N Network

I Information

S Security

Cyberbeveiligingswet

Informatiebrochure

februari 2026

Inleiding

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. Deze richtlijn is de opvolger van de NIS1-richtlijn. 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 met de Cyberbeveiligingswet.[1] Op het moment dat de Cyberbeveiligingswet in werking treedt, vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni). Tegelijkertijd loopt ook de implementatie van de Critical Entities Resilience Directive (CER-richtlijn), die wordt geïmplementeerd in de Wet weerbaarheid kritieke entiteiten (Wwke). De wetten gaan tegelijkertijd in.

Het omzetten van de NIS2-richtlijn in nationale wetgeving vergt zorgvuldigheid, omdat de impact voor Nederlandse organisaties die onder de Cyberbeveiligingswet vallen, groot is. Zo vallen er meer sectoren en daarbinnen meer entiteiten onder de Cyberbeveiligingswet dan onder de Wbni. Voor deze entiteiten gelden verplichtingen als de zorg- en meldplicht en wordt het toezicht op de naleving van verplichtingen ingericht.

Wat zijn de belangrijkste onderdelen van de 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**

1 Zolang deze nog niet in werking is getreden gaat het om een wetsvoorstel. Met het oog op de leesbaarheid van deze brochure wordt hier gesproken van 'Cyberbeveiligingswet.'

Inhoud

Disclaimer

Deze informatiebrochure bevat basisinformatie over de Cyberbeveiligingswet.

1. *Aan de inhoud van deze informatiebrochure kunnen geen rechten worden ontleend.*
2. *Deze informatiebrochure is niet juridisch bindend. Organisaties zijn zelf verantwoordelijk voor het voldoen aan de eisen van Cyberbeveiligingswet.*
3. *Deze informatiebrochure is opgesteld in november 2025 en wordt indien nodig geactualiseerd.*

1

Valt jouw organisatie onder de Cyberbeveiligingswet?

Valt uw organisatie onder de Cyberbeveiligingswet?

Bij de Cyberbeveiligingswet vallen veel organisaties van rechtswege onder de wet. Organisaties zijn zelf verantwoordelijk om te bepalen of zij onder deze wet vallen.

Zelfevaluatietool

Organisaties kunnen met de zelfevaluatietool eerst zelf beoordeling doen of ze onder de Cyberbeveiligingswet vallen en hoe ze worden gekwalificeerd (essentieel of belangrijk). Ook kunnen onderstaande stappen worden doorlopen om te bepalen of zij onder de Cyberbeveiligingswet vallen.

Stap 1 Controleer of jouw organisatie behoort tot een van onderstaande de sectoren

De Cyberbeveiligingswet is van toepassing op de onderstaande sectoren. Zie bijlage 1 en 2 van de Cyberbeveiligingswet voor een gedetailleerd overzicht van deze sectoren en daaronder vallende soorten entiteiten. Entiteiten die domeinnaamregistratiediensten verlenen staan niet vermeld in bijlage 1 of 2 van de Cyberbeveiligingswet. Op deze entiteiten zijn niet alle verplichtingen uit de Cyberbeveiligingswet van toepassing.

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

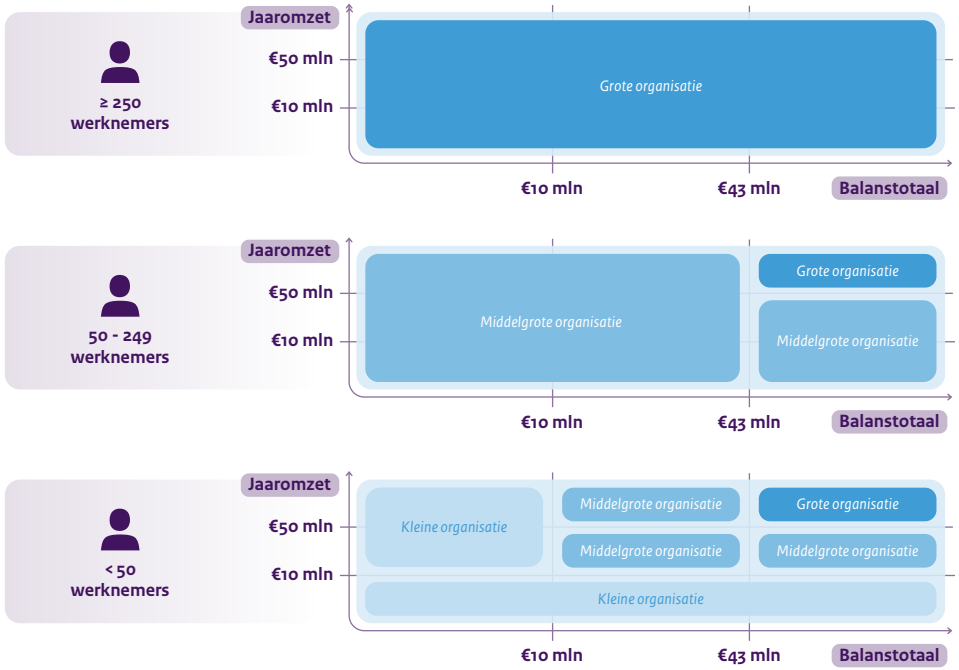
Stap 2 Controleer of jouw organisatie voldoet aan de omvangscriteria

Nadat je hebt gecheckt of jouw organisatie aan te merken is als een soort entiteit genoemd in bijlage 1 of bijlage 2 van de Cyberbeveiligingswet, dient er ook gecontroleerd te worden of jouw organisatie voldoet aan de omvangscriteria om te bepalen of je onder de Cyberbeveiligingswet valt (dit wordt ook wel de size cap genoemd). Hierbij wordt gekeken naar onder andere het aantal medewerkers, de jaaromzet en het balanstotaal. De omvangscriteria alleen zijn niet altijd relevant.

Aanbieders van openbare elektronische communicatienetwerken, aanbieders van openbare elektronische communicatiediensten, (gekwalificeerde) verleners van vertrouwensdiensten, aanbieders van registers voor topleveldomeinnamen, DNS-dienstverleners, verleners van domeinnaamregistratiediensten en overheidsorganisaties vallen altijd onder de Cyberbeveiligingswet, ongeacht hun omvang.

Stap 3 Bepaal aan de hand van het stroomschema of jouw organisatie een essentiële entiteit óf een belangrijke entiteit is

Wanneer duidelijk is dat jouw organisatie onder bijlage 1 of bijlage 2 van de Cyberbeveiligingswet valt én wat de omvang van jouw organisatie is (groot, middelgroot, klein), kan met behulp van stroomschema bijlage 1 en stroomschema bijlage 2 worden vastgesteld of jouw organisatie kwalificeert als een essentiële entiteit óf een belangrijke entiteit. Dit onderscheid is belangrijk, omdat het invloed heeft op de manier waarop toezicht wordt gehouden:



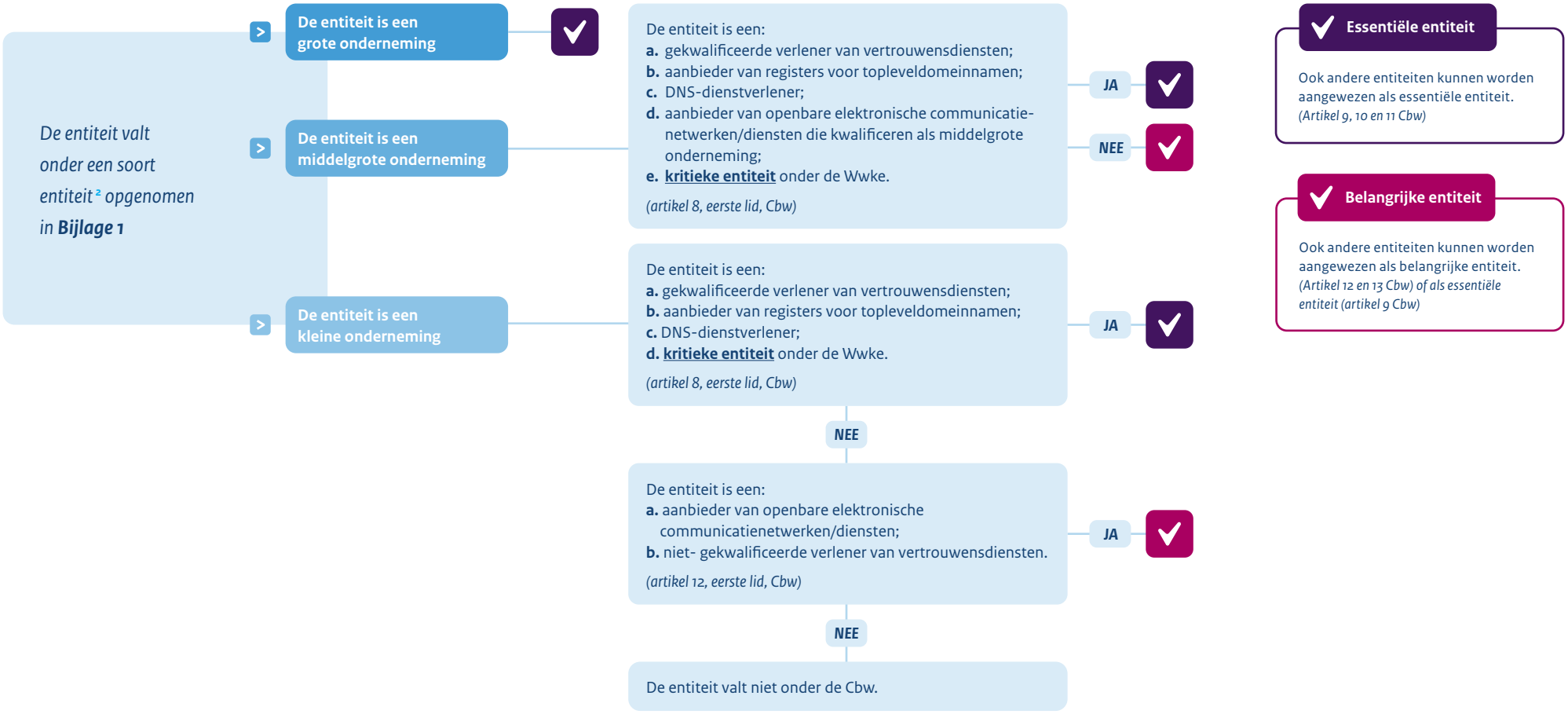
Essentiële entiteit

Essentiële entiteiten staan onder proactief toezicht: de naleving van verplichtingen wordt actief gecontroleerd, ook als er geen incidenten zijn.

Belangrijke entiteit

Belangrijke entiteiten vallen onder reactief toezicht: controles vinden vooral achteraf plaats, bijvoorbeeld naar aanleiding van signalen van niet-naleving of na een incident. Zoals in het stroomschema op de volgende pagina te zien is, zijn ook hier enkele uitzonderingen van toepassing.

Stroomschema: entiteit valt onder Bijlage 1 van de Cyberbeveiligingswet



2 Soort entiteit: een organisatie valt onder Bijlage 1 en/of Bijlage 2 als deze behoort tot een soort entiteit binnen een (sub)sector genoemd in de bijlagen. Bijvoorbeeld: als de organisatie actief is binnen de sector energie, in de subsector elektriciteit én als soort entiteit een elektriciteitsbedrijf is, valt de organisatie onder Bijlage 1.

Stroomschema: entiteit valt onder Bijlage 2 van de Cyberbeveiligingswet

Belangrijke entiteit

Ook andere entiteiten kunnen worden aangewezen als belangrijke entiteit. *(Artikel 12 en 13 Cbw) of als essentiële entiteit (artikel 9 Cbw)*

Essentiële entiteiten

Grote organisaties die behoren tot een van de genoemde sectoren in bijlage 1 van de Cyberbeveiligingswet kwalificeren als een essentiële entiteit.

De volgende soorten organisaties vallen ongeacht hun grootte als essentiële entiteit onder de Cyberbeveiligingswet: centrale en decentrale overheden (zie hieronder voor een nadere toelichting), gekwalificeerde vertrouwensdienstverleners, aanbieders van registers voor topleveldomeinnamen en verleners van DNS-diensten.

Ook middelgrote organisaties, die aanbieder van openbare elektronische communicatienetwerken of -diensten zijn, zijn essentiële entiteiten.

Belangrijke entiteiten

Middelgrote organisaties die behoren tot een van de genoemde sectoren in bijlage 1 van de Cyberbeveiligingswet (en niet op grond van het bovenstaande een essentiële entiteit zijn) kwalificeren als een belangrijke entiteit. Ook middelgrote en grote organisaties die behoren tot een van de genoemde sectoren in bijlage 2 van de Cyberbeveiligingswet kwalificeren als een belangrijke entiteit. Aanbieders van openbare elektronische communicatienetwerken of -diensten en verleners van vertrouwensdiensten, die een kleine of micro organisatie zijn, zijn een belangrijke entiteit.

Overheidsinstanties

Binnen de subsector centrale overheid zijn ministeries, inclusief daartoe behorende dienstonderdelen, en zelfstandige bestuursorganen, essentiële entiteiten. Binnen de subsector decentrale overheid zijn de provincies, gemeenten en waterschappen, en openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties in de zin van de Wet gemeenschappelijke regelingen, essentiële entiteiten. Voor deze instanties geldt dat hun grootte niet relevant is voor de kwalificatie als essentiële entiteit.
Ook geldt dat zij uiteraard moeten voldoen aan de definitie van overheidsinstantie uit artikel 1 van de Cyberbeveiligingswet.

Overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, zijn uitgesloten van het toepassingsgebied van de Cyberbeveiligingswet. Het gaat hierbij in ieder geval om het ministerie van Defensie, de inlichtingen- en veiligheidsdiensten, het openbaar ministerie, de politie en de veiligheidsregio's.

Onderwijs

De Minister van Onderwijs, Cultuur en Wetenschap maakt gebruik van de mogelijkheid om hoger onderwijsinstellingen door een aanwijzing onder de reikwijdte van de Cyberbeveiligingswet te brengen.

2

Wat betekent de Cyberbeveiligingswet voor jouw organisatie?

Wat betekent de Cyberbeveiligingswet voor jouw organisatie?

Organisaties die vallen onder de Cyberbeveiligingswet (NIS2-richtlijn), krijgen onder andere te maken met:

Registratieplicht

Organisaties moeten zich registeren in het nationaal register van entiteiten. Er is hiervoor een online registratievoorziening ontwikkeld. In Nederland gebeurt dat bij het Nationaal Cyber Security Centrum (NCSC) op mijn.ncsc.nl. Na registratie krijgen Cbw-organisaties toegang tot de dienstverlening van het betreffende sectorale CSIRT.

Doordat alle lidstaten van de Europese Unie over zo'n register moeten beschikken, levert dit ook een Europees beeld van het aantal entiteiten onder de NIS2-richtlijn op. Ga naar de website van het NCSC voor meer informatie over het doorlopen van een succesvolle registratie.

Zorgplicht

De zorgplicht houdt in dat organisaties passende en evenredige technische, operationele en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen. Het gaat hierbij om de netwerk- en informatiesystemen die zij gebruiken voor hun werkzaamheden of voor het verlenen van hun diensten waarvoor zij onder de Cyberbeveiligingswet vallen.

De maatregelen die organisaties in het kader van de zorgplicht moeten nemen zijn onder meer beleid voor het doen van een risicoanalyse en beveiliging van de toeleveringsketen.

Meldplicht

Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten melden aan hun Computer Security Incident Response Team (CSIRT) en de toezichthouder. In Nederland is een centraal meldpunt ingericht op mijn.ncsc.nl. In dit meldportaal kunnen organisaties in één keer melden bij hun CSIRT en toezichthouder. Na de melding van een significant incident kan bijstand worden verkregen van het CSIRT. Een incident is significant als het een ernstige verstoring van de diensten of financiële verliezen voor de organisatie veroorzaakt of kan veroorzaken óf andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. In welke specifieke gevallen hiervan sprake is, wordt nog met sectorspecifieke drempelwaarden nader uitgewerkt in ministeriële regelingen.

Bestuurlijke verantwoordelijkheid en trainingplicht voor bestuurders

Onder de Cyberbeveiligingswet wordt cyberbeveiliging niet langer gezien als een technische kwestie, maar als een onderwerp voor de gehele organisatie. Het bestuur is verantwoordelijk voor het beleid en de naleving van de wet. Zo moeten de bestuursleden van de organisaties de maatregelen in het kader van de zorgplicht goedkeuren. Om dit goed te kunnen doen, moeten zij ook een training volgen. Bekijk voor meer informatie de website van het NCSC.

Toezicht

Op de naleving van de verplichtingen uit de Cyberbeveiligingswet wordt toezicht gehouden. Hierbij wordt gekeken naar de naleving van de verplichtingen uit de Cyberbeveiligingswet, zoals de zorg- en meldplicht. Toezichts-maatregelen richten zich tot de organisatie maar kunnen in een uiterst geval ook de individuele bestuurders raken.

Welke maatregelen kan je nemen om aan de zorgplicht te voldoen?

Onder de zorgplicht vallen ten minste:

Maatregel 1 Beleid over risicoanalyse en beveiliging van informatiesystemen;

Maatregel 2 Incidentenbehandeling;

Maatregel 3 Bedrijfscontinuïteit, zoals back-upbeheer en herstelplannen, en crisisbeheer;

Maatregel 4 De beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen de entiteit en haar rechtstreekse leveranciers of dienstverleners;

Maatregel 5 Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

Maatregel 6 Beleid en procedures om de effectiviteit van maatregelen voor het beheersen van cyberbeveiligingsrisico's te beoordelen;

Maatregel 7 Basispraktijken op het gebied van cyberhygiëne en training op het gebied van cyberbeveiliging;

Maatregel 8 Beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

Maatregel 9 Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets; en

Maatregel 10 Wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Voor aanvullende normenkaders kun je kijken naar de ministeriële regelingen voor jouw sector of normenkaders, zoals ISO 27001/NEN 7510 en BIO 2.0.

Wat valt onder meldplicht?

Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten melden aan hun CSIRT en toezichthouder. In Nederland is een centraal meldpunt ingericht op mijn.ncsc.nl. In dit meldportaal kunnen organisaties in één keer melden bij hun CSIRT en toezichthouder.

Er geldt een gefaseerde meldplicht:

Significant incident

Een incident is significant als het een ernstige verstoring van de diensten of financiële verliezen voor de organisatie veroorzaakt of kan veroorzaken óf andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. In welke specifieke gevallen hiervan sprake is, wordt nog in drempelwaarden nader uitgewerkt.

3

Wat kunnen organisaties van de Rijksoverheid verwachten?

Wat kunnen organisaties van de Rijksoverheid verwachten?

De organisaties waarop de Cyberbeveiligingswet van toepassing is kunnen worden ondersteund door een Computer Security Incident Response Team (CSIRT). Het hoofddoel van een CSIRT is om snel en efficiënt te reageren op cyberincidenten, het adequaat afhandelen van een incident en het minimaliseren van schade. Het CSIRT doet dit door onder andere bijstand te verlenen bij cyberdreigingen, informeren over kwetsbaarheden en incidenten, waarschuwingen uit te geven en informatie hierover te verstrekken, en op verzoek van de organisatie diens netwerk- en informatiesystemen scannen.

De taken van het CSIRT zullen voor een groot deel van de organisaties in de praktijk worden uitgevoerd door het Nationaal Cyber Security Centrum (NCSC). Voor enkele soorten organisaties zal een ander CSIRT worden aangewezen. Het gaat naar verwachting om Z-CERT, het CERT Watermanagement (onderdeel van Het Waterschapshuis), de Informatiebeveiligingsdienst (IBD, onderdeel van VNG Realisatie B.V.) en SURFcert. Het NCSC zal in de praktijk daarnaast ook de in de Cyberbeveiligingswet opgenomen taken van het centrale contactpunt uitvoeren. Dit geldt ook voor het beheer van het nationale register van entiteiten.

Bekijk de Cyberbeveiligingswet doorverwijsboom voor een uitgebreid overzicht van de verantwoordelijke ministeries, CSIRTS en toezichthouders per sector (zie bijlage).

Hoe kunt je jouw organisatie voorbereiden?

Begin direct met het digitaal weerbaar maken van jouw organisatie:

- **Breng in kaart of jouw organisatie onder de Cbw valt.** Doe de NIS2 Zelfevaluatie NL van de RDI om te bepalen of jouw organisatie (mogelijk) onder de Cyberbeveiligingswet valt.
- **Registreer jouw organisatie op mijn ncsc.nl.** Na registratie krijgen Cbw-organisaties toegang tot de dienstverlening van het betreffende sectorale CSIRT.
- **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 richting compliance. 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.
- **Ga aan de slag met de tien zorgplichtmaatregelen.** Start tijdig met een grondige risicoanalyse om de maatregelen en vervolgstappen in kaart te brengen. Het NCSC biedt diverse adviesproducten die je hierbij ondersteunen. Bekijk de informatie op: ncsc.nl.

Kijk hier voor meer informatie over deze voorbereidende stappen.

Hoe wordt toezicht gehouden?

Essentiële entiteiten staan onder proactief toezicht: de naleving van verplichtingen wordt actief gecontroleerd, ook als er geen incidenten zijn.

Belangrijke entiteiten vallen onder reactief toezicht: controles vinden achteraf plaats, bijvoorbeeld naar aanleiding van signalen van niet-naleving of na een incident.

Op entiteiten die domeinnaamregistratiediensten verlenen en bestuursleden van essentiële entiteiten en belangrijke entiteiten wordt ook toezicht gehouden. Welk handhavings-instrument door de toezichthouder kan worden ingezet, staat hiernaast in een overzicht.

Handhavingsinstrumentarium

Essentiële entiteiten
- Controlefunctionaris
- Beveiligingsscan
- Beveiligingsaudit
- Openbaarmaking overtreding
- Bindende aanwijzing
- Last onder bestuursdwang
- Last onder dwangsom
- Verzoek tot tijdelijke schorsing certificering of vergunning
- Verzoek tot tijdelijke schorsing bestuurslid
- Bestuurlijke boete

Belangrijke entiteiten
- Beveiligingsscan
- Beveiligingsaudit
- Openbaarmaking overtreding
- Bindende aanwijzing
- Last onder bestuursdwang
- Last onder dwangsom
- Bestuurlijke boete

Entiteiten die domeinnaamregistratie-diensten verlenen
- Bindende aanwijzing
- Last onder bestuursdwang
- Last onder dwangsom
- Bestuurlijke boete

Bestuursleden van essentiële entiteiten en belangrijke entiteiten
- Last onder dwangsom
- Bestuurlijke boete

4

Valt jouw organisatie onder de Cyberbeveiligingswet?

Rechten en verplichtingen per 17 oktober 2024

De NIS2-richtlijn is sinds 17 oktober 2024 geldig in de Europese Unie. In Nederland is het niet gelukt om deze EU-richtlijn op tijd om te zetten in nationale wetgeving. De verwachting is dat de Cyberbeveiligingswet in het tweede kwartaal van 2026 in werking treedt.

Situatie vanaf 17 oktober 2024

Tussen 17 oktober 2024 en de datum van inwerkingtreding van de Cyberbeveiligingswet gelden de plichten, zoals de zorgplicht, meldplicht en registratieplicht, nog niet. Wel hebben organisaties, die van rechtswege vallen onder de NIS2-richtlijn, in die periode enkele rechten door de rechtstreekse werking van een aantal bepalingen uit de richtlijn, zoals het ontvangen van bijstand bij een cyberincident door een Computer Security Incident Response Team (CSIRT).

Taakuitvoering door CSIRT vanaf 17 oktober 2024

Voor de organisaties die onder de hierboven genoemde rechtstreekse werking vallen en dus recht hebben op de CSIRT dienstverlening zal deze taak door het NCSC, Z-CERT en CSIRT-DSP worden ingevuld. Het gaat dan om de volgende CSIRT taken:

- Op verzoek verlenen van bijstand met betrekking tot het realtime of bijna-realtime monitoren van netwerk- en informatiesystemen van bovenbedoelde organisaties.
- Verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie aan genoemde organisaties over cyberdreigingen, kwetsbaarheden en incidenten.
- Reageren op incidenten en verlenen van bijstand aan deze organisaties.
- Op verzoek van de organisatie proactief scannen van de netwerk- en informatie-systemen van de organisatie om kwetsbaarheden.
- Verwerken van vrijwillige meldingen van genoemde organisaties van incidenten, bijna-incidenten en cyberdreigingen.

Registratie in de periode tot inwerkingtreding van de wet

Organisaties kunnen zich vanaf 17 oktober 2024 vrijwillig registreren bij het NCSC. Deze registratie is pas verplicht als in Nederland de Cyberbeveiligingswet in werking treedt (naar verwachting tweede kwartaal 2026).

5

Doorverwijsboom Cyberbeveiligingswet

Doorverwijsboom Cyberbeveiligingswet

Organisaties die onder de Cyberbeveiligingswet vallen, hebben verschillende instanties waar zij terecht kunnen met vragen, meldingen of incidenten. Hieronder een overzicht.

Bijlage 1

Sectoren	Subsector en/of soort entiteit	*Vakdepartement* *Voor sectorspecifieke vragen, aanwijzingen etc.*	*CSIRT* *Voor ondersteuning bij incidenten etc.*	*Toezichthouder* *Voor (de wijze van) toezicht op de naleving van de wet*
Energie	Elektriciteit; stadsverwarming en -koeling; aardgas; waterstof; aardolie.	KGG	NCSC	RDI
Vervoer	Lucht (commerciële luchtvaartmaatschappijen; luchthavens; luchtverkeersleiding), spoor (infrastructuur beheerders, spoorweg ondernemingen); water (vervoersmaatschappijen; havens; verkeersbegeleidingsdiensten voor schepen); weg (wegenautoriteiten; exploitanten van intelligente vervoerssystemen).	IenW	NCSC	ILT
Bankwezen	Kredietinstellingen.	FIN	NCSC	DNB
Infrastructuur financiële markt	Handelsplatformen; centrale tegenpartijen.	FIN	NCSC	AFM

Sectoren	Subsector en/of soort entiteit	*Vakdepartement* *Voor sectorspecifieke vragen, aanwijzingen etc.*	*CSIRT* *Voor ondersteuning bij incidenten etc.*	*Toezichthouder* *Voor (de wijze van) toezicht op de naleving van de wet*
Gezondheidszorg	Zorgaanbieders; laboratoria; onderzoek en ontwikkeling van geneesmiddelen; vervaardiging van farmaceutische basisproducten en -preparaten; vervaardiging van medische hulpmiddelen die van cruciaal belang zijn bij noodsituaties op het gebied van volksgezondheid.	VWS	Z-CERT	IGJ
Drinkwater	Leveranciers en distributeurs van water uit drinkwaterleidingen dat bestemd is voor menselijke consumptie.	IenW	NCSC	ILT
	Leveranciers en distributeurs van verpakt water dat bestemd is voor menselijke consumptie.	IenW	NCSC	NVWA
Afvalwater	Ondernemingen die industrieel afvalwater opvangen of lozen.	IenW	NCSC	ILT
	Waterschappen (huishoudelijk afvalwater).	IenW	CERT-WM	ILT
Digitale infrastructuur	DNS-dienstverleners; verleners van vertrouwensdiensten; register voor topleveldomeinnamen; aanbieders van openbare elektronische communicatienetwerken en communicatiediensten; internetknooppunten; cloudcomputingdiensten; datacentrumdiensten; netwerken voor de levering van inhoud.	EZ	NCSC	RDI
Beheer van ICT-diensten	Aanbieders van beheerde diensten en aanbieders van beheerde beveiligingsdiensten.	EZ	NCSC	RDI

Sectoren	Subsector en/of soort entiteit	*Vakdepartement* *Voor sectorspecifieke vragen, aanwijzingen etc.*	*CSIRT* *Voor ondersteuning bij incidenten etc.*	*Toezichthouder* *Voor (de wijze van) toezicht op de naleving van de wet*
Overheid[1]	Ministeries en zelfstandige bestuursorganen op het niveau van de centrale overheid, voor zover zij kwalificeren als overheidsinstantie.	BZK	NCSC	RDI
	Provincies.	BZK	NCSC	RDI
	Gemeenten.	BZK	IBD	RDI
	Waterschappen.	IenW	CERT-WM	ILT
	Gemeenschappelijke regelingen, voor zover zij kwalificeren als overheidsinstantie.	BZK	ntb*	RDI
Ruimtevaart	Infrastructuur op de grond.	EZ	NCSC	RDI
	Satellietnavigatie.	IenW	NCSC	RDI

**Dit is afhankelijk van de gemeenschappelijke regeling die het betreft. BZK maakt hier een nadere uitwerking van.

Bijlage 2

Sectoren	Subsector en/of soort entiteit	*Vakdepartement* *Voor sectorspecifieke vragen, aanwijzingen etc.*	*CSIRT* *Voor ondersteuning bij incidenten etc.*	*Toezichthouder* *Voor (de wijze van) toezicht op de naleving van de wet*
Post- en koeriersdiensten	Aanbieders van postdiensten, inclusief aanbieders van koeriersdiensten, voor zover zij ten minste één van de stappen in de postbestelketen verzorgen.	EZ	NCSC	RDI
Afvalstoffen-beheer	Ondernemingen die handelingen in het kader van afvalstoffenbeheer uitvoeren, met uitzondering van ondernemingen waarvoor afvalstoffenbeheer niet de voornaamste economische activiteit is.	IenW	NCSC	ILT
Chemische stoffen	Vervaardiging, productie en distributie.	IenW	NCSC	ILT
Levensmiddelen	Productie, verwerking en distributie.	LVVN	NCSC	NVWA
Vervaardiging	Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in de vitrodiagnostiek.	VWS	Z-CERT	IGJ
	Vervaardiging van informaticaproducten en van elektronische en optische producten; vervaardiging van elektrische apparatuur; vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd; vervaardiging van motorvoertuigen, aanhangers en opleggers; vervaardiging van andere transportmiddelen.	EZ	NCSC	RDI

Sectoren	Subsector en/of soort entiteit	*Vakdepartement* *Voor sectorspecifieke vragen, aanwijzingen etc.*	*CSIRT* *Voor ondersteuning bij incidenten etc.*	*Toezichthouder* *Voor (de wijze van) toezicht op de naleving van de wet*
Digitale aanbieders	Online marktplaatsen, online zoekmachines en social netwerken.	EZ	NCSC	RDI
Onderzoek	Onderzoeksinstellingen (met uitzondering van onderwijsinstellingen).	ntb**	ntb**	ntb*
Onderwijs	Hbo- en wo-instellingen.	OCW	ntb	ntb

NB. Kritieke entiteiten onder de **Wet weerbaarheid kritieke entiteiten**, worden niet specifiek in dit overzicht genoemd maar moeten ook aan de Cyberbeveiligingswet voldoen.

Organisaties die onder de Cyberbeveiligingswet vallen, moeten maatregelen nemen om hun netwerk- en informatiesystemen tegen incidenten te beschermen. Hetzelfde geldt voor de fysieke omgeving waarin de systemen zich bevinden. Onder de zorgplicht vallen ten minste de volgende tien maatregelen.

10 Zorgplichtmaatregelen

**Het onderwerp van het onderzoek bepaalt welk ministerie of welke toezichthouder verantwoordelijk is.

februari 2026

Medegefinancierd door de Europese Unie