CENTRE FOR CYBERSECURITY BELGIUM

DE NIS2-RICHTLIJN IN BELGIË

Centre for Cybersecurity Belgium
Onder de autoriteit van de Eerste Minister

Inleiding

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 (de "NIS2-wet") zet de EU-richtlijn 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 (de "NIS2-richtlijn") om.

Om de steeds frequentere cyberdreigingen en de opkomst van nieuwe uitdagingen aan te pakken, heeft de Europese Unie nieuwe wetgeving aangenomen over maatregelen om een gemeenschappelijk hoog cyberbeveiligingsniveau in de hele Unie te waarborgen (Richtlijn 2022/2555 van 14 december 2022 – de zogenaamde “NIS2-richtlijn”). Ze vervangt de 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).

De NIS2-richtlijn voert belangrijke wijzigingen in ten opzichte van de NIS1-richtlijn: uitbreiding van de betrokken sectoren en entiteiten, nieuwe selectie- en registratiemethoden, meer cyberbeveiligingsvereisten, nieuwe termijnen voor het melden van incidenten en versterkte toezichtmechanismen.

De richtlijn is ook bedoeld om de nationale cyberbeveiligingsbeveiligingsstrategie en het nationale beleid op het gebied van cyberbeveiliging te versterken. Het nationale beleid omvat nationale raamwerken en processen voor crisisbeheer op het gebied van cyberbeveiliging, de taken van de bevoegde overheden en nationale en internationale samenwerking.

Als nationale cyberbeveiligingsautoriteit speelt het Centrum voor Cybersecurity België (CCB) een sleutelrol in de coördinatie en implementatie van deze richtlijn. Het CCB vervult de taken van bevoegde autoriteit voor alle sectoren (in samenwerking met de eventuele sectorale overheid), van nationaal CSIRT, van centraal nationaal contactpunt en vertegenwoordigt België in de NIS-samenwerkingsgroep, het CSIRT-netwerk en EU-CyCLONe.

Essentiële en belangrijke entiteiten moeten passende en proportionele maatregelen nemen om hun cyberrisico's te beperken. Deze omvatten niet alleen organisatorische, maar ook technische en operationele maatregelen met een dubbel doel: cyberaanvallen vermijden en in het geval van een succesvolle aanval onderbreking van activiteiten beperken.

Om bedrijven te helpen ontwikkelde het CCB duidelijke richtlijnen in de vorm van CyberFundamentals (CyFun®)-kader. Hierbij geldt een vermoeden van conformiteit als de entiteiten een CyFun®- of ISO/IEC 27001-certificering/-label verkrijgen.

NIS2-entiteiten melden hun significante incidenten aan het nationale CSIRT. Hierdoor kan de mogelijke verspreiding van een incident beperkt en getroffen entiteiten in staat gesteld worden om bijstand te vragen. Door het ontvangen van deze informatie kan het CCB crisissituaties zo goed mogelijk beheren en relevante technische informatie delen met andere entiteiten.

Tot slot speelt het CCB met zijn inspectiedienst (in samenwerking met de eventuele sectorale overheden) ook een rol in het toezicht op de betrokken entiteiten. Het toezicht heeft tot primair doel de entiteiten te versterken in hun cyberweerbaarheid, maar laat ook toe om sancties op te leggen aan entiteiten die de vereiste maatregelen niet nemen.

Het doel van dit document is algemene informatie te verstrekken over de reikwijdte en inhoud van de omzetting van de NIS2-richtlijn[1] in België.

[1] NIS2-wet: https://www.ejustice.just.fgov.be/eli/wet/2024/04/26/2024202344/justel

Koninklijk besluit: https://www.ejustice.just.fgov.be/eli/besluit/2024/06/09/2024005260/justel

Inhoudsopgave

Samenvatting: NIS2 in zeven stappen

Het lijkt erop dat NIS2 van toepassing is op je organisatie maar ue weet niet waar te beginnen? Het CCB heeft een aanbeveling opgesteld over hoe je in slechts zeven stappen aan de Belgische NIS2-wetgeving kan voldoen.

1. **Is NIS2 op mijn organisatie van toepassing?**

   a. In het toepassingsgebied: NIS2-entiteiten: gebruik onze scope tool[2] om te kijken of je organisatie binnen het toepassingsgebied van de Belgische NIS2-wet valt;
   b. In de toeleveringsketen: het CCB beveelt NIS2-eintitieten aan om organisaties die van vitaal belang zijn voor hun cyberbeveiliging te identificeren en hen uit te nodigen om ten minste het CyberFundamentals Framework zekerheidsniveau 'Basic' te implementeren.

2. **Registreer je NIS2-entiteit**

Alle NIS2-entiteiten moeten zich registreren op Safeonweb@Work[3]:

- Entiteiten in de digitale sectoren van de wet moeten zich registreren uiterlijk op 18 december 2024;
- Alle andere NIS2-entiteiten moeten zich uiterlijk op 18 maart 2025 registreren.

3. **Bereid je organisatie voor op het melden en behandelen van significante incidenten vanaf 18 oktober 2024.**

Vanaf 18 oktober 2024 zijn alle NIS2-entiteiten verplicht om significante incidenten aan het CCB te melden (zie gids).

Significante incidenten worden gemeld aan het CCB via het platform voor incidentmeldingen: **https://notif.safeonweb.be** (of telefonisch op +32 (0)2 501 05 60 **alleen voor noodgevallen met betrekking tot NIS2-entiteiten of als het platform niet beschikbaar is**).

Incidenten melden is slechts één onderdeel van een incident response plan. Als jouw organisatie nog geen incident response plan heeft, kan het nuttig zijn om te vertrekken van onze policy template.

4. **Bepaal je CyberFundamentals (CyFun®)-niveau**

Als je voor ons CyFun® Framework kiest, kan je met onze CyFun® Selection Tool het juiste zekerheidsniveau (Basic, Important of Essential) voor je organisatie bepalen.

5. **Plan opleidng rond cyberbeveiliging**

Een basiskennis van risicobeheer en cyberbeveiliging is onontbeerlijk om beslissingen over cyberbeveiligingsstrategieën en -maatregelen op managment- en directieniveau te kunnen nemen. De CCB raadt aan om best vóór april 2025 een opleiding voor het management te plannen. Naast deze opleiding maakt het trainen van medewerkers altijd deel uit van de cyberbeveiligingsmaatregelen.

6. **Implementeer beveiligingsmaatregelen**

NIS2-entiteiten kunnen het CyFun®-framework volgens deze drie stappen gebruiken om te voldoen aan NIS2:

1) Voer een gap analysis uit met behulp van de CyFun® Self-Assessment Tool;
2) Implementeer de vereiste maatregelen. In je implementatieplan moeten de cyberbeveiligingsmaatregelen geleidelijk worden doorgevoerd, rekening houdend met de controletermijnen zoals aangegeven in stap 7 hieronder;
3) Werk je zelfevaluatie bij en verzamel het nodige bewijs om de implementatie te bevestigen.

7. **Laat je cybersecurity controleren**

Essentiële entiteiten moeten hun implementatie regelmatig laten beoordelen en controleren door een derde partij. Dit kan door middel van een CyFun®-certificering die wordt toegekend door een geaccrediteerde en erkende

[2] https://atwork.safeonweb.be/nl/nis2

[3] https://atwork.safeonweb.be/nl/register-my-organisation

conformiteitsbeoordelingsinstantie (CAB). Essentiële entiteiten moeten vóór 18 april 2026 het zekerheidsniveau “basic” of “important” verkrijgen en het eindniveau moet vóór 18 April 2027 gecertificeerd zijn.Belangrijke entiteiten kunnen zich aan dezelfde regelmatige conformiteitsbeoordeling CyFun onderwerpen, dit verleent hen een vermoeden van conformiteit.

Houd er rekening mee dat het beschikken over het juiste CyFun®-label of -certificaat erg belangrijk kan zijn voor de raad van bestuur en de directie om in geval van een incident de conformiteit te kunnen aantonen.

I. Waarom NIS2? En voor wie?

Netwerk- en informatiesystemen hebben zich ontwikkeld tot een centraal onderdeel van ons dagelijks leven door de digitale transformatie en onderlinge verbondenheid van de samenleving. Veel kritieke maatschappelijke en economische activiteiten zijn nu afhankelijk van de vlotte werking van deze systemen.

Deze ontwikkeling heeft geleid tot alsmaar meer cyberdreigingen en -incidenten die een reële bedreiging vormen voor de openbare veiligheid voor burgers, bedrijven en overheden. Tegenwoordig kan een cyberincident ernstige operationele verstoringen in kritieke sectoren veroorzaken, waarbij mensen of bedrijven worden getroffen en aanzienlijke materiële, fysieke of morele schade wordt aangericht.

Alle burgers, bedrijven en overheden moeten zich daarom bewust zijn van het belang van preventieve bescherming tegen cyberbedreigingen en -incidenten.

De volgende infographic geeft een inleidend overzicht van de NIS2-wet:

II. Toepassingsgebied

Om onder de Belgische NIS2-wet te vallen, moet een organisatie (met bepaalde uitzonderingen) in principe:

1. een dienst leveren die is opgenomen in bijlage I of II van de NIS2-wet in de Europese Unie;
2. de in Aanbeveling 2003/361/EG vastgestelde drempels voor middelgrote ondernemingen overschrijden, d.w.z. een aantal werkzame personen van ten minste 50 voltijdse werknemers of een jaaromzet of balanstotaal van meer dan 10 miljoen euro hebben; en
3. in België gevestigd zijn.

A. DE OMVANG ("SIZE-CAP")

De omvang van een entiteit wordt berekend op basis van bijlage I van Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (de "Aanbeveling").

De omvang van een organisatie wordt bepaald aan de hand van twee criteria: het aantal werkzame personen/personeelsbestand (gemeten in voltijdse equivalenten (VTE's)[4]) en de financiële bedragen (jaaromzet en/of jaarlijks balanstotaal). Op enkele uitzonderingen na[5] moet een organisatie ten minste als een middelgrote onderneming in de zin van de Aanbeveling worden beschouwd om onder de NIS2-wet te vallen. Een middelgrote onderneming heeft een aantal werkzame personen van ten minste 50 VTE of een jaaromzet en/of jaarlijks balanstotaal van meer dan 10 miljoen euro.

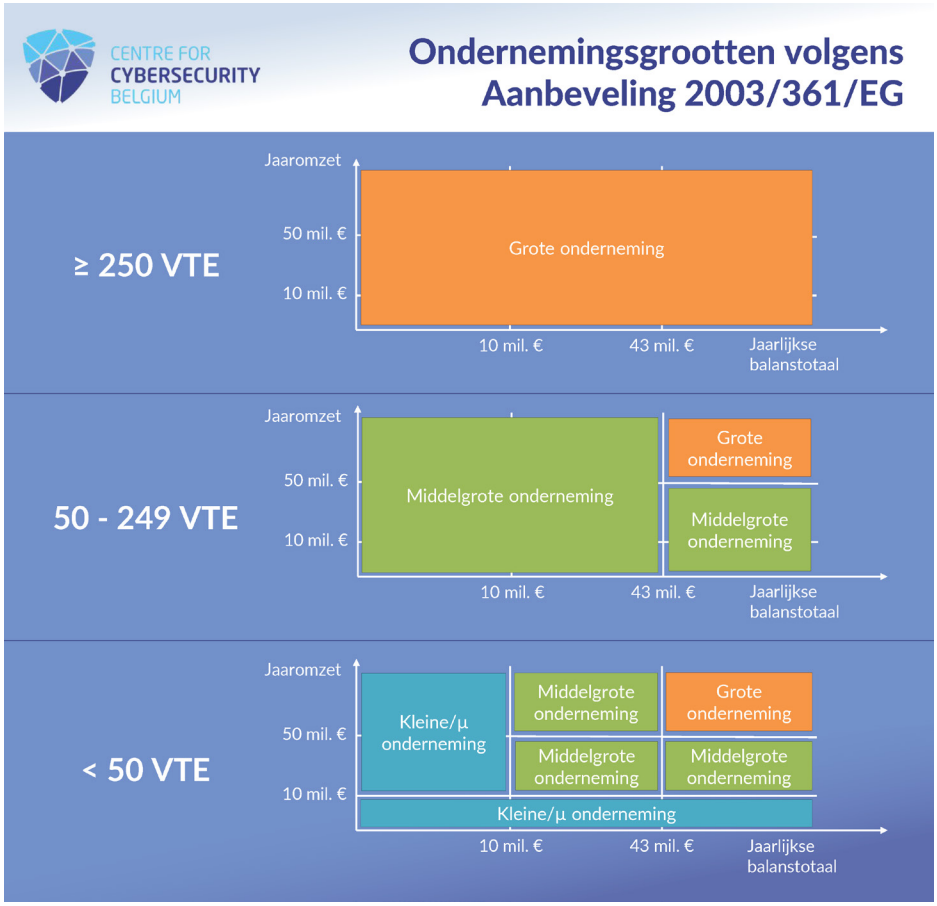
Hoe deze twee criteria precies worden vastgesteld, is terug t vinden in de bijlage van de Aanbeveling zelf en in de "Gebruikersgids bij de definitie van kmo's"[6] van de Commissie. Er dient echter opgemerkt te worden dat een onderneming ervoor kan kiezen om ofwel aan het omzetplafond ofwel aan het balanstotaalplafond te voldoen. Ze mag effectief een van de financiële plafonds overschrijden zonder dat dit gevolgen heeft voor haar kmo-statuut. Er wordt dus alleen gekeken naar het laagste van de twee bedragen.

De grafiek op de volgende pagina geeft de verschillende ondernemingsgroottes visueel weer.

[4] Voltijdse equivalenten (VTE's) (in de Aanbeveling "arbeidsjaareenheden (AJE)" genoemd) zijn het aantal personen dat gedurende het gehele referentiejaar 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, en seizoenarbeid worden in breuken van AJE uitgedrukt. De Aanbeveling en de gids specificeren verder welke werkzame personen moeten worden meegeteld.

[5] Zie p. 7-8.

[6] https://op.europa.eu/en/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1



De Aanbeveling bepaalt in het bijzonder dat de berekening van de omvang van een organisatie die deel uitmaakt van een groep (partner- of verbonden ondernemingen) een consolidatie van de gegevens van de verschillende onderdelen van deze groep inhoudt. Voor meer informatie verwijzen we naar de hierboven vermelde Gebruikersgids van de Commissie of naar de online “SME Wizard” tool[7].

Er zijn evenwel twee belangrijke bijzonderheden met betrekking tot de toepassing van de Aanbeveling in de context van de NIS2-wet:

1) Er kan onder bepaalde omstandigheden worden afgezien van de consolidatie van gegevens van de verschillende componenten binnen een groep, wanneer de netwerk- en informatiesystemen van de betrokken organisatie onafhankelijk zijn van die van verbonden of partnerondernemingen.

2) Het aantal werknemers en de financiële cijfers van een overheidsinstantie die controle uitoefent op een betrokken organisatie mogen niet in aanmerking worden genomen bij het bepalen van de omvang van deze organisatie.

Als we de verschillende mogelijke omvangen combineren met het criterium van de geleverde dienst, krijgen we het volgende toepassingsgebied (met enkele uitzonderingen[8]):

	Middelgrote onderneming	**Grote onderneming**
Diensten van bijlage I	Belangrijke NIS2-entiteit	Essentiële NIS2-entiteit
Diensten van bijlage II	Belangrijke NIS2-entiteit	Belangrijke NIS2-entiteit

Er zijn echter een aantal uitzonderingen op de "size-cap". Bepaalde soorten entiteiten vallen onder het toepassingsgebied van de NIS2-wet, ongeacht hun omvang:

[7] https://ec.europa.eu/growth/tools-databases/SME-Wizard/

[8] Zie lijst onder de tabel.

- Gekwalificeerde verleners van vertrouwensdiensten (essentieel);
- Niet-gekwalificeerde verleners van vertrouwensdiensten (belangrijk indien micro-, kleine of middelgrote ondernemingen en essentieel indien grote ondernemingen);
- DNS-dienstverleners (essentieel);
- Registers van topleveldomeinnamen (essentieel);
- Domeinnaamregistratiediensten (alleen voor de registratieverplichting);
- Aanbieders van openbare elektronische communicatienetwerken (essentieel);
- Aanbieders van openbare elektronische communicatiediensten (essentieel);
- Entiteiten die zijn geïdentificeerd als exploitanten van kritieke infrastructuur overeenkomstig de wet van 1 juli 2011 betreffende de beveiliging en bescherming van kritieke infrastructuren (essentieel);
- Overheidsinstellingen die van de federale staat afhangen (essentieel).

Los van deze regels kan het Centrum voor Cybersecurity België (CCB) ook specifieke entiteiten als "essentieel" of "belangrijk" identificeren, bijvoorbeeld wanneer zij de enige leverancier van een dienst zijn of wanneer de verstoring van de geleverde diensten een significant effect zou kunnen hebben op de openbare veiligheid, de openbare beveiliging of de volksgezondheid.

B. DE GELEVERDE DIENST

Het criterium van de geleverde dienst vereist dat een organisatie al haar diensten aan derden, per sector en subsector, volledig analyseert. Dit is belangrijk, omdat zelfs de meest bijkomstige dienst die wordt geleverd ervoor kan zorgen dat een organisatie als geheel onder de NIS2-wet valt, tenzij anders vermeld in de definitie van de betreffende dienst. Alle diensten die onder de NIS2-wet vallen, worden gedetailleerd beschreven in bijlagen I en II (of in de definities[9]) van de wet en gegroepeerd per sector:

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 markten 5. Gezondheidszorg 6. Drinkwater 7. Afvalwater 8. Digitale infrastructuur 9. Beheer van ICT-diensten (B2B) 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

Het is van groot belang om **de definities van deze diensten te raadplegen** om na te gaan of ze overeenkomen met de werkelijke dienst die door een organisatie wordt verleend.

Voor een beter overzicht van het toepassingsgebied van de wet nodigen we u uit om onze visuele samenvatting op de pagina's 23 en 24 te raadplegen.

[9] Zie artikel 8 van de NIS2-wet.

C. DE VESTIGING

In principe is de Belgische NIS2-wet alleen van toepassing op in België gevestigde entiteiten die hun diensten verlenen of hun activiteiten uitvoeren binnen de EU. Het begrip "vestiging" impliceert eenvoudigweg de feitelijke uitoefening van een activiteit door middel van stabiele regelingen, ongeacht de gekozen rechtsvorm, of dit nu de maatschappelijke zetel, een eenvoudig filiaal of een dochteronderneming met rechtspersoonlijkheid is.

Er zijn echter drie uitzonderingen op de regel van vestiging in België:

1) de Belgische NIS2-wet is van toepassing op aanbieders van openbare elektronische communicatienetwerken en op aanbieders van openbare elektronische communicatiediensten die hun diensten in België aanbieden;

2) de Belgische NIS2-wet is van toepassing op 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, evenals aanbieders van onlinemarktplaatsen, onlinezoekmachines of platformen voor socialenetwerkdiensten, als zij hun hoofdvestiging in België hebben of hun wettelijke vertegenwoordiger in de EU in België gevestigd is;

3) de Belgische NIS2-wet is van toepassing op alle door België opgerichte overheidsinstellingen.

Behoudens de uitzonderingen, geldt dat als een entiteit meerdere vestigingen heeft in verschillende EU-lidstaten, ze onderworpen zal zijn aan de omzettingswetten in elk van de betrokken lidstaten. De verschillende bevoegde nationale autoriteiten zullen samenwerken op het gebied van inspecties en de melding van significante incidenten.

D. IDENTIFICATIE EN TOELEVERINGSKETEN

Het is mogelijk dat bepaalde organisaties constateren, na een grondige analyse van het toepassingsgebied van de NIS2-wet, dat ze niet onder deze wet vallen. Alle niet-NIS2-organisaties dienen zich er echter van bewust te zijn dat de NIS2-wet toch op twee manieren een impact kan hebben.

Ten eerste kan de nationale cyberbeveiligingsautoriteit (het CCB) bepaalde organisaties, ongeacht hun omvang, identificeren als essentiële of belangrijke entiteiten in het kader van de NIS2-wet. Er zijn vier mogelijke situaties die verband houden met het kritieke karakter van de organisatie. Dit proces verloopt in overleg met de betrokken entiteit en andere autoriteiten en wordt beschreven in artikel 11 van de NIS2-wet.

Ten tweede kan een organisatie in de directe toeleveringsketen (*supply chain*) van een NIS2-entiteit vallen en op grond van bijvoorbeeld een contractuele verplichting van die NIS2-entiteit worden geconfronteerd met de verplichting om maatregelen voor het beheer van cyberbeveiligingsrisico's te implementeren. In dit verband adviseert het CCB alle organisaties die zich mogelijk in de toeleveringsketen van een NIS2-entiteit bevinden, om ten minste te voldoen aan de maatregelen die zijn uiteengezet in het CyberFundamentals (CyFun®) Framework level Basic[10].

E. VERHOUDING TUSSEN NIS2 EN DORA

De NIS2-wet bepaalt dat de titels 3 tot en met 5 van de wet (maatregelen voor het beheer van cyberbeveiligingsrisico's, toezicht en sancties, en specifieke bepalingen voor de overheidssectoren) niet van toepassing zijn op entiteiten in de sectoren van het bankwezen en de infrastructuur voor de financiële markt die onder het toepassingsgebied van DORA vallen. DORA is de EU-Verordening 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector, waarin eisen worden gesteld aan de beveiliging van netwerk- en informatiesystemen van financiële entiteiten.

Dit vloeit voort uit de uitsluiting van sectorspecifieke rechtshandelingen van de Unie (de zogenaamde *lex specialis*) in de NIS2 richtlijn. Dergelijke handelingen verplichten NIS2-entiteiten om maatregelen voor het beheer van

[10] https://cyfun.be

cyberbeveiligingsrisico's te nemen of significante incidenten te melden en deze vereisten zijn ten minste gelijkwaardig aan de in NIS2 vastgestelde verplichtingen.

In de praktijk dienen alle NIS2-entiteiten die onder DORA vallen, de verplichtingen van DORA naleven met betrekking tot de maatregelen van de titels 3 tot en met 5 van de NIS2-wet. Dit omvat maatregelen voor het beheer van cyberbeveiligingsrisico's, verplichte en vrijwillige melding van incidenten, toezicht, administratieve maatregelen en boetes. Alle andere bepalingen van de NIS2-wet, zoals die met betrekking tot registratie en de bevoegdheid van het CCB, blijven echter van toepassing op deze entiteiten.

III. Verplichtingen

A. REGISTRATIE

NIS2-entiteiten die onder het toepassingsgebied van de Belgische NIS2-wet vallen, moeten hun organisatie registreren bij het CCB. In de praktijk zal dit gebeuren via een online formulier op Safeonweb@Work[11].

De deadline voor de registratie hangt af van het type entiteit. In principe moeten essentiële en belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen zich binnen **vijf maanden** vanaf de inwerkingtreding van de wet registreren, dus uiterlijk op **18 maart 2025**[12].

Voor de volgende soorten entiteiten uit de digitale sectoren bestaat er een aangepaste regeling:

- 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; en
- aanbieders van platformen voor socialenetwerkdiensten.

Ze moeten zich binnen **twee maanden** na de inwerkingtreding van de wet registreren, en dienen hierbij ook andere informatie te voorzien, dus uiterlijk op **18 december 2024**[13].

Elke entiteit is verplicht om het CCB onmiddellijk (uiterlijk na twee weken) op de hoogte te brengen van wijzigingen in deze informatie.

B. MAATREGELEN VOOR HET BEHEER VAN CYBERBEVEILIGINGSRISICO'S

De maatregelen voor het beheer van cyberbeveiligingsrisico's zijn technische, operationele of organisatorische maatregelen waarmee de betrokken entiteit de risico's met betrekking tot de beveiliging van haar netwerk- en informatiesystemen kan beheren en cyberincidenten kan voorkomen of de gevolgen ervan beperken. De maatregelen worden genomen rekening houdend met de stand van de techniek, de bestaande normen en de kosten ervan.

Voor elke entiteit moeten de te nemen maatregelen passend zijn en in verhouding staan tot de risico's, de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit, de kans dat er zich incidenten voordoen en de ernst ervan.

De NIS2-wet lijst 11 minimale maatregelen op die entiteiten moeten implementeren[14]. Zie het diagram op de volgende pagina voor een overzicht.

[11] https://atwork.safeonweb.be/nl/register-my-organisation

[12] De informatie die moet worden geleverd onder de standaard registratie deadline is te vinden in artikel 13, §1 van de NIS2-wet.

[13] De informatie die moet worden geleverd onder het aangepaste regime is te vinden in artikel 14, §1 van de NIS2-wet.

[14] Zie ook de uitvoeringshandeling van de Commissie: https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

Het CCB heeft een gratis en openbaar beschikbaar framework uitgewerkt, nl. her "CyberFundamentals (CyFun®) Framework", dat elk van deze punten omvat. Met behulp hiervan kunnen NIS2-entiteiten voldoen aan de verplichting om passende en evenredige maatregelen voor het beheer van cyberbeveiligingsrisico's te nemen[15].

C. BEVEILIGING VAN DE TOELEVERINGSKETEN

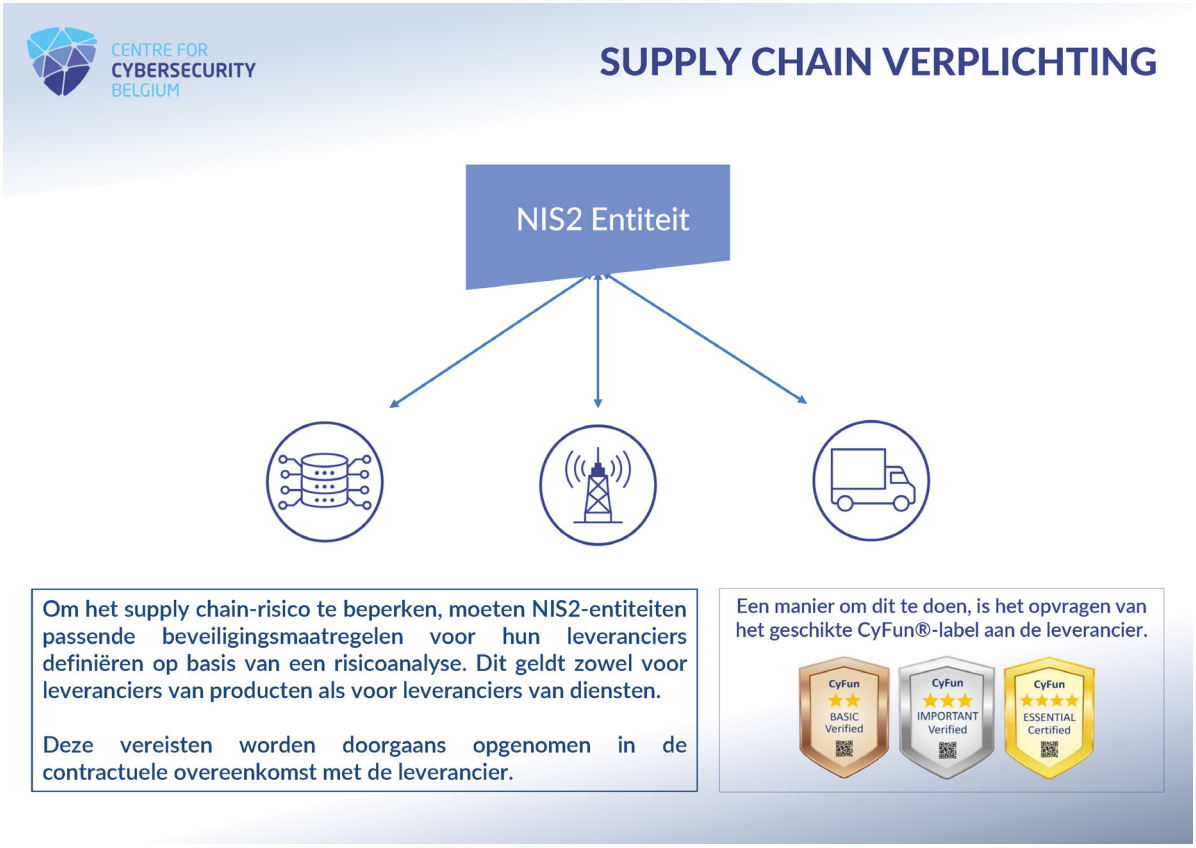
De NIS2-wet vereist dat alle entiteiten die onder het toepassingsgebied van de wet vallen, passende en evenredige maatregelen voor het beheer van cyberbeveiligingsrisico's nemen. Een van deze specifieke maatregelen is de ***"beveiliging van de toeleveringsketen**, met inbegrip van de beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners"*.

De gevolgen van deze verplichting zijn vanuit twee invalshoeken voelbaar. NIS2-entiteiten moeten maatregelen opleggen aan organisaties in hun toeleveringsketen voor het beheer van cyberbeveiligingsrisico's en toezicht op hen houden Daarnaast moeten entiteiten die niet onder het NIS2-toepassingsgebied vallen ook passende en evenredige maatregelen voor het beheer van cyberbeveiligingsrisico's nemen.

De NIS2-wet bepaalt niet hoe de NIS2-entiteiten moeten omgaan met de verplichtingen van de directe toeleveringsketen. Ze laat het aan de entiteiten zelf over om na te gaan of de organisaties in de toeleveringsketen hun verplichtingen nakomen. Het CCB raadt alle NIS2-entiteiten aan om contractueel een label of certificering op te leggen aan de organisaties in hun toeleveringsketen, zoals die in het CyberFundamentals (CyFun®) -framework, op die manier kunnen ze gemakkelijker aantonen dat passende en evenredige maatregelen nemen met betrekking tot cyberveiligheid.

Voor alle entiteiten die niet onder het toepassingsgebied van de NIS2-wet vallen, beveelt het CCB aan om passende en evenredige maatregelen voor het beheer van cyberbeveiligingsrisico's te nemen. Hierdoor zijn ze voorbereid indien ze in de toeleveringsketen van een NIS2-entiteit terechtkomen. Ook hier kunnen ze een beroep doen op het CyFun® -framework om de concrete maatregelen, te identificeren en te implementeren.

[15] Meer informatie in hoofdstuk IV, sectie B.



D. MELDEN VAN INCIDENTEN (ZIE GIDS)

De NIS2-wet verplicht NIS2-entiteiten ook om elk “significant” incident te melden aan het CCB. Een significant incident wordt in de wet als volgt gedefinieerd:

"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:

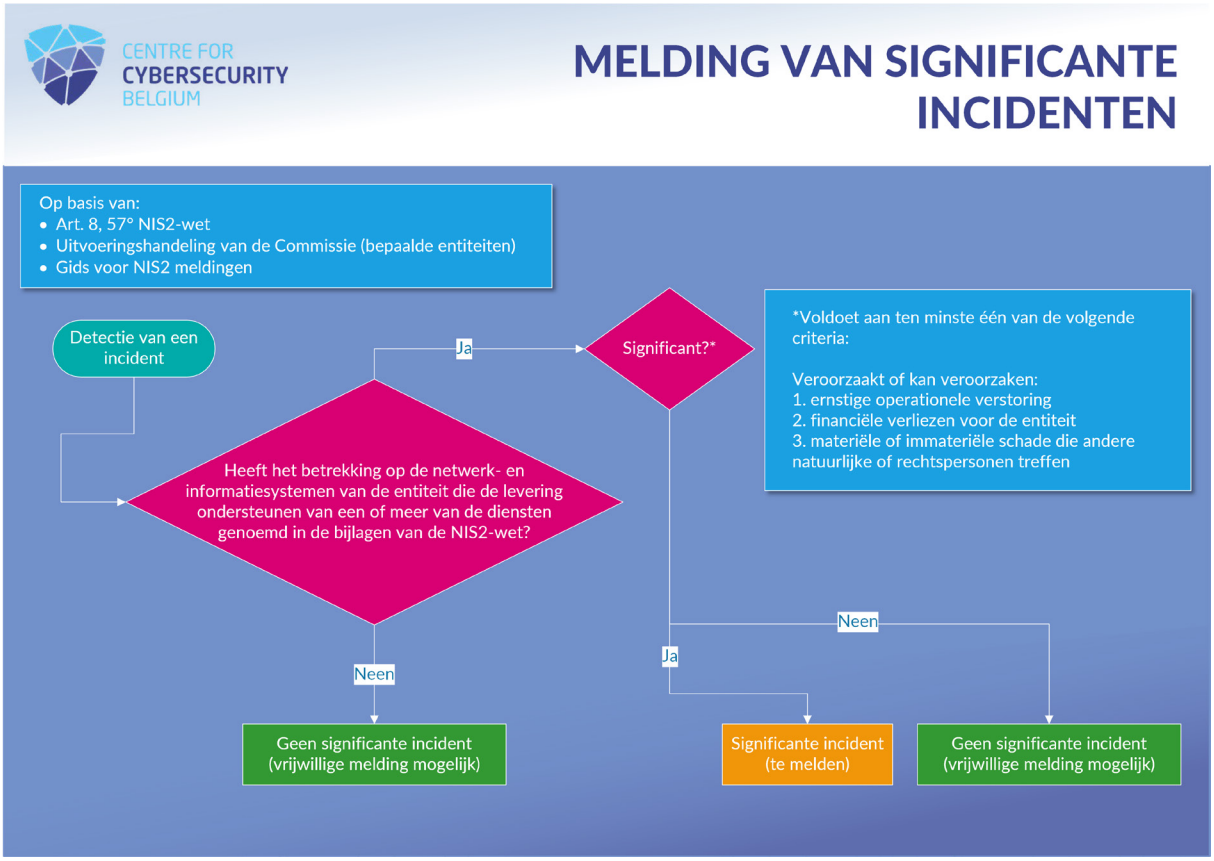
1° een ernstige operationele verstoring van een van de diensten in de sectoren of deelsectoren van de bijlagen I en II of financiële verliezen voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of
2° andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële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

Het incident (zie definitie hierboven) moet gevolgen hebben voor de verlening van een van de diensten in de sectoren of deelsectoren opgesomd in bijlage I en II van de wet, d.w.z. **het moet gevolgen hebben op de netwerk- en informatiesystemen die de verlening van een of meer van deze dienst(en) ondersteunen** (bv. elektriciteitsdistributie).

De verplichte meldingen hebben daarom alleen betrekking op de informatiesystemen en -netwerken waarvan de betrokken entiteit afhankelijk is om de dienst(en) te verlenen die in de bijlagen bij de wet worden opgesomd. Een incident op een geïsoleerd informatiesysteem dat geen verband heeft met de levering van bovengenoemde diensten, hoeft dus niet te worden gemeld.

Bovendien moeten deze gevolgen significant zijn, namelijk het incident moet minstens een van de volgende drie situaties veroorzaken of kunnen veroorzaken:

- een **ernstige operationele verstoring van een van de geleverde diensten** (in de sectoren of subsectoren opgesomd in de bijlagen I en II van de NIS2-wet);
- **financiële verliezen voor de betrokken entiteit**;
- **aanzienlijke materiële, fysieke of morele schade aan andere natuurlijke personen of rechtspersonen**.



Zodra een NIS2-entiteit met een dergelijk incident te maken krijgt, moet ze dit melden aan het CCB. Deze melding verloopt in verschillende stappen (zie ook het schema hieronder):

1) **onverwijld en uiterlijk binnen 24 uur** nadat zij kennis heeft gekregen van het significante incident, bezorgt de entiteit een vroegtijdige waarschuwing;
2) **onverwijld en uiterlijk binnen 72 uur (24 uur voor verleners van vertrouwensdiensten) nadat zij kennis heeft gekregen van het significante incident**, bezorgt de entiteit een incidentmelding;
3) op verzoek van het nationale CSIRT of, indien van toepassing, van de betrokken sectorale overheid, bezorgt de entiteit een tussentijds verslag;
4) **uiterlijk één maand na de in punt 2 bedoelde incidentmelding**, bezorgt de entiteit een eindverslag;
5) indien het eindverslag niet kan worden ingediend omdat het incident nog aan de gang is, bezorgt de entiteit een voortgangsverslag en vervolgens, binnen één maand nadat zij het incident definitief heeft afgehandeld, het eindverslag.

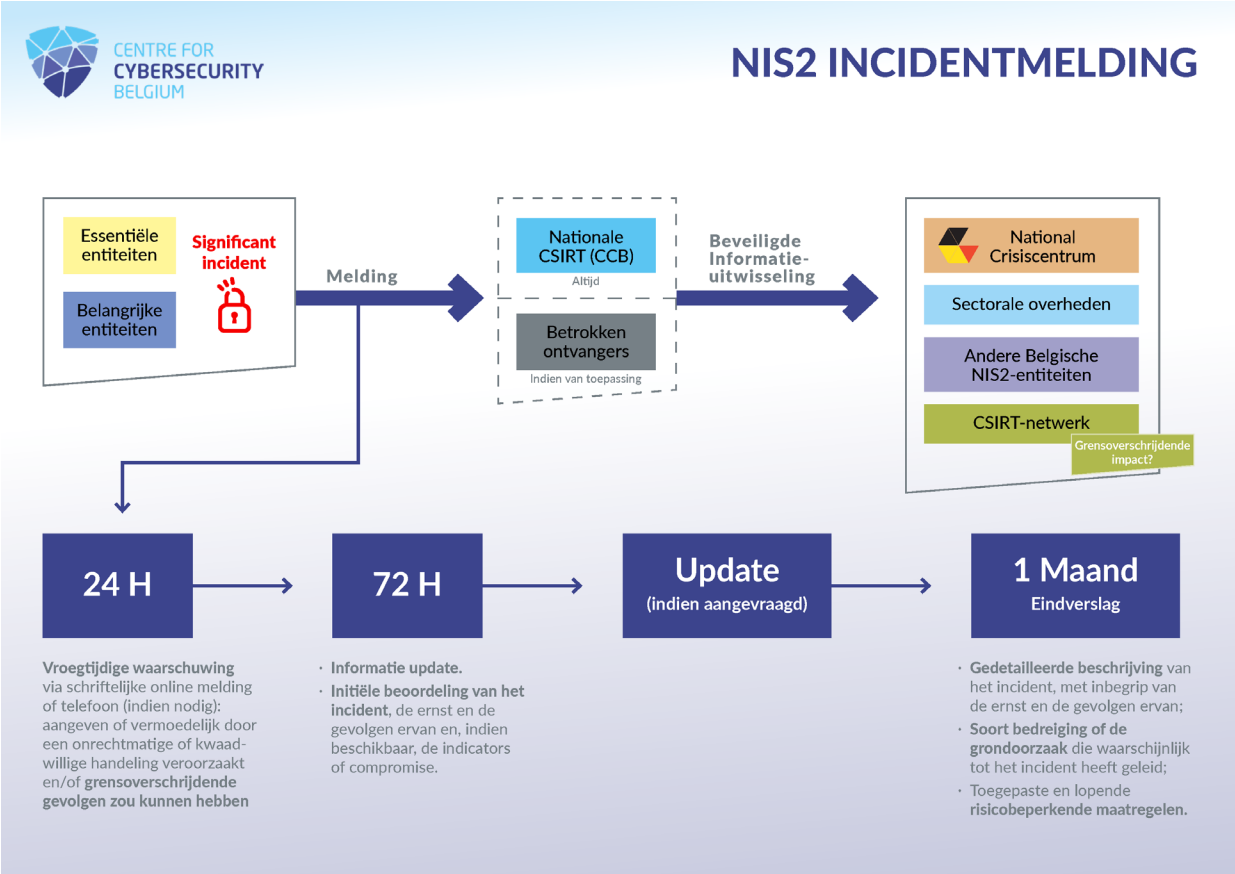
Afhankelijk van de omvang van het incident moet de entiteit ook de ontvangers van haar diensten informeren over het bestaan van het incident en over de maatregelen en correcties die zij kunnen nemen om op het incident te reageren. Het CCB kan de door de entiteit ontvangen informatie binnen de grenzen van het noodzakelijke delen met andere overheden.

Meer informatie over het melden van incidenten is beschikbaar in onze **Gids voor NIS2 meldingen**[16].

NIS2-incidenten kunnen worden gemeld via ons webformulier voor incidentmeldingen: **https://notif.safeonweb.be/nl.**

[16] https://ccb.belgium.be/nl/cert/een-incident-melden

Zie ook de uitvoeringshandeling van de Commissie: https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks



E. VERPLICHTINGEN VOOR HET MANAGEMENT

De NIS2-wet voorziet in verschillende specifieke bepalingen voor het management van NIS2-entiteiten:

1) Bestuursorganen moeten maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren en toezicht houden op de uitvoering.
2) Leden van bestuursorganen moeten een opleiding volgen om te garanderen dat hun kennis en vaardigheden voldoende zijn om risico's te identificeren en praktijken voor het beheer van cyberbeveiligingsrisico's en de impact ervan op de door de entiteit verleende diensten te beoordelen;
3) Bestuursorganen zijn aansprakelijk voor beslissingen op het gebied van beheer van cyberbeveiligingsrisico's, inclusief incidentbeheer;

Het doel van deze maatregelen is ervoor zorgen dat cyberbeveiliging een belangrijk thema wordt voor het management.

In de memorie van toelichting bij de NIS2-wet wordt uitgelegd wat het begrip "lid van een bestuursorgaan" inhoudt:

> *Iedere natuurlijke persoon of rechtspersoon die:*
>
> *(i) een functie uitoefent binnen of in verband met een 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.*
>
> *Indien de entiteit in kwestie een vennootschap naar Belgisch recht is, wordt deze controle bepaald in overeenstemming met artikel 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 bestuursorgaan van die rechtspersoon.

Deze aansprakelijkheidsregels doen geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, noch aan de aansprakelijkheidsregels voor ambtenaren en verkozen of benoemde overheidsfunctionarissen.

Er moet worden opgemerkt dat natuurlijke personen die leidinggevende verantwoordelijkheden op het niveau van directeur of wettelijk vertegenwoordiger in een NIS2-entiteit uitoefenen, tijdelijk kunnen worden uitgesloten van het uitoefenen van leidinggevende verantwoordelijkheden in deze entiteit, indien zij niet voldoen aan de vereisten van de NIS2-wet.

IV. Toezicht

A. ALGEMEEN REGIME

Op het vlak van toezicht maakt de wet een onderscheid tussen belangrijke en essentiële entiteiten:

- belangrijke entiteiten worden "*ex-post*" gecontroleerd, wat betekent dat er pas een inspectie plaatsvindt nadat er een incident heeft plaatsgevonden of wanneer de toezichthoudende overheid over voldoende elementen beschikt om te vermoeden dat een belangrijke entiteit de wet heeft overtreden;
- essentiële entiteiten kunnen "*ex-post*" maar ook "*ex-ante"* worden gecontroleerd, wat betekent dat ze op elk moment moeten kunnen bewijzen dat ze de wet naleven. Daartoe onderwerpt de wet essentiële entiteiten aan een verplichte regelmatige conformiteitsbeoordeling.

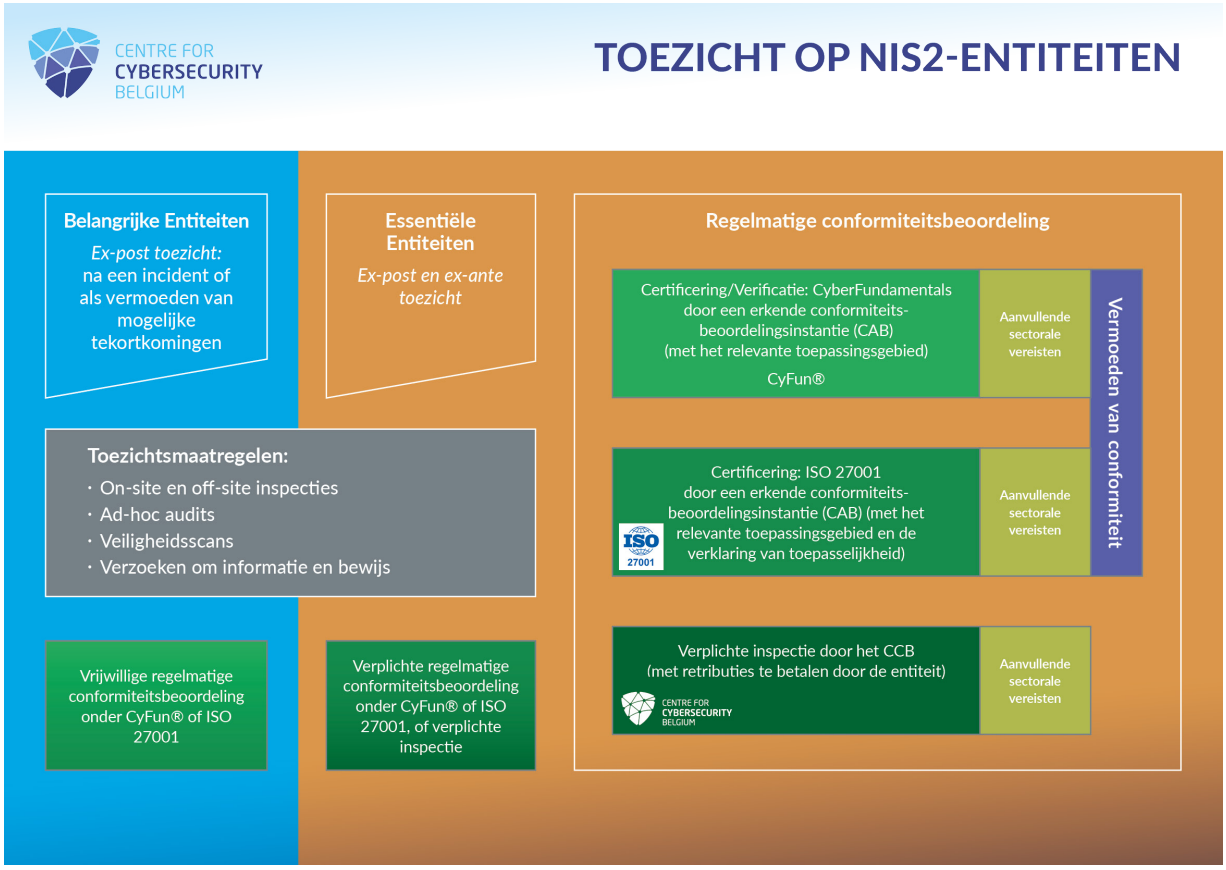
Zo'n verplichte regelmatige conformiteitsbeoordeling kan op drie verschillende manieren worden uitgevoerd:

1) Een certificering (niveau “Essential”) of verificatie (niveau “Important” of “Basic”) van de entiteit onder het **CyberFundamentals (CyFun®)-framework** door een conformiteitsbeoordelingsinstantie (CAB), geaccrediteerd door BELAC en erkend door het CCB, met het relevante toepassingsgebied.
2) Een certificering van de entiteit onder de **ISO/IEC 27001-norm** verleend door een geaccrediteerde CAB met het relevante toepassingsgebied en de *statement of applicability*. Voor ISO/IEC 27001 moet de CAB geaccrediteerd zijn door een accreditatie-instelling die de *Multi-Lateral Agreement* (MLA) waaronder ISO/IEC 27001 valt, heeft ondertekend in het kader van de European co-operation for Accreditation (EA) of het International Accreditation Forum (IAF), en erkend zijn door het CCB.
3) Een **inspectie** door de inspectiedienst van het CCB (voor deze dienst wordt een retributie gevraagd).

Een sectorale overheid kan daarnaast aanvullende vereisten toevoegen die de entiteiten die onder haar sector vallen moeten naleven. Entiteiten die ervoor kiezen om hun regelmatige conformiteitsbeoordeling via CyFun® of ISO/IEC 27001 uit te voeren, kunnen ook gebruikmaken van een vermoeden van conformiteit.

Tijdens de inspectie kan de inspectiedienst inspecties ter plaatse, off-site toezicht, ad-hoc audits beveiligingsscans en algemene verzoeken om informatie en bewijs uitvoeren. Alle NIS2-entiteiten moeten te allen tijde de verzoeken van de inspectiedienst inwilligen. Doen ze dat niet, dan riskeren ze administratieve maatregelen en boetes.

Belangrijke entiteiten kunnen zich ook vrijwillig onderwerpen aan een regelmatige conformiteitsbeoordeling. In dat geval kunnen ze enkel kiezen tussen CyFun® en ISO/IEC 27001.



B. DE CYBERFUNDAMENTALS (CYFUN®)

Het CyberFundamentals (CyFun®) Framework[17] is een reeks concrete maatregelen om:

- gegevens te beschermen;
- het risico op de meest voorkomende cyberaanvallen aanzienlijk te verkleinen;
- de cyberweerbaarheid van een organisatie te vergroten.

Om te reageren op de ernst van de bedreiging waaraan een organisatie wordt blootgesteld, worden naast het startniveau Small, drie zekerheidsniveaus geboden: Basic, Important en Essential. De framework werd gevalideerd met behulp van CERT-aanvalsprofielen (verkregen uit succesvolle aanvallen). De conclusie is dat:

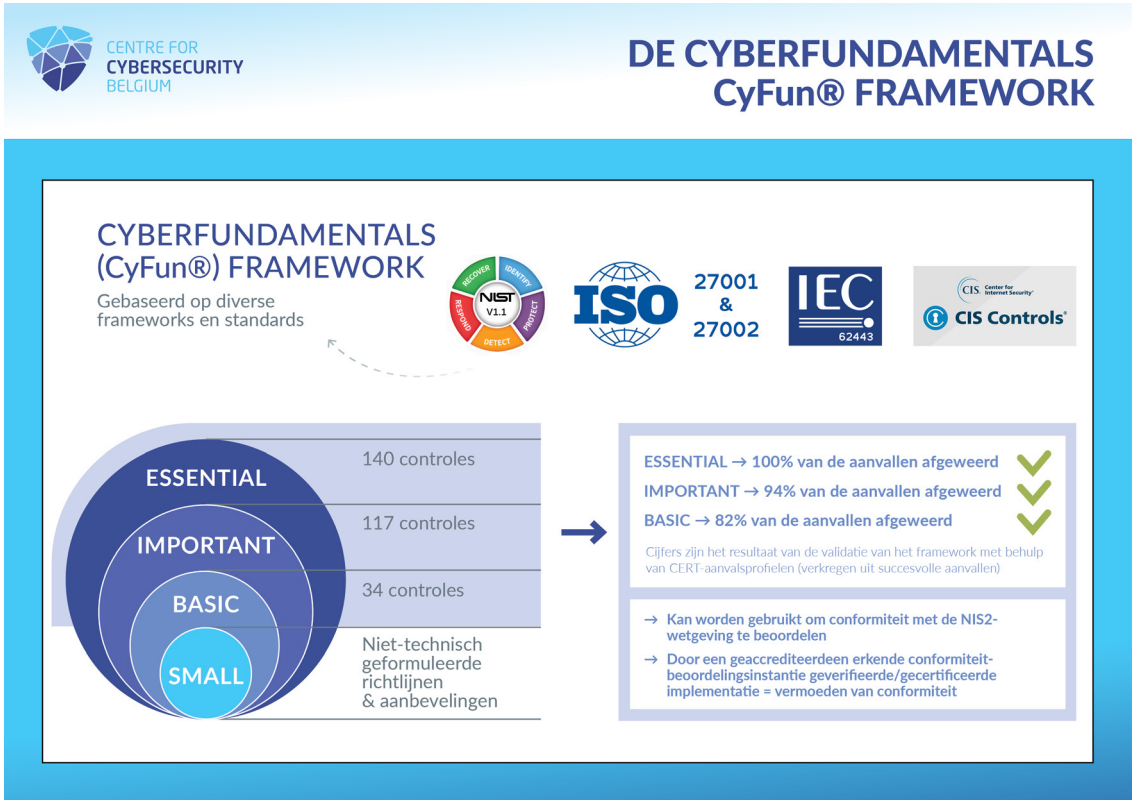
- maatregelen op zekerheidsniveau Basic 82% van de aanvallen kunnen dekken;
- maatregelen op zekerheidsniveau Important 94 % van de aanvallen kunnen dekken;
- maatregelen op zekerheidsniveau Essential 100% van de aanvallen kunnen dekken.

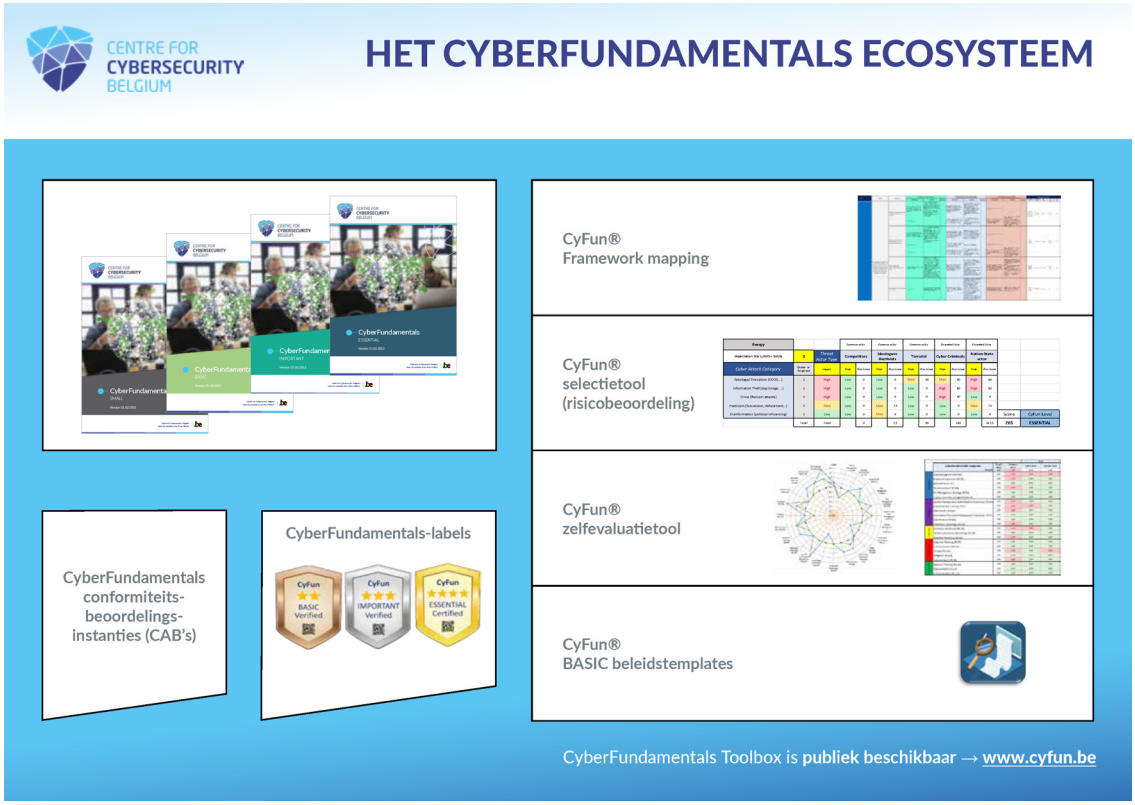
Daarnaast is het CyFun® Framework:

- **gebaseerd op erkende standaarden**: CyFun® selecteert relevante controles op basis van gangbare standaarden zoals NIST CSF, ISO/IEC 27001, CIS Controls en IEC 62443;
- **overeengekomen met de maatregelen die nodig zijn** om de belangrijkste door het CCB geïdentificeerde aanvallen te voorkomen;
- **door iedereen te gebruiken**: elke controle gaat gepaard met richtlijnen om de implementatie te ondersteunen. CyFun®'s self-assessment-tool helpt om een overzicht over de implementatie te behouden;
- **nuttig bij de validering van je implementatie**: de implementatie kan worden gevalideerd door een beoordeling aan te vragen bij een erkende conformiteitsbeoordelingsinstantie. Dit attest geeft je klanten en overheden het bewijs van je implementatie (bv. om te voldoen aan NIS2).

[17] https://cyfun.be

In de context van NIS2 is het CyFun® Framework een handig hulpmiddel, niet alleen voor essentiële entiteiten die onderworpen zijn aan een regelmatige conformiteitsbeoordeling, maar ook voor belangrijke entiteiten. Het is gratis beschikbaar en biedt eenvoudige oplossingen voor risicobeoordeling, zelfbeoordeling en voor het invoeren van de minimale door de NIS2-wet vereiste maatregelen voor het beheer van cyberbeveiligingsrisico's. Bovendien geeft een gevalideerde of gecertificeerde implementatie van het CyFun® Framework de betrokken entiteiten een vermoeden van conformiteit in het kader van het toezicht onder NIS2. Het CCB raadt alle NIS2-entiteiten aan het CyFun® Framework te gebruiken.





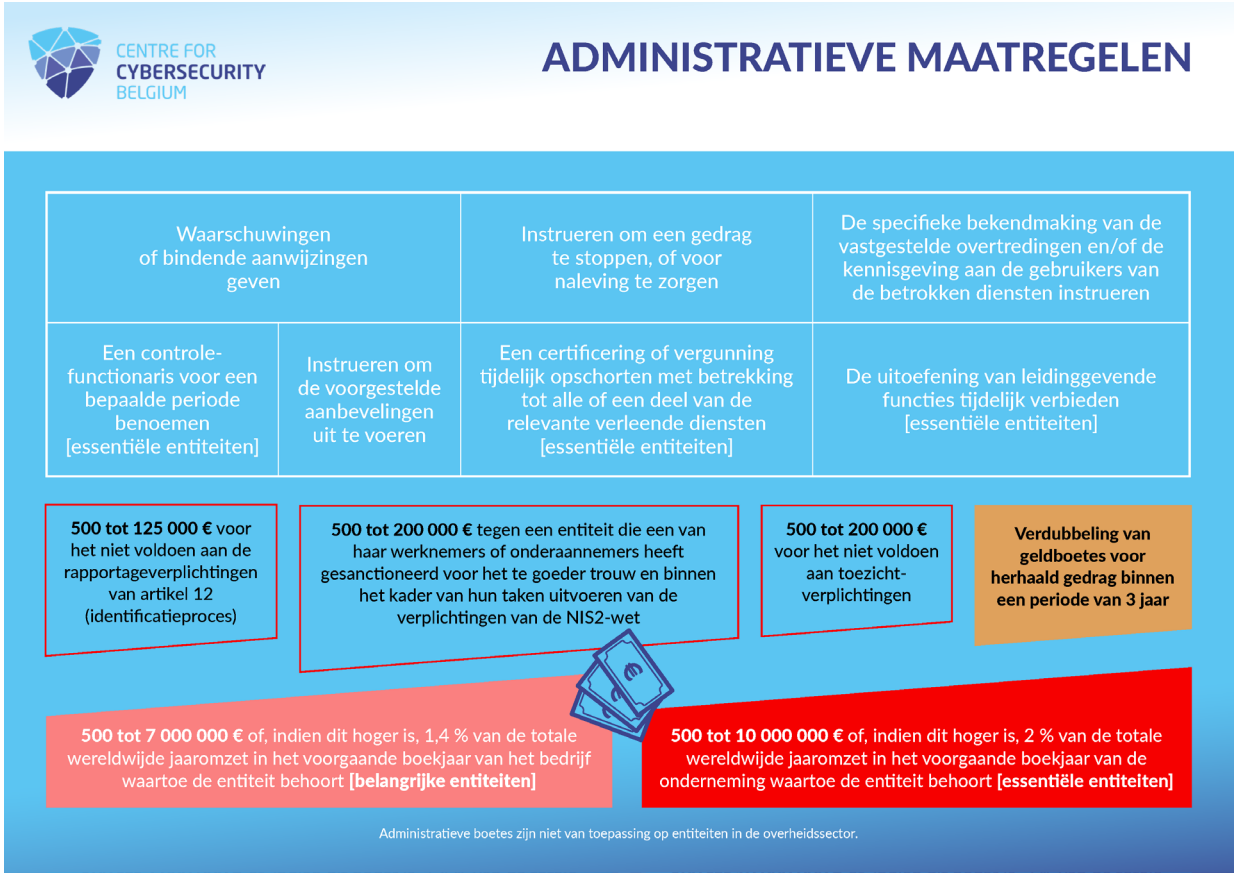
V. Sancties

NIS2-entiteiten die hun verplichtingen niet nakomen, kunnen worden onderworpen aan een reeks administratieve maatregelen en boetes.

Het CCB heeft als hoofddoel een hoog cyberbeveiligingsniveau in het hele land te bereiken, in nauwe samenwerking met alle betrokken entiteiten. Er zijn echter situaties waarin sancties nodig kunnen zijn. Hiervoor voorziet de wet (titel 4, hoofdstuk 2) in een specifieke procedure die de interactie tussen het CCB en de betrokken entiteit beschrijft. Deze procedure omvat de verplichting voor het CCB (of een sectorale overheid) om de entiteit te informeren over haar voornemen om een sanctie op te leggen. Dit ontwerp van beslissing dient voldoende gemotiveerd moet zijn. De entiteit heeft de mogelijkheid om zich vervolgens te verweren.

Als een sanctie nog steeds nodig wordt geacht, moet het CCB rekening houden met een bepaald minimumaantal elementen om een passende en evenredige sanctie te bepalen, bijvoorbeeld de categorie van de entiteit, de ernst van de overtreding, de duur ervan, eerdere overtredingen, schade, nalatigheid etc.

De lijst met mogelijke administratieve maatregelen en boetes is te vinden in de onderstaande infographic:



VI. Tijdlijn

De meeste bepalingen uit het wettelijke kader van NIS2 treden in werking op 18 oktober 2024. Voor de uitvoering van sommige verplichtingen geeft de wet of het koninklijk besluit entiteiten echter meer tijd.

Vanaf 18 oktober 2024 zijn met name de volgende verplichtingen onmiddellijk van toepassing:

- het nemen van de minimale maatregelen voor het beheer van cyberbeveiligingsrisico's;
- het melden van alle significante incidenten;
- zich onderwerpen aan het toezicht en samenwerken met bevoegde overheden;
- voor bestuursorganen: maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren, toezicht houden op de uitvoering van maatregelen, aansprakelijkheid voor overtredingen door de entiteit en het volgen van cyberbeveiligingsopleidingen.

Voor de registratie van entiteiten bij het CCB via Safeonweb@Work voorziet de wet in deadlines:

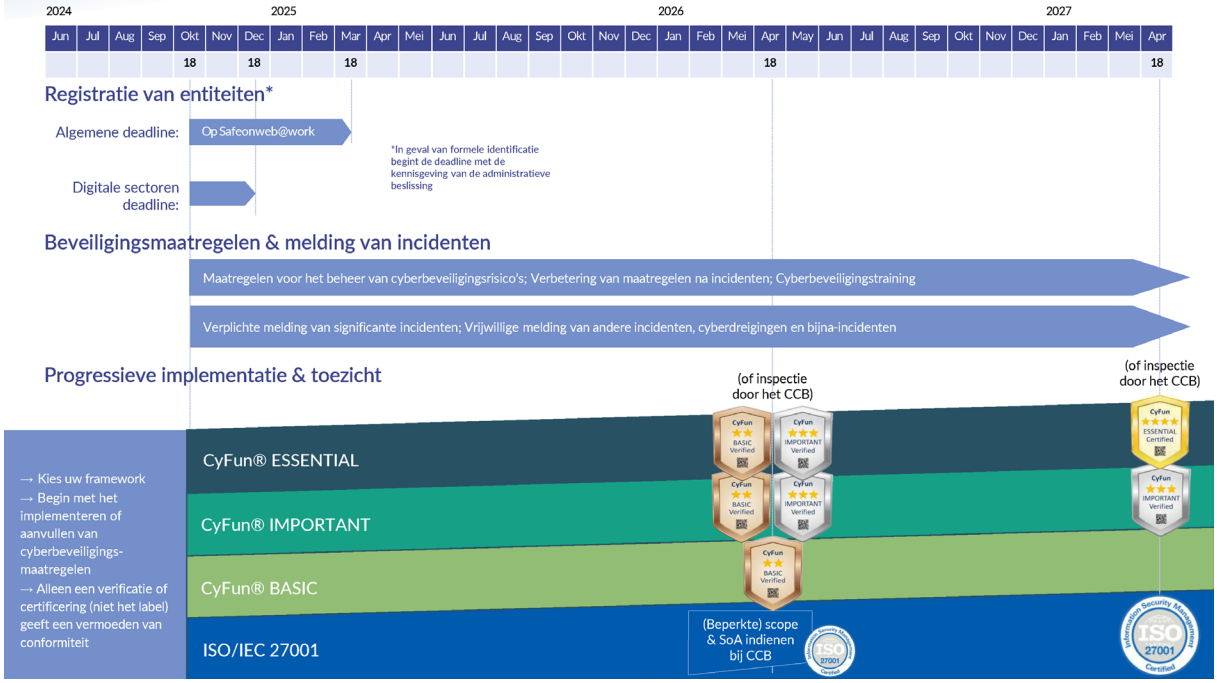
- entiteiten die diensten verlenen die onder de digitale sectoren van de bijlagen vallen, hebben twee maanden de tijd vanaf 18 oktober 2024 om zich te registreren (**uiterlijk tot 18 december 2024**) (lijst in art. 14, §1 van de wet);
- alle andere entiteiten hebben vijf maanden de tijd vanaf 18 oktober 2024 om zich te registreren (**uiterlijk tot 18 maart 2025**).

Het toezicht/de regelmatige conformiteitsbeoordeling van essentiële entiteiten verlopen ook stapsgewijs:

- Voor het CyberFundamentals (CyFun®) Framework:
  - Entiteiten die op basis van hun risicobeoordeling bepalen dat ze moeten voldoen aan het **zekerheidsniveau Basic**, hebben een deadline van 18 maanden (**uiterlijk op 18 april 2026**) om een verificatie te verkrijgen door een geaccrediteerde en erkende conformiteitsbeoordelingsinstantie (hierna "CAB");
  - Entiteiten die op basis van hun risicobeoordeling bepalen dat ze moeten voldoen aan het **zekerheidsniveau Important**, hebben een deadline van 18 maanden (**uiterlijk op 18 april 2026**) om ofwel een Basic of een Important verificatie te verkrijgen door een geaccrediteerde en erkende CAB.
    Indien nodig kunnen zij een eerste verificatie op niveau Basic verkrijgen en na nog eens 12 maanden een verificatie op niveau Important (**uiterlijk op 18 april 2027**);
  - Entiteiten die op basis van hun risicobeoordeling bepalen dat ze moeten voldoen aan het **zekerheidsniveau Essential**, hebben een deadline van 18 maanden (**uiterlijk op 18 april 2026**) om ofwel een Basic of een Important verificatie te verkrijgen door een geaccrediteerde en erkende CAB.
    Ze hebben een extra deadline van 12 maanden (**uiterlijk op 18 april 2027**) waarbinnen ze een zekerheidsniveau Essential certificering moeten verkrijgen door een geaccrediteerde en erkende CAB.
- Entiteiten die kiezen voor ISO/IEC 27001-certificatie, moeten hun toepassingsgebied en *statement of applicability* **uiterlijk op 18 april 2026** indienen bij het CCB **en op uiterlijk 18 april 2027** door een CAB gecertificeerd zijn.
- Entiteiten die ervoor kiezen om rechtstreeks door het CCB te worden geïnspecteerd:
  - **Uiterlijk op 18 april 2026**: hun zelfbeoordeling van CyFun® zekerheidsniveau Basic of Important, of hun ISO/IEC 27001-informatiebeveiligingsbeleid, toepassingsgebied en *statement of applicability* aan het CCB overmaken.
  - **Uiterlijk op 18 april 2027**: verslag over de voortgang m.b.t. de conformiteit.

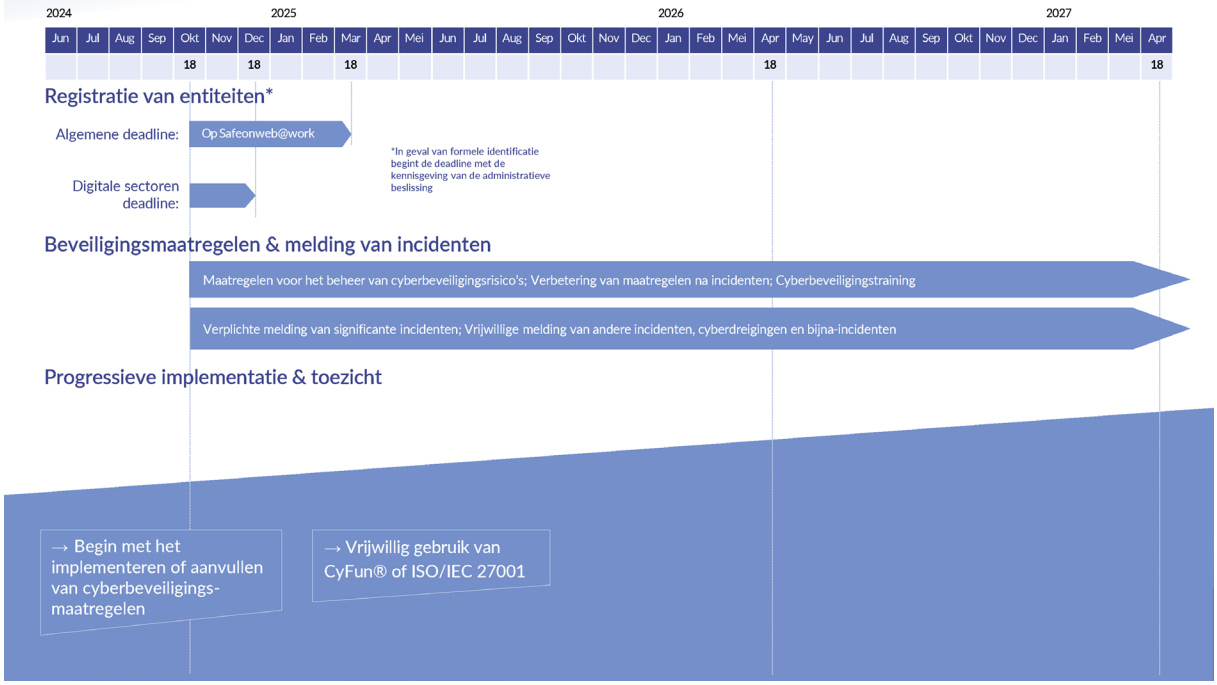
CENTRE FOR CYBERSECURITY BELGIUM

TIJDLIJN IMPLEMENTATIE ESSENTIËLE ENTITEITEN



CENTRE FOR CYBERSECURITY BELGIUM

TIJDLIJN IMPLEMENTATIE BELANGRIJKE ENTITEITEN



CENTRE FOR CYBERSECURITY BELGIUM

BIJLAGE I: ZEER KRITIEKE SECTOREN

SECTOR	SUBSECTOR en/of SOORT ENTITEIT		GROTE ONDERNEMINGEN *aantal werkzame personen van ten minste 250 VTE, of > € 50 mln jaaromzet en € 43 mln jaarlijks balanstotaal*	MIDDELGROTE ONDERNEMINGEN *aantal werkzame personen van ten minste 50 VTE, of > € 10 mln jaaromzet / jaarlijks balanstotaal*	KLEINE & MICRO-ONDERNEMINGEN
1. Energie	Elektriciteit	Elektriciteitsbedrijven; Distributiesysteembeheerders; Transmissiesysteembeheerders; Producenten; Benoemde elektriciteitsmarktbeheerders; Marktdeelnemers; Exploitanten van een laadpunt	Essentieel	Belangrijk*	Alleen indien geïdentificeerd*
	Stadsverwarming en -koeling	Exploitanten van stadsverwarming of stadskoeling			
	Aardolie	Exploitanten van oliepijpleidingen; Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport; Centrale entiteiten voor de voorraadvorming			
	Aardgas	Leveringsbedrijven; Distributiesysteembeheerders; Transmissiesysteembeheerders; Opslagsysteembeheerders; LNG-systeembeheerders; Aardgasbedrijven; Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas			
	Waterstof	Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof			
2. Vervoer	Lucht	Luchtvaartmaatschappijen; Luchthavenbeheerders, luchthavens, en de entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden; Exploitanten op het gebied van verkeersbeheer en -controle die luchtverkeersleidingsdiensten			
	Spoor	Infrastructuurbeheerders; Spoorwegondernemingen			
	Water	Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht; Beheerders van havens en entiteiten die werken en uitrusting in havens beheren; Exploitanten van verkeersbegeleidingssystemen (VBS)			
	Weg	Wegenautoriteiten die verantwoordelijk zijn voor het verkeersbeheer, met uitzondering van overheidsinstanties waarvoor verkeersbeheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteit is; Exploitanten van intelligente vervoerssystemen			
3. Bankwezen	Kredietinstellingen *[DORA Lex specialis]*				
4. Infrastructuur voor de financiële markt	Exploitanten van handelsplatformen; Centrale tegenpartijen *[DORA Lex specialis]*				
5. Gezondheidszorg	Zorgaanbieders; EU-referentielaboratoria; onderzoeks- en ontwikkelingsactiviteiten met betrekking tot geneesmiddelen; vervaardiging van farmaceutische basisproducten en farmaceutische bereidingen; vervaardiging van medische hulpmiddelen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd				
6. Drinkwater	Leveranciers en distributeurs van voor menselijke consumptie bestemd water, alleen indien essentieel deel van hun algemene activiteit				
7. Afvalwater	Ondernemingen die stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater opvangen, lozen of behandelen, alleen indien essentieel onderdeel van hun algemene activiteit				
8. Digitale infrastructuur	Gekwalificeerde verleners van vertrouwensdiensten		Essentieel		
	DNS-dienstverleners [met uitzondering van exploitanten van root-naamservers]				
	Register voor topleveldomeinnamen				
	Aanbieders van openbare elektronischecommunicatienetwerken of openbare elektronischecommunicatiediensten		Essentieel		Belangrijk*
	Niet-gekwalificeerde verleners van vertrouwensdiensten		Essentieel	Belangrijk*	Alleen indien geïdentificeerd*
	Aanbieders van internetknooppunten				
	Aanbieders van cloudcomputingdiensten				
	Aanbieders van datacentrumdiensten				
	Aanbieders van netwerken voor de levering van inhoud				
9. Beheer van ICT-diensten	Aanbieders van beheerde (beveiligings-) diensten				
10. Overheid (uitgezonderd rechterlijke macht, parlementen, centrale banken; nationale veiligheid, openbare veiligheid, defensie of wetshandhaving)	Overheden die van de Federale Staat afhangen		Essentieel		
	Overheden die van de deelgebieden afhangen (na identificatie op basis van een risicobeoordeling van de kritiekheid van de geleverde diensten)		Belangrijk*		
	Hulpverleningszones (waaronder de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp)				
11. Ruimtevaart	Exploitanten van grondfaciliteiten die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronischecommunicatienetwerken		Essentieel	Belangrijk*	Alleen indien geïdentificeerd*

Definities van deze soorten entiteiten zijn te vinden in bijlagen I en II of in artikel 8 van de NIS2-wet.

(*) Het CCB kan bepaalde belangrijke entiteiten als essentiële entiteiten identificeren of andere categorieën van soorten entiteiten binnen een sector als belangrijk of essentieel identificeren, afhankelijk van de kritiekheid van de geleverde diensten en de risico's die worden gelopen.

CENTRE FOR CYBERSECURITY BELGIUM

BIJLAGE II: ANDERE KRITIEKE SECTOREN

SECTOR	SUBSECTOR en/of SOORT ENTITEIT	GROTE ONDERNEMINGEN *aantal werkzame personen van ten minste 250 VTE, of > € 50 mln jaaromzet en € 43 mln jaarlijks balanstotaal*	MIDDELGROTE ONDERNEMINGEN *aantal werkzame personen van ten minste 50 VTE, of > € 10 mln jaaromzet / jaarlijks balanstotaal*	KLEINE & MICRO-ONDERNEMINGEN
1. Post- en koeriers-diensten	Aanbieders van postdiensten, met inbegrip van aanbieders van koeriersdiensten	Belangrijk*		Alleen indien geïdentificeerd*
2. Afvalstoffenbeheer	Alleen indien voornaamste economische activiteit			
3. Chemische stoffen	Vervaardiging van stoffen en distributie van stoffen of mengsels; Productie van voorwerpen uit stoffen of mengsels			
4. Levensmiddelen	Groothandel en industriële productie en verwerking			
5. Vervaardiging	Medische hulpmiddelen (voor in-vitrodiagnostiek); informaticaproducten en van elektronische en optische producten; elektrische apparatuur; machines, apparaten en werktuigen, n.e.g.; motorvoertuigen, aanhangers en opleggers; andere transportmiddelen (NACE C 26-30)			
6. Digitale aanbieders	Aanbieders van onlinemarktplaatsen			
	Onlinezoekmachines			
	Platforms voor socialenetwerkdiensten			
7. Onderzoek	Onderzoeksorganisaties, met uitzondering van onderwijsinstellingen			

(*) Het CCB kan bepaalde belangrijke entiteiten als essentiële entiteiten identificeren of andere categorieën van soorten entiteiten binnen een sector als belangrijk of essentieel identificeren, afhankelijk van de kritiekheid van de geleverde diensten en de risico's die worden gelopen.

Opmerking: Entiteiten die domeinnaamregistratiediensten verlenen, vallen ook onder NIS2, maar zij moeten zich alleen registreren op Safeonweb@Work en een nauwkeurige en volledige database met domeinnaamregistratiegegevens creëren en bijhouden.

DE NIS2-RICHTLIJN IN BELGIË

Verantwoordelijke uitgever:
Centrum voor Cybersecurity België
M. De Bruycker, Directeur-generaal
Wetstraat 18
1000 Brussel

Wettelijk depot:
D/2024/14828/006