Version 1.0
07/2024

CENTRE FOR CYBERSECURITY BELGIUM

Veelgestelde vragen (FAQ)
NIS2 in België

Het doel van dit document is om antwoord te geven op veelgestelde vragen over het wettelijke kader van NIS2 in België. Het is een aanvulling op de informatie die al beschikbaar is op de CCB-website en op Safeonweb@Work.

Inhoudsopgave

AFKORTINGEN & REFERENTIES 3

1. ALGEMEEN - TOEPASSINGSGEBIED 4

1.1. WAT ZIJN DE DOELSTELLINGEN VAN DE NIS2-WET? 4
1.2. WAT IS HET TOEPASSINGSGEBIED VAN DE NIS2-WET? 4
1.3. HOE DE OMVANG VAN EEN ENTITEIT BEREKENEN? 5
1.4. WELKE SECTOREN EN DIENSTEN VALLEN ONDER DE WET? 6
1.5. IS HET MOGELIJK OM DE SECTOREN DIE ONDER DE NIS2-WET VALLEN IN DE TOEKOMST UIT TE BREIDEN? 7
1.6. KAN EEN ENTITEIT ONDER MEER DAN ÉÉN SECTOR VALLEN? 7
1.7. WAT IS HET VERSCHIL TUSSEN "ESSENTIËLE" EN "BELANGRIJKE" ENTITEITEN? 7
1.8. HOE WERKT DE EVENTUELE AANVULLENDE IDENTIFICATIEPROCEDURE? 8
1.9. WAT IS HET TERRITORIALE TOEPASSINGSGEBIED VAN DE WET? WAT MET ENTITEITEN DIE IN MEERDERE LANDEN ACTIEF ZIJN (MULTINATIONALS, ...)? 9
1.10. HOE VERHOUDEN DE DORA-VERORDENING EN DE NIS2-RICHTLIJN ZICH TOT ELKAAR? 10
1.11. VALLEN KRITIEKE INFRASTRUCTUREN (OF KRITIEKE ENTITEITEN VOLGENS DE CER-RICHTLIJN) ONDER HET TOEPASSINGSGEBIED VAN DE NIS2-WET? 11
1.12. VALT EEN ONDERWIJSINSTELLING BINNEN HET TOEPASSINGSGEBIED VAN DE WET? 11
1.13. KUNNEN NACE-CODES WORDEN GEBRUIKT OM TE BEPALEN OF EEN ENTITEIT ONDER DE WET VALT? 11
1.14. HOE WORDT BEPAALD OF EEN ORGANISATIE BINNEN HET TOEPASSINGSGEBIED VAN DE NIS2-WET VALT? 12
1.14.1. Voorafgaand aan het analyseren van de NIS2-wet zelf 12
1.14.2. Wat is de omvang van mijn organisatie? 13
1.14.3. Welke dienst(en) verleent mijn organisatie in de Europese Unie? 14
1.14.4. De oprichting 15
1.14.5. Aanvullende identificatie en toeleveringsketen 16

2. OVERHEIDSSECTOR 17

2.1. HOE IS DE WET VAN TOEPASSING OP DE OVERHEIDSSECTOR? 17
2.2. ZIJN LOKALE OVERHEIDSINSTANTIES ONDERWORPEN AAN DE VERPLICHTINGEN VAN DE WET? 18
2.3. ZIJN DE VERPLICHTINGEN VAN DE WET VAN TOEPASSING OP DE OVERHEIDSINSTANTIES VAN DE GEWESTEN EN DE GEMEENSCHAPPEN? 18

3. VERPLICHTINGEN 19

3.1. WAT ZIJN DE WETTELIJKE VERPLICHTINGEN VOOR DE BETROKKEN ENTITEITEN? 19

3.2. WAT ZIJN DE VERPLICHTINGEN OP HET GEBIED VAN CYBERBEVEILIGINGSMAATREGELEN? 19
3.3. WAT ZIJN DE VERPLICHTINGEN VOOR HET MELDEN VAN INCIDENTEN? 20
3.3.1. Algemene regels *20*
3.3.2. Ontvangers van een verplichte melding van een significant incident *21*
3.3.3. Procedure voor het melden van incidenten *21*
3.3.4. Informatie die moet worden verstrekt bij het melden van een incident *22*
3.3.5. Vertrouwelijkheidsregels die van toepassing zijn op informatie die wordt uitgewisseld tijdens een incident *22*
3.4. WAT GEBEURT ER ALS ER ZICH EEN INCIDENT VOORDOET WAARBIJ OOK PERSOONLIJKE GEGEVENS BETROKKEN ZIJN? 23
3.5. IS HET MOGELIJK OM INCIDENTEN OF CYBERDREIGINGEN VRIJWILLIG TE MELDEN? 23
3.6. WAT ZIJN DE WETTELIJKE VOORWAARDEN OM GEBRUIK TE MAKEN VAN HET BESCHERMEND KADER BIJ HET ONDERZOEKEN EN RAPPORTEREN VAN KWETSBAARHEDEN (ETHISCH HACKEN)? 23
3.7. HOE WORDEN NIS2-ENTITEITEN GEREGISTREERD? 24
3.8. HOE KAN EEN ENTITEIT ZIJN RELATIES MET LEVERANCIERS EN DIRECT DIENSTVERLENERS BEHEREN (TOELEVERINGSKETEN/*SUPPLY CHAIN*)? 25
3.9. HOE VERTROUWELIJK IS DE UITGEWISSELDE INFORMATIE? 25

4. CONTROLE/ TOEZICHT 27

4.1. WIE ZIJN DE BEVOEGDE AUTORITEITEN? 27
4.1.1. Het Centrum voor Cybersecurity België (CCB) *27*
4.1.2. De sectorale overheden *27*
4.1.3. Het Nationaal Crisiscentrum (NCCN) *28*
4.2. KUNNEN BEPAALDE REFERENTIEKADERS DOOR NIS2-ENTITEITEN WORDEN GEBRUIKT OM HUN CONFORMITEIT AAN TE TONEN? 28
4.2.1. Het CyberFundamentals (CyFun®)-raamwerk *28*
4.2.2. ISO/IEC 27001 ..... *29*
4.3. HOE WORDEN DE BETROKKEN ENTITEITEN GECONTROLEERD? 29
4.4. WAT IS EEN CONFORMITEITSBEOORDELINGSINSTANTIE (CAB)? 30
4.5. WAT ZIJN DE TAKEN VAN DE SECTORALE OVERHEDEN? 30
4.6. HOE KAN EEN ENTITEIT BEWIJZEN DAT ZE HAAR VERPLICHTINGEN NALEEFT? 30
4.7. KAN EEN ENTITEIT EEN CYFUN®-ZEKERHEIDSNIVEAU GEBRUIKEN DAT LAGER IS DAN HET NIVEAU DAT AAN HAAR ENTITEITSCATEGORIE IS TOEGEWEZEN? 31
4.8. KAN EEN ENTITEIT DIE EEN AANBIEDER VAN ESSENTIËLE DIENSTEN (AED) UITMAAKTE ONDER NIS1 HAAR ISO27001-CERTIFICERING BEHOUDEN? 31
4.9. WANNEER MOETEN DE BETROKKEN ENTITEITEN DE VERPLICHTINGEN VAN DE WET TOEPASSEN? 32
4.10. WAT ZIJN DE MODALITEITEN VAN DE INSPECTIE? 33
4.11. ZIJN DE ADMINISTRATIEVE MAATREGELEN EN DE ADMINISTRATIEVE GELDBOETES EVENREDIG? WAT ZIJN DE BEDRAGEN VAN DE BOETES? 33
4.12. WELKE ANDERE ADMINISTRATIEVE MAATREGELEN KUNNEN WORDEN GENOMEN? 34
4.12.1. Basismaatregelen *34*
4.12.2. Bijkomende maatregelen *35*
4.13. WAT ZIJN DE VERPLICHTINGEN EN VERANTWOORDELIJKHEDEN VAN HET MANAGEMENT? 35
4.14. WAT IS EEN "BESTUURSORGAAN"? 36

5. ANDERE 37

5.1. MOET DE EUROPESE COMMISSIE NOG UITVOERINGSHANDELINGEN VASTSTELLEN? 37

Afkortingen & Referenties

In dit document worden de volgende afkortingen en verwijzingen gebruikt:

- Aanbeveling (2003/361/EG): Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (beschikbaar op Eur-Lex)
- AVG: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (beschikbaar op Eur-Lex)
- BELAC: Belgische Accreditatie-instelling
- CAB: *Conformity Assessment Body (*Conformiteitsbeoordelingsinstantie)
- CCB: Centrum voor Cybersecurity België (nationale cyberbeveiligingsautoriteit & nationale CSIRT)
- CSIRT: Computer Security Incident Response Team (in België is het CCB het nationale CSIRT)
- CyFun®: Cyberfundamentals-raamwerk (*Cyberfundamentals Framework)*, beschikbaar op SafonwebAtWork
- DORA: Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende de digitale operationele weerbaarheid van de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (beschikbaar op Eur-Lex).
- Koninklijk besluit NIS2: Koninklijk besluit van 9 juni 2024 tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (beschikbaar op Justel)
- NCCN: Nationaal crisiscentrum
- NIS1-richtlijn: Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (beschikbaar op Eur-Lex)
- NIS1-wet: Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (beschikbaar op Justel)
- NIS2-richtlijn: Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (beschikbaar op Eur-Lex)
- NIS2-wet: Wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (beschikbaar op Justel)

1. Algemeen - Toepassingsgebied

1.1. Wat zijn de doelstellingen van de NIS2-wet?

Richtlijn 2022/2555 ("NIS2") en de Belgische NIS2-wet tot omzetting ervan hebben tot doel de cyberweerbaarheid te versterken door zich te richten op de volgende hoofddoelstellingen:

1) Bescherming op het gebied van cyberbeveiliging voor essentiële diensten die in de Europese Unie worden verleend. In vergelijking met de NIS1-richtlijn, breidt de NIS2-richtlijn het aantal essentiële diensten uit in verschillende zeer kritieke sectoren (bijlage I) of andere kritieke sectoren (bijlage II). Het toepassingsgebied wordt nu voornamelijk bepaald door het gebruik van Europese definities (zoals "type-entiteit") en een omvangscriterium (“size-cap”);
2) Versterking van de maatregelen voor risicobeheer op het gebied van cyberbeveiliging die entiteiten moeten nemen, evenals het melden van significante incidenten (met twee categorieën van entiteiten: essentiële of belangrijke);
3) Aanmoedigen van het delen van informatie over incidenten en risico's op het gebied van cyberbeveiliging tussen de betrokken entiteiten en de nationale CSIRT's;
4) Versterking van het toezicht en de sancties;
5) Zorgen voor Europese en nationale samenwerking.

1.2. Wat is het toepassingsgebied van de NIS2-wet?

De NIS2-wet is van toepassing op publieke of private entiteiten die in principe in België zijn gevestigd (er zijn enkele uitzonderingen op deze regel) en die een dienst verlenen binnen de Europese Unie die is opgenomen in bijlage I of II van de wet.

Art. 3 tot 7 NIS2-wet

Om als een aan de wet onderworpen entiteit te worden beschouwd, is het voldoende om, ongeacht de rechtsvorm, ten minste één van de in bijlage I of II van de wet genoemde activiteiten binnen de Europese Unie uit te oefenen en ten minste te worden beschouwd als een middelgrote onderneming in de zin van Aanbeveling 2003/361/EG van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen.

Essentiële entiteiten zijn organisaties die een dienst verlenen die is opgenomen in bijlage I en die voldoen aan de definitie van grote onderneming in de zin van Aanbeveling 2003/361/EG.

Belangrijke entiteiten zijn organisaties die een dienst leveren die:

- is opgenomen in bijlage I en voldoet aan de definitie van een "middelgrote onderneming" in de zin van Aanbeveling 2003/361/EG;
- is opgenomen in bijlage II en voldoet aan de definitie van een middelgrote of grote onderneming zoals gedefinieerd in Aanbeveling 2003/361/EG;

Het is belangrijk om te benadrukken dat het **toepassingsgebied van de NIS2-wet de hele betrokken entiteit omvat** en niet alleen de activiteiten omvat die in de bijlagen bij de wet worden opgesomd.

Tenzij de definitie van dienst opgenomen in de bijlagen rekening houdt met het hoofd- of bijkomstige karakter van de betrokken activiteit, valt een entiteit binnen het toepassingsgebied van de wet, **zelfs als de essentiële dienst die zij verleent slechts een bijkomstig onderdeel is van al haar activiteiten.**

Raadpleeg de volgende afdelingen voor meer informatie.

1.3. Hoe de omvang van een entiteit berekenen?

Art. 3, §1 en §2 NIS2-wet

Voor het toepassingsgebied van de NIS2-wet wordt de omvang van de entiteit berekend op basis van de regels in de bijlage bij de Aanbeveling 2003/361/EG. De Europese Commissie heeft een gedetailleerde gebruikersgids en een berekeningshulpmiddel ter beschikking gesteld.

Een organisatie kwalificeert als middelgrote onderneming wanneer het:

- tussen 50 en 249 mensen in dienst heeft (werknemers, tijdelijk personeel of uitzendkrachten, partners, enz.); of
- een jaaromzet van meer dan €10 miljoen tot €50 miljoen, of een jaarlijks balanstotaal van meer dan €10 miljoen tot €43 miljoen heeft.

Voor de toepassing van deze drempels voor financiële gegevens heeft de betrokken organisatie de keuze om ofwel haar jaaromzet ofwel haar totale jaarbalans te gebruiken. **Een van deze twee cijfers kan de drempel voor een grote onderneming overschrijden**, zonder dat dit gevolgen heeft voor de classificatie van een organisatie als middelgrote onderneming.

Een organisatie kwalificeert als een groot bedrijf als ze:

- 250 of meer mensen in dienst heeft (werknemers, tijdelijk personeel of uitzendkrachten, operators, partners, enz.); of
- een jaarlijkse omzet van meer dan €50 miljoen en een jaarlijks balanstotaal van meer dan €43 miljoen heeft.

Er moet rekening worden gehouden met het feit dat in situaties waarbij "partnerbedrijven" of "verbonden bedrijven" betrokken zijn, een proportionele consolidatie van de gegevens (personeelsbestand en financiële gegevens) van de betrokken entiteit en van deze andere entiteiten moet worden uitgevoerd om de omvang te berekenen.

Op enkele uitzonderingen na wordt een bedrijf als "partner" beschouwd als het tussen 25% en 50% van het kapitaal of de stemrechten (afhankelijk van welke het grootst is) in de betreffende entiteit bezit (of omgekeerd). Dit type relatie beschrijft de situatie van bedrijven die bepaalde financiële partnerschappen aangaan met andere bedrijven, zonder dat het eerste bedrijf daadwerkelijk directe of indirecte zeggenschap uitoefent over het tweede bedrijf.

Met bepaalde uitzonderingen wordt een bedrijf als "verbonden" beschouwd als het meer dan 50% van het kapitaal of de stemrechten (afhankelijk van welke het hoogst is) in de betrokken entiteit bezit (of omgekeerd).

In het geval van partner bedrijven moet het bedrijf in kwestie aan zijn eigen gegevens een deel van het personeelsbestand en de financiële gegevens van het andere bedrijf toevoegen om zijn grootte te bepalen. Dit aandeel weerspiegelt het percentage aandelen of stemrechten dat het bedrijf bezit (de grootste waarde is van toepassing). In het geval van verbonden ondernemingen

moet de onderneming in kwestie 100% van de gegevens van de verbonden onderneming aan haar eigen gegevens toevoegen.

Als een bedrijf bijvoorbeeld een belang van 30% heeft in een ander bedrijf, telt het bij zijn eigen cijfers 30% van het personeelsbestand, de omzet en het balanstotaal van het partnerbedrijf op. Als er meerdere partnerbedrijven zijn, moet dezelfde soort berekening worden gemaakt voor elk partnerbedrijf dat zich direct stroomopwaarts of stroomafwaarts van het bedrijf in kwestie bevindt.

De NIS2-wet voorziet echter in een mechanisme waarmee de nationale cyberbeveiligingsautoriteit (CCB), in geval van een onevenredige situatie, rekening kan houden met de mate van onafhankelijkheid die een entiteit geniet ten opzichte van haar partners en verbonden ondernemingen, met name wat betreft de netwerk- en informatiesystemen die zij gebruikt om haar diensten te verlenen en wat betreft de diensten die zij verleent. Deze elementen moeten geval per geval worden aangetoond aan het CCB door de organisatie die er gebruik van wil maken. De toepassing van dit mechanisme kan ertoe leiden dat een organisatie wordt geherclassificeerd als een belangrijke in plaats van een essentiële entiteit, of helemaal wordt uitgesloten van het toepassingsgebied van de wet.

Zie ook paragraaf 1.14.2. en de gedetailleerde handleiding voor het berekenen van afmetingen voor meer details.

1.4. Welke sectoren en diensten vallen onder de wet?

Bijlagen I en II NIS2-wet; artikel 8 NIS2-wet

De betreffende entiteit moet ten minste een van de diensten leveren die zijn opgenomen in bijlage I of II van de wet (zelfs als deze dienst slechts een bijkomstig deel van de activiteiten uitmaakt - behalve wanneer de definitie zelf de hoofd- of bijkomstige aard van de geleverde dienst als criterium gebruikt) uit een van de volgende sectoren:

Zeer kritieke sectoren (bijlage I)	**Andere kritieke sectoren (bijlage II)**
○ Energie (elektriciteit, stadsverwarming en -koeling, aardolie, aardgas, waterstof) ○ Vervoer (lucht, spoor, water, weg) ○ Bankwezen ○ Infrastructuur voor de financiële markt ○ Gezondheidszorg ○ Drinkwater ○ Afvalwater ○ Digitale infrastructuur ○ Beheer van ICT-diensten ○ Overheid ○ Ruimtevaart	○ Post- en koeriersdiensten ○ Afvalstoffenbeheer ○ Vervaardiging, productie en distributie van chemische stoffen ○ Productie, verwerking en distributie van levensmiddelen ○ Vervaardiging (van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek; van informaticaproducten en van elektronische en optische producten; van elektrische apparatuur; van machines, apparaten en werktuigen, n.e.g., van motorvoertuigen, aanhangers en opleggers; van andere transportmiddelen) ○ Digitale aanbieders ○ Onderzoek

Elke dienst die onder de NIS2-wet valt, **wordt gedefinieerd** in bijlage I of II (met een verwijzing naar de definities in de relevante Europese juridische normen), of in artikel 8 van de NIS2-wet. Om te begrijpen onder welke bijlage de betreffende dienst valt, is het noodzakelijk om deze definities te raadplegen. Daartoe zijn de bijlagen beschikbaar op de website van het Belgisch Staatsblad (na de tekst/het dispositief van de wet).

Zie ook paragraaf 1.14.3 voor meer details en de scope test tool.

1.5. Is het mogelijk om de sectoren die onder de NIS2-wet vallen in de toekomst uit te breiden?

Art. 3, § 6 NIS2-wet

De Koning kan sectoren of deelsectoren aan de bijlagen I en II toevoegen via een besluit vastgesteld na overleg in de Ministerraad, na de raadpleging van de eventuele betrokken sectorale overheden en de nationale cyberbeveiligingsautoriteit (CCB).

Op deze manier kunnen de bijlagen worden uitgebreid als in de toekomst blijkt dat een sector die nog niet onder het toepassingsgebied valt, moet worden opgenomen vanwege zijn belang voor kritieke maatschappelijke en/of economische activiteiten.

1.6. Kan een entiteit onder meer dan één sector vallen?

Art. 8, 34°; 25; 39, lid 2 en 44, §1, lid 2 NIS2-wet

Ja, het is mogelijk dat een entiteit onder meerdere sectoren valt. In dat geval zijn er een aantal overwegingen om rekening mee te houden:

- Strengere verplichtingen hebben voorrang op minder strenge verplichtingen. Als aan het omvangscriterium wordt voldaan (grote onderneming), zal een entiteit die diensten levert die zowel onder bijlage I als bijlage II vallen, als geheel als essentiële entiteit worden aangemerkt;
- De entiteit komt dan mogelijk onder toezicht te staan van de nationale cyberbeveiligingsautoriteit (CCB) en meerdere sectorale overheden. Deze autoriteiten zullen met elkaar samenwerken in het kader van toezicht;
- Een publieke entiteit waarvan de hoofdzakelijke activiteit bestaat uit het verlenen van een dienst die is opgenomen in een andere sector (dan de sector overheid) van de bijlagen bij de wet, valt uitsluitend onder die sector (en niet tegelijkertijd onder die sector en de sector openbaar bestuur).

1.7. Wat is het verschil tussen "essentiële" en "belangrijke" entiteiten?

Art. 39-42; 48, § 1 en § 2; 58 en 59 NIS2-wet.

Essentiële en belangrijke entiteiten worden voornamelijk onderscheiden in het kader van het toezicht en de sancties. Essentiële entiteiten worden proactief "*ex ante*" en reactief "*ex post*" gecontroleerd. Meer specifiek worden essentiële entiteiten onderworpen aan regelmatige conformiteitsbeoordelingen.

Belangrijke entiteiten zijn onderworpen aan "*ex post*"-toezicht, d.w.z. op basis van bewijs, aanwijzingen of informatie dat een belangrijke entiteit haar verplichtingen krachtens de wet niet nakomt.

Voor meer informatie over het toezicht, zie afdeling 4.3.

Voor het overige zijn beide soorten entiteiten onderworpen aan dezelfde verplichtingen, bijvoorbeeld met betrekking tot het melden van incidenten (paragraaf 3.3) of het nemen van maatregelen voor risicobeheer op het gebied van cyberbeveiliging (paragraaf 3.2.).

1.8. Hoe werkt de eventuele aanvullende identificatieprocedure?

Art. 11 NIS2-wet

Op eigen initiatief of -indien van toepassing- op voorstel van de betrokken sectorale overheid, kan de nationale cyberbeveiligingsautoriteit (CCB) een entiteit als essentieel of belangrijk aanmerken, ongeacht haar omvang, in de volgende gevallen:

1. de entiteit is de enige aanbieder, in België, van minstens één dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten, met name in een van de sectoren of deelsectoren van de bijlagen I en II van de Wet;
2. een verstoring van de door de entiteit verleende dienst kan aanzienlijke gevolgen hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;
3. een verstoring van de door de entiteit verleende dienst kan een aanzienlijk systeemrisico met zich brengen, met name voor sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;
4. de entiteit is kritiek vanwege het specifieke belang ervan op nationaal of regionaal niveau voor de specifieke sector of het specifieke type dienst, of voor andere onderling afhankelijke sectoren in België.

Een ontwerpbeslissing tot identificatie wordt voorgelegd aan de betrokken entiteit en vervolgens aan de eventuele betrokken deelgebieden en sectorale overheden, die binnen zestig dagen een niet-gepubliceerd advies uitbrengen.

In geval van een ongunstig advies van een sectorale overheid en indien de nationale cyberbeveiligingsautoriteit haar ontwerpbeslissing wenst te handhaven, wordt de ontwerpbeslissing samen met het advies voorgelegd aan het Strategisch Comité Inlichtingen en Veiligheid, opgericht bij het koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid die een bindend advies uitbrengen. Op basis van dit advies zal het CCB beslissen om al dan niet verder te gaan met de identificatie.

Het CCB beoordeelt de identificatie van essentiële en belangrijke entiteiten ten minste om de twee jaar volgens dezelfde procedures en werkt deze indien nodig bij.

1.9. Wat is het territoriale toepassingsgebied van de wet? Wat met entiteiten die in meerdere landen actief zijn (multinationals, ...)?

Art. 4 NIS2-wet

De Belgische NIS2-wet is in principe van toepassing op in **België gevestigde** entiteiten die hun diensten verlenen of hun activiteiten verrichten in de EU.

Het begrip "entiteit" wordt in artikel 8, 37° van de NIS2-wet gedefinieerd als: *" -een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen"*.

Het vestigingscriterium bestaat uit de daadwerkelijke uitoefening van activiteit door middel van stabiele regelingen, ongeacht de gekozen rechtsvorm, of dit nu de maatschappelijke zetel, een filiaal of een dochteronderneming met rechtspersoonlijkheid is.

De NIS2-wet voorziet in drie uitzonderingen op de regel van vestiging in België:

1) De Belgische wet is van toepassing op aanbieders van openbare elektronische-communicatienetwerken en aanbieders van openbare elektronische-communicatiediensten wanneer zij hun dienst in België aanbieden;
2) De Belgische wet is van toepassing op DNS-dienstverleners, registers voor toplevel domeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook op aanbieders van onlinemarktplaatsen, onlinezoekmachines of platformen voor socialenetwerkdiensten, wanneer zij hun hoofdvestiging in België hebben of hun vertegenwoordiger in de Europese Unie in België gevestigd is*;
3) De Belgische wet is van toepassing op alle door België opgerichte overheidsinstellingen.

Het begrip "hoofdvestiging" verwijst naar de vestiging waar de entiteit beslissingen neemt met betrekking tot maatregelen voor het beheer van cyberbeveiligingsrisico's. Als deze plaats niet kan worden bepaald of zich buiten de EU bevindt, verwijst het naar de vestiging waar de entiteit haar cyberbeveiligingsactiviteiten uitvoert. Als ook deze plaats niet kan worden bepaald, verwijst het begrip naar de vestiging met het grootste aantal werknemers.

(*) Indien een entiteit bedoeld in punt 2) niet in de EU is gevestigd maar er haar diensten verleent, moet ze een vertegenwoordiger aanstellen die gevestigd is in een lidstaat waar ze haar diensten verleent. Als deze vertegenwoordiger in België is gevestigd, wordt de entiteit geacht haar hoofdvestiging in België te hebben.

Als een entiteit meerdere vestigingen heeft in meerdere landen van de Europese Unie, zal ze onderworpen zijn aan omzettingswetten in elk van de betrokken lidstaten. De verschillende bevoegde nationale autoriteiten zullen samenwerken om significante incidenten te inspecteren en te rapporteren.

1.10. Hoe verhouden de DORA-verordening en de NIS2-richtlijn zich tot elkaar?

Art. 6 NIS2-wet
Art. 2 & 47 DORA

De NIS2-richtlijn en de bijbehorende omzettingswet zijn gericht op horizontale cyberbeveiligingsmaatregelen in de EU. Het doel is om de globale cyberbeveiliging in de EU te verbeteren en in het bijzonder om een hoog niveau van cyberbeveiliging te waarborgen voor bepaalde entiteiten die kritiek zijn voor maatschappelijke en economische activiteiten.

De DORA-verordening (Digital Operational Resiliance Act) richt zich specifiek op operatoren in de financiële sector. Het doel is om de operationele weerbaarheid van informatiesystemen in de financiële sector te versterken en de bestaande regelgeving op dit gebied te coördineren.

DORA is van toepassing op de in artikel 2 van de verordening genoemde financiële entiteiten. Dit zijn:

- kredietinstellingen;
- betalingsinstellingen;
- aanbieders van rekeninginformatiediensten;
- instellingen voor elektronisch geld;
- beleggingsondernemingen;
- aanbieders van cryptoactivadiensten;
- centrale effectenbewaarinstellingen;
- centrale tegenpartijen;
- handelsplatformen;
- transactieregisters;
- beheerders van alternatieve beleggingsfondsen;
- beheermaatschappijen;
- aanbieders van datarapporteringsdiensten;
- verzekerings- en herverzekeringsondernemingen;
- verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen;
- instellingen voor bedrijfspensioenvoorziening;
- ratingbureaus;
- beheerders van kritieke benchmarks;
- aanbieders van crowdfundingdiensten;
- securitisatieregisters;
- derde aanbieders van ICT-diensten.

Het toepassingsgebied van NIS2 en DORA overlappen elkaar voor bepaalde entiteiten die actief zijn in de sectoren van het bankwezen en de infrastructuur voor de financiële markt. De NIS2-richtlijn voorziet daarom in een *lex specialis-regel*: wanneer er op Europees niveau gelijkwaardige sectorale vereisten bestaan op het gebied van cyberbeveiliging en melding van significante incidenten, is de specifieke wettelijke norm (in dit geval de DORA-verordening) van toepassing in plaats van de algemene wettelijke norm (in dit geval de NIS2-richtlijn).

Echter, entiteiten in de sectoren van het bankwezen en de infrastructuur voor de financiële markt die onder het toepassingsgebied van zowel de DORA-verordening als de NIS2-richtlijn vallen, moeten zich op dezelfde manier registreren als de andere NIS2-entiteiten.

Ten slotte worden significante incidenten die door DORA-entiteiten worden gemeld, doorgestuurd naar de NIS2-autoriteiten.

1.11. Vallen kritieke infrastructuren (of kritieke entiteiten volgens de CER-richtlijn) onder het toepassingsgebied van de NIS2-wet?

Art. 9, 5° en 25, §2 NIS2-wet

De exploitant van een of meer kritieke infrastructuur(en) die is/zijn geïdentificeerd in het kader van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren (of als kritieke entiteiten in de zin van richtlijn 2022/2557 - CER-richtlijn) wordt beschouwd als een essentiële entiteit in de zin van de NIS2-wet.

De NIS2-autoriteiten en de bevoegde autoriteiten onder de wet van 1 juli 2011 (en de CER-richtlijn) werken samen om toezicht te houden op deze entiteiten.

Meer informatie over kritieke infrastructuren is te vinden op de website van het Nationaal Crisiscentrum.

1.12. Valt een onderwijsinstelling binnen het toepassingsgebied van de wet?

Bijlagen I en II & art. 8, 34° NIS2-wet

De onderwijssector wordt niet expliciet vermeld in de bijlagen I en II van de NIS2-wet.

Daarentegen kunnen publieke onderwijsinstellingen, zoals universiteiten of hogescholen, worden opgenomen in de definitie van een "overheidsinstantie". Daartoe moeten zij:

- voldoen aan het omvangscriterium (zie afdeling 1.3.);
- gevestigd zijn in België (zie afdeling 1.9.);
- voldoet aan de definitie van “overheidsinstantie” in artikel 8, 34° NIS2-wet;
- afhangen van de Federale Staat of van de deelstaten;

Daarnaast kan een onderwijsinstelling ook worden aangemerkt als "zorgaanbieder" in de zin van bijlage I van de NIS2-wet (bijvoorbeeld een universitair ziekenhuis).

1.13. Kunnen NACE-codes worden gebruikt om te bepalen of een entiteit onder de wet valt?

Bijlagen I en II NIS2-wet

Sommige van de in de bijlagen I en II opgenomen diensten verwijzen naar NACE-codes. In België gevestigde entiteiten die diensten verlenen die onder deze NACE-codes vallen, dienen daarom zorgvuldig na te gaan of de NIS2-wet niet op hen van toepassing is.

Voor alle entiteiten die niet in de bovenstaande categorie vallen, zijn NACE-codes geen geldige basis om te bepalen of een entiteit binnen de werkingssfeer van de NIS2-wet valt. Sommige NACE-codes kunnen indicatief door entiteiten worden gebruikt, maar verdere verificatie van hun

exacte economische activiteit is vereist om te bepalen of ze al dan niet binnen -het vaak restrictievere- toepassingsgebied van de NIS2-wet vallen.

1.14. Hoe wordt bepaald of een organisatie binnen het toepassingsgebied van de NIS2-wet valt?

De hieronder uiteengezette methode beschrijft in detail de verschillende stappen van de redenering met betrekking tot het toepassingsgebied van de NIS2-wet. Deze methode beoogt echter niet exhaustief te zijn en is niet de enige methode die kan worden gebruikt.

Dit onderdeel behandelt de volgende items:

1. Voorafgaand aan het analyseren van de NIS2-wet zelf:
    a. Exploiteert mijn organisatie een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren?
    b. Is mijn organisatie een aanbieder van essentiële diensten of een digitale-dienstverlener (NIS1-wet)?
2. Wat is de omvang van mijn organisatie?
3. Welke dienst(en) verleent mijn organisatie in de Europese Unie?
4. Waar in Europa is mijn organisatie gevestigd?
5. Kan mijn organisatie achteraf worden geïdentificeerd of zit mijn organisatie in de toeleveringsketen van een NIS2-entiteit?

Zie ook onze scope test tool.

1.14.1. Voorafgaand aan het analyseren van de NIS2-wet zelf

Voordat we overgaan tot de eigenlijke analyse, moeten we eerst kijken naar twee situaties die een grote invloed hebben op hoe het toepassingsgebied van de NIS2-wet werkt voor de betrokken organisaties.

A. Exploiteert mijn organisatie een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren?

Artikel 3, §4 van de NIS2-wet bepaalt dat de wet automatisch van toepassing is op entiteiten die worden geïdentificeerd als exploitanten van een kritieke infrastructuur in de zin van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren (en in de toekomst op kritieke entiteiten in de zin van de CER-richtlijn), ongeacht hun omvang.

Exploitanten van kritieke infrastructuur hoeven daarom niet te analyseren of hun organisatie binnen het toepassingsgebied van de NIS2 -richtlijn valt: zij worden automatisch aangemerkt als essentiële entiteiten.

B. Is mijn organisatie een aanbieder van essentiële diensten (AED) of een digitale-dienstverlener (DSP)?

Entiteiten die onder de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS1-wet) zijn geïdentificeerd als aanbieders van essentiële diensten (AED's) of die digitale-dienstverleners

(DSP's) uitmaakten, zullen onder de bepalingen van de NIS2-wet vallen. Het toepassingsgebied van de NIS2-richtlijn is gebaseerd op de sectoren die onder de NIS1-richtlijn vallen.

Bij gebrek aan formele identificatie door het CCB moeten aanbieders van essentiële diensten voldoen aan het omvangscriterium (zie volgend punt). Digitale-dienstverleners moesten daarentegen al minstens middelgroot zijn krachtens Aanbeveling 2003/361/EG.

1.14.2. Wat is de omvang van mijn organisatie?

Om binnen het toepassingsgebied van de NIS2-wet te vallen, moet een entiteit een bepaalde omvang hebben. Om deze omvang te berekenen, verwijst de NIS2-wet naar de Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen. Deze aanbeveling definieert de drempels vanaf wanneer een onderneming kan worden beschouwd als een kleine, middelgrote of grote onderneming. Op enkele uitzonderingen na vallen alleen middelgrote en grote ondernemingen onder het toepassingsgebied van de NIS2-wet.

Er moet aan twee voorwaarden worden voldaan om de omvang vast te stellen: het aantal werkzame personen (gemeten in arbeidsjaareenheden (AJE) [1]) en de financiële bedragen (jaaromzet en/of jaarlijks balanstotaal).

Het aantal werknemers moet worden gecombineerd met de financiële bedragen om de grootte van de onderneming te bepalen: een onderneming kan ervoor kiezen om ofwel aan het omzetplafond ofwel aan het balanstotaalplafond te voldoen. Ze **kan een van de financiële plafonds overschrijden zonder dat dit invloed heeft op haar KMO-status**. In principe houden we **daarom alleen rekening met het laagste van de twee** bedragen.

Voorbeeld 1: een onderneming met 35 AJE's (klein) heeft een jaaromzet van € 1.000.000 (klein) en een jaarlijks balanstotaal van € 50.000.000 (groot). Voor de financiële bedragen kiest ze ervoor om alleen rekening te houden met het kleinste: haar jaaromzet. Ze is dus een kleine of micro-onderneming.

Voorbeeld 2: een onderneming met 80 AJE's (middelgroot) heeft een jaaromzet van €1.000.000 (klein) en een jaarlijks balanstotaal van €70.000.000 (groot). Voor de financiële bedragen kiest ze ervoor om alleen rekening te houden met het kleinste bedrag: haar omzet. Aangezien de omzet klein is, maar het aantal werkzame personen middelgroot, is dit een middelgrote onderneming.

U vindt een visueel overzicht van de mogelijke groottes van ondernemingen op onze website.

Als we de verschillende mogelijke groottes combineren met het criterium van de verleende dienst, krijgen we het volgende toepassingsgebied:

- Een middelgrote onderneming heeft een aantal werkzame personen tussen de 50 en 249 AJE's of heeft een jaarlijkse omzet/balanstotaal van meer dan €10 miljoen euro:
  ➔ Ze valt binnen het toepassingsgebied als "belangrijke entiteit" als ze een dienst verleent die is opgenomen in bijlage II van de wet.

[1] De arbeidsjaareenheden (AJE's) komen overeen met het aantal personen dat het gehele desbetreffende jaar voltijds in de betrokken onderneming of voor rekening van deze onderneming heeft gewerkt. Het werk van personen die niet het gehele jaar hebben gewerkt, deeltijdwerk ongeacht de duur ervan en seizoenarbeid worden in breuken van AJE uitgedrukt.

➔ **In principe** valt ze binnen het toepassingsgebied als een "belangrijke entiteit" als ze een dienst verleent die wordt vermeld in bijlage I van de wet.

- Een grote onderneming heeft minstens 250 AJE's in dienst of heeft een jaaromzet van meer dan €50 miljoen en een jaarlijks balanstotaal van meer dan €43 miljoen:
  - ➔ Valt binnen het toepassingsgebied als "belangrijke entiteit" als ze een essentiële dienst verleent die wordt vermeld in bijlage II van de wet.
  - ➔ **In principe** valt ze binnen het toepassingsgebied als een "essentiële entiteit" als ze een dienst verleent die is opgenomen in bijlage I van de wet.

De Aanbeveling bepaalt in het bijzonder dat in het geval van entiteiten die samen als "verbonden ondernemingen" of "partnerondernemingen" zijn gegroepeerd, afhankelijk van de gedefinieerde criteria, de gegevens (aantal voltijdse werknemers & financiële bedragen) van de andere entiteiten die deel uitmaken van de groep entiteiten in aanmerking worden genomen om de omvang te berekenen (zie ook afdeling 1.3.).

Raadpleeg voor meer informatie over de toepassing van de Aanbeveling de Gebruikersgids bij de definitie van kmo's. Deze bevat alle criteria en visuele voorbeelden om u te helpen de Aanbeveling toe te passen. De Commissie heeft ook een hulpmiddel om de omvang van uw organisatie te bepalen.

Er zijn echter een paar **uitzonderingen**. De volgende soorten entiteiten vallen onder het toepassingsgebied van de NIS2-wet, ongeacht hun omvang:

- gekwalificeerde aanbieders van vertrouwensdiensten (essentieel);
- niet-gekwalificeerde aanbieders van vertrouwensdiensten (belangrijk als micro-, kleine, middelgrote ondernemingen en essentieel als grote ondernemingen);
- DNS-dienstverleners (essentieel);
- registers van topleveldomeinnamen (essentieel);
- domeinnaamregistratiediensten (alleen voor registratie);
- aanbieders van openbare elektronischecommunicatienetwerken (essentieel);
- aanbieders van openbare elektronischecommunicatiediensten (essentieel);
- entiteiten die op nationaal niveau als kritieke zijn geïdentificeerd volgens de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van kritieke infrastructuren (essentieel);
- overheidsinstellingen die afhankelijk zijn van de Federale Staat (essentieel).

In het volgende gedeelte wordt uitgelegd hoe u de definities van de diensten geleverd door deze soorten entiteiten kunt vinden.

1.14.3. Welke dienst(en) verleent mijn organisatie in de Europese Unie?

Als de omvang van een entiteit eenmaal bekend is, is het vervolgens noodzakelijk om een gedetailleerde analyse uit te voeren van alle diensten die de entiteit levert, per sector of subsector. Het is belangrijk om elke dienst in kaart te brengen, zelfs als het slechts een bijkomstige activiteit van de entiteit is (tenzij de definitie van de dienst rekening houdt met het feit of het de hoofd- of bijkomstige dienst is).

De bijlagen I en II (of definities) van de NIS2-wet geven details over de betreffende diensten ("type entiteit"), vaak met een verwijzing naar de overeenkomstige Europese wetgeving of naar de definities in artikel 8 van de wet.

De verschillende sectoren en subsectoren zijn de volgende:

Zeer kritieke sectoren (bijlage I)	Andere kritieke sectoren (bijlage II)
1. Energie a. Elektriciteit b. Stadsverwarming en -koeling c. Aardolie d. Aardgas e. Waterstof 2. Vervoer a. Lucht b. Spoor c. Water d. Weg 3. Bankwezen 4. Infrastructuur voor financiële markt 5. Gezondheidszorg 6. Drinkwater 7. Afvalwater 8. Digitale infrastructuur 9. Beheer van ICT-diensten (business-to-business) 10. Overheid 11. Ruimtevaart	1. Post- en koeriersdiensten 2. Afvalstoffenbeheer 3. Vervaardiging, productie en distributie van chemische stoffen 4. Productie, verwerking en distributie van levensmiddelen 5. Vervaardiging a. Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek b. Vervaardiging van informaticaproducten en van elektronische en optische producten c. Vervaardiging van elektrische apparatuur d. Vervaardiging van machines, apparaten en werktuigen, n.e.g. e. Vervaardiging van motorvoertuigen, aanhangers en opleggers f. Vervaardiging van andere transportmiddelen 6. Digitale aanbieders 7. Onderzoek

De diensten die de organisatie levert, moeten gelinkt worden aan de eerder vermelde definities. Aan de voorwaarde met betrekking tot de geleverde dienst is dus voldaan als er overeenstemming is tussen de twee. Het is heel goed mogelijk dat een organisatie meerdere van de genoemde diensten in verschillende sectoren levert (zie afdeling 1.6.).

Kortom, de "belangrijke" entiteiten en de "essentiële" entiteiten zijn als volgt: (met uitzondering van de type entiteiten aan het eind van afdeling 1.14.2. hierboven):

	Middelgroot bedrijf	Grote bedrijven
Diensten van bijlage I	Belangrijk	Essentieel
Diensten van bijlage II	Belangrijk	Belangrijk

1.14.4. De oprichting

In principe is de Belgische NIS2-wet van toepassing op entiteiten **die in België zijn gevestigd en die hun diensten of activiteiten binnen de EU verrichten**.

Het begrip vestiging impliceert eenvoudigweg de daadwerkelijke uitoefening van een activiteit door middel van stabiele regelingen, ongeacht de gekozen rechtsvorm, hetzij via de maatschappelijke zetel, hetzij via een filiaal, hetzij via een dochteronderneming met rechtspersoonlijkheid.

Afhankelijk van het type entiteit zijn er echter bepaalde uitzonderingen op de Belgische vestigingsregel. De regels met betrekking tot het territoriale toepassingsgebied van de Belgische NIS2-wet worden uitgelegd in afdeling 1.9.

1.14.5. Aanvullende identificatie en toeleveringsketen

Niettegenstaande de bovenvermelde regels kan het CCB, indien nodig, bepaalde entiteiten identificeren die in België gevestigd zijn en actief zijn in de sectoren opgesomd in de bijlagen bij de NIS2-wet. Deze bijkomende identificatie gebeurt in overleg met de betrokken organisatie - zie afdeling 1.8.

Ongeacht het toepassingsgebied van de NIS2-wet, mag niet worden vergeten dat een groot aantal organisaties indirect met deze nieuwe wettelijke vereisten te maken krijgt als ze deel uitmaken van de toeleveringsketen van een of meer NIS2-entiteiten. Deze laatste zijn verplicht om de beveiliging van hun eigen toeleveringsketen te garanderen en kunnen daarom contractuele verplichtingen opleggen aan hun directe leveranciers of dienstverleners. Zie paragraaf 3.8.

2. Overheidssector

2.1. Hoe is de wet van toepassing op de overheidssector?

Art. 8, 34° en bijlage I, sector 10 (Overheid) NIS2-wet

Art. 8, 34° van de wet definieert een "overheidsinstantie" als een administratieve overheid bedoeld in artikel 14, § 1, eerste lid, van de gecoördineerde wetten op de Raad van State die aan de volgende criteria voldoet:

a) zij is niet van industriële of commerciële aard;
b) zij oefent niet hoofdzakelijk een activiteit uit, opgesomd in de kolom soort entiteit van een andere sector of deelsector van een van de bijlagen;
c) zij is geen privaatrechtelijke rechtspersoon.

Voor de definitie van het begrip “overheidsinstantie” bepaalt artikel 6, 35) van de Richtlijn dat het begrip als zodanig moet worden erkend in overeenstemming met het nationale recht, met uitzondering van de rechterlijke macht, parlementen en centrale banken. Daarom is besloten om te verwijzen naar bestaande begrippen in het Belgische recht die de betrokken entiteiten dekken, om de toepassingen van verschillende begrippen niet te vermeerderen.

In dit geval is de definitie gebaseerd op het begrip administratieve overheid bedoeld in artikel 14, §1 , eerste lid, van de gecoördineerde wetten van 12 januari 1973 op de Raad van State, waaraan criteria zijn toegevoegd: zij mag niet van industriële of commerciële aard zijn, niet hoofdzakelijk een activiteit uitoefenen die tot een van de andere sectoren of deelsectoren opgenomen in de bijlagen bij de wet en geen privaatrechtelijke rechtspersoon zijn.

Deze definitie moet worden gecombineerd met de categorieën entiteittypen die zijn opgenomen in bijlage I, sector 10 (Overheid):

- Overheidsinstanties die van de Federale Staat afhangen;
- Overheidsinstanties die van de deelgebieden afhangen, geïdentificeerd overeenkomstig artikel 11, § 2, van de wet;
- De hulpverleningszones in de zin van artikel 14 van de wet van 15 mei 2007 betreffende de civiele veiligheid of de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp opgericht door de ordonnantie van 19 juli 1990 houdende oprichting van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp.

Het begrip afhangen volgt uit artikel 5 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens die het met name mogelijk maakt om entiteiten te omvatten die deel uitmaken van het federale en gefedereerde niveau, die door deze overheden zijn opgericht, waarvan de activiteiten in hoofdzaak door de overheden worden gefinancierd, waarvan het beheer onderworpen is aan het toezicht door deze overheden of instellingen, hetzij waarvan de leden van het bestuursorgaan, leidinggevend orgaan of toezichthoudend orgaan voor meer dan de helft door deze overheden of instellingen zijn aangewezen.

Zoals de definitie in art. 8, 34° aangeeft, is een overheidsinstantie die hoofdzakelijk een dienst verleent die is opgenomen in een andere sector of subsector van een van de bijlagen bij de wet (bijvoorbeeld een intercommunale die actief is in de energie- of drinkwatersector, een openbaar

ziekenhuis, een openbare instelling die ICT-diensten verleent, enz.) onderworpen aan de regels van die sector en niet aan die van de sector overheid.

2.2. Zijn lokale overheidsinstanties onderworpen aan de verplichtingen van de wet?

Art. 8, 34° Bijlage I, sector 10 (Openbaar bestuur) NIS2-wet

Lokale overheidsinstanties (gemeenten, provincies, intercommunales, OCMW's, enz.) zijn niet automatisch onderworpen aan de vereisten van de NIS2-wet. In overeenstemming met het beginsel van lokale autonomie dat is vastgelegd in artikel 162 van de Grondwet, mogen lokale besturen, ondanks de uitoefening van een toezichthoudende controle of hun financiering, niet worden beschouwd overheidsinstanties die van de federale staat of van de deelgebieden in de zin van bijlage I van de NIS2-wet.

Deze lokale entiteiten vallen echter onder de bepalingen van de NIS2-wet als ze een dienst verlenen die wordt genoemd in bijlage I of II van de wet en hun omvang groter is dan die van een kleine onderneming.

Lokale publieke entiteiten kunnen ook worden aangewezen door middel van artikel 11, § 1 (aanwijzing door de nationale cyberbeveiligingsautoriteit - CCB), op voorwaarde dat de raadplegingsprocedure worden nageleefd voorzien in artikel 11, § 3. Het initiatief voor een dergelijke aanwijzing kan worden genomen op verzoek van de nationale cyberbeveiligingsautoriteit, de betrokken entiteit of zelfs een gewest.

2.3. Zijn de verplichtingen van de wet van toepassing op de overheidsinstanties van de gewesten en de gemeenschappen?

Art. 11, §2-3 en bijlage I, sector 10 (Overheid) NIS2-wet

Gemeenschaps- en gewestelijke overheidsinstanties behoren tot de overheidsinstanties die onder de NIS2-wet vallen. De nationale cyberbeveiligingsautoriteit (CCB) moet echter eerst een formele identificatieprocedure uitvoeren. Dit houdt in dat op basis van een risicoanalyse wordt beoordeeld welke entiteiten diensten leveren waarvan de verstoring een aanzienlijke impact zou kunnen hebben op kritieke maatschappelijke of economische activiteiten.

In overeenstemming met artikel 11, § 2 en §3 van de NIS2-wet gebeurt deze identificatie in overleg met de betrokken publieke entiteiten en de regeringen van de gefedereerde entiteiten. Aan het einde van deze procedure kan de gewestelijke of gemeenschapsentiteit worden aangeduid als essentiële entiteit of belangrijke entiteit.

3. Verplichtingen

3.1. Wat zijn de wettelijke verplichtingen voor de betrokken entiteiten?

De NIS2-wet legt een aantal verplichtingen op aan essentiële en belangrijke entiteiten:

- het nemen van passende cyberbeveiligingsmaatregelen;
- de tijdige melding van significante incidenten;
- de registratie bij de bevoegde autoriteiten;
- de opleiding van bestuursorganen (paragraaf 4.13.);
- de periodieke conformiteitsbeoordelingen (verplicht voor essentiële entiteiten en vrijwillig voor belangrijke entiteiten);
- informatie-uitwisseling en samenwerking met de relevante autoriteiten.

Deze verschillende verplichtingen worden in de volgende afdeling uitgelegd.

3.2. Wat zijn de verplichtingen op het gebied van cyberbeveiligingsmaatregelen?

Art. 30, 31 en 42 NIS2-wet

Kritieke en belangrijke entiteiten moeten passende en evenredige (technische, operationele en organisatorische) maatregelen nemen om de risico's te beheersen die een bedreiging vormen voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten gebruiken bij het uitvoeren van hun activiteiten of het verlenen van hun diensten, en om de gevolgen van incidenten voor de ontvangers van hun diensten en op andere diensten weg te nemen of te beperken.

Het is belangrijk om te benadrukken dat, in tegenstelling tot de NIS1-wet, het **toepassingsgebied van de NIS2-wet de hele betrokken entiteit omvat** en niet alleen de activiteiten die zijn opgenomen in de bijlagen bij de wet.

Om de praktische uitvoering van deze cyberbeveiligingsmaatregelen te vergemakkelijken, heeft het CCB al een raamwerk ontwikkeld en gratis ter beschikking gesteld aan de betrokken entiteiten: het Cyberfundamentals Framework "(CyFun®) met verschillende niveaus en een analysetool om het meest geschikte niveau te bepalen. De wet en het uitvoeringsbesluit bieden essentiële en belangrijke entiteiten die besluiten het CyFun®-kader of de internationale norm ISO/IEC 27001 (met het toepassingsgebied in lijn met NIS2 - d.w.z. alle netwerk- en informatiesystemen) te gebruiken, een **vermoeden van conformiteit** met betrekking tot beveiligingsmaatregelen.

Opgemerkt moet worden dat het CyFun®-kader van het CCB is afgestemd op het werk van de NIS samenwerkingsgroep op dit gebied.

De minimummaatregelen in de wet zijn gebaseerd op een "*all-risk*"-benadering die erop gericht is netwerk- en informatiesystemen en hun fysieke omgeving te beschermen tegen incidenten, en omvatten ten minste het volgende:

1. beleid inzake risicoanalyse en beveiliging van informatiesystemen;

2. incidentenbehandeling;
3. bedrijfscontinuïteit, zoals back-upbeheer, noodvoorzieningenplannen en crisisbeheer;
4. de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
5. beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
6. beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
7. basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
8. beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
9. beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
10. wanneer gepast, het gebruik van multifactorauthenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit;
11. een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden.

De door kritieke en belangrijke entiteiten te nemen maatregelen moeten **passend en evenredig** zijn. Op dit punt is het belangrijk te specificeren dat, om onevenredige financiële en administratieve lasten voor kritieke en belangrijke entiteiten te vermijden, de maatregelen voor risicobeheer op het gebied van cyberbeveiliging **evenredig moeten zijn met de risico's waaraan** het netwerk- en informatiesysteem in kwestie zijn blootgesteld. In dit verband moeten entiteiten met name rekening houden met **de stand van de techniek** van deze maatregelen en, indien van toepassing, met relevante Europese of internationale **normen**, en met de **kosten van de tenuitvoerlegging van** deze maatregelen.

3.3. Wat zijn de verplichtingen voor het melden van incidenten?

3.3.1. Algemene regels

Art. 8, 5° en 57°; 34 en 35 NIS2-wet

Een incident wordt door de wet gedefinieerd als *" een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt"*.

In het geval van een significant incident, moet de entiteit dit aan het nationale CSIRT (CCB) melden en in bepaalde gevallen ook aan de ontvangers van hun diensten.

De melding vindt plaats in verschillende fasen (zie afdeling 3.3.3): eerst een vroegtijdige waarschuwing binnen 24 uur nadat het incident is ontdekt (*early warning*), vervolgens een formele incidentmelding binnen 72 uur nadat het incident is ontdekt (*initial assessment of the incident*) en tot slot een eindverslag uiterlijk 1 maand na de incidentmelding (*final report*). Tussenin, kan het nationale CSIRT om tussentijdse verslagen verzoeken.

Een significant incident wordt gedefinieerd als: "*elk incident dat significante gevolgen heeft voor de verlening van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II van de wet en dat:*

1. *een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of*
2. *andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.*"

In de praktijk zal het CCB aanbevelingen doen over wanneer een melding vereist is en over de te volgen procedure.

3.3.2. Ontvangers van een verplichte melding van een significant incident

In principe moet elke NIS2-entiteit een incident enkel melden aan het CCB. Het CCB stuurt de meldingen door naar eventuele sectorale overheden en naar het crisiscentrum (voor essentiële entiteiten).

Art. 34, §1 NIS2-wet

Er is echter een uitzondering op deze regel voor entiteiten in de sector bankwezen en sector infrastructuur voor de financiële markt die onder de DORA-verordening vallen. Entiteiten in deze twee sectoren melden hun incident, naargelang het geval, bij de Nationale Bank van België (NBB) of de Autoriteit voor Financiële Diensten en Markten (FSMA), die de incidentmelding automatisch doorsturen naar het CCB.

In voorkomend geval stellen de betrokken entiteiten de ontvangers van hun diensten onverwijld in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van hun diensten. De entiteit deelt ontvangers van hun diensten die mogelijkerwijs door een significante cyberdreiging worden getroffen, onverwijld mee welke maatregelen en correcties die ontvangers kunnen nemen in reactie op die dreiging.

Art. 34, §2 NIS2-wet

3.3.3. Procedure voor het melden van incidenten

De melding van significante incidenten verloopt in verschillende fasen:

Art. 35 NIS2-wet

1. onverwijld en in elk geval binnen **24 uur** nadat zij kennis hebben gekregen van het significante incident, bezorgt de entiteit een vroegtijdige waarschuwing;
2. onverwijld en in elk geval binnen **72 uur** (24 uur voor aanbieders van vertrouwensdiensten) nadat zij kennis hebben gekregen van het significante incident, bezorgt de entiteit een incidentmelding
3. **op verzoek van** het nationale CSIRT of van de eventuele betrokken sectorale overheid, bezorgt de entiteit een tussentijds verslag;
4. uiterlijk **één maand** na de in 2. bedoelde incidentmelding stuurt de entiteit een eindverslag;
5. als het eindverslag niet kan worden verstuurd omdat het incident nog aan de gang is, bezorgt de entiteit een voortgangsverslag en vervolgens, binnen een maand na de definitieve afhandeling van het incident, het eindverslag.

In de praktijk vindt de melding plaats via de procedure op de website van het CCB.

3.3.4. Informatie die moet worden verstrekt bij het melden van een incident

In de verschillende stadia van de melding worden verschillende soorten informatie doorgegeven:

Art. 35 NIS2-wet

- De vroegtijdige waarschuwing geeft aan of het vermoeden bestaat dat het significante incident veroorzaakt is door een onrechtmatige of kwaadwillige handeling en of het grensoverschrijdende gevolgen kan hebben. Deze vroegtijdige waarschuwing bevat alleen de informatie die nodig is om het incident onder de aandacht van het CSIRT te brengen en stelt de betrokken entiteit in staat om zo nodig om bijstand te vragen.
  Een dergelijke waarschuwing mag de middelen van de meldende entiteit niet afleiden van activiteiten op het gebied van incidentenbeheer die prioriteit zouden moeten hebben, om te voorkomen dat de meldingsplicht voor incidenten middelen afleidt van het beheer van significante incidenten of anderszins de inspanningen van de entiteit op dit gebied in gevaar brengt.
- Het doel van de incidentmelding binnen 72 uur is het actualiseren van de informatie die is gecommuniceerd als onderdeel van de vroegtijdige waarschuwing. Het biedt ook een eerste beoordeling van het incident, inclusief de ernst en de gevolgen ervan, evenals indicatoren van aantasting, indien beschikbaar.
  Net als bij vroegtijdige waarschuwing mag de melding van incidenten geen beslag leggen op de middelen van de entiteit, om te voorkomen dat de meldingsplicht middelen afleidt van het beheer van significante incidenten of anderszins de inspanningen van de entiteit op dit gebied in gevaar brengt.
- Het tussentijds verslag bevat relevante updates over de situatie.
- Het eindverslag moet een gedetailleerde beschrijving van het incident bevatten, inclusief de ernst en de gevolgen ervan; het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid; de toegepaste en lopende risicobeperkende maatregelen; en in voorkomend geval, de grensoverschrijdende gevolgen van het incident.
- Het voortgangsverslag bevat zoveel mogelijk van de informatie die in het eindverslag zou moeten staan en die in het bezit is van de entiteit op het moment dat het voortgangsverslag wordt ingediend.

3.3.5. Vertrouwelijkheidsregels die van toepassing zijn op informatie die wordt uitgewisseld tijdens een incident

De NIS2-entiteit en haar onderaannemers beperken de toegang tot informatie met betrekking tot incidenten, in de zin van de NIS2-wet, tot alleen die personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de uitvoering van deze wet.

Art. 26, §3-4 NIS2-wet

Deze regel geldt ook voor het CCB (nationale CSIRT), het NCCN en de sectorale overheid.

Informatie die door een NIS2-entiteit aan het CCB, het NCCN en de sectorale overheid wordt verstrekt, kan worden uitgewisseld met autoriteiten in andere EU-lidstaten en met andere Belgische autoriteiten wanneer dit noodzakelijk is voor de toepassing van wettelijke bepalingen.

Deze overdracht van informatie is echter beperkt tot wat relevant en evenredig is met het doel van de uitwisseling, in overeenstemming met EU-verordening 2016/679 (AVG), de vertrouwelijkheid

van de betreffende informatie en de beveiligings- en commerciële belangen van de NIS2-entiteiten.

3.4. Wat gebeurt er als er zich een incident voordoet waarbij ook persoonlijke gegevens betrokken zijn?

Zoals nu ook het geval is, gaan de meldingen van incidenten in het kader van de wet niet de eventuele meldingen bij een inbreuk in verband met persoonsgegevens vervangen, bijvoorbeeld aan de gegevensbeschermingsautoriteit. Er zullen nog steeds twee aparte meldingen nodig zijn.

De wet voorziet echter in een nauwere samenwerking tussen de nationale cyberbeveiligingsautoriteit en de gegevensbeschermingsautoriteiten. Deze samenwerking zou kunnen leiden tot de ontwikkeling van gemeenschappelijke instrumenten.

Een melding aan het GBA gebeurt via hun website.

3.5. Is het mogelijk om incidenten of cyberdreigingen vrijwillig te melden?

Ja, het nationale CSIRT (CCB) kan ook, op vrijwillige basis, meldingen van incidenten, cyberdreigingen of vermeden incidenten ontvangen van entiteiten die al dan niet onder de NIS2-wet vallen.

Art. 38 NIS2-wet

Zie in dit verband de procedure uitgelegd in afdeling 3.3.

3.6. Wat zijn de wettelijke voorwaarden om gebruik te maken van het beschermend kader bij het onderzoeken en rapporteren van kwetsbaarheden (ethisch hacken)?

De NIS2-wet bevat de bepalingen van de NIS1-wet, die een beschermend kader (*safe harbour)* biedt voor "ethische hackers" of "digitale klokkenluiders".

Art. 22 en 23 NIS2-wet

Om van dit kader te kunnen profiteren, moet de persoon:

- Handelen zonder bedrieglijk opzet of het oogmerk om te schaden;
- Binnen 24 uur na de ontdekking van de kwetsbaarheid een vereenvoudigde melding naar zowel het nationale CSIRT als de verantwoordelijke organisatie sturen;
- Binnen 72 uur na de ontdekking een volledige kennisgeving sturen naar dezelfde ontvangers;
- Zich onthouden van verder te gaan dan wat nodig en evenredig is om het bestaan van een kwetsbaarheid na te gaan en te melden;
- Zich onthouden een kwetsbaarheid openbaar te maken zonder toestemming van het nationale CSIRT.

Bovendien moeten ethische hackers om kwetsbaarheden te kunnen onderzoeken op netwerk- en informatiesystemen van bepaalde organisaties (zoals inlichtingendiensten, defensie, rechterlijke

instanties..) en de informatie die door hen of namens hen wordt verwerkt, voorafgaandelijk een schriftelijke overeenkomst sluiten met deze organisaties.

Op haar website biedt het CCB algemene informatie over ethisch hacken met inbegrip van een pagina gewijd aan de bekendmaking van kwetsbaarheden.

3.7. Hoe worden NIS2-entiteiten geregistreerd?

Essentiële en belangrijke entiteiten moeten zich registreren op het CCB-portaal, Safeonweb@Work.

Art. 13 NIS2-wet

De termijn voor registratie hangt af van het type entiteit. In principe hebben essentiële en belangrijke entiteiten, evenals aanbieders van domeinnaamregistratiediensten, **5 maanden de tijd** om zich te registreren nadat de wet in werking is getreden, d.w.z. uiterlijk **18 maart 2025**. Bij de registratie moeten zij de volgende informatie verstrekken:

1. hun naam en hun registratienummer bij de KBO of een gelijkwaardige inschrijving in de Europese Unie;
2. hun adres en hun actuele contactgegevens, waaronder hun e-mailadres, hun IP-bereiken en hun telefoonnummer;
3. indien van toepassing, de relevante sector en deelsector bedoeld in bijlage I of II van de wet;
4. indien van toepassing, een lijst van de lidstaten waar zij diensten verlenen die binnen het toepassingsgebied van deze wet vallen

Er bestaat een uitzondering voor entiteiten die deze informatie al hebben doorgegeven aan een NIS2 sectorale overheid op grond van een wettelijke verplichting. In dit geval hoeft de informatie alleen maar te worden aangevuld bij autoriteit. Als de informatie verandert, moet dit binnen twee weken worden doorgegeven.

Voor de volgende soorten entiteiten bestaat een licht aangepaste regeling:

Art. 14 NIS2-wet

- DNS-dienstverleners;
- registers voor topleveldomeinnamen;
- entiteiten die domeinnaamregistratiediensten verlenen;
- 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;
- aanbieders van platformen voor socialenetwerkdiensten.

Zij moeten zich binnen **2 maanden** na de inwerkingtreding van de wet, d.w.z. uiterlijk **18 december 2024**, registreren en de volgende informatie verstrekken:

1. hun naam;

2. hun relevante sector, deelsector en soort entiteit bedoeld in bijlage I of II, waar van toepassing;
3. het adres van hun hoofdvestiging en hun andere wettelijke vestigingen in de Unie of, indien deze niet in de Unie zijn gevestigd, van hun vertegenwoordiger;
4. hun actuele contactgegevens, met inbegrip van e-mailadressen en telefoonnummers en, indien van toepassing van hun vertegenwoordiger;
5. de lidstaten waar ze hun diensten verlenen die tot het toepassingsgebied van deze wet behoren;
6. hun IP-bereiken.

Ze moeten het CCB ook in kennis stellen van wijzigingen van deze informatie.

3.8. Hoe kan een entiteit zijn relaties met leveranciers en direct dienstverleners beheren (toeleveringsketen/*supply chain*)?

Entiteiten die onder de NIS2-wet vallen, moeten passende en evenredige maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen.

Art. 30, §3, 4° NIS2-wet

Een van deze maatregelen is de beveiliging van de toeleveringsketen van de entiteit, met inbegrip van de beveiligingsgerelateerde aspecten met betrekking tot de relatie tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners.

Hoewel de vereisten van de NIS2-wet alleen van toepassing zijn op NIS2-entiteiten, moeten zij er toch voor zorgen dat hun rechtstreekse leveranciers en dienstverleners soortgelijke maatregelen treffen. Om de naleving van haar wettelijke verplichtingen te garanderen, kan een NIS2-entiteit contractueel van haar leveranciers of dienstverleners eisen dat zij beschikken over een van de certificeringen die krachtens de NIS2-wet zijn erkend: CyFun® of ISO 27001.

3.9. Hoe vertrouwelijk is de uitgewisselde informatie?

Bevoegde autoriteiten, essentiële of belangrijke entiteiten en hun onderaannemers beperken de toegang tot informatie in het kader van de NIS2-wet tot de personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de uitvoering van deze wet.

Art. 26 NIS2-wet

De informatie die door essentiële of belangrijke entiteiten aan de bevoegde autoriteiten wordt verstrekt mag niettemin worden uitgewisseld met autoriteiten van de Europese Unie, Belgische of buitenlandse autoriteiten, wanneer die uitwisseling noodzakelijk is voor de toepassing van wettelijke bepalingen.

De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling, met name overeenkomstig Verordening (EU) 2016/679 (AVG). Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de beveiligings- en commerciële belangen van essentiële of belangrijke entiteiten beschermd.

De wet voorziet echter wel in de mogelijkheid om op vrijwillige basis informatie uit te wisselen die relevant is voor cyberbeveiliging, met

Art. 27 NIS2-wet

inbegrip van informatie over cyberdreigingen, bijna-incidenten, kwetsbaarheden enz. Deze uitwisseling vindt onder bepaalde voorwaarden plaats in het kader van gemeenschappen voor informatie-uitwisseling, die wordt uitgevoerd door middel van informatie-uitwisselingsregelingen.

4. Controle/ Toezicht

4.1. Wie zijn de bevoegde autoriteiten?

Art. 15, 16 e.v. NIS2-wet en art. 3 koninklijk besluit NIS2

4.1.1. Het Centrum voor Cybersecurity België (CCB)

De nationale cyberbeveiligingsautoriteit (CCB) is verantwoordelijk voor de opvolging, de coördinatie van en het toezicht op de wet. Daartoe combineert de wet de bestaande taken van het CCB met de aanvullingen van de NIS2-richtlijn, met name wat betreft het toezicht op entiteiten. Het CCB is verantwoordelijk voor het toezicht op essentiële en belangrijke entiteiten (met de hulp van de sectorale overheden) en is het centrale contactpunt voor de implementatie van NIS2.

Het nationale computer security incident response team (CSIRT) maakt ook deel uit van de nationale cyberbeveiligingsautoriteit. NIS2-entiteiten zijn verplicht significante incidenten aan dit CSIRT te melden.

4.1.2. De sectorale overheden

De volgende sectorale overheden werden aangewezen:

1. **voor de sector energie**: de federale minister bevoegd voor Energie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de minister per deelsector een andere gemachtigde aanwijzen);
2. **voor de sector vervoer**:
    a. Wat betreft de sector vervoer, met uitzondering van het vervoer over water: de federale minister bevoegd voor Vervoer of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de minister per deelsector een andere gemachtigde aanwijzen);
    b. Wat betreft het vervoer over water: de federale minister bevoegd voor Maritieme Mobiliteit of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie (in voorkomend geval kan de minister per deelsector een andere gemachtigde aanwijzen);
3. **voor de sector gezondheidszorg**:
    a. wat betreft entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen; entiteiten die farmaceutische basisproducten en farmaceutische preparaten vervaardigen; en entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd: het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten (FAGG);
    b. de federale minister bevoegd voor Volksgezondheid of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;
4. **voor de sector digitale infrastructuur:** Belgisch Instituut voor postdiensten en telecommunicatie (BIPT);

5. **voor wat betreft de verleners van vertrouwensdiensten**: e federale minister bevoegd voor Economie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;
6. **voor de sector digitale aanbieders**: de federale minister bevoegd voor Economie of, bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;
7. **voor de sector ruimtevaart en de sector onderzoek**: de federale minister van Wetenschapsbeleid of bij delegatie door deze laatste, een leidend personeelslid van zijn/haar administratie;
8. **voor drinkwater**: het Nationaal Comité voor de beveiliging van de levering en distributie van drinkwater
9. **voor de sector bankwezen**: de Nationale Bank van België (NBB);
10. **voor de sector infrastructuur voor de financiële markt**: de Autoriteit voor Financiële Diensten en Markten (FSMA);
11. **voor de deelsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek**: het Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten.

Sectorale overheden hebben een aantal bevoegdheden. Voor meer informatie, zie afdeling 4.5.

Entiteiten die onder een sectorale overheid vallen, kunnen er terecht voor informatie, bijstand, enz.

4.1.3. Het Nationaal Crisiscentrum (NCCN)

Het Nationaal Crisiscentrum is ook betrokken bij de implementatie van de NIS2-wet, met name wat betreft de melding van incidenten, cybercrisisbeheer en de fysieke beveiligingsmaatregelen die worden genomen door exploitanten van kritieke infrastructuur en kritieke entiteiten (die onder de CER-richtlijn vallen).

4.2. Kunnen bepaalde referentiekaders door NIS2-entiteiten worden gebruikt om hun conformiteit aan te tonen?

Essentiële entiteiten die onderworpen zijn aan een periodieke conformiteitsbeoordelingsverplichting kunnen ervoor kiezen om een van de twee referentiekaders te gebruiken die worden opgesomd in het Koninklijk Besluit NIS2.

Art. 5, §1 Koninklijk besluit NIS2

Het gebruik van deze referentiekaders voor controle wordt uitgelegd in de volgende afdeling (4.3.).

4.2.1. Het CyberFundamentals (CyFun®)-raamwerk

Het CyberFundamentals-raamwerk (*Cyberfundamentals Framework)* is ontwikkeld door het CCB en is gebaseerd op verschillende veelgebruikte cyberbeveiligingsraamwerken of -standaarden, waaronder NIST CSF, ISO 27001/ ISO 27002, CIS Controls en IEC 62443.

Het omvat het startersniveau Small en de verschillende zekerheidsniveaus: Basic, Important en Essential (om zo goed mogelijk in te spelen op de risico's waaraan een organisatie kan worden blootgesteld). Met behulp van een tool kun je het meest geschikte niveau selecteren.

Dit raamwerk is openbaar en gratis beschikbaar op onze Safeonweb@Work-website.

4.2.2. ISO/IEC 27001

De Europese norm ISO/IEC 27001 is een internationaal erkende technische norm die de algemene en gestructureerde aanpak beschrijft voor het beveiligingsbeheer van elk informatiesysteem. Ze is daarom een basisnorm die de algemene principes uiteenzet voor het implementeren van beveiligingsmaatregelen voor informatiesystemen en ze is van toepassing op alle sectoren.

De laatste versie dateert van 2022, maar ze is zonder datumaanduiding in het koninklijk besluit opgenomen, zodat de meest recente versie altijd kan worden toegepast.

4.3. Hoe worden de betrokken entiteiten gecontroleerd?

Art. 39 e.v. NIS2-wet
Art. 6-13 Koninklijk besluit NIS2

Wanneer we het hebben over controle/toezicht in de context van de wet, moeten we een onderscheid maken tussen twee categorieën entiteiten: essentiële entiteiten en belangrijke entiteiten.

Essentiële entiteiten moeten een periodieke conformiteitsbeoordeling ondergaan. Deze beoordeling wordt uitgevoerd op basis van een keuze die de entiteit maakt uit drie opties:

- Een CyberFundamentals (CyFun®) certificering toegekend door een conformiteitsbeoordelingsinstantie (CAB) erkend door het CCB (na accreditatie door BELAC);
- Een ISO/IEC 27001-certificering, toegekend door een conformiteitsbeoordelingsinstantie die is geaccrediteerd door een accreditatie-instelling die de overeenkomst inzake wederzijdse erkenning (*Mutual Recognition Agreement)* (MLA) voor de ISO 27001-norm in het kader van de Europese samenwerking voor accreditatie (*European co-operation for Accreditation*) (EA) of het International Accreditatie Forum (IAF) heeft ondertekend, en die is erkend door het CCB;
- of een inspectie door de inspectiedienst van het CCB (of door een sectorale inspectiedienst).

De inspectiedienst kan ook op elk moment controles uitvoeren op essentiële entiteiten (zonder incident - *ex ante* - en na een incident of als er voldoende bewijs van niet-naleving van de wet beschikbaar is - *ex post*).

Voor belangrijke entiteiten wordt het toezicht alleen "*ex post*" uitgevoerd door de inspectiedienst, d.w.z. na een incident of op basis van bewijzen, aanwijzingen of informatie dat een belangrijke entiteit haar verplichtingen niet nakomt (art. 48, § 2 NIS2-wet). In principe zijn ze dus niet onderworpen aan een periodieke conformiteitsbeoordeling. Deze entiteiten kunnen zich echter vrijwillig onderwerpen aan hetzelfde regime als essentiële entiteiten.

Voor de modaliteiten van de inspectie uitgevoerd door de inspectiedienst, zie afdeling 4.10.

4.4. Wat is een conformiteitsbeoordelingsinstantie (CAB)?

Een Conformiteitsbeoordelingsinstantie (in het Engels: *Conformity assessment body*- "CAB") is een instantie die verantwoordelijk is voor het controleren en certificeren van de naleving van de in het CyFun®-referentiekader of de ISO 27001-norm (toegepast in het kader van de NIS2-wet) vastgestelde eisen door NIS2-entiteiten die onderworpen zijn aan de periodieke conformiteitsbeoordeling (verplicht voor essentiële entiteiten, vrijwillig voor belangrijke entiteiten).

Voor CyFun®, is deze conformiteitsbeoordelingsinstantie geaccrediteerd door de Belgische Accreditatie-instelling (BELAC) en erkend door het CCB. Voor ISO 27001 is deze conformiteitsbeoordelingsinstantie geaccrediteerd door een accreditatie-instelling die de overeenkomst inzake wederzijdse erkenning *(Mutual Recognition Agreement)* (MLA) voor de ISO 27001-norm heeft ondertekend in het kader van de Europese samenwerking voor accreditatie (*European co-operation for Accreditation)* (EA) of het Internationaal Accreditatie Forum (IAF) en erkend door het CCB.

De CAB's spelen een belangrijke rol in onze economie door ervoor te zorgen dat ondernemingen voldoen aan de wettelijke vereisten die aan hen worden opgelegd.

4.5. Wat zijn de taken van de sectorale overheden?

De sectorale overheden spelen ook een rol in de NIS2-wet, vanwege hun kennis en specifieke expertise in elk van de betrokken sectoren. Waar nodig kunnen zij worden betrokken bij de volgende taken:

Art. 11, 13, 24, 25, 33, 34, 39, 44, 51 en 52 NIS2-wet

- Aanvullende identificatie (raadplegen en voorstellen);
- Registratie van entiteiten;
- Organisatie van sectorale oefeningen;
- De gevolgen van een incident voor een sector analyseren en beheren;
- Deelname aan bepaalde werkzaamheden van de NIS samenwerkingsgroep;
- Bewustmaking van entiteiten in hun sector;
- Samenwerking op nationaal niveau;
- Bijkomende maatregelen voor het beheer van cyberbeveiligingsrisico's;
- Melding van incidenten (doorgifte van de melding van significante incidenten aan de sectorale autoriteiten, raadpleging bij verschillende situaties met betrekking tot dit onderwerp)
- Toezicht en inspectie (gezamenlijk of gedelegeerd);
- Administratieve geldboetes.

4.6. Hoe kan een entiteit bewijzen dat ze haar verplichtingen naleeft?

In het kader van de periodieke conformiteitsbeoordeling - die verplicht is voor essentiële entiteiten - zal de entiteit een certificering of label kunnen krijgen, waardoor, tot bewijs van het tegendeel, kan worden

Art. 42 NIS2-wet

Art. 5, §1 Koninklijk besluit NIS2

vermoed dat de entiteit voldoet aan haar verplichtingen op het gebied van cyberbeveiliging.

Deze certificering zal gebaseerd zijn op de twee normen die in het koninklijk besluit worden genoemd: de CyberFundamentals of de internationale norm ISO 27001 (met het juiste toepassingsgebeid en *Statement of Applicability*). Zie in dit verband ook afdeling 4.2.

Uiteraard kan een entiteit ook een ander referentiekader of een andere technische norm gebruiken om haar wettelijke cyberbeveiligingseisen te implementeren. In dat geval geldt het vermoeden van conformiteit niet en moet de entiteit aan de inspectiedienst aantonen dat zij alle vereiste maatregelen toepast, op basis van een concordantietabel (*mapping*) met een van de twee bovengenoemde referentiekaders.

4.7. Kan een entiteit een CyFun®-zekerheidsniveau gebruiken dat lager is dan het niveau dat aan haar entiteitscategorie is toegewezen?

Art. 7 Koninklijk Besluit NIS2

Ja, het koninklijk besluit laat een entiteit toe om een lager CyFun®-niveau te gebruiken (bijvoorbeeld het gebruik van het zekerheidsniveau Important voor een essentiële entiteit) op voorwaarde dat ze dit objectief kan rechtvaardigen op basis van haar risicoanalyse. Deze keuze blijft de exclusieve volledige verantwoordelijkheid van de entiteit in kwestie en heeft geen impact op haar wettelijke kwalificatie als een essentiële of belangrijke entiteit. Er moet worden benadrukt dat deze keuze op elk moment in vraag kan worden gesteld door de inspectiedienst in het kader van zijn controleopdrachten.

Het CCB biedt een tool voor risicobeoordeling aan op Safeonweb@Work zodat een entiteit een geïnformeerde keuze kan maken over Cyfun® zekerheidsniveau dat zij nodig heeft.

4.8. Kan een entiteit die een aanbieder van essentiële diensten (AED) uitmaakte onder NIS1 haar ISO27001-certificering behouden?

Art. 8, 12 en 14-15 Koninklijk besluit NIS2

Als een entiteit die onder NIS1 een aanbieder van essentiële diensten (AED) uitmaakte, een ISO 27001-certificering heeft, kan hij zijn certificering gebruiken als onderdeel van een periodieke conformiteitsbeoordeling in het kader van NIS2. Indien nodig moet het toepassingsgebied van de certificering worden uitgebreid om ervoor te zorgen dat deze alle netwerk- en informatiesystemen van de betreffende entiteit omvat.

De certificering moet worden uitgevoerd door een conformiteitsbeoordelingsinstantie die is geaccrediteerd door BELAC in België (of door een andere geaccrediteerde Europese nationale instantie als deze certificering afkomstig is uit een andere lidstaat) en die is erkend door het CCB.

4.9. Wanneer moeten de betrokken entiteiten de verplichtingen van de wet toepassen?

Art. 13 & 75 NIS2-wet
Art. 22-23 Koninklijk besluit NIS2

De NIS2-wet en het bijhorend koninklijk besluit treden in werking op 18 oktober 2024. Bijgevolg, en behoudens uitzonderingen, zullen **alle verplichtingen** van de wet en het KB **vanaf die datum** van toepassing zijn op essentiële en belangrijke entiteiten (cyberbeveiligingsmaatregelen, melding van incidenten, enz.).

In afwijking hiervan zal de registratieverplichting geleidelijk worden ingevoerd. Het tijdsbestek hangt af van het type entiteit (zie afdeling 3.7):

- In principe hebben entiteiten **5 maanden de tijd** om zich te registreren nadat de wet van kracht is geworden.
- Voor entiteiten in bepaalde informatie- en communicatietechnologiesectoren (cloudcomputingdiensten, DNS-dienstverleners, aanbieders van datacentrumdiensten, enz.) is de uiterste termijn voor registratie **2 maanden** na de inwerkingtreding van de wet.

In afwijking hiervan zal de regelmatige conformiteitsbeoordeling van essentiële entiteiten ook geleidelijke en gedifferentieerd worden ingevoerd, afhankelijk van het gekozen referentiekader:

- **18 maanden na de inwerkingtreding van de wet**, d.w.z. vóór 18 april 2026:
  - Degenen die bepalen dat ze moeten voldoen aan het CyFun® Basic of Important zekerheidsniveau moeten een verificatie laten uitvoeren door een voor CyFun® geaccrediteerde en erkende CAB. Degenen die bepalen dat ze moeten voldoen aan het CyFun® Essential zekerheidsniveau moeten ook een dergelijke Important of Basic verificatie laten uitvoeren;
  - Degenen die gekozen hebben voor ISO 27001 certificering moeten het toepassingsgebied en de verklaring van toepasselijkheid aan het CCB overmaken;
  - Degenen die hebben gekozen voor inspectie door het CCB moeten de CyFun® self-assessment of het beveiligingsbeleid voor de netwerk- en informatiesystemen, het toepassingsgebied en de ISO 27001 verklaring van toepasselijkheid indienen bij het CCB.
- **30 maanden na de inwerkingtreding van de wet**, d.w.z. vóór 18 april 2027:
  - Degenen die bepalen dat ze moeten voldoen aan het zekerheidsniveau CyFun® Essential moeten, in aanvulling op de hierboven genoemde Basic of Important verificatie, certificering verwerven van een geaccrediteerde en erkende CAB voor CyFun®;
  - Degenen die hebben gekozen voor ISO 27001 certificering moeten certificering verkrijgen van een geaccrediteerde en erkende CAB voor ISO 27001;
  - Degenen die hebben gekozen voor inspectie door het CCB moeten een stand van zaken van de voorgang van het conformiteitsproces indienen.

Belangrijke entiteiten zijn niet onderworpen aan een verplichte regelmatige conformiteitsbeoordeling (toezicht *ex-post*). Om ervoor te zorgen dat de cyberbeveiligingsmaatregelen passend en evenredig zijn, zal de inspectiedienst toezicht houden op belangrijke entiteiten, met inachtneming van een vergelijkbare periode van 18 maanden na de inwerkingtreding van de wet (om hen in staat te stellen volledig het vereiste niveau te bereiken).

Als zich bijvoorbeeld begin 2025 een significant cyberincident voordoet, zal de entiteit in kwestie de nodige maatregelen moeten nemen om dit te beheren en aan het CCB te melden, mogelijk onder toezicht van de bevoegde inspectiediensten. We moedigen alle NIS2-entiteiten daarom aan om niet te wachten tot de registratiedeadline en hun eerste conformiteitsbeoordelingen om de vereiste maatregelen te implementeren.

4.10. Wat zijn de modaliteiten van de inspectie?

Art. 44 e.v. NIS2-wet

De inspectiedienst van de nationale cyberbeveiligingsautoriteit is bevoegd om inspecties uit te voeren om te controleren of essentiële en belangrijke entiteiten de maatregelen voor het beheer van cyberbeveiligingsrisico's en de regels voor het melden van incidenten naleven.

Inspecties met betrekking tot essentiële entiteiten kunnen zowel *ex ante* (voorafgaan) als *ex post* (achteraf) worden uitgevoerd. Ze worden uitgevoerd door de inspectiedienst van de nationale cyberbeveiligingsautoriteit of door de aangewezen sectorale inspectiedienst (specifieke/bijkomende sectorale maatregelen). Deze inspecties kunnen, op verzoek van de sectorale overheid, gezamenlijk worden uitgevoerd door voornoemde autoriteiten.

Essentiële entiteiten zijn ook verplicht om regelmatige conformiteitsbeoordelingen te ondergaan. Belangrijke entiteiten kunnen ook vrijwillig een conformiteitsbeoordeling ondergaan op basis van de ISO 27001-norm of CyberFundamentals (zie paragraaf 4.3.).

Inspecties *ex post* van belangrijke entiteiten worden uitgevoerd op basis van indicatoren, zoals het zich voordoen van een incident of objectief bewijs van mogelijke tekortkomingen. Ook deze inspectie kan worden uitgevoerd door de inspectiedienst van het CCB, door de aangewezen sectorale inspectiedienst of door beide. Het doel van gezamenlijke inspecties of inspecties die aan sectorale inspectiediensten worden gedelegeerd, is het vereenvoudigen en rationaliseren van overheidsmiddelen.

De inspecteurs kunnen op locatie gaan, hun vaststellingen optekenen in een proces-verbaal en verslagen opstellen. Op basis van deze vaststellingen kan een procedure worden opgestart om de entiteit aan te manen een einde te maken aan de inbreuk en, indien nodig, de gepaste administratieve maatregelen te nemen, gaande van een waarschuwing tot een administratieve boete.

4.11. Zijn de administratieve maatregelen en de administratieve geldboetes evenredig? Wat zijn de bedragen van de boetes?

Art. 59 NIS2-wet

Het doel van administratieve maatregelen en boetes is om het niveau van cyberbeveiliging van essentiële en belangrijke entiteiten te verhogen. Op voorwaarde dat de wettelijke procedures worden nageleefd (inclusief het horen van de betrokken entiteit, zie artikel 51-57), kan een administratieve maatregel of boete worden opgelegd, op een proportionele manier, rekening houdend met de ernst van de inbreuken, de houding van de entiteit en eventuele recidive.

De volgende administratieve geldboetes kunnen worden opgelegd:

1. Van 500 tot 125.000 euro voor iedereen die niet voldoet aan de informatieverplichtingen waarnaar wordt verwezen in artikel 12;
2. Van 500 tot 200.000 euro voor een entiteit die een persoon die namens haar handelt nadelige gevolgen berokkent ingevolge de uitvoering, te goeder trouw en binnen het kader van zijn functie, van de verplichtingen die voortvloeien uit deze wet;
3. Van €500 tot €200.000 voor iedereen die niet voldoet aan de toezichtverplichtingen;
4. Van 500 tot 7.000.000 euro of 1,4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de belangrijke entiteit behoort (afhankelijk van welk bedrag het hoogst is), de belangrijke entiteit die niet voldoet aan de verplichtingen betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's en/of de rapportageverplichtingen;
5. Van 500 tot 10.000.000 euro of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de essentiële entiteit behoort (afhankelijk van welk bedrag het hoogst is), de essentiële entiteit die niet voldoet aan de verplichtingen betreffende de maatregelen voor het beheer van cyberbeveiligingsrisico's en/of aan de rapportageverplichtingen.

De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen een termijn van drie jaar.

De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

4.12. Welke andere administratieve maatregelen kunnen worden genomen?

4.12.1. Basismaatregelen

De volgende administratieve maatregelen kunnen worden opgelegd aan essentiële en belangrijke entiteiten:

Art. 58 NIS2-wet

1. waarschuwingen geven over inbreuken door de betrokken entiteiten op deze wet;
2. bindende aanwijzingen vaststellen of een bevel uitvaardigen waarin de betrokken entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuken op deze wet te verhelpen;
3. de betrokken entiteiten gelasten een einde te maken aan gedragingen die inbreuk maken op deze wet en af te zien van herhaling van die gedragingen;
4. de betrokken entiteiten gelasten er op een gespecificeerde wijze en binnen een gespecificeerde termijn voor te zorgen dat hun maatregelen voor het beheer van cyberbeveiligingsrisico's in overeenstemming zijn met titel 3 of te voldoen aan de verplichtingen inzake het melden van incidenten bedoeld in dezelfde titel;
5. de betrokken entiteiten gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberdreiging worden beïnvloed, in kennis te stellen van de aard van de dreiging en van alle mogelijke beschermings- of herstelmaatregelen die deze natuurlijke of rechtspersonen kunnen nemen als reactie op die dreiging;
6. de betrokken entiteiten gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;

7. de betrokken entiteiten gelasten aspecten van inbreuken op deze wet op een bepaalde manier openbaar te maken;

Wanneer de betrokken entiteit een essentiële entiteit is:

- het CCB kan voor een bepaalde periode een controlefunctionaris aanwijzen die gedurende een bepaalde periode duidelijk omschreven taken heeft om erop toe te zien dat de betrokken entiteiten voldoen aan de maatregelen voor het beheer van cyberbeveiligingsrisico's en inzake het melden van incidenten
- de in punt 2 bedoelde bindende aanwijzingen omvatten ook de maatregelen die nodig zijn om een incident te voorkomen of te verhelpen, alsmede uiterste termijnen voor de uitvoering van dergelijke maatregelen en voor verslaggeving over de uitvoering ervan.

4.12.2. Bijkomende maatregelen

Als de gevraagde maatregelen niet binnen de gestelde termijn worden ondernomen, kunnen de volgende administratieve maatregelen worden opgelegd aan essentiële entiteiten:

Art. 60 NIS2-wet

1. een certificering of vergunning tijdelijk opschorten met betrekking tot alle of een deel van de relevante door de betrokken entiteit verleende diensten of verrichte activiteiten;
2. natuurlijke personen met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijk vertegenwoordiger in de betrokken entiteit tijdelijk verbieden leidinggevende verantwoordelijkheden in die entiteit uit te oefenen.

De in punt 1 bedoelde tijdelijke opschortingen of verboden worden slechts toegepast tot de betrokken entiteit de maatregelen heeft genomen die nodig zijn om de tekortkomingen te verhelpen of te voldoen aan de vereisten van de bevoegde autoriteit die deze handhavingsmaatregelen heeft opgelegd.

4.13. Wat zijn de verplichtingen en verantwoordelijkheden van het management?

De bestuursorganen van NIS2-entiteiten moeten maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren en toezien op de uitvoering ervan. Als de entiteit haar verplichtingen met betrekking tot het beheer van cyberbeveiligingsrisico's niet nakomt, is het bestuursorgaan aansprakelijk.

Art. 31 & 61 NIS2-wet

Leden van bestuursorganen zijn verplicht om een opleiding te volgen zodat ze over voldoende kennis en vaardigheden beschikken om risico's te identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te beoordelen.

De verantwoordelijken en/of de wettelijke vertegenwoordigers van een NIS2-entiteit moeten de bevoegdheid hebben om ervoor te zorgen dat de entiteit de wet naleeft. Deze personen zijn aansprakelijk indien zijn hun verplichtingen hieromtrent niet nakomen.

Het doel van deze responsabilisering is het transformeren van cyberveiligheid in een onderwerp dat echt van belang is voor de betrokken entiteiten.

4.14. Wat is een "bestuursorgaan"?

Het begrip "bestuursorgaan" wordt niet gedefinieerd in de richtlijn.

Vanuit het oogpunt van het Europees recht, heeft het Hof van Justitie er herhaaldelijk aan herinnerd dat: ten eerste, als een woord of begrip niet in het rechtsinstrument wordt gedefinieerd, de gebruikelijke betekenis ervan moet worden aangehouden; en ten tweede, tenzij anders aangegeven, dat elk begrip in het Europees recht dezelfde definitie moet hebben. Een dergelijke definitie is te vinden in Richtlijn 2013/36, in artikel 3, eerste lid, (7) waar 'leidinggevend orgaan' wordt gedefinieerd als: " *het (de) overeenkomstig nationaal recht aangewezen orgaan (organen) van een instelling welke de bevoegdheid hebben de strategie, doelstellingen en de algemene richting van de instelling vast te stellen, en welke toezichthouden op de bestuurlijke besluitvorming en deze controleert, met inbegrip van de personen die het beleid van de instelling daadwerkelijk bepalen"*.

De memorie van toelichting bij de NIS2-wet definieert "lid van een bestuursorgaan" als volgt:

Iedere natuurlijke of rechtspersoon die:

(i) een functie uitoefent binnen of in verband meteen entiteit die hem of haar in staat stelt (a) die entiteit te beheren en te vertegenwoordigen of (b) namens en voor rekening van die entiteit beslissingen te nemen die juridisch bindend zijn voor die entiteit of deel te nemen, binnen een orgaan van die entiteit, aan besluitvorming over dergelijke beslissingen, of

(ii) controle uitoefent over de entiteit, zijnde de bevoegdheid in rechte of in feite om een beslissende invloed uit te oefenen op de aanstelling van een meerderheid van de bestuurders of zaakvoerders of op de oriëntatie van het beleid.

Als de entiteit in kwestie een vennootschap naar Belgisch recht is, wordt deze zeggenschap bepaald in overeenstemming met artikelen 1:14 tot 1:18 van het Wetboek van Vennootschappen en Verenigingen.

Wanneer de persoon wiens rol wordt onderzocht, een rechtspersoon is, wordt het begrip "lid van een bestuursorgaan" terugwerkend onderzocht en omvat het zowel de rechtspersoon in kwestie als elk lid van een bestuursorgaan van die rechtspersoon.

5. Andere

5.1. Moet de Europese Commissie nog uitvoeringshandelingen vaststellen?

Ja, een uitvoeringshandeling, die uiterlijk op 17 oktober 2024 door de Europese Commissie moet zijn vastgesteld, richt zich op een beperkt aantal entiteiten die onder de richtlijn vallen en waarvoor op Europees niveau op geharmoniseerde wijze in bepaalde regels is voorzien.

Artikel 21, lid 5, alinea 1, van de richtlijn heeft betrekking op de technische en methodologische vereisten inzake maatregelen voor het beheer van cyberbeveiligingsrisico's voor DNS-dienstverleners, registers van topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook aanbieders van onlinemarktplaatsen, onlinezoekmachines en platformen voor socialenetwerkdiensten, en aanbieders van vertrouwensdiensten.

Artikel 23, lid 11 van de richtlijn behandelt het begrip van een significant incident voor DNS-dienstverleners, registers van topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, evenals aanbieders van onlinemarktplaatsen, onlinezoekmachines en platformen voor socialenetwerkdiensten.

In deze bepalingen staat ook dat de Commissie, in de mate van het mogelijk de relevante Europese en internationale normen en technische specificaties moet volgen. De Commissie moet ook advies uitwisselen en samenwerken met de samenwerkingsgroep en ENISA over deze ontwerpuitvoeringshandelingen.

Praktisch gezien zou de toekomstige uitvoeringshandeling uitsluitend betrekking moeten hebben op de volgende elementen (de Commissie heeft aangegeven dat zij, indien mogelijk, beide soorten verduidelijking in één handeling wil opnemen):

- details van de technische en methodologische vereisten inzake maatregelen voor het beheer van cyberbeveiligingsrisico's voor deze specifieke entiteiten;
- details van het begrip significant incident voor deze specifieke entiteiten, met uitzondering van aanbieders van vertrouwensdiensten (*trust service providers)*.

ENISA en de werkgroepen (*workstreams*) van de NIS samenwerkingsgroep werken momenteel aan het verstrekken van advies aan de Commissie ter voorbereiding op de comitéprocedure.

Op basis van deze uitwisselingen zal de Commissie een voorstel voor een uitvoeringshandeling formuleren, dat vervolgens zal worden gedeeld en besproken binnen het NIS2 Comité (zodra dit formeel is opgericht). Het comité moet de comitologieregels van Verordening (EU) nr. 182/2011 volgen.