centrum informatiebeveiliging en privacybescherming

De betekenis van Wbni (NL) en NIB (EU) voor aanbieders binnen de overheid

Analyse en conclusie

februari 2023 [versie 1.1 definitief]

De betekenis van Wbni (NL) en NIB (EU) voor aanbieders binnen de overheid

Titel	De betekenis van Wbni (NL) en NIB (EU) voor aanbieders binnen de overheid
Datum	februari 2023
Versie en status	1.1 definitief
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Individuele praktijk

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt. Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Managementsamenvatting

De Netwerk- en informatiebeveilgingsrichtlijn (NIB richtlijn) en de Wet Beveiliging Netwerk en informatiesystemen (Wbni) kennen een zorgplicht en stellen daarbij globale beveiligingseisen (‘een open norm’) aan digitale dienstverleners (DSP’s). Daarnaast eisen de NIB en de Wbni het nemen van passende en evenredige technische en organisatorische maatregelen aan Aanbieders van Essentiële Diensten (AED’s). Aan overige aanbieders worden geen eisen gesteld aan de beveiliging van hun netwerk- en informatiesystemen. Wel geldt voor alle aanbieders die onder de NIB-richtlijn vallen een meldplicht voor ICT-incidenten.

De NIB-richtlijn is alleen van toepassing op overheidsdiensten die aangemerkt worden als Aanbieder van essentiële diensten (AED). Voor Nederland (en de andere lidstaten) geldt dat de overige overheidsdiensten verantwoordelijk blijven om te zorgen voor de beveiliging van netwerk- en informatiesystemen van overheidsdiensten die niet binnen de werkingssfeer van deze richtlijn vallen. Nederland hanteert hiervoor de Baseline Informatiebeveiliging Overheid (BIO). Zoals ook bij de BIO blijft bij de NIB en de Wbni de verantwoordelijkheid voor het bieden van een passend beveiligingsniveau bij de aanbieder van de digitale dienst. Het is dus in eerste instantie aan de organisaties zelf om te bepalen welke concrete maatregelen voor hen passend en evenredig zijn. De Wbni biedt echter wel de mogelijkheid om desgewenst, bij of krachtens algemene maatregel van bestuur (amvb), voor AED’s of DSP’s (of voor bepaalde categorieën daarvan) nadere regels te stellen over de te treffen beveiligingsmaatregelen.

Vanuit de NIB en de Wbni worden geen inhoudelijke eisen gesteld aan de zorg- en meldplicht, hierdoor wordt met de BIO als normenkader invulling gegeven aan de zorgplicht vanuit de NIB en de Wbni. Wel is ten aanzien van de meldplicht uitbreiding van de BIO-normen nodig; de BIO kent geen meldingsplicht, tenzij het incidenten op BBN-2 niveau zijn. Voor de aanbieders binnen de overheid is het van belang te weten hoe invulling wordt gegeven aan het toezicht door de bevoegde autoriteit, zodat de impact van het toezicht in de kwaliteitsprocessen van de beveiligingsorganisatie van de aanbieders binnen de overheid kan worden meegenomen. Tevens is het de vraag of op Europees niveau een normenkader gaat worden voorgeschreven. Deze kan zodanig gaan afwijken van de BIO dat aanpassing van de BIO noodzakelijk wordt. Sterk punt ten aanzien van de BIO is dat de BIO is gebaseerd op een internationaal erkent normenkader de ISO 27002. Een normenkader op Europees niveau zal immers moeten zijn gebaseerd op een breed geaccepteerd normenkader, zoals de ISO 27002.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

In Nederland zijn bij organisaties vrijwel alle economische en maatschappelijke processen gedigitaliseerd. Deze organisaties zijn hiermee aanbieders en gebruikers van digitale diensten. In 2016 is de richtlijn Netwerk- en Informatiebeveiliging (NIB, vastgelegd in het EU directive 2016/1148[1]) een richtlijn die geldt voor (een groot deel van de) aanbieders van digitale diensten. In Nederland is deze vertaald naar de Wet beveiliging netwerk- en informatiesystemen (Wbni). De Wbni en de NIB-richtlijn gelden ook voor overheden bij het aanbieden van digitale diensten. Op basis van de Wbni, de ontwikkelingen in de NIB en de uitwerking daarvan in Europa is door het CIP een analyse gemaakt van de betekenis ervan voor de BIO in de toekomst.

Zoals ook bij de BIO blijft bij de NIB en de Wbni de verantwoordelijkheid voor het bieden van een passend beveiligingsniveau bij de aanbieder van de digitale dienst. Het is dus in eerste instantie aan de organisaties zelf om te bepalen welke concrete maatregelen voor hen passend en evenredig zijn. De Wbni biedt echter wel de mogelijkheid om desgewenst, bij of krachtens algemene maatregel van bestuur (amvb), voor AED's of DSP's (of voor bepaalde categorieën daarvan) nadere regels te stellen over de te treffen beveiligingsmaatregelen. Bij het op Europees niveau opstellen van richtsnoeren over de beveiligingsmaatregelen is het National Cyber Security Center (NCSC) vanuit Nederland betrokken.

1.2 Een overzicht

Om Nederland digitaal veiliger te maken is een deel van de aanbieders in de Wet beveiliging netwerk- en informatiesystemen (Wbni) aangemerkt als *digitale dienstverleners* (DSP's), *vitale aanbieders* (VA's) of als *overige aanbieder van de Rijksoverheid*. Voor deze organisaties bevat de Wbni wettelijke verplichtingen. Met de Wbni heeft Nederland de Europese richtlijn Netwerk- en Informatiebeveiliging (de NIB-richtlijn) van 2016 geïmplementeerd. De Wbni is daarmee de Nederlandse implementatie van de NIB-richtlijn, zoals vastgelegd in het EU directive 2016/1148[2]. De Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) is in de Wbni opgenomen[3]. De NIB-richtlijn uit 2016 duiden we hieraan als NIB-2016. De NIB bevat maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de EU en bevat een zorg- en een meldingsplicht voor (een groot deel van de) aanbieders van digitale diensten.

Door de Europese Commissie is geconstateerd dat door de toegenomen digitalisering van de markt, het verder ontwikkelen van het dreigingsbeeld en een evaluatie van de NIB-2016 noodzakelijk is deze te

---

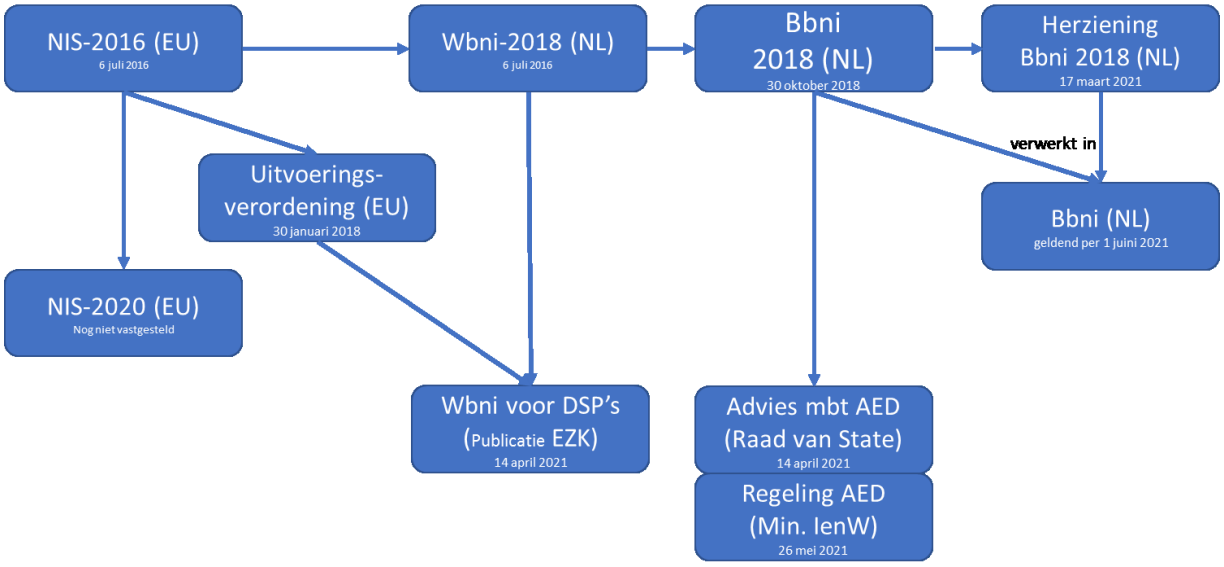
[1] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

[2] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN

[3] https://www.ncsc.nl/over-ncsc/wettelijke-taak

vervangen, waarbij voortgebouwd wordt op die van 2016. Het voorstel[4] maakt deel uit van een breder pakket aan maatregelen van de Europese Commissie op het gebied van cybersecurity en de bescherming van vitale infrastructuur. Het voorstel uit 2020 wordt hier aangeduid als NIB-2020.

Afbeelding 1 Van de aanscherping van de NIB-2016 is een eerste algemene standpuntbepaling van de Nederlandse regering gemaakt[5]. Belangrijk is te melden dan de NIB-2020 nog een voorstel is en dus nog kan wijzigen en dat de NIB-2020 (of de aangepaste versie daarvan) zal leiden tot een aanpassing van de Wbni. Het Besluit beveiliging netwerk- en informatiesystemen (Bbni) stelt regels voor de uitvoering van de Wbni en de NIB van 2016.



Afbeelding 1: De samenhang tussen de EU directives, de Wbni, de Bbni en de uitwerkingen ervan

1.3 Leeswijzer

Dit document bestaat uit 3 delen. In deel 1 wordt de Europese regelgeving en Nederlandse wetgeving op hoofdlijnen beschreven, inclusief de veranderingen die er zijn geweest en veranderingen die er met de nog in behandeling zijnde Europese regelgeving op stapel staan. De veranderingen hebben invloed op de overheid als aanbieder van digitale diensten. De betekenis voor de overheid en in het bijzonder de BIO is beschreven na een analyse van die wet- en regelgeving.

In deel 2 wordt op een dieper niveau de verplichtingen vanuit de wet- en regelgeving beschreven. Om een beter beeld te geven hoe onderscheid gemaakt bij de inhoud van de verplichtingen tussen verschillende categorieën van aanbieders, zijn ook die categorieën beschreven.

---

[4] Voorstel voor een RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148; https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52020PC0823

[5] https://www.parlement.com/id/vlgnpd2hz1ur/herziening_richtlijn_netwerk_en

In deel 3 wordt als achtergrondinformatie uitleg gegeven over de wijze hoe toezicht, handhaving, en controle, met daarbinnen de ondersteuning aan aanbieders, op nationaal en Europees niveau is voorgeschreven vanuit de Europese regelgeving en hoe deze is vormgegeven.

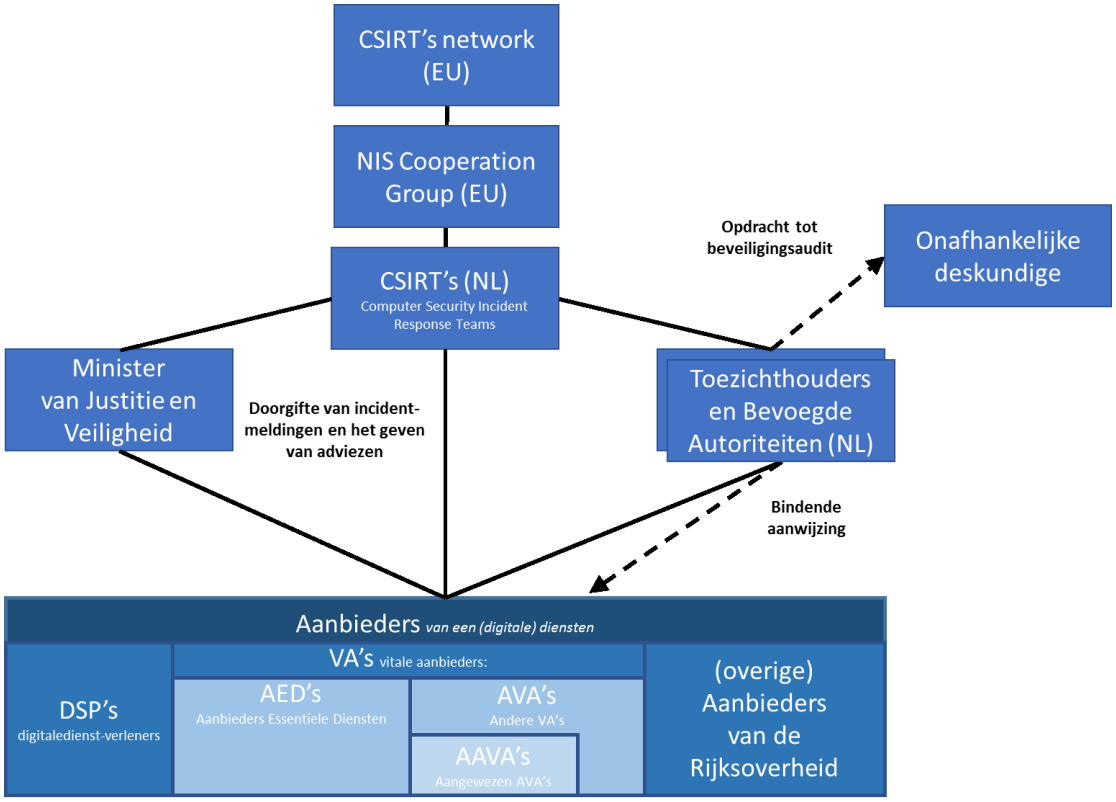
Deel 1 De wet en regelgeving en de betekenis ervan

2 De verander(en)de wet en regelgeving

2.1 Wbni

In de Wbni ligt vast voor welke aanbieders van digitale diensten de wet geldt. Hierbij kan een aanbieder worden aangeduid als *digitale dienstverleners* (DSP's), *vitale aanbieders*[6] (VA's) of als *overige aanbieder van de Rijksoverheid*. Binnen de als VA vallende aanbieders wordt onderscheid gemaakt tussen *aanbieders van essentiële diensten* (EAD's) en van *andere vitale aanbieders* (AVA's). Een deel van de AVA's kan worden aangewezen als *Aangewezen vitale aanbieder* (AAVA). Deze samenhang tussen deze vormen van aanbieders is in het onderste blok in onderstaand schema weergegeven.

Naast aanbieders beschrijft de Wbni organisaties die vanuit de Wbni en de EU Network and Information Security directive (NIS) een wettelijke taak hebben. De belangrijkste relaties tussen de aanbieders en de andere organisaties staat vereenvoudigd in onderstaand schema. Welke relaties er in detail bestaan, is beschreven in de volgende hoofdstukken.



Afbeelding 2: Bbni en de herziening Bbni

Het Besluit beveiliging netwerk- en informatiesystemen (Bbni) stelt regels voor de uitvoering van de Wbni en de NIB van 2016. Het Bbni geldt vanaf 1 juni 2021. In het Bbni staat meer precies welke

[6] Bepaalde processen zijn zo belangrijk voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur. Binnen deze processen zijn een of meerdere organisaties belangrijk voor de continuïteit en weerbaarheid van het proces. Deze organisaties worden aangeduid als vitale aanbieders.

aanbieders onder de VA's vallen en welke onder de AED's vallen. Tevens wordt in de Bbni nadere duiding gegeven aan hun verplichtingen. Overigens wordt in het Bbni daarbij een uitzondering gemaakt voor de beveiligingseisen van financiële instellingen.

Met het Bbni vervalt het Besluit meldplicht cybersecurity.

2.2 De NIB van 2020

De NIB-2020 bevat in vergelijking met de NIB-2016 een breder pakket aan maatregelen op het gebied van cybersecurity[7] en de bescherming van vitale infrastructuur[8], hierdoor wijzigt de NIB-richtlijn op meerdere onderdelen en wijzigt ook de reikwijdte, hoe aanbieders als DSP's worden aangewezen en de zorg- en meldplicht vanuit de NIB-2020 voor aanbieders van digitale diensten.

De NIB-2020 zal leiden tot een verhoging van administratieve lasten voor Rijksoverheid, decentrale overheden en het bedrijfsleven[9] en zullen aan meer organisaties worden opgelegd. In het impact assessment[10] geeft de Europese Commissie aan te rekenen op een initiële verhoging van maximaal 22% van het ICT-budget verwacht in de eerste periode (3-4 jaar) voor bedrijven die nog niet onder de NIB-2016 vallen en voor bedrijven die wel al onder de NIB-2016 vallen schat de Europese Commissie in dat dit 12% zal zijn[11].

[7] COM (2020) 18 - EU-strategie inzake cyberbeveiliging voor het digitale tijdperk

[8] COM (2020) 829 - Richtlijn veerkracht kritieke entiteiten

[9] Algemene standpuntbepaling van de Nederlandse regering; paragraaf 5d.

[10] IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

[11] Algemene standpuntbepaling van de Nederlandse regering; paragraaf 5c.

3 De betekenis voor de BIO en aanbieders binnen de overheid

3.1 Betekenis van de zorg- en de meldplicht voor de overheid en de BIO

De overheid is zich zeer bewust van het belang van een goede beveiliging van hun diensten. Inbreuken op de beveiliging van hun netwerk- en informatiesystemen raken immers direct de uitvoering van de overheidstaken. Met de BIO hanteert de overheid een normenkader met een risico gebaseerde aanpak dat een passend beveiligingsniveau biedt voor de overheid. Een meldplicht van incidenten, zoals voorgeschreven in de NIB en de Wbni, ontbreekt nog wel in de BIO.

De NIB-richtlijn en de Wbni kennen een zorgplicht en stellen daarbij globale beveiligingseisen (‘een open norm’) aan *digitale dienstverleners* (DSP’s) en eisen het nemen van passende en evenredige technische en organisatorische maatregelen aan Aanbieders van Essentiële Diensten (AED’s). Aan overige aanbieders worden geen eisen gesteld aan de beveiliging van hun netwerk- en informatiesystemen. Wel geldt voor alle aanbieders die onder de NIB-richtlijn vallen een meldplicht voor ICT-incidenten.

Hoewel vanuit de NIB en de Wbni geen inhoudelijke eisen wordt gesteld, wordt met de BIO als normenkader invulling gegeven aan de zorgplicht vanuit de NIB en de Wbni. Wel is daarbij ten aanzien van de meldplicht uitbreiding van de BIO-normen nodig; de BIO kent geen meldingsplicht, anders dan in norm 16.1.4.1 van de BIO wordt gesteld dat voor informatiebeveiligingsincidenten op BBN-2 niveau gemeld moeten worden aan het NCSC.

Voor de aanbieders binnen de overheid is het van belang te weten hoe invulling wordt gegeven aan het toezicht door de bevoegde autoriteit, zodat de impact van het toezicht in de kwaliteitsprocessen van de beveiligingsorganisatie van de aanbieders binnen de overheid kan worden meegenomen. Tevens is het de vraag of op Europees niveau een normenkader gaat worden voorgeschreven. Deze kan zodanig gaan afwijken van de BIO dat aanpassing van de BIO noodzakelijk wordt. Sterk punt ten aanzien van de BIO is dat de BIO is gebaseerd op een internationaal erkent normenkader de ISO 27002. Een normenkader op Europees niveau zal immers moeten zijn gebaseerd op een breed geaccepteerd normenkader, mogelijk de ISO 27002. Indien het normenkader op Europees niveau niet op de ISO 27002 wordt gebaseerd en de BIO wel als overheidsnormenkader gaat gelden, hetgeen vanuit harmonisering van normenkaders wel wordt geadviseerd vanuit het CIP, heeft dit gevolgen voor de BIO.

3.2 Zorgplicht: Harmonisering normen

De groeiende samenwerking op alle lagen binnen de maatschappij en daarmee ook op uitvoeringsniveau vraagt om een harmonisatie in de EU van de zorgplicht. Door de ministerraad is besloten de BIO te hanteren als gemeenschappelijk normenkader binnen de overheid. De BIO biedt in relatie tot de bedrijfsvoering binnen de overheid een passend niveau, daar waar het BBN-niveau 1 en 2 betreft. Nog niet is bepaald, bijvoorbeeld in de vorm van een algemene maatregel van bestuur, dat de BIO geldt als een normenkader dat invulling geeft aan de Wbni. Dit biedt binnen de overheid een rechtsgrond die verder gaat dan het besluit van de ministerraad.

Mogelijk biedt een besluit om de ISO 27001/2 te laten gelden voor aanbieders in andere sectoren die vallen onder de Wbni een basis voor harmonisering binnen Nederland. De BIO die een uitwerking is van de ISO 27002 geldt dan voor de overheid en de ISO 27002 voor de overige aanbieders die vallen onder

de Wbni. Hiermee wordt aangesloten op de internationaal gangbare normenkaders en wordt een additionele regeldruk voorkomen.

Europese normenkaders:
Enisa, met het NCSC als Nederlands aanspreekpunt, is gevraagd te komen met een Europees normenkader waarmee invulling wordt gegeven aan de zorgplicht. De vraag is echter op zijn plaats of Enisa zal afwijken van een internationaal gangbare normenkader. Er is hierbij dus de keuze te kiezen voor de BIO en de ISO 27002 of te wachten op een normenkader vanuit Enisa. Er zijn namelijk ook andere internationale best practices, zoals het NIST Framework for Improving Critical Infrastructure Cybersecurity.

3.3 Meldplicht

Inbreuken die ernstige gevolgen kunnen hebben (‘de bijna-ongelukken’) hoeven alleen gemeld te worden bij de toezichthouder en niet bij de bevoegde autoriteit, terwijl echte ongelukken zowel bij de hulpverlenende instantie (CSIRT) als de toezichthouder gemeld moeten worden. Het doel ervan is om de bevoegde autoriteit zo vroeg mogelijk op de hoogte te brengen van inbreuken die aanzienlijke gevolgen kunnen hebben voor de continuïteit van voor de samenleving vitale diensten, en daardoor in staat te stellen om, ter voorkoming of beperking van maatschappelijke ontwrichting, getroffen organisaties al in een vroeg stadium bijstand te verlenen bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen en waar aangewezen ook andere vitale en rijksoverheidsorganisaties te waarschuwen en te adviseren. Om deze reden hoeven bijna-ongelukken alleen gemeld te worden bij de bevoegde autoriteit en niet ook bij de toezichthouder. Op grond van de Wbni hebben vitale aanbieders en aanbieders van essentiële diensten (AED’s) in geval van ernstige incidenten een meldplicht bij het NCSC. AED’s melden ook bij hun sectorale toezichthouder. Digitale dienstverleners melden bij het CSIRT voor DSP’s.

3.4 Toezicht

Toezicht en handhaving vinden plaats bij incidenten met aanzienlijke gevolgen voor de continuïteit van een dienst. Het toezicht wordt uitgevoerd door “bevoegde autoriteiten”. Een bevoegde autoriteit heeft bestuursrechtelijk tot taak er voor zorg te dragen dat de uit de NIB en de Wbni voortvloeiende taken worden uitgevoerd. Zij hebben de mogelijkheid van het nemen van maatregelen als er “bewijzen” zijn. Zo heeft de bevoegde autoriteit toezichtsbevoegdheden en handhavingsinstrumenten, waarover de autoriteiten minimaal beschikken onder een regime van ex-ante toezicht (“toezicht vooraf”) en belangrijke entiteiten onder een regime van onder ex-post toezicht (“toezicht achteraf”). De bevoegde autoriteit kan daartoe een beveiligingsaudit laten uitvoeren. Hierna kan de bevoegde autoriteit, door middel van het geven van een bindende aanwijzing, verplichtingen opleggen tot het nemen van maatregelen.

Is er sprake van een dreiging of een incident dan zijn er computercrisisteams die hulpverlenen. In de Wbni worden deze teams CSIRT genoemd: Computer Security Incident Response Teams.

Deel 2: Verplichtingen voor de aanbieders

4 Zorgplicht: verplichte beveiliging

4.1 Wbni en de NIB van 2016

Wie	Maatregel
AED	**Risico's beheersen:** Het nemen van passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. De maatregelen zorgen, gezien de stand van de techniek, voor een niveau van beveiliging dat is afgestemd op de risico's die zich voordoen[12].
DSP	**Risico's beheersen:** Het nemen van nemen passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen[13], rekening houdend met[14]: a. de beveiliging van systemen en voorzieningen; b. behandeling van incidenten; c. het beheer van de bedrijfscontinuïteit; d. toezicht, controle en testen; e. inachtneming van de internationale normen.
AED, DSP	**Incidenten voorkomen en gevolgen van incidenten beperken:** Het nemen van passende maatregelen om incidenten die de beveiliging van de voor de verlening van de betrokken dienst gebruikte netwerk- en informatiesystemen aantasten, te voorkomen en de gevolgen van dergelijke incidenten zo veel mogelijk te beperken, teneinde de continuïteit van die dienst te waarborgen[15].
AED, DSP	Krachtens algemene maatregel van bestuur nader gegeven regels over de bovenstaande beveiligingsverplichtingen[16].

Tabel 1: verplichtte beveiliging

[12] Wbni art7, lid 1

[13] Wbni art 7 lid 1

[14] Wbni art 7 lid 2

[15] Wbni art 8

[16] Wbni art 9

4.2 NIB van 2020

Ten opzichte van de NIB-richtlijn van 2016 worden in de NIB-richtlijn van 2020 nadere eisen gesteld met betrekking tot het voldoen aan de zorgplicht[17] en de meldplicht[18] door essentiële en belangrijke entiteiten:

1. Is er een lijst met soorten beveiligingsmaatregelen toegevoegd, die genomen moeten worden om aan de zorgplicht te voldoen, waar aanbieders sowieso aan moeten voldoen (zoals beveiliging van de toeleveringsketen en afhandeling van incidenten).
2. Kan de Europese Commissie middels gedelegeerde- en uitvoeringsbesluiten de beveiligingsmaatregelen nader specificeren en daar extra soorten maatregelen aan toevoegen.
3. Kan de Europese Commissie via gedelegeerde besluiten nader bepalen aan welke categorieën essentiële entiteiten certificeringsverplichtingen worden opgelegd.
4. Voor aanbieders van openbare elektronische communicatienetwerken en/of -diensten en aanbieders van vertrouwensdiensten (bijv. het certificaat voor authenticatie van een website), wordt de zorg- en meldplicht uit de respectievelijke sectorale Europese wetgeving verschoven naar de NIB-2020, onder intrekking van de betrokken bepalingen in die sectorale Europese regelgeving.
5. Kan het bestuur van een organisatie aansprakelijk kan worden gesteld voor bijvoorbeeld het niet-naleven van de zorgplicht door hun organisatie.

[17] De eis aan AED's en DSP's om passende technische en organisatorische maatregelen te nemen om hun netwerken informatiesystemen te beveiligen

[18] De verplichting om incidenten met aanzienlijke gevolgen voor de dienstverlening te melden.

5 Verplichte meldplicht voor incidenten

5.1 Wbni en de NIB van 2016

Wie	Maatregel
VA	Het onmiddellijk melden aan Onze Minister van Justitie en Veiligheid van[19]: a. een incident met aanzienlijke gevolgen voor de continuïteit van de door hem verleende dienst; b. een inbreuk op de beveiliging van netwerk- en informatiesystemen die aanzienlijke gevolgen kan hebben voor de continuïteit van de door hem verleende dienst.
AED	Het onmiddellijk melden van een incident aan de bevoegde autoriteit van[20]: a. een incident met aanzienlijke gevolgen voor de continuïteit van de door hem verleende dienst; b. een inbreuk op de beveiliging van netwerk- en informatiesystemen die aanzienlijke gevolgen kan hebben voor de continuïteit van de door hem verleende dienst.
DSP	Het onmiddellijk melden van een incident, ook als de DSP niet valt onder de jurisdictie van Nederland[21], bij Onze Minister van Justitie en Veiligheid en bij de bevoegde autoriteit van: a. een incident dat aanzienlijke gevolgen heeft voor de continuïteit van zijn essentiële dienst[22]. b. de contactgegevens van de functionaris die verantwoordelijk is voor het doen van de melding.
VA, EAD	Om te bepalen of een incident aanzienlijke gevolgen heeft voor de continuïteit van de essentiële dienst, worden in elk geval in aanmerking genomen[23]: a. het aantal gebruikers dat door de verstoring van de dienst wordt getroffen; b. de duur van het incident; c. de omvang van het geografische gebied dat door het incident is getroffen. Voor een AED is dit bij[24]: 1. Niet beschikbaarheid van de dienst in de EU van meer dan 5.000.000 gebruikersuren[25]; 2. Gevolgen voor integriteit, authenticiteit of vertrouwelijkheid met negatieve gevolgen voor meer dan 100.000 gebruikers in de EU; 3. Meer dan 1.000.000 Euro schade voor één of meer gebruikers binnen de EU; 4. Een risico voor de openbare veiligheid; 5. Een risico voor de openbare beveiliging; 6. Een (indirect) risico op een verlies van mensenlevens.

[19] Wbni art 10, lid 1 en lid 2

[20] Wbni art 10, lid 1 en lid 2

[21] Wbni art 10, lid 4

[22] Wbni art 10, lid 3

[23] Wbni art 10, lid 4

[24] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners/Wet+Beveiliging+Netwerk-+en+Informatiesystemen+%28Wbni%29+voor+digitale+medewerkers.pdf; pagina 10

[25] Aantal gebruikers x aantal uren dat de dienst niet beschikbaar is.

	De melding omvat in ieder geval: a. de aard en omvang van het incident; b. het vermoedelijke tijdstip van de aanvang van het incident; c. de mogelijke gevolgen in en buiten Nederland van het incident; d. een prognose van de hersteltijd; e. zo mogelijk, de door de aanbieder genomen of te nemen maatregelen om de gevolgen van het incident te beperken of herhaling hiervan te voorkomen.
AVA	Desgevraagd verstrekt de aanbieder die een melding heeft gedaan bij Onze Minister van Justitie en Veiligheid ook onmiddellijk alle overige gegevens die noodzakelijk zijn om[26]: a. de aanbieder bij te staan bij het treffen van maatregelen om de continuïteit van zijn diensten te waarborgen of te herstellen; b. de risico's in te schatten voor de netwerk- en informatiesystemen van vitale aanbieders, en van andere aanbieders die onderdeel zijn van de rijksoverheid. Dit geldt ook als de aanbieder een incident heeft gemeld bij de bevoegde autoriteit en deze de door haar ontvangen gegevens heeft verstrekt aan Onze Minister van Justitie en Veiligheid[27].
DSP	Het onmiddellijk melden van een incident bij Onze Minister van Justitie en Veiligheid en bij de bevoegde autoriteit van een incident dat aanzienlijke gevolgen heeft voor de continuïteit van zijn essentiële dienst[28]. Dit geldt alleen als de DSP toegang heeft tot de informatie die nodig is om te beoordelen of het incident aanzienlijke gevolgen heeft[29].Desgevraagd verstrekt de DSP het CSIRT voor digitale diensten onverwijld alle overige gegevens die noodzakelijk zijn om[30]: a. de DSP bij te staan bij het treffen van maatregelen om de continuïteit van zijn diensten te waarborgen of te herstellen; a. de risico's in te schatten voor de netwerk- en informatiesystemen van andere DSP's.
DSP	Om te bepalen of een incident aanzienlijke gevolgen heeft als bedoeld in het eerste lid, worden in elk geval in aanmerking genomen[31]: a. het aantal gebruikers dat door de verstoring van de dienst wordt getroffen; b. de duur van het incident; c. de omvang van het geografische gebied dat door het incident is getroffen. d. de omvang van de verstoring van de werking van de dienst; e. de omvang van de gevolgen voor de economische en maatschappelijke activiteiten.

Tabel 2: Verplichte meldplicht voor incidenten

[26] Wbni art 12, lid 1

[27] Wbni art 12, lid 2

[28] Wbni art 13, lid 1

[29] Wbni art 13, lid 3

[30] Wbni art 14

[31] Wbni art 13, lid 2

5.2 NIB van 2020

Ten opzichte van de NIB-richtlijn van 2016 worden in de NIB-richtlijn van 2020 nadere eisen gesteld met betrekking tot het voldoen aan de meldplicht[32] door essentiële en belangrijke entiteiten:

1. Is er een nadere omschrijving van incidenten die gemeld moeten worden;
2. Is er een verbreding van de meldplicht (zoals de verplichting om afnemers van hun dienstverlening te informeren);
3. Is er een nadere invulling van de meidprocedure;
4. Dienen essentiële en belangrijke entiteiten door lidstaten ook aangemoedigd te worden om incidenten waarbij het vermoeden van zware criminele activiteit bestaat te melden aan de relevante opsporingsinstanties. Daarbij kunnen Europol en ENISA een faciliterende rol spelen, of kan een nationale CSIRT bijvoorbeeld een aanbieder adviseren om aangifte te doen.

[32] De verplichting om incidenten met aanzienlijke gevolgen voor de dienstverlening te melden.

6 Vrijwillige melding van incidenten

6.1 Wbni en de NIB van 2016

Wie	Maatregel
Allen	Als een incident aanzienlijke gevolgen heeft voor de continuïteit van een dienst maar niet valt onder de meldplicht voor incidenten, kan de betrokken dienstverlener dat incident melden bij Onze Minister van Justitie en Veiligheid[33]. (De melding wordt niet in behandeling als dat hem onevenredig of overmatig zou belasten, maar kan ook worden doorgestuurd naar: een ander CSIRT; a. een ander computercrisisteam, aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie.)

Tabel 3: Vrijwillige melding van incidenten

6.2 NIB van 2020

De NIB-2020 spreekt niet voer vrijwillige melding van incidenten, maar van vrijwillige melding van relevante informatie, te weten significante incidenten, cyberbedreigingen of bijna-ongelukken. De vrijwillige melding geldt ook voor entiteiten die buiten het toepassingsgebied van deze richtlijn vallen. Vrijwillige rapportage mag niet leiden tot het opleggen van bijkomende verplichtingen aan de rapporterende entiteit, waaraan zij niet onderworpen zou zijn geweest, indien zij de melding niet had ingediend.

[33] Wbni art 16, lid 1

7 Voor wie geldt de Wbni en de NIB

Er wordt onderscheid gemaakt tussen verschillende aanbieders. Binnen de NIB en de Wbni wordt onderscheid gemaakt tussen:

7.1 Digitale dienstverleners (DSP's)

DSP's betreft elke rechtspersoon die een digitale dienst aanbiedt. Een dienst is hierbij[34] een dienst van de informatiemaatschappij, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht. De volgende soorten digitale diensten vallen hieronder[35]:

a) Online marktplaats[36]
b) Online zoekmachine[37]
c) Cloud computerdiensten[38]

Tenzij:

- bij algemene maatregel van bestuur is bepaald dat de NIB niet geldt voor bepaalde categorieën van essentiële diensten of DSP's[39].
- Er sprake is van micro-ondernemingen en kleine ondernemingen[40], ofwel als er minder dan 50 medewerkers zijn en het balans totaal of jaaromzet niet meer is dan 10 miljoen Euro[41].

Indien een DSP een Europese hoofdvestiging heeft in een andere EU-lidstaat, dan valt de DSP onder de wetgeving van dat land. Indien er geen Europese hoofdvestiging is, moet er een vertegenwoordiger in een EU-lidstaat zijn aangewezen.

7.2 Vitale aanbieders (VA's)

Vitale aanbieders (VA's) zijn partijen die een dienst aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. De vakdepartementen zijn beleidsmatig verantwoordelijk voor de vraag welke aanbieders beschouwd moeten worden als vitaal. Vitale aanbieders worden door de respectievelijke vakdepartementen hierover geïnformeerd. Volgens de NIS zijn de VA's:

a) aanbieders van een essentiële dienst;

---

34 Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad (17), art 1, lid 1, onder b)

35 NIB-2016, bijlage III

36 NIB-2016; Artikel 4, 17e lid en overweging nr. 15

37 NIB-2016; Artikel 4, 18e lid en overweging nr. 16

38 NIB-2016; Artikel 4, 19e lid en overweging nr. 17

39 Wbni art 6

40 NIB-2016 art 16, lid 11

41 Om te bepalen of je een DSP bent, kun je het schema hanteren op pagina 5 van: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners/Wet+Beveiliging+Netwerk-+en+Informatiesystemen+%28Wbni%29+voor+digitale+medewerkers.pdf

b) aanbieders van een andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving.

c) Aangewezen vitale aanbieders (hier aangeduid als AVA), zijnde bij algemene maatregel van bestuur of bij besluit van een bij die maatregel genoemd bestuursorgaan aangewezen:

   i) aanbieders van een essentiële dienst of categorieën van zodanige aanbieders;

   ii) andere vitale aanbieders of categorieën van zodanige aanbieders.

7.3 Aanbieders van een essentiële dienst (EAD)

De meeste vitale aanbieders worden in of op grond van het Besluit beveiliging netwerk- en informatiesystemen (Bbni) aangewezen als aanbieder van een essentiële dienst (AED).
In de NIB wordt een EAD aangeduid als[42]:

a) een entiteit verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten;
b) de verlening van die dienst is afhankelijk van netwerk- en informatiesystemen, en
c) een incident zou aanzienlijke verstorende effecten hebben voor de verlening van die dienst, waarbij[43]:
d) de aanbieder een publieke of private entiteit is, waarvan de soort is vermeld in bijlage II van NIB-2016.

In de nieuwe NIB van 2020 wijzigt het aanwijzen van AED's:

1. Moeten DSP's, weer met een uitzondering voor kleine en micro-organisaties, automatisch aan de NIB van 2020 voldoen[44].
2. Is er een uitgebreidere opsomming van sectoren, waarbinnen sprake is van 'essentiële entiteiten. Hierdoor vallen ook de afvalwater, overheidsdiensten en ruimtevaart onder de NIB-2020.

7.4 Andere VA (AVA)

Naast de AED's zijn er ook andere vitale aanbieders van een digitale dienst als categorie beschreven. Dit zijn aanbieders, waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving .

7.5 ('andere aangewezen vitale aanbieder', AAVA)

Een deel van de AVA's kan zijn aangewezen als vitale aanbieder. Deze worden aangeduid als 'andere aangewezen vitale aanbieder' (AAVA).

---

[42] NIB-2016 art 5, lid 2

[43] NIB-2016 art 4, punt 4

[44] De huidige richtlijn omvat publieke en private organisaties in zeven sectoren (energie, vervoer, bankwezen, infrastructuur voor de financiële markt, zorg, drinkwater en digitale infrastructuur) en voor drie digitale diensten (online marktplaatsen, zoekmachines en cloud aanbieders).

7.6 (overige) aanbieders die onderdeel zijn van de rijksoverheid

Overige aanbieders die onderdeel zijn van de rijksoverheid zijn organisaties die behoren tot de Rijksoverheid, maar geen (al dan niet in het Bbni aangewezen) AED zijn[45]:

1. Zijn er binnen de sectoren, die al in 2016 zijn benoemd, extra subsectoren toegevoegd en is de categorie 'belangrijke entiteiten' (important entities) toegevoegd[46];
2. Verdwijnen DSP's als afzonderlijke categorie, maar de aanbieders daarbinnen, blijven binnen de reikwijdte van de richtlijn en worden verdeeld over de categorieën essentieel en belangrijk;
3. Worden essentiële entiteiten niet langer aangewezen door de lidstaten, maar worden organisaties als zodanig aangemerkt, indien ze in één van de in bijlage 1 van de NIB-2020 genoemde sectoren actief zijn. In beginsel geldt een uitzondering voor kleine en micro-aanbieders[47];
4. Worden belangrijke entiteiten niet langer aangewezen door de lidstaten, maar worden organisaties als zodanig aangemerkt, indien ze in één van de genoemde sectoren actief zijn van de bijlage 2 genoemde sectoren. Daarnaast gelden de verplichtingen in de richtlijn ook voor kleine en micro-ondernemingen in sectoren in de bijlagen, indien zij voldoen aan een van de in deze richtlijn genoemde omstandigheden (bijvoorbeeld als ze de enige aanbieder van een dienst in een lidstaat zijn);
5. Kunnen lidstaten extra entiteiten, die diensten in de lidstaat aanbieden, aanwijzen op wie de bepalingen uit de richtlijn van toepassing zijn.

[45] Wbni, Art 3, lid 1 en art 20, lid 3 en Vitale aanbieders | Wet beveiliging netwerk- en informatiesystemen | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

[46] Deze categorie omvat publieke en private organisaties in de sectoren post- en koeriersdiensten; afvalbeheer; fabricage, productie en distributie van chemicaliën; voedselproductie; verwerking en distributie; maakindustrie; en digitale aanbieders.

[47] COM (2003) 361

Deel 3: Toezicht, handhaving en ondersteuning

8 Bevoegde autoriteiten

Nederland heeft meerdere bevoegde autoriteiten. Een bevoegde autoriteit heeft bestuursrechtelijk tot taak er voor zorg te dragen dat de uit de NIB en de Wbni voortvloeiende taken van AED's en de DSP's worden uitgevoerd en is daartoe belast met de handhaving (toezicht en sancties).

8.1 Wat zijn de taken?

De taken van de bevoegde autoriteiten omvatten onder andere:

- Het monitoren van de toepassing van de NIB:
  - Het uitvoeren van "licht en reactief toezicht achteraf".
  - Het nemen van maatregelen, maar alleen als er bewijzen zijn.
- Het contactpunt om meldingen te doen[48], hiertoe:
  - Beschrijven zij de omstandigheden, waarin aanbieders van essentiële diensten incidenten moeten melden.
- Het via een centraal contactpunt melden van incidenten aan de centrale contactpunten van andere betrokken lidstaten.
- Het in stand houden van informele en betrouwbare kanalen voor informatie-uitwisseling.
- Het inbrengen van het belang van het publiek om te worden geïnformeerd over bedreigingen en moet dit belang afgewogen tegen mogelijke commerciële en imagoschade voor de aanbieders van essentiële diensten en digitale dienstverleners die incidenten melden.

8.2 Toezicht en handhaving

Wie	Maatregel
AED, DSP	**Beveiligingsaudit:** Het namens de bevoegde autoriteit bij besluit verplicht laten uitvoeren van een onderzoek door een onafhankelijke deskundige naar de verplichte beveiliging[49], hierbij: worden de resultaten van dat onderzoek binnen een bij het besluit gestelde redelijke termijn verstrekt aan de bevoegde autoriteit[50]: a. wordt het onderzoek uitgevoerd op een door de bevoegde autoriteit voorgeschreven wijze[51]; b. draagt de aanbieder de kosten van het onderzoek, tenzij bij algemene maatregel van bestuur anders is bepaald[52]; c. kunnen bij of krachtens algemene maatregel van bestuur nadere regels worden gesteld[53].
AED, DSP	**Bindende aanwijzing:** Het binnen een gestelde redelijke termijn nemen van maatregelen als niet voldaan wordt

[48] Wbni art 4, lid 1 en lid 2

[49] Wbni art 26, lid 1a

[50] Wbni art 26, lid 1b

[51] Wbni art 26, lid 2

[52] Wbni art 26, lid 3

[53] Wbni art 26, lid 4

	aan de verplichte beveiliging. De bevoegde autoriteit kan daartoe verplichten door middel van het geven van een bindende aanwijzing[54].
AED, DSP	**Last onder bestuursdwang:** De bevoegde autoriteit is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van het bepaalde bij of krachtens deze wet[55].
AED, DSP	**Bestuurlijke boete:** De bevoegde autoriteit kan aan de overtreder een bestuurlijke boete opleggen in geval van[56]: a. overtreding van het bepaalde bij of krachtens deze wet; b. overtreding van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht en is artikel 184 van het Wetboek van Strafrecht niet van toepassing[57]. Hierbij: 1. Bedraagt de boete bedraagt ten hoogste[58]: a. in geval van overtreding van artikel 12 of van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht: 1 miljoen euro; b. in geval van een andere overtreding: 5 miljoen euro. 2. Wordt de werking van het besluit tot oplegging van de boete opgeschort totdat de beroepstermijn is verstreken of, als beroep is ingesteld, op het beroep is beslist[59]. 3. Schorst de tenuitvoerlegging van een dwangbevel dat strekt tot invordering van de boete[60].

Tabel 4: Handhaving

In de NIB van 2016 wordt een nadere invulling gegeven van de toezichtsbevoegdheden en handhavingsinstrumenten waarover de autoriteiten minimaal moeten beschikken bij de uitoefening van toezicht en vallen essentiële entiteiten onder een regime van ex-ante toezicht (“toezicht vooraf”) en belangrijke entiteiten onder een regime van onder ex-post toezicht (“toezicht achteraf”).

8.3 Wie zijn de autoriteiten?

Voor zover de bevoegde autoriteit een minister is, wijst zij voor de betrokken sector of sectoren de toezichthoudende dienst aan. Voor de Digital Service Providers (DSP’s) is de minister van Economische Zaken en Klimaat belast met de handhaving van de Wbni en het Besluit beveiliging netwerk- en informatiesystemen (Bbni) [61].

[54] Wbni art 27

[55] Wbni art 27

[56] Wbni art 27, lid 1

[57] Wbni art 27, lid 5

[58] Wbni art 27, lid 2

[59] Wbni art 27, lid 3

[60] Wbni art 27, lid 4

[61] https://wetten.overheid.nl/BWBR0041520/2021-06-01

Voor aanbieders van essentiële diensten (AED's) geldt het volgende[62]:

AED-sectoren	Bevoegde autoriteit	Toezichthouder dienst
Energie	Minister van Economische Zaken en Klimaat	Agentschap Telecom
Digitale infrastructuur	Minister van Economische Zaken en Klimaat	Agentschap Telecom
Bankwezen	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Infrastructuur voor de financiële markt	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Vervoer	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport
Levering en distributie van drinkwater	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport
Gezondheidszorg	Minister voor Medische zorg en Sport	Inspectie Gezondheidszorg en Jeugd

Tabel 5: AED's

8.4 Samenwerking tussen autoriteiten

Om de gevolgen van ernstige cyberincidenten ook over de landsgrenzen heen te beperken zijn nationale contactpunten voor EU-lidstaten. Namens Nederland is dit het NCSC. Als het NCSC een melding ontvangt die ook voor andere landen relevant is en omgekeerd, wordt deze operationele informatie gedeeld met de contactpunten van de lidstaten. In de NIB van 2016 zijn er twee groepen om samenwerking tussen de lidstaten te faciliteren:

1. de NIB Samenwerkingsgroep (op strategisch niveau) en
2. het Computer Security Incident Response Team (CSIRT) Netwerk (op technisch niveau)

In de NIB van 2020 wordt in aanvulling daarop:

1. een juridische basis gecreëerd voor het Cyber Crises Liaison Organisation Network (CyCLONe) met als doel de coördinatie tussen nationale autoriteiten bij grote cyberincidenten en -crises.
2. Meer elementen die toezien op de samenwerking tussen lidstaten, zoals:
    a. de organisatie van peer reviews tussen lidstaten, waarbij onder meer de nationale capaciteiten en de effectiviteit van het CSIRT door experts uit andere lidstaten wordt beoordeeld.
    b. de vereiste aan lidstaten om een raamwerk voor coordinated vulnerability disclosure (CVD) op te zetten, inclusief het aanwijzen van een autoriteit die als bemiddelaar kan optreden tijdens een CVD-procedure:
        i. ENISA zal een register met bekende kwetsbaarheden gaan bijhouden.
        ii. Dienen lidstaten een maandelijks overzicht van ontvangen meldingen aan ENISA door te geven. Deze informatie zal worden meegenomen in de

[62] Bevoegde autoriteiten | Wet beveiliging netwerk- en informatiesystemen | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

tweejaarlijkse 'cybersecurity state of the union' die door ENISA zal worden opgesteld.

9 Computer Security Incident Response Teams (CSIRT's)

Is er sprake van een dreiging of een incident in netwerk- en informatiesystemen van vitale aanbieders, onderdelen van het Rijk of digitale dienstverleners (DSP's), dan zijn er computercrisisteams die hulp verlenen. In de Wet beveiliging netwerk- en informatiesystemen (Wbni) worden deze teams, in elk geval als het gaat om aanbieders van essentiële diensten (AED's) en DSP's, CSIRT genoemd: Computer Security Incident Response Teams.

9.1 Wat zijn de taken?

Een CSIRT is een bij koninklijk besluit aangewezen instantie[63] en heeft tot doel als computercrisisteam hulp te verlenen. Het CSIRT heeft[64] ten behoeve van voor DSP's de volgende taken[65]:

1) ten minste het:
    a) monitoren van incidenten op nationaal niveau;
    b) ten bate van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;
    c) reageren op incidenten;
    d) zorgen voor een dynamische risico- en incidentanalyse en situatiekennis;
    e) deelnemen aan het CSIRT-netwerk;
2) zorgen voor op samenwerking gerichte contacten met de particuliere sector;
3) ter bevordering van de samenwerking stimuleren de CSIRT's de vaststelling en het gebruik van gemeenschappelijke of gestandaardiseerde praktijken op het gebied van:
    a) procedures voor de behandeling van incidenten en risico's;
    b) systemen voor de classificatie van incidenten, risico's en informatie.

9.2 Wie zijn de CSIRT's

Digitale dienstverleners kunnen terecht bij het CSIRT-DSP[66]; het nationale Cyber Security Incident Response Team voor digitale dienstverleners, zijnde het CSIRT van het Ministerie van EZK. Voor AED's is het Nationaal Cyber Security Centrum (NCSC) op grond van de Wbni het CSIRT. Voor andere vitale aanbieders en onderdelen van het Rijk heeft het NCSC al de rol van computercrisisteam.

[63] Wbni art4, lid 2 punt b

[64] Wbni art 4, lid 4

[65] NIB-2016, bijlage I, punt 2

[66] www.csirtdsp.nl