N  Network

I  Information

S  Security

Cyberbeveiligingswet

Informatiebrochure

augustus 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 is de NIS2-richtlijn geïmplementeerd in de Cyberbeveiligingswet. Met de inwerkingtreding van de Cyberbeveiligingswet is de Wet beveiliging netwerk- en informatiesystemen (Wbni) vervangen. Tegelijkertijd is ook de Critical Entities Resilience Directive (CER-richtlijn) geïmplementeerd in de Wet weerbaarheid kritieke entiteiten (Wwke). Beide wetten zijn op 15 augustus 2026 in werking getreden.

De Cyberbeveiligingswet heeft gevolgen voor organisaties die onder de wet vallen. Daarbij gaat het om veel meer organisaties dan voorheen onder de Wbni vielen. Voor organisaties die onder de Cyberbeveiligingswet vallen, gelden onder meer een registratieplicht, zorgplicht, meldplicht en bestuurlijke verantwoordelijkheid. Ook is het toezicht op de naleving van deze 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

Inhoud

Disclaimer

Deze informatiebrochure bevat basisinformatie over de Cyberbeveiligingswet. Aan de inhoud van deze informatiebrochure kunnen geen rechten worden ontleend. Deze informatiebrochure is niet juridisch bindend. Organisaties zijn zelf verantwoordelijk voor het voldoen aan de eisen in de Cyberbeveiligingswet. Deze informatiebrochure is voor het laatst geactualiseerd in augustus 2026 en wordt indien nodig hierna opnieuw geactualiseerd.

1.

Valt jouw organisatie onder de Cyberbeveiligingswet?

Valt jouw organisatie onder de Cyberbeveiligingswet?

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

Zelfevaluatietool

Organisaties kunnen met de zelfevaluatietool beoordelen of ze onder de Cyberbeveiligingswet vallen en, indien dat het geval is, of zij kwalificeren als essentiële entiteit of belangrijke entiteit. Daarnaast kunnen onderstaande stappen worden doorlopen om te bepalen of een organisatie onder de Cyberbeveiligingswet valt.

Stap 1: Controleer of jouw organisatie behoort tot een van onderstaande 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.

Organisaties die domeinnaamregistratiediensten verlenen staan niet vermeld in bijlage 1 of 2 van de Cyberbeveiligingswet. Op deze organisaties zijn niet alle verplichtingen uit de Cyberbeveiligingswet van toepassing.

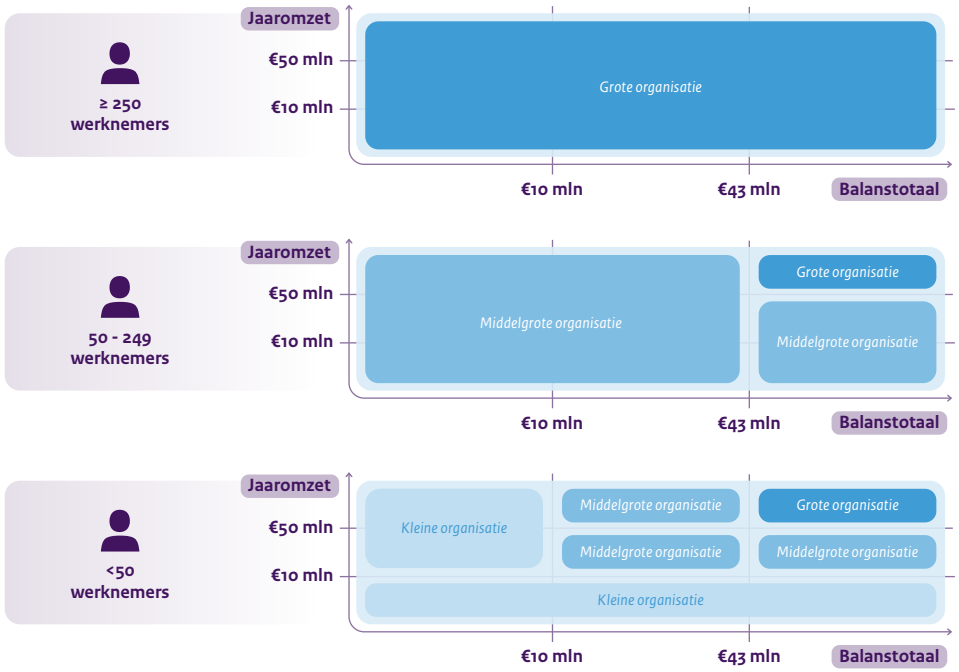
Stap 2: Controleer of jouw organisatie voldoet aan de omvangscriteria

Nadat is vastgesteld dat jouw organisatie behoort tot een soort entiteit die is opgenomen in bijlage 1 of bijlage 2 van de Cyberbeveiligingswet, moet worden beoordeeld of wordt voldaan aan de omvangscriteria. Daarbij wordt onder meer gekeken naar het aantal medewerkers, de jaaromzet en het balanstotaal.

Voor sommige organisaties gelden deze omvangscriteria niet. Zij vallen onder de Cyberbeveiligingswet, ongeacht hun omvang. Dit geldt voor: aanbieders van openbare elektronische communicatienetwerken, aanbieders van openbare elektronische communicatiediensten, (gekwalificeerde) verleners van vertrouwensdiensten, aanbieders van registers voor topleveldomeinnamen, DNS-dienstverleners en overheidsorganisaties, en voor verleners van domeinnaamregistratiediensten.

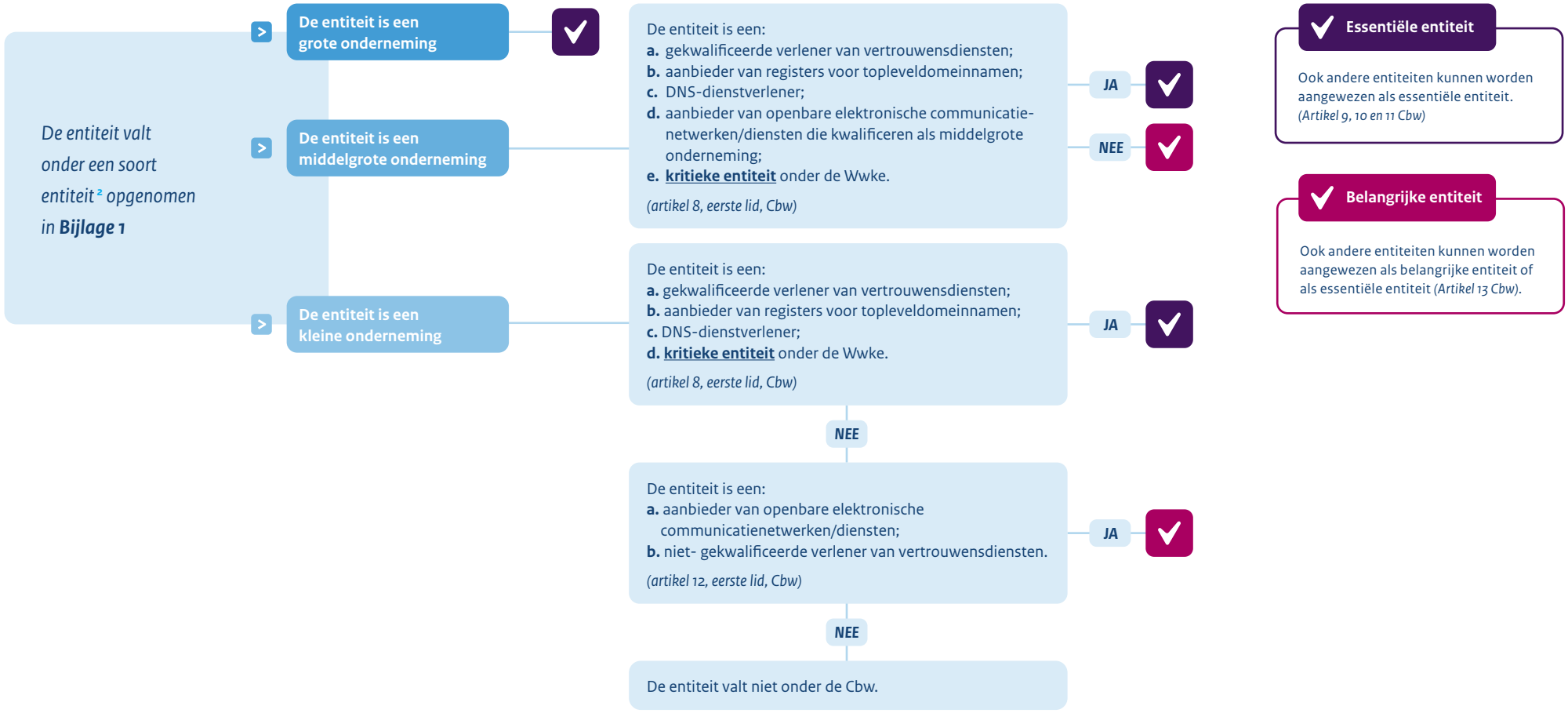
Stap 3: Bepaal aan de hand van het stroomschema of jouw organisatie een essentiële entiteit óf een belangrijke entiteit is

Wanneer duidelijk is dat jouw organisatie onder bijlage 1 of bijlage 2 van de Cyberbeveiligingswet valt én wat de omvang van jouw organisatie is, kan met behulp van de stroomschema's worden bepaald of er sprake is van een essentiële entiteit óf een belangrijke entiteit. Dit onderscheid is belangrijk, omdat het invloed heeft op de manier waarop toezicht wordt gehouden:



- **Essentiële entiteiten staan onder proactief toezicht:** de naleving van verplichtigen wordt actief gecontroleerd, ook als er geen aanwijzingen voor een mogelijke overtreding zijn.
- **Belangrijke entiteiten vallen onder reactief toezicht:** controles vinden achteraf plaats, naar aanleiding van bijvoorbeeld aanwijzingen of informatie over een mogelijke overtreding. 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 of als essentiële entiteit *(Artikel 13 Cbw)*.

Let op

Voor sommige soorten organisaties gelden uitzonderingen op de hoofdregels. Dit geldt bijvoorbeeld voor overheidsinstanties, bekostigde hogescholen en universiteiten, aanbieders van elektronische communicatienetwerken en bepaalde digitale dienstverleners. In onderstaande paragrafen worden deze uitzonderingen toegelicht.

Essentiële entiteiten

Grote organisaties die behoren tot een van de sectoren, genoemd in bijlage 1 van de Cyberbeveiligingswet, kwalificeren als essentiële entiteit. De volgende organisaties kwalificeren, ongeacht hun omvang, 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 aanbieders van openbare elektronische communicatienetwerken of -diensten, die middelgroot zijn, zijn essentiële entiteiten.

Belangrijke entiteiten

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

Relatie met de Wet weerbaarheid kritieke entiteiten

Organisaties die door de vakminister worden aangewezen als kritieke entiteit op grond van de Wet weerbaarheid kritieke entiteiten, kwalificeren van rechtswege als essentiële entiteit onder de Cyberbeveiligingswet. Voor deze organisaties gelden daarom ook de verplichtingen uit de Cyberbeveiligingswet, zoals de registratie-, zorg- en meldplicht.

Overheidsinstanties

Binnen de overheid vallen verschillende organisaties onder de Cyberbeveiligingswet als essentiële entiteit. Het gaat onder meer om ministeries (inclusief daaronder behorende dienstonderdelen), zelfstandige bestuursorganen die als overheidsinstantie kwalificeren, provincies, gemeenten, waterschappen en organisaties die zijn opgericht op grond van de Wet gemeenschappelijke regelingen.

Voor deze organisaties gelden geen omvangscriteria: ook kleinere organisaties kunnen onder de Cyberbeveiligingswet vallen. Wel moeten zij voldoen aan de definitie van overheidsinstantie zoals opgenomen in artikel 1 van de Cyberbeveiligingswet.

Van de Cyberbeveiligingswet zijn overheidsinstanties uitgezonderd die hun werkzaamheden hoofdzakelijk uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving. Hieronder vallen onder meer 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 heeft voor bekostigde hogescholen en universiteiten gebruikgemaakt van de mogelijkheid in de Cyberbeveiligingswet om hoger-onderwijsinstellingen aan te wijzen als belangrijke entiteit. Met de ministeriële regeling waarin deze aanwijzing is vastgelegd, vallen deze instellingen onder de Cyberbeveiligingswet.

Complexe bedrijfsmodellen

Voor organisaties met een complexe bedrijfsstructuur, zoals organisaties met vestigingen in meerdere EU-landen, kan het vaststellen of de Cyberbeveiligingswet van toepassing is, ingewikkeld zijn. In sommige gevallen is niet de Nederlandse Cyberbeveiligingswet van toepassing, maar de nationale wetgeving van een andere EU-lidstaat. De Handreiking complexe bedrijfsmodellen biedt ondersteuning bij het bepalen welke wetgeving op de organisatie van toepassing is.

2.

Wat betekent de Cyberbeveiligingswet voor jouw organisatie?

Wat betekent de Cyberbeveiligingswet voor jouw organisatie?

Organisaties die vallen onder de Cyberbeveiligingswet, krijgen onder andere te maken met:

Registratieplicht

Voor organisaties die onder de Cyberbeveiligingswet vallen, geldt sinds de inwerkingtreding van de wet een registratieplicht. Organisaties registreren zich via MijnNCSC bij het Nationaal Cyber Security Centrum (NCSC). Organisaties krijgen onder meer toegang tot de dienstverlening van het voor hun sector aangewezen CSIRT. Bekijk de website van het NCSC voor meer informatie over het doorlopen van een succesvolle registratie.

Zorgplicht

De zorgplicht houdt in dat essentiële entiteiten en belangrijke entiteiten 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. Zie op pagina 14 een overzicht van de maatregelen die organisaties in het kader van de zorgplicht moeten nemen.

Meldplicht

Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten melden aan hun Computer Security Incident Response Team (CSIRT) en de toezichthouder. Voor het doen van deze meldingen is een centraal meldportaal ingericht op MijnNCSC. 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 de ministeriële regelingen van voor sectoren verantwoordelijke ministers zijn per sector drempelwaarden opgenomen om te bepalen wanneer er sprake is van een significant incident. Organisaties doen er daarom goed aan de ministeriële regeling voor hun sector te raadplegen. Bekijk het overzicht van de ministeriële regelingen.

Bestuurlijke verantwoordelijkheid en trainingsplicht voor bestuurders

De Cyberbeveiligingswet bevat ook enkele verplichtingen voor het bestuur van een essentiële entiteit of belangrijke entiteit. Dat bestuur moet namelijk de maatregelen in het kader van de zorgplicht van de entiteit goedkeuren en toezien op de uitvoering van die maatregelen. Daarnaast moeten de leden van het bestuur een training volgen om zo kennis en vaardigheden te verwerven om bijvoorbeeld de gevolgen van risico's en risicobeheersmaatregelen te kunnen beoordelen.

Toezicht

Op de naleving van de verplichtingen uit de Cyberbeveiligingswet door een organisatie, zoals de zorg- en de meldplicht, wordt toezicht gehouden. In geval van overtredingen zullen handhavingsmaatregelen hoofdzakelijk de organisatie betreffen, maar in bepaalde gevallen (bijvoorbeeld bovengenoemde trainingsplicht) ook de individuele bestuurders raken.

Welke maatregelen moet een organisatie nemen om aan de zorgplicht te voldoen?

De Cyberbeveiligingswet schrijft voor dat organisaties in ieder geval maatregelen moeten treffen op de volgende gebieden:

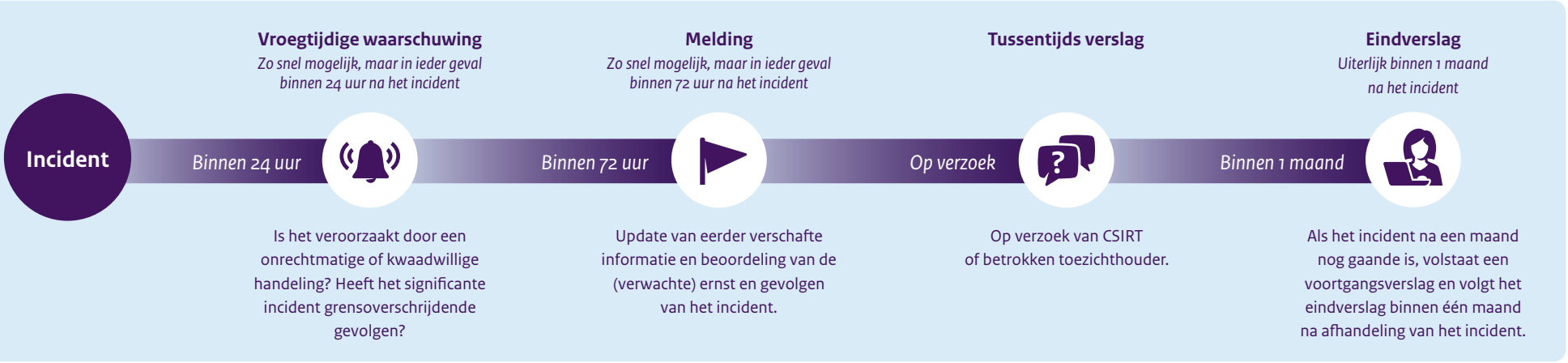
Maatregel 1 Beleid over risicoanalyse en beveiliging van netwerk- en informatiesystemen;
Maatregel 2 Incidentenbehandeling;
Maatregel 3 Bedrijfscontinuïteit, zoals back-upbeheer en herstelplannen, en crisisbeheer;
Maatregel 4 Beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten ten aanzien van de relaties met rechtstreekse leveranciers en dienstverleners;
Maatregel 5 Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, waaronder 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 opleiding op het gebied van cyberbeveiliging;
Maatregel 8 Beleid en procedures voor het gebruik van cryptografie en, waar aangewezen, encryptie;
Maatregel 9 Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets;
Maatregel 10 Waar passend, het gebruik van multifactorauthenticatie- of continue authenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de organisatie.

Deze zorgplichtmaatregelen zijn verder uitgewerkt in het Cyberbeveiligingsbesluit. Daarnaast zijn voor verschillende sectoren in ministeriële regelingen sectorspecifieke voorschriften vastgesteld.

Wat valt onder meldplicht?

Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten melden aan hun CSIRT en toezichthouder. Voor het doen van deze meldingen is een centraal meldportaal ingericht op MijnNCSC. 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 de ministeriële regelingen van voor sectoren verantwoordelijke vakministers zijn per sector drempelwaarden opgenomen om te bepalen wanneer een incident significant is. Deze drempelwaarden kunnen dus verschillen per sector.

Raadpleeg daarom de ministeriële regeling die voor de eigen sector van toepassing is.

3.

Wat kunnen organisaties van de Rijksoverheid verwachten?

Wat kunnen organisaties van de Rijksoverheid verwachten?

De organisaties die onder de Cyberbeveiligingswet vallen, 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 onder meer door bijstand te verlenen bij cyberdreigingen en -incidenten, en door organisaties te waarschuwen voor en informatie te verstrekken over dreigingen, kwetsbaarheden en incidenten. Daarnaast kan het CSIRT bijvoorbeeld ook op verzoek van een organisatie netwerk- en informatiesystemen van die organisatie scannen. Vanwege hun registratie bij het NCSC kunnen organisaties gebruik maken van de dienstverlening van het voor hun sector aangewezen CSIRT.

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 sectoren of soorten organisaties (bijvoorbeeld waterschappen, sector gezondheidszorg) zal een andere instantie als CSIRT worden aangewezen. Het NCSC voert daarnaast de in de Cyberbeveiligingswet opgenomen taken van het centrale contactpunt uit. Ook beheert het NCSC het nationale register van entiteiten.

Bekijk de Cyberbeveiligingswet doorverwijsboom voor een overzicht van de verantwoordelijke ministeries, CSIRTS en toezichthouders per sector.

Hoe kan jouw organisatie voldoen aan de Cyberbeveiligingswet?

Ga aan de slag met het voldoen aan de Cyberbeveiligingswet en het digitaal weerbaar maken van jouw organisatie:

- Breng in kaart of jouw organisatie onder de Cyberbeveiligingswet valt, bijvoorbeeld aan de hand van de NIS2 Zelfevaluatie NL van de RDI.
- Registreer jouw organisatie via MijnNCSC. Hierdoor krijgen organisaties onder meer toegang tot de dienstverlening van het voor hun sector aangewezen CSIRT.
- Beoordeel jouw cybersecuritymaatregelen en identificeer jouw verbeterpunten. Het Cbw Control Framework, ontwikkeld door de Auditdienst Rijk en NOREA, helpt IT-verantwoordelijken om verbeterpunten, uitgaand van de verplichtingen in 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 in de Cyberbeveiligingswet en de daaronder vallende lagere regelgeving.
- Ga aan de slag met de in de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en de sectorale ministeriële regeling vereiste zorgplichtmaatregelen. Voer een grondige risicoanalyse uit om de vereiste maatregelen en vervolgstappen in kaart te brengen. Het NCSC biedt diverse adviesproducten die je hierbij ondersteunen.

Lees meer over deze stappen en de beschikbare hulpmiddelen op de website van het NCSC.

Hoe wordt toezicht gehouden?

De toezichthouder controleert of organisaties voldoen aan de verplichtingen uit de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en de sectorale ministeriële regelingen.

Voor essentiële entiteiten geldt proactief toezicht. Dit betekent dat de toezichthouder actief kan controleren of aan de wettelijke verplichtingen wordt voldaan, ook als er geen aanwijzingen zijn voor een mogelijke overtreding.

Voor belangrijke entiteiten geldt reactief toezicht. De toezichthouder treedt in beginsel pas op als daar aanleiding voor is, bijvoorbeeld na een incident, een melding of andere aanwijzingen voor een mogelijke overtreding.

Voor bepaalde verplichtingen, zoals de verplichte training van bestuurders, ziet de toezichthouder toe op de naleving door de individuele leden van het bestuur. Daarnaast wordt toezicht gehouden op de naleving van de verplichtingen die gelden voor aanbieders van domeinnaamregistratiediensten.

Hieronder is per categorie weergegeven welke handhavingsinstrumenten een toezichthouder kan inzetten.

Handhavingsinstrumentarium

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

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

Entiteiten die domeinnaamregistratiediensten verlenen
- Bindende aanwijzing
- Last onder dwangsom
- Bestuurlijke boete

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

4.

Meer weten?

Meer weten?

De Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten zijn sinds 15 augustus 2026 van kracht. Organisaties die onder de Cyberbeveiligingswet vallen, zijn zelf verantwoordelijk voor het naleven van de hierin opgenomen wettelijke verplichtingen. Meer informatie is te vinden op de website van de NCTV, het NCSC en de ministeries.

augustus 2026

Medegefinancierd door
de Europese Unie