3. Meldplicht

Organisaties moeten significante incidenten melden bij hun Computer Security Incident Response Team (CSIRT) en toezichthouder. Voor het doen van meldingen heeft het NCSC een centraal meldportaal ingericht. Na de melding van een significant incident kan bijstand worden verkregen van het CSIRT. Lees op de website van het NCSC meer over meldplicht.

4. Toezicht

Op naleving van de verplichtingen uit de Cyberbeveiligingswet wordt toezicht gehouden.

Wacht niet af, bereid je voor.

De Rijksoverheid adviseert organisaties om niet af te wachten totdat de Cyberbeveiligingswet in werking is getreden. De risico's die organisaties en systemen lopen, zijn er immers nu ook al.

Doe de NIS2-Zelfevaluatie om er achter te komen of jouw organisatie onder de Cyberbeveiligingswet valt.

Vul de NIS2-Zelfevaluatie tool in om te bepalen of jouw organisatie onder de Cyberbeveiligingswet valt. Ook wordt duidelijk of je organisatie volgens de NIS2-richtlijn wordt gezien als 'essentieel' of 'belangrijk'.

Beoordeel jouw cybersecuritymaatregelen en identificeer jouw verbeterpunten.

Het Cbw Control Framework, ontwikkeld door de Auditdienst Rijk en NOREA, helpt IT-verantwoordelijken om verbeterpunten uit de Cyberbeveiligingswet te identificeren en gerichte stappen te zetten in het cyberveilig maken van jouw organisatie.

Gebruik de NIS2-Quickscan van de RDI om te toetsen of jouw bestaande maatregelen van jouw organisatie voldoen aan de eisen van de NIS2-richtlijn.

Meer over de Cyberbeveiligingswet is te lezen op de websites van de NCTV, het NCSC en op de websites van de betrokken vakdepartementen

Rijksoverheid

Cyberbeveiligingswet. Bereid je voor.

Veel van ons leven en werk speelt zich af in de digitale wereld. Omdat de digitale veiligheid van onze samenleving en economie steeds vaker onder druk staat, heeft de Europese Unie (EU) de NIS2-richtlijn vastgesteld. De NIS2-richtlijn heeft tot doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de EU te bereiken.

In Nederland wordt de NIS2-richtlijn geïmplementeerd in de Cyberbeveiligingswet. Op het moment dat de Cyberbeveiligingswet in werking treedt, vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni).

Belangrijkste onderdelen nieuwe Cyberbeveiligingswet

- Onderscheid tussen essentiële entiteiten en belangrijke entiteiten
- Zorgplicht, registratieplicht en meldplicht
- Bestuurlijke verantwoordelijkheid en trainingsplicht voor bestuurders
- Meer sectoren en organisaties
- Toezicht en handhaving
- Bijstand door Computer Security Incident Response Teams (CSIRT's) bij dreigingen en incidenten

Medegefinancierd door de Europese Unie

De Cyberbeveiligingswet is van toepassing op entiteiten die behoren tot de onderstaande sectoren en een bepaalde omvang hebben.

Eerste check: controleer of jouw organisatie een soort entiteit is genoemd in bijlage 1 of 2 van de Cyberbeveiligingswet

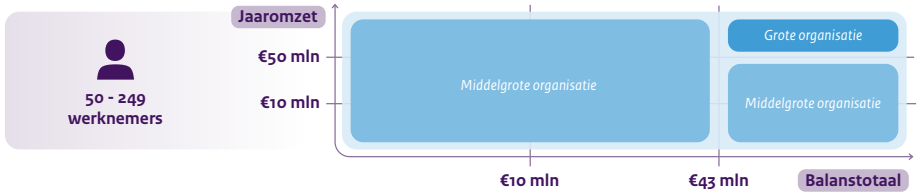
Bijlage 1

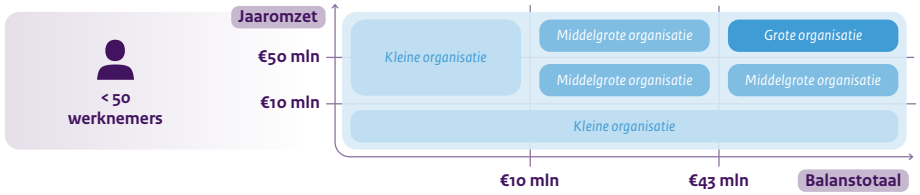
- Energie
- Vervoer
- Bankwezen
- Infrastructuur financiële markt
- Gezondheids-zorg
- Afvalwater
- Overheid
- Drinkwater
- Digitale infrastructuur
- Beheer van ICT-diensten
- Ruimtevaart

Bijlage 2

- Digitale aanbieders
- Post- en koeriersdiensten
- Afvalstoffen-beheer
- Levens-middelen
- Chemische stoffen
- Onderzoek
- Vervaardiging

Tweede check: controleer of jouw organisatie voldoet aan de omvangscriteria





Op basis van de sectoren in bijlage 1 en 2 van de Cyberbeveiligingswet en de omvangscriteria kan bepaald worden of een organisatie als een 'essentiële entiteit' of een 'belangrijke entiteit' wordt beschouwd. Essentiële entiteiten krijgen te maken met proactief toezicht en belangrijke entiteiten krijgen te maken met reactief toezicht.

Wat schrijft de Cyberbeveiligingswet onder andere voor?

1. Registratieplicht

Organisaties die onder de Cyberbeveiligingswet vallen, zijn verplicht gegevens te registreren in het entiteitenregister. In Nederland gebeurt dat bij het Nationaal Cyber Security Centrum (NCSC) op mijn.ncsc.nl. Na registratie krijgen deze organisaties toegang tot de dienstverlening van het betreffende CSIRT. Ga naar mijn.ncsc.nl of naar de website van het NCSC voor meer informatie over het doorlopen van een succesvolle registratie.

2. Zorgplicht

Organisaties moeten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen. Zo schrijft de Cyberbeveiligingswet 10 zorgplichtmaatregelen voor waar organisaties in ieder geval aan moeten voldoen.

Medegefinancierd door de Europese Unie