CARU COMMV. Torhoutsesteenweg 2A/0502 8400 OOSTENDE
Erkend opleidingsorganisator FSMA

OPLEIDINGEN FORMATIONS CONSULTANCY

info@caru-commv.be
https//www.caru-commv.be

CARU OVERHEIDSOPDRACHTEN 2026

THEMANUMMER JULI 2026

CTBER RISICO'S

EUROPESE RICHTLIJN CYBER NIS2 EN DE IMPACT OP DE GEDECENTRALISEERDE EN LOKALE BESTUREN

PROF RUDI CLAEYS

Ed. 07/2026 VEWA Copyright © 2026

1. INLEIDING

1.1 De Europese Directieve NIS2

In 2016 introduceerde de EU de Directive on Security of Network and Information Systems (NIS Directive). Deze NIS1 stelt op het gebied van cybersecurity strenge eisen aan zogenoemde 'essentiële bedrijven'. Dit zijn bijvoorbeeld water-, energie- en telecombedrijven.
De NIS2 is een aanvulling op en uitbreiding van de richtlijn die meer bedrijven aanmerkt als essentieel bedrijf of als een onderneming die belangrijke diensten aan consumenten levert.

Met de NIS2 kunnen organisaties worden aangemerkt als essentieel of belangrijk, **waarbij dezelfde eisen voor cyber-security management en meldingsplicht gelden**.

Het belangrijkste verschil tussen de twee is de **mate van toezicht** op het naleven van de regels.

a) Voor essentiële aanbieders, voornamelijk uit de vitale sectoren, moet het toezicht streng proactief zijn en duidelijk zichtbaar zijn in hun processen. Dit betekent dat toezichthouders controleren of deze organisaties de regels correct toepassen en naleven.
b) Voor belangrijke aanbieders vindt het toezicht plaats achteraf, als er aanwijzingen zijn voor een cyberincident.

1.2 De omzetting in Belgisch recht

Met de wet van 26 april 2024 'Wet tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid' ("NIS2-wet") heeft de federale overheid de Europese NIS 2-richtlijn (Richtlijn (EU) 2022/2555) omgezet in een federale wet die volgens Art. 98 ;op 18 oktober 2024 in werking is getredentreden. (Staatsblad 17/3/2024)

Het KB 9 JUNI 2024. - Koninklijk besluit 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- geeft hieraan de verdere uitvoering.

Art. 3.§ 1. Het Centrum voor Cybersecurity België, opgericht bij het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, wordt aangewezen als nationale cyberbeveiligingsautoriteit.

Art. 4. § 1. De nationale cyberbeveiligingsautoriteit zorgt, in overleg met de relevante belanghebbenden, voor de uitwerking, actualisering en openbaarmaking, met name via haar website, van een referentiekader. Dit kader bevat de praktische modaliteiten voor de

beoordeling van de in artikel 30, § 3, van de NIS2-wet, bedoelde minimale maatregelen voor het beheer van cyberbeveiligingsrisico's
Overeenkomstig de internationale regels met betrekking tot conformiteitsbeoordelingsschema's zijn de in het eerste lid bedoelde relevante belanghebbenden ten minste de autoriteiten vermeld in artikel 15 van de NIS2-wet, de geaccrediteerde instanties en de organisaties die het referentiekader het eerste lid gebruiken.
§ 2. Het referentiekader beschrijft, op evenredige wijze, ten minste de volgende zekerheidsniveaus: basis, belangrijk en essentieel.

De modaliteiten voor de conformiteitsbeoordeling maken het voorwerp uit van volgende hoofdstukken vanhet Koninklijk Besluit:

HOOFDSTUK 4. - Modaliteiten van de regelmatige conformiteitsbeoordeling van essentiële entiteiten
HOOFDSTUK 5. - Modaliteiten van de regelmatige vrijwillige conformiteitsbeoordeling van belangrijke entiteiten door een conformiteitsbeoordelingsinstantie

1.3 Doelstelling

Het doel van de wetgeving is om entiteiten die diensten leveren die essentieel zijn voor het in stand houden van kritieke maatschappelijke of economische activiteiten beter te beveiligen tegen cyberaanvallen en ernstige verstoringen.
Daarnaast moet NIS2 ook leiden tot een goede samenwerking waarbij informatie rond dreigingen en incidenten vlot kan gedeeld worden.

2. TOEPAASINGSGEBIED

De NIS2-wet identificeert overheidsinstanties (federale en gefedereerde overheden) als kritieke dienstverleners, alsook de sectoren energie, vervoer, bankwezen, financiële markten, gezondheid, digitale infrastructuur en ruimtevaart.

Lokale besturen, onder meer gemeenten, provincies, OCMW-verenigingen, vallen niet onder het toepassingsgebied van de NIS2-wet, als ze niet geïdentificeerd zijn als NIS2-entiteiten (essentieel of belangrijk) of ze niet ten minste één van de kritieke activiteiten uit bijlage I of II van de wet uitvoeren.

2.1 Wettelijke omschrijving

Wet

Definitie van het toepassingsgebied Art.3 §3
3° de entiteit is een overheidsinstantie:
a) die van de Federale Staat afhangt;
b) die van de deelgebieden afhangt, geïdentificeerd overeenkomstig artikel 11, § 2;
(*Art.11§ 2. Wat betreft de entiteiten die van de deelgebieden afhangen, identificeert de nationale cyberbeveiligingsautoriteit overheidsinstanties die, na een risicobeoordeling, diensten verlenen waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschappelijke of economische activiteiten.)*
c) die een hulpverleningszone is 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 in de zin van de ordonnantie van 19 juli 1990 houdende oprichting van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp.

Bijlage I bij de wet:

10. Overheid	- Overheidsinstanties die van de Federale Staat afhangen
	- Overheidsinstanties die van de deelgebieden afhangen, geïdentificeerd overeenkomstig artikel 11, § 2, van de wet *§ 2. Wat betreft de entiteiten die van de deelgebieden afhangen, identificeert de nationale cyberbeveiligingsautoriteit overheidsinstanties die, na een risicobeoordeling, diensten verlenen waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschappelijke of economische activiteiten*
	- 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

Lokale overheidsinstellingen (gemeenten, provincies, intercommunales, openbare centra voor maatschappelijk welzijn (ocmw's), gemeentebedrijven enz.) vallen niet automatisch onder de NIS2-verplichtingen. Ze worden namelijk niet expliciet genoemd in de bijlagen van de NIS2-wet in de overheidssector. *(Art. 8, 34°; bijlage I, sector 10 (Overheid) NIS2-wet)*

Hoewel lokale overheidsinstanties zoals hierboven opgesomd voldoen aan de definitie van artikel 8, 34° **hangen ze niet af van de federale Staat**, noch van de gefedereerde entiteiten. *(Art.8 34° "overheidsinstantie": 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).

Overeenkomstig 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.

2.2 Uitzonderlijke toepassing op de lokale besturen

a) Deze lokale entiteiten kunnen echter wel **onder het toepassingsgebied van de NIS2-wet vallen als ze een dienst verlenen die is opgenomen in bijlage I of II van de wet** (andere dan in de sector overheid) en en als een essentiële of belangrijke entiteit beschouwd worden en als ze ten minste als middelgrote onderneming kunnen worden aangemerkt.
(Bijlage I - Zeer kritieke sectoren
Bijlage II - Andere kritieke sectoren)

Hun **kwalificatie als essentiële en belangrijke entiteit** onder de wet hangt dus af van de geleverde dienst en hun omvang.

b) Lokale overheidsinstanties kunnen ook onder het toepaszingsveld vallen als ze worden **aangewezen door middel van artikel 11,** § 1 (aanwijzing door de nationale cyberbeveiligingsautoriteit - CCB), op voorwaarde dat de raadplegingsprocedure, voorzien in artikel 11, § 3, wordt nageleefd. Het initiatief voor een dergelijke aanwijzing kan worden genomen op verzoek van de nationale cyberbeveiligingsautoriteit, de betrokken entiteit of een deelgebied.

(Art. 11. § 1. Onverminderd artikel 6 identificeert de nationale cyberbeveiligingsautoriteit, op eigen initiatief of op voorstel van de eventuele betrokken sectorale overheid, een entiteit als een essentiële of belangrijke entiteit, 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.
§ 2. Wat betreft de entiteiten die van de deelgebieden afhangen, identificeert de nationale cyberbeveiligingsautoriteit overheidsinstanties die, na een risicobeoordeling, diensten verlenen waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschappelijke of economische activiteiten.

2.3 CONCLUSIE: Toepassingsgebied op overheidsinstellingen

NIS2 geeft regels aan lidstaten over alle entiteiten die actief zijn in (zeer) kritieke sectoren. De overheid staat als zeer kritieke sector genoemd onder nr. 10 van de tabel uit Bijlage I.
Centrale overheidsinstanties vallen onder artikel 2 lid 2 onder f onder i) van NIS2.
Lokale overheidsinstanties hebben volgens artikel 2 lid 5 van de Directieve onder a) eerst een besluit van de lidstaat nodig**.**

De lokale en gedecentraliseerde besturen kunnen dus op heden pas onder de toepassing van de wet vallen, als ze onder te brengen zijn in één van volgende categorie

- **Een essentiële entiteit zijn**
- **Ee belangrijke entiteit in de zin van de wet**
- **Of een door CCB aangewezen activiteit**

2.4 Begrip essentiële entiteiten

Art. 9. Zijn essentiële entiteiten:
1° de entiteiten van een in bijlage I bedoelde soort die de plafonds voor middelgrote ondernemingen overschrijden die zijn bepaald in artikel 2, lid 1, van de bijlage bij Aanbeveling nr. 2003/361/EG;
2° de gekwalificeerde verleners van vertrouwensdiensten en de registers voor topleveldomeinnamen, alsook de DNS-dienstverleners, ongeacht hun omvang;
3° de aanbieders van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten die minstens in aanmerking komen als middelgrote ondernemingen uit hoofde van artikel 2 van de bijlage bij Aanbeveling nr. 2003/361/EG;
4° de overheidsinstanties die van de Federale Staat afhangen;
5° de entiteiten bedoeld in artikel 3, § 4;
6° alle andere entiteiten van een in bijlage I of II bedoelde soort die worden geïdentificeerd als essentiële entiteiten overeenkomstig artikel 11.

Essentiële entiteiten zijn grote organisaties die actief zijn in sectoren die als kritiek worden beschouwd voor de maatschappij en economie. Het gaat om bedrijven en instellingen met meer dan 250 medewerkers of een jaaromzet boven de 50 miljoen euro, actief in sectoren zoals energie, drinkwater, transport, bankwezen, gezondheidszorg, digitale infrastructuur en overheid.
De redenering achter deze indeling is dat een cyberincident bij deze organisaties direct grote maatschappelijke gevolgen kan hebben. Denk aan een stroomnetwerk dat uitvalt, een ziekenhuis dat niet meer bij patiëntgegevens kan, of een haven die plat ligt. De NIS2-richtlijn erkent dat juist deze partijen het meest aantrekkelijk zijn als doelwit voor aanvallers en tegelijkertijd het meest kwetsbaar zijn als het misgaat.
Naast de omvangscriteria kunnen ook kleinere organisaties als essentieel worden aangemerkt, namelijk wanneer zij een unieke of onvervangbare rol spelen in hun sector. Dit wordt bepaald door de bevoegde nationale autoriteit, in Nederland de Rijksinspectie Digitale Infrastructuur (RDI).

2.5 Begrip belangrijke entiteiten

Art. 10. Zijn belangrijke entiteiten:
1° de entiteiten van een in bijlage I of II bedoelde soort die niet als essentiële entiteiten worden beschouwd op basis van artikel 9; 2° de entiteiten die worden geïdentificeerd als belangrijke entiteiten overeenkomstig artikel 11.

Art. 11. § 1. Onverminderd artikel 6 identificeert de nationale cyberbeveiligingsautoriteit, op eigen initiatief of op voorstel van de eventuele betrokken sectorale overheid, een entiteit als een essentiële of belangrijke entiteit, 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.

Belangrijke entiteiten zijn middelgrote organisaties die actief zijn in dezelfde kritieke sectoren als essentiële entiteiten, maar kleiner van omvang zijn. Zij hebben doorgaans tussen de 50 en 250 medewerkers en een jaaromzet tussen de 10 en 50 miljoen euro. Daarnaast vallen ook organisaties in aanvullende sectoren, zoals afvalbeheer, chemische industrie, voedselproductie en digitale aanbieders, in deze categorie.
De NIS2-richtlijn breidt met de categorie “belangrijke entiteiten” het toepassingsgebied aanzienlijk uit ten opzichte van de oude NIS1-richtlijn. Veel organisaties die voorheen buiten de scope vielen, zijn nu wettelijk verplicht om maatregelen te treffen op het gebied van NIS2-compliance. Dit geldt ook voor een groot deel van de maakindustrie en toeleveranciers in complexe keten**s.**

2.6 Bepalingsmethode voor uw categorie

Een organisatie bepaalt haar categorie op basis van drie factoren: **de sector** waarin zij actief is, haar **omvang in medewerkers** en **omzet**, en eventuele aanvullende criteria die de nationale toezichthouder hanteert. De NIS2-richtlijn biedt hiervoor een gestructureerd kader dat stap voor stap doorlopen kan worden.
Doorloop de volgende stappen om uw categorie te bepalen:

1. Controleer of uw sector voorkomt in de bijlagen van de NIS2-richtlijn (bijlage I voor essentieel, bijlage II voor belangrijk)
2. Bepaal uw organisatieomvang op basis van medewerkers en jaaromzet(*voor een lokaal bestuur betekent dit de som van de opbrengsten uit de werking, de andere operationele opbrengsten, de werkingssubsidies en de belastingopbrengsten. De gegevens voor de berekening van het aantal werkzame personen en van de jaaromzet hebben betrekking op het laatst afgesloten boekjaar en kan elke twee jaar worden herzien).
3. Ga na of uw organisatie een unieke of kritieke rol vervult die een hogere classificatie rechtvaardigt
4. Raadpleeg de nationale toezichthouder (CCB) of relevante sectorale autoriteit voor bevestiging
5. Leg de uitkomst vast in uw interne documentatie en koppel dit aan uw risicobeleid

2.7 STANDPUNT VVSG

De NIS2-richtlijn heeft ook haar toepassingsgebied uitgebreid, waardoor er meer entiteiten en sectoren worden verplicht maatregelen te nemen. Zo is de richtlijn ***automatisch van toepassing op overheidsdiensten van centraal en regionaal niveau****.*
De lidstaten kunnen zelf beslissen of ook de lokale overheidsinstanties gevat worden

De VVSG is geen voorstander om de lokale besturen mee te nemen als entiteiten die onder de NIS2-verplichtingen vallen omdat er vandaag nog geen duidelijke strategie en doordacht plan van aanpak op tafel ligt dat de cyberweerbaarheid van de lokale besturen verhoogt.
Uiteraard mogen we van de lokale besturen wel verwachten dat ze meer werk maken van het thema en dat het hoger op hun agenda komt. Maar door hen louter een verplichting op te leggen zullen we deze doelstellingen niet halen. Een ondoordachte verplichting zal eerder leiden tot zeer hoge investeringen (vaak dubbel op en zonder alle synergiën te benutten) en verlegt de focus op administratieve lasten en compliance zonder garantie op het effectief verhogen van hun cyberweerbaarheid.

Dit wil allerminst zeggen dat we vandaag al geen actie kunnen of moeten ondernemen. Vanuit de veronderstelling dat de lokale besturen bij een opvolging van de richtlijn wel als belangrijke entiteiten worden beschouwd en vanuit de vaststelling dat lokale besturen vaker slachtoffer worden van cyberaanvallen, is het cruciaal dat we vandaag werk maken van een duidelijke strategie en plan van aanpak. De strategie en bijhorend plan van aanpak moeten een duidelijke richting geven over hoe we de uitdagingen van de lokale besturen rond cyberveiligheid (zie bijlage) structureel en collectief kunnen opnemen. De

uitdagingen rond cyberveiligheid zijn immers van die aard dat zo goed als geen enkel lokaal bestuur deze individueel te baas kan.

Rond de uitdaging 'Technologie' bijvoorbeeld lijkt het ons niet onlogisch dat we (gegeven de versnippering op vlak van IT-systemen) op termijn meer moeten evolueren naar een standaard IT-omgeving waar de lokale besturen vrijblijvend gebruik van kunnen maken. Allereerst moeten we duidelijk en volledig zicht krijgen op de huidige situatie bij de lokale besturen op vlak van (1) ICT-omgeving, (2) ICT-organisatie en (3) de grote lijnen van het applicatielandschap. Rekening houdend met deze AS IS moeten we verschillende scenario's van gewenste situaties definiëren met verschillende ambitieniveaus. Elk scenario bevat de kosten en baten en een gefaseerde roadmap om tot de gewenste situatie te bekomen. Rond elk van de drie hieronder gedefinieerde uitdagingen moeten we zicht krijgen hoe we collectief stappen vooruit kunnen zetten. Eens we over een duidelijk en gedragen plan beschikken kunnen we een (gefaseerde) verplichting voor de lokale besturen overwegen. Een strategie en plan van aanpak laat ons bovendien ook toe om de huidige en toekomstige acties gerichter te kunnen bepalen. De Vlaamse overheid neemt vandaag immers al heel wat acties om de weerbaarheid op vlak van cyberveiligheid bij de lokale besturen te verhogen. Denk aan de cloud landingzone, het Vlaamse cyberresponse team, de cybercase van Lokaal Digitaal (SIEM/SOC as service), het project cyberveilige gemeenten met onder andere toolkit en traject ethisch hacken, cofinanciering audits, ... Al deze projecten hebben hun toegevoegde waarde, maar zijn vooralsnog losse elementen die niet kunnen ondergebracht worden in zo'n ruimere strategie en plan van aanpak.

3. AANSPRAKELIJKHEIDSREGELS

3.1 Omschrijvingen van verplichtingen en verantwoordelijkheden

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 risicobeheersmaatregelen niet nakomt, is het bestuursorgaan aansprakelijk.
Leden van bestuursorganen zijn verplicht om opleiding te volgen om ervoor te zorgen dat hun kennis en vaardigheden voldoende zijn om risico's te identificeren en maatregelen te beoordelen voor het beheer van cyberbeveiligingsrisico's en de impact daarvan op de diensten die door de betrokken entiteit worden geleverd.
De verantwoordelijke natuurlijke personen en/of wettelijke vertegenwoordigers van een entiteit moeten de bevoegdheid hebben om ervoor te zorgen dat de entiteit de wet naleeft. Ze zijn aansprakelijk als ze dit nalaten.
Het doel van deze verantwoordingsplicht is om cyberbeveiliging te veranderen in een onderwerp dat er echt toe doet voor de betrokken entiteiten.
Deze aansprakelijkheidsregels doen geen afbreuk aan de aansprakelijkheidsregels die van toepassing zijn op publieke instellingen, noch aan de aansprakelijkheid van ambtenaren en verkozen of aangestelde ambtenaren.
Natuurlijke personen die leidinggevende functies uitoefenen op het niveau van directeur of wettelijk vertegenwoordiger in een NIS2-entiteit kunnen tijdelijk worden uitgesloten van het uitoefenen van leidinggevende verantwoordelijkheden in deze entiteit, in geval van schending van de vereisten van de NIS2-wet.

NIS 2 heeft ook gevolgen voor de bestuursorganen van ondernemingen die onder NIS2 vallen. De wet stelt hen immers persoonlijk aansprakelijk indien de verplichtingen om maatregelen te nemen ter beheersing van cyberbeveiligingsrisico's niet worden nageleefd. De memorie van toelichting verwijst hiervoor niet enkel naar de raad van bestuur maar ook naar het hoger management als naar meerderheidsaandeelhouders!

3.2 Definitie van het bestuursorgaan in het kader van de NIS2 Wet

Het begrip "bestuursorgaan" is niet gedefinieerd in de richtlijn.
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 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 overeenkomstig artikel 1:14tot 1:18van 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.

3.3 Specifieke aansprakelijkheid binnen NIS2

De NIS2-wet bepaalt in 2 verschillende artikelen wie aansprakelijk gesteld kan worden bij de niet-naleving van de NIS2-wet en stelt telkens dat de NIS2-wet geen afbreuk doet aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, voor ambtenaren en voor verkozen of benoemde mandatarissen.

Hieronder wordt een inschatting gemaakt van de toepassing van deze regelgeving op de lokale besturen op basis van de beschikbare informatie.

De wet zelf bepaalt niet wie als bestuursorgaan ressorteert, maar de memorie van toelichting bepaalt wel wie **als 'lid van een bestuursorgaan'** beschouwd wordt.
Dit gaat zeer ruim.
Het zijn natuurlijke personen of rechtspersonen die ofwel in staat zijn enerzijds het lokaal bestuur te beheren of te vertegenwoordigen of anderzijds namens en voor rekening van het lokaal bestuur beslissingen te nemen of deel te nemen aan de besluitvorming ervan ofwel controle uitoefenen over de entiteit, namelijk de bevoegdheid hebben om een beslissende invloed uit te oefenen op de oriëntatie van het beleid.[1]
Wanneer de persoon wiens rol onderzocht wordt een **rechtspersoon is, omvat het zowel een bestuursorgaan als elk lid van een bestuursorgaan van** die rechtspersoon.
De bestuursorganen van een lokaal bestuur zijn vooreerst de politiek samengestelde organen. Voor de gemeente gaat het om de gemeenteraad, het college voor burgemeester en schepenen (CBS) en de burgemeester, terwijl het voor het OCMW gaat om de raad voor maatschappelijk welzijn, het vast bureau en (de voorzitter van) het bijzonder comité voor de sociale dienst.
Hoewel artikel 33 Decreet Lokaal Bestuur ('DLB') stelt dat de besluiten in de gemeenteraad genomen worden bij volstrekte meerderheid van stemmen en een individueel raadslid dus geen individuele beslissing kan nemen die de gemeenteraad bindt en hoewel artikel 52 DLB stelt dat het CBS een collectief orgaan is omdat de beslissingen in het CBS collegiaal genomen worden, kunnen **zowel de raadsleden als de uitvoerende mandatarissen beschouwd worden als een lid van het bestuursorgaan** volgens artikel 31 NIS2-wet.
Die definitie gaat namelijk zeer ruim en het omvat ook de personen die een functie uitoefenen binnen het bestuur die hen in staat stelt deel te nemen aan de besluitvorming over beslissingen die juridisch bindend zijn voor het bestuur. Dit is zowel van toepassing op de raadsleden als de uitvoerende mandatarissen.
Of de AD als (lid van) een bestuursorgaan beschouwd kan worden volgens artikel 31 NIS2-wet, lijkt af te hangen van welke taken de AD uitoefent. De AD is steeds een personeelslid van de gemeente (artikel 162 DLB) en heeft ook taken die hem of haar zijn gedelegeerd door het CBS/vast bureau[2] of zijn toegewezen[3] via wet of decreet. Die

taken oefent hij of zij uit als personeelslid, maar bij de uitoefening van die taken, kan de AD als (lid van) een bestuursorgaan functioneren. Dit moet steeds geval per geval, afhankelijk van de feiten, beoordeeld worden. Hierbij lijkt de mate waarin de AD handelt naar onderrichtingen van de politieke organen van belang om mee te nemen in de overweging of de AD onder de NIS2-wet handelt als een (lid van) een bestuursorgaan.

- **Artikel 61 NIS2-wet: natuurlijke personen**

Artikel 61 NIS2-wet bepaalt daarnaast dat de natuurlijke personen die het lokaal bestuur kunnen vertegenwoordigen, namens het lokaal bestuur beslissingen kunnen nemen of de bevoegdheid hebben controle uit te oefenen op het lokaal bestuur, de bevoegdheid hebben om ervoor te zorgen dat het lokaal bestuur de NIS2-wet nakomt. Deze personen kunnen aansprakelijk worden gesteld als ze deze verplichting niet nakomen.
Ook hier stelt zich de vraag wie binnen het lokaal bestuur als zulke natuurlijke persoon kan kwalificeren en aldus aansprakelijk kan worden gesteld volgens artikel 61 van de NIS2-wet.
In tegenstelling tot wat artikel 31 betreft (zie hierboven) wordt de verantwoordelijkheid onder artikel 61 niet uitgebreid naar personen met de bevoegdheid om *deel te nemen aan* de besluitvorming over zulke beslissingen, zoals dit wel het geval is onder artikel 31 NIS2-wet. Hierdoor lijkt een onderscheid gemaakt te moeten worden tussen de verschillende mandatarissen, afhankelijk van of ze een individuele dan wel collegiale beslissingsbevoegdheid hebben.
Zo hebben de burgemeester/voorzitter van het vast bureau[4] en de voorzitter van het BCSD[5] in bepaalde situaties wel individuele beslissingsmacht. Als ze die bevoegdheden uitoefenen en hierbij de NIS2-wet niet naleven, zullen zij aansprakelijk kunnen worden gesteld volgens artikel 61 NIS2-wet. Voor de overige mandatarissen lijkt artikel 61 NIS2-wet minder verregaand te zijn.
Wat betreft de AD kan verwezen worden naar diens opdracht om in te staan voor het organisatiebeheersingssysteem (zie artikel 171 DLB). De AD legt daarin de maatregelen en procedures vast om o.a. wetgeving en procedures na te leven. Volgens artikel 219 DLB blijft de AD verantwoordelijk voor dit proces. De organisatiebeheersing is een algemeen instrument, waarbij de toepassing van de NIS2-wetgeving als een concrete toepassing kan worden beschouwd. Het is dus de verantwoordelijkheid van de AD om het organisatiesysteem op die manier uit te werken dat de NIS2-wet nageleefd wordt. Evenwel is het aan de gemeente- of OCMW-raad om het algemene kader van het organisatiebeheersingssysteem goed te keuren. De AD zal zijn of haar toegewezen taak onder het DLB aldus moeten uitvoeren volgens het algemene kader dat door de raad uiteengezet is.
Tot slot, wat betreft de CISO (Chief Information Security Officer) kan worden gesteld dat deze over een adviserende of controlerende functie uitoefent in de organisatie. De CISO is geen bestuurder. In het DLB zijn er geen specifieke verantwoordelijkheden voor de CISO vermeld. De CISO heeft niet de bevoegdheid om het lokaal bestuur in rechte te vertegenwoordigen, noch om namens het lokaal bestuur beslissingen te nemen, noch om er controle op uit te oefenen.
Zoals hierboven al aangegeven, is het aan de bevoegde federale instantie en de rechtbanken en hoven om te oordelen of dit ook effectief zo is. FAQ 2.12 van het CCB lijkt alvast te bevestigen dat de burgemeester in zijn hoedanigheid als vertegenwoordiger van de gemeente volgens artikel 61 NIS2-wet aansprakelijk kan worden gesteld als de NIS2-wet niet wordt nageleefd.

- **Geen afbreuk aan bestaande aansprakelijkheidsregels**

Beide artikelen bepalen bijkomend dat de aansprakelijkheidsregels van de NIS2-wet geen afbreuk doen aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde overheidsfunctionarissen.
De algemene principes rond burgerrechtelijke aansprakelijkheid zijn vastgesteld in boek 6 van het Burgerlijk Wetboek. Artikel 6.5 bepaalt: 'Eenieder is aansprakelijk voor de schade die hij door zijn fout aan een ander veroorzaakt.' Dit maakt dat er bijgevolg sprake moet zijn van een fout, schade en een oorzakelijk verband tussen de fout en de schade vooraleer iemand aansprakelijk kan worden gesteld.
Mandatarissen van een lokaal bestuur genieten echter een beperkte persoonlijke aansprakelijkheid. Het DLB beperkt de burgerrechtelijke aansprakelijkheid van de mandatarissen bij de normale uitoefening van hun mandaat en dit zowel voor raadsleden (artikel 17, §5 en 6 DLB) als voor uitvoerende mandatarissen (artikel 157 DLB). Ze kunnen enkel persoonlijk aansprakelijk worden gesteld bij bedrog, zware schuld of herhaaldelijke lichte schuld. Dit principe geldt ook voor de aansprakelijkheid onder artikel 31 en 61 van de NIS2-wet.
Ook personeelsleden van een lokaal bestuur genieten een beperkte persoonlijke aansprakelijkheid. Dit houdt in dat zij enkel persoonlijk aansprakelijk kunnen worden gesteld bij bedrog of zware schuld of herhaaldelijke lichte schuld. Voor contractuele personeelsleden vloeit dit voort uit de arbeidsovereenkomstenwet (artikel 18) en voor de statutaire personeelsleden uit de wet van 10 februari 2003 betreffende de aansprakelijkheid van en voor personeelsleden in dienst van openbare rechtspersonen (artikel 2 WAPOP).
Zoals hierboven al aangehaald, blijft de AD steeds een personeelslid van het lokaal bestuur (artikel 162 DLB). Hij of zij zal dus ook genieten van de beperkte aansprakelijkheid zoals die van toepassing is op personeelsleden. Zelfs als in concrete situaties geoordeeld zou worden dat de AD als (lid van een) bestuursorgaan kan gelden en hierdoor aansprakelijk kan worden gesteld omwille van inbreuken op de verplichting om passende cyberbeveiligingsmaatregelen te treffen (artikel 31 NIS2-wet) of als de AD onder artikel 61 NIS2-wet aansprakelijk kan worden gesteld, dan blijft de beperkte aansprakelijkheid voor personeelsleden van kracht. Dit geldt ook voor de AD.

1. Voor de volledige definitie, zie De Kamer, doc. 55 3862/001 van 5 maart 2024, p. 46(PDF bestand opent in nieuw venster) of FAQ 3.10 CCB(opent in nieuw venster).
2. Voor de bevoegdheden die gedelegeerd kunnen worden, zie de volgende artikelen in het DLB: 56, 57, 84 en 84.
3. Voor de toegewezen taken in het DLB, zie de volgende artikelen: 20, 57, 74, 85, 170, 171, 172, 173, 217-220, 272, 277 en 279.
4. Zie hiervoor artikelen 133 tot en met 134septies van de gecoördineerde Nieuwe Gemeentewet van 24 juni 1988.
5. Zie hiervoor artikel 114 DLB.

- **Artikel 31, §1 NIS2-wet: bestuursorganen**

Allereerst, stelt de NIS2-wet in artikel 31, §1 dat de bestuursorganen aansprakelijk gesteld kunnen worden voor inbreuken op artikel 30 van de NIS2-wet. Dat artikel handelt over de maatregelen voor het beheer van cyberbeveiligingsrisico's.

NIS 2 Artikel 20 van de Directieve maakt een einde aan die illusie: vandaag, **elke directeur is individueel verantwoordelijk voor cyberparaatheid**- van de tekenkamer tot de rechtszaal. Bestuurskamergebruiken die niet-technische directeuren ooit toestonden te vertrouwen op de goedkeuring van de groep, vormen nu een risico. Toezichthouders richten zich op de inzet van elke directeur, met ruimte voor handhaving van lokale "gold-plating" die de nationale lat mogelijk hoger kan leggen (zie pwc.de). In de praktijk worden directeuren geconfronteerd met de mogelijkheid van directe interviews, verzoeken om bewijs van persoonlijke training en eisen om documenten die doorslaggevende deelname aantonen tijdens inbreuken in de praktijk.

Artikel 20 legt een nieuwe norm vast: louter aanwezigheid en jaarlijkse controlelijsten zijn niet voldoende. In plaats daarvan moeten bestuurders
actief **leiden**, **uitdaging**en **controleren** Cyberrisico in elke bestuurscyclus. Dit omvat:

- **Formele goedkeuring en bezwaar:** Beleidshandtekeningen alleen zijn niet voldoende. Bestuurders moeten aantonen dat zij aannames in twijfel hebben getrokken, onderzoek hebben gedaan naar zwakke punten en hun standpunten hebben vastgelegd, met name afwijkende meningen of nader onderzoek (zie nis-2-directive.com).
- **Verplichte jaarlijkse cybertraining:** Voor elke directeur, geregistreerd op datum en naam. Afwezigheid of wisseling moet leiden tot een herstellogboek, niet tot een stille overstap.
- **Continue betrokkenheid:** Cybertoezicht verschuift van statische 'agendapunten' naar een vast onderdeel van het maandelijkse of kwartaalritme van het bestuur; elke beoordeling, goedkeuring en kritiek moet worden gekoppeld aan een levende bewijsketen.

Doorverwijzing naar IT/compliance-teams biedt geen dekking. Directeuren moeten persoonlijke contactmomenten onderhouden en via gedocumenteerde logs bevestigen dat ze deze hebben onderzocht. proces verbaal, goedgekeurde controles op bestuursniveau en proactief gereageerd op wijzigingen in de regelgeving. Elk element moet audit-klaar en fouttolerant zijn, en centraal op papier of in spreadsheets vastgelegde paden worden nu als risicovol beschouwd.

De NIS2-wet verduidelijkt, in artikel 31, §1 en artikel 61, lid 2 dat deze aansprakelijkheidsregels geen voorrang hebben op of invloed hebben op de specifieke aansprakelijkheidsregels die reeds gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde overheidsfunctionarissen.

*Art. 31. § 1. **De bestuursorganen van essentiële en belangrijke entiteiten** keuren de maatregelen voor het beheer van cyberbeveiligingsrisico's goed die deze entiteiten nemen om te voldoen aan artikel 30, zien toe op de uitvoering ervan en zijn aansprakelijk voor inbreuken door deze entiteiten op dat artikel.*
Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde mandatarissen. § 2. De leden van de bestuursorganen van essentiële en belangrijke entiteiten volgen een opleiding zodat ze over voldoende kennis en vaardigheden beschikken om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de

gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.
Art. 32. ***De essentiële of belangrijke entiteit is verantwoordelijk*** *voor de uitgevoerde risicoanalyse, alsook voor de keuze en uitvoering van de maatregelen bedoeld in artikel 30, § 1. (Art. 30. § 1. De essentiële en belangrijke entiteiten nemen passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij voor hun activiteiten of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.)*

Art. 61. Elke ***natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijke vertegenwoordiger van een essentiële of een belangrijke entiteit*** *op basis van de bevoegdheid om deze te vertegenwoordigen, de bevoegdheid om namens deze entiteit beslissingen te nemen of de bevoegdheid om controle uit te oefenen op deze entiteit, heeft de bevoegdheid om ervoor te zorgen dat deze entiteit deze wet nakomt. Deze personen zijn aansprakelijk voor het niet nakomen van hun verplichtingen om te zorgen voor de naleving van deze wet.*
Dit artikel doet geen afbreuk aan de aansprakelijkheidsregels die gelden voor overheidsinstanties, alsook voor ambtenaren en verkozen of benoemde overheidsfunctionarissen.

Voor de **persoonlijke aansprakelijkheid** van natuurlijke personen die verantwoordelijkheid zijn voor of optreden als wettelijke vertegenwoordigers van een NIS2-entiteit in de overheidssector (“*leidinggevende functie”),* moet hun juridische status worden onderzocht:

- zijn ze **statutaire personeelsleden** ondergeschikt aan de overheidsinstantie, in welk geval zij genieten van de bescherming waarin artikel 2 van de wet van 10 februari 2003 voorziet voor schuld die niet neerkomt op grove schuld; Voor diegenen die onder de wet van 10 februari 2003 vallen, geldt dus de persoonlijke aansprakelijkheid zoals bedoeld in artikel 61, lid 1 wanneer er sprake is van **bedrog, zware schuld of kleine fouten van repetitieve aard** van de manager. (herhaalde lichte fout)
- of zijn ze **contractuele personeelsleden**, in welk geval zij onder artikel 18 van de wet van 3 juli 1978 betreffende de arbeidsovereenkomsten vallen;
- of zijn ze vertegenwoordigers zonder ondergeschiktheidsrelatie ten opzichte van publieke entiteit.

Gezien deze verschillen in bevoegdheden moet elke gemeente die onder NIS2 valt, intern nagaan welke organen in haar concrete situatie kunnen voldoen aan de in de wet vastgelegde aansprakelijkheidsregimes.

Een mogelijke interpretatie van deze aansprakelijkheidsregimes is dat de burgemeester de aansprakelijkheid draagt krachtens artikel 61 van de NIS2-wet, gezien zijn (default) rol als vertegenwoordiger van de gemeente om **toe te zien op de handhaving** van de federale wetgeving, en dat de gemeenteraad de aansprakelijkheid en de verplichtingen draagt in de zin van artikel 31 van de NIS2-wet, gezien zijn taak om toezicht te houden

op en goedkeuring te verlenen aan het organisatorische controlesysteem (waar de meeste cyberbeveiligingsmaatregelen zouden worden geïmplementeerd).
Opgemerkt moet worden dat de regelingen in ieder geval van toepassing zijn zonder afbreuk te doen aan de regels inzake aansprakelijkheid in de publieke sector.

3.4 gewone aansprakelijkheidsregels

Zoals hiervoor al aangehaald is ook hier een onderscheid te maken naargelang het statuut van de "werknemer":

- Voor de statutaire verwijzen we naar de wet van 10/2/2003
- Voor de contractuele naar de Wet op de arbeidsovereenkomsten 3/7/78

Voor degene die als "hulppersoon kunnen beschouwd worden gelden de bijzondere regels voor de buitencontratuele aansprakelijkheid ten overstaan van derden zol voorzien in het Zesde Boek van het Nieuw Burgerlijk Wetboek.

a) Contractuelen

de Arbeidsovereenkomstenwet, met inbegrip van de aansprakelijkheidsbeperkende norm van art. 18, eerste en tweede lid, van deze wet, is van toepassing op personeelsleden in dienst van openbare rechtspersonen, wier toestand niet statutair is geregeld is.
De quasi immuniteit is echter deels verloren gegaan met deinvoering van het Zesde Boek van het nieuw BW waarbij de buitencontractuele aansprakelijkheid voor scade aan derden in hoofde van de "hulppersonen" het karanter heeftgekregen vaneen persoonlijke aansprakelijheid van dehulpperson.

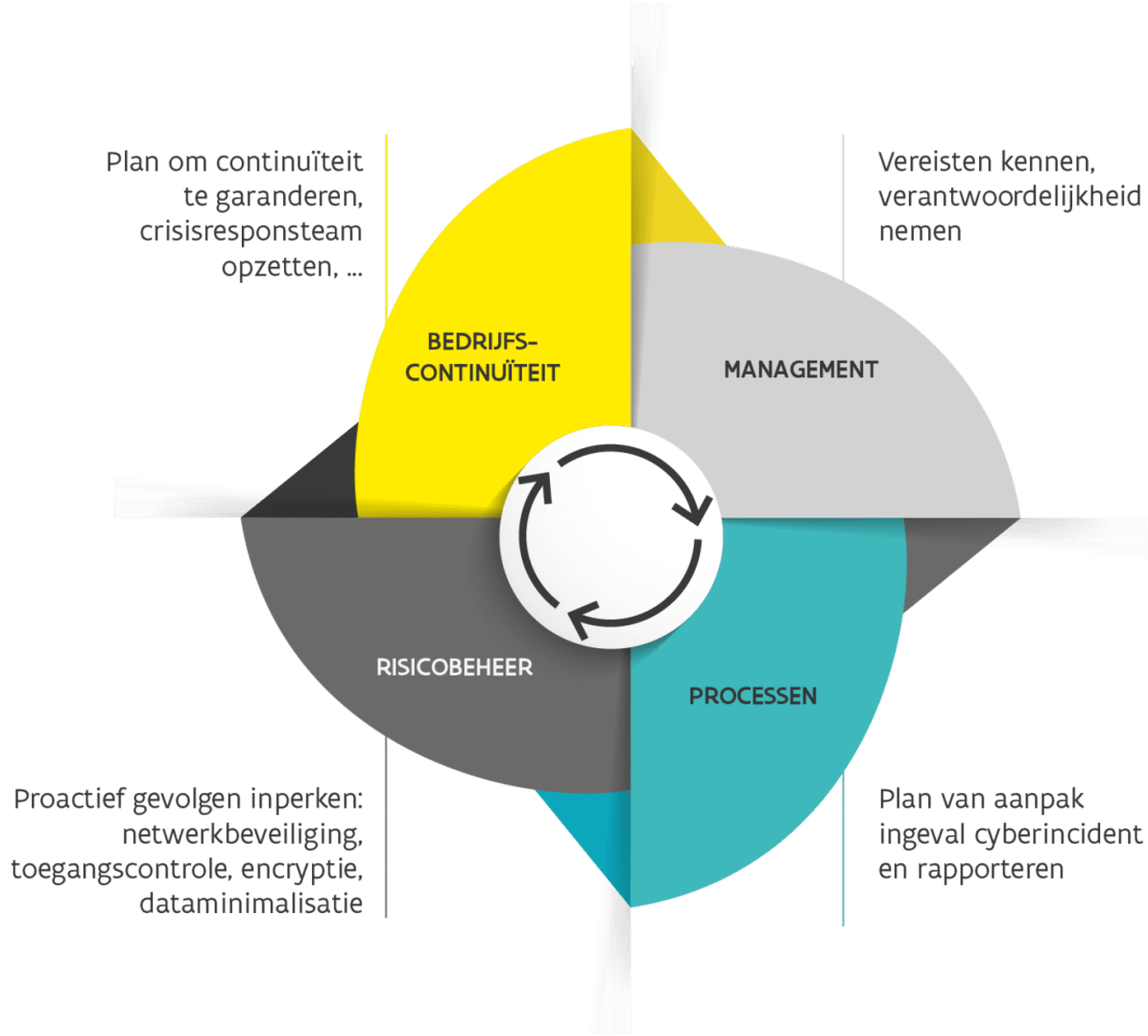
b) statutairen

In het algemeen zijn openbare rechtspersonen hier ook aansprakelijk voor de schade die hun personeelsleden aan derden berokkenen bij de uitoefening van hun dienst, op de wijze waarop aanstellers aansprakelijk zijn voor de schade aangericht door hun aangestelde, en dit ook wanneer de toestand van deze personeelsleden statutair is geregeld of zij gehandeld hebben in de uitoefening van de openbare macht (zie art. 3 Wet 10 februari 2003 betreffende de aansprakelijkheid van en voor personeelsleden in dienst van openbare rechtspersonen, B.S. 27 februari 2003, p. 9558).
Ingeval personeelsleden in dienst van openbare rechtspersonen, wier toestand statutair geregeld is, bij de uitoefening van hun dienst schade berokkenen aan de openbare rechtspersoon of aan derden, zijn ook zij enkel aansprakelijk voor hun bedrog en hun zware schuld. Voor lichte schuld zijn ook zij enkel aansprakelijk als die bij hen eerder gewoonlijk dan toevallig voorkomt (zie art. 2 Wet 10 februari 2003).

Deze aansprakelijkheidsbeperking staat er niet aan in de weg dat de benadeelde derde een aansprakelijkheidsvordering instelt tegen de openbare rechtspersoon als aansteller voor de schade veroorzaakt door de fout van een statutair personeelslid in zijn dienst, ook als het een toevallig voorkomende lichte fout is (Memorie van toelichting, *Pari. St.*, Kamer, 2001-2002, nr. 1736/001, p. 20.)

4. IMPACT OP DE LOKALE BESTUREN EN DE GEDECENTRALISEERDE WELKE ONDER DE NIS2 WET VALLEN

4.1 De impact van de NIS2-wet op de organisatie



4.2 Rol van de leidinggevenden

De NIS2-wet ziet digitale veiligheid als verantwoordelijkheid van de hele organisatie, niet alleen ICT. De wet legt een sterke verantwoordelijkheid bij de organisatie en organisatiebeheersing. Naast de technische aspecten van digitale veiligheid, beschrijft de wet **de rol en de verantwoordelijkheid van leidinggevenden** binnen de organisatie.

De eisen die de NIS2-wet oplegt, kunnen high-level worden samengevat in **4 domeinen:** management, processen, risicobeheer en bedrijfscontinuïteit.

- **Management:** binnen NIS2 moet het management de vereisten kennen en verantwoordelijkheid opnemen om risico's in kaart te brengen en aan te pakken. Zij moeten een cybersecurity training volgen en moeten er ook voor zorgen dat regelmatig bewustzijnscampagnes naar alle medewerkers worden gevoerd zodat er een echte cultuur van veiligheid in de organisatie ontstaat.
- Processen: informatieveiligheid is een cyclisch proces dat duidelijke regels en hulpmiddelen vraagt. NIS2 vereist dat processen rond o.a. informatieclassificatie, aanpak en rapporteren van incidenten, beveiliging van de toeleveringsketen, ontwikkelen van veilige informatiesystemen en digitale hygiëne gedefinieerd worden.
- **Risicobeheer:** wanneer een incident zich voordoet, is het belangrijk om ervoor te zorgen dat de impact beperkt blijft en de dienstverlening gewaarborgd blijft. Door informatie te classificeren en een goed overzicht te behouden van de risico's kan de organisatie zich weerbaar opstellen. Het management houdt te allen tijde een vinger aan de pols en zorgt ervoor dat voldoende middelen (budget en menskracht) beschikbaar zijn.
- **Bedrijfscontinuïteit:** elke organisatie binnen NIS2 dient over een plan te beschikken om de continuïteit te garanderen ingeval van grote cyberaanvallen. Dat kan bijvoorbeeld door de inrichting, testen en evalueren van een incident response en disaster recovery en crisisbeheerplannen.

4.3 Verplichte significant incidentenmelding

Een ander belangrijk aspect van de NIS2-wet is dat alle organisaties elk significant cyberincident moeten melden bij het nationale CSIRT (CCB).

Met significant incident wordt elk incident bedoeld 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 die:

- 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
- andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

Wanneer een lokaal bestuur (die geen NIS2 entiteit is) zo'n cyberincident opmerkt, maakt deze hiervan onmiddellijk melding bij het Vlaamse Cyber Response Team en/of CCB.

4.4 Toezicht

Het eerste niveau van toezicht gebeurt op basis van een zelfevaluatie volgens de criteria die werden opgenomen in het CyberFundamentals(opent in nieuw venster) raamwerk (CyFun®) van het Centrum Cybersecurity België (CCB) of een ISO 27001 certificering. Deze conformiteitsbeoordelingen zijn verplicht voor essentiële entiteiten en facultatief voor belangrijke entiteiten.

Daarnaast kunnen essentiële organisaties te allen tijde aan toezicht worden onderworpen (*ex-ante* en *ex-post*). Bij belangrijke entiteiten gebeurt toezicht enkel achteraf, bijvoorbeeld bij een incident of bij aanwijzingen van een overtreding.
Tijdslijn

- De NIS2-wet trad op 18 oktober 2024 in werking.
- alle overheidsinstanties die in het toepassingsgebied vallen moesten zich voor 18 maart 2025 registreren bij het CCB.
- Overheidsinstanties (die **belangrijk entiteiten** zijn) moesten zich vervolgens alligneren met het niveau belangrijk van het CyberFundamentals raamwerk.
- Overheidsinstanties (die **essentiële entiteiten** zijn) moesten dit eveneens doen

- **Alle andere lokale besturen** moeten uiterlijk op **1 januari 2030** ten minste het niveau basis van het CyberFundamentals raamwerk behalen.

4.5 Minimale maatregelen

Organisaties die onder NIS2 als belangrijk of essentieel gezien worden moeten voldoen aan heel wat verplichtingen rond cybersecurity, risicomanagement en rapporteringen. Zij zullen een efficiënt cyberbeveiligingsbeleid moeten voeren, met passende operationele, organisatorische en technische maatregelen om cyber risico's te detecteren en mitigeren.
Dit met betrokkenheid van bestuursorganen binnen de organisatie die verplichte training moeten krijgen in cybersecurity risicobeheer.

De **maatregelen die minimaal** genomen moeten worden zijn de volgende:

1. Risicoanalyse en cyberbeveiligingsbeleid
2. Procedures voor behandeling van incidenten
3. Bedrijfcontinuïteit en crisisbeheer
4. Beveiliging bij aankoop, ontwikkeling en onderhoud van systemen
5. Beveiliging van de supply chain
6. Beleid en procedures om cybersecurity maatregelen te evalueren
7. Elementaire cybersecurity praktijken en training
8. Beleid en procedures rond cryptografie en toepassing van encryptie
9. Veiligheidsaspecten voor personeel, toegangsbeheer en asset management
10. Multifactor authenticatie
11. Beveiligde communicatiesystemen voor crisissituaties

4.6 Rapportageplicht

NIS2 stroomlijnt ook de **rapportageverplichtingen** met betrekking tot cyberbeveiligingsdreigingen en -inbreuken.
Significante cyber incidenten moeten binnen 24 uur na de ontdekking ervan gemeld worden aan de bevoegde toezichthoudende autoriteiten, gevolgd door een tussentijds verslag binnen 72 uur en een eindverslag van het incident binnen een maand na de eerste melding.

Tot slot wordt er ook ingezet op **kennisdeling binnen de Europese Unie** over de grenzen heen. Organisaties zullen informatie over cyberbeveiligingsrisico's en -maatregelen met elkaar en met de lokale overheid delen via gemeenschappen en geautomatiseerde instrumenten.

4.7 Wat met de lokale besturen die niet onder het toepassingsveld vallen

Alle Vlaamse en lokale besturen, die nu niet gevat zijn volgens de NIS2-wetgeving, moeten **tegen 1 januari 2030** toch de nodige maatregelen nemen om aan het zekerheidsniveau basis te voldoen. Dit is een element van goed bestuur. Het is voor de burgers, verenigingen en bedrijven belangrijk dat ze erop kunnen vertrouwen dat wij als overheid zorgvuldig met persoonsgegevens en andere gevoelige informatie omspringen en deze informatie met de nodige omzichtigheid gebruiken en opslaan en ook de nodige maatregelen treffen om de continuïteit van de dienstverlening te verzekeren.

5. HANDHAVING

Het niet naleven van NIS2 kan leiden tot geldboetes die bij essentiële entiteiten kunnen oplopen tot maximaal 10 miljoen euro of 2% van de jaaromzet en bij belangrijke entiteiten tot 7 miljoen euro of 1,4 % van de jaaromzet.

NIS 2 heeft ook gevolgen voor de bestuurorganen van ondernemingen die onder NIS2 vallen. De wet stelt hen immers persoonlijk aansprakelijk indien de verplichtingen om maatregelen te nemen ter beheersing van cyberbeveiligingsrisico's niet worden nageleefd

6. SUGGESTIES

Ook als de NIS2 Wet op uw loaal bestuur niet van toepassing is wollen we deze themabrief afronden met volgende suggesties:

1. Voorzie nu al een planning voor de te nemen maatregelen tegen de voorziene toepassing in 2030
2. Denk hierbij aan een interne preventie audit
3. Overweeg een verzekering voor de gevolgen van cyber incidenten zowel op de eigen organisatie als op mogelijke derden schadelijders
4. Voorzie een technische bijstand voor herstel
5. Denk na en controleer usw huidige verzekeringsdekking zowel in hoofde van het bestuur maar ook voor uw bestuursorganen en uw leidinggevenden. Zorg hierbij voor de nodige bijstand ook in het kader vaneen eventuele persoonlijke aansprakelijkheid voor uw personeel en mandatarissen/bestuurders als hulppersonen in de zin van het Zesde Boek vann het nieuwe BW

7. BLADWIJZER

Inhoudsopgave