Van chaos naar compliance: NIS2 uitgelegd in gewonemensentaal

Met Gaby Phielix

it local
Happy with it

Even voorstellen

Waarom een webinar over NIS2?

NIS2

NIS2 is de opvolger van de NIS1-richtlijn en heeft een bredere impact. Deze nieuwe richtlijn richt zich op de cyberweerbaarheid in de hele Europese Unie en raakt meer sectoren dan zijn voorganger.

In Nederland moeten ongeveer 10.000 organisaties zich aan deze richtlijn houden. NIS2 stelt minimale eisen aan de maatregelen die organisaties moeten nemen om hun cyberweerbaarheid te verbeteren.


NIS1


AVG


NIST


NIS2


NIS2

Waarom hebben we de NIS2 richtlijn nodig?

Te laat?

Onderdelen NIS2

Zorgplicht

Organisaties moeten zelf een **risicobeoordeling** uitvoeren en op basis daarvan passende maatregelen nemen om de continuïteit van hun diensten te waarborgen en de gebruikte **informatie** te beschermen.

Dit omvat het identificeren en beheren van risico's die de netwerk- en informatiesystemen bedreigen.

Meldplicht

Incidenten die de continuïteit van de dienstverlening aanzienlijk kunnen verstoren, moeten binnen **24 uur** worden gemeld bij de toezichthouder en het **Computer Security Incident Response Team (CSIRT).**

Dit helpt bij het snel reageren op en beperken van de impact van cyberincidenten.

Toezicht

Organisaties die onder de richtlijn vallen, krijgen verplicht toezicht.

Dit betekent dat er regelmatige controles en audits kunnen plaatsvinden om te controleren of de organisatie voldoet aan de gestelde eisen.

Onderdelen NIS2

Beveiligingsmaatregelen

Organisaties moeten sterke **beveiligingsmaatregelen** implementeren, zoals incidentmanagement, netwerkbeveiliging en encryptie.

Dit helpt bij het beschermen van de integriteit, vertrouwelijkheid en beschikbaarheid van hun systemen en gegevens.

Supply chain security

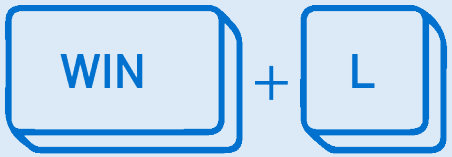
Het is belangrijk om de beveiliging van de **toeleveringsketen** te waarborgen.

Dit betekent dat ook leveranciers en partners moeten voldoen aan de beveiligingseisen om de gehele keten te beschermen.

Training en bewustwording

Medewerkers moeten getraind worden om **cyberdreigingen** te herkennen en te reageren op incidenten.

Dit omvat bijvoorbeeld trainingen over phishing en het gebruik van multi-factor authenticatie (MFA).



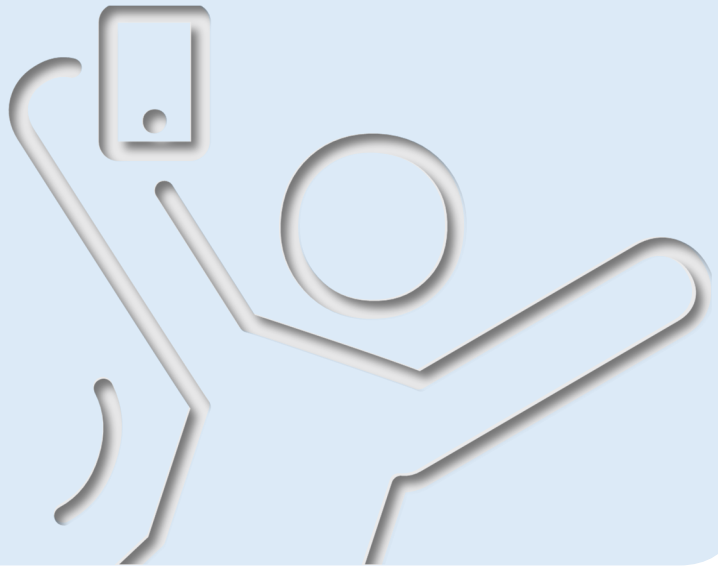
Cybersecurity maatregelen

- Risico management
- Cybersecurity beleid
- Incidentenafhandeling
- Business continuity
- Supply chain security
- Afhandeling van kwetsbaarheden en opvolging
- Beleid en procedures om effectiviteit van maatregelen te beoordelen
- Cryptografie
- Basis cybersecurity hygiëne & training
- Het gebruik van MFA

Incident rapportage verplichting

Rapporteren van incidenten met aanzienlijke gevolgen voor de dienstverlening:

- Binnen **24 uur** vroegtijdige waarschuwing
- Binnen **72 uur** incidentmelding
- Binnen **1 maand** eindverslag



Is NIS2 van toepassing op mijn organisatie?

Grote organisatie

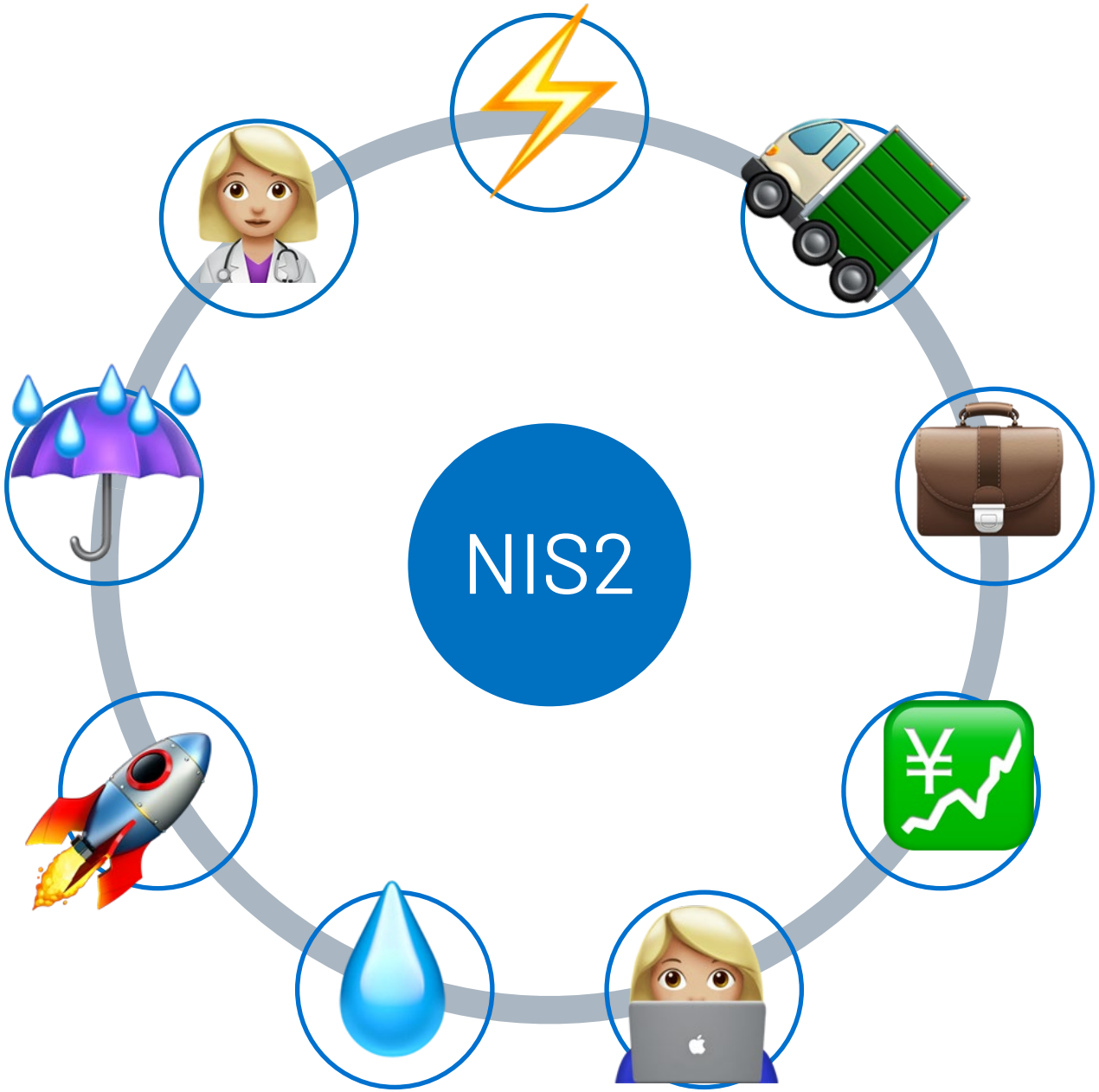
>= 250 medewerkers of Jaaromzet > 50 mio en balanstotaal > 43 mio

Middelgrote organisatie

>= 50 medewerkers of Jaaromzet en balanstotaal > 10 mio

Micro- en kleinbedrijf

< 50 medewerkers en jaaromzet en balanstotaal < 10 mio


NIS2

NIS2: essentiële entiteit

Sector

- Energie
- Transport
- Bankwezen
- Infrastructuur financiële markt
- Gezondheidszorg
- Drinkwater
- Digitale infrastructuur
- Beheerders van ICT-diensten
- Afvalwater
- Overheidsdiensten
- Ruimtevaart

NIS2: belangrijke entiteit

Sector

- Digitale aanbieders
- Post- en koeriersdiensten
- Afvalstoffenbeheer
- Levensmiddelen
- Chemische stoffen
- Onderzoek
- Vervaardiging / manufacturing

Geen NIS2

Uitzonderingen Micro- en kleinbedrijf

Bedrijven op het gebied van: vertrouwensdiensten, domeinnaamregistratie of openbare elektronische-communicatienetwerken of -diensten.

Verantwoordelijke minister voor bepaal de sector kan o.b.v. risicobeoordeling bedrijf alsnog aanwijzen.

Wat betekent dat nu voor jouw organisatie?

Uit welke stappen bestaat NIS2

1. Beheer

Voer een context- en gap-analyse uit om duidelijkheid te krijgen over de verplichtingen, waar jouw organisatie staat ten opzichte van de richtlijn en het ideale implementatieplan. Stel een jaarlijkse cyclus op, die je integreert met de jaarlijkse cyclus van de AVG (**Algemene Verordening Gegevensbescherming**) en de jaarlijkse cyclus voor IT-beveiliging.

2. Beleid en procedures

Ontwikkel beleidsregels en procedures voor werkzaamheden met betrekking tot NIS2. Stel algemene **IT-beveiligingsbeleidsregels** op. Veranker de beleidsregels bij het management, in de jaarlijkse cyclus en in lopende taken.

Wat betekent dat nu voor jouw organisatie?

Uit welke stappen bestaat NIS2

3. Risicomanagement

Breng je bezittingen in kaart en **identificeer** welke waardevolle middelen je hebt. Herken vervolgens de gevaren en zwakke punten die deze middelen kunnen bedreigen.

Voer een **risicobeoordeling** uit om de risico's van deze bedreigingen en kwetsbaarheden te bepalen. Neem ten slotte de juiste maatregelen om deze risico's te verminderen.

Wat betekent dat nu voor jouw organisatie?

Uit welke stappen bestaat NIS2

4. Leveranciers

Zoek uit wie je **belangrijkste leveranciers** zijn en maak duidelijke afspraken met hen. Controleer welke risico's er zijn en zorg voor veiligheidsmaatregelen.

Maak een plan om elk jaar te controleren of alles nog goed gaat. Voor de NIS2-regeling moeten de afspraken met leveranciers specifiek gaan over het delen van informatie, het melden van incidenten, en het naleven van beveiligingsstandaarden.

Wat betekent dat nu voor jouw organisatie?

Uit welke stappen bestaat NIS2

5. Training

Train jouw management over hun eigen **NIS2-verplichtingen** en de verplichtingen van je organisatie. Verzorg als organisatorische beveiligingsmaatregel bewustwordingstrainingen voor alle relevante medewerkers.

6. Incidentmanagement

Stel een procedure en een methode op voor de juiste registratie en afhandeling van incidenten.

Toezicht

NIS2: essentiële entiteit

Essentiële entiteiten:
Boete van 10 mil euro of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar

NIS2: belangrijke entiteit

Belangrijke entiteiten:
Boete tot 7 mil euro 1,4 % of van de totale wereldwijde jaaromzet in het boekjaar

Een handig stappenplan

1. Nulmeting uitvoeren
2. Beleid en procedures opstellen
3. Risicomanagement
4. Leveranciersbeheer
5. Training
6. Incidentmanagement

Handige links

NIS2-richtlijn NIS2-richtlijn - Digitale Overheid

Zorgplicht | Over het NCSC | Nationaal Cyber Security Centrum

IsCompliant: Uw sleutel tot informatiebeveiliging en compliance