiten, wanneer zij overwegen **welke maatregelen** als bedoeld in lid 2, punt d), van dit artikel **passend zijn**, rekening houden met de **specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener** en met **de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners**, met inbegrip van hun veilige ontwikkelingsprocedures. De lidstaten zorgen er ook voor dat de entiteiten, wanneer zij overwegen welke maatregelen als bedoeld in lid 2, punt d), passend zijn, rekening moeten houden met de resultaten van de overeenkomstig artikel 22, lid 1, uitgevoerde gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.

- Op Unieniveau worden beveiligingsrisico's voor de toeleveringsketen beoordeeld.

Wbni

- a.de beveiliging van systemen en voorzieningen;
- b. behandeling van incidenten;
- c. het beheer van de bedrijfscontinuïteit;
- d. toezicht, controle en testen;
- e. inachtneming van de internationale normen.

Bbni Regeling (IenW)

- 1. Risicogebaseerde aanpak
  - De aanbieder heeft een actueel overzicht van de netwerk- en informatiesystemen die zijn essentiële dienst ondersteunen. De aanbieder stelt een risicoanalyse op waarin hij de risico's met betrekking tot de beveiliging beschrijft en ingaat op de wijze waarop hij de risico's naar een passend niveau verkleint. Hij motiveert daarbij waarom dit niveau volgens hem proportioneel en aanvaardbaar is. In die motivering gaat hij in ieder geval in op de organisatiespecifieke en sectorspecifieke risico's, het maatschappelijke belang van zijn essentiële dienst en de stand van de techniek. Hij legt de resultaten van de risicoanalyse schriftelijk vast en verwerkt de resultaten in beveiligings- en beheersmaatregelen.
- 2. Organisatie van netwerk- en informatiebeveiligingsbeheer
  - De aanbieder heeft een informatiebeveiligingsbeleid en -strategie en past deze actief toe. Hij heeft de taken, bevoegdheden en verantwoordelijkheden voor de beveiliging en beheer van zijn netwerk- en informatiesystemen in de organisatie belegd.
- 3. Incidenten voorkomen
  - De aanbieder heeft een gelaagde beveiligingsstrategie die is gebaseerd op de risico's die volgen uit de risicoanalyse. Defense in depth, lifecycle-, asset-, patch-, identificatie- en toegangsmanagement vormen in ieder geval onderdeel van deze strategie. Wanneer hij door relevante instanties zoals leveranciers of betrokken overheidsinstanties geattendeerd wordt op beveiligingsadviezen en dreigingsinformatie, beoordeelt hij of op basis daarvan gegeven de stand der techniek aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's te verkleinen naar een passend niveau. De aanbieder legt de bevindingen van zijn beoordeling schriftelijk vast.
- 4. Detectie en respons
  - De aanbieder heeft de beveiliging van zijn netwerk- en informatiesystemen zodanig ingericht dat hij daarmee incidenten kan detecteren, analyseren en vastleggen en de gevolgen daarvan zo veel mogelijk kan beperken. Hij monitort netwerk- en informatiesystemen structureel op kwetsbaarheden en mogelijke compromittatie en houdt hierbij rekening met de beschikbare dreigingsinformatie. Hij verzorgt het loggen van de handelingen op de netwerk- en informatiesystemen en bewaart deze gegevens lang genoeg om incidenten te kunnen analyseren. Hij hanteert procedures omtrent het optreden bij incidenten.
- 5. Gevolgen van incidenten beperken
  - De aanbieder stelt een bedrijfscontinuïteitsbeleid en crisismanagementbeleid op voor de netwerk- en informatiesystemen. Het crisismanagementbeleid bestaat in ieder geval uit een plan om de essentiële dienst zo spoedig mogelijk te herstellen na een incident. Het crisismanagementbeleid wordt daartoe periodiek in de praktijk beoefend.

- Artikel 3. ISMS
- Artikel 4. Risicoanalyse
- Artikel 5. Verbetercyclus
- Artikel 6. Beschrijving taken, bevoegdheden en verantwoordelijkheden
- Artikel 7. Kwalificaties functionarissen
- Artikel 8. Gedrag van management en medewerkers
- Artikel 9. Netwerk- en informatiesystemen
- Artikel 10. Asset- en lifecyclemanagement
- Artikel 11. Patchmanagement
- Artikel 12. Leveringsmanagement
- Artikel 13. Security by design
- Artikel 14. Fysiek beveiligingsbeleid
- Artikel 15. Logisch toegangsbeveiligingsbeleid
- Artikel 16. Software beveiliging
- Artikel 17. Gecontroleerd wijzigingenbeheer
- Artikel 18. Melden van incidenten, tekortkomingen en kwetsbaarheden
- Artikel 19. Loggen van beveiligingsgerelateerde handelingen
- Artikel 20. Monitoring van netwerk- en informatiesystemen
- Artikel 21. Respons op incident
- Artikel 22. Continuïteitsplannen
- Artikel 23. Herstel door backups

Meldingsplichten bij incidenten

- Bij CSIRT (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam) en/of bevoegde autoriteit melden.

- Onverwijld, **binnen 24 uur** nadat significant incident is ontdekt. Indien van toepassing met informatie of incident door onrechtmatige of kwaadwillende handeling is veroorzaakt of mogelijk grensoverschrijdende gevolgen kan hebben.
- onverwijld en in **elk geval binnen 72 uur** nadat zij kennis hebben gekregen van het significante incident, een incidentmelding indienen met, indien van toepassing, een update van de in punt a) bedoelde informatie, **een initiële beoordeling** van het significante incident, met inbegrip van de ernst en de gevolgen ervan en, indien beschikbaar, **de indicatoren voor aantasting. (Indicators of compromise).**

- uiterlijk één maand na de indiening van het in punt b) bedoelde incidentmelding, een eindverslag indienen waarin het volgende is opgenomen: (voortgangsverslag indien incident nog gaande is)

i) een **gedetailleerde beschrijving** van het incident, met inbegrip van de ernst en de gevolgen ervan;
ii) het soort bedreiging of de **grondoorzaak** die waarschijnlijk tot het incident heeft geleid;
iii) **toegepaste** en lopende **risicobeperkende maatregelen**;
iv) in voorkomend geval, de grensoverschrijdende gevolgen van het incident.

Governance, compliance & training

- 1. De lidstaten zorgen ervoor dat de **bestuursorganen** van essentiële en belangrijke entiteiten de door deze entiteiten **genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren** om te voldoen aan artikel 21, **toezien op de uitvoering ervan en aansprakelijk kunnen worden gesteld voor inbreuken** door de entiteiten op dat artikel.

- De toepassing van dit lid doet geen afbreuk aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen.

- 2. De lidstaten zorgen ervoor dat de **leden van de bestuursorganen** van essentiële en belangrijke entiteiten **een opleiding moeten volgen**, en moedigen essentiële en belangrijke entiteiten aan om regelmatig een soortgelijke opleiding aan hun werknemers aan te bieden, **zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.**

Aansprakelijkheid, handhaving hoge boetes

- a) **een certificering of vergunning tijdelijk op te schorten** of een certificerings- of vergunningsinstantie of een rechterlijke instantie overeenkomstig het nationale recht te verzoeken deze tijdelijk op te schorten **met betrekking tot alle of een deel van de** relevante door de essentiële entiteit **verleende diensten of verrichte activiteiten**;

- b) verzoeken dat de bevoegde organen of rechterlijke instanties overeenkomstig het nationale recht **een natuurlijke persoon met leidinggevende verantwoordelijkheden** op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in de essentiële entiteit **tijdelijk verbieden leidinggevende functies in die entiteit uit te oefenen**.

  - Boete tot **10 miljoen euro of 2% van de totale wereldwijde jaaromzet** voor **vervoersector**, en toezicht vóóraf en achteraf
  - Boete tot **7 miljoen euro of 1,4% van de totale wereldwijde jaaromzet**, toezicht achteraf voor **post- en koeriersdiensten**

Samenvatting

- Meer sectoren in de NIS2
- **Veroer** sector; deelsectoren; lucht, spoor, water, weg.
- Post- en koeriersdiensten
- Beveiligingsverplichtingen, waaronder bijvoorbeeld:
  - **Beleid**, risicoanalyse
  - Encryptie
  - **Bedrijfscontinuïteit**
  - **Toeleveringsketen**
  - **Fysieke beveiliging**
- **G**overnance/ trainingsverplichting voor bestuur (en medewerkers).
- **M**eldingsplicht
- Toezicht &Handhaving
  - **W**aarschuwing
  - **B**indende aanwijzing
  - **O**pschorten **v**ergunning of certificering
  - **Aansprakelijkheid** leidinggevende en **schorsen** leidinggevende
  - Boetes tot max.10 miljoen euro of 2% van de totale wereldwijde jaaromzet

  - **Implementatie in de Wbni uiterlijk 17 oktober 2024!**

Praktische tips

- Maak **budget** vrij voor cybersecurity, zowel techniek als compliance samen
- Kijk alvast naar **bestaande overeenkomsten**, en let op cybersecurity bij **nieuwe** overeenkomsten
- Bespreek de cybersecurity verplichtingen/ NIS2 met klanten en leveranciers
- **Oefenen** met incident respons (zodat je niet misgrijpt als een klant of toezichthouder ergens naar vraagt)

- Voorkom hoge boetes en andere ingrijpende maatregelen, dan:

Cyber – Europe

New EU cybersecurity legislation is credit positive

In May 2022, the European Union (EU) authorities reached provisional agreements on two pieces of legislation which will tighten cybersecurity requirements for companies, and apply them to a wider range of key industries. They will also reinforce the financial services sector's defences against cyberattacks, and make Europe's regulatory framework for preventing and resolving cybersecurity threats more harmonized. The new rules will not in themselves protect against advanced, targeted cyberattacks, but will enhance overall cyber resilience, a credit positive. They will also create an additional financial and administrative burden for businesses, particularly for smaller companies. The new legislation follows an increase in cyberattacks, which are emerging as a risk to financial stability as the EU economy digitalizes rapidly.

NIS2 directive will help economy withstand cyberattack

On 13 May 2022, the European Council and Parliament reached provisional agreement on an updated Network and Information Security Directive (the NIS2 Directive). NIS2 will force companies in key economic sectors to meet stricter cybersecurity requirements, making them better able to manage cyberattacks. This will improve their resilience as digitalization accelerates, and as geopolitical tensions mount. The new legislation addresses weaknesses in the original 2016 NIS Directive. Once formally adopted by the Council and the European Parliament, member states will have to incorporate NIS2 into national law within 21 months.

Ploum
Rotterdam Law Firm

Ploum l Rotterdam Law Firm
Blaak 28, 3011 TA Rotterdam

+31 10 440 6440
info@ploum.nl
www.ploum.nl