N  Network

I  Information

S  Security

Handreiking voor organisaties met complexe bedrijfsmodellen

Cyberbeveiligingswet

NIS2-richtlijn

november 2025

Inhoudsopgave

Disclaimer

Deze handreiking bevat aandachtspunten om het toepassingsbereik van de Cyberbeveiligingswet te verduidelijken.

1. *Aan de inhoud van deze handreiking kunnen geen rechten worden ontleend.*
2. *Deze handreiking is niet juridisch bindend. Organisaties zijn zelf verantwoordelijk voor de beoordeling of zij als een essentiële entiteit óf een belangrijke entiteit onder het toepassingsbereik van de Cyberbeveiligingswet vallen.*
3. *Deze handreiking is opgesteld in oktober 2025 en wordt indien nodig geactualiseerd.*

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 door middel van de Cyberbeveiligingswet. Organisaties die onder deze wet vallen, krijgen onder andere te maken met een registratieplicht, zorgplicht, meldplicht en toezicht.

Voor wie is deze handreiking bedoeld?

Bij de Cyberbeveiligingswet vallen veel organisaties van rechtswege onder de wet. Deze zijn zelf verantwoordelijk om te bepalen of zij onder deze wet vallen, hiervoor kunnen ze onder andere gebruik maken van de zelfevaluatietool van de RDI.

Voor organisaties met een complexe bedrijfsstructuur - zoals organisaties met meerdere vestigingen binnen Nederland, in andere Europese lidstaten of in andere landen - is het vaststellen of zij onder de Cyberbeveiligingswet vallen vaak ingewikkeld.

Deze handreiking is speciaal bedoeld voor deze organisaties. De handreiking biedt ondersteuning bij het bepalen of deze organisaties onder de Cyberbeveiligingswet vallen óf dat zij onder de nationale wetgeving van een andere Europese lidstaat vallen. Deze handreiking is niet van toepassing op aanbieders van openbare elektronische communicatienetwerken, aanbieders van openbare elektronische communicatiediensten, verleners van domeinnaamregistratiediensten en overheidsinstanties.

Hoe gebruik je deze handreiking?

Om vast te stellen of jouw organisatie onder de Cyberbeveiligingswet valt of onder de nationale wetgeving van een andere Europese lidstaat, kan het stappenplan uit hoofdstuk 1 gevolgd worden. Ter verduidelijking kun je de casussen bekijken voor praktijkvoorbeelden van verschillende soorten organisatiestructuren.

Stap 1

Bepaal of jouw organisatie een essentiële entiteit óf een belangrijke entiteit is

a. Controleer of jouw organisatie is aan te merken als een soort entiteit genoemd in Bijlage 1 of 2 van de Cyberbeveiligingswet.

b. Controleer of jouw organisatie voldoet aan de omvangcriteria.

c. Bepaal tot slot aan de hand van het stroomschema of jouw organisatie een essentiële entiteit óf een belangrijke entiteit is.

Stap 2

Bepaal onder welke nationale wetgeving jouw organisatie valt

a. Je hebt vastgesteld of jouw organisatie een essentiële of een belangrijke entiteit is.

b. Bepaal met de jurisdictietabel op pagina 12 onder welke nationale implementatie-wetgeving je valt. Als dit Nederland is, dan val je onder de Cyberbeveiligingswet.

Vijf casussen

Deze handreiking bevat vijf praktijkvoorbeelden van veelvoorkomende organisatie-structuren. Deze voorbeelden helpen organisaties beter te begrijpen in hoeverre de Cyber-beveiligingswet op hen van toepassing is. De volgende structuren worden besproken:

1. Organisatie met meerdere entiteiten, gevestigd in Nederland;
2. Organisatie met meerdere entiteiten in verschillende EU-lidstaten, met hoofdvestiging in Nederland;
3. Organisatie met meerdere entiteiten in verschillende EU-lidstaten, met hoofdvestiging in een andere EU-lidstaat;
4. Organisatie met meerdere entiteiten in zowel EU-lidstaten als landen buiten de EU, met hoofdvestiging in Nederland;
5. Organisatie met meerdere entiteiten in zowel EU-lidstaten als landen buiten de EU, met hoofdvestiging in een andere EU-lidstaat.

Definities

Voordat organisaties aan de slag kunnen met de casussen, volgt hieronder een uitleg over belangrijke begrippen en onderwerpen.

1. Definitie entiteit

Met het begrip entiteit wordt gedoeld op de definitie zoals deze is toegelicht in de Cyberbeveiligingswet:

"Een natuurlijke persoon, een rechtspersoon, een overheidsinstantie, een maatschap als bedoeld in artikel 1655 van boek 7A van het Burgerlijk Wetboek, een vennootschap onder firma als bedoeld in artikel 16 van het Wetboek van Koophandel en een commanditaire vennootschap als bedoeld in artikel 19 van het Wetboek van Koophandel, alsmede een samenwerkingsverband naar buitenlands recht die met één van deze rechtsvormen vergelijkbaar is."

2. Definitie digitale dienstverleners

Wanneer in deze handreiking wordt gesproken over digitale dienstverleners wordt daarmee gedoeld op de volgende entiteiten: DNS-dienstverleners; registers voor topleveldomeinnamen; aanbieders van cloudcomputingdiensten; aanbieders van datacentrumdiensten; aanbieders van netwerken voor de levering van inhoud; aanbieders van beheerde diensten; aanbieders van beheerde beveiligingsdiensten; aanbieders van onlinemarktplaatsen; aanbieders van onlinezoekmachines; en aanbieders van platforms voor socialenetwerkdiensten.

Hieronder vallen uitdrukkelijk niet de aanbieders van openbare elektronische communicatienetwerken, aanbieders van openbare elektronische communicatiediensten, aanbieders van internetknooppunten, verleners van vertrouwensdiensten en verleners van domeinnaamregistratiediensten.

3. Definitie hoofdvestiging

Het begrip hoofdvestiging is in de Cyberbeveiligingswet in relatie tot bovengenoemde digitale dienstverleners als volgt gedefinieerd:

"Een entiteit [...] wordt geacht haar hoofdvestiging in Nederland te hebben indien de beslissingen met betrekking tot de maatregelen voor het beheersen van cyberbeveiligingsrisico's hoofdzakelijk in Nederland worden genomen. Indien deze beslissingen niet hoofdzakelijk in Nederland of een andere lidstaat van de Europese Unie worden genomen of indien niet kan worden bepaald in welke lidstaat van de Europese Unie die beslissingen hoofdzakelijk worden genomen, wordt de hoofdvestiging geacht zich in Nederland te bevinden indien de cyberbeveiligingsactiviteiten in Nederland worden uitgevoerd. Indien de cyberbeveiligingsactiviteiten niet in Nederland of een andere lidstaat van de Europese Unie worden uitgevoerd of niet kan worden bepaald in welke lidstaat van de Europese Unie de cyberbeveiligingsactiviteiten worden uitgevoerd, wordt de hoofdvestiging geacht zich te bevinden in Nederland indien de vestiging van de betrokken entiteit in Nederland het grootste aantal werknemers in de Europese Unie heeft.[1]"

1 Let op: het gaat hier om de regeling in de Cbw ter bepaling van wat de hoofdvestiging is en niet om een hoofdvestiging zoals eventueel aangewezen in de Kamer van Koophandel.

Een entiteit die fungeert als hoofdvestiging, valt niet automatisch zelf onder de Cyberbeveiligingswet. Voor de leesbaarheid van de casussen zijn wij ervan uitgegaan dat de entiteit die fungeert als hoofdvestiging óók actief is in een sector genoemd in Bijlage 1 of 2 van de Cyberbeveiligingswet, voldoet aan de omvangscriteria en kwalificeert als een essentiële entiteit óf een belangrijke entiteit.

4. 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.

Stappenplan

Onderstaand stappenplan, bestaande uit 2 stappen, kan gevolgd worden om vast te stellen of jouw organisatie onder de Cyberbeveiligingswet valt of onder de nationale wetgeving van een andere Europese lidstaat.

Stap 1 Bepaal of jouw organisatie een essentiële entiteit óf een belangrijke entiteit is

a. Controleer of jouw organisatie is aan te merken als een soort entiteit genoemd in Bijlage 1 of 2 van de Cyberbeveiligingswet

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.

Bijlage 1

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

Bijlage 2

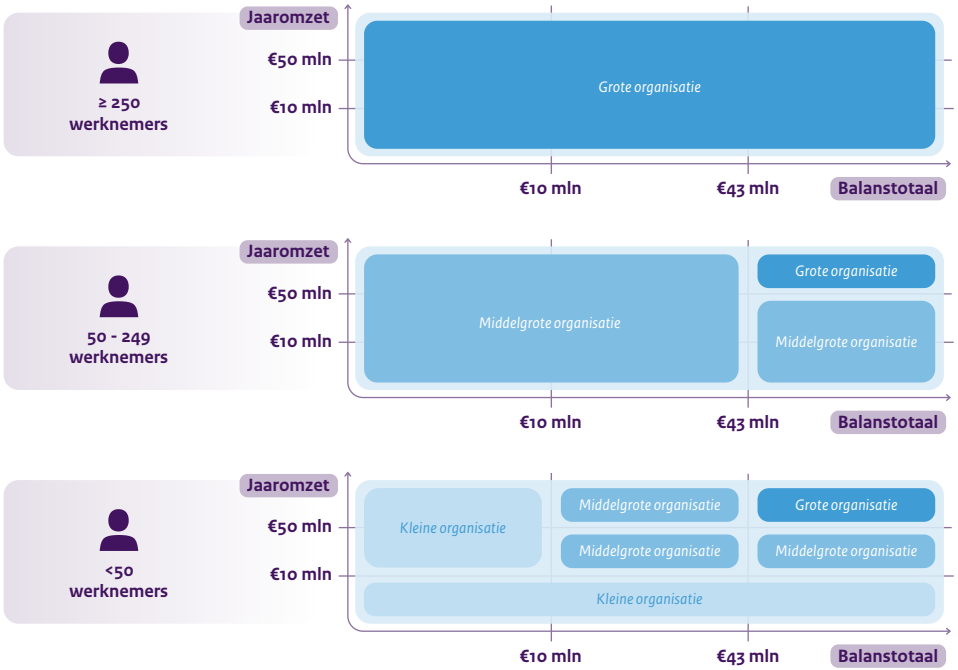
- Digitale aanbieders
- Post- en koeriersdiensten
- Afvalstoffen-beheer
- Levensmiddelen
- Chemische stoffen
- Onderzoek
- Vervaardiging

Entiteiten die **domeinnaamregistratiediensten** verlenen vallen ook onder de NIS2-richtlijn, ongeacht hun omvang, maar behoren niet tot bijlage 1 of 2, aangezien op deze categorie andersoortige verplichtingen van toepassing zijn.

Zie voor meer informatie de website van de NCTV.

b. Controleer of jouw organisatie voldoet aan de omvangscriteria[2]

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 sizecap genoemd).



2 Zie voor informatie over klein of middelgrote ondernemingen (KMO) de Aanbeveling 2003/261/EG en de gebruikersgids
Wat precies wordt verstaan onder MKB is hier te vinden.

Hierbij wordt gekeken naar onder andere het aantal medewerkers, de jaaromzet en het balanstotaal. Goed om te benoemen is dat de omvangscriteria niet altijd relevant zijn. 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 NIS2-richtlijn, ongeacht hun omvang. Zie voor meer informatie de website van de NCTV.

c. 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 het stroomschema op de volgende pagina 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:

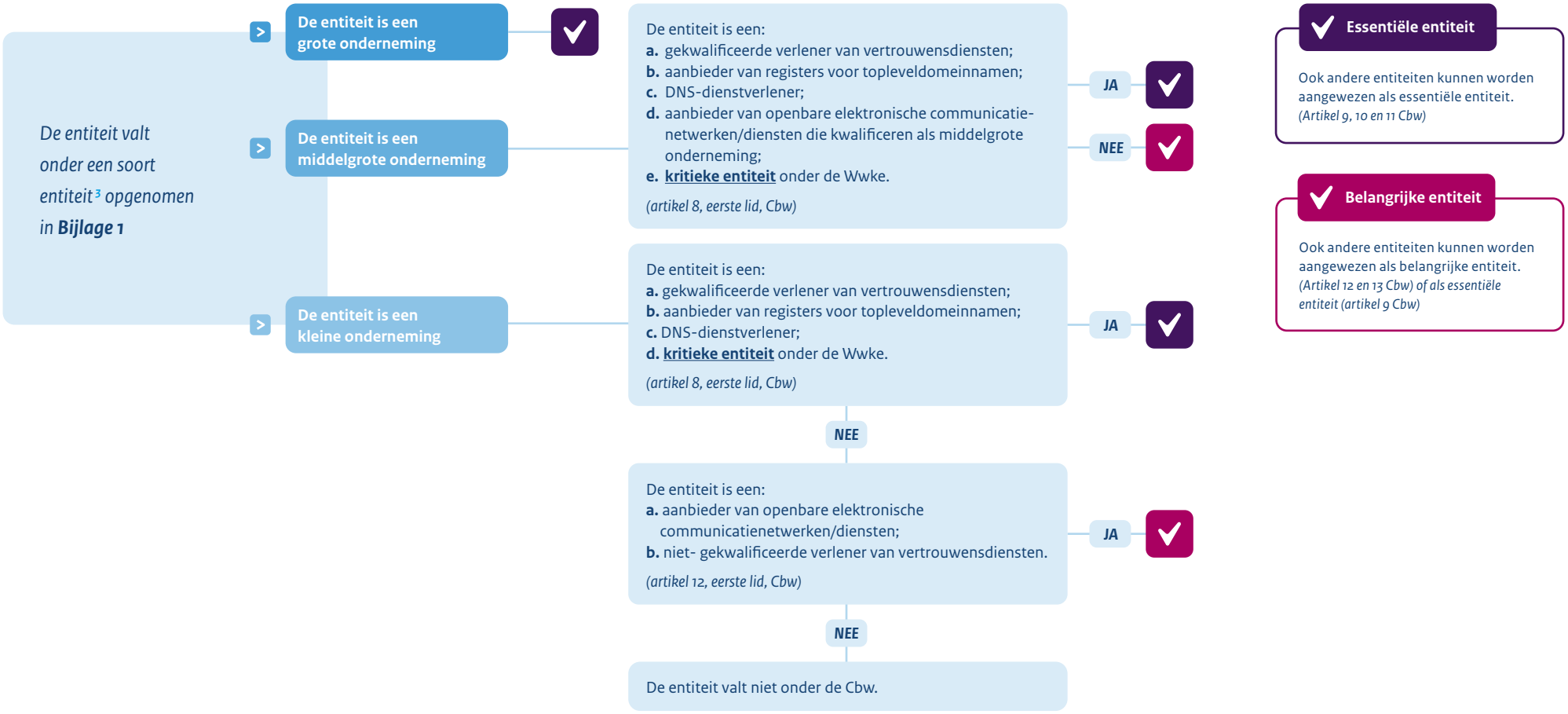
Essentiële entiteit

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



3 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)*

Stap 2 Bepaal onder welke nationale wetgeving jouw organisatie valt

Je hebt vastgesteld dat jouw organisatie kan worden aangemerkt als een essentiële entiteit óf een belangrijke entiteit. Nu kan met behulp van de jurisdictietabel op de volgende pagina bepaald worden of de organisatie onder de Cyberbeveiligingswet valt of onder de nationale implementatiewetgeving van een andere Europese lidstaat. Let op: die wetgeving kan afwijken van de Cyberbeveiligingswet.

Hoofdregel én de uitzondering op de hoofdregel

De hoofdregel én de uitzondering op de hoofdregel zijn essentieel bij het bepalen onder welke wetgeving jouw organisatie valt.

Hoofdregel

Een entiteit valt onder de Cyberbeveiligingswet wanneer:

- de vestigingsplaats zich in Nederland bevindt, én
- de entiteit diensten verleent of activiteiten verricht in Nederland óf een andere lid-staat van de EU.

Als beide voorwaarden van toepassing zijn, valt de entiteit onder de Cyberbeveiligingswet.

Uitzondering

Op de hoofdregel is de volgende uitzondering van toepassing:

Digitale dienstverleners

Digitale dienstverleners kunnen een essentiële entiteit óf een belangrijke entiteit zijn. Dit is afhankelijk van het soort entiteit en de omvang van de entiteit.
Voor digitale dienstverleners geldt de belangrijkste uitzondering, want voor deze entiteiten wordt gekeken naar de vestigingsplaats van de hoofdvestiging óf de vertegenwoordiger:

- Bevindt de hoofdvestiging of vertegenwoordiger zich in Nederland, dan valt de entiteit onder de Cyberbeveiligingswet.
- Bevindt de hoofdvestiging of de vertegenwoordiger zich buiten Nederland, dan valt de entiteit niet onder de Cyberbeveiligingswet, maar onder de nationale implementatiewetgeving van een andere Europese lidstaat.

Jurisdictietabel

Doorloop onderstaande jurisdictietabel om te bepalen onder welke nationale implementatiewetgeving jouw organisatie valt. Hierbij zijn zowel de hoofdregel als de uitzondering van pagina 11 van toepassing.

	Omschrijving entiteit		Vestiging		Activiteiten/diensten	Toepasselijkheid
1	De entiteit is een essentiële entiteit óf een belangrijke entiteit, niet zijnde een entiteit als hieronder bedoeld onder 2	*en*	De entiteit is gevestigd in Nederland	*en*	De entiteit verleent haar diensten of verricht haar activiteiten in Nederland óf een andere lidstaat van de Europese Unie	☑ **De entiteit valt onder de Cyberbeveiligingswet**
2	De entiteit is een essentiële entiteit óf een belangrijke entiteit én is: **a.** DNS-dienstverlener; **b.** register voor topleveldomeinnamen; **c.** aanbieder van cloudcomputingdiensten; **d.** aanbieder van datacentrumdiensten; **e.** aanbieder van netwerken voor de levering van inhoud; **f.** aanbieder van beheerde diensten; **g.** aanbieder van beheerde beveiligingsdiensten; **h.** aanbieder van onlinemarktplaatsen; **i.** aanbieder van onlinezoekmachines; of **j.** aanbieder van platforms voor socialenetwerkdiensten	*en*	De entiteit heeft haar hoofdvestiging[4] óf vertegenwoordiger in Nederland	*en*	De entiteit verleent haar diensten of verricht haar activiteiten in Nederland óf een andere lidstaat van de Europese Unie	☑ **De entiteit valt onder de Cyberbeveiligingswet**

Als een organisatie onder meer categorieën valt

Ten slotte is het belangrijk om te benadrukken dat meerdere jurisdictieregelingen gelijktijdig van toepassing kunnen zijn, wanneer een organisatie onder meerdere categorieën valt. Zo kan een organisatie die zowel fungeert als een internetknooppunt én een aanbieder is van cloudcomputingdiensten, onder zowel punt 1 als punt 2 uit de jurisdictietabel vallen. Dit kan betekenen dat een organisatie zowel onder de Cyberbeveiligingswet valt als onder de nationale implementatiewetgeving van een andere Europese lidstaat.

In de casussen die in het volgende hoofdstuk worden besproken, is uitgegaan van de situatie waarin een organisatie onder jurisdictie 1 of 2 valt, zoals hierboven toegelicht. In de casussen is er tevens vanuit gegaan dat een organisatie geen aanbieder van openbare elektronische communicatienetwerken, of aanbieder van openbare elektronische communicatiediensten of een verlener van domeinnaamregistratiediensten is.

4 Zie artikel 4, vijfde lid, Cbw voor de uitwerking van de term hoofdvestiging in Nederland en artikel 42, eerste lid, Cbw voor de uitwerking van de term vertegenwoordiger.

Casussen

Deze handreiking bevat vijf praktijkvoorbeelden van veelvoorkomende organisatiestructuren. Deze voorbeelden helpen organisaties beter te begrijpen in hoeverre de Cyberbeveiligingswet op hen van toepassing is. De volgende structuren worden besproken:

1. Organisatie met meerdere entiteiten, gevestigd in Nederland;
2. Organisatie met meerdere entiteiten in verschillende EU-lidstaten, met hoofdvestiging in Nederland;
3. Organisatie met meerdere entiteiten in verschillende EU-lidstaten, met hoofdvestiging in een andere EU-lidstaat;
4. Organisatie met meerdere entiteiten in zowel EU-lidstaten als landen buiten de EU, met hoofdvestiging in Nederland;
5. Organisatie met meerdere entiteiten in zowel EU-lidstaten als landen buiten de EU, met hoofdvestiging in een andere EU-lidstaat.

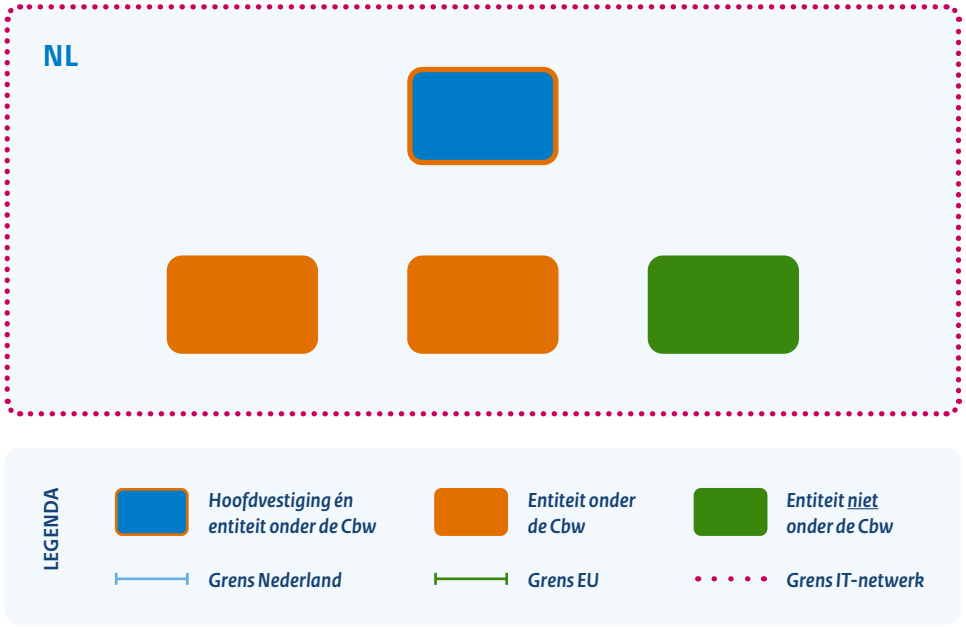
Let op

In de casussen wordt ervan uitgegaan dat er sprake is van één IT-netwerk. Als er sprake is van één IT-netwerk en één van de entiteiten valt onder de Cyberbeveiligingswet, dan dient het gehele IT-netwerk te voldoen aan de eisen die de Cyberbeveiligingswet stelt aan netwerk- en informatiesystemen. Alleen de entiteiten die vallen onder de Cyberbeveiligingswet moeten voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

Als er sprake is van afzonderlijke IT-netwerken dan moeten alleen de IT-netwerken van de entiteiten die onder de Cyberbeveiligingswet vallen aan de eisen uit de Cyberbeveiligingswet voldoen. Het hebben van een IT-netwerk is geen factor die relevant is om te bepalen of je als een essentiële entiteit óf een belangrijke entiteit onder de Cyberbeveiligingswet valt.

Casus 1

Organisatie binnen Nederland



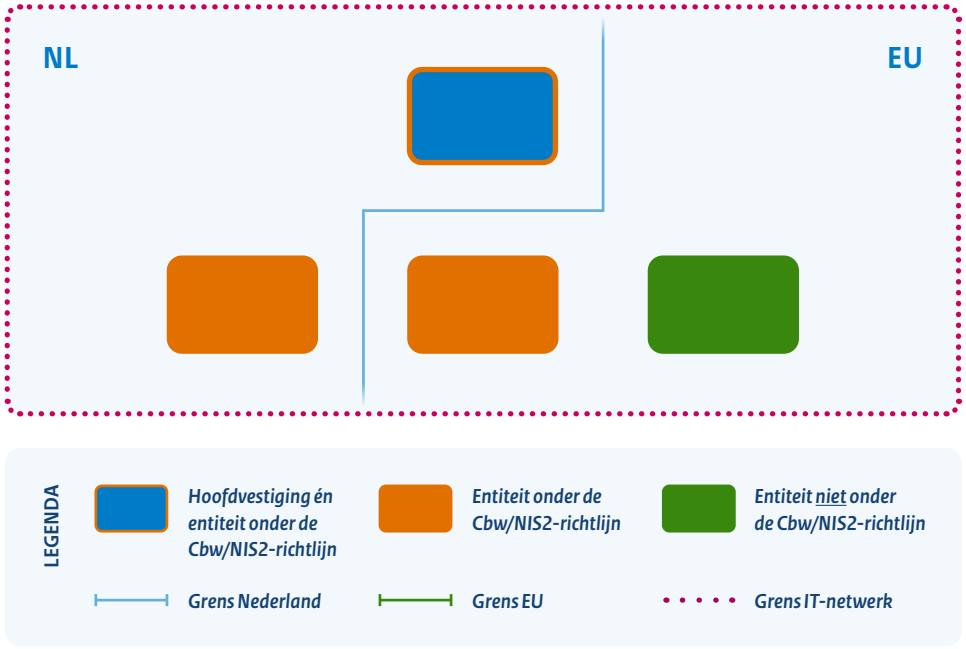
Casus 1 betreft een organisatie die bestaat uit meerdere entiteiten, die allemaal in Nederland gevestigd zijn. Drie van deze entiteiten vallen onder de Cyberbeveiligingswet: de entiteit die fungeert als hoofdvestiging en de oranje gemarkeerde entiteiten. Deze entiteiten zijn een soort entiteit opgenomen in Bijlage 1 of 2 van de Cyberbeveiligingswet, voldoen aan de omvangscriteria en kwalificeren daarmee als een essentiële entiteit óf een belangrijke entiteit. Omdat de hoofdvestiging in Nederland is gevestigd, vallen deze entiteiten - ongeacht of zij digitale dienstverleners zijn - onder de Cyberbeveiligingswet. De groen gemarkeerde entiteit valt niet onder de Cyberbeveiligingswet en hoeft daardoor niet te voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

Meldingen

In geval van een significant incident zijn uitsluitend de organisaties die onder de Cyberbeveiligingswet vallen verplicht om een melding te doen in Nederland bij het CSIRT en de bevoegde autoriteit, via het centrale meldportaal van het NCSC. Indien meerdere Cyberbeveiligingswetplichtige entiteiten binnen de organisatie door hetzelfde incident worden geraakt, moet elke Cyberbeveiligingswet entiteit afzonderlijk een melding doen in Nederland.

Casus 2

Organisatie binnen de Europese Unie - hoofdvestiging in Nederland



Casus 2 betreft een organisatie die bestaat uit meerdere entiteiten verspreid over verschillende Europese lidstaten, met de hoofdvestiging in Nederland. Naast de hoofdvestiging is ook één oranje gemarkeerde entiteit in Nederland gevestigd. Deze entiteiten zijn een soort entiteit opgenomen in Bijlage 1 of 2 van de Cyberbeveiligingswet, voldoen aan de eventuele omvangscriteria en kwalificeren daardoor als een essentiële entiteit óf een belangrijke entiteit. Nu de hoofdvestiging zich in Nederland bevindt, vallen deze entiteiten, ongeacht of zij digitale dienstverleners zijn, onder de Cyberbeveiligingswet.

In deze casus zijn er twee andere entiteiten gevestigd in een andere Europese lidstaat, namelijk Duitsland. Eén daarvan, de oranje gemarkeerde entiteit, is een soort entiteit opgenomen in Bijlage 1 of 2 van de NIS2-richtlijn, voldoet aan de eventuele omvangscriteria en kwalificeert daardoor als een essentiële entiteit óf een belangrijke entiteit. Deze entiteit valt alleen onder de Cyberbeveiligingswet als zij tevens een digitale dienstverlener is, omdat de hoofdvestiging van de organisatie in Nederland is gevestigd. Is dat niet het geval, dan valt deze entiteit onder de nationale implementatiewetgeving van de Europese lidstaat waar ze gevestigd is, in dit geval Duitsland. De groen gemarkeerde entiteit valt niet onder de Cyberbeveiligingswet en hoeft daardoor niet te voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

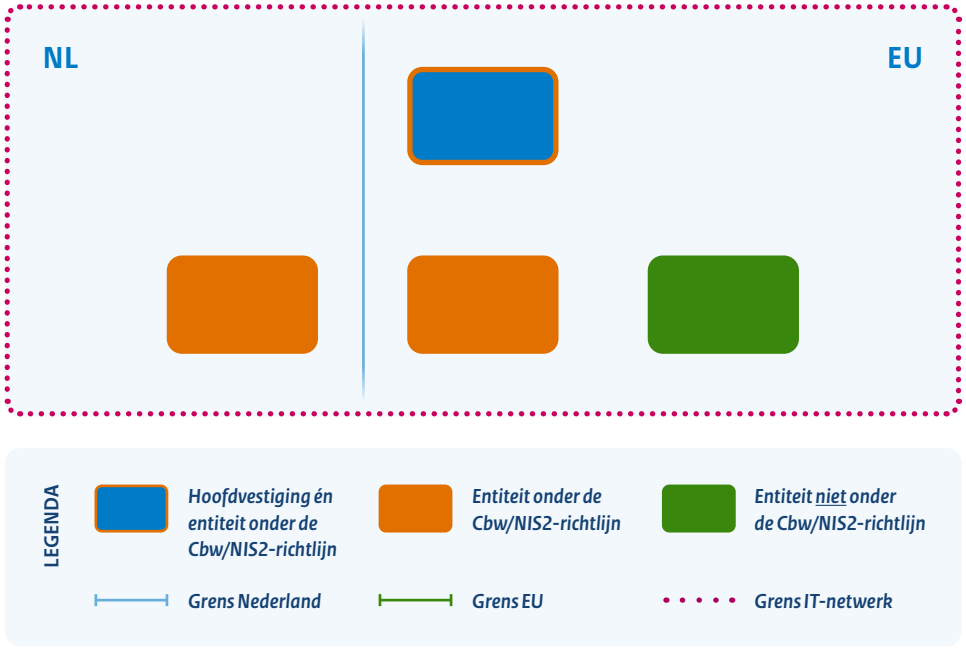
Meldingen

In geval van een significant incident zijn alleen de entiteiten die onder de Cyberbeveiligingswet vallen verplicht om een melding te maken bij het CSIRT en de bevoegde autoriteit, via het centrale meldportaal van het NCSC. Worden meerdere entiteiten die onder de Cyber-beveiligingswet vallen, geraakt door hetzelfde significante incident, dan dient elke entiteit afzonderlijk een melding te maken.

Als een entiteit valt onder de nationale implementatiewetgeving van een andere Europese lidstaat, dan dient de entiteit in die Europese lidstaat een melding te maken. Dit betekent in deze casus dat de oranje gemarkeerde entiteit die zich in Duitsland bevindt, alleen een melding dient te maken in Nederland als zij tevens een digitale dienstverlener is. Dit omdat de hoofd-vestiging in Nederland gevestigd is. Is deze entiteit geen digitale dienstverlener, dan dient zij een melding in Duitsland te maken.

Casus 3

Organisatie binnen de Europese Unie - hoofdvestiging in andere Europese lidstaat dan Nederland



Casus 3 lijkt in grote lijnen op casus 2, met als belangrijkste verschil dat de hoofdvestiging van de organisatie zich in een andere Europese lidstaat bevindt, in dit geval Duitsland. De organisatie bestaat uit meerdere entiteiten verspreid over verschillende Europese lidstaten. Eén oranje gemarkeerde entiteit is in Nederland gevestigd. Deze entiteit is een soort entiteit opgenomen in Bijlage 1 of 2 van de Cyberbeveiligingswet, voldoet aan de eventuele omvangscriteria en kwalificeert daarmee als een essentiële entiteit óf een belangrijke entiteit.

In dit geval is het wél van belang of deze entiteit tevens een digitale dienstverlener is omdat de hoofdvestiging in Duitsland gevestigd is. Is de entiteit een digitale dienstverlener, dan valt zij onder de nationale implementatiewetgeving van de Europese lidstaat waar de hoofdvestiging van de organisatie is gevestigd, in dit geval Duitsland. Indien zij niet kwalificeert als digitale dienstverlener, valt zij onder de Cyberbeveiligingswet.

De hoofdvestiging en één oranje gemarkeerde entiteit zijn in een andere Europese lidstaat gevestigd, namelijk Duitsland. Deze entiteiten zijn een soort entiteit opgenomen in Bijlage 1 of 2 van de NIS2-richtlijn, voldoen aan de eventuele omvangscriteria en kwalificeren daardoor als een essentiële entiteit óf een belangrijke entiteit. Omdat de hoofdvestiging in Duitsland is gevestigd, valt de oranje gemarkeerde entiteit - ongeacht of zij digitale dienstverleners is - onder de nationale implementatiewetgeving van Duitsland en kan daarmee niet onder de Cyberbeveiligingswet vallen. De groen gemarkeerde entiteit valt niet onder de Cyberbeveiligingswet en hoeft daardoor niet te voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

Let op

In deze casus is één oranje gemarkeerde entiteit in Duitsland gevestigd. Deze casus heeft een andere uitkomst wanneer deze oranje gemarkeerde entiteit niet in dezelfde Europese lidstaat is gevestigd als haar hoofdvestiging, in dit geval Duitsland, maar in een andere Europese lidstaat, bijvoorbeeld België. In dat geval is het wél van belang of deze entiteit tevens een digitale dienstverlener is omdat de hoofdvestiging in Duitsland gevestigd is. Is de entiteit een digitale dienstverlener, dan valt zij onder de nationale implementatiewetgeving van het land waar de hoofdvestiging van de organisatie is gevestigd, in dit geval Duitsland. Is de entiteit geen digitale dienstverlener, dan valt zij onder de nationale implementatiewetgeving van Europese lidstaat waar zijzelf gevestigd is, namelijk België.

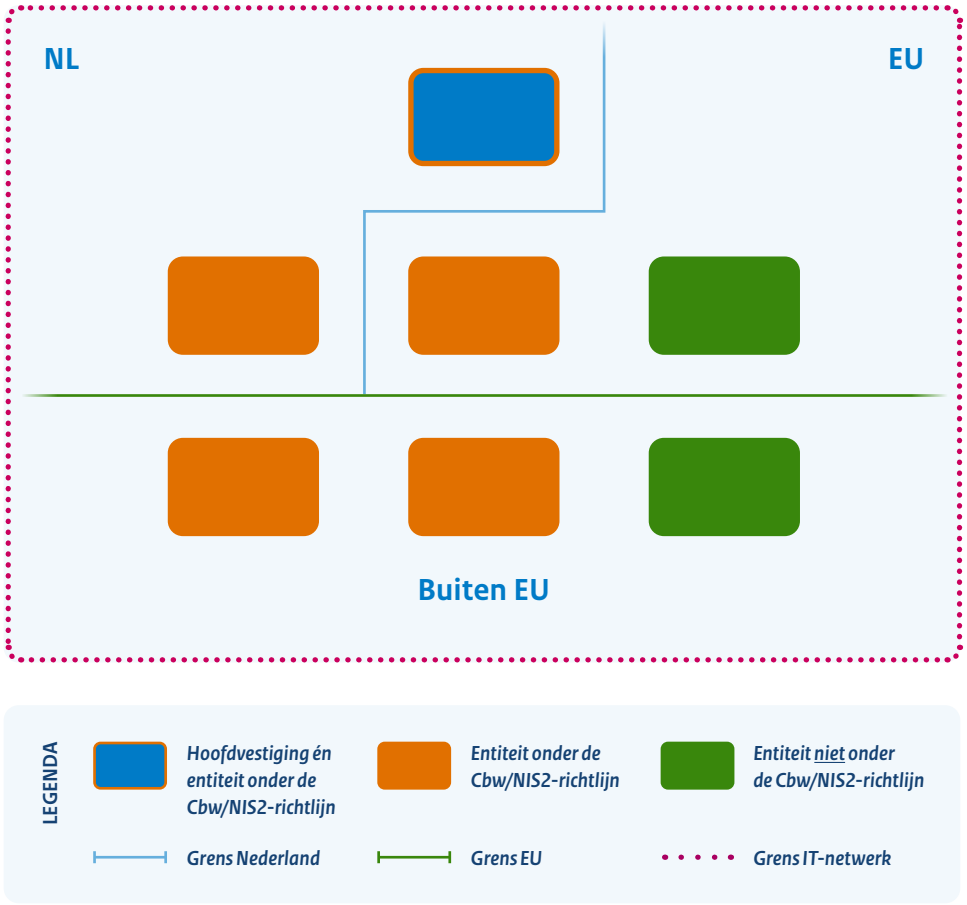
Meldingen

In geval van een significant incident zijn alleen de entiteiten die onder de Cyberbeveiligingswet vallen verplicht om een melding te maken in Nederland bij het CSIRT en de bevoegde autoriteit, via het centrale meldportaal van het NCSC. Worden meerdere entiteiten, die onder de Cyberbeveiligingswet vallen, geraakt door hetzelfde significante incident, dan dient elke entiteit afzonderlijk een melding te maken.

In geval een entiteit valt onder de nationale implementatiewetgeving van een andere Europese lidstaat, dan dient de entiteit in die Europese lidstaat een melding te maken. Dit betekent in deze casus dat de oranje gemarkeerde entiteit die zich in Duitsland bevindt een melding dient te maken in Duitsland.

Casus 4

Mondiale organisatie- hoofdvestiging in Nederland



Casus 4 betreft een organisatie met meerdere entiteiten die gevestigd zijn in zowel verschillende Europese lidstaten als landen buiten de EU. Naast de hoofdvestiging is ook één oranje gemarkeerde entiteit in Nederland gevestigd. Deze entiteiten zijn een soort entiteit opgenomen in Bijlage 1 of 2 van de Cyberbeveiligingswet, voldoen aan de eventuele omvangscriteria en kwalificeren daardoor als een essentiële entiteit óf een belangrijke entiteit. Nu de hoofdvestiging zich in Nederland bevindt, vallen deze entiteiten, ongeacht of zij digitale dienstverleners zijn, onder de Cyberbeveiligingswet.

Daarnaast zijn er twee andere entiteiten gevestigd in een andere Europese lidstaat, namelijk Duitsland. Eén daarvan, de oranje gemarkeerde entiteit, is een soort entiteit opgenomen in Bijlage 1 of 2 van de NIS2-richtlijn, voldoet aan de eventuele omvangscriteria en kwalificeert daardoor als een essentiële entiteit óf een belangrijke entiteit. Deze entiteit valt alleen onder de Cyberbeveiligingswet als zij tevens een digitale dienstverlener is, omdat de hoofdvestiging van de organisatie in Nederland is gevestigd. Is dat niet het geval, dan valt deze entiteit onder de nationale implementatiewetgeving van de Europese lidstaat waar ze gevestigd is, in dit geval Duitsland. De groen gemarkeerde entiteit valt niet onder de Cyberbeveiligingswet en hoeft daardoor niet te voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

Er zijn drie entiteiten gevestigd buiten de EU. Twee daarvan, de oranje gemarkeerde entiteiten, zijn een soort entiteit opgenomen in Bijlage 1 of 2 van de NIS2-richtlijn, voldoen aan de eventuele omvangscriteria en kwalificeren daardoor als essentiële entiteit óf belangrijke entiteit. **Omdat de twee oranje gemarkeerde entiteiten buiten de EU gevestigd zijn, kunnen zij alleen onder de NIS2-richtlijn vallen als zij tevens kwalificeren als digitale dienstverlener.** Omdat de hoofdvestiging van de organisatie in Nederland is gevestigd, vallen deze entiteiten onder de Cyberbeveiligingswet. De groen gemarkeerde entiteit valt niet onder de Cyberbeveiligingswet en hoeft daardoor niet te voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

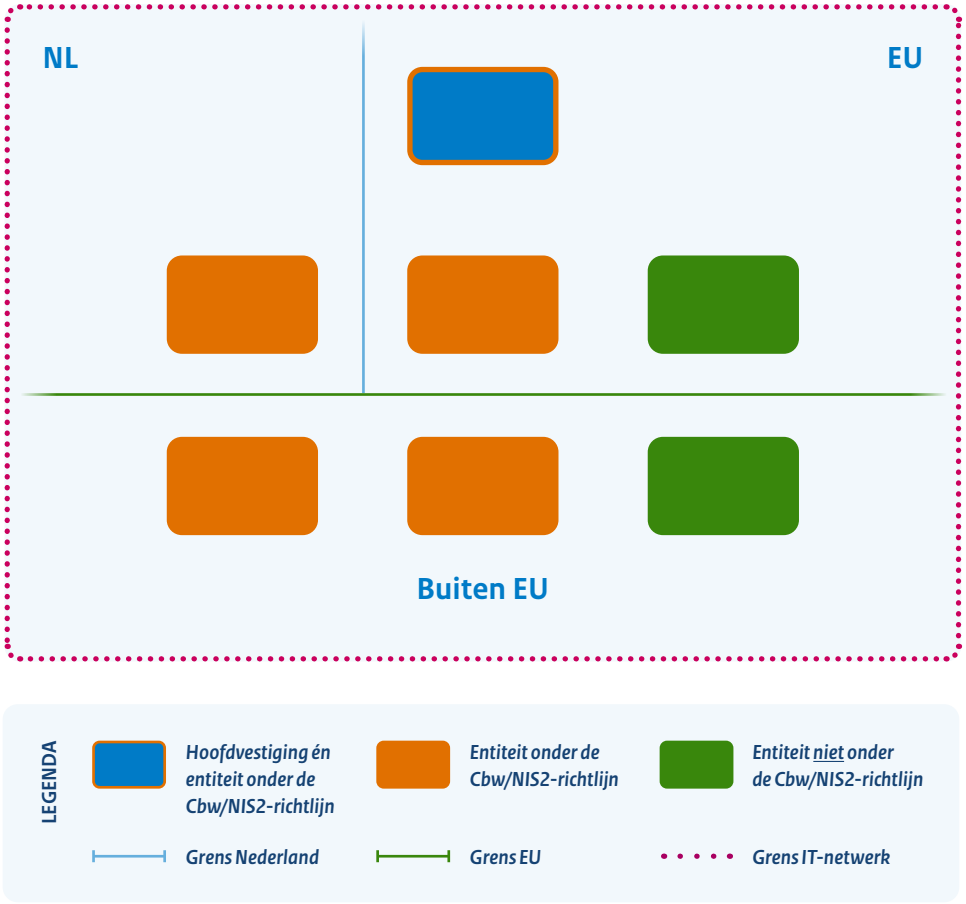
Meldingen

In geval van een significant incident zijn alleen de entiteiten die vallen onder de Cyberbeveiligingswet verplicht om een melding te maken in Nederland bij het CSIRT en de bevoegde autoriteit, via het centrale meldportaal van het NCSC. Worden meerdere entiteiten die onder de Cyberbeveiligingswet vallen, geraakt door hetzelfde significante incident, dan dient elke entiteit afzonderlijk een melding te maken.

In geval een entiteit onder de nationale implementatiewetgeving van een andere Europese lidstaat valt, dan dient de entiteit in die Europese lidstaat een melding te maken. Dit betekent in deze casus dat de oranje gemarkeerde entiteit die zich in Duitsland bevindt, alleen een melding dient te maken in Nederland als zij tevens een digitale dienstverlener is. Dit omdat de hoofdvestiging in Nederland gevestigd is. Is deze entiteit geen digitale dienstverlener, dan dient zij een melding in Duitsland te maken. Voor de oranje gemarkeerde entiteiten buiten de EU, geldt dat zij een melding dient te maken in de Europese lidstaat waar de hoofdvestiging gevestigd is, in dit geval in Nederland.

Casus 5

Mondiale organisatie – hoofdvestiging in een andere Europese lidstaat



Casus 5 lijkt in grote lijnen op casus 4, met als belangrijkste verschil dat de hoofdvestiging van de organisatie zich in een andere Europese lidstaat bevindt, in dit geval Duitsland. De organisatie bestaat uit meerdere entiteiten, die gevestigd zijn in zowel verschillende Europese lidstaten als landen buiten de EU.

Eén oranje gemarkeerde entiteit is in Nederland gevestigd. Deze entiteit is een soort entiteit opgenomen in Bijlage 1 of 2 van de Cyberbeveiligingswet, voldoet aan de eventuele omvangscriteria en kwalificeert daarmee als een essentiële entiteit óf een belangrijke entiteit. In dit geval is wél van belang of deze entiteit tevens een digitale dienstverlener is, omdat de hoofdvestiging in Duitsland gevestigd is. Is de entiteit een digitale dienstverlener, dan valt zij onder de nationale implementatiewetgeving van de Europese lidstaat waar de hoofdvestiging van de organisatie is gevestigd, in dit geval Duitsland. Indien zij niet kwalificeert als digitale dienstverlener, valt zij onder de Cyberbeveiligingswet.

De hoofdvestiging en één oranje gemarkeerde entiteit zijn in een andere Europese lidstaat gevestigd, namelijk Duitsland. Deze entiteiten zijn een soort entiteit opgenomen in Bijlage 1 of 2 van de NIS2-richtlijn, voldoen aan de eventuele omvangscriteria en kwalificeren daardoor als een essentiële entiteit óf een belangrijke entiteit. Omdat de hoofdvestiging in Duitsland is gevestigd, valt de oranje gemarkeerde entiteit - ongeacht of zij digitale dienstverlener is - onder de nationale implementatiewetgeving van Duitsland en kan daarmee niet onder de Cyberbeveiligingswet vallen. De groen gemarkeerde entiteit valt niet onder de Cyberbeveiligingswet en hoeft daardoor niet te voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

Let op

In deze casus is één oranje gemarkeerde entiteit in Duitsland gevestigd. Deze casus heeft een andere uitkomst wanneer deze oranje gemarkeerde entiteit niet in dezelfde Europese lidstaat is gevestigd als haar hoofdvestiging, in dit geval Duitsland, maar in een andere Europese lidstaat, bijvoorbeeld België. In dat geval is het wél van belang of deze entiteit tevens een digitale dienstverlener is omdat de hoofdvestiging in Duitsland gevestigd is. Is de entiteit een digitale dienstverlener, dan valt zij onder de nationale implementatiewetgeving van het land waar de hoofdvestiging van de organisatie is gevestigd, in dit geval Duitsland. Is de entiteit geen digitale dienstverlener, dan valt zij onder de nationale implementatiewetgeving van Europese lidstaat waar zijzelf gevestigd is, namelijk België.

Er zijn drie entiteiten gevestigd buiten de EU. Twee daarvan, de oranje gemarkeerde entiteiten, zijn een soort entiteit opgenomen in Bijlage 1 of 2 van de NIS2-richtlijn voldoen aan de eventuele omvangscriteria en kwalificeren daardoor als een essentiële entiteit óf een belangrijke entiteit. **Omdat de twee oranje gemarkeerde entiteiten buiten de EU gevestigd zijn, kunnen zij alleen onder de NIS2-richtlijn vallen als zij tevens kwalificeren als digitale dienstverlener.** Omdat de hoofdvestiging van de organisatie in Duitsland is gevestigd, vallen deze entiteiten onder de nationale implementatiewetgeving van Duitsland. Zij kunnen niet onder de Cyberbeveiligingswet vallen. De groen gemarkeerde entiteit valt niet onder de Cyberbeveiligingswet en hoeft daardoor niet te voldoen aan de verplichtingen uit de Cyberbeveiligingswet.

Meldingen

In geval van een significant incident zijn alleen de entiteiten die vallen onder de Cyberbeveiligingswet verplicht om een melding te maken in Nederland bij het CSIRT en de bevoegde autoriteit, via het centrale meldportaal van het NCSC. Worden meerdere entiteiten, die onder de Cyberbeveiligingswet vallen, geraakt door hetzelfde significante incident, dan dient elke afzonderlijke entiteit een melding te doen.

Als een entiteit valt onder de nationale implementatiewetgeving van een andere Europese lidstaat, dan dient de entiteit in die Europese lidstaat een melding te doen. Dit betekent in deze casus dat de oranje gemarkeerde entiteit die zich in Nederland bevindt, alleen een melding dient te maken in Duitsland als zij tevens een digitale dienstverlener is. Dit omdat de hoofdvestiging in Duitsland gevestigd is. Is deze entiteit geen digitale dienstverlener, dan dient zij een melding in Duitsland te maken. Voor de oranje gemarkeerde entiteiten buiten de EU, geldt dat zij een melding dient te maken in de Europese lidstaat waar de hoofdvestiging gevestigd is, in dit geval in Duitsland.

Afronding

Deze handreiking is bedoeld om organisaties te ondersteunen bij het bepalen of zij onder de NIS2-richtlijn en daarmee onder de Cyberbeveiligingswet vallen. Hoewel aan dit document geen rechten kunnen worden ontleend, geven de opgenomen casussen inzicht in het toepassingsbereik van de wet en helpen zij organisaties om de regels te vertalen naar hun eigen situatie.

Voor organisaties met een complexe bedrijfsstructuur zijn aanvullende vragen en antwoorden beschikbaar via de website van de NCTV. Verder bieden zowel de NCTV als het NCSC uitgebreide informatie en advies over de Cyberbeveiligingswet. Voor sectorspecifieke vragen kunnen organisaties terecht bij het ministerie dat verantwoordelijk is voor de sector waarin zij actief zijn.

november 2025

Medegefinancierd door
de Europese Unie