Module 1: NIS2 in een notendop

Zes korte lessen over wat elke leidinggevende en elke medewerker van een NIS2-organisatie zou moeten weten, gevolgd door een quiz met 10 vragen. Met 80% bent u geslaagd.

NIS2 Aware · nis2aware.eu · november 2026

LES 1 VAN 6

Waarom NIS2?

Ziekenhuizen, havens, energieleveranciers, voedingsproducenten, clouddiensten: onze economie draait op netwerken en informatiesystemen. Eén ransomware-aanval kan een productie stilleggen, leveringen blokkeren of patiënten in gevaar brengen, en de schade slaat vaak over naar klanten en leveranciers.

De Europese Unie pakte dit eerst aan met de **NIS-richtlijn** in 2016. Die gold voor een beperkt aantal operatoren, en elk land paste ze op zijn eigen manier toe. Haar opvolger, de **NIS2-richtlijn** (Richtlijn (EU) 2022/2555), werd in december 2022 aangenomen om het niveau van cyberbeveiliging in de hele Unie op te trekken.

Wat NIS2 verandert

- **Een ruimer toepassingsgebied:** veel meer sectoren en, als regel, alle middelgrote en grote organisaties in die sectoren.
- **Strengere verplichtingen:** een gemeenschappelijke set risicobeheersmaatregelen en geharmoniseerde meldingstermijnen.
- **Verantwoordelijkheid van de leiding:** het bestuursorgaan moet de cyberbeveiliging goedkeuren en erop toezien, en het moet opgeleid zijn.
- **Echte handhaving:** toezicht door nationale autoriteiten en aanzienlijke boetes.

De richtlijn is niet rechtstreeks van toepassing op bedrijven: elke lidstaat moest ze tegen 17 oktober 2024 omzetten in nationaal recht. In België is dat de NIS2-wet.

OM TE ONTHOUDEN

- NIS2 is Richtlijn (EU) 2022/2555, de opvolger van de NIS-richtlijn van 2016.
- Ze geldt voor meer sectoren en meer organisaties, met strengere regels.
- Ze is van toepassing op bedrijven via het nationale recht.

LES 2 VAN 6

De Belgische NIS2-wet

België heeft NIS2 omgezet met de **wet van 26 april 2024** tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, aangevuld met een **koninklijk besluit van 9 juni 2024**. De wet is in werking getreden op **18 oktober 2024**.

De belangrijkste spelers

Wie	Rol
CCB, Centrum voor Cybersecurity België	Nationale cyberbeveiligingsautoriteit: toezicht, inspecties, sancties en begeleiding. Zijn team CERT.be is het nationale CSIRT dat incidentmeldingen behandelt.
Sectorale overheden	Werken in bepaalde sectoren samen met het CCB (bijvoorbeeld financiën, telecom, energie, vervoer, gezondheid).
Safeonweb@Work (atwork.safeonweb.be)	Het portaal van het CCB waar entiteiten zich registreren en informatie en tools vinden.

CyberFundamentals: de Belgische gereedschapskist

Het CCB ontwikkelde het **CyberFundamentals (CyFun®)**-kader: een reeks concrete beveiligingsmaatregelen met zekerheidsniveaus (Basic, Important en Essential). Een geactualiseerde versie, CyFun 2025, verscheen in oktober 2025. Organisaties kunnen CyFun of de internationale norm **ISO/IEC 27001** gebruiken om hun maatregelen te structureren en hun conformiteit aan te tonen.

> **Goed om te weten:** NIS2 Aware is een onafhankelijke opleidingsverstrekker. Voor officiële informatie verwijst u altijd naar het CCB.

OM TE ONTHOUDEN

- Belgische NIS2-wet: 26 april 2024, van kracht sinds 18 oktober 2024.
- Het CCB is de nationale autoriteit; registratie gebeurt via Safeonweb@Work.
- CyberFundamentals (CyFun) of ISO/IEC 27001 helpen om uw maatregelen te structureren en aan te tonen.

LES 3 VAN 6

Wie valt eronder?

De wet is van toepassing op organisaties die in België gevestigd zijn en aan twee voorwaarden voldoen: ze zijn actief in een **sector** die NIS2 vermeldt, en ze zijn minstens **middelgroot**.

Voorwaarde 1: de sector

Sectoren met een hoge kriticiteit (bijlage I)	Andere kritieke sectoren (bijlage II)
Energie · Vervoer · Bankwezen · Infrastructuur voor de financiële markt · Gezondheidszorg · Drinkwater · Afvalwater · Digitale infrastructuur (cloud, datacenters, DNS, telecom...) · Beheer van ICT-diensten, B2B (beheerde IT- en beveiligingsdiensten) · Overheid · Ruimtevaart	Post- en koeriersdiensten · Afvalbeheer · Chemische stoffen · Productie, verwerking en distributie van levensmiddelen · Vervaardiging (medische hulpmiddelen, informatica- en elektronische producten, elektrische apparatuur, machines, motorvoertuigen, andere transportmiddelen) · Digitale aanbieders (onlinemarktplaatsen, zoekmachines, sociale netwerken) · Onderzoek

Voorwaarde 2: de omvang

- **Middelgroot:** vanaf 50 werknemers, of een jaaromzet en een balanstotaal van meer dan 10 miljoen euro.
- **Groot:** vanaf 250 werknemers, of een omzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro.

Partner- en verbonden ondernemingen (bijvoorbeeld binnen een groep) kunnen meetellen voor deze cijfers.

Uitzonderingen

Sommige organisaties vallen eronder **ongeacht hun omvang**, bijvoorbeeld aanbieders van DNS-diensten, registers voor topleveldomeinnamen, gekwalificeerde verleners van vertrouwensdiensten en sommige aanbieders van openbare elektronische communicatie. Het CCB kan ook specifieke entiteiten aanwijzen.

> **Uw verantwoordelijkheid:** niemand stuurt u een brief. Elke organisatie moet zelf nagaan of ze onder de wet valt.

Valt u er niet onder? Dan kunt u toch geraakt worden: NIS2-entiteiten moeten de beveiliging van hun leveranciers beheren en zullen dus eisen aan u doorgeven.

OM TE ONTHOUDEN

- Twee voorwaarden: een NIS2-sector en minstens middelgroot (50 of meer werknemers, of meer dan 10 miljoen euro omzet en balanstotaal).
- Sommige digitale aanbieders vallen eronder ongeacht hun omvang.
- Elke organisatie moet zelf haar situatie nagaan; leveranciers worden onrechtstreeks geraakt.

LES 4 VAN 6

Essentiële of belangrijke entiteit?

Organisaties die onder de wet vallen, horen bij een van twee categorieën. De kernverplichtingen zijn **dezelfde**; wat verschilt, is de intensiteit van het toezicht en de hoogte van de boetes.

	Essentiële entiteit	Belangrijke entiteit
Typisch profiel	Grote organisaties in sectoren met een hoge kriticiteit (bijlage I), plus enkele specifieke gevallen	Middelgrote organisaties uit bijlage I, en middelgrote of grote uit bijlage II
Toezicht	Proactief (*ex ante*): het CCB kan op elk moment inspecteren	Reactief (*ex post*): vooral na een incident of aanwijzingen van niet-naleving
Conformiteitsbeoordeling	Verplicht en periodiek (CyberFundamentals of ISO/IEC 27001)	Vrijwillig, maar ze geeft een vermoeden van conformiteit
Maximale boete	10 miljoen euro of 2% van de wereldwijde jaaromzet	7 miljoen euro of 1,4% van de wereldwijde jaaromzet

Naast boetes kunnen de autoriteiten bindende instructies geven en, bij essentiële entiteiten die blijven tekortschieten, iemand tijdelijk verbieden leidinggevende functies uit te oefenen.

> **In de praktijk:** voor essentiële entiteiten rolt het CCB de conformiteitsbeoordeling gefaseerd uit. Een eerste mijlpaal viel op 18 april 2026, en er volgen er nog. Ga bij het CCB na welke data voor u gelden.

OM TE ONTHOUDEN

- Dezelfde verplichtingen; ander toezicht en andere boetes.
- Essentieel: proactief toezicht en verplichte conformiteitsbeoordeling; boetes tot 10 miljoen euro of 2%.
- Belangrijk: reactief toezicht; boetes tot 7 miljoen euro of 1,4%.

LES 5 VAN 6

De vier kernverplichtingen

1. Registreren

Entiteiten registreren zich bij het CCB via **Safeonweb@Work**. De termijnen liepen af op 18 december 2024 voor bepaalde digitale aanbieders en op 18 maart 2025 voor alle andere. Een organisatie die later onder de wet valt, moet zich onverwijld registreren.

2. Risicobeheersmaatregelen nemen

De maatregelen moeten passend en evenredig zijn met de risico's, volgens een "alle risico's"-benadering. De wet noemt minstens deze domeinen:

- risicoanalyse en beveiligingsbeleid voor informatiesystemen
- incidentenbehandeling
- bedrijfscontinuïteit: back-ups, herstel na een ramp, crisisbeheer
- beveiliging van de toeleveringsketen
- beveiliging bij de aankoop, ontwikkeling en het onderhoud van systemen, inclusief de behandeling van kwetsbaarheden
- beoordeling van de doeltreffendheid van de maatregelen
- basispraktijken voor cyberhygiëne en opleiding in cyberbeveiliging
- cryptografie en versleuteling
- beveiliging van personeel, toegangsbeheer en beheer van activa
- multifactorauthenticatie en beveiligde communicatie

3. Significante incidenten melden

Termijn	Wat
24 uur	Vroegtijdige waarschuwing aan het CCB nadat u kennis kreeg van een significant incident
72 uur	Incidentmelding met een eerste beoordeling
1 maand	Eindverslag

Waar nodig moeten ook de afnemers van uw diensten worden ingelicht.

4. De leiding betrekken en opleiden

Het bestuursorgaan moet de maatregelen **goedkeuren**, **toezien** op de uitvoering ervan en kan **aansprakelijk** worden gesteld. De leden ervan moeten **een opleiding volgen**; regelmatige opleiding van het personeel wordt ook aangemoedigd.

OM TE ONTHOUDEN

- Registreer u via Safeonweb@Work.
- Neem maatregelen in minstens tien domeinen, van risicoanalyse tot MFA.
- Meld significante incidenten: 24 uur, 72 uur, één maand.
- Het bestuur keurt goed, houdt toezicht, is aansprakelijk en moet opgeleid zijn.

LES 6 VAN 6

Belangrijke data en volgende stappen

December 2022
De NIS2-richtlijn wordt op Europees niveau aangenomen

26 april 2024
De Belgische NIS2-wet wordt aangenomen

18 oktober 2024
Inwerkingtreding in België

18 december 2024
Registratietermijn voor bepaalde digitale aanbieders

18 maart 2025
Registratietermijn voor alle andere entiteiten

Oktober 2025
Publicatie van CyberFundamentals 2025

18 april 2026
Eerste mijlpaal van de conformiteitsbeoordeling voor essentiële entiteiten

2027 en later
Verdere mijlpalen van de conformiteitsbeoordeling voor essentiële entiteiten (na te gaan bij het CCB)

Vijf stappen om nu te zetten

1. **Ga na of u onder de wet valt** en in welke categorie (essentieel of belangrijk).

2. **Registreer u** via Safeonweb@Work als dat nog niet gebeurd is.
3. **Breng uw lacunes in kaart** ten opzichte van CyberFundamentals of ISO/IEC 27001 en plan de verbeteringen.
4. **Organiseer de incidentmelding**: wie beslist, wie meldt, binnen 24 uur.
5. **Leid uw bestuur en uw personeel op**, en bewaar daar het bewijs van.

> U hebt de lessen van module 1 afgerond. Maak de quiz om uw kennis te testen.

OM TE ONTHOUDEN

- Van kracht sinds 18 oktober 2024; de registratietermijnen zijn verstreken.
- Essentiële entiteiten zitten in de fase van de conformiteitsbeoordeling.
- Volgende stappen: toepassingsgebied, registratie, lacuneanalyse, incidentprocedure, opleiding.

Deze module geeft algemene informatie over het Belgische NIS2-kader op datum van november 2026. Ze is geen juridisch advies. Raadpleeg altijd de meest recente informatie van het CCB (ccb.belgium.be en atwork.safeonweb.be).