



NIS2 QUICKSCAN

Val ik onder de Cyberbeveiligingswet (NIS2)?

Check in een paar stappen of je moet voldoen aan de nieuwste eisen van de Cbw.





INLEIDING

Ontdek waar jij 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 de quickscan?

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

Sectorcheck

1 Sectoren van hoog belang

- ☐ Energie
- ☐ Vervoer
- ☐ Bankwezen
- ☐ Financiële marktinfrastructuur
- ☐ 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

2 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 dan verder naar stap 3.

STAP 2 - Omvangscheck

Wie vallen er 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 essentiële en belangrijke entiteiten.

1 Essentiële 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

2 Belangrijke entiteit

- ☐ Sector: actief in sector uit Deel 1 of 2 (blz. 3)
- ☐ Omvang: meer dan 50 fte of meer dan €10 mln jaaromzet

! Heb je de sector en omvang afgevinkt onder essentiële 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 de scan.



Kom je er nog niet helemaal uit?

We denken graag met je mee. Plan vrijblijvend een [NIS2-adviesgesprek](#) in.

STAP 3 - LEVERANCIERS

Wat is als 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.

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 NIS2 niet alleen als een verplichting, maar ook als een kans om je informatiebeveiliging beter op orde te brengen. Organisaties die hier nu mee aan de slag gaan, zijn beter voorbereid op vragen van klanten en opdrachtgevers.

CHECK, DAT WAS HEM ALWEER!

Goed werk — je bent ermee bezig!

We hopen dat deze scan je meer inzicht heeft gegeven in de impact van de Cyberbeveiligingswet op jouw organisatie. Kom je er niet helemaal uit of heb je vragen? We denken graag met je mee.

Transparant

We leggen keuzes, risico's en oplossingen altijd begrijpelijk uit.

Betrouwbaar

We kiezen technologie die bewezen veilig, duurzaam en stabiel is.

Waakzaam

We signaleren risico's en denken vooruit, in plaats van af te wachten.

Heb je vragen over NIS2?



Aron

Jouw aanspreekpunt voor NIS2

Twijfel je over de uitkomst van de scan? Of wil je weten wat NIS2 concreet voor jouw organisatie betekent? We denken graag met je mee.

Plan eenvoudig een vrijblijvende NIS2-check in. Samen bekijken we jouw situatie, brengen we de aandachtspunten in kaart en bespreken we welke vervolgstappen passen bij jouw organisatie.

[Plan een adviesgesprek in](#)

BEREIKBAAR

Ma–vr, 08.00–17.30 uur

BEL ONS

085 273 58 18

STUUR EEN MAIL

hello@inventit.nl