

Databalance

Wat is NIS2 en waarom is het belangrijk?





Alexander Freund

Information Security Consultant

a.freund@ictrecht.nl

NIS 2

Agenda – NIS 2

1 Tijdslijn en achtergrond

2 Scoping

3 Toezicht en Sancties

4 Governance (Bestuur)

5 Registratieplicht

5 Meldplicht

6 Zorgplicht

7 CSIRT

8 Tips voor cyberweerbaarheid

Tijdslijn en achtergrond

2016 NIS opgenomen in de WBNI

2020 EU werkt aan NIS2

2022 NIS2 wordt aangenomen in EU

2023 17 januari - NIS2 treedt in werking

2024 17 oktober - Deadline nationale wetgeving

2024 Eind jaar - Nationale wet aangenomen (verwacht)

2025 Begin Q1 - Implementatie nationale wet (verwacht)

Scoping

Essentiële entiteit:

1) Actief in een sector genoemd in bijlage I

2) Een “grote” organisatie: 250 personen of meer of een jaaronzet van >€50 miljoen en een balanstotaal van >€43 miljoen

Belangrijke entiteit:

1) Actief in een sector genoemd in bijlage I

2) Een “middelgrote” organisatie: 50 – 249 personen met een jaaronzet van €10 - €50 miljoen of een balanstotaal van €10-€43 miljoen

OF

1) Actief in een sector genoemd in bijlage II

2) Een “grote” of “middelgrote” organisatie op basis van bovengenoemde criteria

Bijlage I (Zeer kritieke sectoren)	Bijlage II (Andere kritieke sectoren)
Energie	Post en koeriersdiensten
Vervoer	Afvalstoffenbeheer
Bankwezen	Vervaardiging, productie en distributie van chemische stoffen
Infrastructuur voor de financiële markt	Productie, verwerking en distributie van levensmiddelen
Gezondheidszorg	Vervaardiging
Drinkwater	Digitale aanbieders
Afvalwater	Onderzoek
Digitale infrastructuur	
Beheer van ICT-diensten (business-to-business)	
Overheid	
Ruimtevaart	

Toezicht en Sancties



Toezicht

- Toezichthouder verschilt per sector
- Proactief voor essentiële organisaties
- Reactief toezicht voor belangrijke organisaties



Sancties

Hoge boetes die mogelijk gegeven kunnen worden vanuit de NIS2:

- Essentiële entiteiten: maximaal €10 miljoen of 2% van de jaaromzet
- Belangrijke entiteiten: €7 miljoen of 1,4% van de jaaromzet

Governance (bestuur)



Meer betrokkenheid van het bestuur.



Kennisniveau op het gebied van cyberbeveiliging door opleiding.



Geen apart aansprakelijkheidsregime voor het bestuur bij niet naleven van de verplichtingen. Aangesloten op bestaande regime.

Registratieplicht

Wie? Alle **'essentiële'** en **'belangrijke'** entiteiten



Doel: zicht op de digitale weerbaarheid

Verwacht: mogelijk vanaf medio oktober 2024

Welke gegevens:

- Organisatienaam
- Adres
- Actuele contactgegevens (e-mailadressen, IP-ranges, telefoonnummers)
- Sector en subsector

Meldplicht

24 uur

Binnen 24 uur een mogelijk incident melden bij instanties

Vroegtijdige waarschuwing

72 uur

Daadwerkelijke incidentmelding

Incident, effect en mogelijke oorzaken

1 maand

Verslag met beschrijving van het incident, de oorzaak, genomen maatregelen en de gevolgen van het incident

Mogelijk deadline verlengd als het incident nog gaande is, dan wel tussentijds verslag

Zorgplicht

NIS 2 schrijft voor dat er maatregelen genomen moeten worden voor het beheren van cyberbeveiligingsrisico's

- Risico-gebaseerd
- Rekening houdend met de stand van de techniek en de uitvoeringskosten

NIS2 bevat maatregelen die minimaal geïmplementeerd moeten worden zoals:

- Beleid inzake risicoanalyse en beveiliging van informatiesystemen;
- Incidentbehandeling;
- Bedrijfscontinuïteit;
- Beveiliging van de toeleveranciersketen;
- Cyberhygiëne en training op het gebied van cybersecurity
- Toegangsbeleid
- Multifactor-authenticatie (wanneer gepast)

CSIRT

- 1 Hulp bij incidenten
- 2 Verzamelen en analyse van forensische gegevens bij incidenten
- 3 Scannen van organisaties
- 4 Coördinerende rol bij het bekendmaken van kwetsbaarheden



CSIRT anders voor iedere sector

Tips voor vergroten cyberweerbaarheid

Risico
analyse

Awareness
Campagne

Incident
Management

Training
Intranetposts
Phishingtests

Vulnerability Scans
Virusscanner
End Point Security

Leveranciers
management

Opleidingen
en
Cursussen

Business
Continuity
Management

CCCO

Business Impact Analyse
Tabletop exercise

Vragen?





ICTRECHT
