Concept

Regeling van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van [datum…], houdende regels ten aanzien van de beveiliging van netwerk- en informatiesystemen van entiteiten in de sector overheid ter uitvoering van de Cyberbeveiligingswet (Cyberbeveiligingsregeling sector overheid)

(KetenID WGK027594)

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

Gelet op de artikelen 2, tweede lid, 20 en 24, eerste lid, van het Cyberbeveiligingsbesluit;

Besluit:

Hoofdstuk 1. Algemene bepalingen

Artikel 1 (begripsbepaling)
In deze regeling wordt verstaan onder:
- *BIO2:* Baseline Informatiebeveiliging Overheid 2, versie 1.3 (Stcrt. PM jaartal, PM volgnummer);
- *essentiële dienst:* dienst als bedoeld in de artikelen 7 en 8 van deze regeling;
- *NEN:* norm die door de Stichting Koninklijk Nederlands Normalisatie Instituut is uitgegeven;
- *NEN-EN:* NEN die door het Europees Comité voor Normalisatie is vastgesteld;
- *NEN-EN-ISO/IEC*: NEN-EN die door de International Organization for Standardization en de International Electrotechnical Commission is vastgesteld;
- *VIR-BI*: Besluit voorschrift informatiebeveiliging rijksdienst bijzondere informatie 2025.

Artikel 2 (reikwijdte)
Deze regeling is van toepassing op essentiële entiteiten in de sector overheid, bedoeld in bijlage 1 bij de wet, met uitzondering van de waterschappen.

Hoofdstuk 2. Aanwijzing CSIRT

Artikel 3 (aanwijzing CSIRT)
De Informatiebeveiligingsdienst, onderdeel van VNG Realisatie B.V., is het CSIRT voor entiteitssoorten gemeenten en openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties als bedoeld in artikel 8, eerste, tweede, en derde lid, van de Wet gemeenschappelijke regelingen, voor zover deze openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties kwalificeren als overheidsinstantie en er ten minste één gemeente deelneemt aan de gemeenschappelijke regeling.

Artikel 4 (eisen aan CSIRT)
PM

Artikel 5 (eisen aan CSIRT)
PM

Hoofdstuk 3. Zorgplicht

Paragraaf 1 (informatiebeveiligingsstandaarden)

Artikel 6 (ISO-standaarden en BIO2)

1. De entiteit past de NEN-EN-ISO/IEC 27001:2023 toe op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor beveiliging van netwerk- en informatiesystemen en het vaststellen van het toepassingsgebied van dit managementsysteem.

2. De entiteit past de beheersmaatregelen van de NEN-EN-ISO/IEC 27002:2022 en de overheidsmaatregelen van de BIO2, voor zover deze zien op de beveiliging van netwerk- en informatiesystemen en niet door middel van een markering in de BIO2 zijn uitgezonderd, toe op het formuleren van passende beheersmaatregelen.
3. De entiteit draagt er zorg voor dat de opzet, het bestaan en de werking van de passende beheersmaatregelen aantoonbaar zijn.

Paragraaf 2 (identificeren essentiële diensten)

Artikel 7 (centrale overheden)

1. De entiteiten in de subsector centrale overheden, bedoeld in bijlage 1 bij de wet, houden een overzicht bij van hun essentiële diensten.
2. Een dienst is essentieel als bedoeld in het eerste lid indien een incident ten minste kan leiden tot schade op niveau 3 in minimaal één van de categorieën van de tabel in bijlage 1.

Artikel 8 (decentrale overheden)

1. De entiteiten in de subsector decentrale overheden, bedoeld in bijlage 1 bij de wet, houden een overzicht bij van hun essentiële diensten.
2. Een dienst is essentieel als bedoeld in het eerste lid indien een incident ten minste kan leiden tot schade op niveau hoog in minimaal één van de categorieën van de tabel in bijlage 2.

Hoofdstuk 4 (meldplicht)

Artikel 9 (centrale overheden)

1. Voor een essentiële dienst van een entiteit in de subsector centrale overheden, bedoeld in bijlage 1 bij de wet, is ieder incident een significant incident als bedoeld in artikel 25, tweede lid, van de wet.
2. Voor een niet-essentiële dienst van een entiteit in de subsector centrale overheden, bedoeld in bijlage 1 bij de wet, is een incident een significant incident als bedoeld in artikel 25, tweede lid, van de wet, als het leidt of kan leiden tot:
a. een ernstige operationele verstoring van de dienst als gevolg waarvan de dienstverlening van de entiteit ten minste vier uur niet beschikbaar is;
b. financiële schade voor de staat of de samenleving van meer dan €500.000.000;
c. de ernstige verwonding of de dood van een natuurlijke persoon;
d. misbruik van bedrijfsinformatie van de overheid met financiële schade van meer dan €5.000.000; of
e. de kennisname door onbevoegden van vertrouwelijke informatie op ten minste het niveau Staatsgeheim CONFIDENTIEEL, bedoeld in artikel 4, tweede lid, onder c, van het VIR-BI, NATO CONFIDENTIAL als bedoeld in bijlage E, paragraaf 6, van de NATO Security Policy (Security Within the North Atlantic Treaty Organization, CM(2002)49-REV1) of EU CONFIDENTIAL als bedoeld in artikel 2 van het Besluit 2013/488/EU van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie.
3. In afwijking van het eerste en het tweede lid, onderdeel a, zijn geplande onderbrekingen van de dienst of ingeplande onderhoudswerkzaamheden die worden uitgevoerd door of onder de verantwoordelijkheid van de entiteit, geen significante incidenten.

Artikel 10 (decentrale overheden)

1. Voor een essentiële dienst van een entiteit in de subsector decentrale overheden, bedoeld in bijlage 1 bij de wet, is ieder incident een significant incident als bedoeld in artikel 25, tweede lid, van de wet.

2. Voor een niet-essentiële dienst van een entiteit in de subsector decentrale overheden, bedoeld in bijlage 1 bij de wet, is een incident een significant incident als bedoeld in artikel 25, tweede lid, van de wet, als het leidt of kan leiden tot:
a. een ernstige operationele verstoring van de dienst als gevolg waarvan de dienstverlening van de entiteit ten minste vier uur niet beschikbaar is;
b. financiële gevolgen die niet kunnen worden opgevangen in de reguliere begroting;
c. de ernstige verwonding of de dood van een natuurlijke persoon; of
d. de openbaarmaking van vertrouwelijke informatie op ten minste het niveau Staatsgeheim CONFIDENTIEEL, bedoeld in artikel 4, tweede lid, onder c, van het VIR-BI, NATO CONFIDENTIAL als bedoeld in bijlage E, paragraaf 6, van de NATO Security Policy (Security Within the North Atlantic Treaty Organization, CM(2002)49-REV1) of EU CONFIDENTIAL als bedoeld in artikel 2 van het Besluit 2013/488/EU van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie.
3. In afwijking van het eerste en het tweede lid, onderdeel a, zijn geplande onderbrekingen van de dienst of ingeplande onderhoudswerkzaamheden die worden uitgevoerd door of onder de verantwoordelijkheid van de entiteit, geen significante incidenten.

Hoofdstuk 5. Slotbepalingen

Artikel 11 (Inwerkingtreding)

Deze regeling treedt in werking met ingang van PM.

Artikel 12 (Citeertitel)

Deze regeling wordt aangehaald als: Cyberbeveiligingsregeling sector overheid.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

Concept

Bijlage 1. Te beschermen belangen centrale overheden

Bijlage bij artikel 7

TBB		4	3	2	1
Politieke schade	Geen	Politieke schade voor bewindspersoon	Aftreden bewindspersoon	Aftreden kabinet	Parlementaire crisis
Imagoschade	Geen	Verlies aan publiek respect	Publieke verontwaardiging	Verlies aan vertrouwen	Structureel verlies aan vertrouwen
Diplomatieke schade	Geen	Te herstellen door ambtelijke opschaling	Te herstellen door politieke opschaling	Externe bemiddeling noodzakelijk	Lange termijn schade ten opzichte van bondgenoten; oorlog
Schade vitale processen in de samenleving	Geen invloed	Verlies van zekerheid van continuïteit	Tijdelijk verlies van continuïteit	Langdurig verlies van continuïteit	Blijvende uitval van processen
Letselschade	Geen	Individuele gewonde	Individuele dode, zeer ernstig gewond	Meerdere doden, ernstig gewonden	Groepen doden
Betrouwbaarheidseisen IT-systemen (quickscan BIR[1])	ZL, ZL, ZL	t/m H, H, H	Eén van de aspecten ZH	Alle aspecten ZH	
Rubriceringsniveau, als bedoeld in artikel artikel 4 lid 2 VIR-BI[2]		Ongerubriceerd met merking; Dep. V	Stg. CONFIDENTIEEL	Stg. GEHEIM	Stg. ZEER GEHEIM
NAVO-[3] of EU-rubriceringsniveau[4]		NATO-RESTRICTED Of EU-RESTRICTED	NATO-CONFIDENTIAL of EU-CONFIDENTIAL	NATO SECRET of EU-SECRET	COSMIC TOP SECRET of EU-TOP SECRET
Financiële schade aan de economie of de staat in euro's.	Minder dan 50 mln.	>50 mln.	>500 mln.	>5 mld.	>50 mld.
Financiële schade door misbruik van bedrijfsinformatie in euro's.	Minder dan 1 mln.	>1 mln.	>5 mln.	> 500 mln.	>5 mld.

[1] Volgens Bijlage 2 in *Stcrt.* 2019, 26526.
[2] *Stcrt.* 2025, 30222.
[3] Als bedoeld in bijlage E, paragraaf 6, van de NATO Security Policy (Security Within the North Atlantic Treaty Organization, CM(2002)49-REV1).
[4] Als bedoeld in artikel 2 van het Besluit 2013/488/EU van de Raad van 23 september 2013 betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie.

Bijlage 2. Te beschermen belangen decentrale overheden

Bijlage bij artikel 8

Impactniveau	Zeer laag	Laag	Middel	Hoog	Zeer hoog
Impact op beschikbaarheid (dataverlies - RPO[5]); hoeveel dataverlies is acceptabel	Dataverlies 36 uur	Dataverlies 24 uur	Dataverlies 12 uur	Dataverlies 4 uur	Dataverlies 1 uur
Hersteltijd (RTO[6]); hoe lang mag het proces hinder ondervinden van uitval?	Maximaal 1 week uitval (5 x 8 uur)	Maximaal 2 dagen uitval (2 x 8 uur)	Maximaal 1 dag uitval (1 x 8 uur)	Maximaal 4 uur uitval	Maximaal 1 uur uitval
Impact op belang entiteit	Minimale invloed op kernactiviteiten; weinig invloed op strategische doelstellingen.	Beperkte invloed op sommige kernactiviteiten; enige invloed op strategische doelstellingen.	Duidelijke invloed op meerdere kernactiviteiten; strategie moet mogelijk aangepast worden.	Aanzienlijke invloed op kernactiviteiten; strategische doelstellingen ernstig in gevaar.	Kritieke invloed op de kernactiviteiten; het voortbestaan van de organisatie kan in gevaar komen.
Vervangbaarheid informatie	Informatie is gemakkelijk te vervangen zonder noemenswaardige kosten of inspanning.	Informatie is vervangbaar met enige inspanning of kosten.	Vervanging van de informatie is mogelijk, maar vereist aanzienlijke tijd of middelen.	Informatie is moeilijk te vervangen, met hoge kosten of aanzienlijke inspanning.	Informatie is onvervangbaar, verlies zou een onherstelbare impact hebben.
Te beschermen belangen uit de ABDO[7]/ ABRO[8] of vergelijkbaar		TBB 4	TBB 4	TBB 3	TBB 2 / TBB 1
Classificatie vertrouwelijke informatie	Ongerubriceerd	Dep. V (niveau 1 - standaard)	Dep. V (niveau 2 - weerstand tegen spionage)	Stg. C	Stg.G / Stg. ZG
Schade bij openbaarmaking		Indien kennisname door niet-geautoriseerden nadeel kan toebrengen aan de belangen van één of meerdere afdelingen	Indien kennisname door niet geautoriseerden schade kan toebrengen aan de belangen van de provincie, gemeente of gemeenschappelijke regeling	Indien kennisname door niet geautoriseerden aanzienlijke schade kan toebrengen aan een van de vitale belangen van de provincie, gemeente of gemeenschappelijke regeling	Indien kennisname door niet geautoriseerden ernstige of zeer ernstige schade kan toebrengen aan een van de vitale belangen van de provincie, gemeente of gemeenschappelijke regeling

[5] Recovery Point Objective: De herstelpuntdoelstelling, die weergeeft wat het maximaal toegestane dataverlies is voor de organisatie. Deze hoeveelheid is gemeten in tijd, namelijk de periode tussen de laatste succesvolle data back-up en de verstorende gebeurtenis.
[6] Recovery Time Objective: De hersteltijddoelstelling, die weergeeft wat de maximaal toegestane tijd is dat een systeem of proces offline kan zijn na een incident zonder dat dit gevolgen heeft voor de bedrijfsvoering.
[7] Algemene Beveiligingseisen voor Defensieopdrachten.
[8] Algemene Beveiligingseisen Rijksoverheidsopdrachten.

Concept

Kennisnemen informatie door onbevoegden		Is ongewenst	Moet zoveel mogelijk worden voorkomen	Moet worden voorkomen	Is onacceptabel
Persoonsgegevens		Bevat persoonsgegevens	Bevat bijzondere persoonsgegevens of meerdere collecties van persoonsgegevens.	Bevat meerdere collecties met bijzondere persoonsgegevens	
Politieke schade	Geen politieke gevolgen; nauwelijks merkbaar.	Beperkte politieke gevolgen; klein effect op beleid of relaties.	Duidelijke politieke gevolgen; invloed op beleid of strategische relaties.	Aanzienlijke politieke gevolgen; mogelijk grote beleidswijzigingen of verlies van vertrouwen.	Catastrofale politieke gevolgen; mogelijk leidend tot ontslag of grote beleidscrises.
Diplomatieke schade	Geen diplomatieke schade. De relaties met andere landen zijn stabiel en goed onderhouden, zonder enige negatieve impact. Effect op burgergerichte processen: Geen impact. Burgers merken geen verandering in de dienstverlening, internationale samenwerking of toegang tot buitenlandse diensten.	Klein verlies aan diplomatieke goodwill. Er zijn lichte spanningen, maar deze worden snel en efficiënt opgelost zonder grote gevolgen. Effect op burgergerichte processen: Minimale invloed op internationale samenwerking, bijvoorbeeld lichte vertragingen bij grensoverschrijdende diensten of minder vloeiende samenwerking met buitenlandse partners. Burgers merken nauwelijks iets van de situatie.	Merkbare diplomatieke schade. Relaties met andere landen verslechteren tot een punt waarop samenwerking in bepaalde gebieden moeilijker wordt. Dit kan bijvoorbeeld leiden tot vertragingen in internationale handel, samenwerking of informatie-uitwisseling. Effect op burgergerichte processen: Burgers kunnen langere wachttijden ondervinden bij grensoverschrijdende diensten zoals visa-aanvragen, internationale handel of hulp in het buitenland. Er kunnen ook meer bureaucratische hindernissen ontstaan bij internationale procedures.	Aanzienlijke diplomatieke schade. De relaties met belangrijke diplomatieke partners verslechteren aanzienlijk, wat leidt tot vertragingen of beperkingen in internationale samenwerking, en tot verlies van toegang tot strategische informatie of samenwerkingsovereenkomsten. Effect op burgergerichte processen: Burgers ondervinden duidelijke problemen, zoals een aanzienlijke afname in toegang tot consulaire diensten in het buitenland, problemen bij internationale reis- of handelsregelingen, en moeilijkheden in grensoverschrijdende communicatie en samenwerking. Er is sprake van toenemende ontevredenheid.	Ernstige diplomatieke schade. De diplomatieke relaties met andere landen zijn ernstig verstoord of verbroken, wat kan leiden tot sancties, reisbeperkingen, en ernstige verstoringen in internationale samenwerkingen en handelsrelaties. Effect op burgergerichte processen: Burgers worden geconfronteerd met grote problemen, zoals reisverboden, verlies van consulaire steun in het buitenland, beperkte toegang tot internationale diensten en ernstige verstoringen in de handel. Dit kan leiden tot wijdverspreide ontevredenheid en ernstige gevolgen voor de economie en de toegang tot buitenlandse diensten.
Financiële impact	Op te vangen binnen de begroting van de afdeling	Niet meer op te vangen binnen de begroting van de afdeling	Niet meer op te vangen binnen de begroting van de directie	Niet meer op te vangen binnen de begroting van de provincie, gemeente of gemeenschappelijke regeling	
Directe imagoschade	Geen imagoschade. De reputatie van de organisatie of overheid	Verlies van publiek respect -	Publieke verontwaardiging -	Verlies aan vertrouwen - Aanzienlijke	Structureel verlies aan vertrouwen -

	blijft ongeschonden. Er is geen negatieve publiciteit of perceptie van het publiek. Effect: Geen invloed op de reputatie. De organisatie wordt nog steeds als betrouwbaar, efficiënt en positief gezien.	Lichte imagoschade. Er is sprake van een klein incident of negatieve publiciteit, maar dit blijft beperkt en is snel te herstellen. Effect: Kortdurende negatieve perceptie bij een beperkt publiek, zonder langdurige gevolgen. Vertrouwen wordt snel hersteld door adequate communicatie en acties.	Merkbare imagoschade. Een incident of reeks incidenten leidt tot bredere negatieve aandacht in de media en onder het publiek. Het vertrouwen in de organisatie wordt aangetast, en er is kritiek op het beleid of handelen. Effect: Zichtbare impact op de reputatie, met een afname van vertrouwen en geloofwaardigheid bij een groot deel van het publiek. Herstel vereist actieve maatregelen en verbeterde communicatie.	imagoschade. Een grote misser of reeks van schandalen leidt tot wijdverspreide negatieve berichtgeving en publieke verontwaardiging. Het herstel van het vertrouwen vergt aanzienlijke inspanningen en tijd. Effect: Het vertrouwen in de organisatie wordt ernstig geschaad. Het publiek en de media blijven kritisch, en de negatieve impact houdt lange tijd aan. Grootschalige herziening van beleid of management is nodig om het imago te herstellen.	Ernstige imagoschade. Een crisis of schandaal leidt tot langdurige en diepgaande reputatieschade, mogelijk op internationaal niveau. Het imago van de organisatie is ernstig en mogelijk onherstelbaar beschadigd. Effect: Het vertrouwen in de organisatie is volledig verloren, met blijvende gevolgen voor de geloofwaardigheid en het functioneren. Mogelijk verlies van steun vanuit het publiek, partners of andere stakeholders. Drastische maatregelen zijn nodig, en volledig herstel kan jaren duren of nooit volledig worden bereikt.
Significant verlies van motivatie medewerkers	Geen waarneembaar effect op de motivatie van medewerkers. Effect op burgergerichte processen: Geen merkbare invloed op de kwaliteit van de dienstverlening. Burgers ervaren dezelfde efficiëntie en betrouwbaarheid.	Een lichte afname in motivatie die minimale gevolgen heeft voor de prestaties. Mogelijk kleine vertragingen of minder efficiëntie, maar zonder significante verstoring van de processen. Effect op burgergerichte processen: Kleine vertragingen of incidentele fouten in de dienstverlening, maar geen structurele problemen. Burgers merken mogelijk een lichte afname in de respons of efficiëntie.	Merkbare daling in motivatie wat leidt tot verminderde productiviteit. Dit kan leiden tot vertragingen in besluitvorming, langere doorlooptijden en mogelijk meer fouten. Effect op burgergerichte processen: Verlengde wachttijden voor burgers, fouten in de afhandeling van aanvragen, en lagere kwaliteit van dienstverlening. Burgers kunnen ontevreden raken over de snelheid en kwaliteit van de overheidsdiensten.	Aanzienlijk verlies van motivatie, resulterend in frequente fouten, lange vertragingen en verminderd vermogen om op vragen of klachten van burgers te reageren. Effect op burgergerichte processen: Veel voorkomende vertragingen en kwaliteitsproblemen, waardoor burgers regelmatig problemen ondervinden bij het verkrijgen van diensten. Dit kan leiden tot een afname van het	Extreme demotivatie die leidt tot ernstige verstoringen in de dienstverlening, inclusief aanzienlijke fouten, langdurige vertragingen en mogelijk ook hogere niveaus van verloop onder medewerkers. Effect op burgergerichte processen: Ernstige verstoringen in de burgergerichte processen. Burgers ervaren langdurige wachttijden, fouten in administratieve processen, en een drastische afname in de

				vertrouwen in de overheid.	kwaliteit van dienstverlening, wat resulteert in grote publieke ontevredenheid en mogelijk een vertrouwenscrisis in de overheid.
Belangrijk verlies van management control	Geen verlies van management control. Processen verlopen zoals gepland, met duidelijke sturing en toezicht. Effect op burgergerichte processen: Geen impact. De overheid blijft effectief in het leveren van consistente en betrouwbare diensten aan burgers.	Klein verlies van management control. Er zijn lichte inefficiënties, maar deze worden snel opgemerkt en opgelost zonder grote verstoringen. Effect op burgergerichte processen: Sporadische kleine inefficiënties in de dienstverlening, zoals lichte vertragingen of communicatiemisverstanden. Burgers ervaren incidenteel minder optimale processen, maar dit leidt niet tot serieuze klachten.	Merkbaar verlies van management control. Er ontstaan significante inefficiënties en miscommunicatie tussen verschillende afdelingen, wat resulteert in trager besluitvormingsproces en problemen met het naleven van vastgestelde procedures. Effect op burgergerichte processen: Burgers ondervinden langere wachttijden, inconsistenties in informatieverstrekking of behandeling van aanvragen. Er is een duidelijke afname in de kwaliteit en voorspelbaarheid van overheidsdiensten, wat tot verhoogde frustratie kan leiden.	Aanzienlijk verlies van management control. Het gebrek aan sturing leidt tot fouten in kritieke processen, langdurige vertragingen, en het niet volgen van protocollen. Management reageert langzaam of inadequaat op problemen. Effect op burgergerichte processen: Burgers ervaren systematische vertragingen, onvolledige of foutieve dienstverlening, en gebrek aan adequate opvolging van aanvragen of klachten. Het vertrouwen in de efficiëntie en betrouwbaarheid van de overheid neemt merkbaar af.	Extreem verlies van management control. Het management is vrijwel niet in staat om de operationele processen te beheersen. Er is sprake van een chaotische situatie met frequente fouten, gebrek aan samenhang en ernstige vertragingen. Effect op burgergerichte processen: Ernstige verstoringen in de dienstverlening aan burgers. Diensten worden slecht uitgevoerd of komen zelfs geheel tot stilstand. Burgers ervaren langdurige vertragingen, administratieve chaos en aanzienlijke fouten in hun aanvragen of diensten, wat resulteert in een groot verlies van vertrouwen in de overheidsinstellingen.
Schade vitale processen	Geen verstoring van vitale processen.	Beperkte verstoring van vitale processen; processen kunnen snel worden hervat.	Duidelijke verstoring; vitale processen worden tijdelijk gehinderd.	Aanzienlijke verstoring; vitale processen worden ernstig gehinderd.	Catastrofale verstoring; vitale processen worden onwerkbaar of volledig stilgelegd.
Maatschappelijke impact	Geen of nauwelijks merkbare impact voor de samenleving. De verstoring is beperkt tot een kleine groep mensen of heeft nauwelijks effect	Enige impact op een beperkte groep mensen of specifieke gemeenschap. Het dagelijks leven van burgers wordt licht	Duidelijke impact op meerdere gemeenschappen of een significante groep mensen. Het dagelijks leven van deze mensen	Aanzienlijke impact op de samenleving als geheel of op een groot deel van de bevolking. Diensten of voorzieningen die essentieel zijn voor	Ernstige impact die de hele samenleving raakt. Essentiële diensten vallen langdurig uit of falen, wat mogelijk leidt tot onrust, massale

	op het dagelijks leven van burgers.	verstoord, maar er zijn alternatieven beschikbaar of de verstoring is kortdurend.	wordt merkbaar beïnvloed, bijvoorbeeld door verstoring van een publieke dienst gedurende meerdere dagen.	burgers worden onderbroken, wat leidt tot verstoringen op sociaal, economisch of fysiek gebied.	verstoring van dagelijks leven, en maatschappelijke ontwrichting.
Belang voor de organisatie	Minimale invloed op kernactiviteiten; weinig invloed op strategische doelstellingen.	Beperkte invloed op sommige kernactiviteiten; enige invloed op strategische doelstellingen.	Duidelijke invloed op meerdere kernactiviteiten; strategie moet mogelijk aangepast worden.	Aanzienlijke invloed op kernactiviteiten; strategische doelstellingen ernstig in gevaar.	Kritieke invloed op de kernactiviteiten; het voortbestaan van de organisatie kan in gevaar komen.
Letsel	Geen of minimale fysieke of psychische schade.	Lichte verwondingen of stress die zonder blijvende gevolgen zijn.	Ernstige verwondingen of stress met tijdelijke gevolgen.	Zeer ernstige verwondingen of blijvende psychische schade.	Dodelijke verwondingen of onherstelbare psychische schade
Inbreuk op persoonlijke levenssfeer	Geen of minimale fysieke of psychische schade.	Lichte verwondingen of stress die zonder blijvende gevolgen zijn.	Ernstige verwondingen of stress met tijdelijke gevolgen.	Zeer ernstige verwondingen of blijvende psychische schade.	Catastrofale inbreuk op privacy; ernstige gevolgen voor betrokkenen, mogelijk juridische gevolgen.

Concept

TOELICHTING

ALGEMEEN

Inleiding
De Europese Network and Information Security (NIS2)-richtlijn[9] verplicht tot het implementeren van regels over de beveiliging van netwerk- en informatiesystemen van essentiële en belangrijke entiteiten en de daarvoor benodigde governance binnen de entiteiten. Deze regels zijn omgezet in het voorstel voor de Cyberbeveiligingswet (Cbw[10]) en het Cyberbeveiligingsbesluit (Cbb). In de Cbb is een aantal grondslagen opgenomen voor het stellen van nadere regels voor de verschillende essentiële en belangrijke sectoren (en eventueel voor subsectoren en entiteiten).

Organisaties, in de richtlijn entiteiten genoemd, binnen de sector overheid, zowel op centraal- als decentraal niveau, zijn in de Cbw aangewezen als essentiële entiteiten. In het Cbb is een aantal grondslagen opgenomen om per ministeriële regeling nadere regels te stellen. Deze zien onder meer toe op het aanwijzen van een ander Computer Security Incident Response Team (CSIRT) dan het Nationaal Cyber Security Centrum (NCSC), het stellen van nadere regels voor de zorgplicht die organisaties hebben voor het beveiligen van hun netwerk- en informatiesystemen en het opnemen van sectorspecifieke drempelwaarden voor de meldplicht om te bepalen wanneer zich een significant beveiligingsincident voordoet in een netwerk- en informatiesysteem van een entiteit dat gemeld moet worden aan het CSIRT en de toezichthouder.

Deze ministeriële regeling (hierna: regeling) geldt voor de sector overheid, zowel voor de centrale als de decentrale overheden, met uitzondering van de waterschappen. De waterschappen vallen onder de regeling van de minister van Infrastructuur en Waterstaat. Deze regeling stelt nadere regels voor de zorgplicht vast alsook de drempelwaarden voor de meldplicht en wijst een afwijkend CSIRT aan voor gemeenten en gemeenschappelijke regelingen, voor zover daaraan ten minste één gemeente deelneemt.

Hoofdlijnen van het voorstel
Bij het stellen van nadere regels is het uitgangspunt gehanteerd dat zoveel mogelijk wordt aangesloten bij de bestaande praktijk om daarmee de invoeringslast van deze ministeriële regeling zoveel mogelijk te beperken. Per onderdeel wordt hierop nader ingegaan.

Zorgplicht
Bij de overheid bestaat op dit moment al de Baseline Informatiebeveiliging Overheid (BIO) als interbestuurlijk convenant met een groot aantal zorgplichtbepalingen. Los daarvan zijn er veel andere informatiebeveiligingseisen of zorgplichtbepalingen die vanuit verschillende interbestuurlijke voorzieningen en informatieprocessen wettelijk worden verplicht[11].

De Cbw en het Cbb vestigen een algemene zorgplicht voor een groot aantal maatschappelijke sectoren, waaronder de sector overheid. Naast de grondslag om deze onderwerpen nader uit te werken, biedt de delegatiegrondslag van het Cbb de ruimte om per ministeriële regeling ook zorgplichtbepalingen op te nemen over andere dan de genoemde onderwerpen, zolang die binnen de scope van de NIS2-richtlijn en de Cbw vallen. Met het stellen van nadere regels onder de zorgplicht ontstaat er voor overheidsinstanties, zowel op centraal als decentraal niveau, een algemeen wettelijk uniform en afdwingbaar kader met betrekking tot de zorgplicht voor de beveiliging van netwerk- en informatiesystemen. De noodzaak om deze eisen vanuit andere wet- en regelgeving nogmaals te stellen vervalt daarmee.

---

[9] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 20 mei 2015 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr.910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).
[10] *Kamerstukken II,* 2024/25, 36764, nr. 2.
[11] *Onderzoek wetgevingskader informatieveiligheid,* VKA, 2020.

De keuze is gemaakt om toepassing van de Baseline Informatiebeveiliging Overheid 2 (BIO2)[12] in deze regeling als verplichting op te nemen. Deze keuze is gemaakt om de volgende redenen:

Beperken implementatiedruk van de Cbw bij medeoverheden:
Met het aansluiten bij reeds bestaande normenkaders voor informatiebeveiliging van de overheid administratieve lasten van implementatie voor overheidsorganisaties worden beperkt. Zij dienen immers te voldoen aan normen die zij zich eerder zelf al hebben opgelegd. Bovendien hebben alle koepelorganisaties van medeoverheden in hun consultatiereacties op de Cbw en het Cbb reeds aangegeven graag de BIO te hanteren als invulling van de zorgplicht.

Hanteren van één methodiek binnen de overheid:
Het uitgangspunt is om binnen de overheid één werkwijze te hanteren, zodat overheidspartijen eenzelfde uitgangspunt hebben bij het maken van ketenafspraken en dezelfde taal en denkwereld hanteren richting de burger en het bedrijfsleven.

Als instrument voor het terugdringen van administratieve lastendruk:
Uit de Werkagenda Waardengedreven Digitaliseren[13] en de Nederlandse Cybersecurity Strategie (NLCS)[14] is de wens naar voren is gekomen om de BIO wettelijk te verankeren. Met als reden dat dit de noodzaak verkleint om vanuit verschillende (wettelijke) stelsels, denk bijvoorbeeld aan de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI), eisen te stellen aan de informatiebeveiliging voor overheden. Op dit moment is dat niet mogelijk, omdat de BIO nog een interbestuurlijk convenant is dat niet dezelfde status heeft als een van de genoemde wettelijke regelingen. Door de verankering van de BIO in deze ministeriële regeling zou echter op termijn een versimpeling kunnen worden aangebracht in het aantal van toepassing zijnde wettelijke regelingen ten aanzien van informatiebeveiliging, waardoor verantwoordings- en toezichtlasten voor overheden aanzienlijk kunnen worden teruggedrongen.

Verzoek vanuit alle bestuurslagen
Ten slotte is op 23 september 2025 door het Overheidsbreed Beleidsoverleg Digitalisering Overheid (OBDO) akkoord gegeven op de BIO2 en is de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties geadviseerd om de BIO2 als normenkader voor de zorgplicht op te nemen in de regelgeving onder de Cbw voor de sector overheid.

Verplichtingen
In de regeling zijn om die reden de volgende verplichtingen opgenomen:

De verplichting tot het toepassen van de NEN-EN-ISO/IEC 27001 op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging en het vaststellen van het toepassingsgebied van dit managementsysteem. Voor het bepalen van de context van de entiteit neemt de entiteit minimaal de beschreven context over uit de BIO2 bij het inrichten, implementeren, in stand houden en continu verbeteren van het managementsysteem voor informatiebeveiliging.

De NEN-EN-ISO/IEC 27002 en de verplichte overheidsmaatregelen uit de BIO worden toegepast op het formuleren van passende beheersmaatregelen. Hierbij wordt rekening gehouden met de omgeving(en) waarin de informatiebeveiligingsrisico's voorkomen, gebaseerd op de scope en de onderkende risico's. De beheersmaatregelen uit NEN-EN-ISO/IEC 27002 en de BIO kunnen, waar nodig én gelijkwaardig worden vervangen of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen, zoals voor zorginformatie NEN 7510 en voor Operationele Technologie (OT) de CSIR en IEC 62443 Industriële cybersecurity. Dat kan bijvoorbeeld wanneer een risico dusdanig klein is binnen de organisatie, of wanneer het ingeschatte risico beter afgedekt is met een

[12] PM verwijzing naar publicatie Staatscourant BIO2.
[13] *Kamerstukken II,* 2022/23, 26643, 640, bijlage 1062267.
[14] *Kamerstukken II,* 2022/23, 26643, 925, bijlage 1054176 en bijlage 1054176.

gelijkwaardige beheersmaatregel vanuit andere, specifiekere normenkaders (zoals NEN 7510 voor de zorg of CSIR voor operationele technologie).

Identificeren essentiële diensten
Daarnaast is een bepaling opgenomen die het identificeren van de essentiële diensten voor de centrale en decentrale overheden verplicht stelt. Hiervoor is aangesloten op bestaande werkwijzen bij zowel rijksoverheid als gemeenten[15]. Het doel daarvan is meervoudig:

- het helpt organisaties bij het proportioneel beveiligen van hun netwerk- en informatiesystemen. Het is een onderdeel van het risicomanagement en het geeft inzicht bij welke diensten de beveiliging de hoogste mate van zorgvuldigheid vraagt;
- het helpt bij het proportioneel invullen van de meldplicht, waarbij de focus ligt op het melden van incidenten op systemen van essentiële diensten.

Aanwijzing CSIRT
De entiteiten moeten op basis van de Cbw significante incidenten melden bij het CSIRT en de toezichthouder. In principe is het NCSC standaard aangewezen als het CSIRT voor alle (sub)sectoren en entiteiten tenzij per ministeriële regeling een ander CSIRT is aangewezen. Het aanwijzen van een ander CSIRT kan een keuze zijn voor meer aansluiting bij de bestaande situatie, waarin sommige (sub)sectoren of entiteiten reeds samenwerken met een bestaande organisatie als CSIRT. Op die manier is het niet nodig om nieuwe samenwerkingen in te regelen, en worden uitvoeringslasten voor organisaties beperkt.

Voor de gemeenten wordt de Informatiebeveiligingsdienst (IBD) van de VNG aangewezen als CSIRT. De IBD vervult namelijk deze rol op dit moment al voor de gemeenten, waardoor het voor de uitvoeringsconsequenties het meest logisch is om de huidige samenwerking voort te zetten. Voor gemeenschappelijke regelingen die samenwerkingsverbanden zijn van of met gemeenten, wordt de IBD ook als CSIRT aangewezen.

Het Cyberbeveiligingsbesluit biedt bovendien de mogelijkheid tot het stellen van nadere regels over de functionele, financiële, technische en organisatorische vereisten ten aanzien van een organisatie die op grond van artikel 2, tweede lid, Cbb is aangewezen als CSIRT. Over de eventuele invulling van deze eisen wordt afgestemd tussen het ministerie van Binnenlandse Zaken en het CSIRT.

Meldplicht
De Cbw verplicht entiteiten tot het melden van significante incidenten bij het CSIRT en de bevoegde autoriteit. In de praktijk is voorzien om deze tweeledige melding in te vullen via het meld- en registratieportaal. Entiteiten hoeven dan slechts eenmalig melding te maken van een incident, die wordt gerouteerd naar zowel het ondersteunend CSIRT als de toezichthouder (aangewezen door de bevoegde autoriteit). Artikel 27, eerste lid, Cbw bepaalt dat de entiteit onverwijld of, indien dit niet mogelijk is, binnen 72 uur nadat zij kennis heeft gekregen van het significante incident een melding daarvan doet bij het CSIRT en de bevoegde autoriteit. Het is aan de entiteit om te onderzoeken en vast te stellen of de gestelde drempelwaarden overschreden worden of kunnen worden en te melden indien nodig.

In het Cbb is een delegatiegrondslag opgenomen om bij ministeriële regeling per sector invulling te geven aan de criteria voor het bepalen wanneer sprake is van een significant incident. Hiervoor wordt gekeken naar de gevolgen van een incident in de zin van een operationele verstoring van de diensten van de entiteit, financiële schade voor de eigen entiteit, en materiële en immateriële schade aan andere natuurlijke of rechtspersonen. Deze drempelcriteria zijn in samenwerking met experts vanuit de bestuurslagen en in afstemming met overige vakdepartementen nader uitgewerkt.

[15] Respectievelijk Te Beschermen Belangen (TBB's) en de impact tabel voor de gemeenten die de IBD heeft gepubliceerd. Ook enkele provincies hanteren op dit moment de werkwijze van de gemeenten.

Bij het opstellen van de drempelwaarden voor significante incidenten is gestreefd naar het zoveel mogelijk beperken van de lastendruk voor entiteiten. Tegelijkertijd dient voorkomen te worden dat relevante meldingen niet als significant worden aangemerkt en daardoor niet worden gemeld bij CSIRT en toezichthouder. Tevens is in beschouwing genomen dat de Cbw vereist dat meldingen kort na ontdekking van een incident moeten worden gedaan. Tijd om een (complexe) analyse te maken van de mogelijke gevolgen van het incident — terwijl het incident ook moet worden beheerst — is er vaak niet. Daarom is ervoor gekozen deze analyse zoveel mogelijk naar voren te halen, bij de uitvoering van het risicomanagement en het bepalen van de essentiële diensten. Zodat de meldplicht zich focust op incidenten die betrekking hebben op de belangrijkste te beschermen diensten van overheidsorganisaties.

De algehele lijn daarbij is dat ieder incident op deze essentiële diensten moet worden gemeld vanuit de gedachte dat dit tot grote potentiële schade kan leiden. Bij incidenten op niet-essentiële diensten is de inschatting vooraf dat dit tot lagere schade zal leiden. Dit is geen wetmatigheid, het is denkbaar dat een incident op deze diensten toch tot een hogere schade zal leiden. Voor die diensten bevat de regeling uitgewerkte criteria om te toetsen of het incident gemeld dient te worden.

Deze drempelcriteria zijn zoveel mogelijk in lijn gebracht met reeds bestaande criteria. Voor de sector overheid gaat dit om de TBB's, voor gemeenten om de impacttabel die de IBD bij gemeenten toepast en die ook door enkele provincies worden gebruikt.

De Rijksoverheid kent 4 niveaus binnen de TBB-tabel, gemeenten spreken over 5 impactniveaus. Beide modellen gaan in op de volgende criteria:

- Schade aan personen, denk aan doden of ernstig gewonden als gevolg van het incident.
- Materiële schade, denk aan financieel verlies dat niet binnen de reguliere begroting van de organisatie is op te vangen.
- Integriteit en vertrouwelijkheid, denk aan de openbaarmaking van informatie op het niveau Confidentieel of hoger of de openbaarmaking van verzamelingen aan informatie op het niveau Departementaal-Vertrouwelijk.
- Beschikbaarheid, denk aan uitval van dienstverlening van kernprocessen die een bepaalde tijd voortduurt en waardoor een minimaal aantal personen wordt gehinderd. Of herstel dat niet binnen afzienbare tijd mogelijk is.

Incidenten op essentiële diensten, namelijk systemen met categorie TBB3, TBB2 en TBB1 moeten direct worden gemeld. Voor decentrale overheden geldt dit voor incidenten op systemen in de categorie 'hoog' en 'zeer hoog'. Bij systemen met categorie TBB4, of categorie 'midden', 'laag' en 'zeer laag' is die verwachting er niet en gelden concrete criteria.

Gevolgen
De regeling codificeert de bestaande praktijk op veel vlakken. Op zichzelf geeft dat weinig directe gevolgen. Anders dan voorheen wordt het nu echter een wettelijke verplichting waarop ook toezicht en handhaving uitgevoerd kan worden. Dat betekent dat organisaties die voorheen minder aandacht hadden voor informatiebeveiliging en hierdoor mogelijk 'achterstallig onderhoud' hebben, een extra prikkel krijgen om de beveiliging in lijn te brengen met wat van een overheidsorganisatie verwacht mocht en mag worden.

Zoals bij het onderwerp zorgplicht is aangegeven, biedt deze regeling een goed aanknopingspunt om in overleg met verschillende rijksoverheidspartijen te bezien welke bestaande sectorale regelingen kunnen worden ontdaan van dubbelingen ten opzichte van deze regeling. Dat levert in potentie meer duidelijkheid, minder risico op tegenstrijdigheden en het terugdringen van administratieve last op.

Uitvoering

Zorgplicht
De zorgplicht heeft betrekking op de beveiliging van netwerk- en informatiesystemen. In de bestaande situatie hadden alle overheidslagen (rijksoverheid, provincies, gemeenten en waterschappen) zich vanaf 2018 gecommitteerd aan de BIO. Het effect van de BIO is afhankelijk van aard van de netwerk- en informatiesystemen in de verschillende overheidsorganisaties. Ook in de bestaande situatie is er namelijk sprake van risicomanagement. De eerdergenoemde ISO-standaarden die daarop toezien, staan sinds 2008 op de Pas-toe-of-leg-uit lijst van het Forum Standaardisatie[16]. Deze standaarden zijn toegepast in de verschillende baselines die voorafgaand aan de BIO al per bestuurslaag waren opgesteld. Met andere woorden, van overheidsorganisaties mag worden verwacht dat zij de ISO-standaarden en de BIO in de praktijk hebben gebracht.

De Cbw brengt wel enkele accenten aan. De bedrijfscontinuïteit, crisis(beheer) en de (toeleverings)keten krijgen meer aandacht dan in de bestaande situatie. En verder moeten beveiligde spraak-/tekst- en videoverbindingen en beveiligde noodcommunicatiesystemen worden ingezet wanneer gepast.[17]

Meldplicht
Met name nieuw voor alle overheidsorganisaties is de verplichte meldplicht bij incidenten. Niettemin hebben organisaties ook nu al te maken met een meldplicht bij datalekken waar persoonsgegevens in het geding zijn. Verder hebben alle bestuurslagen, met uitzondering van de provincies, een CSIRT waar bij incidenten contact mee wordt gelegd. Verder bevat de BIO ook een paragraaf over incidentbeheer met een set maatregelen. Tot slot is ervoor gekozen de schade-inschatting ‘aan de voorkant’, bij de zorgplicht, te gebruiken als meetlat voor het melden. Deze meetlat is dezelfde als nu bij gemeenten als rijksoverheid wordt gehanteerd, zodat gemaakte risico-inschattingen niet vanwege de Cbw opnieuw moeten worden gedaan.

Toezicht en handhaving
PM UHT

Financiële gevolgen
Overheidsorganisaties zijn heel verschillend. Om die reden is het zeer complex een inschatting te maken van kosten die met deze verplichtingen gepaard gaan. De ene organisatie zal vanwege zijn aard meer en/of andere maatregelen hebben getroffen dan de ander. De overheid kent reeds het uitgangspunt van risicogestuurd beveiligen: afhankelijk van het te beschermen belang en de dreiging wordt een afweging gemaakt welke maatregelen noodzakelijk zijn. Deze aanpak voorkomt te hoog ingeschatte kosten waar deze eigenlijk niet nodig zijn, maar ook te lage kosteninschattingen die niet toereikend blijken. Uitkomst van deze aanpak is dat organisaties zelf de kosten dragen van beveiliging van hun systemen.

Een algemene inschatting van de kosten is niet te maken. Kosten gerelateerd aan taken, diensten en voorzieningen bestaan voor ongeveer 85% uit taken in medebewind[18] waarvoor telkens eigen financiering is georganiseerd, ook voor de beveiliging ervan. Het kan voorkomen dat overheidsorganisaties niet voldoen aan bestaande verplichtingen die straks onder de Cbw gaan vallen, maar dat is generiek niet in te schatten. Het is niet zuiver om de kosten om aan eerdere, bestaande verplichtingen te voldoen bij deze regeling te betrekken, men moest immers al aan die regels voldoen. Daarom valt ‘achterstallig onderhoud’ buiten de scope van deze paragraaf.

Het ministerie van BZK ondersteunt entiteiten verder door een sectoraal CSIRT voor de overheid aan te wijzen. Deze rol wordt in deze regeling bij respectievelijk het NCSC voor overheidsinstanties van de centrale overheid en provincies, en IBD voor gemeenten en gemeenschappelijke regelingen

[16] *Verkennend onderzoek NEN-ISO/IEC 27001 en 27002*, Forum Standaardisatie, 2014
[17] *Mapping NIS2 en ISO 27002:2022/BIO2*, BIO-overheid.nl, 2024
[18] Zie bijvoorbeeld: *Lokale autonomie verder onder druk*, Binnenlands Bestuur, 2010

waar ten minste één gemeente aan deelneemt, belegd. Deze CSIRT's ondersteunen entiteiten in het geval van incidenten en geven in de praktijk regelmatig beveiligingsadviezen.

Bij het proces van totstandkoming van de Cbw en onderliggende regelgeving is er bovendien regelmatig contact met alle overheidslagen, met als doel om wensen en knelpunten vanuit medeoverheden al in een vroeg stadium van het wetgevingsproces te betrekken. Dat gebeurt onder meer via reguliere overleggen met de koepelvertegenwoordigers van de medeoverheden, vanuit het proces van de Uitvoerbaarheidstoets Decentrale Overheden (UDO) en de werkgroep BIO. Bovendien is op verschillende momenten formeel gecommuniceerd over de voortgang van het wetgevingstraject: via de Minister van Justitie en Veiligheid over de algehele voortgang en via de Verzamelbrieven Digitalisering van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over toepassing voor de overheid. Bovendien biedt BZK aan alle overheidsorganisatie ondersteuning bij alle aspecten van informatiebeveiliging door middel van kennisdeling. Dit gebeurt met name via het Centrum van Informatiebeveiliging en Privacy (CIP) die kennisproducten maakt en ter beschikking stelt. Voorbeelden zijn handreikingen die helpen bij de implementatie van de BIO of webinars en themabijeenkomsten over dit onderwerp. Ook organiseert BZK jaarlijks een overheidsbrede cyberoefening die organisaties helpt bij het organiseren van hun eigen incident- en crisisbeheer.

Bijdrage aan vermindering regeldruk
Reeds voorafgaand aan de onderhandelingen over de NIS2-richtlijn heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties met de verschillende bestuurslagen vanaf het voorjaar van 2019 ambtelijk overleg gevoerd om wetgeving voor te bereiden ter zake van de informatieveiligheid van de overheid.[19] Deze wetgeving moest een eerste stap zijn om een veelheid aan interbestuurlijke informatiebeveiligingseisen en toezicht daarop bij de medeoverheden te vereenvoudigen. Deze vereenvoudiging heeft als doel om de lastendruk bij medeoverheden, die zich nu vooral voordoet bij gemeenten, te verlagen. Het ENSIA-initiatief[20] is een goede illustratie van het verlagen van de lastendruk en wordt al een aantal jaar door gemeenten gebruikt voor hun geharmoniseerde verantwoording over informatiebeveiliging. Het verder brengen van deze harmonisering is bovendien als ambitie opgenomen in de Werkagenda Waardengedreven Digitalisering.[21]

De NIS2-richtlijn geeft de mogelijkheid om de eerste stap van deze ambitie versneld te realiseren. Hierover zijn de verschillende bestuurslagen formeel per brief geïnformeerd op 20 november 2023.[22] Bij het opstellen van lagere regelgeving onder de Cbw is, met het oog op het beperken van de lastendruk, voor medeoverheden het voornemen om maximaal gebruik te maken van bestaande verplichtingen. Voor de nadere invulling van de zorgplicht voor de overheid wordt gebruikgemaakt van de herziene Baseline Informatiebeveiliging Overheid (BIO), waaraan alle overheidslagen zich eerder hebben gecommitteerd.[23] De totstandkoming van de BIO heeft bovendien plaatsgevonden onder coördinatie van Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in samenwerking met alle bestuurslagen. Dit zijn om die reden geen nieuwe verplichtingen.

Advies en consultatie
Internetconsultatie
PM Consultatie en toetsing

Toezichts- en handhavingstoets Rijksinspectie voor Digitale Infrastructuur
PM Consultatie en toetsing wordt pas opgenomen na de internetconsultatie.

---

[19] Wetgeving werd al genoemd als mogelijk instrument in de *Eindrapportage Taskforce Bestuur & Informatieveiligheid Dienstverlening*, februari 2015.
[20] Dit staat voor *Eenduidige Normatiek Single Information Audit*. ENSIA is een initiatief van gemeenten, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Ministerie van Sociale Zaken en Werkgelegenheid. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatiebeveiliging en informatiekwaliteit. Meer informatie is terug te vinden op www.ensia.nl.
[21] *Kamerstukken II* 2022/23, 26643, nr. 940, bijlage 1062267, paragraaf 2.4.
[22] *NIS2 bij de overheid,* https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/nis2-bij-de-overheid-kamerbrief/.
[23] *Stcrt.* 2019, 26526.

Inwerkingtreding

Deze regeling geeft nadere regels onder de Cbw en de Cbb. Om die reden zal deze regeling op hetzelfde moment als de Cbw en Cbb in werking treden.

Concept

ARTIKELSGEWIJZE TOELICHTING

Artikel 1
Op grond van artikel 1 van de Cbw en artikel 1 van het Cbb zijn de in die artikelen genoemde begripsbepalingen ook van toepassing op deze regeling. In artikel 1 van deze regeling wordt een aantal begrippen omschreven, die specifiek voor deze regeling van belang zijn.

Artikel 2
Deze bepaling beperkt de reikwijdte van deze regeling tot de entiteiten die vallen onder de sector overheid, bedoeld in bijlage 1 bij de Cbw, met uitzondering van de waterschappen, waarvoor de Minister van Infrastructuur en Waterstaat de bevoegde autoriteit is.

Artikel 3
Met deze bepaling wordt de IBD aangewezen als CSIRT voor de entiteitssoorten gemeenten en openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties als bedoeld in artikel 8, eerste, tweede, onderscheidenlijk derde lid, van de Wet gemeenschappelijke regelingen , voor zover die laatste voldoen aan de criteria voor overheidsinstanties en er ten minste één gemeente aan deelneemt. Hierbij kan gedacht worden aan een belastingsamenwerking of een omgevingsdienst.

Voor alle andere overheidsentiteiten geldt op basis van artikel 2, eerste lid, van het Cbb dat het NCSC aangewezen wordt als CSIRT.

Artikel 4
PM

Artikel 5
PM

Artikel 6
Deze bepaling verplicht tot de toepassing van de NEN-EN-ISO/IEC 27001:2023, de beheersmaatregelen van de NEN-EN-ISO 27002:2022 en de overheidsmaatregelen van de BIO2. Overheidsorganisaties zijn al bekend met beide ISO-standaarden en de BIO2. De voorganger van de BIO2, de Baseline Informatiebeveiliging Overheid, gold als verplichtende zelfregulering.

Met deze bepaling wordt de toepassing van deze standaarden wettelijk vastgelegd, voor zover de standaarden zien op de beveiliging van netwerk- en informatiesystemen. Deze beperking is noodzakelijk, omdat deze standaarden zien op informatiebeveiliging in bredere zin, inclusief bijvoorbeeld informatie die op papier staat. Dit valt buiten de reikwijdte van de NIS2-richtlijn en daardoor ook van de Cbw en lagere regelgeving. Toepassing ervan kan dus niet in deze regeling worden verplicht.

De verwijzingen naar de beide ISO-standaarden en naar de BIO2 betreffen statische verwijzingen naar een specifieke versie. Dat betekent dat een wijziging van de ISO-standaarden en de BIO2 niet automatisch leidt tot het verplicht worden van de nieuwe versie onder deze regeling. In plaats daarvan zal er altijd een wijziging moeten worden aangebracht in deze regeling om die nieuwe versie van toepassing te laten zijn. Zo wordt gegarandeerd dat een wijziging van de inhoud van deze regeling altijd plaatsvindt nadat hier een weloverwogen besluit over is genomen.

Het eerste lid verplicht de entiteit om de NEN-EN-ISO/IEC 27001:2023 toe te passen op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor beveiliging van informatie in netwerk- en informatiesystemen. Ook moet deze standaard worden toegepast op het vaststellen van het toepassingsgebied van het managementsysteem. Doorgaans zal een dergelijk managementsysteem ook zien op beveiliging van informatie buiten netwerk- en informatiesystemen. Dat is vanzelfsprekend toegestaan, maar zoals hiervoor is uiteengezet, beperkt deze regeling zich tot netwerk- en informatiesystemen.

Verder moet de entiteit passende beheersmaatregelen formuleren. Hiervoor gelden op grond van het tweede lid de beheersmaatregelen uit de NEN-EN-ISO/IEC 27002:2022 en de

overheidsmaatregelen uit deel 2 van de BIO2 als kader. De overige teksten uit de NEN-EN-ISO/IEC 27002:2022 en BIO2 bestaan uit inleiding en toelichting en zijn louter informatief van aard. Deze teksten kunnen nuttig zijn bij het formuleren van de beheersmaatregelen, maar worden niet verplicht gesteld in deze regeling.

Dat de entiteit 'passende' beheersmaatregelen moet formuleren, betekent dat rekening moet worden gehouden met de omgeving(en) waarin de informatiebeveiligingsrisico's gelden, gebaseerd op de scope en de onderkende risico's. 'Passend' houdt ook in dat de beheersmaatregelen uit NEN-EN-ISO/IEC 27002 en de overheidsmaatregelen uit de BIO2 kunnen worden vervangen door of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen. Hierbij kan worden gedacht aan NEN 7510 voor zorginformatie en de CyberSecurity ImplementatieRichtlijn (CSIR) en IEC 62443 Industriële cybersecurity voor Operationele Technologie (OT). De entiteit dient wel aannemelijk te maken dat het vervangen door of combineren met beheersmaatregelen uit andere normen en richtlijnen noodzakelijk is. Ook is het aan de entiteit om aannemelijk te maken dat die beheersmaatregelen gelijkwaardig zijn.

Enkele beheersmaatregelen uit de NEN-EN-ISO/IEC 27002:2022 en daaraan gekoppelde overheidsmaatregelen uit de BIO2 vallen buiten de reikwijdte van de Cbw. Toepassing daarvan wordt daarom in deze regeling niet verplicht gesteld. Een voorbeeld hiervan is een beheersmaatregel die ziet op de bescherming van intellectuele-eigendomsrechten. Dit is een onderwerp dat de Cbw niet regelt. In de BIO2 is door middel van het aanbrengen van een grijze tekstmarkering duidelijk gemaakt welke overheidsmaatregelen buiten de reikwijdte van de Cbw en dus van deze regeling vallen. Voor de in de BIO2 gemarkeerde overheidsmaatregelen geldt dat ook de bijbehorende beheersmaatregelen uit de NEN-EN-ISO/IEC 27002:2022, waarnaar de eerste drie cijfers van de overheidsmaatregelen in de BIO2 verwijzen, buiten de reikwijdte van deze regeling vallen.

Het derde lid verplicht de entiteit ertoe om ervoor zorg te dragen dat de opzet, het bestaan en de werking van de passende beheersmaatregelen aantoonbaar zijn. De BIO2 omvat maatregelen op tactisch niveau. Dit betekent dat deze maatregelen door de entiteit eerst geoperationaliseerd worden voordat ze geïmplementeerd kunnen worden. Deze implementatie moet risicogericht zijn en voldoen aan best practices en marktstandaarden. Onderdeel van de operationalisatie is het kunnen detecteren of de maatregel goed functioneert. Over het hele ontwerp moet worden geborgd dat uitval van één maatregel niet leidt tot een directe kwetsbaarheid in het hele systeem. Hoe de maatregelen zijn geoperationaliseerd, moet via verwijzingen worden vastgelegd. Hiermee toont een entiteit de 'opzet' van maatregelen aan. Al dan niet met behulp van externe partijen of via self-assessments, audits, pentesten, redteam-testen en dergelijke toont een entiteit het 'bestaan' en de 'werking' van maatregelen aan.

Artikel 7

Deze bepaling verplicht entiteiten in de subsector centrale overheden om de diensten die essentieel zijn te identificeren en daarvan een overzicht bij te houden. Dit wordt gedaan door middel van de tabel die is opgenomen als bijlage 1 bij deze regeling. Deze tabel is gebaseerd op de tabel die is opgenomen in de Leidraad te beschermen belangen (TBB). Daarmee kan worden bepaald wat de verwachte gevolgen zijn bij een incident dat betrekking heeft op de betreffende dienst.

Een dienst is essentieel als die binnen minimaal één van de categorieën, bijvoorbeeld 'schade aan vitale belangen van de staat of de samenleving', voldoet aan een drempelwaarde van ten minste niveau TBB 3 of hoger (TBB 2 of TBB 1). Als bijvoorbeeld in één categorie sprake is van het voldoen aan TBB 3 en in de rest van de categorieën gaat het om TBB 4, dan is er niettemin sprake van een essentiële dienst.

Artikel 8

Deze bepaling verplicht entiteiten in de subsector decentrale overheden om de diensten die als essentieel kunnen worden beschouwd, te identificeren en daarvan een overzicht bij te houden. Dit wordt gedaan door middel van de tabel die is opgenomen als bijlage 2 bij deze regeling, die is gebaseerd op de impacttabel die is uitgegeven door de Informatiebeveiligingdienst (IBD) van de

Vereniging van Nederlandse Gemeenten (VNG). Een dienst is essentieel als die in minimaal één van de categorieën, bijvoorbeeld 'schade bij openbaarmaking', voldoet aan een drempelwaarde van ten minste niveau 'hoog' of 'zeer hoog'. Als bijvoorbeeld in één categorie sprake is van het voldoen aan niveau 'hoog' en in de rest van de categorieën betreft het niveau 'laag', dan is er niettemin sprake van een essentiële dienst.

In de categorieën waar ook een passage is opgenomen over het "effect op burgergerichte processen", hoeft niet aan beide genoemde situaties voldaan te zijn. Niet alle decentrale overheden zullen immers te maken hebben met burgergerichte processen. Om in de categorie te vallen is het voldoende dat wordt voldaan aan de eerste alinea van de betreffende categorie.

Artikel 9
Met dit artikel worden de drempelwaarden voor significante incidenten als bedoeld in artikel 25 van de wet geregeld voor de subsector centrale overheid.

Het eerste lid stelt met betrekking tot de essentiële diensten die conform artikel 7 van deze regeling zijn geïdentificeerd dat elk incident te gelden heeft als een significant incident. Er is ingevolge artikel 1 van de wet sprake van een incident als een gebeurtenis de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt. Wanneer een dergelijk incident plaatsvindt met betrekking tot een essentiële dienst, is het, ongeacht de hoeveelheid schade, altijd meldplichtig.

Voor niet-essentiële diensten zijn in het tweede lid specifieke drempelwaarden opgenomen die gebaseerd zijn op een aantal van de criteria uit de Leidraad voor te beschermen belangen.

Het derde lid zondert een verstoring van de beschikbaarheid van zowel essentiële als niet-essentiële diensten in verband met voorziene gevolgen voor netwerk- en informatiesystemen, zoals bij gepland onderhoud of testen, uit van de meldplicht.

Artikel 10
Met dit artikel worden de drempelwaarden voor significante incidenten als bedoeld in artikel 25 van de wet geregeld voor de subsector decentrale overheden.

Het eerste lid stelt met betrekking tot de essentiële diensten die conform artikel 8 van deze regeling zijn geïdentificeerd dat elk incident te gelden heeft als een significant incident. Er is ingevolge artikel 1 van de wet sprake van een incident als een gebeurtenis de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt. Wanneer een dergelijk incident plaatsvindt met betrekking tot een essentiële dienst, is het, ongeacht de hoeveelheid schade, altijd meldplichtig.

In het tweede lid zijn voor niet-essentiële diensten drempelwaarden opgenomen. Het gaat om gevallen waar een incident op een niet-essentiële dienst schade veroorzaakt die in omvang vergelijkbaar is met een incident op een essentiële dienst. De waarden zijn daarom ontleend aan de tabellen in bijlage 1 en bijlage 2.

Het derde lid zondert een verstoring van de beschikbaarheid van zowel essentiële als niet-essentiële diensten in verband met voorziene gevolgen voor netwerk- en informatiesystemen, zoals bij gepland onderhoud of testen, uit van de meldplicht. Zo mogen onderhoudswerkzaamheden die leiden tot beperkte beschikbaarheid of niet-beschikbaarheid van de dienst niet als significante incidenten worden beschouwd. Wanneer een dienst niet beschikbaar is als gevolg van geplande onderbrekingen, zoals onderbrekingen of niet-beschikbaarheid op basis van een vooraf bepaalde contractuele overeenkomst, mag dit ook niet als een significant incident worden beschouwd.

Artikel 11
Dit artikel regelt de inwerkingtreding van deze regeling. De regeling zal tegelijkertijd met de Cbw en het Cbb in werking treden.

Concept

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,