Fendix
consultants

› Next Gen ‹ Control

Val ik onder de Cyber-beveiligingswet (NIS2)?

Check of je moet voldoen aan de nieuwste eisen van de Cbw.

fendix.nl

Inleiding

Met deze scan weet je waar je staat

Per 15 augustus 2026 is de Cyberbeveiligingswet (Cbw) van kracht. Dit is de Nederlandse invulling van de Europese NIS2-richtlijn. Er geldt geen overgangstermijn: vanaf dag één word je waarschijnlijk niet direct gecontroleerd, maar de verantwoordelijkheid geldt direct. Met deze scan weet je precies of je hiermee aan de slag moet.

Waarom deze scan?

Veel organisaties hebben moeite met het bepalen van hun rol binnen de NIS2-richtlijn. Val ik er wel onder? Of toch niet? Er zijn ruim 8.000 organisaties die onder de Cyberbeveiligingswet vallen en daarnaast tienduizenden leveranciers die indirect te maken krijgen met nieuwe eisen. Loop deze scan dus vooral even door!

Stap 1

Sector-check

Deel I

Sectoren van hoog belang

- [ ] Energie
- [ ] Vervoer
- [ ] Bankwezen
- [ ] Financiëlemarktinfrastructuur
- [ ] Gezondheidszorg (incl. zorgaanbieders, laboratoria, farmaceutische productie)
- [ ] Drinkwater
- [ ] Afvalwater
- [ ] Digitale infrastructuur (cloud, datacenters, DNS, CDN, trust service providers, elektronische communicatie)
- [ ] Beheer van ICT-diensten (B2B)
- [ ] Overheid
- [ ] Ruimtevaart

Deel II

Overige kritieke sectoren

- [ ] Post- en koeriersdiensten
- [ ] Afvalstoffenbeheer
- [ ] Chemische stoffen (productie, vervaardiging, distributie)
- [ ] Levensmiddelen (productie, verwerking, distributie)
- [ ] Vervaardiging (medische hulpmiddelen, elektronica, machines, motorvoertuigen, overige transportmiddelen)
- [ ] Digitale aanbieders (online marktplaatsen, zoekmachines, sociale-netwerkdiensten)
- [ ] Onderzoeksinstellingen

Geen enkele optie aangevinkt? Ga direct naar Stap 3.

Omvangcheck

Wie vallen altijd onder de Cbw?

Onder andere aanbieders van openbare elektronische-communicatienetwerken, DNS-dienstverleners, TLD-registries, trust service providers, en organisaties die de enige aanbieder van een kritieke dienst in Nederland zijn vallen altijd onder de Cyberbeveiligingswet. Daarnaast geldt de Cbw voor essentiele en belangrijke entiteiten.

Essentiele entiteit

- [ ] Sector: actief in sector uit Deel I (blz. 3)
- [ ] Omvang: meer dan 250 fte **of** jaaromzet meer dan €50 mln met balanstotaal meer dan €43 mln

Belangrijke entiteit

- [ ] Sector: actief in sector uit Deel I of II (blz. 3)
- [ ] Omvang: meer dan 50 fte **of** meer dan €10 mln jaaromzet

*Heb je de sector **en** omvang afgevinkt onder essentiele **of** belangrijke entiteit? Dan val je direct onder de Cyberbeveiligingswet en moet je in actie komen.*

*Als je alleen in de sector valt, dan val je (nog) niet direct onder de wet. Als je niets hebt aangevinkt, dan val je niet onder de wet. Kijk in beide gevallen nog wel even naar **Stap 3** van deze scan.*

Kom je er nog niet helemaal uit?

Door te starten pak je concurrentievoordeel. Plan hier een vrijblijvende en kosteloze check in.

Leveranciers

Wat als ik niet direct onder de wet val?

Dit is waar de meeste checklists stoppen en waar voor het mkb het echte risico begint. De Cbw kent namelijk ketenwerking. Organisaties die onder de wet vallen, zijn zelf verplicht om de beveiliging van hun leveranciers te beoordelen en te beheersen (onderdeel van de zorgplicht). Zij gaan dat vertalen naar vragenlijsten, audits en contractuele eisen richting jou. Tienduizenden Nederlandse leveranciers krijgen zo alsnog met NIS2-achtige eisen te maken, zonder dat ze zelf “onder de wet” vallen.

To do list

Concrete acties voor als je via de keten geraakt wordt:

- [ ] Breng in kaart welke klanten (mogelijk) onder de Cbw vallen: gebruik **Stap 1 en 2** hierboven ook voor hen.
- [ ] Je kunt op korte termijn security-vragenlijsten, due-diligence-verzoeken of aanvullende contractvoorwaarden vanuit die klanten verwachten. Zorg dat je op hoofdlijnen de volgende zaken kunt aantonen: toegangsbeheer, MFA, patchmanagement, back-upbeleid en je incidentproces.
- [ ] Overweeg een erkend kader (ISO 27001, NEN 7510) als aantoonbaar bewijs: dat bespaart je herhalende, losse vragenlijsten per klant.

Zie dit als een **commerciële kans**, niet alleen als last: leveranciers die dit als eerste op orde hebben, hebben een aantoonbaar voordeel bij offertetrajecten van NIS2-plichtige opdrachtgevers.

Plan een check in met Kilian

Nu inplannen

Check, dat was hem!

Goed werk. Je bent ermee bezig!

We hopen dat deze scan je heeft geholpen. We snappen dat de Cyberbeveiligingswet overweldigend kan zijn, maar maak je geen zorgen.

Heb je hulp nodig?

Twijfel je over de uitkomst, of wil je weten wat er concreet van je gevraagd gaat worden — direct of via een klant? Wij zijn er voor je.

Klik op bovenstaande knop en plan een vrijblijvend adviesgesprek in.
Dan gaan we ervoor zorgen dat jij goed voorbereid bent!

Bel ons
085 773 60 05

Stuur een mail
info@fendix.nl

Bereikbaar maandag t/m vrijdag tussen 09.00 en 17.00 uur.

Fendix
consultants

Next-Gen Consultants

Koplopers in compliance

fendix.nl