VERDONCK KLOOSTER & ASSOCIATES

ONDERZOEK VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

De internationale praktijk van sturing en toezicht op vitale infrastructuren in de digitale overheid

VERDONCK KLOOSTER & ASSOCIATES

ONDERZOEK VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

Joep Janssen, Sander Vols, Stijn Hoorens, Erik Silfversten

DATUM	**19-2-2020**
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20196563
INTERNE TOETS	Pim Schouten

MANAGEMENTSAMENVATTING

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft Verdonck, Klooster & Associates (hierna: VKA) verzocht om te onderzoeken welke (bindende) maatregelen andere (EU) landen voor hun eigen vitale overheden hebben vastgesteld. VKA heeft RAND Europe gevraagd een bijdrage te leveren bij het onderzoek in de andere landen.

Het onderzoek richt zich op:

1. de wijze hoe overheden van andere met Nederland vergelijkbare landen de vitale digitale infrastructuur van de overheid vaststellen;
2. welke (typen) maatregelen zij hiervoor voorschrijven;
3. op welke wijze zij dit uitvoeren;
4. welk toezicht daarop is ingericht.

Het onderzoek is uitgevoerd bij een selectie van grotere, middelgrote en kleinere EU-landen die een hoge mate van cyber-volwassenheid hebben (Estland, Duitsland, Spanje, Verenigd Koninkrijk en Zweden). Tevens is Australië in het onderzoek betrokken, omdat de Australische regering in haar strategie bewust de keuze maakt om te focussen op kritieke en vitale infrastructuren.

De afgelopen jaren zien we veel ontwikkelingen op het gebied van aanwijzingen van digitale infrastructuren die als vitaal worden geacht. Het betreft hier infrastructuren in maatschappelijke sectoren die dusdanig essentieel zijn voor samenlevingen dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. We zien in nationale wetgeving en vanuit Europa steeds meer wetgeving ontstaan die de noodzaak beschrijft van o.a. vitale infrastructuren, vitale sectoren en vitale aanbieders. Vanuit Europa wordt bijvoorbeeld met de NIB richtlijn (richtlijn voor beveiliging van netwerk- en informatiesystemen) getracht om eenheid en samenhang te brengen in het Europese beleid t.a.v. vitale sectoren en daarmee de (digitale) paraatheid te vergroten.

Australië

De Australische overheid stelt diverse eisen en verplichtingen aan de aangewezen kritieke/vitale infrastructuren. Het gaat hier om zowel kritieke/vitale infrastructuren in de private als de publieke sector. Het Critical Infrastructure Center (CIC) ziet er op toe dat consistente en effectieve beveiligings- en risicobeheersmaatregelen worden onderhouden en geïmplementeerd in zowel de private als de publieke kritieke infrastructuur sectoren.
Het CIC hanteert een gelaagde risico gebaseerde toezichtmethodiek. Waarbij ook gekeken wordt naar de houding en het gedrag van de organisatie ten aanzien van het voldoen aan de wet en regelgeving en de naleving. De CIC hanteert hierin vier gradaties waarin het diverse soorten interventies kan inzetten: Ondersteunen, Bijstaan, Corrigeren, Opheffen/verwijderen.

Duitsland

Netwerken en IT-infrastructuur van de federale overheid worden in de NIB-richtlijn niet aangemerkt als kritieke infrastructuur. In plaats daarvan kiest Duitsland ervoor om de algemene bescherming van overheden onder de verantwoordelijkheid van het federale ministerie van Binnenlandse Zaken (BMI) te laten vallen.
Federale Autoriteiten worden door de UP Bund (Umsetzungsplan Bund 2017: Leitlinie für Informationssicherheit in der Bundesverwaltung) verplicht om kritieke bedrijfsprocessen te identificeren - die processen die nodig zijn voor het vervullen van taken en het bereiken van doelen, evenals om de activiteiten of diensten van een organisatie van de federale overheid, een afdeling of een lichaam van essentieel belang. Federale overheden in Duitsland zijn met de bepalingen uit de UP Bund (Implementatieplan voor IT-beveiliging in de federale overheid) verplicht om de 'IT-Grundschutz' volledig te implementeren. Dit betekent ook dat voldaan moet worden aan de eisen van informatiebeveiliging en dat informatiebeveiliging audits moet worden uitgevoerd. Op overheidsniveau voert de werkgroep Informatiebeveiliging Management (Arbeitsgruppe Informationssicherheitsmanagement - AG ISM) jaarlijks onderzoeken uit bij de hele federale overheid, inclusief centrale IT-leveranciers. Deze werkgroep controleert hoe overheden de regels en eisen uit het UP Bund naleven. Op basis van de onderzoeksresultaten produceert het Ministerie van Binnenlandse Zaken (BMI) een rapport met daarin de status van alle afdelings- en IT-leveranciers. UP Bund schrijft voor dat overheden een continu verbeterproces moeten inrichten op basis van een Plan-Do-Check-Act model als onderdeel van een Information Security Management System (ISMS). De overheidsinstellingen moeten zelfstandig de naleving kunnen aantonen en voeren daarom dus regelmatig informatiebeveiligingsaudits, volwassenheids-beoordelingen en/of penetratietesten uit. In de regelgeving wordt niet aangegeven wat er gebeurt als een overheidsinstelling niet voldoet aan de minimale beveiligingsvereisten uit de UP Bund.

Estland

Estland streeft uitgebreide e-governance-initiatieven en gedigitaliseerde oplossingen na. Daarom heeft het land gekozen voor een alomvattend cyberbeveiligingskader dat van toepassing is op alle dienstverleners en organisaties. De Cybersecurity Act, waarbij de NIB-richtlijn is omgezet in Estlandse wetgeving, regelt specifiek de 'vereisten voor het onderhoud van netwerk- en informatiesystemen die essentieel zijn voor het functioneren van de samenleving en de staat'. Het is van toepassing op alle nationale en lokale autoriteiten en particuliere organisaties. Om de veerkracht en beveiliging van vitale overheidsdiensten te bevorderen, stelt de Cybersecurity Act ook eisen voor dienstverleners, die beoordelingen moeten opstellen met inbegrip van de potentiële risico's die van invloed zijn op 'de beveiliging van het systeem', het schadelijke effect inschatten dat cyberincidenten kunnen hebben op het systeem en stelt een procedure vast voor het omgaan met incidenten. Op het gebied van monitoring en compliance hanteert de RIA (Information System Authority) verschillende benaderingen. Ten eerste kan RIA via het Computer Emergency Response Team (CERT-EE) indien nodig helpen bij het beheer van incidenten. Voor overheidsdiensten voert RIA ook beveiligingscontroles en audits uit om de naleving te controleren en mogelijke beveiligingskwetsbaarheden te identificeren.

Spanje

In 2007 heeft de Spaanse regering het Nationaal Centrum voor bescherming van kritieke infrastructuur en cyberveiligheid opgericht (hierna het CNPIC). Deze instantie is verantwoordelijk voor de bevordering, coördinatie en supervisie van alle beleidsmaatregelen en activiteiten met betrekking tot de bescherming van Spaanse kritieke/vitale infrastructuren en cyberveiligheid. CNPIC valt onder de Staatssecretaris van Veiligheid, die toezicht houdt op het nationale systeem voor de bescherming van kritieke infrastructuur en het cybersecuritybeleid van het ministerie van Binnenlandse Zaken. Op strategisch niveau stelt CNPIC de criteria en richtlijnen vast om operationele capaciteiten te mobiliseren binnen overheidsdiensten die samenwerken met vitale infrastructuren en exploitanten. Deze criteria en richtlijnen bevatten preventieve maatregelen om te zorgen voor een permanente, actuele en samenhangende bescherming van het Spaanse strategische infrastructuursysteem tegen bedreigingen die ontstaan bij opzettelijke aanvallen.
Het Spaanse National Cryptologic Centre heeft voorschriften, richtlijnen en aanbevelingen opgesteld om de cybersecurity binnen openbare en particuliere organisaties te verbeteren. Dit worden de CCN-STIC-beveiligingsgidsen genoemd en afkomstig uit het referentiedocument omtrent CSIRT's. Daarbij is een onderscheid aanwezig tussen enerzijds dienstverleners in de publieke en de private sector. Elke sector heeft zijn eigen Computer Emergency Response Team (CERT). De CCN-CERT is voor dienstverleners binnen de overheid, terwijl ICIBE_CERT wordt gebruikt voor dienstverleners in private sectoren. Beide CERT's zorgen voor bescherming tegen cyberaanvallen op de geclassificeerde systemen en reageren op cyberincidenten die bij kritieke/vitale infrastructuursystemen zich kunnen voordoen.
De omzetting van o.a. de NIB-richtlijn in het nationale wetgeving van het Koninklijk Besluit 8/2018 beoogt te waarborgen dat digitale en essentiële dienstverleners de gekozen regelgeving naleven. Spanje is momenteel bezig met het opstellen van de voorschriften die door dit stuk wetgeving zijn geïmplementeerd. Een aangewezen bevoegde autoriteit is ervoor verantwoordelijk dat deze voorschriften worden gehandhaafd. Dit laatste wordt gedaan door bezoeken of door certificering. Wanneer een essentiële dienstverlener als kritisch wordt beschouwd, is de bevoegde autoriteit de CNPIC. Het proactief toezicht heeft de voorkeur, maar latere forensische onderzoeken (reactief toezicht) kan ook na incident worden uitgevoerd.

Verenigd Koninkrijk (VK)

Het VK heeft de NIB-richtlijn omgezet in haar nationale wetgeving: de Network and Information Systems Regulations 2018 (NISR) van 10 mei 2018. De volgende sectoren worden erkend als essentieel in de NISR: energie, vervoer, gezondheid, drinkwatervoorziening en -distributie en digitale infrastructuur, waaronder zowel exploitanten van overheidsdiensten als particuliere diensten. Deze sectoren zijn verder onderverdeeld in sub sectoren, die elk bevoegde autoriteiten (CA's) hebben aangewezen). De overheid is aangewezen als een van de 13 nationale infrastructuursectoren. Het HMG (HFG's Government) Security Policy Framework (SPF) beschrijft de verplichte beschermende beveiligingsresultaten die alle overheidsafdelingen moeten behalen, waaronder ook informatiebeveiliging en cybersecurityvereisten. De beveiligingsstandaarden

definiëren zoveel mogelijk resultaten, waardoor de afdelingen flexibiliteit in de implementatie hebben om sleutelconcepten te interpreteren (bijvoorbeeld 'gevoelig', 'essentieel', 'belangrijk', 'passend') en in hun lokale context in te passen.
Naast de minimale beveiligingsnormen maken overheidsorganisaties meestal ook gebruik van het UK Government Public Services Network (PSN), een krachtig netwerk dat organisaties in de publieke sector wil helpen samen te werken, duplicatie te verminderen en middelen te delen. Specifiek in het kader van het PSN moeten overheidsorganisaties regelmatig 'IT Health Checks' uitvoeren met behulp van onafhankelijke, externe accrediterende beveiliging auditorganisaties. Het doel van de IT Health Checks is tweevoudig:

1. Om zekerheid te bieden dat extern gerichte systemen worden beschermd tegen ongeautoriseerde toegang of wijziging;
2. Verzekeren dat interne netwerken en systemen geen significante zwakke punten vertonen waardoor het ene interne apparaat opzettelijk of onbedoeld invloed kan hebben op de beveiliging van een ander.

Het National Cyber Security Center (NCSC) voert een accreditatieschema (CHECK) uit voor goedgekeurde leveranciers van penetratietests die IT Health Checks voor de overheid kunnen leveren. Als overheidsorganisaties 'kritieke' of 'grote' tekortkomingen hebben als onderdeel van een IT Health Check, dan moet de organisatie een Remediation Action Plan (RAP) opstellen om deze problemen aan te pakken om de PSN-naleving te handhaven.
Verder geldt voor specifieke de kritieke overheidsdiensten dat men jaarlijks een zelfevaluatie moeten uitvoeren op basis van een verstrekte vragenlijst vanuit de Government Security Group (GSG). Hierbij wordt de kanttekening gegeven dat deze zelfevaluaties een oppervlakkig beeld geven van de genomen maatregelen. Om zekerheid te verkrijgen is het vereist dat het proces van zelfevaluatie wordt uitgevoerd door een interne audit afdeling of door een externe auditor.
Als blijkt dat een overheidsdienst niet voldoet aan de gestelde eisen wordt gerapporteerd naar het bestuur van de overheidsdienst. De betreffende overheidsdienst dient dan een herstelplan (inclusief kosten) op te leveren waarbij de GSG zal helpen. De ervaring vanuit het GSG is dat dergelijke rapportages een hefboom vormen om de maatregelen t.a.v. beveiliging en de financiering te verkrijgen vanuit de bestuurders. Indien beveiligingsmaatregelen onvoldoende zijn en persoonsgegevens hierdoor geraakt worden bestaat er ook een mogelijkheid dat de overheidsdienst bestuurlijke boetes krijgt opgelegd op basis van de GDPR.
Als ultimum remedium en in zeldzame gevallen kan GSG besluiten om de crypto grafische toegang tot gevoelige overheidsnetwerken/gerubriceerde informatie van een overheidsdienst in te trekken. Dit kan alleen als een overheidsdienst/afdeling ernstige tekortkomingen heeft in de informatiebeveiliging die niet zijn of tijdig worden opgelost.

Zweden

De Zweedse benadering voor de identificatie van vitale diensten is van toepassing op zowel particuliere als openbare sectoren en organisaties. De Zweedse wetgeving maakt hierbij dus geen onderscheid. Dit omvat verschillende geïdentificeerde vitale sectoren gebieden voor alle of de meeste uitvoerenden organisaties in de publieke sector, zoals gezondheidszorg, lokale overheidsinfrastructuur, openbaar bestuur en sociale verzekeringen. Aangezien het verantwoordelijkheidsbeginsel bepaalt dat elke organisatie de eindverantwoordelijkheid draagt

voor het waarborgen van passende cyberbeveiligings-maatregelen zijn er geen nationale minimumnormen voor cyberveiligheid die van toepassing zijn op alle vitale diensten. Ondanks de afwezigheid van algemene nationale minimumvereisten, zijn er enkele diensten die organisaties verplichten om aan minimale cybersecurityvereisten te voldoen. Om bijvoorbeeld toegang te krijgen tot het Secure Intranet van de Zweedse overheid. Daarvoor moeten deze organisaties cybersecurity-regelingen presenteren in overeenstemming met ISO / IEC 27001: 2014.
In Zweden zijn geen op zichzelf staande mechanismen voor voortdurende monitoring van de naleving van cyberveiligheidseisen, specifiek gericht op uitvoerders van vitale diensten. Wel kunnen de cyberbeveiligingsregelingen van nationale overheidsdiensten worden opgenomen in audits door de Zweedse nationale auditorganisatie (Riksrevisionen). Daarnaast zien we dat bijzondere nalevingsvereisten worden gesteld aan organisaties in de private en publieke sector die zich bezighouden met 'beveiligingsgevoelige activiteiten' (d.w.z. activiteiten die van belang zijn voor de veiligheid van Zweden of die vallen onder een internationale verplichting tot bescherming van de veiligheid die bindend is voor Zweden). Deze worden geleid door de Protective Security Act en Protective Security Ordinance, die beiden op 1 april 2019 in werking zijn getreden. Deze wetten omvatten beveiligingsregels die verwijzen naar preventieve maatregelen die zijn genomen om de beveiligingsgevoelige activiteiten van overheidsinstanties en bedrijven te beschermen tegen spionage, sabotage, terroristische misdrijven en andere misdrijven. De handhaving van deze voorschriften wordt uitgevoerd door de Zweedse nationale beveiligingsdienst, die vrij is om te beslissen waar beschermende beveiligingsinspecties worden uitgevoerd om de bescherming van de meest kritieke infrastructuur van het land te waarborgen.

INHOUDSOPGAVE

1 INLEIDING

1.1 Opdracht en doel

In dit onderzoek wordt onderzocht welke (bindende) maatregelen andere (EU) landen voor hun eigen vitale overheden hebben vastgesteld. Het doel van de opdracht is om inzicht te krijgen in de omgang t.a.v. regelgeving, normstelling en toezicht van andere EU-landen met hun eigen vitale (of vergelijkbare) digitale overheid.

1.2 Vraagstelling

Het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (hierna: BZK) heeft gevraagd om een onderzoek uit te voeren naar de wijze hoe overheden van andere met Nederland vergelijkbare landen de vitale digitale infrastructuur van de overheid vaststellen, welke (typen) maatregelen zij hiervoor voorschrijven, op welke wijze zij dit uitvoeren en welk toezicht daarop is ingericht.

1.3 Doel van dit document

Dit document geeft BZK inzicht in hoe andere landen, vergelijkbaar met Nederland, invulling geven aan de eisen en verplichtingen en het toezicht op de vitale infrastructuur van de digitale overheid.

VKA geeft alleen een feitelijke beschrijving van de praktijk in de vergelijkbare landen en nemen, zoals BZK heeft gevraagd, geen aanbevelingen of adviezen op in het rapport ten aanzien van haar waarnemingen. Het is aan BZK om de resultaten uit dit onderzoek te verwerken.

1.4 Leeswijzer

In hoofdstuk 2 beschrijven we onze onderzoeksopzet
In hoofdstuk 3 geven wij een korte beschrijving van de Nederlandse situatie
In hoofdstuk 4 beschrijven we de situatie in de onderzochte landen.
In bijlage A geven wij de omschrijving van de onderzoekopdracht zoals deze door het Ministerie van BZK geformuleerd is.
In de bijlage B geven wij als achtergrondinformatie per onderzocht land een algemene beschrijving van de rol van het openbaar bestuur bij digitalisering van de samenleving.

2 ONDERZOEKSOPZET

2.1 Inleiding

De onderstaande onderzoekaanpak is gehanteerd om tot een feitelijk juiste en complete beantwoording van de vraag van de opdrachtgever te komen.

2.2 Onderzoekaanpak

De aanpak van het onderzoek is gebaseerd op drie onderzoeksvragen die in deze rapportage worden beantwoord:

1. Op welke wijze/manier andere Europese lidstaten binnen de sector digitale overheid infrastructuur als vitaal hebben aangewezen;
2. Wat voor soorten maatregelen (zorgplichten / meldplichten) deze Europese lidstaten opleggen aan de vitale infrastructuur binnen de sector digitale overheid. Te denken valt hier aan standaarden als de ISO27001 of continuïteitseisen;
3. Hoe en òf deze Europese lidstaten invulling geven aan toezicht op de vitale infrastructuur binnen de sector digitale overheid.

2.3 Onderzoekfases

Het onderzoek is opgedeeld in een drietal fases:

Fase	Activiteit	Deliverable
Kick-off en Voorbereiding	Kick-off	Afgestemde onderzoekopzet
		Bepalen van de te onderzoeken landen
	Voorbereiding onderzoek	Documentstudie
		Afstemmen vragenlijst t.b.v. landen
Uitvoering (Synthese, analyse en concept rapportage)	Verzamelen van benodigde informatie	
	Interviews afnemen	Uitvoeren van interviews
	Aanvullende documentstudie	Aanvullende documenten (n.a.v. interviews) verzameld en opgenomen in documentstudie
	Uitwerken rapportage	Conceptrapportage opgesteld
Afronding	Afstemmen concept rapportage met opdrachtgever	Conceptrapportage afgestemd
	Definitieve rapportage	Definitieve rapportage opgeleverd

2.3.1 Kick-off:

Tijdens de kick-off hebben we de vraagstelling en het gewenste resultaat besproken. Daarnaast hebben we met de opdrachtgever bepaald welke Europese Lidstaten in het onderzoek dienen te worden betrokken en of er vanuit de opdrachtgever relevante contacten aanwezig zijn in de nader te bepalen Europese Lidstaten. Wij hebben in overleg met de opdrachtgever een selecte van grotere, middelgrote en kleinere EU-landen gemaakt die een hoge mate van cyber-volwassenheid hebben (Estland, Duitsland, Spanje, Verenigd Koninkrijk en Zweden). Tevens hebben we Australië in het onderzoek betrokken, omdat de Australische regering in haar strategie bewust de keuze maakt om te focussen op kritieke en vitale infrastructuren. Wij hebben een raamwerk opgesteld dat strookt met de te beantwoorden hoofdvragen, hebben bronnen geïdentificeerd, experts en contacten bij ministeries en overheidsdiensten benaderd en gevraagd mee te werken. Dit raamwerk vormt tevens de basis voor de internationale vergelijking. Het template is ter goedkeuring aan de opdrachtgever voorgelegd voor feedback. Naast de items gerelateerd aan de informatiebehoefte, geeft het raamwerk ruimte voor het vastleggen van contextuele factoren en/of overige relevante toelichting.

2.3.2 Verzamelen van benodigde informatie

Voor elk van de geselecteerde EU landen en Australië is in publiek beschikbare bronnen informatie gezocht over de toepassing van regelgeving, normstelling en toezicht met vitale infrastructuur in de digitale overheid gezocht naar informatiebronnen. Hiervoor zijn twee paden bewandeld:

1. Een gerichte zoekstrategie in publiek beschikbare online bronnen via Google en Google Scholar. Maar ook via de door de landen zelf ter beschikking gestelde openbare documentatie en bronnen, zoals wetgeving en de beschreven werkwijze en interventiemethodieken van de daar aangewezen toezichthouders. De zoekopdrachten die we hierbij hebben gehanteerd hebben betrekking op vitale en kritieke infrastructuren. Ook de omgang met de NIB richtlijn en andere nationale bestuurlijke initiatieven geven een indicatie hoe de gekozen landen omgaan met vitale/kritieke infrastructuren. Een voorbeeld van een relevante bron is “State-of-play of the transposition of the NIS Directive”[1] van de Europese Commissie, die een overzicht geeft van de implementatie van de NIB richtlijn binnen de Europese Landen.
2. Verder is informatie opgevraagd bij de experts/vertegenwoordigers van de landen. Het onderzoeksteam heeft de betreffende ministeries dan wel de aangewezen toezichthouders geïnterviewd. We hebben één of twee semi-gestructureerde interviews gehouden voor de benodigde contextualisering en aanvulling van ontbrekende of onvolledige informatie. Voor alle verzamelde informatie zijn de informatiebronnen nauwkeurig bijgehouden en gearchiveerd. Voor elk geselecteerd land is een (conceptversie van de) synthese van de verzamelde informatie gedeeld met een expert en/of vertegenwoordiger van de betreffende verantwoordelijke overheidsdienst. Gevraagd is om te beoordelen of de informatie accuraat, compleet en up-to-date is, en waar nodig aan te vullen of te corrigeren. Indien een gedocumenteerde bron niet

[1] https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

beschikbaar is, is de verstrekte informatie toegeschreven aan de expert als “personal correspondence”.

Duitsland heeft in een later stadium aangegeven niet in staat te zijn om over dit onderwerp interviews af te geven. Om dit te compenseren hebben wij aanvullend deskresearch uitgevoerd op de gestelde eisen en verplichtingen en het toezicht op vitale infrastructuur in de overheidssector.

Synthese, analyse en concept rapportage
Wij hebben de inzichten over de omgang t.a.v. regelgeving, normstelling en toezicht met vitale digitale overheid in de geselecteerde landen vergeleken en gestructureerd. Vervolgens hebben wij de aanknopingspunten geïdentificeerd voor Nederland.

2.3.3 Afstemmen en opleveren

VKA heeft de opmerkingen en aanmerkingen vanuit de begeleidingsgroep verwerkt en een definitieve rapportage van het onderzoek opgeleverd.

2.4 Scope van het onderzoek

2.4.1 Binnen scope

De scope van het onderzoek richt zich op vitale infrastructuur in de sector digitale overheid, de gestelde eisen en verplichtingen en het toezicht daarop bij de onderzochte landen.

2.4.2 Buiten scope

De NIB-richtlijn staat in beginsel buiten scope tenzij een land de nationale implementatie daarvan dusdanig heeft verweven in de daar van toepassing zijnde wet- en regelgeving.

3 VITALE DIGITALE INFRASTRUCTUUR IN NEDERLAND

3.1 Achtergrond ontwikkeling vitale sectoren

De afgelopen jaren zien we veel ontwikkelingen op het gebied van aanwijzingen van digitale infrastructuren die als vitaal worden geacht. Het betreft hier infrastructuren in maatschappelijke sectoren die dusdanig essentieel zijn voor samenlevingen dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. We zien in nationale wetgeving en vanuit Europa steeds meer wetgeving ontstaan die de noodzaak beschrijft van o.a. vitale infrastructuren, vitale sectoren en vitale aanbieders. Vanuit Europa wordt, met bijvoorbeeld de NIB-richtlijn, getracht om eenheid en samenhang te brengen in het Europese beleid t.a.v. vitale sectoren en daarmee de (digitale) paraatheid te vergroten.[2]

Hierdoor ontstaan diverse zorgplichten en meldplichten waaraan de aangewezen vitale en/of essentiële aanbieders moeten voldoen. Voor de komst van de Europese NIB-richtlijn en de uiteindelijke implementatie van deze eisen in de WBNI waren er in Nederland al meerdere sectoren en onderdelen die als vitaal werden gezien. Nederland liep in 2017 met bijvoorbeeld de voormalige Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) voor op dit vlak. Deze wet is uiteindelijk met de implementatie van de NIB-richtlijn samengegaan in de WBNI. Dit is dan ook de reden dat we in de WBNI een tweedeling zien van soorten “vitale aanbieder/sectoren”.[3] In de huidige wet- en regelgeving zijn nog geen vitale overheidspartijen/diensten aangewezen.

3.2 Huidige aanwijzing binnen Nederland

Op dit moment zijn in Nederland meerdere soorten aanwijzingen die infrastructuren, sectoren, aanbieders of processen als vitaal aanwijzen. Enerzijds zijn daarin zorg- en meldplichten opgenomen waaraan de sectoren en aanbieder moeten voldoen anderzijds zien we de reikende hand vanuit de overheid (NCSC) om bij een dreigende uitval of verstoring directe ondersteuning te bieden.

In Nederland zien we dit terugkomen in o.a. wet en regelgeving en vanuit het NCSC:

1. De door vakdepartementen van de diverse ministeries aangewezen vitale processen binnen Nederland. Dit zijn de zogenaamde A en B categorieën die directe bijstand kunnen krijgen vanuit het Nationaal Cyber Security Centrum (NCSC).[4]
2. WBNI: De door Europa in de NIB-richtlijn aangewezen aanbieders van essentieel diensten (AED’s) zijn door Nederland geïmplementeerd in de WBNI en het onderliggende besluit BBNI. Op basis van een zorgplicht worden eisen gesteld aan AED’s, is hulp en bijstand beschikbaar vanuit de overheid en hebben de AED’s meldplichten aan o.a. toezichthouders en het NCSC. De aanwijzing van AED’s zien we terug in artikel 2 BBNI.

[2] (EU) 2016/1148

[3] Aanbieders van Essentiele Diensten (AED) & andere vitale aanbieders.

[4] https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur

3. Voormalige Wgmc / thans WBNI: Aanbieder van een andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving (de zogenaamde andere vitale aanbieders). Voor deze groep is geen zorgplicht opgenomen maar is een meldplicht van toepassing waardoor hulp en bijstand kan worden geboden. Dit type aanbieders komen uit de voormalige Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) en zijn thans aangewezen in artikel 3 BBNI. Voor deze specifieke groep is in de wet geen toezicht opgenomen.

Uit de voorgaande lijst zien we de sector digitale overheidsprocessen alleen terugkomen als B-categorie, zijnde een vitaal proces. Dit proces is dan door het verantwoordelijk Ministerie BZK aangewezen als een vitaal proces /vitale sector. Deze sector kan dan rekenen op bijstand en hulp vanuit het NCSC als zich incidenten voor doen. In de Nota van Toelichting op het besluit onder de WBNI zien we de sector digitale overheid genoemd worden als sector die in de volgende wijziging/tranche van de WBNI en het besluit zal worden opgenomen.[5] Vanuit VKA interpreteren we dit als volgt: door de sector digitale overheid in de toekomst beter te verankeren in wet- en regelgeving zouden striktere eisen kunnen worden opgelegd aan de sector digitale overheid. Hierbij valt bijvoorbeeld te denken aan zorg- en meldplichten en verantwoording aan een toezichthouder. We zien dit ook terugkomen in onlangs uitgevoerd onderzoek vanuit BZK naar “toezicht en verantwoording informatieveiligheid overheid” waarin de WBNI en de (toekomstige) rol van BZK ter sprake komt.[6]

[5] Staatsblad 8 november 2018, nr. 388.

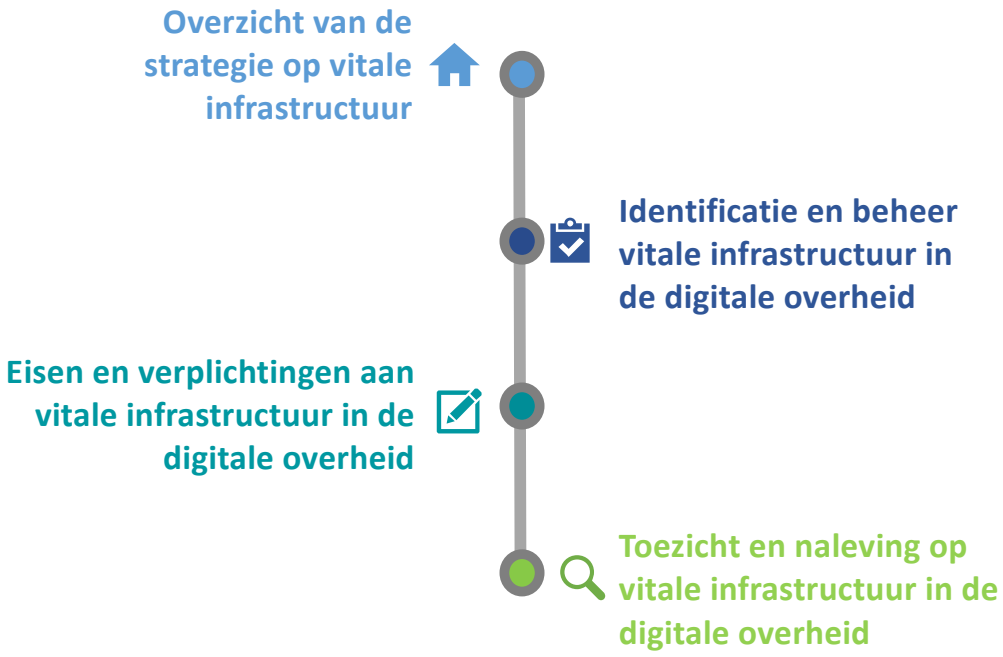
[6] https://www.rijksoverheid.nl/documenten/rapporten/2019/02/28/onderzoek-toezicht-en-verantwoording-informatieveiligheid-overheid 2019, p.25.

4 ONDERZOEK INRICHTING VITALE INFRASTRUCTUREN BUITENLAND

4.1 Inleiding

In het onderzoek is een zestal landen onderzocht. In afstemming met BZK is gekozen voor de EU landen Duitsland, Estland, Spanje, Verenigd Koninkrijk en Zweden. Daarnaast is gekozen voor Australië, omdat de Australische regering in haar strategie bewust de keuze maakt om te focussen op kritieke en vitale infrastructuren. Per land geven we de uiteenzetting op basis van de documentstudie en de uitgevoerde interviews bij de ministeries / toezichthouders op het betreffende beleidsterrein.

Per land zetten we de volgende elementen uiteen. Het betreft informatie uit zowel de wetgeving, literatuur als uit interviews.



4.2 Uitkomsten Australië

OVERZICHT VAN VITALE INFRASTRUCTUUR STRATEGIE IN AUSTRALIË

De Australische regering beschrijft vitale (of kritieke) infrastructuur in haar *Critical Infrastructure Resilience Strategy* als volgt:

> *'die fysieke faciliteiten, toeleveringsketens, informatietechnologieën en communicatienetwerken die, indien vernietigd, aangetast of onbeschikbaar gemaakt voor een langere periode, het sociale of economische welzijn van de natie aanzienlijk zouden beïnvloeden of het vermogen van Australië om nationale defensie uit te voeren en de nationale veiligheid te waarborgen zouden beïnvloeden.'*[7]

De regering identificeert hierbij acht kritiek infrastructuursectoren: telecommunicatie, energie (gas en elektriciteit), water, overheid, transport, gezondheid, banken en financiën en voedsel.

Het doel van de Critical Infrastructure Resilience Strategy is er voor te zorgen dat kritieke infrastructuur continu blijf functioneren. Australië geeft daarbij aan dat een infrastructuur die in hoge mate veerkrachtig is, zorgt dat het leveren van essentiële diensten aan bedrijven, overheden en de gemeenschap kan blijven functioneren. De Australische regering maakt in haar strategie bewust keuze om te focussen op kritieke en vitale infrastructuren.

De overheid ziet hierin voor zichzelf de rol om kritieke infrastructuurorganisaties te helpen bij het verbeteren van hun vermogen om onvoorziene of onverwachte gevaren te beheren. Op deze manier helpt het de essentiële dienstverleners om te kunnen blijven functioneren.[8] De Australische regering heeft daartoe twee overheidsorganen verantwoordelijk gesteld voor de kritieke infrastructuren. Enerzijds het Trusted Information Sharing Network (TISN) anderzijds het Critical Infrastructure Center (CIC).

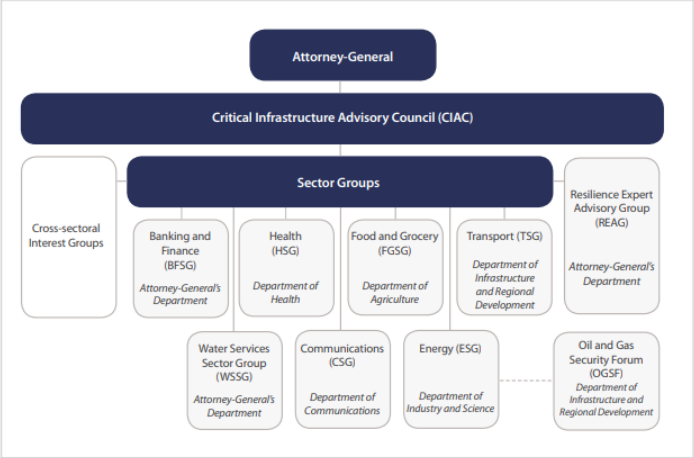
Trusted Information Sharing Network (TSIN)

Het TSIN is in 2003 opgericht en aangewezen als organisatie voor het delen van informatie tussen bedrijven en het opbouwen van weerbaarheid. TISN biedt een veilige omgeving waarin eigenaren en exploitanten van kritieke infrastructuur regelmatig bijeenkomen om informatie te delen en binnen en tussen sectoren samen te werken om uitdagingen op het gebied van beveiliging en bedrijfscontinuïteit aan te pakken.

[7] https://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF

[8] Critical Infrastructure Resilience Strategy, p13.

Coördinatie en strategische begeleiding wordt verzorgd door de Critical Infrastructure Advisory Council (CIAC). CIAC bestaat uit de voorzitters van elk van de TISN-groepen, hooggeplaatste vertegenwoordigers van de Australische overheid van relevante agentschappen en hooggeplaatste vertegenwoordigers van de staat. Zie ook bijgevoegde governance structuur met daarin alle partijen die aangesloten zijn bij TISN.[9]



Critical Infrastructure Center

Het Critical Infrastructure Center (CIC) is in 2017 is opgericht en valt onder de verantwoordelijkheid van het ministerie van Binnenlandse Zaken. De organisatie is opgericht om te reageren op de zich ontwikkelende dreigingsomgeving, met name door buitenlandse inmenging in de kritieke infrastructuur van Australië. Deze instantie is verantwoordelijk voor het beheer en de handhaving van aspecten van de *Security of Critical Infrastructure Act 2018* (the SOCI Act)[10] en de in 2017 hervormde *Telecommunications Act 1997* (TSS reforms).

Naast voorgaande verantwoordelijkheden is CIC ook aangewezen als adviesorgaan bij buitenlandse investeringen in het kader van de Foreign Acquisitions and Takeovers Act 1975 (FATA). Het doel hiervan is dat CIC advies geeft over voorgenomen investeringen vanuit het buitenland. Daarbij richt CIC zich op de nationale veiligheidsrisico's van spionage, sabotage en buitenlandse inmenging. CIC kijkt wat voor effect de buitenlandse betrokkenheid kan hebben op de kritieke infrastructuur van Australië.

Ten aanzien van haar rol uit de SOCA Act ontwikkelt SIC beleid en advies om de complexe nationale veiligheidsrisico's voor de kritieke infrastructuur van Australië aan te pakken. CIC heeft daartoe een strategie gepubliceerd die tot doel heeft om de volledige naleving door kritieke infrastructuurbeheerders en exploitanten van hun verplichtingen uit hoofde van wetgeving te vergemakkelijken. De strategie schetst de belangrijkste verplichtingen voor eigenaren en exploitanten van kritieke infrastructuur en legt de belangrijkste elementen uit van de compliance-aanpak en -activiteiten die CIC uitvoert.[11]

[9] https://www.tisn.gov.au/Pages/the_tisn.aspx

[10] https://www.legislation.gov.au/Details/C2018A00029

[11] Critical Infrastructure Centre Compliance Strategy, https://cicentre.gov.au/document/P10S011

Het strategische doel van CIC is een risico gebaseerde aanpak te hanteren om hogere veerkracht en beveiliging van kritieke infrastructuur te waarborgen. CIC vervult twee rollen om deze doelstelling te bereiken:

1. Ondersteunen van beheerders van kritieke infrastructuur om meer veerkrachtig te zijn en risico's voor de integriteit en continuïteit van de activiteiten te beheren.
2. Ingrijpen om te zorgen dat eigenaren en exploitanten kritieke infrastructuur beschermen tegen een reeks nationale veiligheidsdreigingen, waaronder spionage, sabotage en buitenlandse inmenging.

IDENTIFICATIE EN BEHEER VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

Australië beschikt over een register met daarin de partijen die zowel privaatrechtelijk als publiekrechtelijk verantwoordelijk zijn voor kritieke infrastructuren in Australië. Het gaat daarbij zowel om de operationele eigenaren van de kritieke infrastructuren maar ook om belanghebbenden met ten minste 10% aan belangen of die in staat zijn om de kritieke infrastructuur direct of indirect te beïnvloeden of te beheersen. Het register van kritieke infrastructuur moet ervoor zorgen dat de Australische overheid beter kan bepalen wie in Australië kritieke infrastructuur bezit en beheert. Dergelijke informatie is van belang bij het beoordelen van de potentiële risico's van sabotage, spionage in de kritieke infrastructuur. Het stelt de toezichthouder CIC in staat om gedetailleerde en betere gerichte risicobeoordelingen uit te voeren.

De Minister heeft onder de SOCI Act de bevoegdheid om zelfstandig kritieke infrastructuren aan te wijzen. Het beheren van het register staat onder de verantwoordelijkheid van de Secretaris van het Departement en is niet openbaar. In de wet zijn verder de bevoegdheden beschreven die de Minister en de Secretaris hebben ten aanzien van de kritieke infrastructuren. Deze bevoegdheden zien we ook terugkomen onder de paragraaf toezicht en naleving op de vereisten.

EISEN EN VERPLICHTINGEN AAN VITALE INFRASTRUCTUREN IN DE DIGITALE OVERHEID

De Australische overheid stelt diverse eisen en verplichtingen aan de aangewezen kritieke/vitale infrastructuren. Het gaat hier om zowel kritieke/vitale infrastructuren in de private als de publieke sector. De SOCI Act uit 2018 bevat drie belangrijke maatregelen om de risico’s op kritieke/vitale infrastructuren aan te pakken en te beheersen.

1. Een rapportageverplichting en register met daarin de entiteiten of belanghebbende die verantwoordelijk zijn voor kritieke infrastructuren;
2. De macht om informatie te verzamelen/vorderen: de secretaris van het ministerie van Binnenlandse Zaken kan informatie en documenten verkrijgen van de entiteiten die verantwoordelijk zijn voor kritieke infrastructuren, en;
3. Aanwijzingen geven: de Minister van Binnenlandse Zaken kan aanwijzingen geven aan de entiteiten die verantwoordelijk zijn voor kritieke infrastructuren in gevallen dat er een nationaal veiligheidsrisico bestaat. Waarbij de Minister een aanwijzing kan geven om een handeling te doen of te laten.

NALEVING EN TOEZICHT OP DE VEREISTEN IN DE DIGITALE OVERHEID

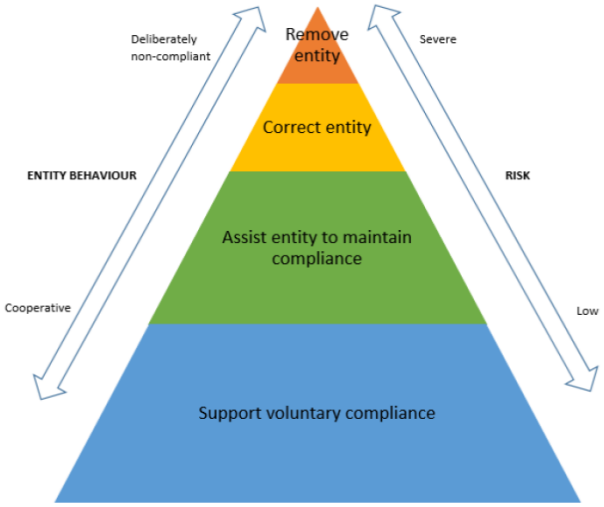
Het Centrum (CIC) ziet er op toe dat consistente en effectieve beveiligings- en risicobeheersmaatregelen worden onderhouden en geïmplementeerd in zowel de private als de publieke kritieke infrastructuur sectoren. Het CIC kan op diverse manier toezicht houden, niet limitatief:

1. Beoordelen of aangeleverde rapportages voldoen aan de rapportagevereisten;
2. Door het verzamelen van informatie;
3. Het uitvragen en inspecteren en bewaren van documentatie;
4. Het laten uitvoeren van audits of zelf uitvoeren van audits;
5. Beoordelen van de complete naleving in de organisatie.

Bij het beoordelen of een organisatie voldoet aan de regels houdt het CIC rekening met drie factoren:

1. **Risico**: welke impact heeft niet-naleving op de nationale veiligheid van Australië? Wat is de aard van het risico? Welke oplossingen zijn er? Hoe effectief zijn ze? Vraagt het risico om dringende actie?
2. **Evenredigheid:** hoe ernstig is het risico van de vastgestelde inbreuk? Zijn er verzwarende omstandigheden?
3. **Betrokkenheid / gedrag en houding van de organisatie:** hoe staat de organisatie tegenover compliance? Hoe coöperatief is de organisatie op basis van betrokkenheid bij het CIC en hun nalevingsgeschiedenis?

Het CIC hanteert dus een gelaagde risico gebaseerde toezichtmethodiek. Waarbij ook gekeken wordt naar de houding en het gedrag van de organisatie ten aanzien van het voldoen aan de wet en regelgeving en de naleving. Hoe meer samenwerking vanuit de kritieke/vitale infrastructuren hoe milder het CIC zicht opstelt. De mate van toezicht is dus volledig afhankelijk hoe de verantwoordelijke voor de kritieke infrastructuur zich opstelt.



Het CIC hanteert hierin vier gradaties waarin het diverse soorten interventies kan inzetten.

1. **Ondersteunen**: Het CIC verstrekt informatie en begeleiding aan entiteiten om hun nalevingsinspanningen te ondersteunen. In deze gradatie zal het CIC de volgende interventies inzetten:
    a. Informatie-uitwisseling;
    b. Aanbidden van adviezen en richtlijnen;
    c. Valideren of de verantwoordelijke aan de nalevingseisen voldoet.

2. **Bijstaan:** Wanneer een organisatie niet volledig conform is maar wel betrokkenheid toont, zal het CIC proberen een overeengekomen manier van handelen met de entiteit vast te stellen zodat deze kan terugkeren naar een voldoende mate van naleving. In deze gradatie zal het CIC de volgende interventies inzetten:
    a. Trainingen en opleidingen aanbieden;
    b. Adviezen geven over dreigingen;
    c. Uitwisselen informatie over best-practices;
    d. Stellen van verwachtingen en normen.

3. **Corrigeren:** Indien de betrokkenheid, onderhandeling en/of bemiddeling niet succesvol zijn, of wanneer het CIC van oordeel is dat dat de entiteit niet te goeder trouw handelt, zal het CIC escaleren naar handhavingsmaatregelen. Dit om naleving te bereiken en het geïdentificeerde risico te verminderen. In deze gradatie zal het CIC de volgende interventies inzetten:
    a. Formele waarschuwingen uitdelen;
    b. Opleggen van een Ministeriële aanwijzing;
    c. Rechterlijk bevel;
    d. Afdwingbare overeenkomst afsluiten;
    e. Opleggen van boetes;
    f. Overgaan tot rechtsvervolging.

4. **Opheffen/verwijderen:** In extreme gevallen waarin niet-naleving een onaanvaardbaar risico voor de nationale veiligheid oplevert of de organisatie niet bereid is om hieraan te voldoen, kan het CIC aanbevelen dat er maatregelen worden genomen om het risico volledig te verwijderen. In deze gradatie zal het CIC de volgende interventies kunnen inzetten:
    a. Het intrekken van de vergunning;
    b. Bevel tot afstoting / verkoop van onderdelen;
    c. Toezichthouder neemt fysiek de controle (bestuursdwang);
    d. Opleggen van een Ministeriële aanwijzing.

4.3 Uitkomsten Duitsland

OVERZICHT VAN VITALE INFRASTRUCTUUR STRATEGIE IN DUITSLAND

Het Federale Bureau voor Informatiebeveiliging (BSI) is met BSI-act uit 2009 aangewezen als de nationale cyberveiligheidsautoriteit van Duitsland en valt onder de verantwoordelijk van het Federale Ministerie van Binnenlandse Zaken. Naast de cyberveiligheidsautoriteit BSI richtte Duitsland met haar Nationale Cyber Security Strategie uit 2011 nog twee toezichtorganen op voor cyberveiligheidskwesties: de National Cyber Security Council en het National Cyber Response Center.

De Nationale Cyber Security Council bestaat uit de Federale Kanselarij, het Federale Ministerie van Buitenlandse Zaken, het Federale Ministerie van Binnenlandse Zaken, het Federale Ministerie van Defensie, het Federale Ministerie voor Economie en Technologie, het Federale Ministerie van Justitie, het Federale Ministerie van Financiën, het federale ministerie van onderwijs en onderzoek, evenals vertegenwoordigers van de federale deelstaten.[12] Vertegenwoordigers van het bedrijfsleven en academici kunnen worden uitgenodigd voor vergaderingen indien dit noodzakelijk wordt geacht. De Raad coördineert preventieve instrumenten en interdisciplinaire benaderingen van cybersecurity in de publieke en private sector.

Het National Cyber Response Center heeft tot doel de operationele samenwerking tussen alle overheidsinstanties te optimaliseren en de coördinatie van beveiligings- en responsmaatregelen voor IT-incidenten te verbeteren. Het Federale Criminele Politiebureau (BKA), Federale Politie (BPOL), Douane Criminologische Dienst (ZKA), Federale Inlichtingendienst (BND), Bundeswehr en autoriteiten die toezicht houden op exploitanten van kritieke infrastructuur nemen allen deel aan het Centrum. Het centrum rapporteert aan de BSI en werkt rechtstreeks samen met het Federaal Bureau voor de Bescherming van de Grondwet (BfV) en het Federaal Bureau voor Civiele Bescherming en Hulp bij rampen (BBK). Het centrum doet aanbevelingen aan de Nationale Cyber Security Council, zowel op regelmatige basis als voor specifieke incidenten; hoewel het in noodsituaties rechtstreeks crisisbeheersingspersoneel van het federale ministerie van Binnenlandse Zaken op de hoogte brengt.

Naast de Duitse nationale cyberbeveiligingsstrategieën van 2011 en 2016[13] zijn ook de NIB-richtlijn implementatiewet en de IT-beveiligingswet relevant voor de sturing en het toezicht op kritieke infrastructuur. Beide wetten passen normen voor informatiebeveiliging toe op kritieke infrastructuur en vereisen dat sectoren en dienstverleners BSI en andere instanties op de hoogte stellen als zich een cyberincident voordoet. De IT-beveiligingswet regelt de beveiliging

[12] Federal Ministry of the Interior. 2011. *Cyber Security Strategy for Germany.* Federal Republic of Germany. As of 31 October 2019:

[13] http://www.bmi.bund.de/cybersicherheitsstrategie/

gerelateerde verplichtingen die van invloed zijn op telemedia-diensten[14] en leveranciers van elektriciteitsnetwerken in het kader van de Energy Economy Act en vereist dat verschillende organisaties passende waarborgen treffen om hun systemen en faciliteiten te beschermen.[15] De BSI-Kritis-voorschriften implementeren nadere vereisten uit de IT Security Act in bepaalde sectoren.[16]

Duitsland ondersteunt verder de publiek-private samenwerkingsverbanden voor het delen van informatie over cyberveiligheid. De alliantie voor cyberbeveiliging[17] biedt een landelijk platform voor het delen van informatie over cyberdreigingen en aanvalsreacties en UP KRITIS[18] richt zich op de bescherming van kritieke infrastructuur, inclusief sectorspecifieke werkgroepen die helpen bij het ontwikkelen van de normen afkomstig uit de IT Security Act. De BSI deelt zelf informatie over geïdentificeerde cybersecurity-kwetsbaarheden en trends in kwaadaardige software-malware met alle geïnteresseerde organisaties en het publiek op zijn website, en analyseert de oorzaken en methoden van huidige cyberaanvallen in zijn jaarverslag over de staat van IT-beveiliging in Duitsland.[19]

IDENTIFICATIE EN BEHEER VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

Netwerken en IT-infrastructuur van de federale overheid worden in de NIB-richtlijn niet aangemerkt als kritieke infrastructuur. In plaats daarvan kiest Duitsland ervoor om de algemene bescherming van overheden onder de verantwoordelijkheid van het federale ministerie van Binnenlandse Zaken (BMI) te laten vallen.

De Duitse Cyber Security-strategie uit 2016 vormt het interdepartementale strategische kader voor de activiteiten van de federale overheid op het gebied van cyberveiligheid. De operationele invulling van deze cyberveiligheid heeft Duitsland in 2017 opgenomen in haar *Umsetzungsplan*

[14] Het gaat hier om telecommunicatie, sociale media, websites.

[15] Paul Voigt. 2018. 'Information Security Considerations: Germany', Practical Law of Thomson Reuters. As of 31 October 2019: https://united-kingdom.taylorwessing.com/en/documents/get/1552/information-security-considerations-germany.pdf_show_on_screen.

[16] Paul Voigt. 2018. 'Information Security Considerations: Germany', Practical Law of Thomson Reuters. As of 31 October 2019: https://united-kingdom.taylorwessing.com/en/documents/get/1552/information-security-considerations-germany.pdf_show_on_screen.
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html.

[18]https://www.kritis.bund.de/SubSites/Kritis/EN/activities/national/cipimplementationplan/cipimplementationplan_node.html

[19] Federal Office for Information Security. 2018. *The State of IT Security in Germany 2018.* Federal Republic of Germany. As of 31 October 2019: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=3

Bund 2017: Leitlinie für Informationssicherheit in der Bundesverwaltung (Hierna: UP BUND).[20] De UP BUND fungeert voor de overheid als het 'regelgevingskader' door minimumveiligheidsnormen en verplichtingen vast te stellen voor alle federale autoriteiten.[21]

Het raamwerk richt zich op de doelstellingen van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) voor alle IT-systemen, services en communicatienetwerkinfrastructuren binnen de federale overheden. Het is van toepassing op alle Ministeries en federale autoriteiten. Ministeries kunnen daarbij zelf kiezen om de reikwijdte van de UP Bund uitbreiden tot andere entiteiten onder haar verantwoordelijkheid. Ieder ministerie is verantwoordelijk voor de implementatie van de UP Bund. De bepalingen van de UP Bund zijn bindend en stellen de minimale beveiligingseisen vast om ervoor te zorgen dat:

1. De federale overheid zich houdt aan de wettelijke richtlijnen en minimumnormen die van toepassing zijn op informatiebeveiliging;
2. De continuïteit wordt gewaarborgd door duurzame en systematische inspanningen voor informatiebeveiliging toe te passen;
3. Informatie- en IT-systemen binnen de federale overheid zijn beveiligd tegen manipulatie, ongeoorloofde toegang en verlies van integriteit.

Federale Autoriteiten worden door de UP Bund verplicht om kritieke bedrijfsprocessen te identificeren - die processen die nodig zijn voor het vervullen van taken en het bereiken van doelen, evenals om de activiteiten of diensten van een organisatie van de federale overheid, een afdeling of een lichaam van essentieel belang.[22] Deze kritieke processen kunnen onderworpen zijn aan aanvullende informatiebeveiligingsvereisten.

De UP Bund schetst voor de federale overheid zowel de informatiebeveiligingsvereisten voor interdepartementale communicatienetwerken als de eisen aan *IT Emergency Prevention en IT Crisis Response*. Op grond van de UP Bund zijn overheden ook verplicht om te rapporteren:

- Afdelingen en agentschappen moeten geïdentificeerde informatiebeveiligingsincidenten melden bij het BSI Situation Center.
- In geval van incidenten zal de BSI informatie verstrekken of als dat noodzakelijk is de coördinatie overnemen. Hierin dienen de IT-dienstverleners van de Federale Autoriteit op een passende wijze te worden betrokken.

---

[20] Umsetzungsplan Bund 2017. As of 7 November 2019: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html

[21] De UP Bund vormt een aanvulling op de IT-strategie van de federale overheid (IT-Strategie der Bundesverwaltung) en de IT-architectuur van de federale overheid (IT-Rahmenarchitektur IT-Steuerung Bund).

[22] Zie de bijbehorende BSI-richtlijnen voor identificatie van kritieke bedrijfsprocessen: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Hochverfuegbarkeit/BandAH/AH3_1_Leitfaden_Phase_S.pdf?__blob=publicationFile&v=1

- De ministeries/overheidspartijen moeten binnen hun eigen beleidsterrein een IT-afdeling oprichten. Deze afdeling moet regelmatig IT-noodoefeningen uitvoeren en documenteren. Deze IT-afdelingen moet ook deelnemen en afstemming zoeken met continuïteitonderdelen binnen het beleidsterrein.

Over het algemeen presenteert de UP Bund een uitgebreide reeks minimumvereisten voor informatiebeveiliging voor de federale autoriteiten. Hoe dit kader wordt gemonitord en geëvalueerd, wordt verder besproken in de volgende paragraaf.

EISEN EN VERPLICHTINGEN AAN VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

De Duitse wetgeving eist dat aanbieders van kritieke/vitale infrastructuur maatregelen treffen op de IT-systemen en -faciliteiten met behulp van de nieuwste technologie.[23] Dit om te zorgen voor de bescherming van de beschikbaarheid, integriteit, authenticiteit en vertrouwelijkheid. Aanbieders moeten aan de toezichthouder BSI tweejaarlijkse aantonen dat hun faciliteiten voldoen aan de vereisten uit de IT-beveiligingswet. De normen die worden opgelegd aan aanbieders van kritieke infrastructuur bevatten in de meeste gevallen een planning van respons op incidenten en het verplicht melden van deze cyberincidenten. [24] De BSI en het federale netwerkagentschap (verantwoordelijk voor de regulering van de markten voor elektriciteit, gas, telecommunicatie, post en spoorwegen) handhaven zowel op de IT Security Act als op de NIB-richtlijn en kunnen boetes opleggen aan kritieke infrastructuurbeheerders (inclusief telecommunicatieproviders) die niet zorgen voor de juiste kennisgevingen of voldoen aan periodieke programma-evaluatie en certificatienormen.

UP Bund (Implementatieplan voor IT-beveiliging in de federale overheid)

Federale overheden in Duitsland zijn met de bepalingen uit de UP Bund (Implementatieplan voor IT-beveiliging in de federale overheid) verplicht om de 'IT-Grundschutz' volledig te implementeren. Dit betekent ook dat voldaan moet worden aan de eisen van informatiebeveiliging en dat informatiebeveiliging audits moet worden uitgevoerd. Deze audits vormen een bouwsteen bij de uitvoering van het Nationaal plan voor de bescherming van informatie-infrastructuur (NPSI) en het Implementatieplan voor IT-beveiliging in de federale overheid (UP Bund). De UP en NPSI werden ontwikkeld onder verantwoordelijkheid van het Federale Ministerie van Binnenlandse Zaken (BMI) en zijn van toepassing op alle federale ministeries en hun bedrijfsonderdelen.

NALEVING EN TOEZICHT OP DE VEREISTEN IN DE DIGITALE OVERHEID

De BSI en het Federal Network Agency (verantwoordelijk voor de regulering van de elektriciteits-, gas-, telecommunicatie-, post- en spoorwegmarkten) handhaven zowel de IT-beveiligingswet als

[23] Paul Voigt. 2018. 'Information Security Considerations: Germany', Practical Law of Thomson Reuters. As of 31 October 2019: https://united-kingdom.taylorwessing.com/en/documents/get/1552/information-security-considerations-germany.pdf_show_on_screen.

[24] Paul Voigt. 2018. 'Information Security Considerations: Germany', Practical Law of Thomson Reuters. As of 31 October 2019: https://united-kingdom.taylorwessing.com/en/documents/get/1552/information-security-considerations-germany.pdf_show_on_screen.

de NIB Implementatiewet en kunnen bestuurlijke boetes opleggen aan kritieke infrastructuurbeheerders (inclusief telecommunicatieproviders). Boetes kunnen worden opgelegd als de aanbieders niet voldoen aan de eis van kennisgevingen of aan de periodieke programma-evaluatie en certificatienormen. Ten aanzien van exploitanten van openbare websites, sociale media en andere online diensten kunnen de boetes oplopen tot € 50.000,-. Binnen Duitsland kunnen verschillende nationale autoriteiten boetes opleggen aan telemedia-dienstverleners die geen passende maatregelen voor gegevensbeveiliging implementeren. De bevoegde overheidsinstantie verschilt per staat (bijv. In Beieren is het Beierse staatsagentschap voor gegevensbescherming verantwoordelijk voor het opleggen van boetes aan telemedia-serviceproviders).

UP Bund (Implementatieplan voor IT-beveiliging in de federale overheid)
Op overheidsniveau voert de werkgroep Informatiebeveiliging Management (Arbeitsgruppe Informationssicherheitsmanagement - AG ISM) jaarlijks onderzoeken uit bij de hele federale overheid, inclusief centrale IT-leveranciers. Deze werkgroep controleert hoe overheden de regels en eisen uit het UP Bund naleven. Op basis van de onderzoeksresultaten produceert het Ministerie van Binnenlandse Zaken (BMI) een rapport met daarin de status van alle afdelings- en IT-leveranciers.

Op Ministerieel en Departementaal niveau moeten informatiebeveiligingsmaatregelen regelmatig worden gecontroleerd op effectieve implementatie, tijdigheid, volledigheid en adequaatheid om beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen. Het is daarbij van belang dat de onafhankelijkheid van de auditors wordt gewaarborgd en dat deze in de audit zowel in gaat op de technische, organisatorische en procedurele aspecten.[25] UP Bund schrijft voor dat overheden een continu verbeterproces moeten inrichten op basis van een Plan-Do-Check-Act model als onderdeel van een Information Security Management System (ISMS). De overheidsinstellingen moeten zelfstandig de naleving kunnen aantonen en voeren daarom dus regelmatig informatiebeveiligingsaudits, volwassenheidsbeoordelingen en/of penetratietesten uit.

In de regelgeving wordt niet aangegeven wat er gebeurt als een overheidsinstelling niet voldoet aan de minimale beveiligingsvereisten uit de UP Bund.

[25] Umsetzungsplan Bund 2017. As of 7 November 2019: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html

4.4 Uitkomsten Estland

OVERZICHT VAN VITALE INFRASTRUCTUUR STRATEGIE IN ESTLAND

In Estland wordt de bescherming van vitale/kritieke infrastructuur gecontroleerd door de Information System Authority (RIA), een agentschap van het ministerie van Economische Zaken en Communicatie.[26] De activiteiten van de RIA worden gereguleerd door vier instrumenten:

1. De Cybersecurity Act: Deze wet legt de verplichtingen vast voor dienstverleners om de cyberbeveiliging van netwerk- en informatiesystemen te waarborgen en de basis voor meldingen van cyberincidenten; de wet bevat ook de criteria voor cyberincidenten met een significante impact. Bovendien regelt de wet de taken van de informatiesysteemautoriteit bij het coördineren van cyberveiligheid en het organiseren van grensoverschrijdende samenwerking.[27]
2. De Emergency Act: Deze wet voorziet in de rechtsgrondslagen voor crisisbeheersing, inclusief het voorbereiden en oplossen van een noodsituatie en het waarborgen van de continuïteit van vitale diensten.[28]
3. Een verordening over de vereisten voor risicoanalyse en informatiesystemen en een beschrijving van beveiligingsmaatregelen.[29]
4. De NIB-richtlijn.[30]

Bij het vervullen van haar taken draagt RIA bij aan de implementatie van de Cyber Security-strategie van het land, waarin de nadruk wordt gelegd op de noodzaak om verdere manieren te ontwikkelen om kritieke infrastructuur te beschermen tegen verschillende beveiligingsrisico's.[31]

IDENTIFICATIE EN BEHEER VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

Estland streeft uitgebreide e-governance-initiatieven en gedigitaliseerde oplossingen na. Daarom heeft het land gekozen voor een alomvattend cyberbeveiligingskader dat van toepassing is op alle dienstverleners en organisaties.[32] Volgens Kitsing (2011) gaat Estland's sterke traditie in het ontwikkelen van ICT-oplossingen terug tot investeringen in cybernetica en computerprogrammeer onderzoek vanaf de jaren zestig, waardoor de professionele gemeenschap goed gepositioneerd is in het bevorderen van ICT-ontwikkeling nadat het land de onafhankelijkheid van de Sovjet-Unie had hersteld in 1991.[33] Estlandse politici willen ook graag ICT-oplossingen omarmen als een manier om een 'minimale en efficiënte staat' te realiseren.[34] Daartoe heeft het land sinds 1997

[26] Interview met een werknemer van de RIA, 26 September 2019.

[27] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523052018003/

[28] https://www.riigiteataja.ee/en/eli/513062017001/

[29] https://www.ria.ee/sites/default/files/content-editors/KIIK/requirements-for-risk-analysis.pdf

[30] RIA (2019). https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html

[31] Estonian Ministry of Economic Affairs and Communications (2019, 30). https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

[32] Interview met een werknemer van de RIA, 26 September 2019.

[33] Kitsing (2019, 5), https://onlinelibrary.wiley.com/doi/pdf/10.2202/1944-2866.1095.

[34] Kitsing (2019, 6).

verschillende initiatieven genomen om het gebruik van ICT-toepassingen in het openbaar bestuur te stimuleren.[35]

Het huidige kader bouwt voort op twee belangrijke stukken wetgeving die betrekking hebben op gebieden die relevant zijn voor de bescherming van kritieke infrastructuur: de Emergency Act en de Cybersecurity Act. De Emergency Act definieert de kritieke infrastructuursectoren van Estland, waaronder diensten die een significante impact hebben op het functioneren van de samenleving en waarvan de onderbreking een onmiddellijke bedreiging vormt voor het leven of de gezondheid van mensen of voor de werking van een andere vitale dienst van dienst van algemeen belang.[36] De Emergency Act (hoofdstuk 5) somt een lijst op van verschillende vitale diensten en wijst verantwoordelijkheden toe voor het verzekeren van de dienstverlening aan verschillende ministeries. Zo is bijvoorbeeld het ministerie van Economische Zaken en Communicatie belast met het toezicht op de veerkracht en de paraatheid van dienstverleners in de sectoren die verband houden met gegevensoverdracht, digitale identificatie en digitale ondertekening.[37] De organisaties die worden beschouwd als aanbieders van vitale diensten zijn verplicht om analyses van risicobeoordeling te verstrekken, beoordeeld door de relevante serviceorganisator.[38] Deze materialen worden verder gebruikt om analyses op nationaal niveau op te stellen over de implicaties van afhankelijkheden tussen verschillende dienstverleners en sectoren. [39]

EISEN EN VERPLICHTINGEN AAN VITALE INFRASTRUCTUREN IN DE DIGITALE OVERHEID

De Cybersecurity Act, waarbij de NIB-richtlijn is omgezet in Estlandse wetgeving, regelt specifiek de 'vereisten voor het onderhoud van netwerk- en informatiesystemen die essentieel zijn voor het functioneren van de samenleving en de staat'.[40] Het is van toepassing op alle nationale en lokale autoriteiten en particuliere organisaties die een jaaromzet van meer dan € 10.000.000,- hebben of meer dan 50 personeelsleden in dienst hebben.[41] Het legt de verplichtingen vast voor dienstverleners om de cybersecurity van netwerk- en informatiesystemen te waarborgen en de basis voor meldingen van cyberincidenten; de wet bevat ook de criteria voor cyberincidenten met een significante impact.[42] Bovendien regelt het ‘de taken van de informatiesysteemautoriteit bij het coördineren van cyberveiligheid en het organiseren van grensoverschrijdende samenwerking’ en houdt het een register bij van cyberincidenten.[43]

Om de veerkracht en beveiliging van vitale overheidsdiensten te bevorderen, stelt de Cybersecurity Act ook eisen voor dienstverleners, die beoordelingen moeten opstellen met

[35] E-Estonia (2019). https://e-estonia.com/

[36] Riigi Teataja (2017, § 2 (4)).

[37] Riigi Teataja (2017, § 36 (7)-(8)).

[38] ENISA (2014, 19).

[39] ENISA (2014, 19).

[40] Riigi Teataja (2018, § 1 (1)).

[41] Riigi Teataja (2018, § 1 (3)) + interview met een werknemer van de RIA, 26 September 2019.

[42] https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html

[43] https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html

inbegrip van de potentiële risico's die van invloed zijn op 'de beveiliging van het systeem', het schadelijke effect inschatten dat cyberincidenten kunnen hebben op het systeem en stelt een procedure vast voor het omgaan met incidenten.[44] Serviceproviders zijn ook verplicht om de opkomst van incidenten die een bedreiging voor hun veiligheid vormen te monitoren, de effectiviteit van hun risicobeperkende strategieën te evalueren en te documenteren. In overeenstemming met de NIS-richtlijn moeten deze organisaties ook de RIA op de hoogte stellen van cyberincidenten.

NALEVING EN TOEZICHT OP DE VEREISTEN IN DE DIGITALE OVERHEID

Op het gebied van monitoring en compliance hanteert RIA verschillende benaderingen. Ten eerste kan RIA via het Computer Emergency Response Team (CERT-EE) indien nodig helpen bij het beheer van incidenten. Voor overheidsdiensten voert RIA ook beveiligingscontroles en audits uit om de naleving te controleren en mogelijke beveiligingskwetsbaarheden te identificeren. Als RIA constateert dat een organisatie of serviceprovider niet voldoet aan de cyberbeveiligingsvereisten uit de Cybersecurity Act, kan het boetes opleggen tot € 20.000,-. [45] Tot op heden zijn dergelijke boetes door de RIA nog niet opgelegd.

Omdat de serviceproviders verantwoordelijk blijven voor de beveiliging van hun netwerken, hebben ze er belang bij RIA's suggestie te implementeren om hun betrouwbaarheid te maximaliseren.[46] Over het algemeen is het huidige kader voldoende gebleken om een efficiënt beheer van de netwerk- en infrastructuurbeveiliging in Estland te waarborgen.[47] Er blijven echter enkele kleine problemen bestaan. Niet alle dienstverleners, zowel in de openbare als in de particuliere sector, voldoen aan de vereisten van de twee besluiten, ondanks de dreiging van de boetes. Dit komt vooral door het gebrek aan financiële en personele middelen om de vereisten van de wetgeving te kunnen implementeren. Verder heeft RIA enkele problemen in de beveiliging van de toeleveringsketen geïdentificeerd. Sommige diensten zijn niet noodzakelijk ‘vitaal’, maar aangezien hele sectoren van de economie afhankelijk zijn, zou een verstoring in de keten tot problemen kunnen leiden. Een voorbeeld van dergelijke 'knelpunten' is het aanbieden van diensten met betrekking tot online platforms die transportbedrijven gebruiken om tickets te verkopen. RIA is momenteel bezig met het in kaart brengen van de toeleveringsketens van kritieke sectoren om ‘knelpunten’ te identificeren en manieren te vinden om hun integriteit te waarborgen. Bij gebrek aan een ‘concrete methodologie’ werkt het nauw samen met de bedrijven in de sectoren om ‘knelpunten’ te vinden. Dit is echter nog in ontwikkeling en het is onduidelijk hoe deze providers in de toekomst zouden worden ingekapseld door de Cybersecurity Act.[48]

[44] Riigi Teataja (2018, § 7 (2)).

[45] Interview met een werknemer van de RIA, 26 September 2019.

[46] Interview met een werknemer van de RIA, 26 September 2019.

[47] Interview met een werknemer van de RIA, 26 September 2019.

[48] Interview met een werknemer van de RIA, 26 September 2019.

4.5 Uitkomsten Spanje

OVERZICHT VAN VITALE INFRASTRUCTUUR STRATEGIE IN SPANJE

Spanje heeft in 2019 een Nationale Cybersecurity Strategie gelanceerd.[1] Hierin geeft de regering aan dat cyberspace niet alleen virtueel is maar ook afhankelijk is van fysieke en logische elementen. Apparatuur, componenten en systemen binnen communicatienetwerken kunnen worden blootgesteld aan storingen waardoor ze niet meer correct werken. Kwaadaardige acties kunnen de juiste werking van vitale/kritieke infrastructuren en daarvan afhankelijke essentiële diensten in gevaar brengen. Dit risico ziet Spanje versterkt worden door het belang van commerciële criteria boven beveiligingscriteria bij het ontwerpen van hardware- en software, systemen en services. Al deze aspecten en de toenemende interconnectiviteit tussen deze systemen kunnen cascade-effecten veroorzaken met onvoorspelbare resultaten.

In 2007 heeft de Spaanse regering het Nationaal Centrum voor bescherming van kritieke infrastructuur en cyberveiligheid opgericht (hierna het CNPIC).[49] Deze instantie is verantwoordelijk voor de bevordering, coördinatie en supervisie van alle beleidsmaatregelen en activiteiten met betrekking tot de bescherming van Spaanse kritieke/vitale infrastructuren en cyberveiligheid. [50] CNPIC valt onder de Staatssecretaris van Veiligheid, die toezicht houdt op het nationale systeem voor de bescherming van kritieke infrastructuur en het cybersecuritybeleid van het ministerie van Binnenlandse Zaken. Het CNPIC speelt een centrale rol bij het verminderen van bedreigingen door adequate mechanismen op te zetten om de essentiële diensten en vitale infrastructuren van Spanje te beschermen.[51]

De activiteiten en het mandaat van de CNPIC zijn wettelijk neergelegd in de *Ley 8/2011* en bij Koninklijk Besluit 704/2011. Naast deze wetgeving heeft Spanje de Europese NIB-richtlijn omgezet in de Wet 36/2015, die gericht is op nationale veiligheid; en het Koninklijk Besluit 3/2010, dat het nationale beveiligingskader van Spanje regelt. Voortgaande wetgevingen bepalen de norm voor de beveiliging van informatiesystemen in de publieke sector.[52]

De CNPIC pakt de cyberveiligheidsrisico's aan op drie manieren:

1. Ten eerste heeft het een systeem voor de bescherming van kritieke infrastructuur ingesteld (CIP-systeem). Dit systeem faciliteert de samenwerking tussen particuliere organisaties en de publieke sector die een gezamenlijke verantwoordelijkheid hebben bij het leveren van essentiële diensten en veiligheid aan burgers in Spanje.
2. Ten tweede hanteert het CNPIC een uitgebreide aanpak voor beveiligingskwesties waarbij men de nadruk legt op systeemrisico's in de fysieke, cyber- en individuele beveiligingsdimensies.

[49] CNPIC: *Centro Nacional de Protección de Infraestructuras y Ciberseguridad.*

[50] National Centre for Critical Infrastructure Protection and Cybersecurity [CNPIC]. 2019. 'The Center - Origins.' As of 30 October 2019: http://www.cnpic.es/

[51] Interview met een werknemer van CNPIC, 24 Oktober 2019.

[52] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

3. Tot slot bevordert de CNPIC de publiek-private partnerschappen om te zorgen voor een effectieve samenwerking tussen publieke en private actoren die zich bezighouden met de bescherming van kritieke infrastructuur. Dit stimuleert de particuliere en openbare organisaties om de verantwoordelijkheid te delen bij het waarborgen van de bescherming en veiligheid van de essentiële diensten. Hierdoor ontstaat een nauwere samenwerking tussen de CNPIC en organisaties verantwoordelijkheid voor de kritieke infrastructuur.

De Spaanse regering publiceerde in 2019 haar nationale cybersecurity-strategie, deze strategie beschrijft hoe Spanje de toekomstige NIB-richtlijn wilde omzetten in haar nationale cybersecurity-systeem.[53] De strategie heeft tot doel een uitgebreid en geïntegreerd beveiligingsmodel te genereren dat zowel functioneert op technisch, operationeel en strategisch niveau.

IDENTIFICATIE EN BEHEER VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

Essentiële diensten in de Spaanse context

Na de oprichting van het CNPIC wilde het een overzicht/register maken van infrastructuren in samenwerking met de nationale politie en de Guardia Civil. De missie van het CNPIC werd later uitgebreid om te bouwen aan een sterker en uitgebreider beveiligingssysteem in Spanje.[54] Met deze nieuwe taak verbeterde de CNPIC haar samenwerking met de verschillende actoren die deel uitmaken van het beveiligingslandschap in Spanje, waaronder de publieke en private instanties die vitale infrastructuur beheren en de essentiële dienstverleners.[55]

Naast de zeven sectoren uit de Europese NIB-richtlijn heeft Spanje de volgende sectoren ook in haar CIP-strategie opgenomen: administratie/overheid[56], ruimtevaart, nucleaire industrie, chemische industrie, onderzoek, water, energie, voedsel, gezondheid, ICT en financiële systeem.[57] Deze lijst van sectoren is opgenomen in de sectorale strategische plannen (PES) en opgenomen als bijlage bij wet 8/2011. Aangegeven is dat de aanwijzing van individuele partijen in de sectoren vertrouwelijk is en slechts op beperkte basis met officiële instanties wordt gedeeld.[58]

In de Spaanse context worden essentiële diensten gedefinieerd als "de dienst die nodig is voor het onderhoud van de fundamentele sociale functies, gezondheid, veiligheid, sociaal en economisch

[53] Departamento de Seguridad Nacional, Presidencia Del Gobierno. 2019. National Cybersecurity Strategy. Madrid: Gobierno de Espagña. As of 30 October 2019: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy

[54] Schriftelijke input van een CNPIC werknemer, 24 Oktober 2019.

[55] National Centre for Critical Infrastructure Protection and Cybersecurity [CNPIC]. 2019. 'The Center - Origins.' As of 30 October 2019: http://www.cnpic.es/en/Presentacion/index.html

[56] Het gaat hier expliciet om: Ministerie van de President, Ministerie van Binnenlandse Zaken, Ministerie van Defensie, het Nationaal Inlichtingencentrum en het Ministerie van Territoriaal beleid en openbaar bestuur.

[57] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

[58] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

welzijn van de burgers, of de effectieve werking van de Staatservices en Overheidsdiensten".[59] De nationale commissie voor de bescherming van kritieke infrastructuur (PIC-commissie) is verantwoordelijk voor het herzien en aanpassen van de lijst van essentiële diensten en ervoor te zorgen dat deze voldoen aan de normen die zijn vastgelegd in de NIB-richtlijn.[60] De PIC-commissie wijst ook kritieke exploitanten aan om toe te treden tot het CIP-systeem, op basis van het feit dat ten minste een van de infrastructuren die de exploitant in beheer heeft als een kritieke infrastructuur wordt beschouwd.

EISEN EN VERPLICHTINGEN AAN VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

Eenmaal aangewezen kritieke/vitale aanbieders moeten de aanbevelingen vanuit de CNPIC en het *'CIP Planning Template'* implementeren om de bescherming van de kritieke/vitale infrastructuur te optimaliseren.[61]

Het *'CIP Planning Template'* bestaat uit een lijst van documenten en instrumenten, die samen de nodige maatregelen bevatten om de bescherming van kritieke infrastructuur te waarborgen. Gebaseerd op de Wet 8/2011 en het Koninklijke Besluit 704/2011 en bouwt voort op de set normatieve teksten die de kritische maatregelen definiëren om de bescherming van kritieke infrastructuren te waarborgen.[62] De gezamenlijk overheidsdepartementen hebben de publieke en private exploitanten van kritieke/vitale infrastructuren samengebracht om het *'CIP Planning Template'* op te stellen.

Op strategisch niveau stelt CNPIC de criteria en richtlijnen vast om operationele capaciteiten te mobiliseren binnen overheidsdiensten die samenwerken met vitale infrastructuren en exploitanten. Deze criteria en richtlijnen bevatten preventieve maatregelen om te zorgen voor een permanente, actuele en samenhangende bescherming van het Spaanse strategische infrastructuursysteem tegen bedreigingen die ontstaan bij opzettelijke aanvallen.[63]

---

[59] National Centre for Critical Infrastructure Protection and Cybersecurity [CNPIC]. 2019. 'FAQs - CNPIC - What is an essential service? What is a Critical Infrastructure? And a Strategical Infrastructure?' As of 30 October 2019:http://www.cnpic.es/en/Preguntas_Frecuentes/What_is_an_essential_servicex_What_is_a_Critical_Infrastructurex_And_a_Strategical_Infrastructurex/index.html

[60] Interview met een werknemer van CNPIC, 24 Oktober 2019..

[61] National Centre for Critical Infrastructure Protection and Cybersecurity [CNPIC]. 2019. 'FAQs - CNPIC - What are critical operators and who are they?' As of 30 October 2019: http://www.cnpic.es/en/Preguntas_Frecuentes/Que_y_quienes_son_operadores_criticos/index.html

[62] National Centre for Critical Infrastructure Protection and Cybersecurity [CNPIC]. 2019. CNPIC - What is the critical infrastructure protection planning system?' As of 30 October 2019: http://www.cnpic.es/en/Preguntas_Frecuentes/que_es_el_sistema_de_planificacion_PIC/index.html

[63] National Centre for Critical Infrastructure Protection and Cybersecurity [CNPIC]. 2019. 'CNPIC - What is the critical infrastructure protection planning system?' As of 30 October 2019: http://www.cnpic.es/en/Preguntas_Frecuentes/que_es_el_sistema_de_planificacion_PIC/index.html

De nationale bescherming van kritieke infrastructuur wordt aangevuld met specifieke sectorale strategische plannen (PES). Deze sectorale strategische plannen wijzen de essentiële diensten aan binnen de 12 sectoren die moeten voldoen aan de CIP-maatregelen.[64] De plannen beschrijven hoe de essentiële diensten werken, welke kwetsbaarheden ze hebben en wat voor mogelijke gevolgen uitval heeft en beschrijft strategische maatregelen in het geval dat onderhoud moet worden gepleegd.[65]

Op operationeel niveau moeten de aangewezen vitale/kritieke infrastructuur beheerders een Operational Security Plans (PSO) en Specific Protection Plan (PPE) hebben opgesteld. Deze zijn in Spanje essentieel om te voldoen aan de opgestelde CIP-voorschriften.

- Het PSO beschrijft het overkoepelende beveiligingsbeleid voor de vitale/kritieke infrastructuur beheerders en geeft een overzicht van de geleverde essentiële diensten, welke risicoanalysemethode men toepast en welke criteria worden gebruikt om een passend beveiligingsbeheer te implementeren.[66]
- Het PPE is bedoeld als leidraad voor de identificatie van infrastructuur en de beveiligingsorganisatie. Het presenteert de resultaten uit risicoanalyses en een actieplan om de infrastructuur voldoende te beveiligen.

Tot slot bestaan er nog operationele ondersteuningsplannen (PAO's). Deze zijn ontwikkeld door een nationale beleidsgroep die verantwoordelijk is voor de bescherming van kritieke infrastructuur in Spanje.

- PAO's schrijven geplande bewakings-, preventie-, beschermings- en reactiemaatregelen voor die overheidsdiensten moeten nemen indien sprake is van een onmiddellijke dreiging gericht op de kritieke/vitale infrastructuur of als het Nationaal plan voor bescherming van kritieke infrastructuur door de toezichthouder CNPIC wordt geactiveerd. De maatregelen vormen daarbij een aanvulling op de specifieke beschermingsplannen (*zie de PPE*) die door de vitale/kritieke infrastructuur beheerders zelf al worden gehanteerd.

Aanvullende maatregelen en hulpmiddelen

Het Spaanse National Cryptologic Centre heeft voorschriften, richtlijnen en aanbevelingen opgesteld om de cybersecurity binnen openbare en particuliere organisaties te verbeteren. Dit worden de CCN-STIC-beveiligingsgidsen genoemd en afkomstig uit het referentiedocument omtrent CSIRT's.[67] Daarbij is een onderscheid aanwezig tussen enerzijds dienstverleners in de

[64] National Centre for Critical Infrastructure Protection and Cybersecurity [CNPIC]. 2019c. 'CNPIC - What is the critical infrastructure protection planning system?' As of 30 October 2019: http://www.cnpic.es/en/Preguntas_Frecuentes/que_es_el_sistema_de_planificacion_PIC/index.html

[65] Interview met een werknemer van CNPIC, 24 Oktober 2019.

[66] National Centre for Critical Infrastructure Protection and Cybersecurity [CNPIC]. 2019. 'CNPIC - What is the critical infrastructure protection planning system?' As of 30 October 2019: http://www.cnpic.es/en/Preguntas_Frecuentes/que_es_el_sistema_de_planificacion_PIC/index.html

[67] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

publieke en de private sector. Elke sector heeft zijn eigen Computer Emergency Response Team (CERT). De CCN-CERT is voor dienstverleners binnen de overheid, terwijl ICIBE_CERT wordt gebruikt voor dienstverleners in private sectoren.[68] Beide CERT's zorgen voor bescherming tegen cyberaanvallen op de geclassificeerde systemen en reageren op cyberincidenten die bij kritieke/vitale infrastructuursystemen zich kunnen voordoen.[69]

Naast de CERT's heeft het Spaanse National Cryptologic Centre zogenaamde *guides* beschikbaar gesteld. Deze *guides* vormen een hulpmiddel om per sector te bepalen welke aanbieders (privaat of publiek) essentiële diensten leveren. Het CNPIC en de CCN-CERT hebben gezamenlijk deze tool ontwikkelt. Voor iedere sector heeft men een eigen methodologie toegepast waarbij rekening houdend is gehouden de specifieke bijzonderheden die spelen in de sector. Met de tool kunnen essentiële dienstverlener bepalen hoe afhankelijk ze zijn van andere netwerken en informatiesystemen. Verder dient men ook te beoordelen hoe afhankelijk de essentiële dienstverlener is van andere sectoren, wat de geografische reikwijdte is van de dienst, of beschikbare alternatieven aanwezig zijn, het aantal gebruikers dat gebruik maakt van de dienst, hoeveelheid goederen de dienst heeft en impact van de dienstverlening bij uitval.

De hiervoor beschreven tool kan niet worden gedeeld met VKA, omdat deze alleen wordt aangeboden in Spanje bij de sectorale strategische plannen (zie PES). Deze PES plannen zijn eveneens niet beschikbaar omdat deze vertrouwelijk zijn.[70]

NALEVING EN TOEZICHT OP DE VEREISTEN IN DE DIGITALE OVERHEID

De omzetting van o.a. de NIB-richtlijn in het nationale wetgeving van het Koninklijk Besluit 8/2018 beoogt te waarborgen dat digitale en essentiële dienstverleners de gekozen regelgeving naleven. Spanje is momenteel bezig met het opstellen van de voorschriften die door dit stuk wetgeving zijn geïmplementeerd.[71]

Een aangewezen bevoegde autoriteit is ervoor verantwoordelijk dat deze voorschriften worden gehandhaafd. Dit laatste wordt gedaan door bezoeken of door certificering. Wanneer een essentiële dienstverlener als kritisch wordt beschouwd, is de bevoegde autoriteit de CNPIC. Het proactief toezicht heeft de voorkeur, maar latere forensische onderzoeken (reactief toezicht) kan ook na incident worden uitgevoerd. Voor kritieke infrastructuren en essentiële diensten kan ook onafhankelijk toezicht door derden worden gedaan via een certificeringsproces. Het koninklijk omzettingsbesluit 12/2018 bevat een lijst met sancties bij het niet-naleven van de wet.[72]

[68] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

[69] Centro Criptológico Nacional, [CCN-CERT]. 2019c. 'Mission and objectives' As of 30 October 2019: https://www.ccn-cert.cni.es/en/about-us/mission-and-objectives.html

[70] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

[71] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

[72] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

Volgens de geïnterviewde moet voor de bescherming van de vitale diensten van de overheid adequate maatregelen worden opgenomen om de omvang van het totale project (zie strategie) te beheren en moeten sterke publiek-private partnerschappen worden opgezet.[73] Daarbij geeft de geïnterviewde aan dat regeringen niet moeten onderschatten hoeveel informatiesystemen en netwerken reeds onder de NIB-richtlijn vallen. Daarbij gaf de geïnterviewde aan dat Spanje deze kwestie heeft aangepakt met behulp van een formele procedure die helpt bij het identificeren en definiëren van de systemen die moeten worden beschermd en gecontroleerd.[74] Tot slot merkte de Spaanse overheidsfunctionaris op dat publiek-private samenwerking waardevol is gebleken voor de bescherming van de vitale overheidsdiensten van Spanje. Op basis van de Spaanse ervaring geeft hij aan dat succesvolle beveiligingsmodellen integrale kaders vereisen, die ook rekening houden met fysieke beveiliging en logische beveiliging.[75]

[73] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

[74] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

[75] Schriftelijke reactie van een CNPIC werknemer, 24 Oktober 2019.

4.6 Uitkomsten Verenigd Koninkrijk

OVERZICHT VAN VITALE INFRASTRUCTUUR STRATEGIE IN HET VERENIGD KONINKRIJK

Beleid omtrent de bescherming van vitale infrastructuren in het Verenigd Koninkrijk bestaat al langere tijd. De initiële strategie was gericht op fysieke bescherming van vitale infrastructuren vanwege de toenmalige dreiging van terrorisme afkomstig uit Noord-Ierland. Later is meer focus komen te liggen op cybersecurity.[76] De regering van het Verenigd Koninkrijk (VK) definieert de huidige 'kritieke nationale infrastructuur' (CNI) dan ook als:

> *'Die kritieke elementen van infrastructuur (namelijk activa, faciliteiten, systemen, netwerken of processen en de essentiële werknemers die deze exploiteren en faciliteren), waarvan het verlies of compromitering kan resulteren in: a) grote nadelige gevolgen voor de beschikbaarheid, integriteit of levering van essentiële diensten - inclusief die diensten waarvan de integriteit, indien aangetast, zou kunnen leiden tot aanzienlijk verlies van mensenlevens of slachtoffers - rekening houdend met aanzienlijke economische of sociale gevolgen; en / of b) significante gevolgen voor de nationale veiligheid, de nationale defensie of het functioneren van de staat'.*[77]

Er bestaan 13 CNI-sectoren: chemie, civiele nucleaire industrie, communicatie, defensie, hulpdiensten, energie, financiën, voedsel, overheid, gezondheid, ruimte, vervoer en water.[78] Niet alle organisaties/partijen binnen deze sectoren wordt echter als kritisch beschouwd. De regering bepaalt de strategische aanpak voor de bescherming van kritieke infrastructuur (CIP).[79] Het bestuur van CIP wordt geleid door de National Security Council (NSC). De feitelijke verantwoordelijkheid voor de bescherming van de kritieke infrastructuren binnen de sectoren worden gedragen door een of meerdere Lead Government Department(s) (LGD) die zijn aangewezen door de overheid.[80] Bijvoorbeeld: het Department of Business, Energy and Industrial (BEIS) is verantwoordelijk voor de kritieke sector Energie (evenals Chemie, Civiel nucleair, Ruimtevaart). De LGD's moeten jaarlijkse sector veiligheids- en weerbaarheidsplannen (*Resilience*

[76] Interview met een werknemer van het Department of Government Cyber Defence - Government Security Group of the Cabinet Office, 14 November 2019.

[77] Centre for the protection of National Infrastructure [CPNI]. 2019a. 'Critical National Infrastructure.' As of 25 October 2019: https://www.cpni.gov.uk/critical-national-infrastructure-0

[78] Centre for the protection of National Infrastructure [CPNI]. 2019a. 'Critical National Infrastructure.' As of 25 October 2019: https://www.cpni.gov.uk/critical-national-infrastructure-0

[79] Centre for the protection of National Infrastructure [CPNI]. 2019b. 'Who we work with.' As of 25 October 2019: https://www.cpni.gov.uk/who-we-work

[80] An overview of critical sectors, sub-sectors and LGDs can be found in: Cabinet office. 2016. *Summary of the 2016 Sector Security and Resilience Plans*. ondon: Cabinet Office, p.6. As of 25 October 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/568546/sector_security_resilience_plans_14_11_2016.pdf

Plans) opstellen, waarbij de veerkracht van de sector wordt getoetst aan alle potentiële risico's voor de kritieke infrastructuur.[81]

Voor kritieke infrastructuren van de overheid is de Government Security Group de hoofdafdeling. Deze afdeling valt onder het Cabinet Office (Civil Contingencies Office) en rapporteert aan de Nationale veiligheidsraad. De Government Security Group biedt advies en hulpmiddelen aan overheidsactoren die als kritiek worden aangewezen. Voor de aanwijzing en identificatie van deze kritieke overheidsactoren wordt gebruik gemaakt van kriticiteit richtlijnen waarbij voornamelijk wordt gekeken naar:[82]

1. Gebruiksschaal (bijv. hoe breed wordt de overheidsservice gebruikt);
2. Financiële schaal (bijv. hoeveel geld is erbij betrokken);
3. Wat is het belang van gebruikers (bijv. is het een kritieke dienst voor burgers of bedrijven);
4. Zijn er alternatieve leveringsmechanismen (bijv. als de dienst niet beschikbaar is, zijn er dan andere manieren toch de dienst te kunnen ontvangen).

Of een overheidsdienst/infrastructuur kritiek is, wordt sterk beïnvloedt door wettelijke vereisten. Zo kan een dienst van de overheid bijvoorbeeld niet kritisch worden geacht in de termen van de normale definitie, maar kan wetgeving eisen stellen aan de beschikbaarheid (bijv. een overheidsdienst moet binnen 48 uur reageren). Door een beschikbaarheidseis in wetgeving wordt de overheidsdienst dan als vitaal aangemerkt.[83]

Het is hierbij belangrijk om te realiseren dat een groot deel van de infrastructuur die overheidsdiensten exploiteren, niet langer in (fysiek) beheer is van deze overheidspartijen. Veel van de kritieke elementen die zorgen voor de dienst zijn in handen van externe exploitanten.[84] De eigenaren en exploitanten van de kritieke infrastructuren, zijn zelf verantwoordelijk voor het verbeteren van de beveiliging en veerkracht door onderhoud, trainingen, investeringen en risicobeoordelingen.[85] Het Centrum voor de bescherming van de nationale infrastructuur (CPNI) ondersteunt de bescherming van kritieke infrastructuur door alle actoren in kritieke sectoren te

[81] Cabinet Office. 2019. *Public Summary of Sector Security and Resilience Plans 2018*. London: Cabinet Office. As of 25 October 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf

[82] Interview met een werknemer van het Department of Government Cyber Defence - Government Security Group of the Cabinet Office, 14 November 2019.

[83] Interview met een werknemer van het Department of Government Cyber Defence - Government Security Group of the Cabinet Office, 14 November 2019.

[84] Interview met een werknemer van het Department of Government Cyber Defence - Government Security Group of the Cabinet Office, 14 November 2019.

[85] Cabinet Office. 2019. *Public Summary of Sector Security and Resilience Plans 2018*. London: Cabinet Office. As of 25 October 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786206/20190215_PublicSummaryOfSectorSecurityAndResiliencePlans2018.pdf

adviseren over het aanpakken van kwetsbaarheden van de kritieke infrastructuur voor terrorisme en andere bedreigingen en is verantwoording verschuldigd aan de directeur-generaal van MI5.[86]

Het National Cyber Security Center (NCSC) maakt deel uit van het Government Communications Headquarters (GCHQ) en is verantwoordelijk voor de bescherming van de IT-netwerken, gegevens en systemen van kritieke sectoren tegen cyberaanvallen. Het NCSC is het enige contactpunt voor Europese partners en fungeert als het Computer Security Incident Response Team (CSIRT).

Voor de strategische aanpak voor de bescherming van kritieke infrastructuur CIP zijn drie documenten van bijzonder belang:

1. De nationale veiligheidsstrategie en de strategische defensie- en veiligheidsevaluatie (NSS en SDSR) uit 2015, waarin de nationale veiligheidsdoelstellingen en belangen van het VK worden uiteengezet, ook ten aanzien van de kritieke nationale infrastructuur van het land.[87]
2. De Nationale Cyber Security Strategie 2016-2021, die de strategie van de Britse overheid bepaalt om het land, en zijn kritieke nationale infrastructuur, veilig en veerkrachtig te maken in cyberspace.[88]
3. Het National Risks Register (NRR), waarin de Britse overheid de waarschijnlijkheid en potentiële impact van risico's zoals kwaadaardige bedreigingen en natuurlijke gevaren voor kritieke nationale infrastructuur heeft opgenomen en beoordeeld.[89]

IDENTIFICATIE EN BEHEER VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

Het VK heeft de NIB-richtlijn omgezet in haar nationale wetgeving: de Network and Information Systems Regulations 2018 (NISR) van 10 mei 2018.[90] De volgende sectoren worden erkend als essentieel in de NISR: energie, vervoer, gezondheid, drinkwatervoorziening en -distributie en digitale infrastructuur, waaronder zowel exploitanten van overheidsdiensten als particuliere

---

[86] Centre for the protection of National Infrastructure [CPNI]. 2019c. 'About CPNI.' As of 25 October 2019: https://www.cpni.gov.uk/about-cpni

[87] HM Government. 2015. *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*. London: HM Government. As of 25 October 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf

[88] HM Government. 2016. *The National Cyber Security Strategy 2016-2021*. London: HM Government. As of 25 October 2019: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[89] Cabinet Office. 2017. *National Risks Register (NRR): 2017 edition*. London: Cabinet Office. As of 25 October 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

[90] *The Network and Information Systems Regulations 2018*. No. 506. As of 25 October 2019: http://www.legislation.gov.uk/uksi/2018/506/contents/made

diensten. Deze sectoren zijn verder onderverdeeld in sub sectoren, die elk bevoegde autoriteiten (CA's) hebben aangewezen).[91]

Enkele artikelen van de NISR beschrijven de drempelvereisten voor een dienst die als "essentieel" moet worden beschouwd. NISR-vereisten zijn van toepassing op Operators van Essential Services (OES's) en Relevant Digital Service Providers (RDSP's). Bovendien kunnen digitale diensten met betrekking tot de 13 eerder genoemde kritieke sectoren ook als kritisch of essentieel worden beschouwd in de context van de NISR. Bovendien breidt het NCSS-gedeelte over de bescherming van de kritieke nationale infrastructuur van het VK tegen cyberaanvallen zich nog verder uit door "andere prioritaire sectoren".[92] Deze andere prioritaire sectoren zijn de meest succesvolle en waardevolle bedrijven en organisaties in het VK die "meer ondersteuning nodig hebben".[93] Deze omvatten bijvoorbeeld bedrijven en organisaties die belangrijke intellectuele eigendom bezitten, grote hoeveelheden persoonlijke gegevens bewaren, bijzonder kwetsbaar zijn voor aanvallen met ernstige gevolgen voor de stabiliteit van het land (zoals mediaorganisaties), digitale dienstverleners die e-commerce en de digitale economie van het VK mogelijk maken en invloedrijke marktkrachten en autoriteiten. In het Jaarverslag 2018 van het NCSC wordt gesteld dat de NCSC, LGD's en de industrie gezamenlijk een proces hebben ontwikkeld om de systemen te identificeren die cruciaal zijn voor de dagelijkse werking van de kritieke nationale infrastructuur van het VK, zodat de industrie en de overheid zich kunnen concentreren op die gebieden waar verbeteringen in cybersecurity de meeste impact zouden hebben.[94]

De Gemengde Commissie voor de nationale veiligheidsstrategie van het Britse parlement merkte in 2018 echter op dat het onduidelijk is "hoe de regering deze kwestie beheert of hoe zij prioriteit geeft aan haar inspanningen tussen CNI-sectoren", en dat het "de regering de variëteit en complexiteit van de CNI-sectoren en de invloed hiervan op de aanpak van de regering onvoldoende onderkent". [95] Bovendien voerde ze aan dat de hoge mate van classificatie van de

---

[91] *The Network and Information Systems Regulations 2018*. No. 506. pp.20-21. As of 25 October 2019: http://www.legislation.gov.uk/uksi/2018/506/contents/made

[92] HM Government. 2016. *The National Cyber Security Strategy 2016-2021*. London: HM Government. p.39. As of 25 October 2019: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[93] HM Government. 2016. *The National Cyber Security Strategy 2016-2021*. London: HM Government. p.40. As of 25 October 2019: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[94] National Cyber Security Centre [NCSC]. 2018. *Annual Review: Making the UK the safest place to live and work online*. London: NCSC. As of 25 October 2019: https://www.ncsc.gov.uk/files/ncsc_2018-annual-review.pdf

[95] UK Parliament. 2018. 'Cyber Security of the UK's Critical National Infrastructure.' As of 25 October 2019: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170806.htm#_idTextAnchor008

aanpak van de Britse regering het voor de particuliere sector moeilijk maakt om de prioriteiten van de regering te begrijpen, ondanks het streven van het partnerschap om CNI veerkracht tegen cyberaanvallen op te bouwen".[96]

EISEN EN VERPLICHTINGEN AAN VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

Aangezien de overheid wordt aangewezen als een van de 13 nationale infrastructuursectoren, is er ook een reeks specifieke voorschriften en vereisten die verder gaan dan die welke in de NISR zijn uiteengezet. Het HMG (HFG's Government) Security Policy Framework (SPF) beschrijft de verplichte beschermende beveiligingsresultaten die alle overheidsafdelingen moeten behalen, waaronder ook informatiebeveiliging en cybersecurityvereisten. In het bijzonder definieert de SPF de minimale beveiligingsmaatregelen die alle afdelingen wettelijk verplicht zijn om hun informatie, technologie en digitale diensten te beveiligen om te voldoen aan hun verplichtingen op het gebied van SPF en nationale cyberveiligheidsstrategieën. De SPF legt wettelijke verplichtingen voor beveiligingsafdelingen vast. De beveiligingsstandaarden definiëren zoveel mogelijk resultaten, waardoor de afdelingen flexibiliteit in de implementatie hebben om sleutelconcepten te interpreteren (bijvoorbeeld 'gevoelig', 'essentieel', 'belangrijk', 'passend') en in hun lokale context in te passen.[97] De UK Minimum Cyber Security Standard bevat tien sets minimale beveiligingsmaatregelen, zoals weergegeven in tabel 1. Dit zijn minimumvereisten en van overheidsdiensten wordt verwacht dat ze deze waar mogelijk proberen te overtreffen. De Britse regering heeft ook de ambitie om in de loop van de tijd de minimumvereisten te verhogen om de technologische ontwikkeling bij te houden of nieuwe bedreigingen of kwetsbaarheden aan te pakken.

[96] UK Parliament. 2018. 'Cyber Security of the UK's Critical National Infrastructure.' As of 25 October 2019: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170806.htm#_idTextAnchor008

[97] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710816/HMG-Security-Policy-Framework-v1.1.doc.pdf

Tabel 1 VK Minimum Cyber Security Standard[98]

	IDENTIFY
1	Afdelingen zetten passende cyber security governance-processen in.
2	Afdelingen identificeren en catalogiseren gevoelige informatie waarover zij beschikken.
3	Afdelingen identificeren en catalogiseren de belangrijkste operationele diensten die zij leveren.
4	De noodzaak voor gebruikers om toegang te krijgen tot gevoelige informatie of belangrijke operationele diensten moet worden geanalyseerd en voortdurend worden beheerd.
	PROTECT
5	Toegang tot gevoelige informatie en belangrijke operationele diensten wordt alleen verleend aan geïdentificeerde, geverifieerde en geautoriseerde gebruikers of systemen.
6	Systemen die gevoelige informatie of belangrijke operationele diensten verwerken, moeten worden beschermd tegen bekende kwetsbaarheden.
7	Account met hoge rechten mogen niet kwetsbaar zijn voor veel voorkomende cyberaanvallen.
	DETECT
8	Afdelingen nemen maatregelen om veel voorkomende cyberaanvallen op te sporen.
	RESPOND
9	Afdelingen moeten een gedefinieerde, geplande en geteste reactie hebben op cyberveiligheidsincidenten die van invloed zijn op gevoelige informatie of belangrijke operationele diensten.
	RECOVER
10	Afdelingen beschikken over goed gedefinieerde en geteste processen om de continuïteit van belangrijke operationele services te garanderen in geval van storing of compromitering.

Naast de minimale beveiligingsnormen maken overheidsorganisaties meestal ook gebruik van het UK Government Public Services Network (PSN), een krachtig netwerk dat organisaties in de publieke sector wil helpen samen te werken, duplicatie te verminderen en middelen te delen.[99] Om organisaties in de publieke sector toegang te geven tot PSN moeten ze PSN-conformiteit tonen, wat een extra manier inhoudt om beveiligingsregelingen aan de overheid te melden. Kort gezegd vereist PSN-compliancy dat de volgende aspecten worden verstrekt of voldaan (waarvan vele overlappen met de Minimum Cyber Security Standard):

- Verstrekking van een netwerkdiagram van de volledige netwerkinfrastructuur voor aansluiting op PSN

[98] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf

[99] https://www.gov.uk/government/groups/public-services-network

- Naleving van de volgende vereisten:
    - Operationele vereisten:
        - Kwetsbaarheid en patchbeheer
        - Veilige configuratie
        - Fysieke beveiliging
        - Beschermende bewaking en inbraakdetectie
        - Reactie op beveiligingsincidenten
    - Verificatie en toegangscontrole
    - Grensbeveiliging en interfaces
    - Bescherming van gegevens in opslag rust en transport
    - Scheiding van gegevens door gebruiker en administratie
    - Gebruikersbeveiliging
    - Regelmatige beveiligingstests[100]

Om de overheidsinstellingen te helpen bij hun inspanningen om de infrastructuur en diensten te beveiligen, fungeert het NCSC als de nationale technische autoriteit voor cyberveiligheid en biedt het advies en operationele cybersecurityondersteuning aan overheidsorganisaties. Het NCSC biedt ook een set hulpmiddelen en diensten aan organisaties in de publieke sector in het kader van het 'Active Cyber Defense' (ACD) -programma. ACD is een NCSC-programma dat cyberaanvallen op een relatief geautomatiseerde en schaalbare manier probeert aan te pakken om de nationale weerbaarheid te verbeteren. Het ACD-programma omvat momenteel vijf tools en services die gratis worden aangeboden aan overheidsdepartementen en organisaties in de publieke sector:

1. Mail Check - een platform voor het beoordelen van de naleving van e-mailbeveiliging die DMARC-rapporten van de hele publieke sector verzamelt, verwerkt en analyseert.
2. Web controle - een service waarmee organisaties veelvoorkomende website kwetsbaarheden kunnen identificeren en oplossen.
3. Protective Domain Name System (PDNS) - een beveiligde DNS-service voor de publieke sector.
4. Oefening in een kader - een kader voor het uitvoeren van cyberveiligheidsoefeningen voor de overheid.
5. Openbaarmaking van kwetsbaarheden - het aanbieden van kwetsbaarheidsrapportage en openbaarmaking van kwetsbaarheden.[101]

Naast de ACD beheert het NCSC ook een cybersecurity-aanpak, dit zijn de Cyber Essentials. Deze zijn gericht op het helpen van overheidsorganisaties bij het kiezen van leveranciers met passende minimale cybersecurity-eisen en daarmee ook bij het verbeteren van de cybersecurity-positie in de kritieke infrastructuur ketens.[102]

[100] Raadpleeg de PSN-webpagina voor meer informatie over de PSN-vereisten: https://www.gov.uk/guidance/apply-for-a-public-services-network-psn-connection-compliance-certificate

[101] https://www.ncsc.gov.uk/section/products-services/active-cyber-defence

[102] https://www.cyberessentials.ncsc.gov.uk

De Cyber Essentials omvatten vijf gebieden:

1. Firewalls
2. Veilige configuraties
3. Beheersing van gebruikers toegang
4. Malware bescherming
5. Patch management[103]

Organisaties kunnen ervoor kiezen om zichzelf te certificeren volgens de vereisten voor een Cyber Essentials-certificering, of een onafhankelijk certificatieproces doorlopen door een externe instantie die door het NCSC is geaccrediteerd, waardoor organisaties een Cyber Essential Plus-certificering kunnen verkrijgen.

TOEZICHT EN NALEVING OP DE VEREISTEN IN DE DIGITALE OVERHEID

Volgens de NISR, wordt toezicht op de Operators van Essential Services (OES's) uitgeoefend door sectorspecifieke Competent Authorities.[104] Bovendien biedt het NCSC technische ondersteuning en begeleiding aan de OES's. De Information Commissioner VK (ICO) is verantwoordelijk voor het toezicht op de Relevant Digital Service Providers. In plaats van een uitgebreide controlelijst,[105] vereist het NCSC dat organisaties die verantwoordelijk zijn voor vitale diensten en activiteiten, een aantal principes begrijpen die zijn vastgelegd in het Cyber Assessment Framework (CAF) van het NCSC en moeten kunnen beoordelen of hun praktijken in overeenstemming zijn met de principes en een aantal gespecificeerde hoge- niveau doelstellingen.[106]

Het toezicht op OES's is proactief: de Competent Authorities voeren regelmatig audits uit bij de OES's waarop ze toezicht houden, en zorgen ervoor dat ze voldoen aan de NISR. Ze bieden ook sectorale begeleiding en advies over versterking van de veerkracht.[107] Bovendien moeten OES's de betrokken autoriteiten binnen 72 uur op de hoogte brengen van een incident. Competent Authorities hebben de bevoegdheid om boetes uit te delen.

Anderzijds is het toezicht op Relevant Digital Service Providers door de ICO uitsluitend reactief. In tegenstelling tot OES's worden Relevant Digital Service Providers niet gecontroleerd. Ze moeten

---

[103] https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure

[104]De volledige lijst van nationale bevoegde autoriteiten: T*he Network and Information Systems Regulations 2018*. No. 506. 'Designated Competent Authorities.' As of 25 October 2019: http://www.legislation.gov.uk/uksi/2018/506/schedule/1

[105] Piggin, Richard. 2018. 'Protecting our critical infrastructure: Understanding new cyber security laws.' As of 25 October 2019: https://www.atkinsglobal.com/~/media/Files/A/Atkins-Corporate/uk-and-europe/services-documents/cyber/protecting-our-critical-infrastructure.pdf

[106] National Cyber Security Centre [NCSC]. As of 25 October 2019: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance

[107] Piggin, Richard. 2018. 'Protecting our critical infrastructure: Understanding new cyber security laws.' As of 25 October 2019: https://www.atkinsglobal.com/~/media/Files/A/Atkins-Corporate/uk-and-europe/services-documents/cyber/protecting-our-critical-infrastructure.pdf

echter wel ernstige incidenten melden aan de ICO, waardoor ze kunnen worden onderworpen aan onderzoek.[108] Zowel de CA's als de ICO hebben verschillende bevoegdheden om de NISR af te dwingen. In het geval van de ICO omvat dit informatiemeldingen, handhavingsmeldingen, strafmeldingen en inspectiebevoegdheden.[109] Boetes van ICO en de CA's kunnen oplopen tot 17 miljoen GBP.[110]

Specifiek in het kader van het PSN moeten overheidsorganisaties regelmatig 'IT Health Checks' uitvoeren met behulp van onafhankelijke, externe accrediterende beveiliging auditorganisaties.[111] Het doel van de IT Health Checks is tweevoudig:

1. Om zekerheid te bieden dat extern gerichte systemen worden beschermd tegen ongeautoriseerde toegang of wijziging;
2. Verzekeren dat interne netwerken en systemen geen significante zwakke punten vertonen waardoor het ene interne apparaat opzettelijk of onbedoeld invloed kan hebben op de beveiliging van een ander.

Het NCSC voert een accreditatieschema uit voor goedgekeurde leveranciers van penetratietests die IT Health Checks voor de overheid kunnen leveren.[112]

Als overheidsorganisaties 'kritieke' of 'grote' tekortkomingen hebben als onderdeel van een IT Health Check, dan moet de organisatie een Remediation Action Plan (RAP) opstellen om deze problemen aan te pakken om de PSN-naleving te handhaven. Een RAP moet minimaal informatie bevatten over:

- Specifieke acties die moeten worden ondernomen;
- Geplande start- en afronding van de werkzaamheden;
- Gegevens van de verantwoordelijke persoon;
- Een onderbouwde uitspraak waarin wordt uitgelegd hoe vergelijkbare problemen in de toekomst worden voorkomen.

Verder geldt voor specifieke de kritieke overheidsdiensten dat men jaarlijks een zelfevaluatie moeten uitvoeren op basis van een verstrekte vragenlijst vanuit de Government Security Group. Hierbij wordt de kanttekening gegeven dat deze zelfevaluaties een oppervlakkig beeld geven van

[108] Information Commissioner UK [ICO]. 2019. 'Enforcement.' As of 25 October 2019: https://ico.org.uk/for-organisations/the-guide-to-nis/enforcement/

[109] Information Commissioner UK [ICO]. 2019. 'Enforcement.' As of 25 October 2019: https://ico.org.uk/for-organisations/the-guide-to-nis/enforcement/

[110] *The Network and Information Systems Regulations 2018*. No. 506. Art. 17. As of 25 October 2019: http://www.legislation.gov.uk/uksi/2018/506/contents/made

[111] https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance/it-health-check-ithc-supporting-guidance

[112] https://www.ncsc.gov.uk/section/products-services/ncsc-certification

de genomen maatregelen. Om zekerheid te verkrijgen is het vereist dat het proces van zelfevaluatie wordt uitgevoerd door een interne audit afdeling of door een externe auditor.[113]

Naast zelfevaluatie heeft de Government Security Group ook de beschikking over een RED-team dat beveiliging binnen een overheidsdienst kan testen. Deze testen worden uitgevoerd via een GBEST-assessment methodiek die een afgeleide is van de CBEST banken-methode.[114] Het uitvoeren van een GBEST assessment is arbeidsintensief waardoor jaarlijks slechts 6 tot 8 GBEST assessments kunnen worden uitgevoerd terwijl er 45 overheidsdepartementen zijn binnen het Verenigd Koninkrijk. De overheid van het Verenigd Koninkrijk is dan ook aan het verkennen of deze GBEST methode breder kan worden ingezet of kan worden aangepast zodat de assessments sneller kunnen worden uitgevoerd (bijvoorbeeld door de scope in te perken of te zorgen voor meer automatisering).[115]

Government Security Group ziet nog vele uitdagingen met name ten aanzien van:[116]

1. Gebruik van oude legacy IT-apparatuur;
2. Het slimmer hergebruiken en centraal inzetten van oplossingen en methodes (in plaats dat elk overheidsorgaan het zelf aanpakt);
3. Het meer inzetten op overheid brede beveiligingsplatforms met gemeenschappelijke beveiligingscomponenten voor ingewikkelde beveiligingsproblemen (platform-as-a-service voor de overheid). Veel overheidsdiensten binnen het Verenigd Koninkrijk maken bijvoorbeeld gebruik van online services die financiële transacties bieden, dit zou meer gestandaardiseerd en gefaciliteerd kunnen worden door de centrale overheid.

Als blijkt dat een overheidsdienst niet voldoet aan de gestelde eisen wordt gerapporteerd naar het bestuur van de overheidsdienst. De betreffende overheidsdienst dient dan een herstelplan (inclusief kosten) op te leveren waarbij de Government Security Group (GSG) zal helpen. De ervaring vanuit het GSG is dat dergelijke rapportages een hefboom vormen om de maatregelen t.a.v. beveiliging en de financiering te verkrijgen vanuit de bestuurders.[117] Indien beveiligingsmaatregelen onvoldoende zijn en persoonsgegevens hierdoor geraakt worden bestaat er ook een mogelijkheid dat de overheidsdienst bestuurlijke boetes krijgt opgelegd op basis van de GDPR.

Als ultimum remedium en in zeldzame gevallen kan GSG besluiten om de crypto grafische toegang tot gevoelige overheidsnetwerken/gerubriceerde informatie van een overheidsdienst in te

---

[113] Interview met een werknemer van het Department of Government Cyber Defence - Government Security Group of the Cabinet Office, 14 November 2019.

[114] https://www.crest-approved.org/gbest/index.html

[115] Interview met een werknemer van het Department of Government Cyber Defence - Government Security Group of the Cabinet Office, 14 November 2019.

[116] Interview met een werknemer van het Department of Government Cyber Defence - Government Security Group of the Cabinet Office, 14 November 2019.

[117]Interview met een werknemer van het Department of Government Cyber Defence - Government Security Group of the Cabinet Office, 14 November 2019.

trekken. Dit kan alleen als een overheidsdienst/afdeling ernstige tekortkomingen heeft in de informatiebeveiliging die niet zijn of tijdig worden opgelost.[118]

[118] Interview met een werknemer van het Department of Government Cyber Defence - Government Security Group of the Cabinet Office, 14 November 2019.

4.7 Uitkomsten Zweden

OVERZICHT VAN VITALE INFRASTRUCTUUR STRATEGIE IN ZWEDEN

In Zweden is de bescherming van kritieke infrastructuur over het algemeen gekoppeld aan ‘vitale maatschappelijke functies’, geïdentificeerd als diensten die worden verleend op het niveau van de lokale, regionale en nationale autoriteiten.[119] In 2011 is een strategie voor de bescherming van deze infrastructuren aangenomen.[120] De strategie definieert 'vitale maatschappelijke functies' als functies die zo belangrijk zijn dat verlies of ernstige verstoring grote risico's of gevaren voor het leven met zich mee kan brengen en de gezondheid van de bevolking, de functionaliteit van de samenleving of de fundamentele waarden van de samenleving.

Drie jaar na de publicatie van de strategie heeft het Zweedse bureau voor civiele contingenties (MSB) een actieplan opgesteld voor de implementatie van de strategie, waarin werd opgeroepen tot een drieledige aanpak die de nadruk legde op een systeembenadering op meerdere niveaus en een ruim begrip van risicotypes.[121]

Alle diensten die het uitvoeren van vitale maatschappelijke functies ondersteunen, kunnen als essentieel worden beschouwd, hoewel kritieke infrastructuur in de Zweedse terminologie voornamelijk fysieke structuren betreffen. Zweden wijst in totaal 11 sectoren aan die ‘vitaal’ worden aangemerkt:[122]

1. Energievoorziening
2. Financiële diensten
3. Gezondheidszorg
4. Informatie en communicatie
5. Voedselvoorziening
6. Veiligheid en beveiliging
7. Transport
8. Handel en industrie
9. Lokale overheidsinfrastructuur
10. Publieke administratie
11. Sociale verzekering

De bescherming van kritieke infrastructuur in Zweden werkt volgens de drie fundamentele principes van het Zweedse crisisbeheersingssysteem:

---

[119] RECIPE Guidelines: Resilience of Critical Infrastructure Protection:
As of 7 November 2019: https://ec.europa.eu/echo/sites/echo-site/files/recipe_guidelines.pdf 14-15.

[120] MSB: A functioning society in a changing world. As of 7 November 2019:
http://www.qcert.org/sites/default/files/public/documents/SE-CIIP-RP-A%20Functioning%20Society%20In%20A%20Changing%20World-Eng-2011.pdf

[121] MSB: Samhällsviktig verksamhet. As of 7 November 2019: https://www.msb.se/samhallsviktigverksamhet

[122] MSB: Samhällsviktig verksamhet. As of 7 November 2019: https://www.msb.se/samhallsviktigverksamhet

1. Het verantwoordelijkheidsbeginsel, dat bepaalt dat het agentschap of de afdeling die verantwoordelijk is voor een functie, die verantwoordelijkheid ook tijdens een crisissituatie moet behouden.
2. Het gelijkheidsbeginsel, dat bepaalt dat functies zo normaal mogelijk moeten blijven tijdens de crisis.
3. Het subsidiariteitsbeginsel, dat bepaalt dat beslissingen moeten worden genomen op het meest directe of lokale niveau dat het dichtste bij de ervaren problematiek staat.

In de praktijk betekent dit dat de bescherming van kritieke infrastructuur wordt uitgevoerd via een systeem van gedistribueerde verantwoordelijkheid waarbij organisaties de verantwoordelijkheid dragen om de voortdurende bescherming van vitale infrastructuur of diensten die zij exploiteren of bieden te waarborgen. Het Zweedse Civil Contingencies Agency (MSB) heeft een overkoepelend mandaat om zowel crisisbeheersing als voortdurende bescherming van kritieke infrastructuur te coördineren.

Deze aanpak strekt zich ook uit tot cyberbeveiliging en de cyberbeveiliging van vitale diensten. Binnen de Zweedse context wordt cybersecurity benaderd vanuit het perspectief van vertrouwelijkheid, integriteit en beschikbaarheid en toegepast op alle organisaties - zowel publieke als private. Volgens het verantwoordelijkheidsbeginsel dragen alle organisaties fundamenteel de verantwoordelijkheid om te zorgen voor passende cybersecurity-regelingen. Er is echter ook een verzameling van zeven overheidsorganisaties met extra verantwoordelijkheden of directe toezichthoudende taken voor bepaalde organisaties, zoals weergegeven in tabel 1.

Tabel 1 Overheidsinstanties die verantwoordelijk zijn voor cyberbeveiliging van vitale diensten[123]

Organisatie	Verantwoordelijkheden
De Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap (MSB)	De overkoepelende verantwoordelijkheid van MSB is de coördinatie van nationale inspanningen op het gebied van cyberveiligheid.
De Zweedse Data Protectie Autoriteit (*Datainspektionen)*	De Zweedse Autoriteit voor gegevensbescherming is de regelgevende autoriteit die verantwoordelijk is voor de bescherming van de persoonlijke integriteit en gegevens.
De Zweedse strijdkrachten (Försvarsmakten)	De Zweedse strijdkrachten hebben taken op het gebied van informatiebeveiliging ter ondersteuning van de nationale veiligheid met betrekking tot beveiligde cryptografische functies, beveiliging en signaalbescherming.

[123]Bron: MSB: Myndigeter med ansvar. 7 November 2019: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/informationssakerhet-i-samhallet/myndigheter-med-ansvar/

De Zweedse defensie-materieeladministratie (Försvarets materielverk (FMV))	FMV voert sinds het einde van de jaren tachtig evaluaties uit van IT-producten en -systemen binnen zijn eigen organisatie en is al lang actief betrokken bij de internationale normalisatiewerkzaamheden op het gebied van informatiebeveiliging.
Het nationale radio-eenheid voor defensie (Försvarets radioanstalt (FRA))	FRA heeft twee kerngebieden: informatiebeveiliging en signaalinlichtingendiensten.
De Post- en Telecom-autoriteit (Post- och telestyrelsen (PTS))	PTS controleert de gebieden van elektronische communicatie en post in Zweden. De taken van de autoriteit omvatten het bevorderen van toegang tot veilige en efficiënte elektronische communicatie, waaronder telecommunicatie, internet en radio.
Het Agentschap voor digitale overheid (Myndigheten för digital förvaltning (DIGG))	De missie van DIGG is het coördineren en ondersteunen van de digitalisering van het openbaar bestuur om het openbaar bestuur efficiënter en effectiever te maken.

IDENTIFICATIE EN BEHEER VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

De Zweedse benadering voor de identificatie van vitale diensten is van toepassing op zowel particuliere als openbare sectoren en organisaties. De Zweedse wetgeving maakt hierbij dus geen onderscheid. Zoals opgemerkt in de vorige paragraaf, omvat dit verschillende geïdentificeerde vitale sectoren gebieden voor alle of de meeste uitvoerenden organisaties in de publieke sector zijn, zoals gezondheidszorg, lokale overheidsinfrastructuur, openbaar bestuur en sociale verzekeringen. De basis van de Zweedse benadering voor de identificatie van vitale diensten is een ‘alle gevarenbenadering’ die ernaar streeft alle mogelijke risico's voor de Zweedse belangen te omvatten.

De MSB heeft richtlijnen gepubliceerd voor het uitvoeren van identificatie en in kaart brengen van vitale diensten op organisatorisch, geografisch of op het gebied van verantwoordelijkheidsniveau. Deze worden geadresseerd aan alle personen die betrokken zijn bij vitale diensten - inclusief lokale gemeenten, provincies, nationale overheidsdiensten en particuliere actoren.[124]

Het basisprincipe voor de identificatie van vitale diensten is om nauw samen te werken met degenen die over belangrijke kennis van het bedrijf beschikken, waaronder beleidsmakers en operationeel personeel. Dit is nodig om essentiële bedrijfsprocessen te identificeren en wat een significante verstoring daarvan zou kunnen vormen. Het MSB-document bevat specifieke richtlijnen, afhankelijk van of de identificatie plaatsvindt op organisatorisch, geografisch of verantwoordelijkheidsgebied. Over het algemeen kent het proces drie overkoepelende stappen:

[124] MSB: Vägledning för identifiering av samhällsviktig verksamhet. As of 7 November 2019: https://www.msb.se/contentassets/d8fca23b124c4686a629970fd2c1aa31/vagledning-for-identifiering-av-samhallsviktig-verksamhet-msb1408---juni-2019.pdf

1. **Mapping** - identificeren en in kaart brengen van alle potentieel vitale services door een lijst te maken van alle bedrijfsprocessen en services. Het is belangrijk om in deze stap niet te beginnen met de analyse van hun relatieve belang om zo te voorkomen dat het identificatieproces wordt vertraagd.

2. **Analyse van geïdentificeerde diensten** - een stapsgewijze analyse van elke geïdentificeerde dienst om op een wetenschappelijke wijze te beoordelen of de dienst een vitale dienst is of niet. De volgende criteria kunnen daarbij onderdeel zijn van de analyse:
    a. Welke negatieve gevolgen kunnen optreden in geval van verstoring van de dienstverlening in de context van democratie, maatschappelijke functies, individueel welzijn en vrijheden, het milieu en de nationale soevereiniteit?
    b. Heeft de dienstverlening onderscheidende kenmerken die de dienst bijzonder belangrijk maakt?
    c. Welke gevolgen zou een mogelijke verstoring van de dienstverlening hebben voor andere bedrijven?
    d. Welke invloed zou een mogelijke verstoring van de dienstverlening op het publiek hebben?
    e. Is de dienst van belang bij bepaalde maatschappelijke verstoringen?
    f. Zijn er bepaalde tijdstippen of perioden waarin de dienst bijzonder vitaal is voor de samenleving?

3. **Beoordeling** - op basis van de resultaten uit stap 2 wordt bepaald of de dienst als vitaal wordt beschouwd. Daarna volgt nog een controle om te bepalen of aan een van de volgende twee voorwaarden wordt voldaan:
    a. Het falen van, of een ernstige verstoring van activiteiten die alleen of samen met overeenkomstige gebeurtenissen in andere diensten in een korte periode kunnen leiden tot een ernstige crisis in de samenleving.
    b. De dienst is noodzakelijk of zeer essentieel om een crisis die zich al in de samenleving heeft voorgedaan, te beheersen, zodat de negatieve effecten zo klein mogelijk zijn.

De resultaten van de analyse moeten worden samengevat in een rapport dat alle vitale services binnen de organisatie opsomt en onderbouwingen bevat waarom de dienst als vitaal moeten worden beschouwd. MSB benadrukt dat de identificatie van vitale diensten de basis vormt voor systematische inspanningen voor de bescherming van vitale diensten, waaronder cyberbeveiliging. MSB geeft verder aan dat de identificatie van vitale diensten ook bredere inspanningen ondersteunt ter bescherming van Zweden met betrekking tot civiele verdediging, de organisatie van nationale defensie, nationale risicobeoordelingen en andere veiligheidsbeoordelingen.

EISEN EN VERPLICHTINGEN AAN VITALE INFRASTRUCTUUR IN DE DIGITALE OVERHEID

De Zweedse nationale cyberveiligheidsstrategie beschrijft de overkoepelende doelstellingen en doelstellingen van cybersecurity voor Zweden:[125]

1. Zorgen voor een systematische en alomvattende benadering van cyberbeveiliging
2. Verbetering van netwerk-, product- en systeembeveiliging
3. Verbetering van de mogelijkheden om cyberaanvallen en andere incidenten te voorkomen, detecteren en beheren
4. Het vergroten van de mogelijkheid om cybercriminaliteit te voorkomen en te bestrijden
5. Vergroten van kennis en bevorderen van expertise
6. Verbetering van internationale samenwerking

MSB heeft een overkoepelende coördinatierol voor de uitvoering van de strategie en maakt gebruik van een nationale coördinatiegroep om te coördineren tussen de belangrijkste actoren met cybersecurity-verantwoordelijkheden (The Information Security Coordination Group (Samverkansgruppen för informationssäkerhet (SAMFI)).[126]

SAMFI omvat MSB, de strijdkrachten, FRA, FMV, PTS, de politie en de beveiligingsdiensten.[127] Ter ondersteuning van de implementatie van de nationale cyberveiligheidsstrategie heeft SAMFI een gezamenlijk actieplan voor cyberveiligheid ontwikkeld dat uit 77 doelstellingen bestaat, verdeeld over de zes hierboven beschreven strategische prioriteiten. De verantwoordelijkheid voor de implementatie van de 77 doelstellingen is verspreid over de leden van SAMFI. Hoewel geen van de doelstellingen specifiek is gericht op de bescherming van vitale diensten of vitale overheidsdiensten, ondersteunen de verschillende doelstellingen indirect de verbetering van kritieke infrastructuurbescherming.

Vanuit operationeel perspectief biedt MSB actief advies en ondersteuning aan exploitanten van vitale services om hen te helpen hun verantwoordelijkheden op het gebied van cyberbeveiliging te nemen. Aangezien het verantwoordelijkheidsbeginsel bepaalt dat elke organisatie de eindverantwoordelijkheid draagt voor het waarborgen van passende cyberbeveiligings-maatregelen zijn er geen nationale minimumnormen voor cyberveiligheid die van toepassing zijn op alle vitale diensten. In plaats daarvan biedt MSB de volgende ondersteuning aan organisaties, zoals weergegeven in tabel 2.

---

[125] Swedish Ministry of Justice (2016, 15-16) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy

[126] MSB: Samverkan inom informationssäkerhet. As of 7 November 2019: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/samverkan-inom-informationssakerhet/

[127] Försvarets radioanstalt (FRA), Försvarets materielverk (FMV)/Sveriges Certifieringsorgan för IT-säkerhet (CSEC), Post- och telestyrelsen (PTS), Säkerhetspolisen (Säpo), Försvarsmakten (FM)/Militära underrättelse- och säkerhetstjänsten (MUST).

Tabel 2 Ondersteuningsmechanismen en initiatieven voor cyberbeveiliging gecoördineerd door MSB

Initiative	Description
Methodologische ondersteuning voor systematische informatiebeveiliging *(Metodstöd för systematiskt informationssäkerhetsarbete)*	Een set van leer hulpmiddelen en voorbeelden voor de implementatie van de Zweedse versie van ISO/IEC 27001:2014 en ISO/IEC 27002:2014.
Informatie beveiligingsopleidingen voor gebruikers (*Datorstödd informationssäkerhetsutbildning för användare (DISA*)	Een set van bewustzijn verhogende en educatieve hulpmiddelen gericht op gebruiker.
Computer Emergency Response Team (CERT-SE)	MSB omvat ook CERT-SE. Dit is het Nationale CERT van Zweden, Het instituut ondersteunt de volgends Zweedse instituties, maar is daar niet toe beperkt: overheidsinstanties, regionale autoriteiten, gemeenten, ondernemingen en bedrijven. Bovendien is CERT-SE ook de CERT-autoriteit van Zweden en heeft het extra verantwoordelijkheden binnen de overheid.
Cyber Range en Training Omgeving (CRATE)	MSB werkt samen met het Zweedse Defensieonderzoeksbureau (FOI), dat de Cyber Range en Trainingsomgeving levert, waarmee het mogelijk is om computernetwerken te maken voor experimenten, wedstrijden en oefeningen in cyberveiligheid.

Ondanks de afwezigheid van algemene nationale minimumvereisten, zijn er enkele diensten die organisaties verplichten om aan minimale cybersecurityvereisten te voldoen. Om bijvoorbeeld toegang te krijgen tot het Secure Intranet van de Zweedse overheid. Daarvoor moeten deze organisaties cybersecurity-regelingen presenteren in overeenstemming met ISO / IEC 27001: 2014.[128]

Ook de nationale overheidsdiensten hebben de wettelijke verplichting voor minimale cybersecurity-regelingen in overeenstemming met ISO / IEC 27001: 2014 en ISO / IEC 27002: 2014 en moeten verplicht incidenten rapporteren.[129] Tot slot heeft Zweden voor vitale diensten die onder de NIB-richtlijn vallen een nieuwe wet geïmplementeerd (Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018: 1174)), waarmee de eisen uit de NIB-richtlijn nationaal zijn geïmplementeerd.

[128] MSB: SGSI. As of 7 November 2019: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/sakra-kommunikationer/sgsi/

[129] Informationsäkerhet.se: Rättsliga krav på informationssäkerhet i olika verksamheter. As of 7 November 2019: https://www.informationssakerhet.se/lagar--regelverk/rattsliga-krav-pa-informationssakerhet-i-olika-verksamheter/

TOEZICHT EN NALEVING OP DE VEREISTEN IN DE DIGITALE OVERHEID

In Zweden zijn geen op zichzelf staande mechanismen voor voortdurende monitoring van de naleving van cyberveiligheidseisen, specifiek gericht op uitvoerders van vitale diensten. Wel kunnen de cyberbeveiligingsregelingen van nationale overheidsdiensten worden opgenomen in audits door de Zweedse nationale auditorganisatie (Riksrevisionen). Daarnaast zien we dat bijzondere nalevingsvereisten worden gesteld aan organisaties in de private en publieke sector die zich bezighouden met 'beveiligingsgevoelige activiteiten' (d.w.z. activiteiten die van belang zijn voor de veiligheid van Zweden of die vallen onder een internationale verplichting tot bescherming van de veiligheid die bindend is voor Zweden). Deze worden geleid door de Protective Security Act en Protective Security Ordinance, die beiden op 1 april 2019 in werking zijn getreden. Deze wetten omvatten beveiligingsregels die verwijzen naar preventieve maatregelen die zijn genomen om de beveiligingsgevoelige activiteiten van overheidsinstanties en bedrijven te beschermen tegen spionage, sabotage, terroristische misdrijven en andere misdrijven. De handhaving van deze voorschriften wordt uitgevoerd door de Zweedse nationale beveiligingsdienst, die vrij is om te beslissen waar beschermende beveiligingsinspecties worden uitgevoerd om de bescherming van de meest kritieke infrastructuur van het land te waarborgen.

A Opdrachtomschrijving BZK

Opdracht

Uitvoeren van onderzoek naar de wijze hoe overheden van andere (EU) landen hun vitale digitale processen vaststellen in het licht van de NIB richtlijn, welke (typen) maatregelen zij hiervoor voorschrijven, op welke wijze zij dit doen en welk toezicht zij daarop uitoefenen.

Achtergrond

De Wet beveiliging netwerk- en informatiesystemen (WBNI) ziet toe op verplichtingen voor vitale digitale infrastructuur van Nederland, dus ook de delen van de digitale overheid die vitaal zijn. Dat zijn onderdelen die niet tot heel kort niet beschikbaar mogen zijn. Een te lange uitval/stilstand leidt tot of een economisch dan wel maatschappelijk probleem/onrust. Uit deze wet volgt geen extra zorgplicht richting de vitale voorzieningen van de digitale overheid (wel voor andere sectoren). Echter, vanuit het gegeven dat de digitale overheid nu voor het eerst onderdeel is van de vitale infrastructuur in Nederland wordt er vanuit beleidsmatig oogpunt nader verkend of en aan welke aanvullende beveiligingsvereisten moet worden voldaan in het kader van deze nieuwe vitaal- aanmerking. De WBNI vloeit voort uit de Europese NIB richtlijn, er moet worden onderzocht welke (bindende) maatregelen andere (EU) landen voor hun eigen vitale overheden hebben vastgesteld.

Het onderzoek sluit aan bij de Brede Agenda Digitale Overheid op het onderdeel: “Onze dienstverlening maken we persoonlijker”, actielijn “Verhogen informatieveiligheid”.
Daarnaast sluit het onderzoek aan op de Kamerbrief “Verhogen informatieveiligheid bij de overheid” (Kamerstukken II 2018/19, 26643, 574), aldaar: “Verankering in wet- en regelgeving”.
De aard en het doel van de Opdracht Doel van de opdracht: verkrijgen van inzicht in de omgang t.a.v. regelgeving, normstelling en toezicht van andere EU landen met hun eigen vitale (of vergelijkbare) digitale overheid.

Het beoogde resultaat Eindproduct

Aan het einde van de onderzoeksperiode wordt een onderzoeksrapport in PDF (ter publicatie) en WORD (voor intern gebruik) opgeleverd aan BZK/DIO met de uitkomsten van de onderzoeksactiviteiten. Het rapport dient te voldoen aan de toegankelijkheidseisen van DigiToegankelijk.nl.

B Bijlage: Achtergrond onderzochte landen

Australië

POLITIEKE STRUCTUUR

Het regeringssysteem van Australië is gebaseerd op de liberale democratische traditie, die religieuze tolerantie en vrijheid van meningsuiting en vereniging omvat. De overheid en haar praktijk weerspiegelen Britse en Noord-Amerikaanse modellen, maar zijn uniek Australisch.

Australië werd opgericht op 1 januari 1901 - Federation Day - toen zes voormalige Britse koloniën - nu de zes Staten van Australië - overeenkwamen een unie te vormen. De Australische grondwet, die op 1 januari 1901 van kracht werd, legt het kader vast voor het Australische regeringssysteem.

Er zijn ongeveer 900 lokale overheidsinstanties in Australië. De bevoegdheden van de lokale overheid variëren per staat en vallen onder de verantwoordelijkheid van de centrale overheid. Sommige lokale overheidsinstanties exploiteren transport- en energiebedrijven. De financiering van de lokale overheidsinstanties komt voornamelijk vanuit de centrale overheid. De verantwoordelijkheden van de lokale overheid omvatten doorgaans stadsplanning, toezicht op bouwvoorschriften, lokale wegen, water, riolering en afwatering, afval en sanitaire voorzieningen en recreatieve voorzieningen voor gemeenschappen.

DIGITALE STRATEGIE

Australië heeft haar strategie voor digitale transformatie gepubliceerd, met als doel burgers toegang te geven tot alle overheidsdiensten tegen 2025. Met als doel om ervoor te zorgen dat de overheid "gemakkelijk in de omgang is"; "Geïnformeerd door" burgers; en "geschikt voor het digitale tijdperk".

Het slagen van de strategie is afhankelijk is van de succesvolle afronding van het project om een digitaal identiteitssysteem voor gebruikers te creëren. Als dat gebeurt, kunnen Australiërs die hun digitale ID gebruiken, ervoor kiezen om gepersonaliseerde services te ontvangen, hen te waarschuwen dat ze in aanmerking komen voor verschillende services en herinneringen te ontvangen wanneer bijvoorbeeld betalingen moeten worden gedaan.[130]

E-GOVERNMENT ONTWIKKELINGEN[131]

Australië was aanvankelijk snel lid van de wereldwijde e-overheidstrend en ontwikkelde zelfs een internationale reputatie als een vroege leider op dit gebied (rond 1999). Een gezamenlijke aanpak van e-government werd echter niet bereikt.

---

[130] https://www.globalgovernmentforum.com/australia-launches-digital-transformation-strategy/

[131] Introducing integrated e-government in Australia, https://www.acs.org.au/content/dam/acs/acs-publications/E-Gov%20Report.pdf

In 2016 heeft de federale overheid een agentschap opgericht om de digitale en ICT-agenda's van de overheid te beheren: het Digital Transformation Agency. Het agentschap wil digitale levering integreren binnen de federale overheid en ook de transparantie van de ICT- en digitale projecten van de overheid verbeteren. Een van de projecten is het Trusted Digital Identity Framework. Dit schetst een consistente benadering van digitale identiteit in Australië en is een belangrijk onderdeel van de geïntegreerde benadering van e-government. In de federale begroting 2018-2019 werd hiervoor ongeveer $ 92,4 miljoen aan financiering veilig gesteld om de infrastructuur te creëren die een eID (Govpass) zal ondersteunen. De Australische regering streeft ernaar om eind juni 2019 pilot diensten uit te rollen naar een half miljoen gebruikers.

Lokale overheden leveren ook diensten online. Een toonaangevende speler is de regering van New South Wales, die een aanmeldingsservice biedt voor veilige toegang tot overheidstransacties; waarbij meer dan 1,5 miljoen klanten zich hebben aangemeld. Victoria is een andere leider. In mei 2016 heeft het de Victorian Government Information Technology Strategie uitgebracht, die de stappen schetst die de overheid neemt om de beveiliging van informatie en infrastructuur te verbeteren die cruciaal zijn voor de goede werking van e-government.

DIGITAL RESILIENCE

Het Australian Cyber Security Centre (ACSC) is een intergouvernementele en inter-agency unit van de Australische overheid die verantwoordelijk is voor cyberveiligheid, waaronder het analyseren, onderzoeken en rapporteren van cyberdreigingen en het coördineren van nationale veiligheidscapaciteiten en -operaties voor incidenten van cybercriminaliteit, cyberterrorisme en cyberwarfare. Het ACSC wordt gehost door het Australische directoraat Signals. Het centrum wordt geleid door de nationale cybercoördinator, onder toezicht van de Cyber Security Operations Board en is de gezamenlijke verantwoordelijkheid van de minister van Defensie en de minister van Binnenlandse Zaken.

Cyber Security Operations Board

Het Cyber Security Operations Board (CSOB) is een secretariaat en instantie op hoofdniveau die verantwoordelijk is voor strategisch toezicht op de operationele cyberbeveiligingsmogelijkheden van de overheid en de coördinatie van cyberbeveiligingsmaatregelen. Het houdt specifiek toezicht op het werk van het Australian Cyber Security Centre.

Nationale cybercoördinator

De nationale cybercoördinator van het ministerie van Binnenlandse Zaken is verantwoordelijk voor het nationale leiderschap op het gebied van cyberveiligheidsbeleid, coördinatie van prioriteiten voor Australische operationele cyberveiligheid agentschappen en de implementatie van de Cyber Security Strategie van de Australische overheid. De nationale cybercoördinator zorgt ook voor effectieve partnerschappen tussen staats- en territoriumregeringen, de particuliere sector, niet-gouvernementele organisaties, de onderzoek gemeenschap en internationale partners.

Cybersecurity binnen de overheid [132]

In oktober 2018 is het Protective Security Policy Framework (PSPF) van kracht geworden. De PSPF helpt entiteiten van de Australische overheid om 'hun mensen, informatie en infrastructuur te beschermen, zowel thuis als in het buitenland'. In het kader van het PSPF willen overheidsentiteiten informatiebeveiliging bereiken door aandacht te besteden aan vier belangrijke gebieden: gevoelige en gerubriceerde informatie; toegang tot informatie; informatie beschermen tegen cyberdreigingen; en robuuste ICT-systemen. Overheidsorganen worden geleid door de Australian Information Information Manual en een online hub voor cyberveiligheidsinformatie, beide onder beheer van het ACSC.

OVERZICHT VAN CYBERSECURITY REGELGEVING / STRATEGIEËN AUSTRALIË [133]

Wetgeving / strategieën	**Status**
Nationale strategie: overkoepelende doctrine die nationale, gecoördineerde afschrikmiddelen en reacties op cyberdreigingen begeleidt.	Australia's National Security Strategy 2013 [134]
Militair: strategieën voor offensieve of defensieve militaire capaciteiten in cyberspace.	Defence White paper in 2016 [135]
Content: wetten die bepaalde digitale inhoud reguleren of beperken.	x
Privacy: strategieën voor het verzamelen en verwerken van persoonlijke gegevens.	Privacy Act 1988[136]
Kritieke infrastructuur: strategieën voor het verminderen van cyberbeveiligingsbedreigingen voor kritieke infrastructuurnetwerken en het vergroten van de veerkracht.	x
Handel: wetten betreffende digitale handel en het aanbieden van internetdiensten.	Electronic Transactions Act 1999 [137]
Cybercriminaliteit: strategieën of wetgeving ter bestrijding van cybercriminaliteit.	Cybercrime Legislation Amendment Act 2012 [138]

[132] https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1819/Quick_Guides/PSDigitalTransformation

[133] CSIS (Center for Strategic & International Studies) Global Cyber Strategies Index, 2019.

[134] https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf

[135] http://www.defence.gov.au/whitepaper/Docs/2016-Defence-White-Paper.pdf

[136] https://www.legislation.gov.au/Details/C2015C00089

[137] https://www.legislation.gov.au/Details/C2011C00445

[138] https://www.legislation.gov.au/Details/C2012A00120

Duitsland

POLITIEKE STRUCTUUR

Duitsland is een federale republiek met 16 staten - of 'Länder' - een daarvan is de hoofdstad Berlijn. Deze deelstaten hebben hun eigen wetgevende en uitvoerende organen. Op federaal niveau wordt de wetgevende macht uitgeoefend door een parlement dat bestaat uit twee kamers met verschillende bevoegdheden. Leden van de Tweede Kamer worden om de vier jaar gekozen door middel van rechtstreeks kiesrecht, op basis van een combinatie van stemmen bij meerderheid en evenredige vertegenwoordiging. Partijen moeten ten minste 5% van de nationale stemmen winnen, of drie kiesdistricten om vertegenwoordiging te verkrijgen. De Eerste Kamer bestaat uit 69 leden, aangewezen door de regeringen van de deelstaten, in verhouding tot hun bevolking.

Het staatshoofd is de federale president, gekozen voor een periode van vijf jaar door de federale conventie. De uitvoerende macht is in handen van de federale regering, voorgedragen door de Tweede Kamer (Bondsdag) en geleid door de kanselier.

DIGITALE STRATEGIE

Het federale ministerie van Onderwijs en Onderzoek heeft een op hightech georiënteerde strategie ontwikkeld die gericht is op het stimuleren van het wetenschappelijk en economisch potentieel van Duitsland en het vinden van oplossingen voor wereldwijde en nationale uitdagingen. Duitsland streeft naar een wereldwijde leidende positie op het gebied van innovatie via een reeks geformuleerde doelen, gedefinieerde prioriteiten en nieuwe instrumenten binnen een breed scala van verschillende innovatiegebieden.

De hiervoor genoemde hightech-strategie is het eerste brede nationale concept en deelt een gezamenlijke visie van de belangrijkste belanghebbenden betrokken bij innovatie. Deze strategie is gebaseerd op vijf pijlers:

1. Prioriteit geven aan toekomstige uitdagingen met betrekking tot welvaart en levenskwaliteit;
2. Consolidering van middelen en bevordering van overdracht;
3. Versterking van de dynamiek van innovatie in de industrie;
4. Het scheppen van gunstige voorwaarden voor innovatie; en
5. Versterking van dialoog en participatie

E-GOVERNMENT ONTWIKKELINGEN

Op 18 augustus 2017 is de wet tot verbetering van de online toegang tot administratieve diensten (Onlinezugangsgesetz, OZG) in werking getreden. Federale, Länder en lokale overheden waren nu gelijkgesteld om uitgebreide maatregelen te nemen om de beschikbare elektronische overheidsdiensten te promoten. Uitgangspunten van de regelgeving: 1. Alle (geschikte) administratieve diensten moeten online beschikbaar zijn binnen vijf jaar na de inwerkingtreding van de wet; 2.Federale deelstaten en gemeentelijke e-overheidsdiensten moeten beschikbaar zijn via een nieuw opgezet federaal online portaal en de online portals van de deelstaten en; 3.

Toegang tot alle administratieve services in het portaalnetwerk moet worden toegestaan via een beveiligde account voor één gebruiker.

DIGITAL RESILIENCE

Duitsland heeft in 2009 een overeenkomst gesloten over samenwerking op het gebied van IT-beveiligingsonderzoek tussen het Federale Ministerie van Onderwijs en Onderzoek (BMBF) en het Federale Ministerie van Binnenlandse Zaken (BMI). Het IT Security Research-programma omvat onderzoek en ontwikkeling in nieuwe informatiebeveiligingstechnologieën.[139] Het BMBF ondersteunt sinds 2011 drie onderzoekscentra die toonaangevende universitaire en niet-universitaire instellingen op het gebied van cybersecurity samenbrengen.

Federaal Agentschap voor Informatiebeveiliging (BSI)

Het federale kantoor voor informatiebeveiliging is de centrale IT-beveiligingsdienstverlener voor de Duitse overheid. Een van de belangrijkste taken is het bieden van ondersteuning aan federale autoriteiten op het gebied van IT-beveiliging. BSI onderzoekt beveiligingsrisico's verbonden aan het gebruik van IT en ontwikkelt preventieve beveiligingsmaatregelen. Het biedt informatie over risico's en bedreigingen met betrekking tot het gebruik van informatietechnologie en zoekt naar passende oplossingen. Dit werk omvat IT-beveiligingstests en beoordeling van IT-systemen, inclusief de ontwikkeling ervan. Dit doet BSI in samenwerking met de industrie.

OVERZICHT VAN CYBERSECURITY REGELGEVING / STRATEGIEËN DUITSLAND [140]

Wetgeving / strategieën	**Status**
Nationale strategie: overkoepelende doctrine die nationale, gecoördineerde afschrikmiddelen en reacties op cyberdreigingen begeleidt.	German National Cyber Security Strategy 2016 [141]
Militair: strategieën voor offensieve of defensieve militaire capaciteiten in cyberspace.	White Paper on German Security Policy and the Future of the Bundeswehr 2016 [142]
Content: wetten die bepaalde digitale inhoud reguleren of beperken.	Netzdurchsetzunggesetz, NetzDG 2017 [143]
Privacy: strategieën voor het verzamelen en verwerken van persoonlijke gegevens.	GDPR 2018

[139] ITU, Global Cybersecurity Index (GCI) 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

[140] CSIS (Center for Strategic & International Studies) Global Cyber Strategies Index, 2019.

[141] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/view

[142] http://www.gmfus.org/file/8970/download

[143] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2

Kritieke infrastructuur: strategieën voor het verminderen van cyberbeveiligings-bedreigingen voor kritieke infrastructuur-netwerken en het vergroten van de veerkracht.	BSI Act – BSIG2009 [144]
Handel: wetten betreffende digitale handel en het aanbieden van internetdiensten.	Signaturgesetz, SiG 2001[145]
Cybercriminaliteit: strategieën of wetgeving ter bestrijding van cybercriminaliteit.	German Criminal Code 2008 [146]

[144] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=4

[145] https://germanlawarchive.iuscomp.org/?p=690

[146] http://www.gesetze-im-internet.de/englisch_stgb/index.html

Estland

POLITIEKE STRUCTUUR

Estland is een parlementaire republiek. De wetgevende macht ligt in het parlement met één kamer, de State Assembly (Riigikogu). De Algemene Vergadering heeft 101 leden, gekozen door de volksstemmen voor een termijn van vier jaar. Het staatshoofd van Estland is de president, door de Riigikogu gekozen voor een termijn van vijf jaar. De regering, die uitvoerende macht uitoefent, wordt gevormd door de premier, voorgedragen door de president en in totaal 14 ministers. De regering wordt benoemd door de president met goedkeuring van het parlement.

Estland is verdeeld in 15 provincies en 213 stedelijke en landelijke gemeenten (steden en parochies), waarvan de bevoegdheden en verantwoordelijkheden zijn vastgelegd in de wet van de lokale overheidsorganisatie van juni 1993. De regering van elke provincie wordt geleid door een gouverneur van de provincie.

DIGITALE STRATEGIE

De drie Baltische staten hebben een digitaal trilateraal memorandum of understanding voor cyberveiligheid ondertekend en is de eerste digitaal ondertekende bilaterale internationale overeenkomst. Daarna volgende voor Estland de lancering van X-Road. X-Road biedt een betere ondersteuning voor gestandaardiseerde vertrouwensdiensten, waardoor het geschikter is voor grensoverschrijdende diensten en internationaal gebruik en past binnen de EU-regelgeving.

De regering van Estland heeft een conceptvoorstel omtrent Cloud-gebruik binnen de overheid en data ambassades geratificeerd. De overheidscloud zorgt voor digitale continuïteit van Estland, verhoogt de kwaliteit van e-services en moet verschillende IT-beveiligingsrisico's voorkomen. Bovendien ondersteunt de implementatie van Cloud technologie in de publieke sector de innovatie en ontwikkeling van de Estse informatiemaatschappij. Estland definieert deze data ambassades als datacenters in een geallieerd buitenland dat gegevens van kritieke overheidsinformatiesystemen en kritieke servicetoepassingen redundant opslaat. Deze data ambassades helpen de digitale en gegevenscontinuïteit van Estland te waarborgen.

E-GOVERNMENT ONTWIKKELINGEN

Er is momenteel geen algemene e-overheidswetgeving in Estland.

DIGITAL RESILIENCE

In 2018 is de Cybersecurity Act in werking getreden, die tot doel had de beveiliging van digitale systemen te versterken die worden gebruikt bij het leveren van vitale en andere maatschappelijk belangrijke diensten aan het publiek.

Estland heeft haar derde Cybersecurity-strategie 2019-2022 gelanceerd. Doelstellingen in deze nieuwe strategie zijn: 1. Estland is een duurzame digitale samenleving die steunt op sterke technologische veerkracht en (nood)paraatheid; 2. De Estse cybersecurity-industrie is sterk, innovatief, onderzoek gericht en wereldwijd concurrerend; 3. Estland is een geloofwaardige en

capabele partner op internationaal gebied en; 4. Estland is een 'cybergeletterde' samenleving en zorgt voor voldoende en toekomstgericht talentaanbod.

CERT Estland

Het Computer Emergency Response Team van Estland (CERT Estonia), opgericht in 2006, is een organisatie die verantwoordelijk is voor het beheer van beveiligingsincidenten in '.ee'-computernetwerken. Het is zijn taak om Estse internetgebruikers te helpen bij de uitvoering van preventieve maatregelen om mogelijke schade door beveiligingsincidenten te verminderen en hen te helpen bij het reageren op mogelijke beveiligingsbedreigingen. CERT Estland behandelt beveiligingsincidenten die zich voordoen in Estse netwerken of incidenten waarvan burgers, of instellingen in Estland of in het buitenland op de hoogte zijn gesteld.

OVERZICHT VAN CYBERSECURITY REGELGEVING / STRATEGIEËN ESTLAND [147]

Wetgeving / strategieën	**Status**
Nationale strategie: overkoepelende doctrine die nationale, gecoördineerde afschrikmiddelen en reacties op cyberdreigingen begeleidt.	Cyber Security Strategy 2019-2022 [148]
Militair: strategieën voor offensieve of defensieve militaire capaciteiten in cyberspace.	National Defence Strategy Estonia in 2010 [149]
Content: wetten die bepaalde digitale inhoud reguleren of beperken.	x
Privacy: strategieën voor het verzamelen en verwerken van persoonlijke gegevens.	GDPR 2018
Kritieke infrastructuur: strategieën voor het verminderen van cyberbeveiligingsbedreigingen voor kritieke infrastructuurnetwerken en het vergroten van de veerkracht.	Cybersecurity Act 2018 [150]
Handel: wetten betreffende digitale handel en het aanbieden van internetdiensten.	Digital Signatures Act 2013 [151]
Cybercriminaliteit: strategieën of wetgeving ter bestrijding van cybercriminaliteit.	x

[147] CSIS (Center for Strategic & International Studies) Global Cyber Strategies Index, 2019.

[148] https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

[149] http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf

[150] https://www.riigiteataja.ee/en/eli/523052018003/consolide

[151] https://www.riigiteataja.ee/en/eli/530102013080/consolide

Spanje

POLITIEKE STRUCTUUR

Spanje is een constitutionele monarchie. De wetgevende macht is in handen van een tweekamerstelsel (Cortes Generales), bestaande uit een Tweede Kamer (Congres van Afgevaardigden) en een Eerste Kamer (Senaat). Volgens de bepalingen van de grondwet van 1978 heeft Spanje een gedecentraliseerd systeem aangenomen met 17 autonome regio's (autonome gemeenschappen) die zelfbestuursrecht genieten met betrekking tot lokale aangelegenheden, naast twee 'autonome steden'. Deze gemeenschappen kiezen hun eigen parlementen, die op hun beurt lokale overheden voordragen.

DIGITAL STRATEGIE

In de Raad van Ministers van 2 oktober heeft de regering het "Digital Transformation Plan for the General Administration (GA) en de daarbij behorende openbare instellingen (PA's) (ICT-strategie) aangenomen".

E-GOVERNMENT ONTWIKKELINGEN

De centrale overheid ontwikkelt het vierde nationale actieplan (2019-2021), waarbij rekening wordt gehouden met bijdragen van overheidsdiensten, burgers en andere vertegenwoordigers van het maatschappelijk middenveld. De algemene doelstellingen van het nationale actieplan zijn:

1. Bevordering en vergemakkelijking van de betrokkenheid van burgers bij het besluitvormingsproces van overheidsdiensten.
2. Verbetering van de transparantie, kwaliteit en beschikbaarheid van open gegevens als mechanismen voor verantwoordingsplicht bij activiteiten van het openbaar bestuur.
3. Ontwikkeling van een systeem voor openbare integriteit dat ethische waarden bevordert, goede praktijken van openbaar bestuur versterkt en het vertrouwen van burgers in overheidsdiensten vergroot.
4. Maak burgers en ambtenaren bewust van de waarden van open overheid, in overeenstemming met de doelstellingen van de Agenda 2030 voor duurzame ontwikkeling.

DIGITAL RESILIENCE

De nationale veiligheidsstrategie 2017, aangenomen door de regering in de ministerraad op 1 december 2017. De strategie houdt rekening met veranderingen in het technologische landschap en omvatte de oprichting van een Nationaal Cybersecurity Forum om de samenwerking van publieke en private te bevorderen. De vijf doelstellingen van de strategie zijn:

1. Beveiliging en veerkracht van netwerken en informatie- en communicatiesystemen van de publieke sector en essentiële diensten;
2. Veilig en betrouwbaar gebruik van cyberspace;
3. Bescherming van het sociale en economische ecosysteem en de burgers;
4. Beveiligingscultuur en -bewustzijn en ontwikkeling van menselijke en technische beveiligingsmogelijkheden;
5. Cyberspace-beveiliging op internationaal niveau.

CCN-CERT

Spanje heeft eind 2016 een CERT opgericht voor de Spaanse Overheid. De CCN-CERT valt onder het Security Incident Response Information National Cryptologic Center.

OVERZICHT VAN CYBERSECURITY REGELGEVING / STRATEGIEËN SPANJE [152]

Wetgeving / strategieën	Status
Nationale strategie: overkoepelende doctrine die nationale, gecoördineerde afschrikmiddelen en reacties op cyberdreigingen begeleidt.	National Cyber Security Strategy 2019 [153]
Militair: strategieën voor offensieve of defensieve militaire capaciteiten in cyberspace.	The National Security Strategy 2017 [154]
Content: wetten die bepaalde digitale inhoud reguleren of beperken.	x
Privacy: strategieën voor het verzamelen en verwerken van persoonlijke gegevens.	GDPR 2018
Kritieke infrastructuur: strategieën voor het verminderen van cyberbeveiligingsbedreigingen voor kritieke infrastructuurnetwerken en het vergroten van de veerkracht.	Ley 9/2014, de 9 de mayo, General de Telecomunicaciones [155]
Handel: wetten betreffende digitale handel en het aanbieden van internetdiensten.	x
Cybercriminaliteit: strategieën of wetgeving ter bestrijding van cybercriminaliteit.	x

[152] CSIS (Center for Strategic & International Studies) Global Cyber Strategies Index, 2019.

[153] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy

[154] https://www.lamoncloa.gob.es/documents/estrategiaseguridad_baja_julio.pdf

[155] https://www.boe.es/buscar/pdf/2014/BOE-A-2014-4950-consolidado.pdf

Verenigd Koninkrijk

POLITIEKE STRUCTUUR

Het Verenigd Koninkrijk is de oudste constitutionele monarchie in Europa. De wetgevende macht is in handen van het parlement, gedeeld tussen het Lagerhuis en het Hogerhuis.
Een grondige hervorming van de grondwet in de afgelopen twaalf jaar bracht een programma naar voren voor een substantiële decentralisatie van de macht door de oprichting van een parlement en de uitvoerende macht in Schotland, een assemblee in Wales, en op langere termijn, de machtsverdeling op regionaal niveau in Engeland.

DIGITALE STRATEGIE

In de digitale strategie van de Engelse overheid wordt uiteengezet hoe de overheid haar digitale diensten opnieuw zal ontwerpen om ze zo eenvoudig en gemakkelijk te maken dat iedereen die ze kan gebruiken. Deze strategie geeft aan dat de overheidsstandaard digitaal zal gaan worden.

E-GOVERNMENT ONTWIKKELINGEN

De Digital Economy Act 2017, aangekondigd in de Queen's Speech in mei 2016. Deze kondigt een aantal verbintenissen vanuit de regering aan ten aanzien van de digitale economie. Ondanks het feit dat het Verenigd Koninkrijk opvalt als een goed aan het netwerk verbonden land (meer dan negen van de tien huizen en bedrijven hebben toegang tot supersnelle breedband), moet de wet de basis leggen voor het voortouw in de digitale economie. De wet heeft vijf hoofddoelstellingen:

1. Snelle breedband en ondersteuning voor consumenten;
2. Digitale infrastructuur mogelijk maken;
3. Bescherming van intellectueel eigendom;
4. Digitale overheidsdiensten;
5. Bescherming van burgers in de digitale wereld.

DIGITAL RESILIENCE

Op 7 april 2014 heeft de Britse regering de details aangekondigd van een nieuw overheidsschema om bedrijven te helpen online veilig te blijven. Het schema is gebaseerd op de technische richtlijnen van Cyber Essentials om te bepalen welke beveiligingsmaatregelen organisaties binnen hun IT-systeem moeten hebben om erop te kunnen vertrouwen dat ze het risico van internet gebaseerde bedreigingen beginnen te verkleinen. Het Verenigd Koninkrijk heeft uiteindelijk in 2016 haar tweede vijfjarige nationale cyberveiligheidsstrategie uitgegeven.[156] Met deze strategie wil het Verenigd Koninkrijk het land maken tot een van de veiligste plaatsen ter wereld om online zaken te doen en de investeringen in cyberveiligheid te verdubbelen in vergelijking met het eerste plan.[157] Het Verenigd Koninkrijk doet dan ook een totale investering van £ 1,9 miljard om de cyberbeveiliging aanzienlijk te transformeren.

---

[156] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[157] ITU, Global Cybersecurity Index (GCI) 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

OVERZICHT VAN CYBERSECURITY REGELGEVING / STRATEGIEËN VERENIGD KONINKRIJK [158]

Wetgeving / strategieën	Status
Nationale strategie: overkoepelende doctrine die nationale, gecoördineerde afschrikmiddelen en reacties op cyberdreigingen begeleidt.	National Cybersecurity Strategy 2016-2021[159]
Militair: strategieën voor offensieve of defensieve militaire capaciteiten in cyberspace.	The National Security Strategy 2010 [160]
Content: wetten die bepaalde digitale inhoud reguleren of beperken.	x
Privacy: strategieën voor het verzamelen en verwerken van persoonlijke gegevens.	GDPR 2018
Kritieke infrastructuur: strategieën voor het verminderen van cyberbeveiligingsbedreigingen voor kritieke infrastructuurnetwerken en het vergroten van de veerkracht.	Communications Act 2003 [161]
Handel: wetten betreffende digitale handel en het aanbieden van internetdiensten.	Digital Economy Act 2017 [162]
Cybercriminaliteit: strategieën of wetgeving ter bestrijding van cybercriminaliteit.	x

[158] CSIS (Center for Strategic & International Studies) Global Cyber Strategies Index, 2019.

[159] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[160] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[161] http://www.legislation.gov.uk/ukpga/2003/21/contents

[162] http://www.legislation.gov.uk/ukpga/2017/30/contents/enacted/data.htm

Zweden

POLITIEKE STRUCTUUR

Zweden is een constitutionele monarchie met een representatieve democratie gebaseerd op een parlementair regeringssysteem. De Monarch heeft geen politieke macht. De wetgevende macht is in handen van een één kamerkamerparlement (Riksdagen). In totaal zijn er drie niveaus van openbaar bestuur in Zweden: +/- 400 centrale overheidsinstanties, 21 regionale overheidsinstanties (provinciale raden) en 290 lokale overheidsinstanties (gemeenten).

Regionale en lokale autoriteiten zijn onafhankelijk van de regering. Verder zijn er 21 provinciale bestuursraden in Zweden, één in elke provincie. Het werk van een provinciale raad van bestuur is gebaseerd op zijn rol als vertegenwoordiger van de centrale overheid in de regio en coördinator voor aangelegenheden die door de centrale overheid zijn doorgegeven.

DIGITALE STRATEGIE

De digitale agenda voor Zweden stelt een doel voor het ICT-beleid, dat Zweden de beste ter wereld moet worden om de mogelijkheden van digitalisering te benutten.

E-GOVERNMENT ONTWIKKELINGEN

E-Governement activiteiten worden gereguleerd door de algemene wetten en verordeningen inzake het openbaar bestuur in Zweden.

DIGITAL RESILIENCE

Zweden heeft de beschikking over een IT Incident Center (SITIC). De rol van het Incident Center is het ondersteunen van publieke inspanningen om bescherming te bieden tegen IT-incidenten. Zweden maakt daarnaast deel uit van de Nordic National CERT Collaboration, waaronder Denemarken, Finland, IJsland, Noorwegen. Het doel van deze CERT is technische samenwerking en cyberveiligheidsoefeningen om de cyberparaatheid te beoordelen en te versterken, incidentenresponsprocessen te onderzoeken en het delen van informatie in de Noordse regio om continu te blijven verbeteren.[163]

OVERZICHT VAN CYBERSECURITY REGELGEVING / STRATEGIEËN ZWEDEN [164]

Wetgeving / strategieën	**Status**
Nationale strategie: overkoepelende doctrine die nationale, gecoördineerde afschrikmiddelen en reacties op cyberdreigingen begeleidt.	National Cyber Security Strategy 2017 [165]

[163] ITU, Global Cybersecurity Index (GCI) 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

[164] CSIS (Center for Strategic & International Studies) Global Cyber Strategies Index, 2019.

[165] https://www.government.se/4970ac/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213

Militair: strategieën voor offensieve of defensieve militaire capaciteiten in cyberspace.	The National Security Strategy 2017 [166]
Content: wetten die bepaalde digitale inhoud reguleren of beperken.	x
Privacy: strategieën voor het verzamelen en verwerken van persoonlijke gegevens.	GDPR 2018
Kritieke infrastructuur: strategieën voor het verminderen van cyberbeveiligingsbedreigingen voor kritieke infrastructuurnetwerken en het vergroten van de veerkracht.	Lag (2003:389) om Elektronisk Kommunikation 2004 [167]
Handel: wetten betreffende digitale handel en het aanbieden van internetdiensten.	x
Cybercriminaliteit: strategieën of wetgeving ter bestrijding van cybercriminaliteit.	x

[166] https://www.government.se/4aa5de/contentassets/0e04164d7eed462aa511ab03c890372e/national-security-strategy.pdf

[167] https://wipolex.wipo.int/en/text/242555