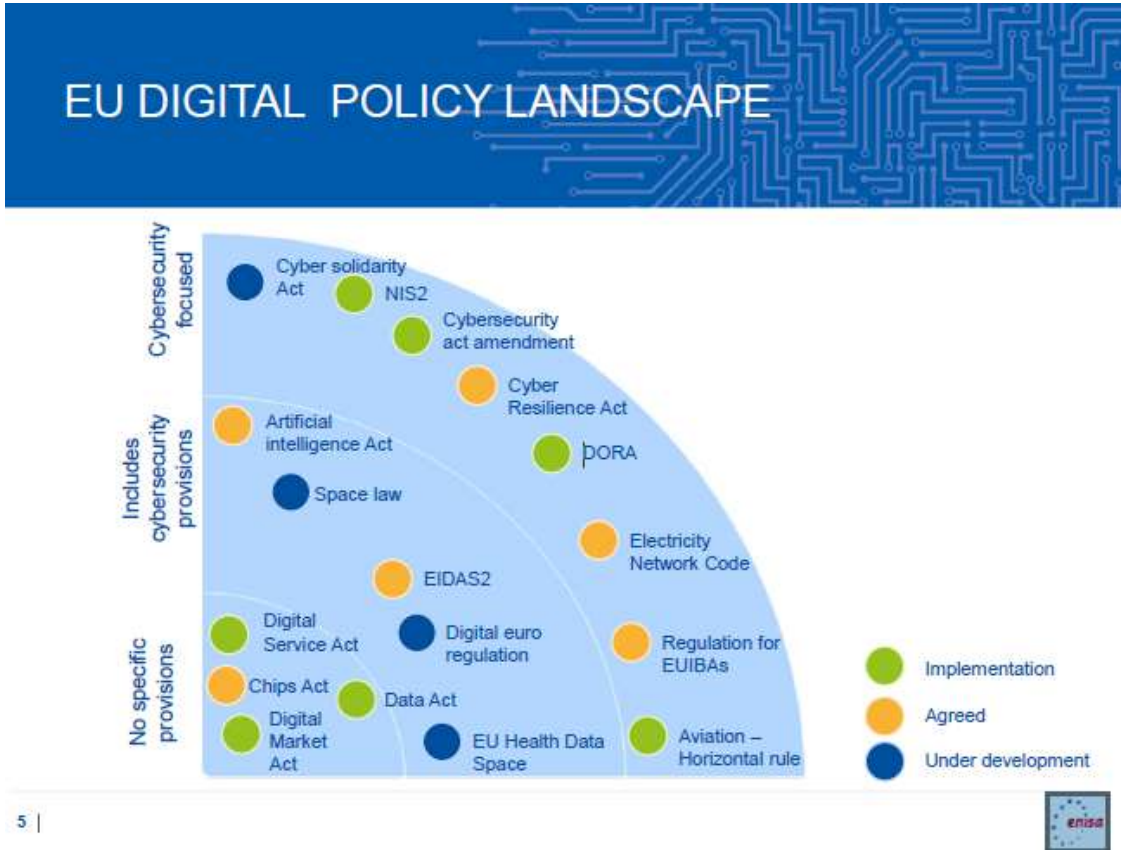
CYBERVEILIG NEDERLAND

Overzicht Europese cybersecurity wet- en regelgeving

Juni 2024

Er is op dit moment veel cybersecurity wet- en regelgeving in ontwikkeling

- Cyberbeveiligingswet (NIS2)
- Radioapparatenrichtlijn (RED)
- Cyber Resilience Act (CRA)
- Wet inzake cybersolidariteit (CSA)
- Cyberbeveiligingswet (mandaat ENISA)



De NIS2 is gericht op het verhoging van het niveau van cyberweerbaarheid binnen de EU

Artikel 1

Onderwerp

1. Deze richtlijn voorziet in maatregelen die erop gericht zijn een hoog gemeenschappelijk niveau van cyberbeveiliging in de [Europese] Unie te bereiken, teneinde de werking van de interne markt te verbeteren.

De wet geeft minder vrijheid aan lidstaten voor wat betreft de ondersteuning door CSIRT's, de zorgplicht én de meldplicht

- **Ontvangen** van **relevante dreigingsinformatie**
- **CSIRT-ondersteuning** vanuit het NCSC/CSIRT-DSP bij het treffen van maatregelen om de continuïteit van diensten te waarborgen of te herstellen (advies)

Het nemen van **passende cybersecurity maatregelen** (risico's beheersen, incidenten voorkomen en gevolgen van incidenten beperken) waarbij een **minimale set van maatregelen** wordt vereist **(zie artikel 21 lid 2)**

Digitale (bijna-) incidenten die voldoen aan drempelwaarde **melden bij CSIRT** (voor bijstand) **en toezichthouder** (controle)

Getrapte melding:
"early warning" binnen 24 uur, melding binnen 72 uur, eindverslag binnen 1 maand)

Rechten

Plichten

Toezicht

Sinds 2016 is er een Europese richtlijn die in de EU het niveau van cybersecurity moet verhogen

6 juli 2016

Network & Information Systems directive (NIS)

→

9 november 2018

Wet beveiliging netwerk- en informatiesystemen (Wbni)

16 januari 2023

Network & Information Systems directive 2 (NIS2)

→

17 oktober 2024 =
implementatie datum Cyberbeveiligingswet (Cbw)
Deze wordt echter pas medio 2025 verwacht

Overgangssituatie i.v.m. niet halen 17 oktober

NIS2 van kracht, maar nog niet omgezet in Nederlandse wetgeving

Planning is eind 2024 stemming in Tweede Kamer en medio 2025 omgezet in Nederlandse wetgeving

Wbni blijft van kracht

Dit betekent dat organisaties die nog niet onder de Wbni vallen en wel onder de Cbw nog niet aan de (zorg- en meld)plichten hoeven te voldoen, maar wel (CSIRT) rechten kunnen ontlenen bij een incident

De reikwijdte van de NIS2 is breder: essentiële en belangrijke sectoren

NIS	NIS2	Toezicht
Sectoren	Essentiële sectoren	Proactief
• Energie • Vervoer • Bankwezen • Infrastructuur financiële markt • Gezondheidszorg • Drinkwater • Digitale infrastructuur	• Alle NIS-sectoren (muv DSP's) • Afvalwater • Beheer van ICT-diensten • Overheid • Ruimtevaart	De toezichthouder waar de aanbieder onder valt
	Belangrijke sectoren	Reactief
Digitale dienstverleners	• Post- en koeriersdiensten • Afvalstoffenbeheer • Chemische industrie • Levensmiddelenindustrie • Maakindustrie • Digitale aanbieders • Onderzoek	De toezichthouder waar de aanbieder onder valt
• Aanbieders van clouddiensten • Online zoekmachines • Online marktplaatsen		

Zelfevaluatie: https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

Bron: Bijlage I en II in de NIS2 - https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555

De extra maatregelen zien toe op een basisniveau van digitale veiligheid

Basismaatregelen vanuit de NIS2 (artikel 21 lid 2)
a. **Beleid** inzake **risicoanalyse** en **beveiliging van informatiesystemen**
b. **Incidentenbehandeling**
c. **Bedrijfscontinuïteit**, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer
d. **Beveiliging** van de **toeleveringsketen**
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. **Multifactor authenticatie**, **continue-authenticatieoplossingen**, **beveiligde communicatie**

Cbw: Governance / bestuurder aan zet

In artikel 31 lid 4 en artikel 36 NIS2:

*…De lidstaten kunnen besluiten **passende**, **evenredige** en **doeltreffende toezichts- en handhavingsmaatregelen** ten aanzien van die instanties te nemen in overeenstemming met de nationale wetgevings- en institutionele kaders…*

*…De vastgestelde sancties moeten **doeltreffend**, **evenredig** en **afschrikkend** zijn…*

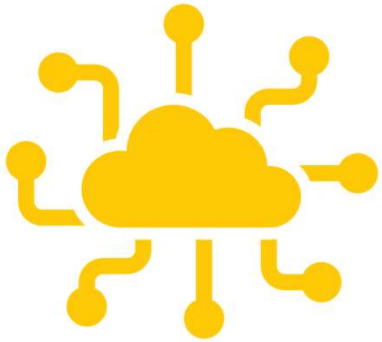
De consequenties, deels in uitzonderlijke situaties op te leggen, zijn uitgewerkt in de Cbw (art. 75-77):

- Handhavingsinstanties krijgen verregaande bevoegdheden tot ingrijpen
- Handhavingsinstanties krijgen verregaande bevoegdheden bij het uitblijven van maatregelen door een entiteit
  - Het opschorten van een vergunning of certificering van een essentiële entiteit
  - De algemeen directeur of wettelijke vertegenwoordiger van een essentiële entiteit tijdelijk verbieden leiding te geven
- Er kunnen boetes worden opgelegd (art. 77 Cbw) van 10 miljoen euro of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar

De Radioapparatenrichtlijn (RED) is gericht op apparaten in het radiospectrum

In de RED (Radioapparatenrichtlijn, 2014/53/EU), staan eisen die ervoor zorgen dat apparaten:

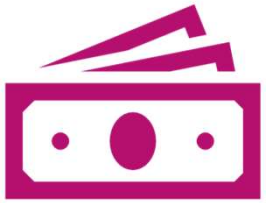
- andere apparatuur niet onacceptabel veel storen
- voldoende immuun zijn voor storende signalen
- geen gevaar vormen voor de gezondheid en veiligheid
- efficiënt en effectief gebruikmaken van het radiospectrum.



Daar komen vanaf 1 augustus 2025 eisen voor de cyberveiligheid bij

De cybersecurityeisen van de RED richten zich op drie aspecten

Netwerk-bescherming



Fraude-bescherming

Bescherming persoonsgegevens

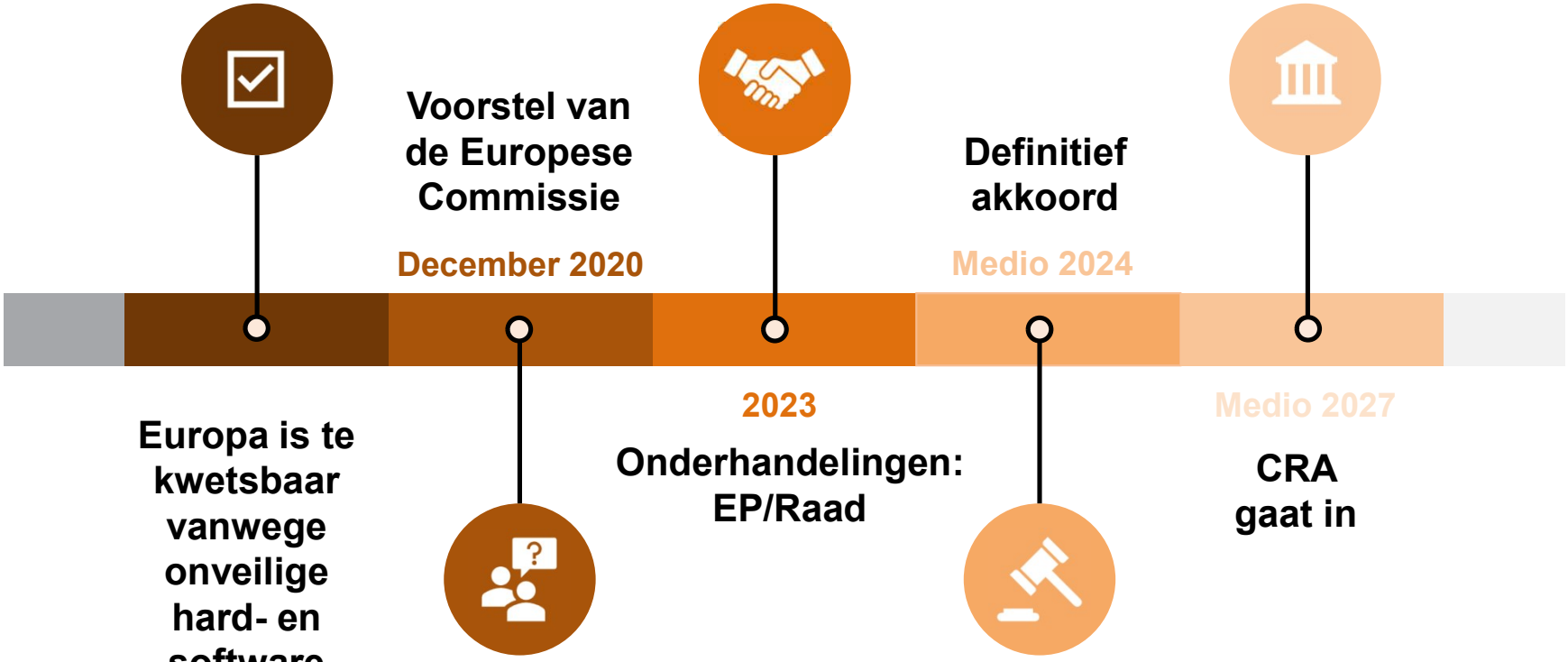
Aanvullende RED eisen treden op 1 augustus 2025 in werking

De Cyber Resilience Act (CRA) richt zich op de cybersecurity van hard- en software

CRA stelt **essentiële cybersecurity-eisen** aan **vrijwel alle hardware, software en losse componenten** die vanaf 2027 in de EU op de markt worden aangeboden:

- **Geharmoniseerde regels** bij het in de handel brengen van producten of software met een digitale component
- Een **kader van cyberbeveiligingsvereisten** voor de planning, het ontwerp, de ontwikkeling en het onderhoud van dergelijke producten, met verplichtingen waaraan in elke fase van de waardeketen moet worden voldaan
- Een verplichting om **zorgplicht** te verlenen voor de gehele levenscyclus van dergelijke producten. De ondersteuningsperiode voor fabrikanten moet ten minste vijf jaar zijn;
- Fabrikanten moeten de regels **36 maanden na inwerkingtreding** toepassen
- CRA is **een Act, geen richtlijn**: deze hoeft niet worden omgezet in Nederlandse wetgeving (anders dan wel het geval is bij de NIS2 of de GDPR)

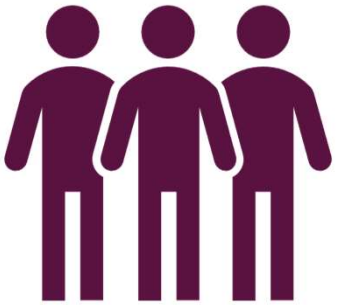
De verwachting is dat er een definitief akkoord komt medio 2024 en dat de CRA ingaat in 2027



De Cyber Solidarity Act (CSA) richt zich op samenwerking in geval van grote nood bij grote dreigingen en incidenten

De CSA voorziet in een **set van maatregelen** ter **versterking** van de **solidariteit** en de **capaciteit** in de Europese Unie om voor te bereiden en te reageren op cybersecurity dreigingen en incidenten:

- Opzetten van een zogenoemd **Europees Cyberschild**
- Inrichten van een **Europees Cybernoodmechanisme**
- Opstellen van een **Europees Evaluatiemechanisme** voor **cyberincidenten**



De Cyber Security Act - CSA is voornamelijk gericht op certificering binnen het cyberdomein

De CSA is een Europees certificeringsstelsel voor producten, diensten en processen op het gebied van cybersecurity:

- Versterkt het Agentschap van de EU voor cyberbeveiliging (Enisa):
  - Verantwoordelijk voor het **informeren** van het **publiek** over de **certificeringsregelingen**
  - Het **afgegeven van certificaten** via een speciale website
  - **Coördinatie** in geval van **grootschalige grensoverschrijdende cyberaanvallen en -crises**
- Stelt een **kader** voor **cyberbeveiligingscertificering** voor **producten** en **diensten** vast
- Drietal beveiligingsniveaus: laag, substantieel en hoog

CYBERVEILIG NEDERLAND

Liesbeth Holterman

info@cyberveilignederland.nl