Uitvoeringsanalyse Digital Decade Regelgeving beveiliging netwerk- en informatiesystemen

Auteurs: Frank van Zutphen en Anneleen van Beek | juni 2024

#digitaldecadeNL

Samenvatting

De komende jaren komt er vanuit de Digital Decade veel nieuwe Europese wet- en regelgeving op gemeenten af. VNG zet de uitvoeringsanalyse in als één van de instrumenten om de gevolgen van (Europese) regelgeving voor gemeenten inzichtelijk te maken en deze in te brengen in de beleidsontwikkeling van het Rijk. Met als doelen om eventuele uitvoeringsproblemen vroegtijdig in beeld te brengen en om het handelingsperspectief te bieden voor implementatie door gemeenten. Dit rapport brengt deze gevolgen en het handelingsperspectief in kaart voor de volgende regelgeving:

- Beveiliging van netwerk- en informatiesystemen richtlijn 2 (NIS2);
- Cyberbeveiligingsverordening;
- Cyberweerbaarheidsverordening;
- Critical Entities Resilience richtlijn (CER).

Deze regelgeving maakt onderdeel uit van de EU-strategie inzake cyberbeveiliging; één van de belangrijke wetgevingsinitiatieven en/of -strategieën die de weg naar het digitale decennium in overeenstemming brengt met de prioriteit van de Commissie “Een Europa dat klaar is voor het digitale tijdperk.” Cyberbeveiliging, zoals gedefinieerd in artikel 2, lid 1, van de Cyberbeveiligingsverordening, *“betekent de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen die door cyberdreigingen worden getroffen, te beschermen.*” In de Nederlandse context spreken we van beveiligen van netwerk- en informatiesystemen.

Om te komen tot deze rapportage zijn experts uit 57 gemeenten in vier expertgroepen vanuit verschillende bedrijfsvoeringsthema’s (Juridisch, I&A, Dienstverlening en Finance & Control) in meerdere rondes met elkaar in gesprek gegaan over de impact en uitvoeringsconsequenties van de regelgeving. In een klankbordgroep hebben alle disciplines gezamenlijk de bevindingen gevalideerd, waarna het rapport is opgesteld dat tot slot ter review is voorgelegd aan de begeleidingscommissie en actief deelnemende gemeenten.

Impact op hoofdlijnen

Het Ministerie van BZK heeft gemeenten als essentiële entiteit aangewezen, waardoor de NIS2 van toepassing is/wordt op gemeenten. De wijzigingen door de NIS2 voor de werkwijze van gemeente komen door generieke, inhoudelijke en informatieverplichtingen.

De lidstaten hebben veel ruimte bij de vertaling en verdere invulling van de NIS2-richtlijn naar nationale regelgeving. De nog te maken keuzes kunnen kleine of grote gevolgen hebben voor de uitvoeringsconsequenties bij gemeenten. In het rapport is hiervan een uitwerking gemaakt in een minimale en een maximale variant van invulling met een duiding van de uitvoeringsconsequenties.

Van de bepalingen over de toezicht- en handhavingsinstrumenten is het nog niet goed mogelijk om de impact te duiden. In de opsomming in lid 2 van artikel 32 NIS2-richtlijn is een uitgebreid overzicht opgenomen van de bevoegdheden die de bevoegde autoriteiten ten minste moeten hebben. Een belangrijk aandachtspunt hierbij is dat het hebben van een bevoegdheid iets anders is dan het toepassen of gebruiken van diezelfde bevoegdheid. Over het toepassen of gebruiken van bevoegdheden door de toezichthouder is er op dit moment nog geen duidelijkheid. Een ander uitvoeringsrisico is de mogelijke stapeling van toezicht door verschillende toezichthouders

(bijvoorbeeld omdat gemeenten zowel moeten voldoen aan de NIS2 als de AVG en omdat er mogelijk meer toezichthouders bijkomen voor toezicht op kritieke sectoren die onder de NIS2 vallen en waarvoor gemeenten taken uitvoeren (zoals vervoer, drinkwater, afvalbeheer en gezondheidszorg)).

In de huidige situatie hebben gemeenten de Baseline Informatiebeveiliging Overheid (BIO) om de beveiliging van netwerk en informatiesystemen te beheren zoals de NIS2 beoogd. Dit is beschreven in hoofdstuk 2 van deze rapportage. De BIO is geen wettelijke verplichting, maar is een vorm van zelfregulering. De AVG is een wettelijke verplichting die gaat over het beschermen van persoonsgegevens en het treffen van maatregelen op de verwerkingen van persoonsgegevens. Zowel de NIS2-verplichtingen als de AVG richten zich op het adresseren van risico's en het nemen van passende maatregelen. Er zijn ook verschillen. De NIS2-richtlijn richt zich op het grotere geheel van digitale veiligheid met een focus op continuïteit van belangrijke en essentiële processen, terwijl de AVG focust op de bescherming van individuele rechten. Het Ministerie van BZK is voornemens om de Baseline Informatiebeveiliging Overheid (BIO) wettelijk te gaan verankeren en om in de reeds geplande modernisering van de BIO de eisen van de NIS2-richtlijn mee te nemen. Dit moet gebeuren in lagere regelgeving.

In de NIS2-verplichtingen is het continu beheren van informatiebeveiligingsrisico's een belangrijk aspect. Het gaat om een continu verbeterproces waarin de actualiteit en volledigheid van beveiligingsmaatregelen regelmatig moet worden vergeleken met actuele dreigingen. Dit is een grote inspanning als dit voor een gemeente nog geen gemeengoed is. Bovendien moet dit ingepast worden in de rest van het gemeentelijk risicomanagement (ook wel kwaliteitsmanagementsysteem of controlesysteem).

Toerusting gemeenten en gewenste vervolgacties

In de kern komt het er op neer dat gemeenten niet voldoende toegerust zijn voor een doeltreffende uitvoering van de nieuwe regelgeving vanwege onvoldoende mensen (vanwege krapte op de arbeidsmarkt) en onvoldoende financiële middelen (die voor het komende jaar al niet meer te organiseren zijn én vanwege het financiële ravijn in 2026). Daarom is de eerste randvoorwaarde dat er - in lijn met artikel 2 Financiële-verhoudingswet - gezorgd dient te worden voor een adequate financiële dekking vanuit de Rijksoverheid van de extra uitvoeringskosten bij gemeenten om te voldoen aan de nieuwe regelgeving voor het beveiligen van netwerk- en informatiesystemen.

Bij de verdere invulling van de nationale regelgeving is het van belang dat de regelgeving uitvoerbaar is voor verschillende typen gemeenten. Zo moet deze regelgeving uitvoerbaar zijn voor grote gemeenten waar mogelijk een team van medewerkers betrokken is bij het beveiligen van netwerk- en informatiesystemen én voor kleine gemeenten, die niet kunnen beschikken over zo'n team. Het is van belang om beide perspectieven nadrukkelijk mee te nemen bij de verdere uitwerking van de nationale regelgeving (en bij de ondersteuning vanuit bijvoorbeeld de IBD).
De tweede randvoorwaarde is daarom opgenomen dat er bij de verdere uitwerking van de nationale regelgeving (wet en lagere regelgeving) voldoende aandacht is voor de uitvoeringsconsequenties bij de gemeenten. Hiervoor moet - conform de Code Interbestuurlijke Verhoudingen - een zorgvuldig UDO-proces worden doorlopen door de betrokken departementen en de VNG namens de gemeenten. De UDO staat voor Uitvoerbaarheidstoets Decentrale Overheden en is het proces waarmee vakdepartementen samen met het Ministerie van BZK en koepels van decentrale overheden (IPO, VNG en UvW) samen het beleid uitwerken dat invloed heeft op decentrale overheden.

Naast de twee hierboven genoemde randvoorwaarden sluit het rapport af met zes gewenste vervolgacties:

1. Bepaal de (extra) uitvoeringskosten voor gemeenten van (verschillende varianten voor) de verdere invulling van het toezicht, weeg de uitvoeringskosten ook mee bij de besluitvorming over de invulling van het toezicht en zorg voor een adequate financiële dekking van de eventuele extra uitvoeringskosten voor gemeenten.
2. Het is van belang dat de uitwerking van termen als bestuursorganen, leden van bestuursorganen, aansprakelijkheid, verantwoordelijkheid en doelgroep van de opleidingen in relatie tot de NIS2-richtlijn ondubbelzinnig zijn en worden uitgewerkt in de Cyberbeveiligingswet.
3. Er is een meerjarig organisatieontwikkelingstraject nodig om de regelgeving bij gemeenten te implementeren. Zorg voor een realistische termijn waarbij gemeenten de tijd krijgen om aan de gestelde eisen van de wetgeving te kunnen voldoen (bijvoorbeeld door opschorting van de Nederlandse handhaving op dit punt gedurende die overgangsperiode).
4. Zorg voor passende implementatieondersteuning voor grote én kleine gemeenten in de vorm van onder meer handreikingen en ander ondersteuningsmateriaal voor de vraagstukken waar gemeenten in de uitvoering mee te maken gaan krijgen voor alle relevante gemeentelijke rollen betrokken bij de beveiliging van netwerk- en informatiesystemen (CISO, lijnmanagers én management).
5. Werk uit wat de NIS2-richtlijn betekent voor de verschillende type samenwerkingsverbanden waarbinnen gemeenten opereren.
6. Onderzoek de opleidingsbehoeften van de verschillende groepen bestuurders bij gemeenten alvorens een concrete verplichting voor het volgen van opleidingen vast te leggen in de Nederlandse regelgeving.

Wat kan een gemeente nu doen? Wat volgend jaar?

Het is voor gemeenten belangrijk om te weten wat zij nu alvast kunnen doen als no-regret maatregelen in verband met de nieuwe NIS2-regelgeving die op korte termijn omgezet gaat worden naar nationale regelgeving (Cyberbeveiligingswet en lagere regelgeving). Dit moet echter nog wel gebeuren, daarom is het op dit moment nog niet goed mogelijk om in detail aan te geven wat gemeenten dan moeten doen om in de toekomst te kunnen voldoen aan de nieuwe regelgeving.

Om beter voorbereid te zijn op de NIS2-richtlijn kan de gemeente alvast inzetten op het (nog) beter voldoen aan de BIO. Dan zet de gemeente in ieder geval een stap in de goede richting. Dit sluit ook aan bij de oproep van het Ministerie van BZK aan de koepels om prioriteit te maken van het toepassen van de huidige BIO.

Verder is het aan te raden om nog enigszins terughoudend te zijn met verdere stappen ten aanzien van NIS2, omdat nog niet bekend is hoe de verdere vertaling en invulling van de NIS2-richtlijn naar nationale regelgeving eruit komt te zien én omdat verschillende informatieproducten van de IBD nog aangepast moeten gaan worden nadat er duidelijkheid is over de nieuwe invulling van de nationale regelgeving.

Inhoud

1. Inleiding

1.1. Achtergrond

De komende jaren komt er vanuit de Digital Decade veel nieuwe Europese wet- en regelgeving op gemeenten af. Deze uitvoeringsanalyse is één van de instrumenten die VNG inzet om de gevolgen voor gemeenten in kaart te brengen van de netwerk- en informatiebeveiligingswetgeving en deze in te brengen in de beleidsontwikkeling van het Rijk. Met als doel om eventuele uitvoeringsproblemen vroegtijdig in beeld te brengen. Immers, deze problemen zijn achteraf veel moeilijker te repareren dan wanneer ze in de beleidsvoorbereiding aan het licht komen. Een tweede doel is om gezamenlijk in beeld te brengen wat gemeenten moeten doen om aan de netwerk- en informatiebeveiligingswetgeving te voldoen om zo de hoeveelheid werk te verdelen, om van elkaar te kunnen leren en om als gemeente goed voorbereid te zijn op een succesvolle implementatie.

De EU-strategie inzake cyberbeveiliging[1] is één van de belangrijke wetgevingsinitiatieven en/of -strategieën die de weg naar het digitale decennium in overeenstemming brengt met de prioriteit van de Commissie “Een Europa dat klaar is voor het digitale tijdperk.”[2]

Cyberbeveiliging, zoals gedefinieerd in artikel 2, lid 1, van de Cyberbeveiligingsverordening, *“betekent de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen die door cyberdreigingen worden getroffen, te beschermen.”*

In de Nederlandse context spreken we van beveiligen van netwerk- en informatiesystemen.

1.2. Vraagstelling

De onderzoeksvragen voor deze analyse zijn:

- Wat wijzigt er in de werkwijze van de gemeente door de EU-regelgeving?[3]
- Wat betekenen deze veranderingen voor de gemeentelijke organisatie wanneer deze in samenhang worden beschouwd?
- Is de gemeente voldoende toegerust voor een doeltreffende uitvoering?
- Welke kosten en besparingen voor de gemeentelijke uitvoering zijn aan deze wijziging verbonden?
- Wat zijn de verwachte effecten van de stapeling van de EU-regelgeving[4] voor gemeenten?
- Hoe kan deze EU-regelgeving in samenhang worden geïmplementeerd (uitgevoerd) en wat zijn de randvoorwaarden en risico’s?

---

1 https://digital-strategy.ec.europa.eu/nl/policies/cybersecurity-strategy.

2 https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

3 De Europese Commissie heeft, als onderdeel van de Digital Decade, een aantal regelgevende voorstellen die uitmonden in een verordening of richtlijn en die we hierna gemakshalve benoemen als regelgeving. Een ‘verordening’ is een bindende rechtshandeling die in de hele EU van toepassing is. Een ‘richtlijn’ is een rechtshandeling die een bepaald doel vastlegt dat alle EU-landen moeten bereiken. Zij mogen echter zelf de wetgeving vaststellen om dat doel te bereiken.

4 Aangezien dit de eerste van de zes analyses/clusters is, is de stapeling van de EU-regelgeving hier nog niet te bepalen. Voor deze analyse is de onderzoeksvraag daardoor ‘Wat zijn de verwachte effecten van de EU-regelgeving voor gemeenten?’

1.3. Aanpak & methodologie

Het onderzoek is uitgevoerd in de periode van januari tot en met mei 2024. In deze paragraaf is de onderzoeksaanpak beschreven en is een korte toelichting gegeven op de gehanteerde methodologie om de onderzoeksvragen te kunnen beantwoorden.

Onderzoeksaanpak

Het pakket aan wet -en regelgeving dat vanuit de Digital Decade op gemeenten afkomt, raakt alle gemeenten. Door een gezamenlijke aanpak te kiezen wordt voorkomen dat 342 gemeenten dit allemaal zelfstandig moeten uitzoeken. Door inzicht en overzicht te verschaffen wordt duidelijk welke werkzaamheden gedaan moeten worden om aan de EU-wetgeving te voldoen, maar ook hoe deze wetgeving en de resultaten van de gezamenlijke aanpak kunnen bijdragen aan verschillende maatschappelijke opgaven.

Op dit moment zijn er 27 regelgeving, richtlijnen en verordeningen bekend die onder de Digital Decade geschaard worden. Om deze te vertalen naar effecten voor de gemeenten is gekozen voor een clustering. Met deze clustering wordt het mogelijk om expertise gericht uit te vragen. Daarnaast wordt de samenhang tussen deze set van regelgeving, richtlijnen en verordeningen inzichtelijk.

De wetgevingsclusters, die behandeld gaan worden, zijn:
1. Cybersecurity;
2. Data -en informatie-uitwisseling;
3. Kunstmatige intelligentie, privacy en dataprotectie;
4. Elektronische identificatie;
5. Urban air mobility;
6. Consumentenbescherming en regulering van platforms.

Een reguliere impactanalyse beschouwt de impact op de volle breedte van de gemeentelijke bedrijfsvoering (primaire processen en SCOPAFIJTH-elementen[5]). Uit de eerdere verkenning van de eerste 13 regelgeving onder de Digital Decade[6] bleek de noodzaak om verschillende regelgeving in samenhang te onderzoeken. Daarom is gekozen voor een andere aanpak, in de vorm van 5 expertgroepen:
- **Juridische zaken:** juridische analyse en uitwerking van wetgeving op hoofdlijnen voor andere expertgroepen.
- **Informatie & Automatisering**: security, informatievoorziening en technologie, archief.
- **Financiën en control**: financiën, administratieve organisatie, inkoop, verantwoording en monitoring.
- **P&O**: personeel en organisatie, huisvesting.[7]
- **Publieksdienstverlening**: dienstverlening, communicatie.

---

[5] SCOPAFIJTH is een acroniem voor ondersteunende processen in een organisatie. Hieronder wordt verstaan: Security (en privacy), Communicatie, Organisatie, Personeel, Administratieve organisatie, Financiën, Informatievoorziening, Juridisch, Technologie en Huisvesting. In dit rapport zijn deze elementen alleen beschreven als deze relevant zijn.

[6] Zie: https://vng.nl/nieuws/13-nieuwe-wetten-publicatie-impactanalyse-digital-decade.

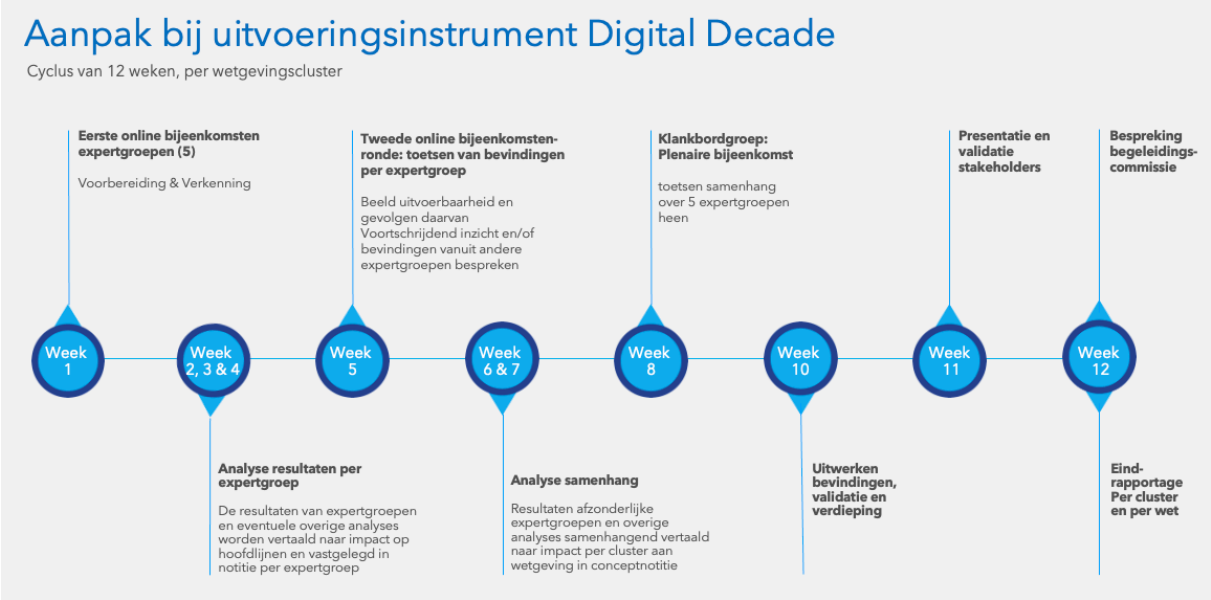
[7] In het plan van aanpak was ook een P&O expertgroep opgenomen; vanwege beperkte animo vanuit gemeenten zijn er echter geen bijeenkomsten met de P&O expertgroep gehouden.

Met deze expertgroepen is de cyberbeveiligingsregelgeving besproken, in twee gespreksrondes en één klankbordgroep. Voor de klankbordgroep zijn alle deelnemers aan de verschillende expertgroepen uitgenodigd om gezamenlijk te reflecteren op de bevindingen uit de afzonderlijke expertgroepen. Na de klankbordgroep is de conceptversie van de uitvoeringsanalyse opgesteld en uitgezet onder de deelnemers voor een schriftelijke review.

In de tweede helft van mei is de internetconsultatie van de Cyberbeveiligingswet gestart.[8] De teksten van dit wetsvoorstel waren ten tijde van de expertbijeenkomsten voor deze analyse niet bekend; dit rapport gaat daarom niet over de specifieke uitvoeringsconsequenties van de Cyberbeveiligingswet.[9] Er is in de rapportagefase nog wel een vergelijking gemaakt tussen de uitkomsten uit deze analyse en enkele van de bepalingen uit het wetsvoorstel (en waar relevant is dit ook opgenomen in het rapport).

Ter begeleiding van het onderzoek is een begeleidingscommissie ingericht. Deze bestaat uit VNG Beleid, VNG Realisatie, het Ministerie van BZK en enkele gemeentelijke vertegenwoordigers. De rol van de begeleidingscommissie is de procesmatige begeleiding van het onderzoek, het inbrengen van wensen/aandachtspunten/vragen voor de analyse, het bespreken van het plan van aanpak en het conceptrapport en het vaststellen van het eindrapport.

Bovenstaande aanpak resulteert in een doorlooptijd van 12 weken en ziet er als volgt uit:



1.4. Leeswijzer

Na dit inleidende hoofdstuk is in hoofdstuk 2 een algemene introductie gegeven van de huidige situatie op het gebied van het beveiligen van netwerk- en informatiesystemen en een introductie van de EU-regelgeving voor het beveiligen van netwerk- en informatiesystemen. In hoofdstuk 3 is een vergelijking gemaakt van de bestaande en de nieuwe verplichtingen waarbij nadrukkelijk is gekeken naar het uitvoeringsperspectief bij de nieuwe verplichtingen. In hoofdstuk 4 is ingegaan op het

8 https://www.internetconsultatie.nl/cyberbeveiligingswet/b1.

9 De uitvoeringsconsequenties van de Cyberbeveiligingswet voor gemeenten dienen nog nader te worden bepaald.

handelingsperspectief voor gemeenten (wat kunnen/moeten gemeenten doen). In hoofdstuk 5 zijn de conclusies uitgeschreven en de onderzoeksvragen beantwoord en zijn de aanbevelingen in samenhang gepresenteerd. Achtergrondinformatie is in de bijlagen opgenomen.

2. Digital Decade: Beveiliging van netwerk- en informatiesystemen

Dit hoofdstuk start met een beschrijving van de huidige situatie van het beveiligen van netwerk en informatiesystemen bij gemeenten. Vervolgens wordt aan de hand van de zeven w's (wie, wat, waar, wanneer, waarom, op welke wijze en met welke middelen) een introductie gegeven van de EU-regelgeving in scope van deze analyse die gaat over het beveiligen van netwerk en informatiesystemen. Het gaat om de volgende regelgeving:

- Beveiliging van netwerk- en informatiesystemen richtlijn 2 (NIS2);[10]
- Cyberbeveiligingsverordening;[11]
- Cyberweerbaarheidsverordening;[12]
- Critical Entities Resilience richtlijn (CER).[13]

Tevens onderzocht en buiten scope geplaatst zijn:

- Radio Equipment Directive;[14]
- Digital Operational Resilience Act (DORA).[15]

2.1. Beschrijving huidige situatie

Deze paragraaf beschrijft hoe in de huidige situatie gemeenten met de inzet van de Baseline Informatiebeveiliging Overheid hun netwerk- en informatiesystemen beveiligen. In het kader van de Algemene verordening gegevensbescherming (AVG) hebben gemeenten de verplichting om passende maatregelen te treffen om verwerkingen van persoonsgegevens te beveiligen.[16]

Baseline Informatiebeveiliging Overheid

In de huidige situatie wordt de Baseline Informatiebeveiliging Overheid (BIO) ingezet als normenkader voor informatiebeveiliging binnen de gehele overheid. De Baseline Informatiebeveiliging Overheid (BIO) is geheel gestructureerd volgens NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017. Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit'- lijst met verplichte standaarden voor de publieke sector, volgens het comply or explain principe. Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen.

De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid. Met klem vermeldt zij dat de BIO deze normen niet vervangt.[17] Sinds 1 januari 2020 is de BIO de officiële richtlijn op het gebied van informatiebeveiliging die alle gemeenten volgen.[18]

---

10 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2555&from=EN.
11 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32019R0881.
12 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454.
13 https://eur-lex.europa.eu/eli/dir/2022/2557/oj.
14 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053.
15 https://eur-lex.europa.eu/eli/reg/2022/2554/oj.
16 Zie artikel 32 AVG.
17 https://www.bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf.
18 https://vng.nl/files/vng/brieven/2019/20190107_ledenbrief_standaardverklaring-baseline-informatiebeveiliging-overheid.pdf.

Bij de vaststelling van de BIO is afgesproken dat deze wordt geëvalueerd. Dat is inmiddels gebeurd.[19] De evaluatie gaat leiden tot een BIO2.0.

De BIO (deel 1) bestaat uit een beschrijving van hoe de risicobeoordelingen systematisch kunnen plaatsvinden en een gedeelte dat gaat over de uitvoering van op de risico's afgestemde maatregelen voor het beheer van netwerk- en informatiebeveiligingsrisico's (BIO, deel 2):

- Risicomanagement is een systematisch proces om de risico's voor informatiebeveiliging te identificeren, beoordelen en prioriteren.
- Beveiligingsmaatregelen zijn acties of procedures die worden geïmplementeerd om geïdentificeerde risico's te mitigeren. Deze kunnen generiek zijn voor de hele organisatie of specifiek voor een bepaald informatiesysteem.

Risicobeheer in de BIO

De BIO geeft aan dat gemeenten moeten beschikken over een Information Security Management System (ISMS) waarin het risicobeheerproces centraal staat, zodat risico's adequaat worden beheerd. In de handreiking van de Informatiebeveiligingsdienst (IBD)[20] over ISMS voor zowel BIO als AVG is deze procesgerichte benadering voor informatiebeveiliging beschreven. Voor het opzetten, implementeren en onderhouden van een ISMS kan NEN-ISO 27001 worden gevolgd. Daarom is deze internationale norm, als ook de NEN-ISO 27002, voor gemeenten beschikbaar gesteld door de IBD en via een registratie bij NEN-connect[21] gratis te downloaden bij de NEN.

Het doel van het ISMS is het continu beoordelen of beveiligingsmaatregelen passend en effectief zijn, en of deze bijgesteld moeten worden. Het moet gemeenten helpen om risico's te beheersen, passende beveiligingsmaatregelen te treffen, lering te trekken uit incidenten en daarmee de betrouwbaarheid en de kwaliteit van de informatievoorziening en bedrijfscontinuïteit te waarborgen.

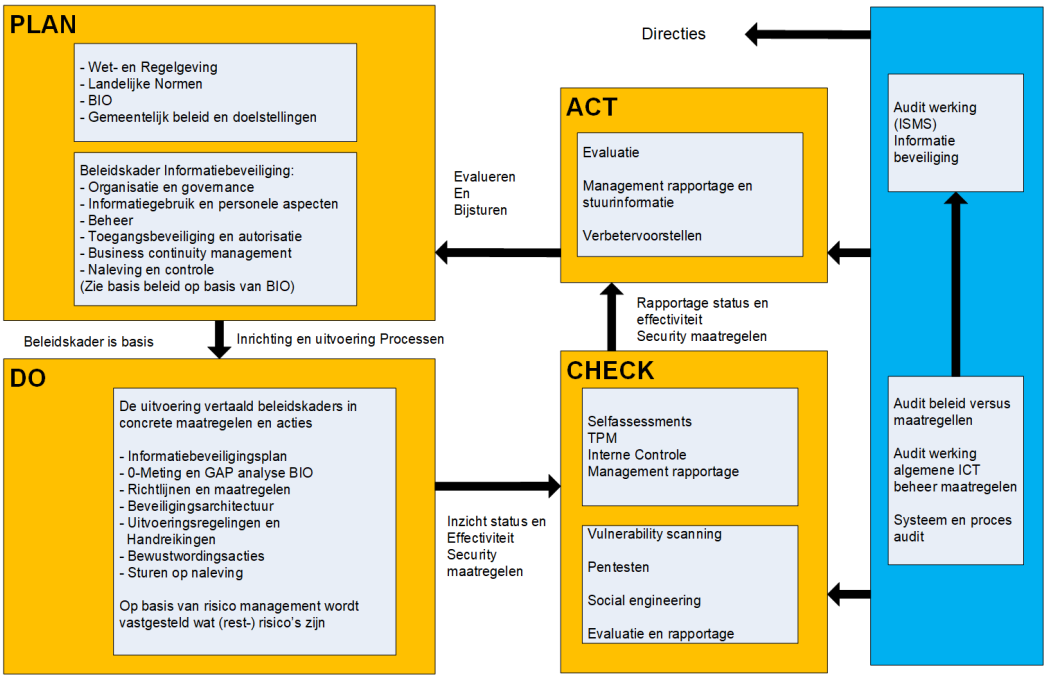
Voor het effectueren van informatiebeveiliging en privacy wordt binnen het ISMS gewerkt met een verbetercyclus, zoals de Plan, Do, Check, Act (PDCA)-cyclus. In de handreiking van de IBD wordt beschreven dat het proces van informatiebeveiliging en privacy gekoppeld dient te zijn aan de Planning en Control (P&C)-cyclus van de gemeente. Over informatiebeveiliging en privacy wordt verantwoording afgelegd door de organisatieonderdelen in de vorm van reguliere voortgangsrapportages. Een dergelijke cyclus is veelal vastgelegd in de gemeentelijke begrotings- en verantwoordingssystematiek. Aansluiting hierbij voorkomt dat informatiebeveiliging en privacy als een eigenstandig onderwerp wordt behandeld en daardoor laag geprioriteerd wordt.

Na het uitvoeren van risicoanalyses en vaststellen van wat nodig is om de gevonden risico's te beheersen, worden maatregelen getroffen. Vervolgens wordt gecontroleerd of die maatregelen het gewenste effect hebben (controle). Risico's kunnen in de tijd gezien veranderen (omdat de omgeving en bedreigingen ook veranderen). Daarom is het belangrijk om periodiek controles uit te voeren. Via een vastgesteld auditplan worden jaarlijks keuzes gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd. Deze controles kunnen dus aanleiding geven tot bijsturing in de maatregelen. Daarnaast kan het totaalpakket van eisen, maatregelen en controle aan een herijking toe zijn (evaluatie). Het goed doorlopen van de stappen kan op elk moment zorgen voor een passend beveiligingsniveau. Figuur 2.1 geeft de werking van het ISMS binnen gemeenten aan.

---

19 https://bio-overheid.nl/media/0qxksxwi/20221117-rapport-evaluatie-bio-berenschot.pdf.
20 https://www.informatiebeveiligingsdienst.nl.
21 Zie: https://connect.nen.nl/Portal.

Figuur 2.1 Werking van het ISMS binnen gemeenten (overgenomen van de IBD)



Information Security Management System

Beveiligingsmaatregelen BIO

De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om het risico te beperken. Om deze eisen af te dekken worden passende maatregelen getroffen of wordt het (rest-) risico geaccepteerd. Dit kan een ingewikkeld proces zijn. De BIO heeft dit vereenvoudigd: op basis van de generieke schades en dreigingen voor de overheid zijn standaard basisbeveiligingsniveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. Per bedrijfsproces bepaalt het lijnmanagement het BBN; de BIO biedt daarvoor een zogenaamde BBN-toets. In de BIO staat per BBN beschreven aan welke controls uit de ISO 27002 moet worden voldaan. Bij alle controls dient, op basis van een individuele risicoafweging, bepaald te worden hoe aan de beveiligingsdoelstelling van de control voldaan kan worden. Daarbij zijn de controls, waar van toepassing, gedeeltelijk uitgewerkt in verplichte, concrete overheidsmaatregelen. De implementatierichtlijnen uit de ISO 27002 kunnen daarbij als inspiratiebron worden gebruikt. De verzameling te nemen maatregelen per control omvat in ieder geval de bij die control behorende overheidsmaatregelen. De controls zijn toebedeeld aan rollen, waarmee de verdeling over verantwoordelijken makkelijker is. Verder staat in de BIO vermeld welke handreikingen gebruikt kunnen worden voor de implementatie van de controls en maatregelen. De IBD levert deze handreikingen voor gemeenten in de vorm van BIO-OP producten, zoals het 'Wachtwoordbeleid' en het 'Voorbeeld informatiebeveiligingsbeleid gemeenten'.[22]

Informatiebeveiliging en procesautomatisering/kritieke entiteiten

Gemeenten zijn de afgelopen jaren voornamelijk aan de slag gegaan met het beschermen van informatie door middel van de implementatie van de BIO. Deze implementatie is gericht op bescherming van informatie in de ICT van de gemeente, waar meer nadruk ligt op bescherming van

[22] Zie voor alle producten: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/.

vertrouwelijkheid. Gemeenten gebruiken ook automatisering voor besturing van industriële toepassingen, denk hierbij aan besturing van bruggen en sluizen, verkeerslichten, maar ook gebouwbeheerssystemen. Deze industriële automatisering wordt ook wel OT (operationele technologie) of PA (procesautomatisering) genoemd. De IBD heeft een handreiking gemaakt over hoe gemeenten, OT/PA kunnen opnemen in hun informatiebeveiligingsbeleid.[23]

Evaluatie BIO

In 2022 is in opdracht van het Directoraat-generaal Digitalisering en Overheidsorganisatie van het Ministerie van BZK een evaluatie van de BIO uitgevoerd.[24] In deze evaluatie worden op hoofdlijnen de volgende punten geconcludeerd.

Bijdragen aan beleidsdoelen:

- Draagt bij aan het bereiken en versterken van het digitale fundament, maar wekt soms onterecht de verwachting bij bestuurders dat voldoen aan de BIO betekent dat de feitelijke informatieveiligheid van de organisatie op orde is.
- Maakt deels inzichtelijk voor bestuurders en het hoger management welke normen gelden.
- Een goede basis en gezamenlijke taal voor het beleidsdoel samenwerking op het gebied van informatiebeveiliging in ketens (tussen overheidspartijen).

Waarbij ook een aantal uitdagingen worden gezien. De belangrijkste zijn dat organisatorische risicobeheer minder goed uit de verf komt. Ook het systematische beheren (PDCA-cyclus) van informatiebeveiligingsrisico's en meten van effectiviteit van maatregelen (ISMS) kan meer centraal gezet worden. Dit kan door de informatiebeveiligingsfunctie in overeenstemming te laten zijn met organisatiebreed risicomanagement en inrichtingsprincipes. In de huidige situatie wordt de BIO gezien als een 'afvinklijstje'. Hoewel de BIO gebaseerd is op en gestructureerd is volgens de NENISO/IEC 27001:2017, bijlage A en NENISO/IEC 27002:2017, aangevuld met specifieke overheidsmaatregelen, is de conclusie dat de BIO niet als zodanig wordt ervaren, maar als eigen, op zichzelf staand normenkader. Er zou meer nadruk moeten komen op dat de ISO-standaard als basis wordt gehanteerd en dat de aanvullingen vanuit de BIO 'slechts' de norm en enkele specifieke overheidsmaatregelen zijn. Er is behoefte om meer sturing te kunnen geven aan informatiebeveiliging. Dit kan door het 'sturen op volwassenheid'. Dit voorkomt dat informatiebeveiliging een eenmalige inspanning of het aflopen van een afvinklijst is. Een hogere volwassenheid helpt om informatiebeveiliging daadwerkelijk onderdeel te laten zijn van de PDCA-cyclus en draagt daarmee bij aan feitelijke informatieveiligheid.

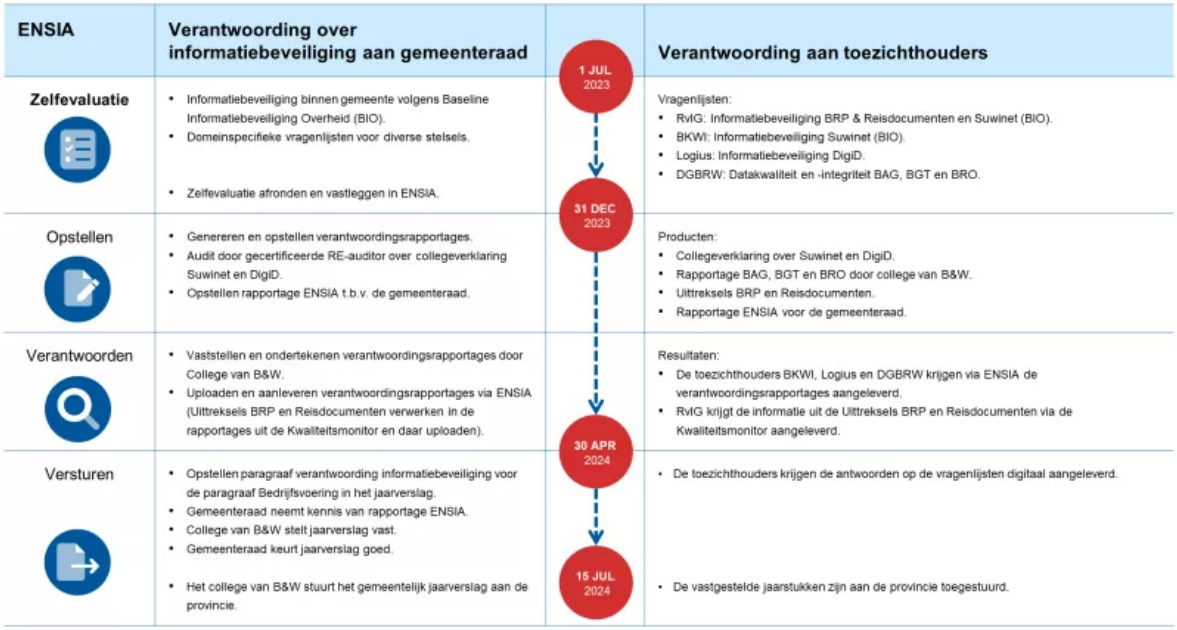
Op specifieke onderwerpen wordt aangegeven dat ondersteuning nodig is op hoe organisaties toezicht moeten houden op leveranciers. In de evaluatie is ook gekeken naar in hoeverre bedrijf continuïteitsmanagement (BCM) voldoende is uitgewerkt in de BIO en of procesautomatisering onderdeel moet zijn van de BIO. In het kader van een doelgericht toepassingsgebied en hanteerbaar beheer en onderhoud is in de evaluatie aangegeven dat het verstandiger om de procesautomatisering vooral in de speciaal daarvoor opgestelde normenkaders te laten. Het BCM in de BIO moet gaan over het informatiebeveiligingsaspect.

[23] Zie: https://www.informatiebeveiligingsdienst.nl/product/handreiking-procesautomatisering-pa-beleid/.
[24] https://bio-overheid.nl/media/0qxksxwi/20221117-rapport-evaluatie-bio-berenschot.pdf.

Eenduidige Normatiek Single Information Audit (ENSIA)

Over het functioneren van de informatiebeveiliging en privacy, wordt conform de P&C-cyclus binnen de gemeente en richting het college van B en W verantwoording afgelegd door het management. Het college van B en W legt vervolgens horizontaal verantwoording af aan de gemeenteraad en verticaal aan de toezichthouders. Sinds 2015 gebruiken de gemeenten daarvoor ENSIA. In de volgende figuur is aangeven hoe dit verloopt.

Figuur 2.2 De verantwoording via ENSIA, overgenomen van Ensia site VNG[25]



Rol Informatiebeveiligingsdienst (IBD)

De IBD is de sectorale Computer Security Incident Response Team (CSIRT) voor alle Nederlandse gemeenten en onderdeel van VNG. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD draagt namens gemeenten bij aan de BIO en geeft regelmatig kennisproducten[26] uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

Doelen van de IBD:

- Integrale coördinatie (24*7), preventie en detectie op gemeentespecifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging inclusief woordvoering & communicatieadvies.
- Adviseren en ondersteunen van gemeenten op hun informatiebeveiligingsvraagstukken (gebaseerd op gemeenschappelijk normenkader BIO) – onder andere in collectieve projecten van gemeenten.
- Kennisdeling tussen gemeenten, met leveranciers en andere overheden.
- Ondersteunen van gemeenten bij het implementeren van privacy en informatiebeveiliging.

25 https://vng.nl/projecten/ensia.
26 https://www.informatiebeveiligingsdienst.nl/producten/.

De doelgroep van de IBD-CSIRT bestaat uit:

- Nederlandse gemeenten
- ICT-samenwerkingsverbanden van gemeenten
- Intergemeentelijke sociale diensten
- Gemeentelijke belastingsamenwerkingen
- VNG

Andere organisaties, zoals overige gemeentelijke samenwerkingsverbanden / gemeenschappelijke regelingen, medeoverheden, ondernemingen waarin de gemeente participeert en semioverheden, kunnen gebruik maken van de generieke producten van de IBD maar hebben geen directe aansluiting op de CSIRT.

2.2. Probleemanalyse (concrete huidige problemen)

De NIS2-richtlijn beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken. Uit een evaluatie van de NIS1-richtlijn[27] blijkt dat lidstaten de richtlijn op uiteenlopende wijze uitvoeren. Zo zijn de hiervoor genoemde verplichtingen op nationaal niveau op aanzienlijk verschillende wijze uitgevoerd, waardoor er verschillen zijn op het gebied van het type maatregel en het detailniveau. Dit geldt ook voor de bepalingen uit de richtlijnen over toezicht en handhaving. Verder zijn er tussen de lidstaten verschillen op het gebied van de aanwijzingen van aanbieders die onder het NIS1-regime vallen. Deze verschillen tussen lidstaten leiden tot een versnippering van de interne markt en kunnen een nadelig effect hebben op het functioneren van de interne markt, met gevolgen voor onder meer de grensoverstijgende dienstverlening.

Deze probleemanalyse wordt onderschreven in het wetvoorstel Cyberbeveiliging ter implementatie van de NIS2-richtlijn.[28] Opmerkelijk genoeg wordt in de probleemanalyse van de Cyberbeveiligingswet alleen ingegaan op de probleemanalyse op Europees niveau en niet op de probleemanalyse op nationaal niveau (voor Nederland).[29]

2.3. Introductie EU-regelgeving voor beveiliging van netwerk- en informatiesystemen

Aan de hand van de zeven w's (wie, wat, waar, wanneer, waarom, op welke wijze en met welke middelen), wordt hier een introductie[30] gegeven van de EU-regelgeving in scope van deze analyse die gaat over het beveiligen van netwerk en informatiesystemen.

---

27 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2555&from=EN.

28 https://www.internetconsultatie.nl/cyberbeveiligingswet/b1.

29 Zie https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12602.

30 Hier volgt een korte beschrijving van elk van de wetgevingsinitiatieven die in overeenstemming zijn met het huidige EU-kader voor cyberbeveiliging en relevant voor gemeenten. In de bijlage B volgt een uitgebreidere beschrijving. Deze beschrijving volgt een structuur van wanneer (status van de wetgeving), wat (doelstellingen en belangrijkste inhoud van het initiatief) en wie (belanghebbenden waarop de handeling rechtstreeks betrekking heeft).

Het gaat over de volgende regelgeving:

- Beveiliging van netwerk- en informatiesystemen richtlijn 2 (NIS2);[31]
- Cyberbeveiligingsverordening;[32]
- Cyberweerbaarheidsverordening;[33]
- Critical Entities Resilience richtlijn (CER).[34]

Wie

Beveiliging van netwerk- en informatiesystemen richtlijn 2 (NIS2)[35]

De NIS2-richtlijn introduceert de begrippen essentiële entiteiten en belangrijke entiteiten. De lidstaten stellen uiterlijk op 17 april 2025 een lijst van deze entiteiten op. Het gaat om entiteiten die vallen binnen de volgende sectoren:

1. Essentiële entiteiten (categorie 1): energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, beheer van ICT-diensten (business-to-business), overheid en ruimtevaart.
2. Belangrijke entiteiten (categorie 2): post- en koeriersdiensten; afvalstoffenbeheer, vervaardiging, productie en distributie van chemische stoffen, productie, verwerking en distributie van levensmiddelen, vervaardiging, digitale aanbieders en onderzoek.

Deze wet is van toepassing op "een overheidsinstantie op regionaal niveau, zoals gedefinieerd door een lidstaat in overeenstemming met het nationale recht, die, na een op risico's gebaseerde beoordeling, diensten verleent waarvan de verstoring een aanzienlijke impact kan hebben op kritieke maatschappelijke of economische activiteiten". De lidstaten kunnen bepalen dat deze richtlijn van toepassing is op overheidsinstanties op lokaal niveau. Dit zal afhangen van de nationale keuzes die elke lidstaat maakt bij de omzetting van de richtlijn in zijn nationale wetgeving.

Het Ministerie van BZK heeft in het wetsvoorstel voor de Cyberbeveiligingswet gemeenten als essentiële entiteit aangewezen.[36]

Cyberbeveiligingsverordening[37]

De cyberbeveiligingsverordening voorziet in een EU-brede certificeringsregeling voor cyberbeveiliging. Eenmaal goedgekeurd, moeten of kunnen Nederlandse gemeenten aan die certificeringen voldoen en van hun aanbieders eisen dat zij zich daaraan houden. De verplichting is afhankelijk van of dit geëist gaat worden door de EU. De certificering zal aantonen dat wordt voldaan aan de verschillende cyberbeveiligingsvereisten die zijn opgenomen in de NIS 2-richtlijn, de Cyberweerbaarheidsverordening en eerdere eisen uit eIDAS.[38] Ook zal uit de komende AI verordening[39] aanvullende eisen voortkomen.

---

31 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2555&from=EN.
32 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32019R0881.
33 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454.
34 https://eur-lex.europa.eu/eli/dir/2022/2557/oj.
35 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2555&from=EN.
36 Dit is opgenomen in artikel 8 lid 1h van het wetsvoorstel voor de Cyberbeveiligingswet, zie https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12561.
37 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32019R0881.
38 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32014R0910.
39 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

Bovendien kent de wetgeving European Union Agency for Cybersecurity (ENISA), het EU-agentschap voor cyberbeveiliging. ENISA stelt nieuwe mandaten op met betrekking tot het opzetten en onderhouden van het Europees cyberbeveiligingskader, en geeft bijstand aan de lidstaten bij de ontwikkeling van hun nationale strategieën of het aanbieden van cyberbeveiligingsopleidingen. ENISA moet ervoor zorgen dat deze certificeringsregelingen een belangrijke rol spelen in de verschillende cyberbeveiligingswetgeving.

Cyberweerbaarheidsverordening[40]

Deze verordening verplicht fabrikanten, importeurs en distributeurs van producten met digitale elementen om gedurende hun hele levenscyclus een zorgplicht te bieden. Deze regels omvatten het plaatsen van de producten op de markt door middel van een proces van conformiteitsbeoordeling van de eisen voor het ontwerp, de ontwikkeling en de productie van dergelijke producten.

De Cyberweerbaarheidsverordening is relevant voor Nederlandse gemeenten, omdat gemeenten bij het inzetten van digitale producten er zeker van kunnen zijn dat deze producten aan de veiligheidseisen van de EU voldoen, ze kunnen er rechten aan ontlenen, bijvoorbeeld ten aanzien van zorgplicht van de leverancier. Deze relevantie geldt ook voor als gemeenten onderling aan elkaar ICT-diensten leveren zoals in een shared service center met ICT-diensten.

Critical Entities Resilience richtlijn (CER)[41]

Volgens deze richtlijn wordt onder "kritieke entiteit" verstaan een publieke of private entiteit die door een lidstaat is aangemerkt als behorend tot een van de in de bijlage bij de richtlijn genoemde categorieën. De sectoren zijn de volgende: energie, vervoer, bankwezen, financiële markt infrastructuur, gezondheid, drinkwater, afvalwater, digitale infrastructuur, openbaar bestuur, ruimtevaart, productie, verwerking en distributie van voedsel.

Van de (zoals hierbovengenoemde) sectoren die in de richtlijn zijn opgenomen, worden in de bijlage van de CER "overheidsinstanties van centrale overheden zoals gedefinieerd door de lidstaten in overeenstemming met het nationale recht" genoemd. Hoewel gemeenten niet tot de centrale overheid behoren vallen ze mogelijk onder een andere categorie. Bijvoorbeeld wanneer een overheidsinstantie op lokaal niveau afvalwater beheert.

Computer Security Incident Response Team (CSIRT)[42]

NIS2 verplicht lidstaten om in nationale wet- en regelgeving te voorzien in een meldplicht bij cybersecurity incidenten ‘met aanzienlijke gevolgen’. Naar verwachting zal de Informatiebeveiligingsdienst (IBD) voor gemeenten de CSIRT (ook bekend als CERT (computer emergency respons team) worden.

Toezichthouder[43]

De Rijksinspectie Digitale Infrastructuur (RDI) is op dit moment toezichthouder op de naleving van de Wet beveiliging netwerk- en Informatiesystemen (Wbni) voor de energiesector, de digitale infrastructuur en voor digitale dienstverleners. De NIS2-richtlijn richt zich op meer sectoren dan de

40 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454.
41 https://eur-lex.europa.eu/eli/dir/2022/2557/oj.
42 https://vng.nl/sites/default/files/2023-11/brief-nis2-bij-de-overheid.pdf.
43 https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/nis2-wbni2.

huidige NIS-richtlijn. Namens de Minister van EZK wordt de RDI toezichthouder op de volgende sectoren:

- Energie;
- Digitale infrastructuur;
- Ruimtevaart;
- Vervaardiging/Manufacturing;
- Digitale aanbieders;
- Overheidsdiensten;
- Post- en koeriersdiensten;
- Onderzoek;
- Beheer van ICT-diensten.

Namens de Minister van BZK wordt de RDI toezichthouder voor de sector:

- Overheidsdiensten.

Organisaties die actief zijn in andere sectoren waar de NIS2 zich op richt, vallen onder het toezicht van de betreffende sectorale toezichthouder.

Wat

NIS2-richtlijn

De NIS2-richtlijn voorziet in maatregelen die erop gericht zijn een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren.

Met het oog hierop voorziet deze richtlijn in:

a) Verplichtingen die de lidstaten voorschrijven dat zij nationale cyberbeveiligingsstrategieën vaststellen, en bevoegde autoriteiten, cybercrisisbeheerautoriteiten, centrale contactpunten op het gebied van cyberbeveiliging (centrale contactpunten) en Computer Security Incident Response Teams (CSIRT's) aanwijzen of instellen;
b) Risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging voor entiteiten van het type waarnaar in bijlage I of II van de NIS2-richtlijn wordt verwezen alsmede voor entiteiten die uit hoofde van Richtlijn (EU) 2022/2557 als kritieke entiteiten worden aangemerkt;
c) Regels en verplichtingen met betrekking tot het delen van cyberbeveiligingsinformatie;
d) Toezichts- en handhavingsverplichtingen voor de lidstaten.

NIS2 bevat vereisten, waaronder een bredere reeks verplichte maatregelen, voor het beheer van cyberbeveiligingsrisico's (artikel 21) en nieuwe vereisten voor het melden van incidenten (artikel 23). De vrijwillige melding vanuit de voorgaande NIS van incidenten is nog steeds van kracht.

Om aan te tonen dat aan de vereisten van artikel 21 is voldaan, kunnen de lidstaten van essentiële en belangrijke entiteiten verlangen dat zij gebruikmaken van ICT-producten, -diensten en -processen die door de essentiële of belangrijke entiteit zijn ontwikkeld of van derden zijn aangekocht en die zijn gecertificeerd in het kader van Europese cyberbeveiligingscertificeringsregelingen overeenkomstig de Cyberbeveiligingsverordening.

Cyberbeveiligingsverordening

Deze verordening voert een EU-breed cyberbeveiligingscertificeringskader in voor de vaststelling van Europese cyberbeveiligingscertificeringsregelingen om een adequaat niveau van cyberbeveiliging van ICT-producten, -diensten en -processen in de Unie te waarborgen.

Op 18 april 2023 heeft de Commissie een gerichte wijziging van deze verordening voorgesteld, die tot doel heeft de vaststelling van Europese regelingen voor cyberbeveiligingscertificering voor "beheerde beveiligingsdiensten" mogelijk te maken.

Er zijn enkele nationale regelingen voor cyberbeveiliging, maar er is geen gemeenschappelijk kader voor de lidstaten. De nieuwe Europese cyberbeveiligingscertificeringsregelingen zullen in de plaats komen van de nationale regelingen voor cyberbeveiligingscertificering, wanneer er sprake is van overlapping in hun toepassingsgebied. Elke lidstaat moet voor de toepassing van de wet een nationale cyberbeveiligingscertificeringsautoriteit aanwijzen. In Nederland (RDI) verantwoordelijk.

De cyberbeveiligingscertificering is vrijwillig, tenzij dit verplicht wordt gesteld op grond van het toepasselijke Unierecht. De certificering zal een manier zijn om aan te tonen dat wordt voldaan aan de vereisten die zijn vastgesteld in de NIS 2-richtlijn, de eIDAS-verordening, de Cyberweerbaarheidsverordening en de AI-verordening.[44]

Cyberweerbaarheidsverordening

De cyberweerbaarheidsverordening stelt horizontale cyberbeveiligingsvereisten vast voor alle producten met digitale elementen (bv. VPN's, identiteits- en toegangsbeheersystemen, antivirusprogramma's, wachtwoordbeheerders) die op de Europese markt worden geplaatst of beschikbaar worden gesteld.

Critical Entities Resilience

Overeenkomstig het in artikel 1 omschreven toepassingsgebied van deze richtlijn:

1. Bevat verplichtingen voor de lidstaten om specifieke maatregelen te nemen om ervoor te zorgen dat diensten die essentieel zijn voor de instandhouding van vitale maatschappelijke functies op onbelemmerde wijze op de Europese markt worden verleend, met name verplichtingen om kritieke entiteiten te identificeren en kritieke entiteiten te ondersteunen bij het nakomen van de verplichtingen die aan hen worden opgelegd;
2. Stelt verplichtingen vast voor kritieke entiteiten om hun veerkracht en hun vermogen om essentiële diensten te verlenen te vergroten;
3. Stelt regels vast voor het toezicht op kritieke entiteiten, voor de handhaving en voor de identificatie van kritieke entiteiten van bijzonder Europees belang, en voor adviesmissies om de maatregelen te beoordelen die deze entiteiten hebben genomen om aan de in de richtlijn gespecificeerde verplichtingen te voldoen;
4. Stelt gemeenschappelijke procedures vast voor samenwerking en verslaglegging over de toepassing van de richtlijn;
5. Bevat maatregelen om kritieke entiteiten een hoge mate van veerkracht te bieden om de verlening van essentiële diensten binnen de Unie te waarborgen en de werking van de interne markt te verbeteren.

[44] Voor eIDAS en de AI-verordening worden in de komende rondes uitvoeringsanalyses opgesteld.

Samenhang verschillende EU-regelgeving over beveiliging van netwerk en informatiesystemen

Deze uitvoeringsanalyse beschouwt de NIS2 als overkoepelende cybersecurityregelgeving voor gemeenten, waar de Cyberbeveiligingsverordening, Cyberweerbaarheidsverordening worden toegepast als het gaat om het gebruik van beveiligingscertificering. De CER-richtlijn richt zich op de bescherming van organisaties tegen *fysieke* dreigingen, zoals de gevolgen van (terroristische) misdrijven, sabotage en natuurrampen waar de NIS2-richtlijn richt zich op *digitale* (cyber) risico's voor netwerk- en informatiesystemen.

Voor zowel de fysieke (CER) en digitale (NIS2) weerbaarheid komt er een plicht (tot nemen van beveiligingsmaatregelen) en een meldplicht (van incidenten). Deze plichten gaan gelden voor organisaties die een dienst verlenen die belangrijk, essentieel of kritiek is voor het functioneren van de maatschappij of economie. Onder de NIS2 vallen diverse kritieke sectoren waarbinnen lokale overheden wettelijke taken uitvoeren, zoals vervoer (spoor, water, en weg), gezondheidszorg, drinkwater, en afvalbeheer. Bijvoorbeeld: de kritieke sector vervoer betreft de procesautomatisering (PA) van gemeenten, die beveiligd wordt volgens ISA62443-normen (uitgewerkt in de CSIR[45] en niet opgenomen in de BIO). Denk hierbij aan sluizen, verkeerslichten en bruggen. Op dezelfde manier heeft de gezondheidszorg NEN7510 (gebaseerd op ISO27001) als norm.

Buiten scope

Radio Equipment Directive[46]

Deze richtlijn is in Nederland geïmplementeerd in de Telecommunicatiewet (wijziging in wet van 3 februari 2016), het Besluit Radioapparaten 2016, Besluit elektromagnetische compatibiliteit 2016 en Regeling elektromagnetische compatibiliteit 2016. Het Besluit Radioapparaten 2016 is in 2024 weer gewijzigd vanwege een gedelegeerd besluit van de Europese Commissie.[47]

De gevolgen van deze richtlijn zijn voor de gemeenten in zoverre relevant dat zij geen zendinrichtingen in gebruik mogen nemen die niet de CE-markeringen hebben die voorgeschreven zijn, tenzij voor test- en demonstratiedoeleinden. Daarmee is deze richtlijn vooral van toepassing op toeleveranciers van gemeenten, en kan worden volstaan met het vereisen van het CE-keurmerk, met dien verstande dat deze richtlijn voor oudere apparatuur of bijzondere maatwerksituaties wel relevant kan zijn voor gemeenten:

a) als men zelf componenten geïntegreerd heeft in vaste zendinstallaties (dan geldt de CE-markeringsplicht niet, maar moet wel zelf gedocumenteerd worden dat dit geen verstoringen voor anderen doet ontstaan)
b) dat het goed is bestaande apparatuur na te lopen en na te gaan of hier nog actie op moet worden ondernomen.[48]

Deze richtlijn is in dit verdere onderzoek buiten scope geplaatst.

---

45 https://www.informatiebeveiligingsdienst.nl/nieuws/cybersecurity-implementatierichtlijn-objecten-csir-beveiliging-van-proces-automatisering-van-gemeenten/.

46 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053.

47 Deze passage over de RED is gebaseerd op het memo 'RED van toepassing op gemeenten' d.d. 5 april 2024 van Hooghiemstra & Partners.

48 Hierbij dient te worden opgemerkt dat het CE-keurmerk pas sinds 2017 bestaat; zendapparatuur die voor december 2016 in gebruik is genomen, was nog niet onderhevig aan de CE-markeringsplicht

Digital Operational Resilience Act (DORA)[49]

Deze verordening stelt regels om de financiële sector in de EU beter te beschermen en weerbaarder te maken tegen het toenemende risico van cyberaanvallen en datalekken e.d. De verordening is begin 2023 van kracht geworden en de lidstaten moeten hieraan per 17 januari 2025 voldoen.

DORA stelt eisen aan financiële instellingen wat betreft IT-risicomanagement, IT-incidenten, periodieke testen van digitale weerbaarheid en de beheersing van risico's bij uitbesteding aan IT-dienstverleners. Daarnaast bevat de verordening regelingen voor het tussen lidstaten uitwisselen van informatie over cyberdreigingen.

Artikel 2 van DORA bepaalt het toepassingsgebied van de verordening. Het gaat om een breed palet aan financiële dienstverleners. Deze worden in de verordening aangeduid als *financiële entiteiten*. Verderop in de verordening (Artikel 3, onderdeel 31) wordt nader gespecificeerd wat onder *kredietinstelling* wordt verstaan. Het gaat dan om een instelling die terugbetaalbare gelden aantrekt van het publiek (dat wil zeggen spaargelden en dergelijke) en krediet verleent.

Hoewel gemeenten kredieten kunnen verstrekken en via stadsbanken van lening financiële activiteiten uitvoeren, vallen zij niet onder de definitie uit de verordening. Immers, zij hebben geen activiteiten die gericht zijn op het ter beschikking krijgen van opvorderbare gelden van het publiek.

Daarom kan geconcludeerd worden dat noch gemeenten, noch stadsbanken van lening vallen onder het toepassingsbereik van de DORA. Daarmee is deze verordening buiten scope geplaatst.

Wanneer

De NIS2-richtlijn is in januari 2023 in werking getreden en moet vóór 17 oktober 2024 door alle EU-lidstaten in nationale wetgeving zijn omgezet. Doordat het Nederlandse wetgevingstraject vertraging heeft opgelopen, is de verwachting dat de wet minimaal vijf maanden na 17 oktober 2024 van kracht gaat worden.[50]

De Europese cyberbeveiligingsverordening is op 27 juni 2019 in werking getreden.

Het voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen (Cyberweerbaarheidsverordening) is op 15 september 2022 door de Commissie gepresenteerd. Een datum voor inwerkingtreding is nog niet bekend.

De Critical Entities Resilience richtlijn is op 16 januari 2023 in werking getreden. Uiterlijk op 17 oktober 2024 dienen de lidstaten de maatregelen vast te stellen en bekend te maken die nodig zijn om aan deze richtlijn te voldoen. Zij stellen de Commissie daarvan onverwijld in kennis. Zij passen die bepalingen toe met ingang van 18 oktober 2024. Elke lidstaat stelt uiterlijk op 17 januari 2026 een strategie vast om de veerkracht van kritieke entiteiten te vergroten (de "strategie"). Uiterlijk op 17 juli 2027 dient de Commissie bij het Europees Parlement en de Raad een verslag in waarin wordt beoordeeld in hoeverre elke lidstaat de nodige maatregelen heeft genomen om aan deze richtlijn te voldoen.

---

49 https://eur-lex.europa.eu/eli/reg/2022/2554/oj.

50 Uitstelbrief van J&V, NIS2 en CER

Waarom

De EU-regelgeving voor beveiliging van netwerk- en informatiesystemen voorziet in maatregelen die erop gericht zijn een hoog gemeenschappelijk niveau van cyberbeveiliging, cyberweerbaarheid en vertrouwen in de Unie te bereiken, teneinde de werking van de interne markt te verbeteren.

Op welke wijze

De NIS2 wordt op dit moment door het Ministerie van JenV vertaald naar nationale wetgeving in de Cyberbeveiligingswet (als opvolger van de Wbni). In mei 2024 is de internetconsulatie gestart: de fase waarin organisaties kunnen reageren op de wetteksten die uit de vertaling van de NIS2-richtlijn voortkomen.[51] Dit conceptwetsvoorstel zal een bovenliggende wet zijn. De verantwoordelijke hiervoor is het Ministerie van JenV. Hieronder komen aanvullende regelingen (AMvB's) die per vakministerie (en/of bovensectoraal) worden ingevuld; de Ministeries van BZK, IenW, VWS en JenV moeten hiervoor zorgdragen.

Met welke middelen

Het is nog onbekend op welke wijze de implementatie en uitvoering van de EU-regelgeving voor het beveiligen van netwerk- en informatiesystemen gefinancierd gaat worden. Het gaat daarbij om benodigde investeringen ter verhogen van de digitale weerbaarheid van de gemeentelijke organisaties en het implementeren van aankomende wet- en regelgeving.

2.4. Samenhangende ontwikkelingen

Er zijn verschillende samenhangende ontwikkelingen die ook gevolgen hebben voor de uitvoerbaarheid van het beveiligen van netwerk- en informatiesystemen. Achtereenvolgens wordt ingegaan op de krappe arbeidsmarkt, financiële tekorten bij gemeenten en de overige vijf thema's uit de Digital Decade.

Krappe arbeidsmarkt

De gemeentelijke uitvoering is krachtig, maar ook kwetsbaar.[52] Voor veel gemeenten is het aantrekken van voldoende capaciteit en de juiste expertise (over de gehele linie) een grote uitdaging vanwege de krappe arbeidsmarkt. Deze vraag wordt des te urgenter vanwege de grotere behoefte aan specialistische kennis bij gemeenten. Dit vraagstuk speelt in het bijzonder ook binnen het thema informatiebeveiliging.

Financiële tekorten bij gemeenten

Nederlandse gemeenten kampen met structurele financiële uitdagingen, de gemeentelijke financiën staan onder meer onder druk vanwege de tekorten in het sociaal domein.[53] Gemeenten zijn hierdoor genoodzaakt om te bezuinigen en dit zorgt onder meer voor lagere gemeentelijke investeringen in wegen, scholen en andere voorzieningen.

---

51 https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/nis2-wbni2.

52 VNG (2020), *Uitvoeringskracht van gemeenten. Hoe sterk zijn onze schouders?*

53 Zie bv. BDO (2023), *BDO-Benchmark Nederlandse gemeenten 2022. Tekorten nemen af, uitdagingen groter. Incidentele voordelen maskeren structurele problematiek*.

Los van de huidige situatie koersen gemeenten af op een financieel ravijn in 2026.[54] Extra geld vrijmaken binnen de gemeentelijke begrotingen voor het beveiligen van netwerk- en informatiesystemen is daarmee niet vanzelfsprekend. Gemeenten moeten de komende jaren al veel pijnlijke keuzes maken.

Overige thema's Digital Decade

De Digital Decade is een programma van de Europese Commissie dat tot doel heeft om de digitale transformatie van Europa te versnellen en te versterken, het concurrentievermogen van Europa te verbeteren, digitale inclusie te bevorderen en tegelijkertijd de digitale soevereiniteit van Europa te waarborgen. Gemeenten zullen aan verschillende EU-regelgeving moeten gaan voldoen.[55]

In de volgende figuur is de Europese regelgeving opgenomen die onderdeel uitmaakt van de Digital Decade. Implementatie en uitvoering van deze regelgeving gaat veel vragen van de uitvoering bij gemeenten.

Figuur 2.3 Europese wet- en regelgeving Digital Decade

[54] Zie bv. https://vng.nl/nieuws/webinar-over-financieel-ravijn-gat-mogelijk-nog-dieper. Vanaf 2026 krijgen gemeenten € 3 miljard per jaar minder. In de voorjaarsnota van 2024 heeft het kabinet maatregelen genomen waardoor dit tekort per saldo met € 1 miljard per jaar wordt gedempt. Er blijft echter wel een structureel tekort over van € 2 miljard per jaar.

[55] Zie https://vng.nl/nieuws/expertgroepen-digital-decade-gaan-in-2024-van-start.

3. Bestaande versus nieuwe verplichtingen

In dit hoofdstuk is een uitwerking gemaakt van de bestaande verplichtingen op het gebied van beveiligen van netwerk- en informatiesystemen en nieuwe verplichtingen die volgen uit de NIS2-richtlijn (zoals aangegeven in hoofdstuk 2 beschouwen we in deze analyse de NIS2-richtlijn als overkoepelende wetgeving). Daarbij is eerst gekeken naar de mogelijke vrijheidsgraden (ruimte) voor de verdere vertaling naar Nederlandse wetgeving en is van verschillende mogelijke vertalingen (varianten) op hoofdlijnen gekeken naar de mogelijke uitvoeringsconsequenties van de mogelijke vertalingen. Hiermee kan informatie over de uitvoeringsconsequenties en uitvoerbaarheid in een vroeg stadium worden meegenomen bij de verdere vertaling van de EU-richtlijn naar Nederlandse wetgeving.

Achtereenvolgens wordt ingegaan op de generieke verplichtingen, inhoudelijke verplichtingen en informatieverplichtingen van de NIS-2-richtlijn.

3.1. Generieke verplichtingen

In artikel 20 (Governance) van de NIS2-richtlijn zijn verschillende generieke verplichtingen voor de lidstaten opgenomen. Artikel 20 van de NIS2-richtlijn luidt:[56]

1. De lidstaten zorgen ervoor dat de bestuursorganen van essentiële en belangrijke entiteiten de door deze entiteiten genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren om te voldoen aan artikel 21, toezien op de uitvoering ervan en aansprakelijk kunnen worden gesteld voor inbreuken door de entiteiten op dat artikel.
   De toepassing van dit lid doet geen afbreuk aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen.
2. De lidstaten zorgen ervoor dat de leden van de bestuursorganen van essentiële en belangrijke entiteiten een opleiding moeten volgen, en moedigen essentiële en belangrijke entiteiten aan om regelmatig een soortgelijke opleiding aan hun werknemers aan te bieden, zodat zij voldoende kennis en vaardigheden verwerven 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.

In het navolgende is achtereenvolgens ingegaan op de volgende specifieke termen uit de richtlijn: bestuursorganen van essentiële en belangrijke entiteiten, aansprakelijkheid, verantwoordelijkheid[57] en opleiding.

In deze analyse is uitgegaan van de Nederlandse vertaling van de NIS2-richtlijn. Mogelijk zijn er inhoudelijke verschillen tussen de Engelse, Duitse en Nederlandse vertaling van artikel 20. In de Nederlandse vertaling zijn 'bestuursorganen' en 'leden van bestuursorganen' opgenomen en in de Duitse vertaling van 'Leitungsorgane' en 'Mitglieder der Leitungsorgane', terwijl in de Engelse vertaling de termen 'management bodies' en 'members of management bodies' zijn opgenomen. Dit

[56] Zie https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2555&from=EN.

[57] De term 'verantwoordelijkheid' komt niet in artikel 20 van de richtlijn terug. Vanwege spraakverwarring in het veld over deze term is hier in deze paragraaf wel aandacht aan besteed.

zorgt ervoor dat er verschillende interpretaties mogelijk zijn voor de uitleg van de NIS2-richtlijn. Waar relevant is dat in dit hoofdstuk benoemd.

Bestuursorganen van essentiële en belangrijke entiteiten

In artikel 1:1 Algemene wet bestuursrecht en artikel 6 Gemeentewet is meer informatie te vinden over de inhoud van het begrip bestuursorgaan. Het Ministerie van BZK heeft in het wetsvoorstel voor de Cyberbeveiligingswet gemeenten als essentiële entiteit aangewezen.[58] Redenen hiervoor zijn dat de overheid zelf ook een maatschappelijke taak heeft om op een zorgvuldige manier om te gaan met gegevens van burgers en bedrijven en dat de overheid ook een voorbeeldfunctie heeft. Dit betekent dat de NIS2-richtlijn van toepassing is/wordt op gemeenten.

Gemeenten participeren - in verschillende juridische vormen - in samenwerkingsverbanden, gemeenschappelijke regelingen, etc.[59] In het wetsvoorstel van de Cyberbeveiligingswet is in artikel 8 lid 1h ook opgenomen 'alsmede gemeenschappelijke regelingen voor zover deze laatste kwalificeren als entiteit van het in bijlage 1 of 2 van de NIS2-richtlijn bedoelde soort en als overheidsinstantie'.[60] Het is op dit moment echter nog niet duidelijk wat de NIS2-richtlijn betekent voor de onder artikel 6 punt 35 van de NIS2-richtlijn vallende verschillende type samenwerkingsverbanden waarbinnen gemeenten acteren.[61]

Gewenste vervolgactie: Werk uit wat de NIS2-richtlijn betekent voor de verschillende type samenwerkingsverbanden waarbinnen gemeenten opereren.

Aansprakelijkheid

In lid 1 van artikel 20 van de NIS2-richtlijn is opgenomen: *'de lidstaten zorgen ervoor dat de bestuursorganen … aansprakelijk kunnen worden gesteld …'*. Daarbij wordt in de passage onder lid 1 nog opgemerkt '*De toepassing van dit lid doet geen afbreuk aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen.*'

In lid 2 artikel 9:1 Awb is de volgende algemene bepaling opgenomen die hiermee samenhangt: *'Een gedraging van een persoon, werkzaam onder de verantwoordelijkheid van een bestuursorgaan, wordt aangemerkt als een gedraging van dat bestuursorgaan.'*

Er zijn verschillende vrijheidsgraden bij de verdere invulling van het begrip aansprakelijkheid. In de volgende tabel zijn hiervoor varianten gepresenteerd en is eveneens aangegeven wat de belangrijkste uitvoeringsconsequenties en risico's zijn bij de betreffende vertaling.

---

58 Dit is opgenomen in artikel 8 lid 1h van het wetsvoorstel voor de Cyberbeveiligingswet, zie https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12561.

59 Zie https://vng.nl/artikelen/gemeentelijke-samenwerking-in-kaart-gebracht.

60 In artikel 22 van de Cyberbeveiligingswet is opgenomen dat de Minister van BZK uiterlijk op 17 januari 2025 een nationaal register opstelt van entiteiten die conform de Cyberbeveiligingswet essentiële entiteit of belangrijke entiteit zijn. Dit kan mogelijk houvast gaan bieden voor gemeentelijke organisaties.

61 Daarbij is ook het onderscheid tussen mandateren en delegeren relevant: Mandateren is de bevoegdheid om in naam van een ander te handelen, zonder de daarbij behorende verantwoordelijkheid. Bij delegeren gaan zowel de bevoegdheid als de verantwoordelijkheid over naar de ander.

Tabel 3.1 Varianten + uitvoeringsconsequenties aansprakelijkheid

	Invulling door NL Rijksoverheid (minimaal)	Invulling door NL Rijksoverheid (maximaal)
Variant	Aansprakelijkheid bestuursorgaan	Bestuurdersaansprakelijkheid
Uitvoerings-consequenties	+ sluit aan bij bestaande regels aansprakelijkheid	+ onderschrijven belang - niet gebruikelijk in NL - collectieve besluitvorming? - vinden nieuwe bestuurders?

In de minimale vertaling van de richtlijn moet de Nederlandse overheid ervoor zorgen dat bestuursorganen aansprakelijk kunnen worden voor inbreuken op artikel 21 van de NIS2-richtlijn. Dit sluit ook aan bij de bestaande Nederlandse regelgeving op het gebied van aansprakelijkheid van bestuursorganen.

Een andere mogelijke invulling van aansprakelijkheid door Nederland is door te gaan werken met een aansprakelijkheid van bestuurders.[62] Een belangrijk argument hiervoor is dat daarmee duidelijk het belang van het beveiligen van netwerk- en informatiesystemen wordt benadrukt.[63] Bestuurdersaansprakelijkheid brengt verschillende nadelen en risico's met zich mee. Zo is het nu niet gebruikelijk dat bestuurders aansprakelijk kunnen worden gesteld voor hun gedragingen.[64] Als een bestuurder door de NIS2-richtlijn wel aansprakelijk kan worden gesteld voor de beveiliging van netwerk- en informatiesystemen en niet voor andere zaken, dan kan dat tot scheve keuzes gaan leiden waarbij risico's op het gebied van netwerk- en informatiesystemen tot nul worden gereduceerd waardoor er op andere vlakken weer nieuwe risico's ontstaan (als extreem voorbeeld: het ontslaan van de badmeester in het zwembad om een specialist op het gebied van informatiebeveiliging voor het zwembad aan te kunnen nemen; voor de veiligheid in het zwembad kan de bestuurder dan niet persoonlijk aansprakelijk gesteld worden, voor de informatiebeveiliging weer wel). Aansprakelijkheid van bestuurders kan het ook lastiger maken om goede bestuurders te vinden.

Daarnaast sluit aansprakelijkheid van een individuele bestuurder ook niet aan bij de wijze waarop besluitvorming binnen gemeenten wordt gedaan. In gemeenten is sprake van collectieve besluitvorming (door het college van B en W) en dat schuurt met een persoonlijke aansprakelijkheid van bestuurders. Als de wethouder onder wie het beveiligen van netwerk- en informatiesystemen valt vindt dat er extra geïnvesteerd moet worden in informatiebeveiliging dan kan het college besluiten om daarin niet mee te gaan en het geld te gebruiken voor andere activiteiten (bv. verlenen van jeugdzorg of het openhouden van de bibliotheek). Het kan dan tot vreemde situaties leiden als de wethouder vervolgens wel persoonlijk aansprakelijk kan worden gesteld.

Alles overziend brengt bestuurdersaansprakelijk hele serieuze uitvoeringsrisico's bij gemeenten met zich mee. Gegeven de uitvoeringsrisico's is het van belang om hier een hele zorgvuldige afweging te maken van de voor- en nadelen van de invulling van de aansprakelijkheid. In het wetsvoorstel voor de Cyberbeveiligingswet zijn geen aparte bepalingen opgenomen met betrekking tot de aansprakelijkheid van bestuurders, het wetsvoorstel lijkt daarbij aan te sluiten bij de invulling zoals

[62] Het gemeentebestuur bestaat uit een (gemeente)raad, een college (van burgemeester en wethouders) en een burgemeester (zie artikel 6 Gemeentewet).

[63] Overigens zijn er ook voldoende andere mogelijkheden om dit belang te benadrukken zonder een bestuurder meteen aansprakelijk te stellen.

[64] Er zijn incidenteel wel voorbeelden waar een ambtenaar persoonlijk aansprakelijk werd gesteld blijkt uit enkele uitspraken van de Hoge Raad.

geschetst in de minimale variant. In de MvT van de Cyberbeveiligingswet is hierover op pagina 24 opgenomen:[65] “De NIS2-richtlijn breidt de aansprakelijkheid van deze organen echter niet uit.” Het is nog wel van belang om ondubbelzinnig aan te geven of bestuurders van gemeenten wel of niet aansprakelijk gesteld kunnen worden op grond van de NIS2-richtlijn.

Verantwoordelijkheid

In artikel 20 van de NIS2-richtlijn komt het begrip verantwoordelijkheid niet terug. Tegelijk wordt er wel gesproken over de vraag of bestuurders of zelfs specifieke functionarissen (zoals de gemeentesecretaris) binnen de gemeente verantwoordelijk moeten worden voor het beveiligen van netwerk- en informatiesystemen.[66] In de volgende tabel zijn hiervoor varianten gepresenteerd en is eveneens aangegeven wat de belangrijkste uitvoeringsconsequenties en risico’s zijn bij de betreffende vertaling.

Tabel 3.2 Varianten + uitvoeringsconsequenties verantwoordelijkheid

	Invulling door NL Rijksoverheid (minimaal)	**Invulling door NL Rijksoverheid (maximaal)**	
Variant	Bestuursorgaan is verantwoordelijk	Specifieke functionaris (gemeentesecretaris) is verantwoordelijk	Specifieke bestuurder (wethouder) is verantwoordelijk
Uitvoerings-consequenties	+ sluit aan bij bestaande structuren	+ functionaris krijgt positie - verantwoordelijkheid zonder bevoegdheden	+ bestuurder krijgt positie - verantwoordelijkheid zonder bevoegdheden (collectieve besluitvorming)

Er zijn verschillende beelden of de NIS2-richtlijn wel of niet voorschrijft dat er een aparte uitwerking moet worden gemaakt van de verantwoordelijkheden binnen bestuursorganen.[67] Gemeenten dienen (als bestuursorgaan) te voldoen aan veel verschillende verplichtingen en hebben zelf (fijnmazig) geregeld wie wat doet en wie waarvoor verantwoordelijk is.

In de BIO versie 1 is opgenomen welke functionarissen verantwoordelijk zijn voor de uitvoering van een control: secretaris/algemeen directeur, proceseigenaar en/of (interne of externe) dienstenleverancier.[68] De BIO kent echter geen wettelijke basis, maar is gebaseerd op een zelfverplichting. Bij de wettelijke vastlegging van de BIO krijgt de term ‘verantwoordelijkheid’ mogelijk ook een andere juridische lading.

Een voordeel van het wettelijk vastleggen van de verantwoordelijkheid voor de beveiliging van netwerk- en informatiesystemen bij een specifieke functionaris (gemeentesecretaris) of bestuurder (wethouder) zorgt er wel voor dat de betreffende functionaris of bestuurder een betere positionering binnen de gemeente krijgt. Voor het regelen van een betere positionering zijn er overigens ook andere (minder ingrijpende) alternatieven denkbaar. In de Algemene verordening gegevensbescherming (AVG) is bijvoorbeeld een aparte afdeling opgenomen voor de functionaris

[65] Zie: https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12562.
[66] Dit hangt ook samen met het vraagstuk van de aansprakelijkheid.
[67] Dit is afhankelijk van de uitleg van de vertalingen van de Engelse termen ‘management bodies’ en ‘members of management bodies’. In de MvT van de Cyberbeveiligingswet stelt het Ministerie van BZK opmerkelijk genoeg dat met ‘management bodies’ in artikel 20 van de NIS2-richtlijn het bestuur van een organisatie wordt bedoeld, wat de reden is om in artikel 26 lid 1 aan te geven dat het bestuur toeziet op de maatregelen en de uitvoering van de maatregelen.
[68] Zie https://bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf.

voor gegevensbescherming, maar daarin worden onder meer taken beschreven en geen verantwoordelijkheden.

Een belangrijk aandachtspunt bij het beleggen van de verantwoordelijkheid bij een functionaris of bestuurder is dat iemand pas echt verantwoordelijk kan worden gehouden als de betreffende persoon voldoende bevoegdheden heeft om beslissingen te nemen en om voldoende (financiële) middelen in te zetten. Uit het voorgaande kwam naar voren dat ook wethouders ook beperkte bevoegdheden (vanwege de collectieve besluitvorming door het college). Wat kan een functionaris of bestuurder die het nodig vindt dat investeringen worden gedaan in informatiebeveiliging, maar die niet krijgt? Dit kan tot serieuze issues in de uitvoering leiden.

In de Cyberbeveiligingswet is in lid 1 van artikel 26 (governance) opgenomen dat de maatregelen (bedoeld in artikel 23) zijn onderworpen aan goedkeuring door het bestuur van de desbetreffende essentiële entiteit of belangrijke entiteit en dat het bestuur toeziet op de maatregelen en de uitvoering van de maatregelen. In het wetsvoorstel zijn buiten het bestuur geen specifieke functionarissen binnen een organisatie benoemd die verantwoordelijk zijn voor de beveiliging van netwerk- en informatiesystemen.

Opleiding

In lid 2 van artikel 20 van de NIS2-richtlijn is opgenomen dat *'leden van bestuursorganen … een opleiding moeten volgen … zodat zij voldoende kennis en vaardigheden verwerven 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.'* In lid 2 van artikel wordt onderscheid gemaakt naar leden van bestuursorganen (verplichting) en werknemers[69] (moedigen aan). In de volgende tabel zijn hiervoor varianten gepresenteerd en is eveneens aangegeven wat de belangrijkste uitvoeringsconsequenties en risico's zijn bij de betreffende vertaling.

Tabel 3.3 Varianten + uitvoeringsconsequenties opleiding leden van bestuursorganen

	Invulling door NL Rijksoverheid (minimaal)	**Invulling door NL Rijksoverheid (maximaal)**
Variant	"Is het bestuur bekend met de 10 bestuurlijke principes voor informatiebeveiliging?"	Volgen opleiding (dagdeel, dagen, meer?)
Uitvoerings-consequenties	Beperkt	+ opdoen (en toepassen) kennis - kosten opleiding + tijd deelnemers

De Nederlandse overheid heeft vrijheidsgraden om invulling te geven aan de verplichting voor leden van bestuursorganen (of bestuurders) om een opleiding te volgen. Enerzijds kan dit worden ingevuld door bestuurders bijvoorbeeld kennis te laten nemen van de tien bestuurlijke principes voor informatiebeveiliging (zie ook vraag 11 van de ENSIA rapportage). Anderzijds kan er ook voor worden gekozen om wettelijk vast te leggen dat bestuurders een bepaalde opleiding moeten volgen. Het voordeel van het volgen van een opleiding is dat de bestuurders hiermee kennis kunnen opdoen en toepassen. Tegelijk kost het volgen van een opleiding ook tijd en geld.

[69] De term werknemers is hier overigens wat vreemd, de term medewerkers (dus zowel werknemers als externen) lijkt hier passender.

Het is bij de verdere invulling van deze verplichting vooral relevant dat de opleiding aansluit bij de rol van de bestuurder. De rol van een raadslid is anders dan de rol van een wethouder. En de rol van de wethouder die het beveiligen van netwerk- en informatiesystemen in zijn portefeuille heeft is anders dan de rol van de andere wethouders. Het is hierbij van belang dat niet wordt gestart met het wettelijk vastleggen welke opleiding moet worden gevolgd, maar dat wordt gestart vanuit de verschillende behoeften en de verschillende rollen van de bestuurders bij gemeenten.

Gewenste vervolgactie: Onderzoek de opleidingsbehoeften van de verschillende groepen bestuurders bij gemeenten alvorens een concrete verplichting voor het volgen van opleidingen vast te leggen in de Nederlandse regelgeving.

Lid 2 van artikel 20 van de NIS2-richtlijn stelt eveneens: '*lidstaten … moedigen essentiële en belangrijke entiteiten aan om regelmatig een soortgelijke opleiding aan hun werknemers aan te bieden …'*. Het is belangrijk om hier te constateren dat aanmoedigen iets anders is dan verplichten, dus het is de vraag of regelgeving hier het passende instrument is. Er kan ook aan alternatieve instrumenten voor de Rijksoverheid worden gedacht zoals bijvoorbeeld het verstrekken van subsidies voor medewerkers voor het volgen van dergelijke opleidingen.

In artikel 26 lid 8 van de Cyberbeveiligingswet is opgenomen dat bij onder meer gemeenten als 'leden van het bestuur' worden aangemerkt 'leden van de ambtelijke leiding' voor zover het gaat om de *verplichtingen met betrekking tot kennis en vaardigheden* (artikel 26 lid 2 t/m lid 6). In de MvT van de Cyberbeveiligingswet is aangegeven dat *in ieder geval* de secretaris (gemeentesecretaris) deel uitmaakt van de ambtelijke leiding. Het is daarbij (nog) niet duidelijk wie verder onder de ambtelijke leiding van een gemeente moet worden verstaan (directie, managementteam?). De verplichting inzake kennis en vaardigheden zou dan niet van toepassing zijn voor het college van B en W en voor gemeenteraadsleden.[70] Deze invulling van de NIS2-richtlijn is niet meegenomen in de expertbijeenkomsten voor deze uitvoeringsanalyse, vandaar dat het niet goed mogelijk is om de belangrijkste uitvoeringsconsequenties hiervan goed te kunnen duiden. De gewenste vervolgactie met betrekking tot de opleidingsbehoeften blijft overigens wel van toepassing.

In artikel 26 lid 7 Cyberbeveiligingswet is daarbij nog opgenomen: '*Indien een rechtspersoon een lid van het bestuur van een essentiële entiteit of belangrijke entiteit is, rusten de verplichtingen uit het tweede, derde en vierde lid hoofdelijk op een ieder die van die rechtspersoon bestuurder is.'* Het is denkbaar dat een gemeente één van de bestuurders is van een samenwerkingsverband. Een gemeente is een rechtspersoon en als een gemeente bestuurder is van een samenwerkingsverband is artikel 26 lid 7 van toepassing. In dat geval rusten de verplichtingen van het tweede, derde en vierde lid hoofdelijk op een ieder die van die rechtspersoon bestuurder is, waarbij de afbakening van leden van bestuur gemaakt in artikel 26 lid 8 weer niet van toepassing is op artikel 26 lid 7. Deze verplichting lijkt meer verdergaand te zijn dan de overige verplichtingen in artikel 26.[71]

[70] In de MvT van de Cyberbeveiligingswet is hierover op pagina 24 opgenomen 'Dergelijke verplichtingen passen niet goed bij politiek benoemde ambtsdragers zoals een Minister of wethouder.' Zie: https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12562.

[71] Opmerkelijk genoeg wordt artikel 26 lid 7 niet nader toegelicht in de MvT van de Cyberbeveiligingswet, die onderdeel is van de internetconsultatie.

Uit paragraaf 3.1 blijkt dat er nog veel onduidelijkheid is over de exacte reikwijdte en betekenis van verschillende termen. Het is van belang voor een goede uitvoering dat hier geen onduidelijkheid over is bij gemeenten.

Gewenste vervolgactie: Het is van belang dat de uitwerking van termen als bestuursorganen, leden van bestuursorganen, aansprakelijkheid, verantwoordelijkheid en doelgroep van de opleidingen in relatie tot de NIS2-richtlijn ondubbelzinnig zijn en worden uitgewerkt in de Cyberbeveiligingswet.

3.2. Inhoudelijke verplichtingen

Naast de generieke verplichtingen volgen er uit de NIS2-richtlijn ook inhoudelijke verplichtingen. De inhoudelijke verplichtingen richten zich op maatregelen voor het beheer van risico's voor het beveiligen van netwerk en informatiesystemen. De inhoudelijke verplichting is opgenomen in artikel 21 van de NIS2-richtlijn. Artikel 21 van de NIS2-richtlijn luidt:[72]

NIS2 artikel 21, lid 1

1. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden 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.
   Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met de uitvoeringskosten, zorgen de in de eerste alinea bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

NIS2 artikel 21, lid2

2. De in lid 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende (artikelen 21, lid 2 a) t/m j).
   a) Beleid inzake risicoanalyse en beveiliging van informatiesystemen;
   b) Incidentenbehandeling;
   c) Bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;
   d) De beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
   e) Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
   f) Beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
   g) Basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
   h) Beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
   i) Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

[72] Zie https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2555&from=EN.

j) Wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

In artikel 21 zijn drie aspecten te onderscheiden, namelijk a) het in beeld hebben van informatiebeveiligingsrisico's en b) het beheren hiervan (lid 1) en c) het nemen van maatregelen om de risico's te mitigeren (lid 2). Ze zijn onderling nauw verbonden; Het is nodig om in beeld te hebben wat de risico's zijn om gerichte maatregelen te kunnen nemen die tot doel hebben netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen. Op deze manier worden maatregelen gekoppeld aan informatiebeveiligingsrisico's om te zorgen dat de kans op het optreden van een incident met een grote impact (de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen) verminderd wordt. Daarbij is het nodig om de risico's te beheren en maatregelen te treffen die alle gevaren omvat. Hiervoor is het nodig steeds te weten of de maatregelen effectief zijn. Dit vergt een systematische analyse. Dit wordt ook beschreven in aanwijzing (78) van de richtlijn "Maatregelen voor het beheer van cyberbeveiligingsrisico's moeten voorzien in een systemische analyse…" In artikel 23 (zorgplicht) van de Cyberbeveiligingswet zijn verplichtingen opgenomen voor essentiële en belangrijke entiteiten die (nagenoeg volledig) aansluiten op de bepalingen in artikel 21 van de NIS2-richtlijn. In het vierde lid van artikel 23 Cyberbeveiligingswet is opgenomen dat bij of krachten algemene maatregel van bestuur nadere regels worden gesteld over de in het eerste lid bedoelde maatregelen.[73]

In de huidige situatie hebben gemeenten de BIO om deze drie aspecten te organiseren. Dit is beschreven in hoofdstuk 2 van deze rapportage. De BIO is geen wettelijke verplichting, maar is een vorm van zelfregulering. De AVG is een wettelijke verplichting die gaat over het beschermen van persoonsgegevens en het treffen van maatregelen op de verwerkingen van persoonsgegevens. Zowel de NIS2-verplichtingen als de AVG richten zich op het adresseren van risico's en het nemen van passende maatregelen. Er zijn ook verschillen. De NIS2-richtlijnricht zich op het grotere geheel van digitale veiligheid met een focus op continuïteit van belangrijke en essentiële processen, terwijl de AVG focust op de bescherming van individuele rechten. Het Ministerie van BZK is voornemens om de Baseline Informatiebeveiliging Overheid (BIO) wettelijk te gaan verankeren en om in de reeds geplande modernisering van de BIO de eisen van de NIS2-richtlijn mee te nemen.[74] Dit moet gebeuren in lagere regelgeving (AMvB). Hierbij zijn een aantal aandachtspunten mee te geven:[75]

- Gemeenten geven aan dat het systematische beheren (PDCA-cyclus) van informatiebeveiligingsrisico's en meten van effectiviteit van maatregelen (ISMS) meer centraal gezet zou moeten worden in de BIO. Dit is ook gebleken uit de evaluatie van de BIO (zie hoofdstuk 2). Een mogelijke wijze om dit te bereiken is om de ISO 27001 meer centraal te stellen. De BIO is immers gebaseerd op en gestructureerd volgens de ISO 27001 (zie hoofdstuk 2).[76]

[73] Deze uitwerking is op het moment van schrijven van dit rapport nog niet bekend.
[74] Begin juni 2024 is een consultatie van de BIO 2.0 gestart. Deze verloopt via Github https://minbzk.github.io/Baseline-Informatiebeveiliging-Overheid/ en loopt tot 5 juli 2024. De aanpassingen die hierin zijn voorzien, zijn niet meegenomen in de eventuele uitvoeringsconsequenties van deze analyse.
[75] Deels komen deze aandachtspunten ook de eerder genoemde evaluatie van de BIO, we noemen deze punten hier ook omdat ze tijdens de uitvoeringsanalyse nog actueel waren.
[76] In de BIO 2.0 versie die ter consultatie ligt, is de ISO27001 meer centraal gesteld.

- Het meer centraal stellen van het risicobeheer voorkomt ook dat de focus kan komen te liggen op het afvinken van maatregelen en informatiebeveiliging als een eenmalige inspanning wordt gezien.
- Het is hierbij ook nodig om rekening te houden met de volwassenheid van het organisatiebrede risicobeheer van gemeenten waar het beheer van informatiebeveiligingsrisico's een onderdeel van is. Door alleen verplichte eisen aan het beheren van informatiebeveiligingsrisico's te stellen, bestaat het risico op het uit de pas lopen met de rest van het gemeentelijke risicomanagement. Van belang is ook om hier de samenhang te bewaken tussen de informatiebeveiligingseisen voor verwerken van persoonsgegevens die voortvloeien uit de AVG.
- Een certificering van een internationale normering toont aan dat een organisatie intern het risicobeheer heeft geregeld en voldoet aan de gestelde eisen. Dit zou bijvoorbeeld kunnen via een verplichte certificering van de internationale ISO27001 norm. Gemeenten geven aan dat zo'n gecertificeerde norm meer duidelijkheid kan geven waaraan moet worden voldaan. Voor de meeste gemeenten zal dit echter een grote inspanning vergen om hieraan te voldoen omdat de meeste gemeenten nog niet systematisch de effectiviteit van maatregelen en informatie-beveiligingsrisico's beheren (dat is nodig om gecertificeerd aan de verplichte normering te voldoen). Ook zonder certificering kan een gemeente aan de gestelde verplichtingen voldoen, zolang de gemeente maar kan aantonen dat de gemeente de maatregelen heeft getroffen t.a.v. de onderwerpen die in NIS2 artikel 21 lid 2 sub a t/m j zijn opgenomen.
- Voor de meeste gemeenten geldt een groeipad om eerst te komen tot een ingericht risicobeheer en vervolgens een werkend ISMS. Een werkend ISMS is nog geen gemeengoed, en is een grote inspanning als een gemeente dit nog niet heeft. Dit zal een meerjarig organisatie-ontwikkelingstraject vergen met aandacht voor de uitvoerbaarheid voor grote én kleine gemeente zonder geld en middelen (zie hiervoor paragraaf 3.4). Het is randvoorwaardelijk dat hier financiële middelen voor beschikbaar komen.
- De BIO-maatregelen komen grotendeels overeen met de aandachtsgebieden vanuit NIS2. Waar dit nog niet zo is, worden in de reeds geplande modernisering van de BIO de eisen van de NIS2-richtlijn mee genomen:
  - Specifiek voor (art 21, 2) geldt dat er meer hulp nodig is bij het borgen van leveranciers-management in de keten. Dit geldt met name in de mate van uitvoerbaarheid van de beveiliging van de toeleveringsketen als individuele gemeente met grote leveranciers afspraken moeten maken.[77]
  - Om te voorkomen dat het hele vakgebied van bedrijfscontinuïteitsmanagement (BCM) onder informatiebeveiliging gaat vallen, moet duidelijk worden dat de verplichting van NIS2 (lid 21, art 2 (c)) gaat om informatiebeveiligingsaspect binnen BCM en niet het BCM als geheel. In de evaluatie van de BIO wordt dit ook zo geadviseerd.
  - Beveiliging van operationele techniek (OT)/procesautomatisering (PA) staat niet expliciet in NIS2, artikel 21, lid 2 als aandachtsgebieden genoemd, maar omdat er geen onderscheid wordt gemaakt in de techniek (kantoorautomatisering vs. OT/PA) in de NIS2 kan verondersteld worden dat OT/PA-beveiliging er impliciet bij hoort. Daarnaast worden een aantal sectoren in de bijlage van NIS2 genoemd zoals vervoer en afvalwater waardoor OT/PA-beveiliging onder de NIS2 valt. Dit zou kunnen betekenen dat de ISA62443 en de CSIR-uitwerking (maatregelen voor beheer van OT/PA systemen, zie hoofdstuk 2) van toepassing kunnen worden voor gemeenten. Zodra de CSIR in nationale regelgeving verplicht wordt gesteld, gaat dit een zware last leggen op de gemeente. Gemeenten fungeren als wegbeheerders en zijn derhalve verantwoordelijk voor de beveiliging van

[77] Hier zou de Cyberweerbaarheidsverordening in potentie baat moeten bieden.

fysiek op afstand bestuurbare infrastructuur (operationele technologieën zoals verkeerslichten, bruggen en slagbomen). Voor de andere sectoren, zoals de gezondheidszorg (GGD), afvalwaterbeheer en drinkwatervoorziening, dient nagegaan te worden of de taken gedelegeerd of gemandateerd zijn en of daaruit aanvullende maatregelen worden gesteld. Het Ministerie van IenW werkt dit uit voor de sector vervoer, het Ministerie van VWS werkt dit uit voor de sector gezondheidszorg. Dit kan mogelijk extra inspanning vergen van gemeenten om deze maatregelen te implementeren.

Gewenste vervolgactie: Er is een meerjarig organisatieontwikkelingstraject nodig om de regelgeving bij gemeenten te implementeren. Zorg voor een realistische termijn waarbij gemeenten de tijd krijgen om aan de gestelde eisen van de wetgeving te kunnen voldoen (bijvoorbeeld door opschorting van de Nederlandse handhaving op dit punt gedurende die overgangsperiode).

3.3. Informatieverplichtingen

Naast de generieke verplichtingen en de inhoudelijke verplichtingen volgen er uit de NIS2-richtlijn ook verschillende informatieverplichtingen. Inhoudelijke verplichtingen zijn verplichtingen om direct te voldoen aan normen, standaarden, gedragscodes en alle overige eisen gericht op het borgen van publieke doelen. Informatieverplichtingen zijn verplichtingen tot het verschaffen van informatie over handelingen en gedragingen die volgen uit inhoudelijke verplichtingen. Informatieverplichtingen zijn weer verder onder te verdelen in rapportageverplichtingen (artikel 23 NIS2) en toezicht (artikel 24 NIS2). In het navolgende zijn beide onderwerpen nader uitgewerkt.

Rapportageverplichtingen

In artikel 23 van de NIS2-richtlijn zijn onder het kopje ‘rapportageverplichtingen’ bepalingen opgenomen wanneer bestuursorganen een melding door moeten geven aan hun CSIRT.[78] In de tekst hieronder zijn de verplichtingen voor bestuursorganen opgenomen.

1. ... dat essentiële en belangrijke entiteiten elk incident dat aanzienlijke gevolgen heeft voor de verlening van hun diensten als bedoeld in lid 3 (significant incident) onverwijld meldt bij zijn CSIRT of …
2. ... dat essentiële en belangrijke entiteiten de ontvangers van hun diensten die mogelijkerwijs door een significante cyberdreiging worden getroffen, onverwijld meedelen welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indien nodig stellen de entiteiten die ontvangers ook in kennis van de significante cyberdreiging zelf.
3. Een incident wordt als significant beschouwd als het …
4. De lidstaten zorgen ervoor dat de betrokken entiteiten, voor de in lid 1 bedoelde melding, …
   a) onverwijld en in elk geval binnen 24 uur ... een vroegtijdige waarschuwing geven ...;
   b) onverwijld en in elk geval binnen 72 uur ... een incidentmelding indienen met, indien van toepassing, een update van de in punt a) bedoelde informatie, een initiële beoordeling van het significante incident ...;
   c) op verzoek van het CSIRT ... een tussentijds verslag indienen over relevante updates van de situatie;

[78] Eigenlijk is de titel van dit artikel ‘rapportageverplichtingen’ hier ietwat verwarrend. Dit artikel gaat namelijk alleen over de rapportageverplichtingen die samenhangen met het melden van significante incidenten (of zoals het in de BIO is genoemd ‘rapportage van informatiebeveiligingsgebeurtenissen’) en niet over bijvoorbeeld rapportageverplichtingen die volgen uit het toezicht.

d) uiterlijk één maand na indiening ... een eindverslag indienen waarin het volgende is opgenomen ...

e) indien het incident nog aan de gang ... een voortgangsverslag indienen en binnen één maand nadat zij het incident hebben afgehandeld, een eindverslag indienen.

In de volgende tabel is een vergelijking gemaakt tussen de nieuwe verplichtingen en de huidige verplichtingen en de mate waarin er nog aandachtspunten of vrijheidsgraden zijn met betrekking tot de verdere invulling van de begrippen.

Tabel 3.5 Verschillen verplichtingen melding incidenten

	EU-verplichting	Huidige verplichting	Aandachtspunten
Incident significant	- een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; - andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.	Een (informatie) beveiligingsincident is een enkele of serie van ongewenste of onverwachte gebeurtenissen die een significante kans hebben op het veroorzaken van een ramp, het compromitteren van de bedrijfsprocessen en een bedreiging vormen ten aanzien van de beveiliging.	Afbakening begrip 'significant incident'?
Meedelen aan ontvangers van diensten	- welke maatregelen ontvangers kunnen nemen ... - indien nodig ... ook in kennis van de significante cyberdreiging zelf.	Analyses van de beveiligingsincidenten worden gedeeld met de relevante partners ...	Mogelijke verzwaring vanwege 'ontvangers' in plaats van 'relevante partners'
Melding aan CSIRT	- binnen 24 uur vroegtijdige waarschuwing - binnen 72 uur incidentmelding - tussentijds verslag - binnen 1 maand eindverslag - voortgangsverslag + eindverslag	Informatiebeveiligingsincidenten ... behoren zo snel mogelijk (binnen 72 uur) ... te worden gemeld aan ... de sectorale CSIRT (IBD).	- Verzwaring van frequentie van meldingen - Afbakening: Welke informatie moet worden opgenomen in de meldingen?

In de bovenstaande tabel is een overzicht opgenomen van de belangrijkste verschillen tussen de huidige en de nieuwe verplichtingen voor het melden van informatiebeveiligingsincidenten. Ook hier zijn er verschillende begrippen die nog nader ingevuld moeten worden zoals de definities van een significant incident. Blijft de definitie van een significant incident hetzelfde als nu of wordt deze verder aangescherpt (waardoor er mogelijk meer incidenten gemeld moeten worden).[79] Een mogelijke 'verzwaring' hangt samen met de verplichting om ontvangers van hun diensten onverwijld mee te delen welke maatregelen zij kunnen nemen in reactie op de dreiging. Ook is er een verzwaring in het aantal meldingen en verslagen per informatiebeveiligingsincident. In de artikelen 28 tot en met 31 van het wetsvoorstel voor de Cyberbeveiligingswet is opgenomen welke informatie in de meldingen moet worden opgenomen. Een laatste mogelijke verzwaring is dat de huidige

[79] In de nog op te stellen algemene maatregel van bestuur wordt nog een uitwerking gemaakt van de definitie van een significant incident.

meldingen onder de BIO een vormvrij karakter hebben, waardoor deze op dit moment ook relatief minder tijd kosten.

Per saldo is het de verwachting dat het rapporteren over informatiebeveiligingsincidenten per incident meer tijd gaat kosten, maar in vergelijking met de algemene en inhoudelijke verplichtingen en mogelijke verplichtingen volgend uit het toezicht zijn de impact en uitvoeringskosten voor dit onderdeel naar verwachting relatief beperkt. Daarbij is het ook relevant om goed te kijken naar de samenhang van het melden van een datalek bij de Autoriteit Persoonsgegevens en het melden over een informatiebeveiligingsincident bij de CSIRT.

De bepalingen uit artikel 23 van de NIS2-richtlijn zijn overgenomen in de artikelen 27 tot en met 32 van de Cyberbeveiligingswet met enkele kleine aanvullingen. Wel is in artikel 37 van de Cyberbeveiligingswet een bepaling opgenomen dat nog nadere regels kunnen worden gesteld over de artikelen 27 tot en met 32; hierover is op dit moment nog niets bekend.

Toezichts- en handhavingsmaatregelen

In artikel 32 van de NIS2-richtlijn zijn de toezichts- en handhavingsmaatregelen met betrekking tot essentiële entiteiten opgenomen. In de volgende tekst zijn enkele relevante onderdelen opgenomen.

1. De lidstaten zorgen ervoor dat de toezichts- of handhavingsmaatregelen die met betrekking tot de in deze richtlijn vastgestelde verplichtingen aan essentiële entiteiten worden opgelegd, doeltreffend, evenredig en afschrikkend zijn, rekening houdend met de omstandigheden van elk afzonderlijk geval.
2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot essentiële entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten minste:
   a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles die worden uitgevoerd door daartoe opgeleide professionals;
   b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door een onafhankelijke instantie of een bevoegde autoriteit;
   c) ad-hoc audits, ook in gevallen waarin dat gerechtvaardigd is op grond van een significant incident of inbreuk op deze richtlijn door de essentiële entiteit;
   d) beveiligingsscans op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit;
   e) verzoeken om informatie die nodig is om de door de betrokken entiteit genomen maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen, met inbegrip van gedocumenteerd cyberbeveiligingsbeleid, alsmede de naleving van de verplichting op grond van artikel 27 om bij de bevoegde autoriteiten informatie in te dienen;
   f) verzoeken om toegang tot gegevens, documenten en informatie die nodig zijn voor de uitoefening van hun toezichthoudende taken;
   g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

De Rijksinspectie Digitale Infrastructuur (RDI) is op dit moment al de toezichthouder voor de naleving van de Wet beveiliging netwerk- en informatiesystemen (Wbni) voor de energiesector, de digitale

infrastructuur en voor digitale dienstverleners. De RDI wordt straks ook de bevoegde autoriteit voor de toezichts- en handhavingsmaatregelen van de NIS2-richtlijn bij overheidsdiensten.[80]

In de opsomming in lid 2 van artikel 32 NIS2-richtlijn is een uitgebreid overzicht opgenomen van de bevoegdheden die de bevoegde autoriteiten ten minste moeten hebben. Een belangrijk aandachtspunt hierbij is dat het hebben van een bevoegdheid iets anders is dan het toepassen of gebruiken van diezelfde bevoegdheid. Als er een hamer in een gereedschapskist zit, wil niet zeggen dat die hamer ook overal voor gebruikt moet worden. De lidstaten (en dus ook de Rijksoverheid) hebben (veel) ruimte om te bepalen in welke gevallen (of events) bevoegdheden kunnen worden toegepast en met welke frequentie (hoe vaak). Daarbij is er bijvoorbeeld ook ruimte voor risicogebaseerd toezicht.

Gemeenten hebben grote zorgen over de nadere uitwerking van het toepassen van de verschillende bevoegdheden en in het bijzonder over de informatie die gemeenten aan moeten gaan leveren aan de RDI zodat de RDI ook adequate informatie heeft voor het uitvoeren van het toezicht. Deze zorgen worden onder meer vergroot door vele publicaties over miljoenenboetes en bestuurdersaansprakelijkheid. Het is van belang dat gemeenten hier snel duidelijkheid over krijgen.

Het Ministerie van BZK heeft in haar brief aan de koepels IPO, VNG en UvW[81] aangegeven dat zij maximaal gebruik wil maken van de bestaande toezichts- en verantwoordingsinstrumenten en waar nodig deze instrumenten versterken en optimaal op elkaar laten aansluiten. Dit ook om een eventuele extra lastendruk te minimaliseren. Daarbij wordt in beginsel gekeken naar een versterking van de ENSIA-systematiek, zodat lokale verantwoording en toezicht op informatieveiligheid worden gebundeld.

Tabel 3.6 Varianten + uitvoeringsconsequenties toezichts- en handhavingsmaatregelen

	Invulling door NL Rijksoverheid (minimaal)	**Invulling door NL Rijksoverheid (maximaal)**
Variant	Verantwoording over informatiebeleid aan gemeenteraad (vgl. Wet open overheid)	Verantwoording over informatiebeleid aan gemeenteraad + toezichthouder (vgl. ENSIA)
Uitvoerings-consequenties	+ sluit aan bij bestaande verantwoording	+ beter inzicht toezichthouder - tijd bestuursorgaan - uitvoeringsrisico: tijd rapporteren aan toezichthouder gaat ten koste van voldoen aan inhoudelijke verplichtingen - uitvoeringsrisico: stapeling van toezicht door verschillende toezichthouders

Ook bij de invulling van de toezichts- en handhavingsmaatregelen zijn verschillende varianten denkbaar. Bij een minimale invulling wordt aangesloten bij de reguliere verantwoording aan de gemeenteraad, waarbij de raadsleden dankzij de (mogelijk) verplichte opleiding voor raadsleden dan ook weten hoe zij de verantwoording over het informatiebeleid moeten beoordelen. Vergelijk dit bijvoorbeeld met de verantwoording over de Wet open overheid, waarbij de gemeente in de

[80] Zie https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/nis2-wbni2.

[81] Zie https://vng.nl/sites/default/files/2023-11/brief-nis2-bij-de-overheid.pdf waarin is opgenomen hoe het Ministerie van BZK het toezicht en de verantwoording willen inrichten.

jaarlijkse verantwoording (jaarverslag) verslag doet van de uitvoering van de wet (artikel 3.5 Woo). Extra uitvoeringslasten kunnen in dat geval beperkt blijven.

Bij een ruimere invulling van de verantwoording (naast verantwoording aan de gemeenteraad, ook aan de toezichthouder) is het uiteraard de vraag hoe deze verantwoording eruit komt te zien. Het uitgangspunt van het Ministerie van BZK is om hierbij aan te sluiten bij de ENSIA-systematiek die mogelijk nog wel versterkt dient te worden. Dit zorgt in ieder geval voor een beter inzicht bij de toezichthouder, maar kost het bestuursorgaan ook meer tijd als naast de eigen rapportages extra rapportages moeten worden gemaakt voor de toezichthouder. Daarbij is veelvuldig opgemerkt dat - vanwege beperkte gemeentelijke capaciteit - de tijd aan het rapporteren aan de toezichthouder ten koste gaat van de tijd om te voldoen aan de inhoudelijke verplichtingen zelf. En dat dit ook tot inhoudelijke verschuivingen kan leiden (vooral voldoen aan eisen van toezichthouder in plaats van weerbaar zijn tegen dreigingen van buitenaf). Een ander uitvoeringsrisico is de mogelijke stapeling van toezicht door verschillende toezichthouders (bijvoorbeeld omdat gemeenten zowel moeten voldoen aan de NIS2 als de AVG en omdat er mogelijk meer toezichthouders bijkomen voor toezicht op kritieke sectoren die onder de NIS2 vallen en waarvoor gemeenten taken uitvoeren (zoals vervoer, drinkwater, afvalbeheer en gezondheidszorg)).

Opgemerkt dient te worden dat het gemeenten op dit moment heel veel tijd en werk kost om te verantwoorden aan de hand van de bestaande ENSIA-systematiek. Bij een verdere versterking van de ENSIA-systematiek is het dan ook van belang om goed te onderzoeken hoe de uitvoeringslasten van het toezicht voor gemeenten ook echt tot een minimum beperkt kunnen blijven.

Gewenste vervolgactie: Bepaal de (extra) uitvoeringskosten voor gemeenten van (verschillende varianten voor) de verdere invulling van het toezicht, weeg de uitvoeringskosten ook mee bij de besluitvorming over de invulling van het toezicht en zorg voor een adequate financiële dekking van de eventuele extra uitvoeringskosten voor gemeenten.

Het toezicht moet in ieder geval bijdragen aan het beter kunnen realiseren van de inhoudelijke doelstellingen van het NIS2-richtlijn, niet ten koste gaan van het realiseren van deze inhoudelijke doelstellingen. Heel streng toezicht kan bijvoorbeeld opportuun zijn als partijen zich zonder dat toezicht niet aan de inhoudelijke verplichtingen houden. Voor het toezicht op de NIS2-richtlijn ligt risicogebaseerd toezicht voor de hand, waarbij toezichtinstrumenten pas actief worden ingezet op het moment dat de toezichthouder signalen krijgt dat de informatiebeveiliging niet op orde is.

In §16.2 van de Cyberbeveiligingswet zijn bepalingen opgenomen met betrekking tot de handhaving ten aanzien van essentiële entiteiten (met voor gemeenten relevante artikelen over controlefunctionaris, beveiligingsscan, gerichte beveiligingsaudit, ad hoc beveiligingsaudit, openbaarmaking overtreding, aanwijzing, last onder bestuursdwang en bestuurlijke boete). Het is niet goed mogelijk om de impact van deze instrumenten te duiden, de gewenste vervolgactie met betrekking tot de uitvoeringskosten blijft hierbij wel relevant.

3.4. Beschouwing

Uit dit hoofdstuk komt naar voren dat de lidstaten veel ruimte hebben bij de vertaling en verdere invulling van de NIS2-richtlijn naar nationale regelgeving én dat nog te maken keuzes kleine of grote gevolgen kunnen hebben voor de uitvoeringskosten bij gemeenten. Het is daarom van belang dat er bij de verdere uitwerking van de nationale regelgeving (wetten en lagere regelgeving) voldoende

aandacht is voor de uitvoeringsconsequenties bij de gemeenten. Hiervoor moet - conform de Code Interbestuurlijke Verhoudingen – een zorgvuldig UDO-proces worden doorlopen door de betrokken departementen en de VNG namens de gemeenten. De UDO staat voor Uitvoerbaarheidstoets Decentrale Overheden en is het proces waarmee vakdepartementen samen met het Ministerie van BZK en koepels van decentrale overheden (IPO, VNG en UvW) samen het beleid uitwerken dat invloed heeft op decentrale overheden.[82]

Randvoorwaarde: Het is vanwege de mogelijk substantiële uitvoeringsconsequenties van essentieel belang dat er bij de verdere vertaling en uitwerking van de NIS2-richtlijn (en andere EU-richtlijnen) naar nationale regelgeving een zorgvuldig UDO-proces wordt doorlopen en waarin de inzichten uit deze uitvoeringsanalyse worden meegenomen.

Het vraagstuk van de uitvoerbaarheid is voor dit onderwerp wellicht nog relevanter dan voor andere vraagstukken vanwege de verschillen tussen gemeenten en vanwege de financiële situatie van gemeenten. Bij de verdere invulling van de nationale regelgeving is het van belang dat de regelgeving uitvoerbaar is voor verschillende typen gemeenten. Zo moet de nationale regelgeving uitvoerbaar zijn voor grote gemeenten waar mogelijk een team van medewerkers betrokken is bij het beveiligen van netwerk- en informatiesystemen én voor kleine gemeenten die niet kunnen beschikken over zo'n team. Het is van belang om beide perspectieven nadrukkelijk mee te nemen bij de verdere uitwerking van de nationale regelgeving (en bij de ondersteuning vanuit bijvoorbeeld de IBD[83]).

Daarnaast is de financiële situatie van gemeenten een belangrijk aandachtspunt. Nederlandse gemeenten kampen met structurele financiële uitdagingen, de gemeentelijke financiën staan onder meer onder druk vanwege de tekorten in het sociaal domein.[84] Gemeenten zijn hierdoor genoodzaakt om te bezuinigen. Los van de huidige situatie koersen gemeenten af op een financieel ravijn in 2026.[85] Extra geld vrijmaken binnen de gemeentelijke begrotingen voor het beveiligen van netwerk- en informatiesystemen is daarmee niet vanzelfsprekend. Gemeenten moeten de komende jaren al veel pijnlijke keuzes maken.

Het is bij de verdere uitwerking en invulling van de nationale regelgeving daarom ook van belang om rekening te houden met twee scenario's:

1. De Rijksoverheid stelt wel (voldoende) financiële middelen beschikbaar voor gemeenten (in lijn met artikel 2 Financiële-verhoudingswet).
2. De Rijksoverheid stelt geen financiële middelen beschikbaar voor gemeenten.

De nationale ambities op het gebied van het beveiligen van netwerk- en informatiesystemen die in de regelgeving tot uitdrukking komen dienen in overeenstemming te zijn met de financiële middelen

---

82 Zie https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/beleidskompas/achtergrond-beleidskompas/verplichte-kwaliteitseisen/uitvoerbaarheidstoets-decentrale-overheden-en-normenkader-interbestuurlijke-verhoudingen voor meer informatie over het UDO-proces.

83 De IBD heeft bv. een aparte handreiking gemaakt van de BIO voor kleine gemeenten. Zie: https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2021/04/201907-Handreiking-BIO-voor-kleine-gemeenten-v1.01.docx.

84 Zie bijvoorbeeld BDO (2023), *BDO-Benchmark Nederlandse gemeenten 2022. Tekorten nemen af, uitdagingen groter. Incidentele voordelen maskeren structurele problematiek*.

85 Zie bijvoorbeeld https://vng.nl/nieuws/webinar-over-financieel-ravijn-gat-mogelijk-nog-dieper. Vanaf 2026 krijgen gemeenten € 3 miljard per jaar minder. In de voorjaarsnota van 2024 heeft het kabinet maatregelen genomen waardoor dit tekort per saldo met € 1 miljard per jaar wordt gedempt. Er blijft echter wel een structureel tekort over van € 2 miljard per jaar.

vanuit de Rijksoverheid, zodat gemeenten op ook een goede manier invulling kunnen geven aan de nationale ambities en wet- en regelgeving.

Randvoorwaarde: Zorg - in lijn met artikel 2 Financiële-verhoudingswet - voor een adequate financiële dekking vanuit de Rijksoverheid van de extra uitvoeringskosten bij gemeenten om te voldoen aan de nieuwe regelgeving voor het beveiligen van netwerk- en informatiesystemen.

4. Handelingsperspectief voor gemeenten

In dit hoofdstuk is een nadere uitwerking gemaakt van het handelingsperspectief voor gemeenten met betrekking tot het beveiligen van netwerk- en informatiesystemen. Wat kunnen gemeenten op de korte termijn alvast doen en wat moeten gemeenten op de iets langere termijn doen als de NIS2-richtlijn is omgezet in nationale regelgeving.

In dit hoofdstuk is eerst ingegaan op de concrete veranderingen voor gemeenten (voor zover dat op dit moment al te bepalen is) en daarna op wat gemeenten op dit moment al kunnen doen.

4.1. Wat verandert er nu concreet voor een gemeente?

Rollen, verantwoordelijkheden, taken en werkzaamheden

De IBD heeft een handreiking Functieprofielen Informatiebeveiliging[86] met een omschrijving van het takenpakket, de verantwoordelijkheden en bevoegdheden van de gemeentelijke informatiebeveiligingsfuncties. Het beschrijft functieprofielen voor de Chief Information Security Officer (CISO), de (Domein / Decentrale) Information Security Officer (D)ISO) en Technical Information Security Officer (TISO). Tevens vormt het een leidraad om de noodzakelijke taken, op niveau, toe te wijzen aan meerdere personen wanneer de gemeente een grotere informatiebeveiligingsorganisatie nodig heeft. Deze functieprofielen zijn een leidraad voor gemeenten of gemeentelijke organisaties. Zij kunnen deze profielen onder meer gebruiken in het wervingsproces en/of bij het intern vastleggen van taken, verantwoordelijkheden en bevoegdheden van de informatiebeveiligingsfuncties.

Aanvullend op de handreiking Functieprofielen Informatiebeveiliging is in de BIO beschreven waar de onderdelen van de BIO op verschillende plaatsen in de organisatie worden toegepast op grond van verschillende verantwoordelijkheden en gezagsverhoudingen. De BIO onderscheidt hier drie (hoofd)rollen: de secretaris/algemeen directeur, de proceseigenaar en de dienstenleverancier. Deze rollen zijn beschreven vanuit het perspectief van informatiebeveiliging. Er zijn uiteraard meer rollen betrokken bij informatiebeveiliging, zoals toezichthouder en medewerker, maar het gaat hier om de verantwoordelijke voor de uitvoering van de control op informatiebeveiliging. Ook in de handreiking information security management system (ISMS) worden de betrokken rollen beschreven.[87]

In de BIO staat aangegeven welke controls voor welke rol toepasselijk zijn. Omdat de overheid pluriform is georganiseerd, is deze toedeling indicatief. De BIO verplicht wel om de controls en overheidsmaatregelen die bij de rollen staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding. In het algemeen is de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden, terug te vinden in het informatie-beveiligingsbeleid van de organisatie.

Naast de beschikbare omschrijvingen van de rollen, verantwoordelijkheden, taken en werkzaamheden, heeft de IBD een heel pallet aan kennisproducten[88] die gemeenten kunnen helpen

[86] https://www.informatiebeveiligingsdienst.nl/product/handreiking-functieprofielen-informatiebeveiliging/.
[87] https://www.informatiebeveiligingsdienst.nl/product/isms-v1-0/.
[88] https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/.

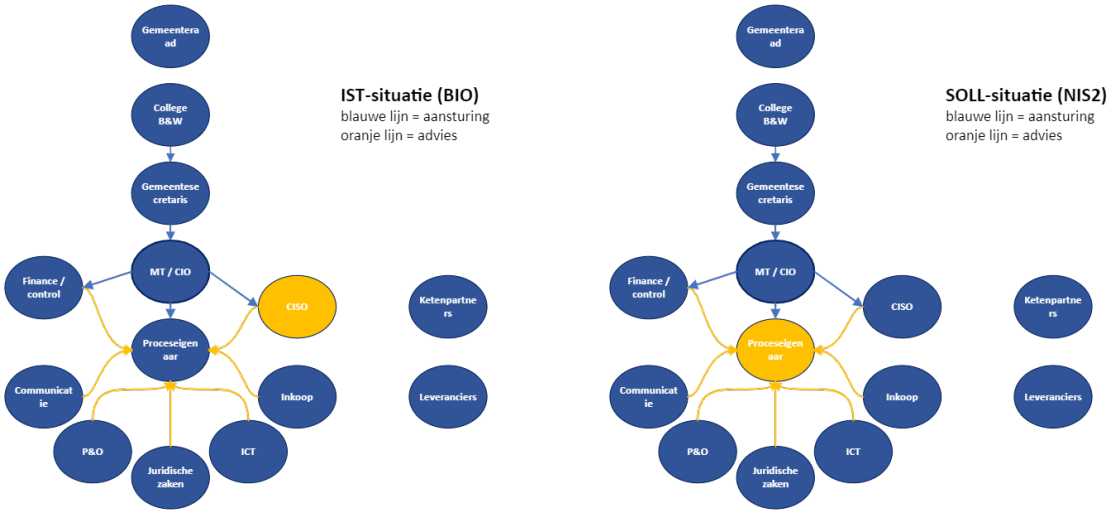
bij de implementatie van de BIO. Daarnaast is er een CISO-toolkit en zijn er handreikingen en factsheets voor bestuurders en lijnmanagers.

De bestaande beschikbare omschrijvingen van de rollen, verantwoordelijkheden, taken en werkzaamheden van de informatiebeveiligingsfunctie binnen de gemeenten en de kennisproducten van de IBD zijn met de komst van de NIS2-regelgeving nog steeds van toepassing. We zien wel dat dat informatiebeveiliging nu in de praktijk nog vaak als het onderwerp van de CISO wordt gezien, terwijl dit juist een vraagstuk zou moeten zijn van de proceseigenaar, waar bestuur en/of ambtelijke leiding meer op zou kunnen sturen. Daar gaat de volgende paragraaf over.

Beveiliging van netwerk- en informatiesystemen als organisatievraagstuk

De beveiliging van netwerk- en informatiesystemen is niet alleen het vraagstuk van CISO. Er zijn veel verschillende rollen binnen de gemeente die te maken hebben of gaan krijgen met het vraagstuk van de beveiliging van netwerk- en informatiesystemen. In de volgende figuur zijn verschillende rollen binnen de gemeente gepresenteerd inclusief de 'verschuiving' van het zwaartepunt.

Figuur 4.1 Beveiliging van netwerk- en informatiesystemen als organisatievraagstuk



Informatiebeveiliging wordt nu in de praktijk nog vaak als het onderwerp van de CISO[89] gezien, terwijl dit juist een vraagstuk zou moeten zijn van de proceseigenaar waarbij de CISO vanzelfsprekend de proceseigenaar kan adviseren en ondersteunen bij het daadwerkelijk vaststellen van de maatregelen voor de beveiliging van netwerk- en informatiesystemen.[90] Vergelijkbaar met de adviserende rol andere professionals binnen de gemeente op personele vraagstukken, juridische vraagstukken (inclusief privacy), inkoopvraagstukken, etc.

---

89 In de praktijk valt de CISO vaak onder de afdeling ICT, om het verschil tussen nieuwe en oude situatie goed duidelijk te maken is hier voor de CISO een aparte bol opgenomen. Er zijn ook nog andere rollen te onderscheiden zoals bv. informatiebeheer of archivering. Voor de eenvoud van de figuur zijn deze niet apart opgenomen in de figuur.

90 Dit plaatje toont de 'uitvoeringspraktijk' zoals die naar voren is gekomen uit de expertbijeenkomsten, niet hoe het met de BIO zou moeten zijn. Zo geeft de IBD in haar handreikingen over de BIO aan dat onder de proceseigenaar de lijnmanager wordt verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces of informatiesysteem.

Daarbij is het ook van belang dat er vanuit de (ambtelijke) leiding (college van B en W, gemeentesecretaris, MT/CIO) voldoende wordt gestuurd richting de proceseigenaren op het vraagstuk van de beveiliging van netwerk- en informatiesystemen. Dit kan mogelijk ook worden ingericht door de controlfunctie binnen de gemeenten hierin een rol te geven om te borgen dat proceseigenaren hier voldoende aandacht voor hebben.

In specifieke situaties of events kunnen verschillende rollen worden betrokken bij het vraagstuk. Bij bijvoorbeeld de inkoop van nieuwe applicaties betrekt de proceseigenaar de CISO, inkoop, ICT, financiën en juridische zaken om tot een goede aanbesteding te komen waarbij onder meer de beveiliging van netwerk- en informatiesystemen één van de relevante onderwerpen is.

Dit sluit aan bij het zogenoemde 3-lines-model waarbij het management (de eerste lijn) het meeste in staat om risico's te managen en in control te zijn. De internal audit, als derde lijn, dient erop toe te zien dat de beheersmaatregelen en in controls daadwerkelijk operationeel zijn. De tweede lijn heeft een belangrijke rol om de eerste lijn te faciliteren met deze verantwoordelijkheden en te controleren of dit ook daadwerkelijk gebeurt.

4.2. Wat kan een gemeente nu doen? Wat volgend jaar?

Het is voor gemeenten belangrijk om te weten wat zij nu alvast kunnen doen als no-regret maatregelen in verband met de nieuwe NIS2-regelgeving die op korte termijn omgezet gaat worden naar nationale regelgeving (Cyberbeveiligingswet en lagere regelgeving). Uit hoofdstuk 3 kwam naar voren dat de lidstaten nog veel ruimte hebben bij de omzetting van de NIS2-richtlijn naar nationale regelgeving en dat het op dit moment daarom nog niet goed mogelijk is om in detail aan te geven wat gemeenten dan moeten doen om in de toekomst te kunnen voldoen aan de nieuwe regelgeving.

Het Ministerie van BZK is voornemens om de Baseline Informatiebeveiliging Overheid (BIO) wettelijk te gaan verankeren en om in de reeds geplande modernisering van de BIO de eisen van de NIS2-richtlijn mee te nemen. Om beter voorbereid te zijn op de NIS2-richtlijn kan de gemeente alvast inzetten op het (nog) beter voldoen aan de BIO. Dan zet de gemeente in ieder geval een stap in de goede richting. Dit sluit ook aan bij de oproep van het Ministerie van BZK aan de koepels om prioriteit te maken van het toepassen van de huidige BIO.[91]

Verder is het aan te raden om nog enigszins terughoudend te zijn met verdere stappen ten aanzien van NIS2, omdat nog niet bekend is hoe de verdere vertaling en invulling van de NIS2-richtlijn naar nationale regelgeving eruit komt te zien én omdat verschillende informatieproducten van de IBD nog aangepast moeten gaan worden nadat er duidelijkheid is over de nieuwe invulling van de nationale regelgeving.

Gewenste vervolgactie: Zorg voor passende implementatieondersteuning voor grote én kleine gemeenten in de vorm van onder meer handreikingen en ander ondersteuningsmateriaal voor de vraagstukken waar gemeenten in de uitvoering mee te maken gaan krijgen voor alle relevante gemeentelijke rollen betrokken bij de beveiliging van netwerk- en informatiesystemen (CISO, lijnmanagers én management).

[91] Zie https://vng.nl/sites/default/files/2023-11/brief-nis2-bij-de-overheid.pdf waarin deze oproep is opgenomen.

5. Conclusies en aanbevelingen

In dit hoofdstuk zijn de conclusies en aanbevelingen opgenomen van de uitvoeringsanalyse. De aanbevelingen geven richting aan de gewenste vervolgacties voor een succesvolle en tijdige implementatie van de Europese wetgeving die gaat over netwerk- en informatiebeveiliging.

5.1. Beantwoording onderzoeksvragen

Wat wijzigt er in de werkwijze van de gemeente door de EU-regelgeving?

Gemeenten krijgen te maken met de volgende regelgeving in het kader van de beveiliging van netwerk en informatiesystemen:

- Beveiliging van netwerk- en informatiesystemen richtlijn 2 (NIS2);
- Cyberbeveiligingsverordening;
- Cyberweerbaarheidsverordening;
- Critical Entities Resilience richtlijn (CER).

Deze uitvoeringsanalyse beschouwt de NIS2 als overkoepelende cybersecurityregelgeving voor gemeenten, waar de Cyberbeveiligingsverordening en de Cyberweerbaarheidsverordening worden toegepast als het gaat om het gebruik van beveiligingscertificering. De CER-richtlijn richt zich op de bescherming van organisaties tegen *fysieke* dreigingen, zoals de gevolgen van (terroristische) misdrijven, sabotage en natuurrampen waar de NIS2-richtlijn richt zich op *digitale* (cyber) risico's voor netwerk- en informatiesystemen. Voor zowel de fysieke (CER) en digitale (NIS2) weerbaarheid komt er een plicht (tot nemen van beveiligingsmaatregelen) en een meldplicht (van incidenten). Deze plichten gaan gelden voor organisaties die een dienst verlenen die belangrijk, essentieel of kritiek is voor het functioneren van de maatschappij of economie. Onder de NIS2 vallen diverse kritieke sectoren waarbinnen lokale overheden wettelijke taken uitvoeren, zoals vervoer (spoor, water, en weg), gezondheidszorg, drinkwater, en afvalbeheer.

Het Ministerie van BZK heeft in het wetsvoorstel voor de Cyberbeveiligingswet gemeenten als essentiële entiteit aangewezen. Redenen hiervoor zijn dat de overheid zelf ook een maatschappelijke taak heeft om op een zorgvuldige manier om te gaan met gegevens van burgers en bedrijven en dat de overheid ook een voorbeeldfunctie heeft. Dit betekent dat de NIS2-richtlijn van toepassing is/wordt op gemeenten.

De wijzigingen door de NIS2 voor de werkwijze van gemeente komen door generieke verplichtingen, inhoudelijke- en informatieverplichtingen.

Generieke verplichtingen

Generieke verplichtingen uit de NIS2-richtlijn moeten ervoor zorgen dat het bestuursorgaan van de gemeente als essentiële entiteit maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeurt, toeziet op de uitvoering ervan en aansprakelijk kan worden gesteld voor inbreuken door entiteiten op artikel 21.

Daarnaast moeten leden van bestuursorganen van gemeenten een opleiding volgen en regelmatig een soortgelijke opleiding aan hun werknemers aanbieden zodat zij voldoende kennis en vaardigheden verwerven 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.

Inhoudelijke verplichtingen

Naast de generieke verplichtingen volgen er uit de NIS2-richtlijn ook inhoudelijke verplichtingen. De inhoudelijke verplichtingen richten zich op maatregelen voor het beheer van risico's voor het beveiligen van netwerk- en informatiesystemen.

Informatieverplichtingen

Gemeenten moeten significante incidenten melden bij hun CSIRT en moeten de ontvangers van hun diensten die mogelijke worden getroffen door een significante cyberdreiging mededelen welke maatregelen ze kunnen nemen in reactie op die dreiging.

Toezichts- en handhavingsmaatregelen

In de NIS2-richtlijn is een uitgebreid overzicht opgenomen van de bevoegdheden die de bevoegde autoriteiten ten minste moeten hebben. Een belangrijk aandachtspunt hierbij is dat het hebben van een bevoegdheid iets anders is dan het toepassen of gebruiken van diezelfde bevoegdheid. De lidstaten (en dus ook de Rijksoverheid) hebben (veel) ruimte om te bepalen in welke gevallen (of events) bevoegdheden kunnen worden toegepast en met welke frequentie (hoe vaak). Daarbij is er bijvoorbeeld ook ruimte voor risicogebaseerd toezicht.

Wat betekenen deze veranderingen voor de gemeentelijke organisatie wanneer deze in samenhang worden beschouwd?

De lidstaten hebben veel ruimte bij de vertaling en verdere invulling van de NIS2-richtlijn naar nationale regelgeving. De nog te maken keuzes kunnen kleine of grote gevolgen hebben voor de uitvoeringsconsequenties bij gemeenten. Het is daarom van belang dat er bij de verdere uitwerking van de nationale regelgeving voldoende aandacht is voor de uitvoeringsconsequenties bij de gemeenten. Hiervoor moet - conform de Code Interbestuurlijke Verhoudingen - een zorgvuldig UDO-proces worden doorlopen door de betrokken departementen en de VNG namens de gemeenten. De UDO staat voor Uitvoerbaarheidstoets Decentrale Overheden en is het proces waarmee vakdepartementen samen met het Ministerie van BZK en koepels van decentrale overheden (IPO, VNG en UvW) samen het beleid uitwerken dat invloed heeft op decentrale overheden. In deze uitvoeringsanalyse is een uitwerking gemaakt van de mogelijke betekenis van verschillende begrippen en de mogelijke uitvoeringsconsequenties daarvan. In het navolgende zijn deze kort besproken.

In artikel 1:1 Algemene wet bestuursrecht en artikel 6 Gemeentewet is meer informatie te vinden over de inhoud van het begrip ***bestuursorgaan***. Het is op dit moment nog niet duidelijk wat de NIS2-richtlijn betekent voor de onder artikel 6 punt 35 van de richtlijn vallende verschillende typen samenwerkingsverbanden waarbinnen gemeenten acteren.

Er zijn verschillende vrijheidsgraden bij de verdere invulling van het begrip ***aansprakelijkheid***. In het wetsvoorstel voor de Cyberbeveiligingswet zijn geen aparte bepalingen opgenomen met betrekking tot de aansprakelijkheid van bestuurders; het wetsvoorstel sluit daarbij aan bij de invulling zoals geschetst in de minimale variant. Dit sluit ook aan bij de bestaande Nederlandse regelgeving op het gebied van aansprakelijkheid van bestuursorganen. Het is nog wel van belang om ondubbelzinnig aan

te geven of bestuurders van gemeenten wel of niet aansprakelijk gesteld kunnen worden op grond van de NIS2-richtlijn.

Er zijn verschillende beelden of de NIS2-richtlijn wel of niet voorschrijft dat er een aparte uitwerking moet worden gemaakt van de ***verantwoordelijkheden*** binnen bestuursorganen. Gemeenten dienen (als bestuursorgaan) te voldoen aan veel verschillende verplichtingen en hebben zelf (fijnmazig) geregeld wie wat doet en wie waarvoor verantwoordelijk is. In de BIO versie 1 is opgenomen welke functionarissen verantwoordelijk zijn voor de uitvoering van een control: secretaris/algemeen directeur, proceseigenaar en/of (interne of externe) dienstenleverancier. De BIO kent echter geen wettelijke basis, maar is gebaseerd op een zelfverplichting. Bij de wettelijke vastlegging van de BIO krijgt de term 'verantwoordelijkheid' mogelijk ook een andere juridische lading.

In artikel 26 lid 8 van de Cyberbeveiligingswet is opgenomen dat bij onder meer gemeenten als 'leden van het bestuur' worden aangemerkt 'leden van de ambtelijke leiding' voor zover het gaat om de ***verplichtingen met betrekking tot kennis en vaardigheden*** (artikel 26 lid 2 t/m lid 6). In de MvT van de Cyberbeveiligingswet is aangegeven dat *in ieder geval* de secretaris (gemeentesecretaris) deel uitmaakt van de ambtelijke leiding. Het is daarbij (nog) niet duidelijk wie verder onder de ambtelijke leiding van een gemeente moet worden verstaan (directie, managementteam?). De verplichting inzake kennis en vaardigheden zou dan niet van toepassing zijn voor het college van B en W en voor gemeenteraadsleden. Deze invulling van de NIS2-richtlijn is niet meegenomen in de expertbijeenkomsten voor deze uitvoeringsanalyse (deze vonden plaats voor publicatie van het wetsvoorstel), vandaar dat het niet goed mogelijk is om de belangrijkste uitvoeringsconsequenties hiervan goed te kunnen duiden (hiervoor is een aparte aanbeveling opgenomen).

Uit deze uitvoeringsanalyse blijkt dat er nog veel onduidelijkheid is over de exacte reikwijdte en betekenis van verschillende termen. Het is van belang voor een goede uitvoering dat hier geen onduidelijkheid over is bij gemeenten. Vandaar de gewenste vervolgactie dat de uitwerking van termen als bestuursorganen, leden van bestuursorganen, aansprakelijkheid, verantwoordelijkheid en doelgroep van de opleidingen in relatie tot de NIS2-richtlijn ondubbelzinnig zijn en worden uitgewerkt in de Cyberbeveiligingswet.

In de huidige situatie hebben gemeenten de Baseline Informatiebeveiliging Overheid (BIO) om de beveiliging van netwerk en informatiesystemen te beheren zoals de NIS2 beoogd. Dit is beschreven in hoofdstuk 2 van deze rapportage. De BIO is geen wettelijke verplichting, maar is een vorm van zelfregulering. De AVG is een wettelijke verplichting die gaat over het beschermen van persoonsgegevens en het treffen van maatregelen op de verwerkingen van persoonsgegevens. Zowel de NIS2-verplichtingen als de AVG richten zich op het adresseren van risico's en het nemen van passende maatregelen. Er zijn ook verschillen. De NIS2-richtlijn richt zich op het grotere geheel van digitale veiligheid met een focus op continuïteit van belangrijke en essentiële processen, terwijl de AVG focust op de bescherming van individuele rechten. Het Ministerie van BZK is voornemens om de Baseline Informatiebeveiliging Overheid (BIO) wettelijk te gaan verankeren en om in de reeds geplande modernisering van de BIO de eisen van de NIS2-richtlijn mee te nemen. Dit moet gebeuren in lagere regelgeving (AMvB)Om beter voorbereid te zijn op de NIS2-richtlijn kan de gemeente alvast inzetten op het (nog) beter voldoen aan de BIO. Dan zet de gemeente in ieder geval een stap in de goede richting. Dit sluit ook aan bij de oproep van het Ministerie van BZK aan de koepels om prioriteit te geven aan het toepassen van de huidige BIO.

Voor gemeenten geldt dat er per informatiebeveiligingsincident vaker dan nu moet worden gerapporteerd over informatiebeveiligingsincidenten (***meldingsplicht***). De verzwaring van het aantal meldingen hangt af van de precieze definitie van significante incidenten.

Het ***toezicht en handhaven*** moet in ieder geval bijdragen aan het beter kunnen realiseren van de inhoudelijke doelstellingen van de NIS2-richtlijn en niet ten koste gaan van het realiseren van deze inhoudelijke doelstellingen. Heel streng toezicht kan bijvoorbeeld opportuun zijn als partijen zich zonder dat toezicht niet aan de inhoudelijke verplichtingen houden. In de opsomming in lid 2 van artikel 32 NIS2-richtlijn is een uitgebreid overzicht opgenomen van de bevoegdheden die de bevoegde autoriteiten ten minste moeten hebben. Een belangrijk aandachtspunt hierbij is dat het hebben van een bevoegdheid iets anders is dan het toepassen of gebruiken van diezelfde bevoegdheid. Over het toepassen of gebruiken van bevoegdheden door de toezichthouder is er op dit moment nog geen duidelijkheid. Voor het toezicht op de NIS2-richtlijn ligt risicogebaseerd toezicht voor de hand, waarbij toezichtinstrumenten pas actief worden ingezet op het moment dat de toezichthouder signalen krijgt dat de informatiebeveiliging niet op orde is. Het is niet goed mogelijk om de impact van deze instrumenten nu te duiden (hiervoor is een aparte aanbeveling opgenomen).

Beveiliging van netwerk- en informatiesystemen als organisatievraagstuk

De beveiliging van netwerk- en informatiesystemen is niet alleen het vraagstuk van de CISO. Er zijn veel verschillende rollen binnen de gemeente die te maken hebben of gaan krijgen met het vraagstuk van de beveiliging van netwerk- en informatiesystemen.

Informatiebeveiliging wordt nu in de praktijk nog vaak als het onderwerp van de CISO gezien, terwijl dit juist een vraagstuk zou moeten zijn van de proceseigenaar. Waarbij de CISO vanzelfsprekend de proceseigenaar kan adviseren en ondersteunen bij het daadwerkelijk vaststellen van de maatregelen voor de beveiliging van netwerk- en informatiesystemen. Vergelijkbaar met de adviserende rol van andere professionals binnen de gemeente op personele vraagstukken, juridische vraagstukken (inclusief privacy), inkoopvraagstukken, etc.

Daarbij is het ook van belang dat er vanuit de (ambtelijke) leiding (college van B en W, gemeentesecretaris, MT/CIO) voldoende wordt gestuurd richting de proceseigenaren op het vraagstuk van de beveiliging van netwerk- en informatiesystemen. Dit kan mogelijk ook worden ingericht door de controlfunctie binnen de gemeenten hierin een rol te geven om te borgen dat proceseigenaren hier voldoende aandacht voor hebben.

Dit sluit aan bij het zogenoemde 3-lines-model waarbij het management (de eerste lijn) het meeste in staat om risico's te managen en in control te zijn. De internal audit, als derde lijn, dient erop toe te zien dat de beheersmaatregelen en in controls daadwerkelijk operationeel zijn. De tweede lijn heeft een belangrijke rol om de eerste lijn te faciliteren met deze verantwoordelijkheden en te controleren of dit ook daadwerkelijk gebeurt.

Continu organisatorisch breed risicobeheer

Voor de meeste gemeenten geldt dat het systematische beheren (PDCA-cyclus) van informatiebeveiligingsrisico's en meten van effectiviteit van maatregelen (ISMS) meer centraal gezet zou moeten worden geplaatst in de organisatie. Het gaat om een continu verbeterproces waarin de actualiteit en volledigheid van beveiligingsmaatregelen regelmatig moet worden vergeleken met actuele dreigingen. Dit is een grote inspanning als dit voor een gemeente nog geen gemeengoed is.

Bovendien moet dit ingepast worden in de rest van het gemeentelijk risicomanagement (ook wel kwaliteitsmanagementsysteem of controlesysteem). Dit zal een meerjarig organisatieontwikkelingstraject vergen met aandacht voor de uitvoerbaarheid voor grote én kleine gemeente zonder geld en middelen. Het is randvoorwaardelijk dat hier financiële middelen voor beschikbaar komen.

Is de gemeente voldoende toegerust voor een doeltreffende uitvoering?

Gemeenten zijn niet voldoende toegerust voor een doeltreffende uitvoering van de nieuwe regelgeving vanwege onvoldoende mensen (vanwege krapte op de arbeidsmarkt) en onvoldoende financiële middelen (die voor het komende jaar al niet meer te organiseren zijn én vanwege het financiële ravijn in 2026). Vandaar de randvoorwaarde dat er voldoende financiële middelen moeten zijn voor implementatie en uitvoering van de beveiliging van netwerk- en informatiesystemen bij gemeenten.

Bij de verdere invulling van de nationale regelgeving is het van belang dat de regelgeving uitvoerbaar is voor verschillende typen gemeenten. Zo moet de nationale regelgeving uitvoerbaar zijn voor grote gemeenten waar mogelijk een team van medewerkers betrokken is bij het beveiligen van netwerk- en informatiesystemen én voor kleine gemeenten die niet kunnen beschikken over zo'n team. Het is van belang om beide perspectieven nadrukkelijk mee te nemen bij de verdere uitwerking van de nationale regelgeving (en bij de ondersteuning vanuit bijvoorbeeld de IBD).

Welke kosten en besparingen voor de gemeentelijke uitvoering zijn aan deze wijziging verbonden?

Een goede inschatting van de kosten en besparingen voor de gemeentelijke uitvoering is op dit moment nog niet te maken. De vertaling van de NIS2-richtlijn in het conceptwetsvoorstel Cyberbeveiliging ligt sinds eind mei ter consultatie. Dit conceptwetsvoorstel is een kaderwetgeving. In onderliggende regelgeving, die nog niet beschikbaar is, zal het Ministerie van BZK verder invulling geven aan verplichtingen voor het beveiligen van netwerk- en informatiesystemen voor gemeente. Belangrijke mogelijke kostencomponenten zijn de implementatie van de informatiebeveiliging in de organisatie, het uitvoeren van risicoanalyses, het nemen van risicomaatregelen, opleidingen en het rapporteren / verantwoorden over informatiebeveiliging.

We zien hierbij dat gemeenten voor een tweeledige taak staan: enerzijds de netwerk- en informatiebeveiliging verder op orde brengen en anderzijds systematisch, organisatiebreed uitvoering geven aan het verplichte risicobeheer en treffen van maatregelen om de netwerk- en informatiebeveiliging in een continue proces te verbeteren. De structurele betrokkenheid van eigenaren van primaire processen binnen een gemeente (en samenwerkingsverbanden) en opdrachtgever(s) bij (de besturing van) de uitvoering van informatiebeveiliging zullen hieraan moet bijdragen. Dit vergt een investering in kennis van het belang van en vaardigheden in het beveiligen van netwerk- en informatiesystemen op alle niveaus. Dit legt een druk op de gemeentelijke middelen.

Voor het verplicht beveiligen van de netwerk- en informatiesystemen en het vergroten van de digitale weerbaarheid van de gemeentelijke organisaties en het implementeren van de aankomende wet- en regelgeving is het randvoorwaardelijk dat de benodigde middelen voor gemeenten beschikbaar zijn.

Incidenten kunnen tot hoge gemeentelijke kosten leiden. De hoogte van de kosten per voorkomen incident (en daarmee besparingen) zijn echter niet goed te bepalen.

Wat zijn de verwachte effecten van de EU-regelgeving voor gemeenten?

Een belangrijk beoogd effect van de EU-regelgeving is een stijging van de bewustwording van risico's op het gebied van netwerk- en informatiesystemen bij gemeenten en bij bestuurders en medewerkers van gemeenten. Gemeenten zijn naar verwachting beter in staat is om risico's te beheersen en hierop in control te zijn. Dit helpt om de continuïteit en betrouwbaarheid van hun dienstverlening en informatievoorziening te borgen.

Hoe kan deze EU-regelgeving in samenhang worden geïmplementeerd (uitgevoerd) en wat zijn de randvoorwaarden en risico's?

Als eerste zijn er twee randvoorwaarden gedefinieerd die ingevuld moeten worden zodat gemeenten met succes kunnen voldoen aan de nieuwe regelgeving:

Randvoorwaarde: Het is vanwege de mogelijk substantiële uitvoeringsconsequenties van essentieel belang dat er bij de verdere vertaling en uitwerking van de NIS2-richtlijn (en andere EU-richtlijnen) naar nationale regelgeving een zorgvuldig UDO-proces wordt doorlopen, waarin de inzichten uit deze uitvoeringsanalyse worden meegenomen.

Randvoorwaarde: Zorg - in lijn met artikel 2 Financiële-verhoudingswet - voor een adequate financiële dekking vanuit de Rijksoverheid van de extra uitvoeringskosten bij gemeenten om te voldoen aan de nieuwe regelgeving voor het beveiligen van netwerk- en informatiesystemen.

Het Ministerie van BZK is voornemens om de Baseline Informatiebeveiliging Overheid (BIO) wettelijk te gaan verankeren en om in de reeds geplande modernisering van de BIO de eisen van de NIS2-richtlijn mee te nemen. Om beter voorbereid te zijn op de NIS2-richtlijn kan de gemeente alvast inzetten op het (nog) beter voldoen aan de BIO. Dan zet de gemeente in ieder geval een stap in de goede richting. Dit sluit ook aan bij de oproep van het Ministerie van BZK aan de koepels om prioriteit te maken van het toepassen van de huidige BIO.

Verder is het aan te raden om nog enigszins terughoudend te zijn met verdere stappen ten aanzien van NIS2, omdat nog niet bekend is hoe de verdere vertaling en invulling van de NIS2-richtlijn naar nationale regelgeving eruit komt te zien én omdat verschillende informatieproducten van de IBD nog aangepast moeten gaan worden nadat er duidelijkheid is over de nieuwe invulling van de nationale regelgeving.

Een veelgenoemd risico is een te zware invulling van het (externe) toezicht en de handhaving. Daarbij is veelvuldig opgemerkt dat - vanwege beperkte gemeentelijke capaciteit - de tijd die besteed moet worden aan het rapporteren aan de toezichthouder ten koste gaat van de tijd om te voldoen aan de inhoudelijke verplichtingen zelf. En dat dit ook tot inhoudelijke verschuivingen kan leiden (vooral voldoen aan eisen van toezichthouder in plaats van weerbaar zijn tegen dreigingen van buitenaf).
Een ander uitvoeringsrisico is de mogelijke stapeling van toezicht door verschillende toezichthouders (bijvoorbeeld omdat gemeenten zowel moeten voldoen aan de NIS2 als de AVG en omdat er mogelijk meer toezichthouders bijkomen voor toezicht op kritieke sectoren die onder de NIS2 vallen en waarvoor gemeenten taken uitvoeren (zoals vervoer, drinkwater, afvalbeheer en gezondheidszorg)).

5.2. Aanbevelingen

In deze paragraaf zijn de aanbevelingen uit het rapport in samenhang gepresenteerd. Het is een overzicht van de gewenste vervolgacties die nodig zijn voor een succesvolle implementatie van de Europese wetgeving die gaat over de beveiliging van netwerk- en informatiesystemen. Daarbij zijn de volgende gewenste vervolgacties geïdentificeerd:

Gewenste vervolgactie: Bepaal de (extra) uitvoeringskosten voor gemeenten van (verschillende varianten voor) de verdere invulling van het toezicht, weeg de uitvoeringskosten ook mee bij de besluitvorming over de invulling van het toezicht en zorg voor een adequate financiële dekking van de eventuele extra uitvoeringskosten voor gemeenten.

Gewenste vervolgactie: Het is van belang dat de uitwerking van termen als bestuursorganen, leden van bestuursorganen, aansprakelijkheid, verantwoordelijkheid en doelgroep van de opleidingen in relatie tot de NIS2-richtlijn ondubbelzinnig zijn en worden uitgewerkt in de Cyberbeveiligingswet.

Gewenste vervolgactie: Er is een meerjarig organisatieontwikkelingstraject nodig om de regelgeving bij gemeenten te implementeren. Zorg voor een realistische termijn waarbij gemeenten de tijd krijgen om aan de gestelde eisen van de wetgeving te kunnen voldoen (bijvoorbeeld door opschorting van de Nederlandse handhaving op dit punt gedurende die overgangsperiode).

Gewenste vervolgactie: Zorg voor passende implementatieondersteuning voor grote én kleine gemeenten in de vorm van onder meer handreikingen en ander ondersteuningsmateriaal voor de vraagstukken waar gemeenten in de uitvoering mee te maken gaan krijgen voor alle relevante gemeentelijke rollen betrokken bij de beveiliging van netwerk- en informatiesystemen (CISO, lijnmanagers én management).

Gewenste vervolgactie: Werk uit wat de NIS2-richtlijn betekent voor de verschillende type samenwerkingsverbanden waarbinnen gemeenten opereren.

Gewenste vervolgactie: Onderzoek de opleidingsbehoeften van de verschillende groepen bestuurders bij gemeenten alvorens een concrete verplichting voor het volgen van opleidingen vast te leggen in de Nederlandse regelgeving.

Bijlage A: Expertgroepen, begeleidingscommissie en overige betrokkenen

Expertgroep juridisch

Naam	Functie	Gemeente
K. Wilbrink	Jurist	VNG
C. Dohmen-Spruit	Senior jurist privacy	Zoetermeer
U. Faber	Juridisch adviseur	Eemsdelta
E. Rooke	Adviseur bestuurlijke zaken voor de Woo	Utrecht
J. Vogel	Senior juridisch adviseur	IJsselstein
E. van Meerkerk	Strategisch juridisch adviseur	Alkmaar
T. Kuijt	Jurist	Leiden
M. Vergragt	Juridisch adviseur	Woerden
T. Asbreuk	Juridisch adviseur	Oldenzaal
B. Grosheide	Strategisch juridisch adviseur	Dijk en Waard
J. Ruwen-Stuursma	Privacy Officer	Meerinzicht
W. Koning	CISO	Eemsdelta
C. Drenth	Functionaris voor gegevensbescherming	Eemsdelta

Expertgroep informatisering en automatisering

Naam	Functie	Gemeente
J. Hintzbergen	Adviseur informatiebeveiliging	VNG
M. Vehmeijer	Projectleider digitalisering en bedrijfsvoering	De Ronde Venen
E. Zijlstra	CISO	Nijmegen
N. Noorland	Strategisch adviseur Informatieveiligheid	Rotterdam
M. Rutten	CIO	‘s-Hertogenbosch
T. Quist	CISO	Dijk en Waard
F. Hut	CISO	Haarlem
J. Koortens	CISO	Medemblik
A. Potters	Enterprise Architect	Tilburg
E. Zomer	Enterprise architect	Zwolle
C. Meijerink	CISO	Apeldoorn
A. Bijvoet	CISO	Assen
S. Paulusma	Adviseur Informatiebeveiliging	Zoetermeer
B. Woudenberg	CIO/programmaleider digitale organisatie	Wageningen
C. Nellen	Adviseur informatiemanagement & beleid	Helmond
R. van der Heide	CISO	Enschede
V. Verhagen	CISO	Barneveld
J. van der Sluis	CISO/ teamleider Informatieveiligheid	BAR

A. Dekker	Technisch Specialist Informatie Veiligheid	Emmen
L. Bloemendaal	CISO	Nieuwkoop
M. van Vliet	CISO	Utrecht
D. Kluijtmans	CISO	Nedeweert
J. D. Waasdorp	CISO	Maasdriel/Zaltbommel
P. Zuiderwijk	CISO	De Ronde Venen

Expertgroep publieksdienstverlening

Naam	**Functie**	**Gemeente**
W. van den Eeckhout	Strategisch informatieadviseur Dienstverlening	Nijmegen
F. Willemsen	Adviseur Dienstverlening	Amsterdam
M. Koenders	Beleidsadviseur Dienstverlening	Midden-Groningen
M. Robins	Senior informatie adviseur	Land van Cuijk
D. Heuts	Adviseur Informatiemanagement	Sittard-Geleen
E. Kasdorp	Projectleider online dienstverlening	Midden-Groningen
M. de Bruijn	Informatiemanager Digitale Dienst/Communicatie	Zoetermeer
M. de Bijl	Adviseur innovatie	Dimpact
M. van Mierlo	Strategisch adviseur dienstverlening	Amsterdam
F. Veenstra	Projectleider Dienstverlening	Nijmegen
M. de Boer	Strategisch adviseur Dienstverlening	Dijk en Waard

Expertgroep financieel

Naam	**Functie**	**Gemeente**
W. Caelers	Financieel adviseur	Nederweert
R. Hunting	Concerncontroller	Nieuwegein
A. Dokter	Teamleider financiën	Montfoort
R. Bakema	Concerncontroller / secretaris FAMO	Westland
K. Vingerhoets	Controller	Oirschot
F. van Manen	Functionaris Gegevensbescherming	Pijnacker-Nootdorp
A. van den Berge	Concerncontroller	Goes

Begeleidingscommissie

Naam	Functie	Organisatie
Richard de Klerk	CISO	Gemeente Amersfoort
Martijn Groenewegen	CIO	Gemeente Eindhoven
Hetty Lucassen	MT-lid Digitale Overheid	Ministerie van BZK
Ingrid Zondervan	Afdelingshoofd Strategie, Internationaal en Communicatie	Ministerie van BZK
Dirk van Brederode	Teamleider Digitale Samenleving	VNG
Koen Wortmann	MT-lid	VNG Realisatie

Overige betrokkenen

Naam	Functie	Organisatie
Jule Hintzbergen	Adviseur	IBD
Remco Groet	Strategisch adviseur	IBD
Kees Hintzbergen	Adviseur (CSIRT)	IBD
Kenneth Sleijpen	Strategisch adviseur	IBD
Jonas Onland	Programmamanager Digitale transformatie en Europa	VNG
Kato Vierbergen	Programmamanager Agenda Digitale Veiligheid	VNG
Nikki Nguyen	Senior Beleidsadviseur	VNG
Walter van Holst	Jurist	VNG Realisatie
Sophie van Velzen	Beleidsmedewerker Digitale Overheid	VNG Realisatie
Yvonne Brink	Themacoördinator Digital Decade	VNG Realisatie
Maurice van Erven	Business Analist	VNG Realisatie

Bijlage B Uitgebreide beschrijving Europese wetgeving netwerk- en informatiebeveiliging

Beveiliging van Network en Informatie Systemen richtlijn 2 (NIS 2)

Wanneer?

De NIS2-richtlijn is in januari 2023 in werking getreden en moet vóór 17 oktober 2024 door alle EU-lidstaten in nationale wetgeving zijn omgezet.

Wie?

De wet introduceert de begrippen essentiële entiteiten en belangrijke entiteiten. De lidstaten stellen uiterlijk op 17 april 2025 een lijst van deze entiteiten op. Het gaat om entiteiten die vallen binnen de volgende sectoren:

1. Essentiële entiteiten (categorie 1): energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, beheer van ICT-diensten (business-to-business), overheid en ruimtevaart.
2. Belangrijke entiteiten (categorie 2): post- en koeriersdiensten; afvalstoffenbeheer, vervaardiging, productie en distributie van chemische stoffen, productie, verwerking en distributie van levensmiddelen, vervaardiging, digitale aanbieders en onderzoek.

Het is belangrijk om te benadrukken dat de wetgeving de overheidssector aanwijst als een "essentiële entiteit". Concreet geeft het aan dat:

1. Deze wet is van toepassing op " **een overheidsinstantie op regionaal niveau**, zoals gedefinieerd door een lidstaat in overeenstemming met het nationale recht, die, na een op risico's gebaseerde beoordeling, diensten verleent waarvan de verstoring een aanzienlijke impact kan hebben op kritieke maatschappelijke of economische activiteiten".
2. En dat de lidstaten kunnen bepalen dat deze richtlijn van toepassing is op **overheidsinstanties op lokaal niveau**. Dit zal afhangen van de nationale keuzes die elke lidstaat maakt bij de omzetting van de richtlijn in zijn nationale wetgeving.

Wat?

De richtlijn voorziet in maatregelen die erop gericht zijn een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie te bereiken, teneinde de werking van de interne markt te verbeteren.

Met het oog hierop voorziet deze richtlijn in:

1. Verplichtingen die de lidstaten voorschrijven dat zij nationale cyberbeveiligingsstrategieën vaststellen, en bevoegde autoriteiten, cybercrisisbeheerautoriteiten, centrale contactpunten op het gebied van cyberbeveiliging (centrale contactpunten) en computer security incident response teams (CSIRT's) aanwijzen of instellen;
2. Risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging voor entiteiten van het type waarnaar in bijlage I of II wordt verwezen alsmede voor entiteiten die uit hoofde van Richtlijn (EU) 2022/2557 als kritieke entiteiten worden aangemerkt;
3. Regels en verplichtingen met betrekking tot het delen van cyberbeveiligingsinformatie;
4. Toezichts- en handhavingsverplichtingen voor de lidstaten.

NIS2 bevat vereisten, waaronder een bredere reeks verplichte maatregelen voor het beheer van cyberbeveiligingsrisico's (artikel 21) en nieuwe vereisten voor het melden van incidenten (artikel 23). De vrijwillige melding vanuit de voorgaande NIS van incidenten is nog steeds van kracht.

Om aan te tonen dat aan de vereisten van artikel 21 is voldaan, kunnen de lidstaten van essentiële en belangrijke entiteiten verlangen dat zij gebruikmaken van ICT-producten, -diensten en -processen die door de essentiële of belangrijke entiteit zijn ontwikkeld of van derden zijn aangekocht en die zijn gecertificeerd in het kader van Europese cyberbeveiligingscertificeringsregelingen overeenkomstig de Cyberbeveiligingsverordening.

Cyberbeveiligingsverordening

Wanneer?

De Europese cyberbeveiligingsverordening is op 27 juni 2019 in werking getreden.

Wat?

Deze verordening voert een EU-breed cyberbeveiligingscertificeringskader in voor de vaststelling van Europese cyberbeveiligingscertificeringsregelingen om een adequaat niveau van cyberbeveiliging van ICT-producten, -diensten en -processen in de Unie te waarborgen.

Op 18 april 2023 heeft de Commissie een gerichte wijziging van deze verordening voorgesteld, die tot doel heeft de vaststelling van Europese regelingen voor cyberbeveiligingscertificering voor "beheerde beveiligingsdiensten" mogelijk te maken.

Er zijn enkele nationale regelingen voor cyberbeveiliging, maar er is geen gemeenschappelijk kader voor de lidstaten. De nieuwe Europese cyberbeveiligingscertificeringsregelingen zullen in de plaats komen van de nationale regelingen voor cyberbeveiligingscertificering, wanneer er sprake is van overlapping in hun toepassingsgebied. Elke lidstaat moet voor de toepassing van de wet een nationale cyberbeveiligingscertificeringsautoriteit aanwijzen. In Nederland is de Rijksinspectie Digitale Infrastructuur (RDI) verantwoordelijk.

In elk Europees systeem moet met name het volgende worden gespecificeerd:
1. De categorieën producten en diensten die onder de richtlijn vallen;
2. De cyberbeveiligingsvereisten, zoals normen of technische specificaties;
3. Het type evaluatie, zoals zelfevaluatie of een derde partij;
4. Het beoogde betrouwbaarheidsniveau.

De cyberbeveiligingscertificering is vrijwillig, tenzij dit verplicht wordt gesteld op grond van het toepasselijke Unierecht. Ze zullen een manier zijn om aan te tonen dat wordt voldaan aan de vereisten die zijn vastgesteld in de NIS 2-richtlijn, de eIDAS-verordening (portemonnee voor digitale identiteit), de Cyberweerbaarheidsverordening en de AI-verordening.

Er zijn momenteel drie cyberbeveiligingsregelingen in ontwikkeling: de Europese cyberbeveiligingscertificeringsregeling op basis van gemeenschappelijke criteria, de Europese certificeringsregeling voor clouddiensten en de Europese cyberbeveiligingscertificeringsregeling voor 5G.

Bovendien kent de wetgeving Enisa, het EU-agentschap voor cyberbeveiliging, nieuwe mandaten toe met betrekking tot het opzetten en onderhouden van het Europees cyberbeveiligingskader, bijstand aan de lidstaten bij de ontwikkeling van hun nationale strategieën of het aanbieden van cyberbeveiligingsopleidingen. Enisa moet ervoor zorgen dat deze certificeringsregelingen een belangrijke rol spelen in de verschillende cyberbeveiligingswetgeving.

Wie?

Organisaties, fabrikanten of leveranciers die betrokken zijn bij het ontwerp en de ontwikkeling van ICT-producten, -diensten of -processen moeten gaan profiteren van de daaruit voortvloeiende certificaten, aangezien dit het voor hen gemakkelijker zal maken om over de grenzen heen handel te drijven en voor kopers om de veiligheidskenmerken van het product of de dienst te begrijpen.

De cyberbeveiligingsverordening voorziet in een EU-brede certificeringsregeling voor cyberbeveiliging. Eenmaal goedgekeurd, moeten of kunnen Nederlandse gemeenten aan die certificeringen voldoen en van hun aanbieders eisen dat zij zich daaraan houden. De verplichting is afhankelijk van of dit geëist gaat worden door de EU. Het zal aantonen dat wordt voldaan aan de verschillende cyberbeveiligingsvereisten die zijn opgenomen in de NIS 2-richtlijn, eIDAS, de AI-verordening en de Cyberweerbaarheidsverordening.

Cyberweerbaarheidsverordening

Wanneer?

Het voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen (Cyberweerbaarheidsverordening) is op 15 september 2022 door de Commissie gepresenteerd.

Wat?

Het voorstel stelt horizontale cyberbeveiligingsvereisten vast voor alle producten met digitale elementen (bv. VPN's, identiteits- en toegangsbeheersystemen, antivirusprogramma's, wachtwoordbeheerders) die op de interne markt worden geplaatst of beschikbaar worden gesteld.

Terwijl dit voorstel betrekking heeft op producten met digitale elementen die in de handel worden gebracht, heeft NIS 2 tot doel een hoog niveau van cyberbeveiliging te waarborgen voor diensten die door essentiële en belangrijke entiteiten worden geleverd (passende en evenredige technische, operationele en organisatorische cyberbeveiligingsmaatregelen).

Het voorstel heeft betrekking op een breed scala aan apparaten: alle producten die direct of indirect zijn verbonden met een ander apparaat of netwerk, met inbegrip van hardware, software en ondersteunende diensten.

De toekomstige wet heeft tot doel te zorgen voor een betere bescherming van consumenten door de verantwoordelijkheid van fabrikanten te vergroten door hen te verplichten beveiligingsondersteuning en software-updates te bieden om geïdentificeerde kwetsbaarheden aan te pakken, en hen informatie te verstrekken over de cyberbeveiliging van producten die zij kopen en gebruiken. De wet zal voorzien in één reeks regels voor cyberbeveiliging voor bedrijven in de EU. Het zal het aantal cyberbeveiligingsincidenten verminderen, de transparantie en het vertrouwen van

consumenten in producten met digitale elementen vergroten en een betere bescherming van hun gegevens en privacy garanderen.

Wie?

Het zou fabrikanten, importeurs en distributeurs van producten met digitale elementen verplichten om gedurende hun hele levenscyclus een zorgplicht te bieden. Deze regels omvatten het plaatsen van de producten op de markt door middel van een proces van conformiteitsbeoordeling van de eisen voor het ontwerp, de ontwikkeling en de productie van dergelijke producten.

De Cyberweerbaarheidsverordening is relevant voor Nederlandse gemeenten, omdat de eis van producten met digitale elementen door juristen in overweging moet worden genomen bij het sluiten van een contract met dergelijke aanbieders.

Critical Entities Resilience richtlijn

Wanneer?

De richtlijn is op 16 januari 2023 in werking getreden. Uiterlijk op 17 oktober 2024 dienen de lidstaten de maatregelen vast te stellen en bekend te maken die nodig zijn om aan deze richtlijn te voldoen. Zij stellen de Commissie daarvan onverwijld in kennis. Zij passen die bepalingen toe met ingang van 18 oktober 2024. Elke lidstaat stelt uiterlijk op 17 januari 2026 een strategie vast om de veerkracht van kritieke entiteiten te vergroten (de "strategie"). Uiterlijk op 17 juli 2027 dient de Commissie bij het Europees Parlement en de Raad een verslag in waarin wordt beoordeeld in hoeverre elke lidstaat de nodige maatregelen heeft genomen om aan deze richtlijn te voldoen.

Wat?

Overeenkomstig het in artikel 1 omschreven toepassingsgebied van deze richtlijn:

- Bevat verplichtingen voor de lidstaten om specifieke maatregelen te nemen om ervoor te zorgen dat diensten die essentieel zijn voor de instandhouding van vitale maatschappelijke functies op onbelemmerde wijze op de interne markt worden verleend, met name verplichtingen om kritieke entiteiten te identificeren en kritieke entiteiten te ondersteunen bij het nakomen van de verplichtingen die aan hen worden opgelegd;
- Stelt verplichtingen vast voor kritieke entiteiten om hun veerkracht en hun vermogen om essentiële diensten te verlenen te vergroten;
- Stelt regels vast voor het toezicht op kritieke entiteiten, voor de handhaving en voor de identificatie van kritieke entiteiten van bijzonder Europees belang, en voor adviesmissies om de maatregelen te beoordelen die deze entiteiten hebben genomen om aan de in de richtlijn gespecificeerde verplichtingen te voldoen;
- Stelt gemeenschappelijke procedures vast voor samenwerking en verslaglegging over de toepassing van de richtlijn;
- Bevat maatregelen om kritieke entiteiten een hoge mate van veerkracht te bieden om de verlening van essentiële diensten binnen de Unie te waarborgen en de werking van de interne markt te verbeteren.

De lidstaten moeten uiterlijk op 17 juli 2026 de kritieke entiteiten voor de in de CER-richtlijn genoemde sectoren identificeren. Zij zullen deze lijst van essentiële diensten gebruiken om risicobeoordelingen uit te voeren en vervolgens de kritieke entiteiten te identificeren. Eenmaal

geïdentificeerd, zullen de kritieke entiteiten maatregelen moeten nemen om hun veerkracht te vergroten.

In artikel 13 van de richtlijn worden enkele maatregelen opgesomd die kritieke entiteiten zullen moeten nemen om veerkrachtiger te worden:

a) incidenten te voorkomen, waarbij terdege rekening wordt gehouden met maatregelen ter beperking van het risico op rampen en aanpassing aan de klimaatverandering;
b) te zorgen voor een adequate fysieke beveiliging van hun gebouwen en kritieke infrastructuur, waarbij terdege rekening wordt gehouden met bijvoorbeeld omheiningen, barrières, instrumenten en routines voor perimeterbewaking, detectieapparatuur en toegangscontroles;
c) te reageren op, weerstand te bieden aan en de gevolgen van incidenten te beperken, waarbij terdege rekening wordt gehouden met de toepassing van procedures en protocollen voor risico- en crisisbeheer en met alarmeringsroutines;
d) te herstellen van incidenten, terdege rekening houdend met bedrijfscontinuïteitsmaatregelen en het in kaart brengen van alternatieve toeleveringsketens, teneinde de verlening van de essentiële dienst te hervatten;
e) (e) te zorgen voor een adequaat beheer van de veiligheid van de werknemers, waarbij terdege rekening wordt gehouden met maatregelen zoals het vaststellen van categorieën personeel die kritieke functies uitoefenen, het vaststellen van toegangsrechten tot gebouwen, kritieke infrastructuur en gevoelige informatie, het opzetten van procedures voor antecedentenonderzoeken overeenkomstig artikel 14 en het aanwijzen van de categorieën personen die dergelijke antecedentenonderzoeken moeten ondergaan, en het vaststellen van passende opleidingseisen en kwalificaties. De lidstaten zorgen ervoor dat kritieke entiteiten rekening houden met het personeel van externe dienstverleners bij het vaststellen van de categorieën personeel die kritieke functies uitoefenen.
f) het relevante personeel bewuster te maken van de onder a) tot en met e) bedoelde maatregelen, waarbij naar behoren rekening wordt gehouden met opleidingen, voorlichtingsmateriaal en oefeningen.

Wie?

Lidstaten en kritieke entiteiten.

Volgens deze richtlijn wordt onder "kritieke entiteit" verstaan een publieke of private entiteit die door een lidstaat is aangemerkt als behorend tot een van de in de bijlage bij de richtlijn genoemde categorieën. De sectoren zijn de volgende: energie, vervoer, bankwezen, financiële markt infrastructuur, gezondheid, drinkwater, afvalwater, digitale infrastructuur, overheid, ruimtevaart, productie, verwerking en distributie van voedsel.

Van de sectoren die in de richtlijn zijn opgenomen, worden in de bijlage "overheidsinstanties van **centrale overheden** zoals gedefinieerd door de lidstaten in overeenstemming met het nationale recht" genoemd. Het is dus mogelijk dat gemeenten niet onder deze categorie vallen, maar onder elke andere categorie wanneer een overheidsinstantie op lokaal niveau bijvoorbeeld afvalwater beheert en door haar lidstaat als een kritieke entiteit wordt aangemerkt.

Bijlage C: Gebruikte bronnen

Rapporten en studies

BDO (2023), *BDO-Benchmark Nederlandse gemeenten 2022. Tekorten nemen af, uitdagingen groter. Incidentele voordelen maskeren structurele problematiek*

Hooghiemstra & Partners (2023), *DORA van toepassing op gemeenten, memo d.d. 18 december 2023*

Hooghiemstra & Partners (2024), *RED van toepassing op gemeenten, memo d.d. 5 april 2024*

VNG (2020), *Uitvoeringskracht van gemeenten. Hoe sterk zijn onze schouders?*

Internet

https://bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf

https://bio-overheid.nl/media/0qxksxwi/20221117-rapport-evaluatie-bio-berenschot.pdf

https://digital-strategy.ec.europa.eu/nl/policies/cybersecurity-strategy

https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/

https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf

https://eur-lex.europa.eu/eli/dir/2022/2557/oj

https://eur-lex.europa.eu/eli/reg/2022/2554/oj

https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32022L2555&from=EN

https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32019R0881

https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32014R0910

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

https://minbzk.github.io/Baseline-Informatiebeveiliging-Overheid/

https://www.informatiebeveiligingsdienst.nl

https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

https://www.informatiebeveiligingsdienst.nl/nieuws/cybersecurity-implementatierichtlijn-objecten-csir-beveiliging-van-proces-automatisering-van-gemeenten/

https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/

https://www.informatiebeveiligingsdienst.nl/product/handreiking-functieprofielen-informatiebeveiliging/

https://www.informatiebeveiligingsdienst.nl/product/handreiking-procesautomatisering-pa-beleid/

https://www.informatiebeveiligingsdienst.nl/product/isms-v1-0/

https://www.informatiebeveiligingsdienst.nl/producten/

https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2021/04/201907-Handreiking-BIO-voor-kleine-gemeenten-v1.01.docx

https://www.internetconsultatie.nl/cyberbeveiligingswet/b1

https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12561

https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12562

https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12602

https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/beleidskompas/achtergrond-beleidskompas/verplichte-kwaliteitseisen/uitvoerbaarheidstoets-decentrale-overheden-en-normenkader-interbestuurlijke-verhoudingen

https://connect.nen.nl/Portal

https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/nis2-wbni2

https://vng.nl/artikelen/gemeentelijke-samenwerking-in-kaart-gebracht

https://vng.nl/files/vng/brieven/2019/20190107_ledenbrief_standaardverklaring-baseline-informatiebeveiliging-overheid.pdf

https://vng.nl/nieuws/13-nieuwe-wetten-publicatie-impactanalyse-digital-decade

https://vng.nl/nieuws/webinar-over-financieel-ravijn-gat-mogelijk-nog-dieper

https://vng.nl/nieuws/expertgroepen-digital-decade-gaan-in-2024-van-start

https://vng.nl/projecten/ensia

https://vng.nl/sites/default/files/2023-11/brief-nis2-bij-de-overheid.pdf