Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021

Inhoudsopgave

	Voorwoord	**4**
	Samenvatting	**5**
1	**Inleiding**	**12**
1.1	Aanleiding	12
1.2	De betrokken toezichthouders	12
1.3	Afbakening	13
1.3.1	Het begrip ‘cybersecurity’	13
1.3.2	Het begrip ‘vitaal’	14
1.3.3	Overzicht vitale processen en toezichthouders	14
1.4	Eerste interne beeld van toezicht op digitale vitale weerbaarheid	16
1.5	Leeswijzer	17
2	**Doelstelling en gemeenschappelijk kader**	**18**
2.1	Doelstelling	18
2.2	Gemeenschappelijk kader	18
2.2.1	Grondslag en verantwoordelijkheden	19
2.2.2	Proces van toezicht	19
2.2.3	Thema’s 2020	20
3	**Het toezicht op cybersecurity bij vitale processen**	**22**
3.1	Achtergrond: doelstelling, wijze van toezicht en oordeelsvorming.	22
3.2	Context: normenkader, volwassenheidsniveaus en toetsingskader	23
3.3	Context: plannings- en beleidscyclus	23
3.4	Context: wet- en regelgeving	24
3.5	Context: governance	24
3.6	Meerjarenperspectief	24
4	**Resultaten toezicht op cybersecurity vitale processen**	**26**
4.1	Inleiding	26
4.2	Toezichtresultaten	26
5	**Stand van zaken aanbevelingen Eerste Beeld**	**34**
5.1	Aanbevelingen Eerste Beeld	34
5.2	Stand van zaken aanbevelingen	34
5.3	Conclusie	38

6	**Conclusies en aandachtspunten**	**39**
6.1	Conclusies	39
6.2	Aandachtspunten	42
7	**Doorontwikkeling samenhangend inspectiebeeld**	**45**
	Bijlagen	
I	**Het hoe en wat van het toezicht op cybersecurity bij vitale processen**	**47**
II	**Gebruikte afkortingen**	**59**

Voorwoord

Bepaalde processen, zoals de energie- en drinkwatervoorziening, verwerking van nucleair materiaal, transport en financieel verkeer, zijn zo belangrijk voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Al deze processen vormen de Nederlandse vitale infrastructuur. Door de toenemende digitalisering van de samenleving zijn vitale processen daar steeds meer afhankelijk van. Het is daarom van groot belang dat deze vitale processen weerbaar zijn tegen cyberdreigingen. Toezicht levert een belangrijke bijdrage aan die weerbaarheid. Vandaar dat een aantal toezichthouders vanuit hun wettelijke kaders de handen ineen hebben geslagen om de stand van de cybersecurity bij vitale processen in samenhang – over de verschillende sectoren heen – in beeld te brengen. Voor u ligt het eerste samenhangend inspectiebeeld, samengesteld door de verschillende toezichthouders onder coördinatie van de Inspectie Justitie en Veiligheid.

Het beeld laat zien dat er op het gebied van digitaal weerbare, en dus veilige, vitale processen en aanbieders op een aantal terreinen inmiddels de nodige stappen zijn gezet. Ook laat het inspectiebeeld zien dat er in de breedte nog veel werk aan de winkel is en dat het werk nooit af is. Als het gaat om cybersecurity is er voortdurende alertheid, adequaat handelen en scherpte nodig. De toezichthouders hebben de ambitie om het toezicht daarop in gezamenlijkheid door te ontwikkelen en jaarlijks een staat van de cybersecurity van vitale processen en vitale aanbieders op te leveren. Enkele van de bij dit inspectiebeeld betrokken toezichthouders vervullen daarbij, gezien de wijze waarop zij het toezicht op cyber al hebben ingericht, een voortrekkersrol. Die goede voorbeelden nodigen andere toezichthouders uit om die te volgen.

Digitalisering is in onze samenleving niet meer weg te denken; het biedt veel kansen maar ook risico’s. Toezichthouders kijken mee in de praktijk en bieden de spiegel aan organisaties, beleidsmakers en uitvoerders. Toezicht helpt beleid en uitvoering om de weerbaarheid tegen kwetsbaarheden te verhogen en zo die kansen in de samenleving veilig te benutten.

H.C.D. Korvinus
Inspecteur-generaal Inspectie Justitie en Veiligheid

Samenvatting

Inleiding

Naar aanleiding van het Cybersecuritybeeld Nederland 2019 (CSBN 2019) heeft het kabinet, met het oog op de toenemende digitale dreiging en de achterblijvende digitale weerbaarheid van Nederland, aangekondigd om onder regie van de minister van Justitie en Veiligheid extra maatregelen te treffen om de weerbaarheid van vitale processen tegen cyberdreigingen te versterken. Een van die maatregelen richt zich op het versterken van het toezicht. Toezicht vormt volgens het kabinet een krachtige impuls voor vitale aanbieders om blijvend te werken aan een hoog niveau van digitale weerbaarheid en continuïteit. In de kabinetsreactie wordt aangegeven dat de Inspectie Justitie en Veiligheid samen met andere rijksinspecties en toezichthouders zorgdraagt voor een samenhangend inspectiebeeld en onderlinge kennis en expertise tussen inspecties en toezichthouders.

Dit samenhangend inspectiebeeld 2020-2021 is opgesteld door de toezichthouders die sinds de implementatie van de Europese netwerk- en informatieveiligheid-richtlijn (NIB-richtlijn) in de Wet beveiliging netwerk- en informatiesystemen (Wbni) samenwerken. Dit betreffen:

- Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)
- Agentschap Telecom (AT)
- De Nederlandsche Bank (DNB)
- Inspectie Gezondheidszorg en Jeugd (IGJ)
- Inspectie Justitie en Veiligheid (IJenV)
- Inspectie Leefomgeving en Transport (ILT).

De doelstelling van dit samenhangend inspectiebeeld is het enerzijds informeren over de ontwikkeling van en binnen het toezicht op cybersecurity. Anderzijds is het doel om in samenhang zo goed als nu mogelijk is in beeld brengen van de resultaten van toezicht door de betrokken toezichthouders op cybersecurity van vitale processen.

In dit samenhangend inspectiebeeld wordt het begrip ‘vitaal’ in brede zin toegepast: het gaat hierbij om processen die door vakdepartementen als vitale processen zijn aangemerkt. Een overzicht van deze processen is opgenomen in tabel a. Deze wordt indien nodig geactualiseerd en gepubliceerd op de website van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De aanbieders van een groot deel van deze processen zijn tevens op basis van de Wbni als vitaal aangewezen.

In dit samenhangend inspectiebeeld zijn de toezichtresultaten over de niet-vitale processen, gezien de doelstelling van dit document, niet meegenomen.

De bij dit inspectiebeeld betrokken toezichthouders hebben – vooruitlopend op het opstellen van een samenhangend inspectiebeeld over de cybersecurity van de vitale processen – in maart 2020 de stand van zaken in beeld gebracht van het toezicht op cybersecurity bij organisaties c.q. processen die behoren tot de vitale sectoren in Nederland. Doordat dat eerste beeld een interne werking had, is dat niet gepubliceerd. In dat beeld hebben de toezichthouders een aantal aanbevelingen gedaan aan de minister van JenV – als coördinerend cyberminister – en aan zijn collega-vakministers van Economische Zaken en Klimaat (EZK), Financiën (Fin), Infrastructuur en Waterstaat (IenW) en Volksgezondheid, Welzijn en Sport (VWS). De wijze waarop door hen opvolging is gegeven aan deze aanbevelingen, is verwerkt in de onderstaande conclusies.

Gemeenschappelijk kader

De toezichthouders willen in de verdere ontwikkeling van het inspectiebeeld een gemeenschappelijk kader met generieke doelstellingen hanteren. Dat is er nu nog niet. Ze hebben als aanzet daarvoor een eerste kader met thema's geschetst dat het vertrekpunt vormt voor die ambitie. Daarvoor is de zogenaamde 'kapstok' vanuit het Besluit beveiliging netwerk- en informatiesystemen (Bbni) gehanteerd die de volgende vijf beveiligingsdomeinen bevat: risico gebaseerde aanpak, organisatie van netwerk- en informatiebeveiligingsbeheer, incidenten voorkomen, detectie en respons alsmede gevolgen van incidenten beperken. De thema's waarover de verschillende toezichthouders in dit inspectiebeeld rapporteren, zijn in dit kader opgenomen. De ambitie voor de doorontwikkeling van dit kader is hieronder opgenomen.

Achtergrond en context van het toezicht op cybersecurity bij vitale processen door de betrokken toezichthouders

Het algemene toezicht dat de betrokken toezichthouders uitvoeren, verrichten zij op basis van verschillende sectorale en in meerdere gevallen internationale wet- en regelgeving. Bij een aantal van de betrokken toezichthouders is het toezicht op cybersecurity onderdeel van de plannings- en beleidscyclus. De focus op de digitale vitale processen maakt daar in de meeste gevallen impliciet onderdeel van uit.

Een aantal van de betrokken toezichthouders heeft een expliciet doel geformuleerd voor het toezicht op cybersecurity van vitale processen. Andere hebben dat nog niet. Wel heeft het onderwerp bij alle toezichthouders de aandacht en wordt daarop georganiseerd. De toezichthouders die toezicht bij Wbni-vitale organisaties houden doen dit op gelijksoortige wijze. Een gemene deler bij alle toezichthouders is de risicogerichte en informatiegestuurde aanpak. De normenkaders die de toezichthouders bij vitale organisaties hanteren zijn, voor zover beschikbaar, sectorspecifiek. Deze variëren van dynamische kaders op basis van open normen tot specifieke normen vanuit de sector zelf. Drie van de betrokken toezichthouders hanteren zogenaamde volwassenheidsniveaus bij de normenkaders waardoor ontwikkelingen bij vitale aanbieders en sectoren zelf kunnen worden geduid en ook onderling kunnen worden vergeleken.

De meer specifieke beschrijving van het hoe en wat van het toezicht op cybersecurity bij vitale processen is opgenomen in bijlage I.

Resultaten toezicht op cybersecurity vitale processen

De resultaten in dit inspectiebeeld hebben betrekking op meerdere vitale sectoren: nucleair, energie en digitale infrastructuur, elektronische vertrouwensdiensten, telecom, financieel, openbare orde en veiligheid, luchtvaart, drinkwater en maritiem. De rode draden en meest opvallende zaken ervan zijn verwerkt in onderstaande conclusies. Deze hebben enerzijds betrekking op het toezicht zelf. Anderzijds gaan deze over de beelden over de stand van de cybersecurity bij de vitale sectoren die onder toezicht staan.

Conclusies bij beelden toezicht cybersecurity.

1. De toezichthouders maken jaarlijks ieder hun sectorspecifieke afwegingen bij de onderwerpen van het toezicht. Dit gebeurt onder andere op basis van algemene en sectorspecifieke risico's en informatie. De specifieke toezichtresultaten zijn daarom jaarlijks per sector verschillend en geven niet per definitie in een enkel jaar een rode draad om te herkennen in de volledige stand van de cybersecurity bij de vitale processen. Toch heeft het door de toezichthouders gehanteerde generieke kader een eerste houvast geboden om voor delen van de daarin benoemde vijf beveiligingsdomeinen inzicht te krijgen in de stand van zaken op cybersecurity bij de vitale sectoren. Maar de opbrengst van het toezicht is in dit stadium nóg niet rijk genoeg om over alle thema's een diepgaande samenhangende uitspraak te doen die iets zegt over de stand van de vijf beveiligingsdomeinen in het kader. Het leidt daarom nog niet tot een onderling vergelijkbare opbrengst en levert nog geen allesomvattend en compleet inzicht op. Met elke komende jaarlijkse toezichtcyclus zal dat beeld echter vollediger worden en de komende jaren verder worden ontwikkeld.

   Er zijn meerdere relevante bevindingen in dit samenhangend inspectiebeeld opgenomen. Zo komt uit de toezichtresultaten van ANVS, AT, DNB en ILT naar voren dat over de gehele linie van bekeken vitale organisaties voldoende bewustzijn aanwezig is van het belang van digitale weerbaarheid. Voor de sector nucleair is na een nulmeting gebleken dat het niveau van digitale weerbaarheid over de hele linie in ieder geval een basaal niveau raakt of overstijgt. De sector vertrouwensdiensten laat ook over de hele linie een volwassen beeld zien. In een enkel geval was sprake van een bijzondere casus, zoals het in 2020 door ILT gestarte onderzoek naar de toestand van de cybersecurity en besturing bij Stichting Waternet in het kader van de leveringszekerheid en kwaliteit van drinkwater. De resultaten van dit onderzoek zijn onlangs aan de Tweede Kamer aangeboden.[1]

   Alle vier voornoemde toezichthouders hebben op basis van de inspecties en analyses in hun toezicht verbeterpunten en/of knelpunten gevonden bij vitale organisaties. Een belangrijke conclusie daarbij is dat de onderzochte organisaties op basis van die bevindingen verbetermaatregelen hebben getroffen. Hiermee wordt de noodzaak van deskundig en professioneel toezicht op cybersecurity benadrukt: ondanks het bewustzijn en professioneel niveau bij onder toezicht gestelde organisaties is een eveneens professionele en kritische blik van de toezichthouder van meerwaarde om potentiële risico's of dreigingen bij die vitale sectoren te signaleren en hen te wijzen op het nemen van passende maatregelen.

[1] Onderzoeksrapport Stichting Waternet | Rapport | Inspectie Leefomgeving en Transport (ILT) (ilent.nl).

Conclusies bij inrichting toezicht cybersecurity

2. Duidelijk is dat voor de meeste van de in Nederland vitaal verklaarde processen en sectoren een toezichthouder aangewezen is, maar nog geen volledig dekkend toezicht op cybersecurity bij alle vitale processen in Nederland is geregeld. Bij de meeste van die vitale sectoren is in 2020 toezicht op cybersecurity uitgevoerd. De breedte en diepgang van het toezicht verschilt per sector. Enkele processen of sectoren kennen geen aangewezen toezichthoudende instantie. Dit betreft plaats- en tijdsbepaling middels GPS, chemie, digitale overheidsprocessen en inzet defensie. Daarnaast zijn enkele processen voor wat betreft cybersecurity nog niet in scope van bestaand toezicht: dit geldt voor keren en beheren waterkwantiteit, enkele processen van de sector transport en het proces inzet politie. Ook zijn nog niet van elke sector alle processen in het toezicht meegenomen. Desondanks laat dit eerste samenhangend inspectiebeeld zien dat de toezichthouders hun inspecties in de meeste gevallen weten te richten op de stand van cybersecurity bij vitale processen. Daarmee begint het toezicht op cybersecurity bij vitale processen steeds meer een onderdeel van hun bredere toezichtprogramma te worden.

3. Er zijn meerdere ontwikkelingen die maken dat het toezicht op vitale processen door toezichthouders waarschijnlijk toeneemt. Vitale sectoren in Nederland kennen verschillende grondslagen voor toezicht op cybersecurity. Inmiddels is op Europees niveau een voorstel gedaan voor de vervanging van de oorspronkelijke NIB-richtlijn door een nieuwe richtlijn. Het ziet ernaar uit dat het aantal vitale sectoren daardoor gaat toenemen. Daarnaast wordt in Nederland overwogen de Wbni te wijzigen; daar is nog niet mee begonnen. Hierdoor komen in principe alle vitale processen (voor wat betreft de daaronder vallende netwerk- en informatiesystemen) onder het volledige Wbni-regime te vallen. De verschillen in kaders tussen de aanbieders blijven bestaan totdat de Wbni is gewijzigd. Daarnaast zullen ook geluiden uit de samenleving om bepaalde processen of hele infrastructuren vitaal te verklaren leiden tot een grotere toezichtdruk op de toezichthouders. Ontwikkelingen rond de zorg en de voedselvoorziening zullen waarschijnlijk gevolgen hebben voor de vitale processen.

4. Uit de resultaten in dit inspectiebeeld wordt duidelijk dat het toezicht op cybersecurity bij enkele toezichthouders nog in een opbouwende fase is en bij een aantal andere integraal deel uitmaakt van het totale toezicht bij vitale sectoren. Voorbeelden van die laatste groep zijn ANVS, AT en DNB. Daarom kunnen er voor de sectoren nucleair, financieel, energie, ICT/Telecom, digitale infrastructuur en elektronische vertrouwensdiensten op basis van de toezichtresultaten uitspraken worden gedaan over de stand van cybersecurity.

   Andere toezichthouders zoals IJenV en ILT zijn in opbouw. Met name ILT heeft het afgelopen jaar een flinke inhaalslag gemaakt, met het onderzoek bij Stichting Waternet als beeldend resultaat: er is onvoldoende grip op de cybersecurity waardoor er een verhoogd risico aanwezig is op een cyberincident met mogelijke gevolgen voor de kwaliteit en/of de continuïteit van drinkwater. De opbouw betekent met name dat deze toezichthouders op dit moment naast de uitvoering van toezicht, een substantieel deel van hun tijd moeten besteden aan de ontwikkeling van het toezicht op cybersecurity bij hun vitale sectoren en processen en de deskundigheid en kennis daarvoor moeten aantrekken of ontwikkelen.

IGJ heeft aandacht voor het onderwerp cybersecurity, maar vanuit haar taakuitvoering op dit moment geen vitale organisaties onder toezicht. Een wijziging van de NIB-richtlijn heeft hier mogelijk impact op als de sector gezondheidszorg ook voor Nederland vitaal verklaard zou worden.

5. Goed toezicht kost tijd en middelen. Jaarlijks worden keuzes gemaakt die beïnvloed worden onder meer aard en omvang van de sector en beschikbare toezichtcapaciteit. Voor enkele toezichthouders geldt dat de beschikbare kennis en capaciteit op dit moment nog beperkt is waardoor zij keuzes moeten maken in hun jaarlijkse programmering die niet altijd in de pas lopen met bestuurlijke of maatschappelijke verwachtingen. Een gewijzigde NIB-richtlijn zal mogelijk een substantiële impact hebben op het aantal en de omvang van de sectoren en het toezicht daarop. Extra financiële middelen zijn in dat geval noodzakelijk. Tevens neemt de aard van dreigingen en digitale risico's toe, zoals blijkt uit diverse rapportages, zoals het CSBN. Als de prioritering in beleid ten aanzien van digitalisering en cybersecurity in de komende kabinetsperiode toeneemt, zal dat, gezien de voorgaande conclusies een opdrijvend effect hebben op de verwachtingen richting toezichthouders. De recente motie over de uitbreiding van de toezichtcapaciteit van AP en het Adviesrapport 'Integrale aanpak cyberweerbaarheid' van de Cybersecurityraad (CSR) laten zien dat 'boots on the ground' en voldoende middelen onmisbaar zijn.

Aandachtspunten

De toezichthouders signaleren een aantal aandachtspunten voor de onder toezicht staande organisaties, voor de beleidsverantwoordelijke ministeries en voor zichzelf. Deze aandachtspunten hebben tot doel om de digitale weerbaarheid van vitale processen en aanbieders te verhogen, het bewustzijn voor cybersecurity te vergroten en de professionaliteit en kwaliteit van het toezicht in de breedte te verbeteren.

1. Aandacht én inhoud

Er is bij een aanzienlijk deel van de vitale organisaties sprake van bewustzijn op cybersecurity. Dat is geenszins een reden om achterover te leunen. Toezicht gaat namelijk veel meer om het bevorderen van het gewenste gedrag, dan om het vinden van de misstap. Daarom blijft de noodzaak van voortdurende aandacht voor dit onderwerp, zowel bij de betreffende vitale organisaties als bij beleidsdepartementen en toezichthouders zelf. Cybersecurity is geen onderwerp van de IT afdeling alleen, maar juist ook van de business en verdient daarom organisatie breed voortdurende aandacht en verbetering.

De toenemende inzet en afhankelijkheid ten aanzien van digitale dienstverlening, waaronder clouddiensten wordt door alle toezichthouders gesignaleerd. Een adequaat inzicht en beheersing van risico's in de toeleverantieketen zien zij als prioriteit. In het licht van toenemende digitale afhankelijkheden in toeleverantie en ketens wijzen de toezichthouders tevens op het belang van adequaat business continuïteit management.

Er is aandacht nodig voor de impact van nieuwe technologieën. In de uitvoering van de toezichtpraktijk worden toezichthouders vaak in een vroeg stadium geconfronteerd met de inzet van bijzondere nieuwe oplossingen, bijvoorbeeld Artificial Intelligence (AI).

2. Meer samenhang in het beeld
Het proces om te komen tot een samenhangend inspectiebeeld 2020 heeft de aan dit beeld werkende toezichthouders geleerd dat zij de komende jaren meer aandacht willen geven aan het definiëren van generieke thema's en de wijze waarop invulling wordt gegeven aan het benutten van het generieke kader onder het Bbni.

3. Ontwikkeling toezicht cybersecurity vitale processen
Het zou goed zijn als toezichthouders hun processen en werkwijze op elkaar laten aansluiten. Voordelen daarvan zijn dat kennis en mensen beter en efficiënter kunnen worden uitgewisseld, dat resultaten sector overstijgend beter vergelijkbaar worden en er eenduidige sectorbeelden met rode draden gemaakt kunnen worden en de rode draad er uitgelicht kan worden. Ook kunnen er meer vergelijkbare niveaus worden gecreëerd tussen de toezichthouders onderling.

Het is van belang dat Europese en nationale wetgeving aansluitend op elkaar is. De toezichthouders vragen daarbij aandacht voor het goed op elkaar aansluiten van de diverse wetgevingsinitiatieven. Uitvoerbaarheid, handhaafbaarheid en aansluiting bij bestaande, al dan niet sectorale, toezichtspraktijken zijn daarbij onderwerpen van aandacht. Besluiten in Brussel die leiden tot een toename van bijv. AED's in vitale sectoren vragen ook om een uitbreiding van passende middelen.

Verstoring van vitale processen kunnen grensoverschrijdende gevolgen hebben en vitale aanbieders kunnen in meerdere lidstaten actief zijn. Het is daarom – en mede met het oog op de Europese wetgevingsinitiatieven – van belang dat toezichthouders op cybersecurity in verschillende Europese lidstaten meer structureel gaan samenwerken.

4. Professionaliseer het toezicht op cybersecurity verder
Cybersecurity vraagt kennis en expertise; die zijn nog niet standaard bij alle toezichthouders aanwezig. Van belang is dat kennis en producten worden gedeeld zodat nieuwkomers sneller een gelijkwaardige partner kunnen zijn met de voorlopers. Dat is een belangrijke constatering in het licht van het toenemend belang van digitale dreigingen en verstoringen en de noodzakelijke digitale weerbaarheid.

De toezichthouders vragen daarom aandacht voor voldoende voorwaarden en middelen om aan een voorziene toename in de vraag naar toezicht op digitale processen te voldoen. Dit betreft niet enkel geld, maar ook de beschikbaarheid van goed personeel. Het Rijk, maar ook opleidingsinstituten, zouden in hun opleidingstrajecten en traineeships aandacht kunnen geven aan de benodigde skills voor inspecteurs en auditors. Op deze manier kan de komende jaren een kweekvijver van potentiële professionals worden gevormd.

Doorontwikkeling samenhangend inspectiebeeld

Dit beeld is een belangrijke stap in de doorontwikkeling naar een volwaardig en samenhangend inspectiebeeld van de cybersecurity bij vitale processen. De betrokken toezichthouders hebben de ambitie om dit proces de komende jaren gezamenlijk verder op te pakken. Het inspectiebeeld zal inzicht bieden in de mate waarin vitale aanbieders werken aan een hoog niveau van digitale weerbaarheid en continuïteit. Die doorontwikkeling zal stapsgewijs tot stand komen. Hierbij worden twee lijnen opgepakt:

1. Een beeld op basis van een gemeenschappelijk basiskader. Dat basiskader zal een aantal gedeelde indicatoren bevatten die, op termijn aangevuld met volwassenheidsniveaus, door alle toezichthouders kunnen worden ingezet bij hun toezicht.
2. Het uitvoeren van toezicht op een gezamenlijk geselecteerd aandachtsgebied of thema. Dit leidt ertoe dat elk van de betrokken toezichthouders dat onderwerp in hun toezicht betrekt. Ook willen de toezichthouders onderzoeken in hoeverre een thema gecoördineerd kan worden opgepakt door één multidisciplinair team dat wordt samengesteld uit inspecteurs van de verschillende toezichthouders.

Voor de doorontwikkeling is het van belang dat bij de toezichthouders geïnvesteerd wordt in gezamenlijke kennis en technieken van het toezicht.

De uitkomsten van het samenhangend inspectiebeeld kunnen tevens als input dienen voor het Cybersecuritybeeld Nederland (CSBN) dat jaarlijks door de NCTV wordt vastgesteld.

1 Inleiding

1.1 Aanleiding

Naar aanleiding van het Cybersecuritybeeld Nederland 2019 (CSBN) heeft het kabinet, met het oog op de toenemende digitale dreiging en de achterblijvende digitale weerbaarheid van Nederland, aangekondigd om onder regie van de minister van Justitie en Veiligheid extra maatregelen te treffen om de weerbaarheid van vitale processen tegen cyberdreigingen te versterken.[2] Het CSBN laat zien dat vrijwel alle vitale processen en diensten volledig afhankelijk zijn van ICT. De grootste dreiging die is vastgesteld is die van spionage, verstoring en sabotage vanuit statelijke actoren. Tegelijkertijd is geconstateerd dat de weerbaarheid tegen dit soort cyberdreigingen niet overal op orde is.

Een van die maatregelen richt zich op het versterken van het toezicht. Toezicht vormt volgens het kabinet een krachtige impuls voor vitale aanbieders om blijvend te werken aan een hoog niveau van digitale weerbaarheid en continuïteit. In de kabinetsreactie wordt aangegeven dat de Inspectie Justitie en Veiligheid samen met andere rijksinspecties en toezichthouders zorgdraagt voor een samenhangend inspectiebeeld en onderlinge kennis en expertise tussen inspecties en toezichthouders.

1.2 De betrokken toezichthouders

Dit samenhangend inspectiebeeld 2020-2021 is opgesteld door de toezichthouders die sinds de implementatie van de Europese netwerk- en informatieveiligheid-richtlijn (hierna: NIB-richtlijn)[3] in de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni) samenwerken. Dit betreffen:

- Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)
- Agentschap Telecom (AT)
- De Nederlandsche Bank (DNB)
- Inspectie Gezondheidszorg en Jeugd (IGJ)
- Inspectie Justitie en Veiligheid (IJenV)
- Inspectie Leefomgeving en Transport (ILT).

[2] Beleidsreactie CSBN2019 en voortgangsrapportage NCSA, 12 juni 2019, kenmerk 2623298.
[3] RICHTLIJN (EU) 2016/1148 VAN HET EUROPEES PARLEMENT EN DE RAAD van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

Deze toezichthouders werken sinds de aanloop naar de inwerkingtreding van de Wbni per november 2018 samen door het uitwisselen van kennis en ervaring om daarmee van elkaar te leren. De toezichthouders hebben een vast overleg, dat dient als gremium om met elkaar de verdere professionalisering van het toezicht op het terrein van digitale veiligheid voor zowel de Information Technology (IT) als de Operations Technology (OT), de procesautomatisering van de vitale processen vorm te geven. Inmiddels heeft dat overleg een bredere scope en richt het zich naast de specifieke Wbni-invalshoek ook op cybersecurity bij andere vitale processen. De samenstelling van deze groep betrokken toezichthouders houdt verband met het in dit inspectiebeeld gehanteerde brede begrip van 'vitaal'; zie paragraaf 1.3.1.

Deze sectorale toezichthouders zijn verschillend georganiseerd en in verschillende fasen van ontwikkeling bij de inrichting en uitvoering van het cybertoezicht. Elke sector heeft specifieke kenmerken en eisen ten aanzien van cybersecurity; dat vraagt van de betreffende toezichthouders andere inhoudelijke expertises. Het is de generieke component van cybersecurity die voor deze betrokken toezichthouders de aanleiding geeft om gezamenlijk op te trekken bij het toezicht op cybersecurity van vitale processen. Om daarmee bij te dragen aan de versterking van de digitale weerbaarheid van vitale processen.

Opgemerkt wordt dat de toezichthouders over hun uitgevoerde toezicht verantwoording afleggen via de reguliere verantwoordingslijnen in jaarverslagen c.q. jaarbeelden. Deze reguliere wijze van verantwoording blijft gehandhaafd; dit gezamenlijk opgesteld inspectiebeeld heeft tot doel om de toezichtresultaten over cybersecurity bij de vitale processen en aanbieders in samenhang in beeld te brengen.

Bijzondere positie Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens (AP) is ook een van de betrokken toezichthouders, maar neemt een relatief bijzondere positie in ten opzichte van de andere toezichthouders. De AP houdt namelijk geen toezicht op een specifiek soort organisaties of een specifieke sector of vitaal proces zelf. De AP houdt toezicht krachtens de Algemene Verordening Gegevensbescherming (AVG) op álle organisaties, publiek of privaat, die persoonsgegevens verwerken. Onder deze organisaties vallen ook de vitale aanbieders, voor zover zij hierbij persoonsgegevens verwerken. De AP heeft hierdoor een toezichthoudende rol dwars door verschillende vitale processen heen. Daarbij richt het toezicht van de AP zich niet uitsluitend op de cybersecurity, maar vormt het adequaat beveiligen van persoonsgegevens een belangrijk vereiste voor AVG-conforme gegevensverwerking. De AP werkt daarbij nauw samen met de bij dit beeld betrokken toezichthouders om incidenten aan te pakken die tevens inbreuken in verband met persoonsgegevens betreffen.

Vanwege de bijzondere rol van de AP is de AP in dit inspectiebeeld niet verder opgenomen bij de uitwerkingen per onderwerp/deelvraag en behoort zij ook niet tot de inhoudelijk bij dit beeld betrokken toezichthouders.

1.3 Afbakening

1.3.1 Het begrip 'cybersecurity'

In dit inspectiebeeld wordt onder cybersecurity of digitale veiligheid verstaan: alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing,

uitval of misbruik van een informatiesysteem of computer.[4] Onderdeel hiervan is het beveiligen van de informatie (data). Cybersecurity of digitale veiligheid zijn daarmee nauw verbonden met informatiebeveiliging. Informatiebeveiliging gaat namelijk over de maatregelen en procedures om beschikbaarheid, vertrouwelijkheid en integriteit van informatie(voorziening) en de verwerking van informatie te garanderen en de gevolgen van informatiediefstal of andere incidenten tot een acceptabel niveau te beperken. Het gaat daarbij om maatregelen, procedures en processen die een organisatie treft om beveiligingsproblemen te voorkomen, op te sporen, te onderdrukken en op te lossen. Cybersecurity heeft, naast informatiebeveiliging, zoals hierboven al toegelicht ook een belangrijke rol ten aanzien van de continuïteit van processen, systemen ter voorkoming van maatschappelijke ontwrichting.

1.3.2 Het begrip 'vitaal'

In dit samenhangend inspectiebeeld wordt het begrip 'vitaal' in brede zin toegepast: het gaat hierbij om processen die door vakdepartementen als vitale processen zijn aangemerkt. Een overzicht van deze processen is opgenomen in tabel a. Deze wordt indien nodig geactualiseerd en gepubliceerd op de website van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (hierna: NCTV). De aanbieders van een groot deel van deze processen zijn tevens op basis van de Wbni als vitaal aangewezen.
De vitale processen zijn op basis van verschillende grondslagen geïdentificeerd. Enerzijds door criteria van de vakdepartementen en anderzijds op basis van de categorieën zoals vastgelegd in de Wbni. De Wbni maakt onderscheid tussen twee soorten vitale aanbieders: Aanbieders van Essentiële Diensten (AED) en Andere Aanbieders Van Vitale diensten (AAVA). AAVA's worden niet in de NIB-richtlijn genoemd.

Overigens kan de lijst met vitale processen de komende jaren veranderen. Inmiddels heeft de Europese Commissie een voorstel gedaan voor een nieuwe richtlijn met maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de EU, als vervanging van de oorspronkelijke NIB-richtlijn.[5] Ook wordt in Nederland overwogen de Wbni te wijzigen zodat er geen verschil meer zit tussen de plichten voor AED's en AAVA's. Hierdoor komen in principe alle vitale processen (voor wat betreft de daaronder vallende netwerk- en informatiesystemen) onder de Wbni te vallen. Er is nog niet gestart met het wijzigingstraject.

1.3.3 Overzicht vitale processen en toezichthouders

Dit inspectiebeeld brengt beelden over cybersecurity bij vitale processen samen die afkomstig zijn van de betrokken toezichthouders. ANVS, AT, DNB en ILT houden toezicht op AED's of AAVA's op basis van de Wbni; IGJ en IJenV doen dat niet. Uit de vorige paragraaf blijkt dat de basis waarop processen en aanbieders vitaal zijn verklaard, op verschillende wijze is gerelateerd aan wet- en regelgeving. In onderstaande tabel a is het overzicht opgenomen van de in Nederland als vitaal beoordeelde processen en wie de toezichthouders zijn.

[4] Cybersecurity Woordenboek. Van cybersecurity naar Nederlands; uitgave van Cyberveilig Nederland, 2019.
[5] Network and information systems (NIS Directive). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148; 20 december 2020.

Tabel a. *Totaaloverzicht toezicht op cybersecurity*

Vitaal proces	sector	grondslag			Toezichthouder
		NIB	Wbni		
			AED[1]	AAVA[2]	
Landelijk transport en distributie elektriciteit	Energie	*	*		AT
Regionale distributie elektriciteit	Energie	*	*		AT
Gasproductie, landelijk transport en distributie gas	Energie	*	*		AT
Regionale distributie gas	Energie	*	*		AT
Olievoorziening	Energie	*	*		AT
Internet en datadiensten	ICT/Telecom	*	*		AT
Internettoegang en dataverkeer	Digitale infra-structuur	EECC			AT
Spraakdienst en SMS	ICT/Telecom	EECC			AT
Plaats- en tijdsbepaling middels GNSS					-
Drinkwatervoorziening	Drinkwater	*	*		ILT
Keren en beheren waterkwantiteit	Water			*	- +
Vlucht- en vliegtuigafhandeling	Transport	*	*		ILT
Scheepvaartafwikkeling		*	*		ILT
Vervoer van personen en goederen over (hoofd)spoorweginfrastructuur	Transport	*			ILT++
Vervoer over (hoofd)wegennet	Transport	*			ILT++
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	Chemie				Nnb +++
Opslag, productie en verwerking nucleair materiaal	Nucleair			*	ANVS
Toonbankbetalingsverkeer	Financieel	*	*	*	DNB
Massaal giraal betalingsverkeer	Financieel	*	*	*	DNB
Hoogwaardig betalingsverkeer tussen banken	Financieel	*	*	*	DNB
Effectenverkeer	Financieel	*	*	*	DNB
Communicatie met en tussen hulpdiensten middels 112 en C2000	OOV	EECC			AT en IJenV

Inzet politie	OOV				IJenV
Basisregistraties personen en organisaties	Digitale overheids-processen				onbekend
Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties)					-
Elektronisch berichtenverkeer en informatieverschaffing aan burgers					-
Identificatie en authenticatie van burgers en bedrijven	Vertrouwens-diensten	eIDAS			AT
Inzet defensie	Defensie				-

[1] AED: Aanbieder Essentiële Dienst. Hiervoor geldt de Wbni-zorgplicht en -meldplicht waarop toezicht wordt gehouden.

[2] AAVA: Andere Aangewezen Vitale Aanbieder. Hiervoor geldt alleen een Wbni-meldplicht bij het NCSC en hierop wordt geen toezicht gehouden.

\+ Nog geen toezichthouder aangewezen.
++ Deze processen zijn (inmiddels) door het betrokken vakdepartement als vitaal aangemerkt; daarbinnen worden de AED's aangewezen. Dit vindt plaats in 2021.
+++ Chemie: Omgevingsdiensten zijn toezichthouder, ILT is tweedelijns toezichthouder. Voor cybersecurity is echter (nog) geen toezichthouder aangewezen..

Geen vitaal proces in NL					
Gezondheidszorg ++++		*			IGJ

++++ De sector gezondheidszorg waar de IGJ toezicht op houdt, is wel Europees NIB-vitaal maar in het kader van de Wbni tot op heden niet vitaal verklaard en er zijn ook geen AED's in de zorg aangewezen. Het ministerie van VWS gaat opnieuw beoordelen wat er van de zorg of delen van de zorg vitaal verklaard zal worden. Het is nu nog niet duidelijk welke consequenties dat gaat hebben voor het toezicht van de IGJ en dat van anderen als bepaalde delen van de zorg vitaal worden verklaard.

1.4 Eerste interne beeld van toezicht op digitale vitale weerbaarheid

De bij het toezicht op vitale processen en aanbieders betrokken toezichthouders hebben – vooruitlopend op het opstellen van een samenhangend inspectiebeeld over de cybersecurity van de vitale processen – in maart 2020 de stand van zaken in beeld gebracht van het toezicht op cybersecurity bij organisaties die behoren tot de vitale processen in Nederland. Daarmee hebben zij een gemeenschappelijk vertrekpunt geformuleerd voor de ontwikkeling van het samenhangend inspectiebeeld. Doordat dat eerste Beeld een interne werking had, is dat niet gepubliceerd. In dat Beeld hebben de toezichthouders een aantal aanbevelingen gedaan. Dat eerste Beeld is op 11 maart 2020 aan de minister van Justitie en Veiligheid, als coördinerend minister voor cyber, aangeboden. De minister van JenV heeft het aan zijn collega-vakministers van Economische Zaken en Klimaat (EZK), Financiën (FIN), Infrastructuur en Waterstaat (IenW) en Volksgezondheid, Welzijn

en Sport (VWS) aangeboden en hen verzocht de aanbevelingen – voor zover die tot hen gericht zijn – te doen opvolgen. Dit betreffen de volgende aanbevelingen.

1. Stimuleer de betrokken toezichthouders om te komen tot een gemeenschappelijk kader voor toezicht op cybersecurity vitale processen, waarbij er ruimte blijft voor de verscheidenheid per vitaal proces en voor sectorale invulling.
2. Zorg voor een toereikende grondslag voor die toezichthouders waar dat nog niet het geval is. En daar waar nog geen toezichthouder voor een vitaal proces bekend is, zorgdragen dat hierin wordt voorzien.
3. Bezie op welke wijze er meer samenhang kan worden gerealiseerd tussen de lijst vitale processen van de NCTV, de NIB-vitale processen en de vitale processen conform de Wbni.
4. Zorg te dragen dat de betrokken toezichthouders invulling geven aan het toezicht op cybersecurity voor de vitale processen en hiervoor ook voldoende middelen beschikbaar krijgen.

In hoofdstuk 5 wordt ingegaan op de wijze waarop tot nu toe opvolging is gegeven aan de aanbevelingen.

1.5 Leeswijzer

In hoofdstuk 2 zijn de doelstelling en het gemeenschappelijk kader met de geselecteerde thema's voor dit samenhangend inspectiebeeld beschreven. Hoofdstuk 3 biedt op hoofdlijnen inzicht in de achtergrond en context van het toezicht door de betrokken toezichthouders op cybersecurity bij de vitale processen. In hoofdstuk 4 zijn de resultaten beschreven van het toezicht dat de toezichthouders in 2020 en begin 2021 hebben uitgevoerd op cybersecurity bij de verschillende vitale aanbieders en processen. Hoofdstuk 5 geeft de stand van de opvolging van de aanbevelingen uit het eerste Beeld. In hoofdstuk 6 zijn de conclusies en een aantal aandachtspunten beschreven. Tot slot schetsen de toezichthouders in hoofdstuk 7 hun ambitie voor de doorontwikkeling van het samenhangend inspectiebeeld. Bijlage I geeft de meer specifieke beschrijving van de achtergrond en context van het toezicht uit hoofdstuk 3; bijlage II bevat de gebruikte afkortingen.

2 Doelstelling en gemeenschappelijk kader

2.1 Doelstelling

De doelstelling van dit samenhangend inspectiebeeld is het enerzijds informeren over de ontwikkeling van en binnen het toezicht op cybersecurity. Anderzijds is het doel om in samenhang zo goed als nu mogelijk is in beeld brengen van de resultaten van toezicht door de betrokken toezichthouders op cybersecurity van vitale processen.

Dit document is een belangrijke stap in de ontwikkeling naar een volwaardig en samenhangend inspectiebeeld. De omvang en inhoud van de hierboven benoemde doelstellingen verhouden zich daarom in dit inspectiebeeld naar verwachting anders tot elkaar dan in de volgende inspectiebeelden het geval zal zijn. Voorzien wordt dat er steeds meer bruikbare data beschikbaar zal zijn om de samenhangende resultaten van het toezicht in beeld te kunnen brengen, waardoor deze doelstelling meer ruimte krijgt in de toekomstige documenten. De toezichthouders hebben de ambitie uitgesproken om dit proces de komende jaren gezamenlijk verder uit te werken. Dat toekomstige inspectiebeeld zal een beeld geven van de staat van de cybersecurity van de vitale processen en de vitale aanbieders en inzicht bieden in de mate waarin vitale aanbieders werken aan een hoog niveau van digitale weerbaarheid en continuïteit. In hoofdstuk 7 wordt nader ingegaan op de doorontwikkeling van het samenhangend inspectiebeeld.

In dit samenhangend inspectiebeeld zijn de toezichtresultaten over de niet-vitale processen, gezien de doelstelling van dit document, niet meegenomen.

De toezichthouders gaan in de verdere ontwikkeling van het inspectiebeeld van de cybersecurity vitale processen een gemeenschappelijk kader met generieke doelstellingen hanteren. In het inspectiebeeld brengen zij in samenhang de uitkomsten van hun toezicht in beeld.

2.2 Gemeenschappelijk kader

In deze paragraaf wordt beschreven op welke wijze de betrokken toezichthouders hun toezichtproces op cybersecurity bij vitale processen hebben ingericht. Vervolgens wordt een gemeenschappelijk kader gepresenteerd waarin thema's zijn opgenomen waarover door de betrokken toezichthouders in dit samenhangend inspectiebeeld wordt gerapporteerd. Zoals in het vorige hoofdstuk is toegelicht zijn

de ANVS, AT, DNB en ILT Wbni-toezichthouders; IGJ en IJenV zijn dat niet. Hieronder worden de verschillende elementen beschreven vanuit het perspectief van de Wbni-processen.

2.2.1 Grondslag en verantwoordelijkheden

De betrokken Wbni-toezichthouders dragen vanuit hun rol bij aan een nadere invulling van de zorgplicht zoals deze is opgenomen in de Wbni. De zorgplicht geeft aan dat AED's passende en evenredige technische en organisatorische maatregelen nemen om hun diensten te beveiligen. Verder nemen zij passende maatregelen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. De toezichthouders inspecteren dit door middel van het uitvoeren van inspecties gericht op opzet, bestaan en werking van het risicomanagementproces en het treffen van passende en evenredige beheersingsmaatregelen.

Het hanteren van een open norm is een belangrijk onderdeel van dit actieve toezicht(beleid). Een open norm is principle based opgesteld in plaats van rule based. Hierbij geven de AED's zelf aan op welke wijze zij invulling geven aan de beheersdoelstellingen. Tijdens een inspectie stelt de toezichthouder vast dat de getroffen maatregelen al dan niet in lijn zijn met de beheersdoelstellingen. Wel is het zo dat binnen sommige sectoren specifieke – soms internationaal verplichte – normen noodzakelijk zijn om de regelgeving uitvoerbaar en handhaafbaar te maken. Desbetreffende bevoegde autoriteit kan specifieke normen nader uitwerken in specifieke sectorale regelgeving.[6] De grondslag hiervoor is opgenomen in het Bbni dat op 1 juni 2021 geheel in werking is getreden.

Omdat toezichthouders beperkte capaciteit hebben, werken zij risico gebaseerd. Hierbij houden zij onder andere rekening met het risicoprofiel, het volwassenheidsniveau van de AED's en hun naleefgedrag ten aanzien van de digitale weerbaarheidseisen. Door deze risico gebaseerde aanpak brengen zij prioriteiten aan in hun jaarplannen. Het gevolg is dat de toezichthouders jaarlijks een aantal thema's onderkennen die zij nader inspecteren. Deze thema's worden op verschillende niveaus vastgesteld:

1. Thema's die gelden voor alle sectoren. Bijvoorbeeld ransomware aanvallen en patch management.
2. Thema's die sectorspecifiek zijn. Bijvoorbeeld SIMswapping en hackaanvallen op de OT security.
3. Thema's die AED specifiek zijn. Bijvoorbeeld een overname van een AED door een andere AED.

Dit samenhangend inspectiebeeld omvat thema's op het eerste en tweede niveau. AED-specifieke thema's vallen buiten de scope, omdat hiervan geen algemeen beeld is af te leiden.

2.2.2 Proces van toezicht

Elke toezichthouder heeft het toezichtproces op zijn eigen wijze ingericht, afgestemd op de sectorspecifieke kenmerken en interne werkwijzen. Toch wordt in deze

[6] Ten aanzien van het hanteren van open normen kent de ILT een afwijkende werkwijze. Het ministerie van IenW heeft naar aanleiding van een HUF-toets door de ILT een Ministeriële regeling opgesteld met meer concrete normen waarmee invulling wordt gegeven aan de zorgplicht in de sectoren waar de ILT is aangewezen als toezichthouder.

paragraaf het proces van het toezicht op cybersecurity beschreven dat in algemene zin door de toezichthouders wordt gevolgd. Hiermee wordt aangegeven op welke wijze de toezichthouders de informatie hebben verzameld die voor dit inspectiebeeld is gebruikt. Zij hebben voor hun toezicht allerlei activiteiten uitgevoerd die uiteindelijk gericht zijn op gedragsinterventies naar de organisaties waarop zij toezicht houden. In hoofdstuk 3 en bijlage I wordt dit uitgebreid toegelicht.

Het kwaliteitstoezicht door elke toezichthouder wordt uitgevoerd door middel van inspecties. Om dit toezicht effectief uit te kunnen voeren is het belangrijk om de AED's goed te begrijpen. In het proces van toezicht wordt hier dan ook veel aandacht aan besteed. Het proces van toezicht kent de volgende stappen:

1. Kennismaking. Met nieuwe toegewezen AED's vindt een kennismaking plaats. Op hoofdlijnen wordt algemene bedrijfsinformatie over de AED verzameld, kan de AED een toelichting geven op haar organisatie en kan de toezichthouder het proces van toezicht toelichten.
2. Begrip van het bedrijf. Na de kennismaking voert de toezichthouder analyses uit om het risicoprofiel van de AED, inclusief de Te Beschermen Belangen (TBB's) compleet te maken.
3. Inventarisatie. Op basis van een inventarisatie krijgt de toezichthouder inzicht in de sterke en zwakke punten ten aanzien van de digitale weerbaarheid van de AED.
4. Risicoanalyse. Op basis van het risicoprofiel, de sterke en zwakke punten en overige informatie zoals incidenten en dreigingen, voert de toezichthouder een risicoanalyse uit. Op basis van de risicoanalyse worden thema's voor inspecties geselecteerd.
5. Planning. De geselecteerde thema's worden in een planning verwerkt.
6. Inspectie. Conform planning worden de inspecties en mogelijk andere toezichtactiviteiten uitgevoerd.
7. Rapportage. Door de toezichthouder wordt over de uitkomsten van het onderzoek gerapporteerd.

2.2.3 Thema's 2020

Zoals hierboven is aangegeven willen de toezichthouders in de verdere ontwikkeling van het inspectiebeeld een gemeenschappelijk kader met generieke doelstellingen hanteren. Dat is er nu nog niet. Als eerste aanzet daarvoor wordt hieronder een eerste kader met thema's geschetst dat het vertrekpunt vormt voor die ambitie.

Om inzicht te geven in de thema's van de verschillende toezichthouders is de zogenaamde 'kapstok' vanuit het Bbni gehanteerd. Het Bbni duidt de vitale aanbieders aan die onder de verplichtingen van de Wbni vallen en kent de volgende beveiligingsdomeinen:

- Risico gebaseerde aanpak: dit domein omvat onder andere het uitvoeren van risicoanalyses. Onderdeel van de risicoanalyse is het beschrijven van de risico's en de wijze waarop de risico's tot een aanvaardbaar niveau worden verkleind.
- Organisatie van netwerk- en informatiebeveiligingsbeheer: dit domein omvat onder andere de informatiebeveiligingsstrategie en de uitwerking hiervan in beleid en taken, bevoegdheden en verantwoordelijkheden.

- Incidenten voorkomen: dit domein omvat onder andere de wijze waarop defense in depth, life cycle management, asset management en patch management worden toegepast.
- Detectie en respons: dit domein omvat onder andere de maatregelen om incidenten te detecteren, analyseren en de impact zo veel mogelijk te beperken.
- Gevolgen van incidenten beperken: dit domein omvat onder andere bedrijfscontinuïteits- en crisismanagement.

In afbeelding 1 is per toezichthouder aangegeven welke thema's zij voor dit inspectiebeeld in 2020 hebben geselecteerd. Deze thema's zijn ingedeeld naar de beveiligingsdomeinen waardoor een begin van een generiek kader tot stand is gebracht. Elke toezichthouder heeft op basis van een eigen risicoafweging een keuze gemaakt voor de geselecteerde thema's bij een of meer beveiligingsdomeinen. Daardoor is dit kader nu niet compleet en heeft het voor elke toezichthouder geleid tot deelwaarnemingen bij één of enkele beveiligingsdomeinen. Bij de doorontwikkeling van het inspectiebeeld willen de toezichthouders een meer allesomvattende selectie over alle beveiligingsdomeinen in kaart brengen.

In hoofdstuk 4 zijn de resultaten van het toezicht op deze thema's beschreven. Hoewel IJenV geen Wbni-toezichthouder is, volgt zij voor het toezicht op de vitale processen in de OOV-sector wel de indeling van dit generieke kader. Het cybertoezicht door de ILT op basis van sectorale regelgeving is in onderstaand overzicht niet meegenomen. Cybersecurity is bijvoorbeeld onderdeel van het risicomanagementsysteem van drinkwaterbedrijven dat in de Drinkwaterwet wordt voorgeschreven. De ILT heeft op die basis de leveringsplannen van de tien drinkwaterbedrijven beoordeeld. Onderdeel daarvan waren tien auditrapporten op basis van de PA-beveiligingsnorm. De sector gezondheidszorg waar de IGJ toezicht op houdt, is wel Europees NIB-vitaal maar in het kader van de Wbni niet vitaal verklaard en er zijn ook geen AED's in de zorg aangewezen. IGJ heeft daarom voor dit inspectiebeeld geen thema's benoemd.

	Risicogebaseerde Aanpak	Organisatie van netwerk- en informatiebeveiligings-beheer	Incidenten voorkomen	Detectie & Response	Gevolgen van Incidenten beperken
ANVS	1. Asset Management	1. Mitigeren aanvalspaden 2. Netwerksegmentatie 3. Access management	1. Testen en Oefenen	1. Testen en Oefenen	1. Backup & Restore
AT	1. General IT Controls en technische vereisten	1. General IT Controls en technische vereisten	1. Detectie, Logging en Monitoring 2. General IT Controls en technische vereisten	1. General IT Controls en technische vereisten	1. General IT Controls en technische vereisten 2. Incidenten-onderzoek
DNB	Operational Risks	Operational Risks	Operational Risks	Operational Risks	Operational Risks
IGJ	Nvt	Nvt	Nvt	Nvt	Nvt
IJenV	1. Risicomanagement Meldkamers				
ILT		1. Onderzoek drinkwaterbedrijf Stichting Waternet	1. Kwetsbaarheden en patchmanagement operational technology		

Afbeelding 1. *Geselecteerde thema's toezichthouders 2020.*

3 Het toezicht op cybersecurity bij vitale processen

Omdat dit het eerste document is dat in samenhang een beeld geeft van de stand van de cybersecurity bij vitale processen, wordt in dit hoofdstuk op hoofdlijnen inzicht gegeven in de achtergrond en context van het toezicht op cybersecurity bij de vitale processen door de betrokken toezichthouders.

De meer specifieke beschrijving van het hoe en wat van het toezicht op cybersecurity bij vitale processen is als nadere toelichting opgenomen in bijlage I.

3.1 Achtergrond: doelstelling, wijze van toezicht en oordeelsvorming.

Dit onderwerp valt uiteen in de visie op cybersecurity van de toezichthouder, het doel van het toezicht en hoe de toezichthouder zich een oordeel vormt over de stand van zaken van de cybersecurity van de onder toezicht gestelde vitale organisatie(s) of vitale processen.

Een aantal van de betrokken toezichthouders heeft een expliciet doel geformuleerd voor het toezicht op cybersecurity van vitale processen. Andere hebben dat nog niet. Wel heeft het onderwerp bij alle toezichthouders de aandacht en wordt daarop georganiseerd. Doelstelling is veelal om maatschappelijke risico’s te beheersen en organisaties te stimuleren in het vergroten van weerbaarheid en het nemen van eigen verantwoordelijkheid. Het toezicht op cybersecurity is bij enkele van de betrokken toezichthouders nog volop in ontwikkeling.

De toezichthouders die toezicht bij Wbni-vitale organisaties houden doen dit op gelijksoortige wijze. Zij zetten meerdere instrumenten in om zich een oordeel te vormen over de stand van zaken van cybersecurity. Een gemene deler bij alle toezichthouders is de risicogerichte en informatiegestuurde aanpak. Zo worden vragenlijsten ingezet, wordt op locatie geïnspecteerd, vinden interviews plaats, wordt gebruik gemaakt van self-assessments en worden resultaten van pen-testen en red-teaming (doorlopende testen) benut.

3.2 Context: normenkader, volwassenheidsniveaus en toetsingskader

De normenkaders die de toezichthouders bij vitale organisaties hanteren zijn, voor zover beschikbaar, sectorspecifiek. Deze variëren van dynamische kaders op basis van open normen tot specifieke normen vanuit de sector zelf. Waar geen specifieke normen beschikbaar zijn, worden de betrouwbare en veelgebruikte standaarden voor 'cybersecurity' gebruikt, zoals de ISO27000, NIST, ETSI of de NEN. Drie van de betrokken toezichthouders hanteren volwassenheidsniveaus bij de normenkaders.

Voor het uitvoeren van toezicht op cybersecurity zijn bepaalde documenten relevant. In onderstaande tabel b is aangegeven of de toezichthouder inzicht heeft in de beschikbaarheid van deze documenten bij de onder toezicht gestelde organisaties of dat deze documenten beschikbaar zijn bij de instellingen en als zodanig door de toezichthouder opvraagbaar zijn.

Tabel b. *Beschikbaarheid relevante documenten ten behoeve van toezicht.*

	ANVS	AT	DNB	IGJ*	ILT**	IJenV*
Cybersecurity beleidsplan	Ja	Ja	Ja	Nee	Nee	Nee
informatiebeveiligingsplan	Ja	Ja	Ja	Nee	Ja	Nee
dreigingsanalyse per vitaal proces	Ja	Ja	Ja	Nee	deels	Nee
risicoanalyse per vitaal proces	Ja	Ja	Ja	Nee	deels	Nee
Disaster Recovery Plan	Ja	Ja	Ja	Nee	deels	Nee
Incident Response Plan	Ja	Ja	Ja	Nee	deels	Nee
incidentenregister voor cybersecurity-incidenten en –meldingen	Ja	Ja	Ja	Nee	Nee	Nee
anders: auditrapporten	-	-	-	-	Ja	-

* Geen Wbni-toezichthouder.

** Vanuit Wbni nog geen volledig beeld, maar ook uit het reguliere toezicht op bijvoorbeeld leveringsplannen drinkwaterbedrijven zijn documenten beschikbaar.

3.3 Context: plannings- en beleidscyclus

In deze paragraaf wordt aangegeven in hoeverre het toezicht op cybersecurity onderdeel is van de plannings- en beleidscyclus.

Bij een aantal van de betrokken toezichthouders is het toezicht op cybersecurity onderdeel van de plannings- en beleidscyclus. De focus op de digitale vitale processen maakt daar in de meeste gevallen impliciet onderdeel van uit. In de meeste gevallen wordt het toezicht uitgevoerd op basis van een risicoanalyse.

De betrokken toezichthouders die toezicht op de digitale vitale processen houden, voeren dat actueel uit en hebben recente resultaten.

3.4 Context: wet- en regelgeving

Het algemene toezicht dat de betrokken toezichthouders uitvoeren, verrichten zij op basis van verschillende sectorale en in meerdere gevallen internationale wet- en regelgeving. In tabel c is hiervan een overzicht opgenomen.

Ondanks deze diversiteit aan regelgeving, staat dit een vergelijkbare en samenhangende aanpak van het toezicht in beginsel niet in de weg. Dit komt ook naar voren uit de conclusie bij het onderwerp normenkaders. Vanuit de ambitie om in gezamenlijkheid tot een samenhangend inspectiebeeld te komen zijn wel een meer eenduidige wettelijke grondslag en bevoegdheden en daarmee meer evenwicht en samenhang tussen de lijst vitale processen van de NCTV, de NIB-vitale (soorten) entiteiten en de vitale processen conform de Wbni wenselijk.

Tabel c. *Overzicht toezichthouders in relatie tot grondslag toezicht*

	Vitaal proces NCTV-lijst	NIB	Wbni
ANVS	+	-	+
AT	+	+	+
DNB	+	+	+
IGJ	-	+	-
ILT	+	+	+
IJenV	+	-	-

In de Europese NIB-richtlijn is één sector als vitaal aangewezen die in Nederland niet als vitale sector is geïdentificeerd en op dit moment ook niet in de Wbni is opgenomen. Dit betreft de sector gezondheidszorg. De IGJ is hiervoor de toezichthouder. Door het Ministerie van VWS is in 2021 een vitaal-beoordelingsanalyse gestart voor de sector Gezondheidszorg, waaruit moet blijken of gezondheidszorg een proces is van vitaal belang.

3.5 Context: governance

De betrokken toezichthouders hebben verschillende rechtsvormen. Dit varieert van een rijksinspectie als onderdeel van een ministerie, een agentschap, ZBO of NV.

De toezichthouders voeren daadwerkelijk toezicht uit op cybersecurity bij de vitale organisaties en vitale processen waar zij toezichthouder voor zijn.

De meeste van de betrokken toezichthouders hebben intensieve contacten met Europese partners over toezicht op het digitale domein en zijn actief betrokken bij werkgroepen en gezamenlijke toezichtactiviteiten.

3.6 Meerjarenperspectief

In het laatste onderdeel van dit hoofdstuk wordt beschreven welke ontwikkelingen en ambities er op de lange termijn bij de betrokken toezichthouders op het gebied

van het toezicht op cybersecurity zijn. In bijlage I is dit voor elke toezichthouder uitgebreid beschreven.

De betrokken toezichthouders werken vrijwel allemaal aan het opzetten of aan het doorontwikkelen van het toezicht op cybersecurity. Het is hierbij van belang om aandacht te hebben voor de capaciteit en deskundigheid die nodig zijn voor het uitvoeren van het toezicht in het kader van de Wbni. Zo wordt nagedacht over de inzet van meer menscapaciteit op initiatieven die moeten leiden tot de verdere opbouw van kennis en kunde voor alle toezichthouders. Hierbij wordt actief de samenwerking opgezocht met andere toezichthouders en wordt er gekeken naar mogelijkheden tot uitwisseling en samenwerking. Ook breder, bijvoorbeeld internationaal en met andere toezichtspartijen en/of private partijen, wordt gekeken naar de mogelijkheden om kennis uit te wisselen en elkaar te informeren over (toekomstige) onderzoeken en/of thema’s van onderzoeken.

4 Resultaten toezicht op cybersecurity vitale processen

4.1 Inleiding

In dit hoofdstuk worden de resultaten beschreven van het toezicht dat de betrokken toezichthouders in 2020 en begin 2021 hebben uitgevoerd op cybersecurity bij de verschillende vitale aanbieders en processen.

Zoals in paragraaf 2.3 is uitgelegd, willen de toezichthouders de resultaten van het toezicht in samenhang in beeld brengen. Daarmee beogen ze om vanuit de vaak volstrekt verschillende toezichtsectoren toch een generiek en samenhangend beeld te schetsen op aspecten die generiek zijn vanuit de gemeenschappelijke basis: de beveiligingsdomeinen uit de Wbni.

Hieronder zijn eerst de toezichtresultaten van elke betrokken toezichthouder beschreven. Omdat voor de gezondheidszorg in Nederland geen vitale processen of aanbieders zijn aangewezen, heeft de IGJ geen toezicht gehouden dat zich – in het kader van de in de hierboven weergegeven beveiligingsdomeinen – specifiek richt op thema's van cybersecurity.

4.2 Toezichtresultaten

Hieronder wordt per toezichthouder aangegeven:

- in een tabel de geselecteerde thema's uit het kader met de beveiligingsdomeinen, afgeleid van de tabel in paragraaf 2.2.3;
- bij welke vitale sector(en) toezicht is uitgeoefend;
- wat het onderwerp en aanleiding van het toezicht zijn geweest;
- wat het algemene beeld van de resultaten van het toezicht is.

Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)

Tabel d. *Geselecteerde thema's ANVS per beveiligingsdomein*

Risico-gebaseerde aanpak	Organisatie van netwerk- en informatiebevei-ligingsbeheer	Incidenten voorkomen	Detectie & response	Gevolgen van incidenten beperken
Asset Management	-Mitigeren aanvalspaden -Netwerksegmentatie -Access management	Testen en Oefenen	Testen en Oefenen	Backup & Restore

Vitale sector: Nucleair

Onderwerp: Onafhankelijk administratief en technisch onderzoek naar de wijze van en mate waarin de acht nucleaire organisaties (zes op basis van een vergunning Kernenergiewet en twee op basis van het Geheimhoudingsbesluit Kernenergiewet) de algehele cyberweerstand hebben georganiseerd, in procedures hebben vastgelegd en in de praktijk hebben geïmplementeerd. Het onderzoek omvatte alle domeinen van cybersecurity: identificeer, bescherm, detecteer, reageer en herstel (gebaseerd op het NIST framework en de CMMI volwassenheidsniveaus). Het doel is het beoordelen van de werking in de praktijk, verbeteren van het toezicht en het opstellen van een integraal cybersecurity-sectorbeeld.

Aanleiding: Wens om te komen tot meer zicht op de algehele digitale weerbaarheid van de nucleaire sector. Tevens de wens om de stand van de digitale weerbaarheid te kunnen kwantificeren middels volwassenheidsniveaus gerelateerd aan het vigerende dreigingsbeeld per bedrijf/nucleaire activiteit (waarmee de voortgang inzichtelijk kan worden gemaakt).

Algemeen beeld: Bij alle nucleaire organisaties zijn door een gedetailleerde technische analyse knelpunten in de opzet en werking van de digitale processen van de security, de kantoorautomatisering (IT) en de primaire processen (OT) geconstateerd, die in potentie kunnen leiden tot beveiligingskwesties variërend van gering tot kritiek/hoog. Deze knelpunten zijn door de nucleaire organisaties direct geadresseerd en gemitigeerd. Hierop zijn inspecties uitgevoerd.

De ANVS voldoet met de Ministeriele Regeling Security, de DBT en dit recente onderzoek aan de eisen die binnen de Wbni gesteld worden:

- Er zijn in overleg met de sector drempelwaarden voor het melden van incidenten opgesteld (in lijn met de IAEA structuur op systeemniveau).
- De referentiedreiging is in overleg met de sector vastgesteld en deze wordt periodiek geactualiseerd.
- De te beschermen belangen zijn vastgesteld: geen emissie van nucleair materiaal, het voorkomen van sabotage en het weglekken van proliferatie gevoelige informatie.
- Er is een meldformulier conform de eisen van de Ministeriele Regeling en Wbni met daarin safety en security aspecten.

Door dit onderzoek is op alle domeinen een gedetailleerd beeld verkregen over de actuele stand van zaken met betrekking tot cyberweerstand per individuele nucleaire organisatie. Het niveau van digitale weerbaarheid overstijgt over de hele

linie het basis niveau (ad hoc en initieel). Echter de nucleaire sector in Nederland is erg divers, van een gesloten kerncentrale tot innovatieve technologische bedrijven. Hierdoor variëren de volwassenheidsniveaus sterk, van een gemiddelde cyber hygiëne (vastgelegd en herhalend) tot een goede cyber hygiëne (gedefinieerd en gemanaged). Het gewenste niveau per organisatie (grading toepassen) van digitale weerbaarheid wordt per nucleaire organisatie door de ANVS vastgesteld in 2021/2022.

Alle rapporten (individueel en sectorbeeld) zijn gerubriceerd als Staatsgeheim-confidentieel. De resultaten gecombineerd vormen het integraal sectorbeeld dat op 21 januari 2021 is aangeboden aan de minister en staatssecretaris van IenW. Dit sectorbeeld geldt als een nulmeting ten behoeve van een verdere gestructureerde versterking en verdieping van het toezicht op de cyberweerbaarheid in de sector Nucleair. Middels verbeterplannen, de focus op voortdurend verbeteren en het toezicht op deze activiteiten zal de digitale weerbaarheid van de nucleaire sector in de komende tijd verbeteren.

Agentschap Telecom (AT)

Tabel e. *Geselecteerde thema's AT per beveiligingsdomein*

Risico-gebaseerde aanpak	Organisatie van netwerk- en informatiebevei-ligingsbeheer	Incidenten voorkomen	Detectie & response	Gevolgen van incidenten beperken
General IT Controls en technische vereisten	General IT Controls en technische vereisten	-Detectie, Logging en Monitoring -General IT Controls en technische vereisten	General IT Controls en technische vereisten	-General IT Controls en technische vereisten -Incidenten-onderzoek

Vitale sectoren: Energie en Digitale Infrastructuur

Onderwerp: Detectie, Logging en Monitoring

Aanleiding: Het is in de praktijk zo goed als onmogelijk om indringers buiten de deur te houden met alleen preventieve maatregelen. Goede maatregelen zijn noodzakelijk om onder andere hackaanvallen te detecteren en netwerk- en informatiesystemen dienen faciliteiten te bieden voor logging en monitoring. Randvoorwaardelijk voor deze activiteiten zijn een betrouwbare inrichting van asset management, segmentering van systemen en een aansluiting op het incident management proces. De toezichtresultaten zijn verkregen uit sectorspecifieke inspecties naar de security van de Operationele Techniek (OT).

Algemeen beeld: De AED's in beide sectoren zijn zich bewust van het belang van de combinatie van preventieve en detectieve maatregelen om de essentiële dienst te beveiligen. Zij hebben passende en evenredige maatregelen getroffen. Hierbij is rekening gehouden met de mate van automatisering en omvang van de AED. Specifiek voor de netbeheerders valt het op dat zij elkaar proactief opzoeken om kennis te delen en samen te werken op het gebied van cybersecurity. Dit is een ontwikkeling die Agentschap Telecom in haar toezicht stimuleert. Tevens hebben de

AED's de drive om steeds verder te verbeteren. Zo signaleert Agentschap Telecom dat steeds meer AED's zich laten certificeren voor ISO27001, monitoring steeds effectiever inregelen door nieuwe risicoscenario's toe te voegen en externe expertise inschakelen. Agentschap Telecom heeft tijdens haar inspecties bevindingen gedaan en discussies gevoerd die hebben geleid tot aanscherpingen en verbeteringen. Aanvullend op de thema inspectie is Agentschap Telecom eind 2020 gestart met een onderzoek om te inventariseren welke ketenafhankelijkheden en concentratie risico's aanwezig zijn binnen energiesector.

AT

Vitale sector: Digitale vertrouwensdiensten

Onderwerp: General IT-controls en QSCD's

Aanleiding: Aanleiding voor full-inspectie bij onder toezicht gestelden in deze sector is telkens een Conformiteitsbeoordelingsrapport dat wordt opgesteld door een geaccrediteerde conformiteitsbeoordelaar. Op basis van het geschetste beeld beoordeelt AT eigenstandig de betreffende provider op alle in de eIDAS verplicht gestelde eisen. Daarnaast is er in 2020 specifiek aandacht besteed aan de technische vereisten rond de QSCD's (gekwalificeerde dragers van ondertekensleutels van vertrouwensdiensten), als thema-onderzoek.

Algemeen beeld: De huidige stand van zaken rond de opvolging van eIDAS-eisen bij de gekwalificeerde aanbieders van vertrouwensdiensten is beoordeeld als goed. Daar waar tekortkomingen optreden vindt reactie en eventuele reparatie snel plaats.

Vanaf 2020 is bijzondere aandacht voor identificatie op afstand (digitaal) als onderdeel van vertrouwensdiensten. Naar een bijzondere toepassing hiervan met AI-technologie bij een van de providers is AT een specifiek onderzoek gestart, omdat hier nog weinig ervaring, kennis en kunde over is opgedaan. Het is de verwachting dat in de toekomst veel vaker AI-technologieën ingezet gaan worden die onderdeel moeten worden van het inspectieproces. Het is belangrijk dat AT voor het toezicht meer ervaring en kennis hierover opbouwt.

AT

Vitale sector: Telecom

Onderwerp: Telecom Security (bereikbaarheid 112)

Incidentonderzoek, samen met IGJ en IJenV

Aanleiding: Op maandag 24 juni 2019 vond tussen 15.34 uur en 18.52 uur een storing plaats in het telefonienetwerk van KPN. Als gevolg van de storing konden klanten van KPN via het vaste en het mobiele netwerk nagenoeg niet meer bellen of gebeld worden. Hierdoor was ook de 112-alarmcentrale onbereikbaar. Burgers konden via het alarmnummer 112 geen hulp inroepen van brandweer, politie of ambulance. Ook de door KPN geleverde 0800- en 0900-nummers - zoals het landelijke servicenummer 0900-8844 van de politie - waren als gevolg van de storing niet meer bereikbaar.

Op diezelfde dag kampte KPN ook met een storing van NL-Alert via 4G, hoewel deze los stond van de telefoniestoring. De storing van NL-Alert duurde bijna 24 uur, van

12.00 uur tot de volgende dag 11.40 uur. Om de burgers te informeren over de storing van 112 en 0900-8844 werden die dag zowel regionale als landelijke NL-Alertberichten verzonden. Geen enkele gebruiker die verbonden was met het 4G-netwerk van KPN kon deze NL-Alertberichten echter ontvangen.

Algemeen beeld: AT heeft op basis van zijn onderzoek geconcludeerd dat, indien de maatregelen die zijn vastgelegd in het actieplan worden uitgevoerd, de robuustheid van het 112- en telefonienetwerk wordt bevorderd en de kans op herhaling van de telefoniestoring van 24 juni 2019 minimaliseert. KPN heeft naar aanleiding van de storingen inmiddels een aantal belangrijke passende maatregelen voor 112 en telefonie getroffen. Ook voor NL-Alert zijn maatregelen getroffen.

Op basis van deze conclusies komt naar voren dat het noodzakelijk is dat organisaties een verdere professionaliseringsslag gaan maken. Om dit te kunnen bereiken zijn per deelonderzoek aanbevelingen gedaan. AT zal in het reguliere toezicht in 2021 toezien of KPN voldoet aan de wettelijke verplichting op de genomen en nog uit te voeren passende en noodzakelijke maatregelen. AT wil periodiek over de voortgang van het actieplan en de implementatie van de aanbevelingen geïnformeerd worden.

De Nederlandsche Bank (DNB)

Tabel f. *Geselecteerde thema's DNB per beveiligingsdomein*

Risico-gebaseerde aanpak	Organisatie van netwerk- en informatiebevei-ligingsbeheer	Incidenten voorkomen	Detectie & response	Gevolgen van incidenten beperken
Operational risks	Operational risks	Operational risks	Operational risks	Operational risks

Vitale sector: Financieel

Onderwerp: Toezicht op operationele en IT risico's

Aanleiding: Cyberrisico's staan hoog op de agenda van de financiële kerninfrastructuur (FKI) en DNB. Vanuit DNB wordt toezicht gehouden op de manier waarop deze risico's door de FKI beheerst worden. Dit toezicht wordt onder meer uitgevoerd door middel van cyber gerelateerde onderzoeken. Periodiek onderhoudt DNB contact met de instellingen om voortgang van bevindingen uit onderzoeken te monitoren en om nieuwe risico's te identificeren. Tevens worden door DNB Threat Intelligence Based Ethical Red Teaming (TIBER) testen gecoördineerd.

Algemeen beeld: Binnen de financiële kerninfrastructuur staat digitale weerbaarheid en specifiek weerbaarheid tegen cyberaanvallen hoog op de agenda. Er is hierbij onder meer specifieke aandacht voor de weerbaarheid tegen DDoS aanvallen. De verbeteracties zijn in het kader van continu monitoren van DDoS dreigingen en het aanpassen van de maatregelen daarop. Dit geldt ook in bredere zin voor cyberdreigingen. Er is continu aandacht nodig voor het proces van identificeren van dreigingen, het treffen van preventieve maatregelen, het versterken van detectieve maatregelen en het voorbereid zijn op en het kunnen herstellen van cyberaanvallen. Op het gebied van patch management bestaat het beeld dat er goede stappen zijn gezet maar dat er nog ruimte is voor verdere verbetering.

In de financiële sector vindt veel uitwisseling plaats tussen instellingen over cyberdreigingen en incidenten zodat van elkaar geleerd wordt en sneller gereageerd kan worden. Informatiedeling met en door de overheid over dreigingen en incidenten is een aandachtspunt, evenals het risico op een onoverzichtelijk geheel van afspraken en overleggremia.

Voor de sector geldt dat er concentratierisico's bestaan (onder andere bij aanbieders van DDoS preventie diensten) en/of snel kan gaan ontstaan (onder andere bij aanbieders van clouddiensten). Instellingen en toezichthouders dienen hier al aandacht aan te besteden in het kader van bestaande sector wet- en regelgeving. Aandacht voor de risico's van kritieke dienstverleners zal de komende periode toenemen, mede door enkele Europese wet- en regelgevingsvoorstellen.

Inspectie Justitie en Veiligheid (IJenV)

Tabel g. *Geselecteerde thema's IJenV per beveiligingsdomein*

Risico-gebaseerde aanpak	Organisatie van netwerk- en informatiebevei-ligingsbeheer	Incidenten voorkomen	Detectie & response	Gevolgen van incidenten beperken
Risicomanagement meldkamers				

Vitale sector: OOV (openbare orde en veiligheid)

Onderwerp: Informatiebeveiliging van meldkamers: onderzoek naar het vormgeven van risicomanagement.

Aanleiding: De meldkamers voor politie, brandweer, ambulance en marechaussee zijn zo belangrijk voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting kan leiden en een bedreiging vormt voor de nationale veiligheid. De meldkamers zijn daarom onderdeel van de Nederlandse vitale infrastructuur. De meldkamers zijn knooppunten voor communicatie en informatie in nood- en crisissituaties. Voor wie in nood verkeert, is de meldkamer het eerste contact met de hulpdiensten van de brandweer, ambulance, politie en de marechaussee. Een verstoring van de meldkamerprocessen kan de uitvoeringstaken van de meldkamers ernstig in gevaar brengen. Tijdens eerder onderzoek waren er aanwijzingen dat binnen de meldkamers zeer beperkt aandacht was voor informatiebeveiliging en dat zij mogelijk onvoldoende weerbaar zijn tegen verstoring van de uitvoeringstaken door cyberincidenten.

Het beheer van de meldkamers ligt sinds 2020 bij de Nationale Politie die daarvoor een speciaal organisatieonderdeel vormde: de Landelijke meldkamersamenwerking, de LMS. Het thematisch onderzoek dat de IJenV bij de LMS heeft uitgevoerd, richt zich op het risicomanagement, als basisvoorwaarde voor informatiebeveiliging. Daarmee is cybersecurity in het vitale proces Communicatie met en tussen hulpdiensten voor het eerst in beeld gebracht.

Algemeen beeld: Het onderzoek is nog niet afgerond waardoor er geen resultaat in dit inspectiebeeld is opgenomen. De uitkomsten zullen naar verwachting medio 2021 worden gepubliceerd.

Inspectie Leefomgeving en Transport (ILT)

Tabel h. *Geselecteerde thema's ILT per beveiligingsdomein*

Risico-gebaseerde aanpak	Organisatie van netwerk- en informatiebevei-ligingsbeheer	Incidenten voorkomen	Detectie & response	Gevolgen van incidenten beperken
	1. Onderzoek drinkwaterbedrijf Stichting Waternet	1. Kwetsbaarheden en patchmanagement operational technology		

Vitale sectoren: Luchtvaart, drinkwater, maritiem

Onderwerp: Kwetsbaarheden- en patchmanagement van de operational technology

Aanleiding: Er is een verkenning naar kwetsbaarheden- en patchmanagement van de procesautomatisering uitgevoerd op basis van een self-assessment. Er is per sector naar de volgende aspecten gevraagd:

- Inbedding cybersecurity en awareness OT-security;
- Inrichting kwetsbaarhedenmanagement;
- Inrichting patchmanagement.

Algemeen beeld: De uitkomsten van de verkenning geven voor wat betreft de inrichting van het kwetsbaarheden- en patchmanagement een bemoedigend beeld. Op basis van de self-assessments is het algemene beeld dat de AED's binnen deze sectoren zich bewust zijn van het belang ervan. De resultaten vormen voor de ILT input voor de verdere inrichting van het toezicht en eventueel vervolgonderzoek.

ILT

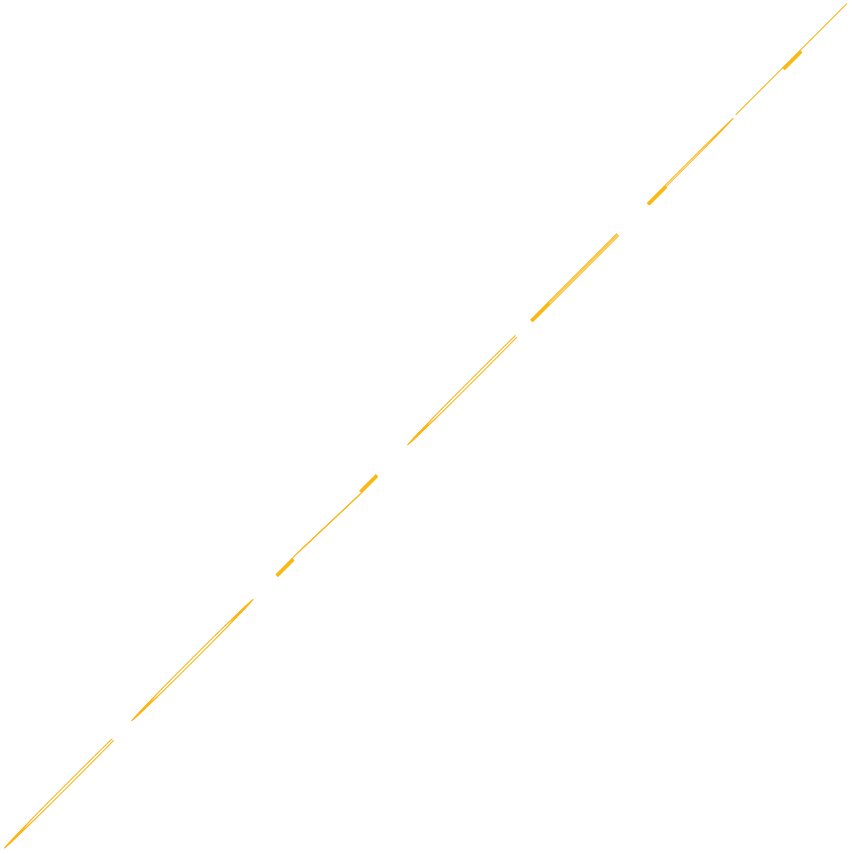
Vitale sector: Drinkwater

Onderwerp: Onderzoek naar de toestand van cybersecurity bij drinkwaterbedrijf (Stichting Waternet).[7] Het doel van dit onderzoek was vast te stellen in hoeverre er sprake was van risico's voor de waarborging van de kwaliteit en leveringszekerheid van drinkwater.

Aanleiding: De ILT houdt bij Waternet toezicht op de drinkwatervoorziening en op het deel van de cybersecurity dat betrekking heeft op de drinkwaterveiligheid en leveringszekerheid. In de media kwam in september en november 2020 het signaal naar voren dat de cybersecurity bij Waternet niet op orde zou zijn en dat de besturing bij Waternet verbeteringen ten aanzien van cybersecurity zou belemmeren. Dit signaal, in combinatie met de uitkomst van een bestuurlijk gesprek met Waternet over dit signaal, was voor de ILT reden om te besluiten tot een eigen onderzoek. Het doel van dit onderzoek was vast te stellen in hoeverre er sprake was van risico's voor de waarborging van de kwaliteit en leveringszekerheid van drinkwater.

[7] Onderzoeksrapport is te vinden op: Onderzoeksrapport Stichting Waternet | Rapport | Inspectie Leefomgeving en Transport (ILT) (ilent.nl).

Beeld/resultaat: Uit onderzoek van de ILT blijkt dat de drinkwaterorganisatie zowel op bestuurlijk als organisatorisch niveau onvoldoende grip heeft op de eigen cybersecurity. Dit wordt veroorzaakt door tekortkomingen in de uitvoering van de wettelijke zorg- en meldplicht en de besturing van de organisatie. Hierdoor is een verhoogd risico aanwezig op een cyberincident met mogelijke gevolgen voor de kwaliteit en/of de continuïteit van drinkwater. Er zijn geen aanwijzingen dat de kwaliteit en levering van het drinkwater acuut in gevaar zijn. De ILT heeft Stichting Waternet onder verscherpt toezicht geplaatst. Daarnaast zal de ILT in 2021 nader onderzoek instellen in hoeverre de andere AED's binnen het beleidsdomein van IenW voldoen aan de zorg- en meldplicht uit de Wbni.



5 Stand van zaken aanbevelingen Eerste Beeld

5.1 Aanbevelingen Eerste Beeld

Zoals in hoofdstuk 1 is aangegeven, zijn de aanbevelingen die de toezichthouders naar aanleiding van het eerste gezamenlijke Beeld toezicht cybersecurity vitale processen in maart 2020 hebben geformuleerd, aan de betrokken bewindspersonen aangeboden. In dat beeld hebben de toezichthouders aan de minister van JenV als coördinerend minister voor cybersecurity en aan de betrokken vakministers (EZK, FIN, IenW en VWS) de volgende aanbevelingen gedaan:

1. Stimuleer de betrokken toezichthouders om te komen tot een gemeenschappelijk kader voor toezicht op cybersecurity vitale processen, waarbij er ruimte blijft voor de verscheidenheid per vitaal proces en voor sectorale invulling.
2. Zorg voor een toereikende grondslag voor die toezichthouders waar dat nog niet het geval is. En daar waar nog geen toezichthouder voor een vitaal proces bekend is, zorgdragen dat hierin wordt voorzien.
3. Bezie op welke wijze er meer samenhang kan worden gerealiseerd tussen de lijst vitale processen van de NCTV, de NIB-vitale processen en de vitale processen conform de Wbni.
4. Draag er zorg voor dat de betrokken toezichthouders invulling geven aan het toezicht op cybersecurity voor de vitale processen en hiervoor ook voldoende middelen beschikbaar krijgen.

5.2 Stand van zaken aanbevelingen

Het is voor het naar de toekomst toe goed kunnen doorontwikkelen van het samenhangend inspectiebeeld van belang inzicht te hebben in welke mate de bewindspersonen gevolg hebben gegeven aan deze aanbevelingen. De toezichthouders hebben bij de betreffende departementen de stand van zaken daarover – een jaar later – opgevraagd. Hieronder is per aanbeveling de rode draad van die stand van zaken bij alle departementen weergegeven.

Aanbeveling 1: *Stimuleer de betrokken toezichthouders om te komen tot een gemeenschappelijk kader voor toezicht op cybersecurity vitale processen, waarbij er ruimte blijft voor de verscheidenheid per vitaal proces en voor sectorale invulling.*

Alle ministeries zijn eensgezind in hun opvatting dat het Besluit beveiliging netwerk en informatiesystemen (Bbni) het gemeenschappelijk kader kan vormen voor toezicht op cybersecurity bij vitale processen en aanbieders van essentiële diensten. Er is een gemeenschappelijke taal en begrippenlijst.[8] De minister van Justitie en Veiligheid heeft vanuit diens coördinerende rol invulling aan de aanbeveling gegeven door het wijzigen van het Bbni dat op 1 juni 2021 in werking is getreden. De wijziging maakt een meer uniforme invulling van het toezicht op de zorgplicht mogelijk, waarbij tegelijk ook rekening gehouden kan worden met sectorspecifieke regelgeving als maatwerk naast het Bbni.

Dit betekent dat er breed draagvlak is bij de ministeries om, rekening houdend met de grote verschillen tussen de sectoren waarop toezicht wordt gehouden, een generiek toetsingskader te gaan ontwikkelen voor het toezicht op cybersecurity bij vitale processen en aanbieders van essentiële diensten.

Aanbeveling 2: *Zorg voor een toereikende grondslag voor die toezichthouders waar dat nog niet het geval is. En daar waar nog geen toezichthouder voor een vitaal proces bekend is, zorgdragen dat hierin wordt voorzien.*

Uit de reacties van de ministeries wordt duidelijk dat de meeste van hen vinden dat voor de onder hun verantwoordelijkheid vallende vitale sectoren een toereikende wettelijke grondslag voor het toezicht op cybersecurity is. Dit geldt voor twee toezichthouders niet.

ILT heeft aangegeven dat voor een aantal sectoren nog (sector)specifieke normen, voor zover mogelijk, nodig zijn om de Wbni en Bbni uitvoerbaar en handhaafbaar te maken. De beleidskern van IenW heeft met het oog hierop een Ministeriële regeling in voorbereiding die naar verwachting per 1 juli 2021 van kracht wordt.

De sector gezondheidszorg waar de IGJ toezicht op houdt, is tot op heden niet vitaal verklaard waardoor er ook geen AED's in de zorg zijn aangewezen. VWS gaat opnieuw beoordelen welke delen van de zorg vitaal verklaard zouden moeten worden. De IGJ zal hierbij in een later stadium – zodra duidelijk wordt welke processen en/of onderdelen eventueel vitaal worden – betrokken worden. Het is dus nu nog niet duidelijk welke consequenties dat gaat hebben voor het toezicht van de IGJ en dat van anderen als bepaalde delen van de zorg vitaal worden verklaard. Een overzicht van de dekking van toezicht op cybersecurity bij vitale processen is in onderstaande tabel i opgenomen.

Tabel i. *Lijst vitale processen met overzicht van resultaten toezicht in beeld.*

Vitaal proces	sector	Toezicht	
		Toezicht-houder	**Resultaten cybersecurity in beeld**
Landelijk transport en distributie elektriciteit	Energie	AT	Ja

[8] Cybersecurity woordenboek maakt lastige terminologie begrijpelijk | Nieuwsbericht | Nationaal Cyber Security Centrum (ncsc.nl).

Regionale distributie elektriciteit	Energie	AT	Ja
Gasproductie, landelijk transport en distributie gas	Energie	AT	Ja
Regionale distributie gas	Energie	AT	Ja
Olievoorziening	Energie	AT	Ja
Internet en datadiensten	ICT/Telecom	AT	Ja
Internettoegang en dataverkeer	Digitale infra-structuur	AT	Ja
Spraakdienst en SMS	ICT/Telecom	AT	Ja
Plaats- en tijdsbepaling middels GPS		-	onbekend
Drinkwatervoorziening	Drinkwater	ILT	Deels
Keren en beheren waterkwantiteit	Water	ILT	Nee +
Vlucht- en vliegtuigafhandeling	Transport	ILT	Deels
Scheepvaartafwikkeling		ILT	Deels
Vervoer van personen en goederen over (hoofd)spoorweginfrastructuur	Transport	ILT	Nee +
Vervoer over (hoofd)wegennet	Transport	ILT	Nee +
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	Chemie	Nog onbekend ++	onbekend
Opslag, productie en verwerking nucleair materiaal	Nucleair	ANVS	Ja
Toonbankbetalingsverkeer	Financieel	DNB	Ja
Massaal giraal betalingsverkeer	Financieel	DNB	Ja
Hoogwaardig betalingsverkeer tussen banken	Financieel	DNB	Ja
Effectenverkeer	Financieel	DNB	Ja
Communicatie met en tussen hulpdiensten middels 112 en C2000	OOV	AT en IJenV	Ja
Inzet politie	OOV	IJenV	Nee
Basisregistraties personen en organisaties	Digitale overheids-processen	onbekend	Nee
Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties)		-	Nee
Elektronisch berichtenverkeer en		-	Nee

informatieverschaffing aan burgers			
Identificatie en authenticatie van burgers en bedrijven	Vertrouwens-diensten	AT	Ja
Inzet defensie	Defensie	-	Nee
Geen vitaal proces in NL			
Gezondheidszorg +++		IGJ	steekproeven

+ Voor deze sectoren zijn nog geen AED's aangewezen en is de zorgplicht uit de Wbni nog niet van toepassing. Er kunnen mogelijk wel andere kaders van toepassing zijn zoals de BIO en bijvoorbeeld voor RWS de CSIR.
++ Chemie: Omgevingsdiensten zijn toezichthouder, ILT is tweedelijns toezichthouder. Voor cybersecurity is (nog) geen toezichthouder aangewezen.
+++ De sector gezondheidszorg waar de IGJ toezicht op houdt, is wel Europees NIB-vitaal maar in het kader van de Wbni tot op heden niet vitaal verklaard en er zijn ook geen AED's in de zorg aangewezen.

Aanbeveling 3: *Bezie op welke wijze er meer samenhang kan worden gerealiseerd tussen de lijst vitale processen van de NCTV, de NIB-vitale processen en de vitale processen conform de Wbni.*

Uit de reacties van de ministeries blijkt dat er meerdere ontwikkelingen zijn die maken dat wordt tegemoet gekomen aan deze aanbeveling. De belangrijkste betreft een voorstel voor de herziening van de NIB-richtlijn van de Europese Commissie die op 16 december 2020 is gepubliceerd. Hierin worden sectoren van essentiële diensten uitgebreid en een nieuw regime toegevoegd voor sectoren die vallen onder belangrijke diensten. Daarnaast wijzigt het identificatieproces doordat alle middelgrote en grote aanbieders onder de NIB-richtlijn vallen. Hiervoor worden uniforme drempelwaarden gehanteerd. Tenslotte heeft de EC in de herziening gedetailleerde regels voor het toezicht en handhaving opgesteld, zodat een samenhangend toezichtsraamwerk wordt gecreëerd, waarbij onderscheid wordt gemaakt tussen essentiële en belangrijke diensten. Hierin worden onder andere minimum eisen voor het toezicht opgelegd en minimale/maximale sancties.

Daarnaast zullen de door de Europese Commissie voorgestelde wijziging van de NIB-richtlijn en de voorgestelde Critical Entity Resilience (CER)-richtlijn ook consequenties hebben voor de samenhang tussen de verschillende entiteiten.

Een andere belangrijke ontwikkeling die van belang is bij deze aanbeveling vloeit voort uit de Kabinetsreactie op het rapport «Voorbereiden op digitale ontwrichting» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). Hierin geeft het Kabinet aan dat er een wetswijzigingstraject wordt gestart zodat voor alle vitale aanbieders het volledige regime van de Wbni van toepassing wordt, voor zover sectorale wetgeving niet reeds dezelfde of strengere eisen stelt. Door ook andere vitale aanbieders onder het volledige regime van de Wbni te brengen, moeten zij aan de zorgplicht en daarmee aan een gemeenschappelijk basisniveau van beveiligingsdoelen voldoen.

De conclusie over de stand van zaken van deze derde aanbeveling is dat er concrete stappen worden gezet om meer samenhang tussen de verschillende soorten vitale processen te realiseren. Het tempo hiervan hangt af van zowel Europese als

nationale wetgevingstrajecten. Het zal daarom nog wel geruime tijd duren voordat dit daadwerkelijk is geëffectueerd.

Aanbeveling 4: *Draag er zorg voor dat de betrokken toezichthouders invulling geven aan het toezicht op cybersecurity voor de vitale processen en hiervoor ook voldoende middelen beschikbaar krijgen.*

De financiering van het toezicht op cybersecurity vindt niet separaat via een centrale voorziening plaats. Elke toezichthouder zal zelf – al dan niet in afstemming met het departement – de financiële en personele middelen moeten alloceren.

Het beeld over deze aanbeveling is dat enkele toezichthouders (AT en DNB) over voldoende middelen beschikken om specifiek toezicht te houden op cybersecurity bij vitale processen. Andere toezichthouders geven aan tot nu toe onvoldoende middelen beschikbaar te hebben of maken daarover nog nadere afspraken met het beleidsdepartement. Zij kunnen daarom nog niet in de volle omvang toezicht op cybersecurity bij de vitale aanbieders en processen uitvoeren.

5.3 Conclusie

De algemene conclusie is dat de betrokken departementen positief staan tegenover de in het eerste Beeld gedane aanbevelingen. Ze ondersteunen de noodzaak om, rekening houdend met sectorspecifieke verschillen, tot één generiek kader te komen. Het Bbni dat op 1 juni 2021 in werking is getreden, kan hiervoor als basis dienen. De aanbeveling om meer samenhang tussen de verschillende lijsten met vitale processen te realiseren wordt de komende jaren naar alle waarschijnlijkheid ingevuld door meerdere ontwikkelingen die al in gang zijn gezet. Dit betreft een voorstel voor de herziening van de NIB-richtlijn van de Europese Commissie. Daarnaast geeft het Kabinet in zijn reactie op het rapport «Voorbereiden op digitale ontwrichting» van de WRR aan dat door een wetswijzigingstraject er naartoe wordt gewerkt dat voor alle vitale aanbieders het volledige regime van de Wbni van toepassing wordt.

Verder concluderen de toezichthouders dat over de gehele linie bezien de aanbevelingen over een voldoende grondslag voor het toezicht op alle vitale processen en over voldoende middelen, onvoldoende opvolging hebben gekregen. Dat betekent dat het toezicht op cybersecurity bij alle vitale processen en aanbieders – in een context waarin de aanpak van cybersecurity steeds urgenter wordt – niet bij alle toezichthouders die rol en positie kan aannemen die noodzakelijk is. Als een nieuw kabinet meer prioriteit aan cybersecurity geeft zullen deze hogere ambities mogelijk ook tot extra benodigde middelen voor de uitvoering van het toezicht leiden. Daarnaast is de verwachting dat ook de nieuwe en wijzigende regelgeving vanuit de EU tot extra taken voor toezichthouders leidt.

6 Conclusies en aandachtspunten

6.1 Conclusies

Op basis van de bevindingen in dit eerste samenhangend inspectiebeeld formuleren de betrokken toezichthouders meerdere conclusies. Deze hebben enerzijds betrekking op het toezicht zelf. Anderzijds gaan deze over de beelden over de stand van de cybersecurity bij de vitale sectoren die onder toezicht staan.

Conclusies bij beelden toezicht cybersecurity (hoofdstuk 4).

1. De toezichthouders maken jaarlijks ieder hun sectorspecifieke afwegingen bij de onderwerpen van het toezicht. Dit gebeurt onder andere op basis van algemene en sectorspecifieke risico's en informatie, maar ook op basis van de aard en omvang van de sector en de beschikbare kennis en capaciteit bij de toezichthouder. Toezichthouders kunnen en zullen niet altijd elke steen omkeren en maken beredeneerde keuzes in het toezicht dat zij uitvoeren. De specifieke toezichtresultaten zijn daarom jaarlijks per sector verschillend en geven niet per definitie in een enkel jaar een rode draad om te herkennen in de volledige stand van de cybersecurity bij de vitale processen.
   Dat wil niet zeggen dat op lange termijn geen rode draad ontstaat. Het door de toezichthouders gehanteerde generieke kader, gebaseerd op bekende standaarden voor cybersecurity van bijvoorbeeld ISO en NIST, en dat ook terugkomt in het per 1 juni 2021 volledig in werking getreden Bbni, heeft een eerste houvast geboden om voor delen van de daarin benoemde vijf beveiligingsdomeinen inzicht te krijgen in de stand van zaken op cybersecurity bij de vitale sectoren. Het toezicht op cybersecurity is een jong veld; het loopt nog maar kort. De opbrengst van het toezicht is daarom nóg niet rijk genoeg om over alle thema's een diepgaande samenhangende uitspraak te doen die iets zegt over de stand van de vijf beveiligingsdomeinen in het kader. Met andere woorden: dat leidt in dit stadium nog niet tot een onderling vergelijkbare opbrengst en levert nog geen allesomvattend en compleet inzicht op. Met elke komende jaarlijkse toezichtcyclus zal dat beeld echter vollediger worden en de komende jaren verder worden ontwikkeld.

   Bovenstaande conclusie betekent niet dat er geen sprake is van relevante bevindingen of beelden die het waard zijn om te delen in dit samenhangend inspectiebeeld. Zo komt in algemene zin uit de toezichtresultaten van ANVS, AT, DNB en ILT naar voren dat over de gehele linie van bekeken vitale organisaties voldoende bewustzijn aanwezig is over het belang van digitale

weerbaarheid. Voor de sector nucleair is na een nulmeting gebleken dat het niveau van digitale weerbaarheid over de hele linie in ieder geval een basaal niveau raakt of overstijgt. De sector vertrouwensdiensten laat ook over de hele linie een volwassen beeld zien. In een enkel geval was sprake van een bijzondere casus, zoals het in 2020 door ILT gestarte onderzoek naar de toestand van de cybersecurity en besturing bij Stichting Waternet in het kader van de leveringszekerheid en kwaliteit van drinkwater, waarvan de resultaten onlangs zijn aangeboden aan de Tweede Kamer.[9]

Alle vier voornoemde toezichthouders hebben op basis van de inspecties en analyses in hun toezicht verbeterpunten en/of knelpunten gevonden bij vitale organisaties. Een belangrijke conclusie daarbij is dat de onderzochte organisaties op basis van die bevindingen verbetermaatregelen hebben getroffen. Hiermee wordt de noodzaak van deskundig en professioneel toezicht op cybersecurity benadrukt: ondanks het bewustzijn en professioneel niveau bij onder toezicht gestelde organisaties is een eveneens professionele en kritische blik van de toezichthouder van meerwaarde om potentiële risico's of dreigingen bij die vitale sectoren te signaleren en hen te wijzen op het nemen van passende maatregelen.

Zowel DNB als ILT heeft specifiek aandacht geschonken aan kwetsbaarheden- en patchmanagement en kwamen tot het beeld dat het met het bewustzijn op dat punt goed gesteld was, plus dat er ruimte is voor verbetering.
Een ander onderwerp dat naar voor kwam bij toezichthouders AT en DNB, betrof digitale 'concentratierisico's' in de toeleverantieketen (Supply Chain) van vitale organisaties. Onder meer ten aanzien van Clouddienstverlening. Beide toezichthouders hebben ervoor gekozen om in 2020 en 2021 extra aandacht aan dit onderwerp te besteden.

Twee andere observaties die in de besprekingen van de beelden tussen toezichthouders naar voren kwamen, betroffen het belang van adequaat business continuity management en de opkomst van nieuwe technologie. Ten aanzien van het eerste punt onderstrepen de toezichthouders dat continuïteit en robuustheid van netwerk- en informatiesystemen belangrijk is. Dit wordt niet alleen bereikt met preventieve maatregelen, maar ook met maatregelen voor crisis en herstel. Ten aanzien van het tweede punt betreft de observatie dat nieuwe technologieën, zoals Artificial Intelligence (AI), een grote druk leggen op de normatieve kennis en kunde van toezichthouders bij de beoordeling van nieuwe bijzondere toepassingen in de staande praktijk.

Conclusies bij inrichting toezicht cybersecurity (hoofdstuk 5)

2. Uit de lijst met vitale processen (zie tabel i in hoofdstuk 5) wordt duidelijk dat voor de meeste van de in Nederland vitaal verklaarde processen en sectoren een toezichthouder aangewezen is, maar nog geen volledig dekkend toezicht op cybersecurity bij alle vitale processen in Nederland is geregeld. Bij de meeste van die vitale sectoren is in 2020 toezicht op cybersecurity uitgevoerd. Zoals geschetst onder conclusie 1, verschilt de breedte en diepgang van het toezicht per sector. Enkele processen of sectoren kennen geen aangewezen toezichthoudende instantie. Dit betreft plaats- en tijdsbepaling middels GPS, chemie, digitale overheidsprocessen en inzet defensie. Daarnaast zijn enkele processen voor wat betreft cybersecurity nog niet in scope van bestaand

[9] Onderzoeksrapport Stichting Waternet | Rapport | Inspectie Leefomgeving en Transport (ILT) (ilent.nl).

toezicht: dit geldt voor keren en beheren waterkwantiteit, enkele processen van de sector transport en het proces inzet politie. Daarnaast zijn nog niet van elke sector alle processen in het toezicht meegenomen. Ook het aanwijzen van AED's in bepaalde sectoren dat nog moet plaatsvinden, maakt dat het toezicht zich in een groeifase bevindt. Desondanks laat dit eerste samenhangend inspectiebeeld met hoofdstuk 4 en de conclusies onder 1 en 2 zien dat de toezichthouders hun inspecties in de meeste gevallen weten te richten op de stand van cybersecurity bij vitale processen. Daarmee begint het toezicht op cybersecurity bij vitale processen steeds meer een onderdeel van hun bredere toezichtprogramma te worden.

3. Er zijn meerdere ontwikkelingen die maken dat het toezicht op vitale processen door toezichthouders waarschijnlijk toeneemt. Vitale sectoren in Nederland kennen verschillende grondslagen voor toezicht op cybersecurity. Inmiddels is op Europees niveau een voorstel gedaan voor de vervanging van de oorspronkelijke NIB-richtlijn door een nieuwe richtlijn. Het ziet ernaar uit dat het aantal vitale sectoren daardoor gaat toenemen. Daarnaast wordt in Nederland overwogen de Wbni te wijzigen; daar is nog niet mee begonnen. Hierdoor komen in principe alle vitale processen (voor wat betreft de daaronder vallende netwerk- en informatiesystemen) onder het volledige Wbni-regime te vallen. Zij dienen zo ook aan de zorgplicht en meldplicht te voldoen, voor zover sectorale wetgeving niet reeds dezelfde of strengere eisen stelt. De verschillen in kaders tussen de aanbieders blijven bestaan totdat de Wbni is gewijzigd. Daarnaast zullen ook geluiden uit de samenleving om bepaalde processen of hele infrastructuren vitaal te verklaren leiden tot een grotere toezichtdruk op de toezichthouders. Ontwikkelingen rond de zorg en de voedselvoorziening zullen waarschijnlijk gevolgen hebben voor de vitale processen.

4. Uit de resultaten wordt duidelijk dat het toezicht op cybersecurity bij enkele toezichthouders nog in een opbouwende fase is en bij een aantal andere toezichthouders integraal deel uitmaakt van het totale toezicht bij vitale sectoren. Voorbeelden van die laatste groep zijn ANVS, AT en DNB. Daarom kunnen voor de sectoren nucleair, financieel, energie, ICT/Telecom, digitale infrastructuur en elektronische vertrouwensdiensten op basis van de toezichtresultaten uitspraken worden gedaan over de stand van cybersecurity.

   Andere toezichthouders zoals IJenV en ILT zijn in opbouw en met name ILT heeft het afgelopen jaar een flinke inhaalslag gemaakt, met het onderzoek bij de Stichting Waternet als beeldend resultaat. De opbouw betekent met name dat deze toezichthouders op dit moment naast de uitvoering van toezicht, een substantieel deel van hun tijd moeten besteden aan de ontwikkeling van het toezicht op cybersecurity bij hun vitale sectoren en processen en de deskundigheid en kennis daarvoor moeten aantrekken of ontwikkelen.

   IGJ heeft aandacht voor het onderwerp cybersecurity, maar vanuit haar taakuitvoering op dit moment geen vitale organisaties onder toezicht. Een wijziging van de NIB-richtlijn heeft hier mogelijk impact op.

5. Goed toezicht kost tijd en middelen. Zoals reeds naar voren kwam in conclusie 1, worden jaarlijks keuzes gemaakt op basis van verschillende variabelen, waaronder aard en omvang van de sector en beschikbare toezichtcapaciteit. Voor enkele toezichthouders geldt dat de beschikbare kennis en capaciteit op dit moment nog beperkt is. Dat brengt met zich mee dat zij keuzes moeten

maken in hun jaarlijkse programmering die niet altijd in de pas lopen met bestuurlijke of maatschappelijke verwachtingen. In conclusie 3 kwam naar voren dat een wijziging van de NIB-richtlijn mogelijk een substantiële impact zal hebben op het aantal en de omvang van de sectoren en het toezicht daarop. Extra financiële middelen zijn in dat geval noodzakelijk. Tevens neemt de aard van dreigingen en digitale risico's toe, zoals blijkt uit diverse rapportages. Als de prioritering in beleid ten aanzien van digitalisering en cybersecurity in de komende kabinetsperiode toeneemt, zal dat, gezien de voorgaande conclusies een opdrijvend effect hebben op de verwachtingen richting toezichthouders. De recente motie over de uitbreiding van de toezichtcapaciteit van AP en het CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' laten zien dat 'boots on the ground' en voldoende middelen onmisbaar zijn.

6.2 Aandachtspunten

De betrokken toezichthouders signaleren een aantal aandachtspunten voor de onder toezicht staande organisaties, voor de beleidsverantwoordelijke ministeries en voor zichzelf. Deze aandachtspunten hebben tot doel om de digitale weerbaarheid van vitale processen en aanbieders te verhogen, het bewustzijn voor cybersecurity te vergroten en de professionaliteit en kwaliteit van het toezicht in de breedte te verbeteren.

1. Aandacht én inhoud

Afgaand op de bevindingen over 2020 kan worden gezegd dat sprake is van bewustzijn op cybersecurity bij een aanzienlijk deel van de vitale organisaties. Dat is geenszins een reden om achterover te leunen. Toezicht gaat namelijk veel meer om het bevorderen van het gewenste gedrag, dan om het vinden van de misstap. Alle toezichthouders onderschrijven daarom bij dit beeld de noodzaak van voortdurende aandacht voor dit onderwerp, zowel bij de betreffende vitale organisaties als bij beleidsdepartementen en toezichthouders zelf. Cybersecurity is geen onderwerp van de IT afdeling alleen, maar juist van de business en verdient daarom voortdurende aandacht en verbetering.

De toenemende inzet en afhankelijkheid ten aanzien van digitale dienstverlening, waaronder Clouddiensten wordt door alle toezichthouders gesignaleerd. Een adequaat inzicht en beheersing van supply chain risks zien zij als prioriteit. Vanuit de omliggende ketens ontstaan diverse risico's, bijvoorbeeld door ongewenste concentratie van diensten, afhankelijkheid, continuïteitsrisico's en risico's op het gebied van veiligheid en integriteit. Dit onderwerp zal in 2021 en verder een belangrijk thema in cybersecurity blijven en ook de aandacht van diverse toezichthouders hebben. In het licht van toenemende digitale afhankelijkheden in toeleverantie en ketens wijzen de toezichthouders tevens op het belang van adequaat business continuity management.

Tot slot vragen de toezichthouders aandacht voor de impact van nieuwe technologieën. In de uitvoering van de toezichtpraktijk worden zij vaak in een vroeg stadium geconfronteerd met de inzet van bijzondere nieuwe oplossingen, bijvoorbeeld AI.

2. Meer samenhang in het beeld

Het proces om te komen tot een samenhangend inspectiebeeld 2020 heeft de aan dit beeld werkende toezichthouders geleerd dat zij de komende jaren meer aandacht willen geven aan het definiëren van generieke thema's en de wijze waarop invulling wordt gegeven aan het benutten van het generieke kader onder het Bbni. Het speelveld is jong, daarom is samenwerking tussen de toezichthouders belangrijk en daar waar mogelijk van elkaar te leren. Sectorale verschillen in de toezichtprogramma's zullen echter altijd bestaan en noodzakelijk zijn vanwege de verschillende risico's per sector en soms zelfs per vitale organisatie. Dit aandachtspunt wordt verder uitgediept in het volgende hoofdstuk.

3. Ontwikkeling toezicht cybersecurity vitale processen

In conclusie 3 kwam naar voren dat niet bij alle vitale sectoren is voorzien in een specifiek aangewezen toezichthouder, maar dat cybersecurity in een groot deel van de sectoren wel steeds meer aandacht krijgt in het toezicht. Het zou goed zijn als toezichthouders hun processen en werkwijze op elkaar laten aansluiten. Voordelen daarvan zijn dat kennis en mensen beter en efficiënter kunnen worden uitgewisseld, dat resultaten sector overstijgend beter vergelijkbaar worden en er eenduidige sectorbeelden met rode draden gemaakt kunnen worden en de rode draad eruit lichten en er meer vergelijkbare niveaus kunnen worden gecreëerd tussen de toezichthouders onderling.

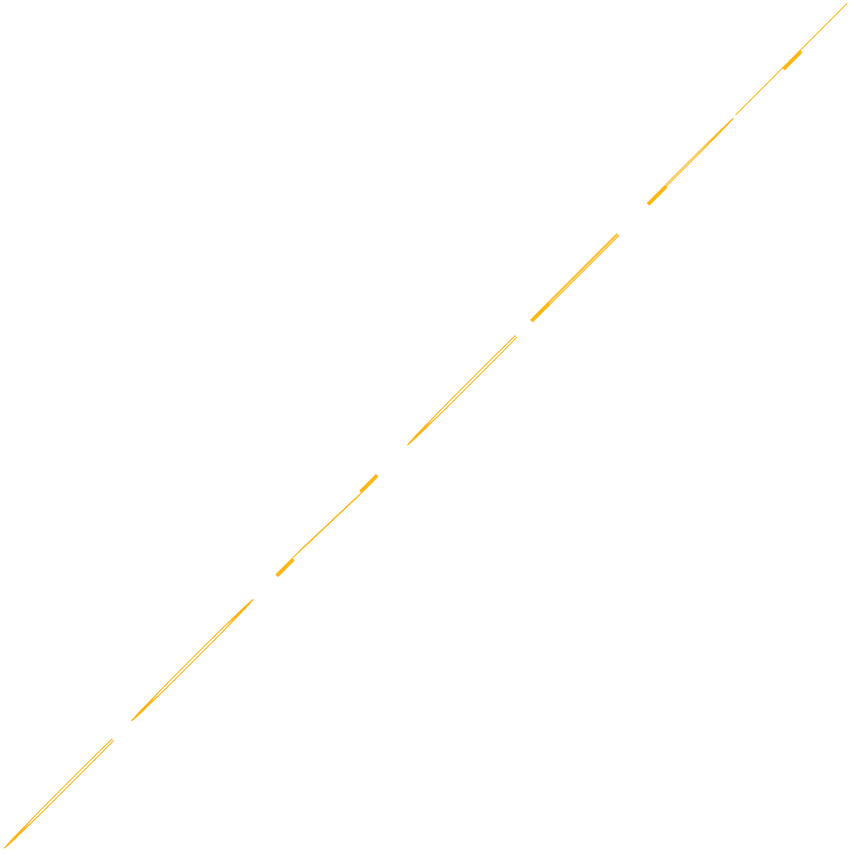
In conclusie 4 kwam naar voren dat aankomende wet- en regelgeving op nationaal en Europees niveau hier de komende jaren mogelijk impact op heeft. Het is hierbij van belang dat Europese en nationale wetgeving aansluitend op elkaar is. De toezichthouders vragen daarbij aandacht voor het goed op elkaar aansluiten van de diverse wetgevingsinitiatieven. Zo is in de huidige wijzigingsvoorstellen voor de NIB-richtlijn, de CER-richtlijn en (voor de financiële sector) de DORA verordening nog steeds sprake van verschil in definities en scope. Hier zullen toezichthouders en beleids-/wetgevers gezamenlijk op kunnen trekken in de commentaar en onderhandelingsrondes. Uitvoerbaarheid, handhaafbaarheid en aansluiting bij bestaande, al dan niet sectorale, toezichtspraktijken zijn daarbij onderwerpen van aandacht. Besluiten in Brussel die leiden tot een toename van bijv. AED's in vitale sectoren vragen ook om een uitbreiding van passende middelen.

Verstoring van vitale processen kunnen grensoverschrijdende gevolgen hebben en vitale aanbieders kunnen in meerdere lidstaten actief zijn. Het is daarom van belang dat toezichthouders op cybersecurity in verschillende Europese lidstaten meer structureel gaan samenwerken. Mede met het oog op de Europese wetgevingsinitiatieven is ook het meer structureel samenwerken tussen toezichthouders in verschillende Europese lidstaten een aandachtspunt.

4. Professionaliseer het toezicht op cybersecurity verder

De betrokken toezichthouders hebben allen geleerd dat cybersecurity een thema is dat je er niet zomaar bij pakt in je bestaande toezichtprogrammering. Het vraagt kennis en expertise die nog niet standaard bij alle toezichthouders aanwezig is en het delen van kennis en producten zodat nieuwkomers sneller een gelijkwaardige partner kunnen zijn met de voorlopers. Dat is een belangrijke constatering in het licht van het toenemend belang van digitale dreigingen en verstoringen en de noodzakelijke digitale weerbaarheid. Toezichthoudende professionals bestaan, ook IT professionals bestaan. Maar een 'hybride' variant, de cybersecurity toezichthouder, is zeldzaam.

De toezichthouders vragen daarom aandacht voor voldoende voorwaarden en middelen om aan een voorziene toename in de vraag naar toezicht op digitale processen te voldoen. Dit betreft niet enkel geld, maar ook de beschikbaarheid van goed personeel. Het Rijk, maar ook opleidingsinstituten, zouden in hun opleidingstrajecten en traineeships aandacht kunnen geven aan de benodigde skills voor inspecteurs en auditors. Ook kan nadere samenwerking met onderwijsinstellingen hieraan bijdragen. Op deze manier kan de komende jaren een kweekvijver van potentiële professionals worden gevormd. Ook zal werk maken van digitale geletterdheid[10] uiteindelijk voor een grotere vijver van inhoudelijk goede toezichthouders zorgen. Deze aanpassing van het curriculum zal het onderwijs in Nederland van basis tot voortgezet 'digitaler' maken.



[10] https://www.slo.nl/vakportalen/vakportaal-digitale-geletterdheid/

7 Doorontwikkeling samenhangend inspectiebeeld

Dit beeld is een belangrijke stap in de doorontwikkeling naar een volwaardig en samenhangend inspectiebeeld van de cybersecurity bij vitale processen. De betrokken toezichthouders hebben de ambitie om dit proces de komende jaren gezamenlijk verder op te pakken. Het inspectiebeeld zal inzicht bieden in de mate waarin vitale aanbieders werken aan een hoog niveau van digitale weerbaarheid en continuïteit. Het zal de resultaten van het toezicht op cybersecurity beschrijven en daarmee een beeld geven van de staat van de cybersecurity van de vitale processen en de vitale aanbieders. Door hierover op een eenduidige wijze te rapporteren kan de weerbaarheid van de verschillende vitale processen met elkaar worden vergeleken en kan er waar nodig door de verantwoordelijke bewindspersonen worden geïntervenieerd.

Die doorontwikkeling zal stapsgewijs tot stand komen. Hierbij worden, gevolg gevend aan de aandachtspunten in paragraaf 6.2, twee lijnen opgepakt:

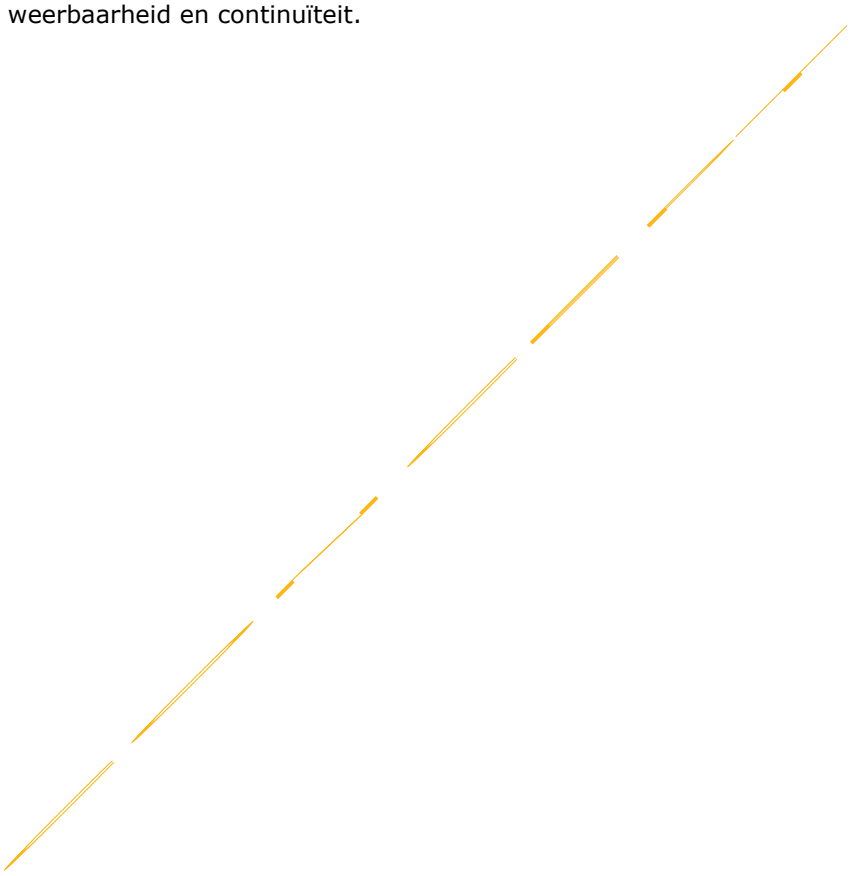
1. Een beeld op basis van een gemeenschappelijk basiskader. Dat basiskader zal een aantal gedeelde indicatoren bevatten die door alle toezichthouders kunnen worden ingezet bij hun toezicht. Op termijn kunnen hieraan volwassenheidsniveaus worden toegevoegd waardoor ontwikkelingen bij vitale aanbieders en sectoren zelf kunnen worden geduid en ook onderling kunnen worden vergeleken.
2. Het uitvoeren van toezicht op een gezamenlijk geselecteerd aandachtsgebied of thema. Dit leidt ertoe dat elk van de betrokken toezichthouders dat onderwerp in hun toezicht betrekt, een en ander voor zover specifieke of sectorale regelgeving hiervoor ruimte biedt. Ook willen de toezichthouders onderzoeken in hoeverre een thema gecoördineerd kan worden opgepakt door één multidisciplinair team dat wordt samengesteld uit inspecteurs van de verschillende toezichthouders. Dit vraagt om gecoördineerd voorbereiden op de algemene aanpak en gewenste opbrengst, waarbij voldoende ruimte bestaat voor de toezichthouders om daarin hun eigen aanpak op de uitvoering te hanteren. Daarbij is het tevens belangrijk om te kijken naar het lexicon in het toezicht, het hanteren van dezelfde begrippen en definities om te voorkomen dat de resultaten in de uitvoering alsnog uiteen lopen.

Voor de doorontwikkeling is het van belang dat bij de toezichthouders geïnvesteerd wordt in gezamenlijke kennis en technieken van het toezicht. Hierbij wordt in ieder geval gedacht aan de ontwikkeling van een centrale kennisbank/platform voor toezichthouders, het gezamenlijk opzetten van methoden, technieken, hulpmiddelen

en – waar nodig – voorschriften en het uitwisselen van toezichtmethodologie en -strategie.

In dit inspectiebeeld ligt de focus op het toezicht op de zorgplicht. In het volgende inspectiebeeld zal ook aandacht worden besteed aan het toezicht op de meldplicht op grond van de Wbni.

De uitkomsten van het samenhangend inspectiebeeld kunnen tevens als input dienen voor het Cybersecuritybeeld Nederland (CSBN) dat jaarlijks door de NCTV wordt vastgesteld. Het CSBN biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en risico's. De focus ligt daarbij op de nationale veiligheid. Daarmee geven de toezichthouders een krachtige impuls aan vitale aanbieders om blijvend te werken aan een hoog niveau van digitale weerbaarheid en continuïteit.



I

Het hoe en wat van het toezicht op cybersecurity bij vitale processen

In hoofdstuk 3 is op hoofdlijnen ingegaan op de achtergrond en context van het toezicht op cybersecurity bij de vitale processen door de betrokken toezichthouders. In deze bijlage wordt hier nader en gedetailleerd inzicht in gegeven.

Per toezichthouder wordt in deze bijlage aan de hand van doelstelling, wijze van toezicht en oordeelsvorming, de achtergrond geschetst. Vervolgens wordt per toezichthouder beschreven in welke context de toezichthouder zich bevindt, zoals het normenkader, toetsingskader en volwassenheidsniveaus. Tenslotte sluit het hoofdstuk af met een vooruitblik en wordt per toezichthouder ingegaan op een meerjarenperspectief.

Achtergrond: doelstelling, wijze van toezicht en oordeelsvorming.
Dit onderwerp valt uiteen in de visie op cybersecurity van de Toezichthouder, het doel van het toezicht en hoe de toezichthouder zich een oordeel vormt over de stand van zaken van de cybersecurity van de onder toezicht gestelde vitale organisatie(s) of vitale processen.

De Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS) houdt toezicht op de vergunninghouders die beveiligingsmaatregelen treffen die vanuit realistisch oogpunt en proportioneel gezien nodig zijn tegen bedreigingen. Voor de ANVS is het doel het tegemoetkomen aan de Ministeriële regeling beveiliging nucleaire inrichtingen en splijtstoffen en het continu verbeteren door de vergunninghouder. De ANVS streeft ernaar dat de integrale beveiliging van nucleaire organisaties in lijn is met de Nederlandse wet- en regelgeving, en met de internationale verplichtingen. De ANVS streeft ernaar om, op basis van deze wet- en regelgeving, een volwaardig, realistisch, risicogestuurd en proportioneel beveiligingsbeleid bij de nucleaire vergunninghouders te realiseren. De omvang en diepte van dit beveiligingsbeleid is gekoppeld aan het huidige en verwachte referentiedreiging die door de ANVS aan de sector Nucleair beschikbaar wordt gesteld.

ANVS vormt zich een oordeel door gebruik te maken van de volgende toezichtvormen: schriftelijke vragen, op locatie inspecteren, data-analyse, interviews, beoordeling van self-assessments, pentesten, red-teaming.

Het Agentschap Telecom (AT) hanteert een dynamische benadering voor het toezicht. Het systeemtoezicht is gebaseerd op open normen. AT werkt samen met partners in de gehele keten. Er is een gezamenlijke rol om (het vertrouwen in) het systeem werkend te houden. AT heeft daarmee een aanvullende rol in het

versterken van het vertrouwen in de digitale vitale systemen waarop het toezicht houdt.

Voor AT is het doel het beschermen van de publieke belangen en het zo klein mogelijk maken en houden van de maatschappelijke risico's. Binnen het toezicht op basis van de Wbni, Telecommunicatiewet en de eIDAS-verordening is het toezicht gericht op een voortdurend verbeteren van de sectoren en het leren van incidenten. Toezicht is meer dan handhaven.

AT maakt periodiek een analyse van relevante trends en ontwikkelingen, met oog voor maatschappelijke, politieke, technische en juridische ontwikkelingen. Daarbij wordt gebruik gemaakt van schriftelijke vragen, op locatie inspecteren, data-analyse, interviews, beoordeling self-assessments en door externe auditors uitgevoerde auditverslagen en het analyseren en onderzoeken van incidentmeldingen, monitoring en analyse van openbare bronnen, bezoeken van symposia/congressen, (laten) uitvoeren van onderzoeken en het uitvoeren van reality checks. Voor de sectoren Energie en Digitale Infrastructuur en openbare elektronische communicatienetwerken en –diensten wordt tevens (in de nabije toekomst) gebruik gemaakt van de resultaten van pentesten en red-teaming. Ten aanzien van vertrouwensdiensten worden de resultaten van pentesten bijvoorbeeld verkregen als onderdeel van informatie-uitwisseling met convenantpartners.

De Nederlandse Bank (DNB) heeft structureel aandacht voor en inzicht in de beheersing van informatiebeveiliging in de sector. De resultaten van het toezicht dragen bij aan het vergroten van kennis en het weerbaarder maken van de systemen.

DNB draagt er zorg voor dat de instellingen hun verantwoordelijkheid nemen en zorgen voor een goede werking van de vitale financiële processen. Instellingen en hun (kritieke) dienstverleners moeten kunnen aantonen dat zij hun informatiebeveiliging op orde hebben.

DNB toezicht vormt zich een oordeel over cybersecurity door middel van het stellen van schriftelijke vragen, het uitvoeren van gerichte inspecties, data-analyse, het houden van interviews en de beoordeling van self-assessments (jaarlijkse uitvraag als onderdeel van het IT Supervisory Review and Evaluation Process (SREP). Daarnaast worden resultaten van pentesten en red-teaming benut.

De Inspectie Gezondheidszorg en Jeugd (IGJ) beschouwt goede informatiebeveiliging als een voorwaarde voor continuïteit van zorg.

Het toezicht van IGJ is gericht op het continu verbeteren van de processen binnen de gezondheidszorg en jeugdzorg.

IGJ gaat ervan uit dat het de verantwoordelijkheid van de zorgaanbieders is om een managementsysteem voor informatiebeveiliging in te richten op grond van NEN7510. De IGJ controleert hierop actief via steekproeven, waarbij schriftelijke vragen worden gesteld, op locatie wordt geïnspecteerd en auditresultaten van de betrokken aanbieders worden beoordeeld.

De Inspectie Justitie en Veiligheid (IJenV) streeft ernaar dat door het signaleren van risico's organisaties worden aangezet tot verbetering. De IJenV richt zich op het gebied van cybersecurity (weerbaarheid) op zowel vitale als niet-vitale processen bij al haar toezicht ondervindende organisaties.

Met betrekking tot vitale processen is de IJenV geen toezichthouder in de zin van de Wbni/Bbni. Wel houdt de IJenV toezicht op de vitaal verklaarde processen 'communicatie met en tussen hulpdiensten middels 112 en C2000' en 'inzet politie' binnen de sector OOV. Deze processen zijn wel vitaal maar niet opgenomen in de Europese NIB-richtlijn en ook niet in de Wbni waardoor er voor deze processen geen AED's en andere vitale aanbieders zijn aangewezen. Deze vitale processen vallen onder de verantwoordelijkheid van het ministerie van Justitie en Veiligheid. De IJenV sluit zoveel mogelijk aan bij de risico gebaseerde aanpak en werkwijze van de toezichthouders die wel toezicht houden in het kader van de Wbni/Bbni.

Hoofddoel van het toezicht door de JenV is om bij te dragen aan een rechtvaardige en veilige samenleving. Dit doet de Inspectie door toezicht te houden op uitvoeringsorganisaties op het terrein van Justitie en Veiligheid. Het toezicht op cybersecurity bij deze uitvoeringsorganisaties is in ontwikkeling. In het meerjarenplan van de IJenV is het toezicht op cybersecurity en de aanpak cybercriminaliteit definitief verankerd. De grootste dreiging van cybersecurity vormt de cybercriminaliteit. Voor de vitale processen vormen de in uitvoering zijnde en geplande onderzoeken met betrekking tot risicomanagement de eerste stappen naar een integraal toezicht op cyber.

De IJenV voert het toezicht op cyber uit langs de volgende drie lijnen:

1. Toezicht op weerbaarbaarheid van de JenV-organisatie tegen cyberdreigingen in relatie tot continuïteit taakuitvoering;
2. Toezicht bij JenV-organisatie die taken hebben op het gebied van cybersecurity en cybercrime;
3. Versterking regie kabinetsbrede aanpak cyberdreigingen: de coördinerende rol van de Inspectie ten aanzien van toezicht bij digitale vitale processen.

De Inspectie leefomgeving en Transport (ILT) streeft middels het toezicht naar een hoog gemeenschappelijk niveau van beveiliging van netwerk en informatiesystemen. De ILT vormt zich nog geen oordeel over de stand van zaken van de cybersecurity van de onder toezicht gestelde vitale organisatie(s) of vitale processen.

Het toezicht op cybersecurity is voor de ILT een nieuwe toezichttaak. Het jaar 2020 stond met name in het teken van informatie verzamelen en een beeld vormen van het speelveld. Ook is het jaar gebruikt om samenwerkingsverbanden met andere toezichthouders op te starten. In het voorjaar 2021 wordt een toezichtvisie cybersecurity afgerond.

Het in kaart brengen van het speelveld en daarmee een beeld vormen is voor de ILT in 2020 een continu proces geweest. De ILT is gestart met het toezicht van de sector drinkwatervoorziening. Ook heeft een verkenning op patchmanagement onder Aanbieders van Essentiele Diensten plaatsgevonden.

Het inrichten van het toezicht is dan ook nog volop in ontwikkeling.

Context: normenkader, volwassenheidsniveaus en toetsingskader

Normenkaders

De normenkaders die worden gehanteerd door de toezichthouders zijn sectorspecifiek. Hieronder vindt per toezichthouder een opsomming van de specifieke normenkaders die zij gebruiken. Deze opsomming is niet uitputtend maar geeft een beeld van de normen die worden gehanteerd.

ANVS: De eisen voor de nucleaire vergunninghouders zijn gebaseerd op onder meer ISO27001/ISO27002/IEC62443, alsmede internationale aanbevelingen vanuit het internationaal Atoomenergieagentschap (IAEA).

AT: Agentschap Telecom houdt voor de hier beschreven vitale processen toezicht op basis van een open norm. Open normering is dynamisch, zorgt er voor dat gericht kan worden op de actuele risico's en biedt maatwerk en flexibiliteit. De invulling van de open norm kan meebewegen met de stand van zaken bij partijen in een sector. AT hanteert een 'Principle Based' normenkader op basis van ISO27K. Middels een vertaaltabel is er een aansluiting met het ENISA normenkader gemaakt.

Wbni sectoren Energie en Digitale Infrastructuur

De wet schrijft geen normenkader voor. Dit doet recht aan de vele verschijningsvormen van kaders in verschillende sectoren en de ontwikkelingen hierin. AT heeft onder meer gebruik gemaakt van de publicaties van ENISA (Europees Agentschap voor netwerk- en informatiebeveiliging) om de onderwerpen te bepalen die in het eerste jaar Wbni-toezicht behandeld worden.

In de NIB-richtlijn is aangegeven dat ENISA de lidstaten en de Commissie met deskundigheid en advies moet bijstaan en de uitwisseling van 'best practices' moet faciliteren.

Openbare elektronische communicatienetwerken en -diensten

De wet schrijft geen normenkader voor. Recent is het Besluit veiligheid en integriteit telecommunicatie gepubliceerd; hierin is ook de aankondiging van een regeling gedaan die voor specifieke onderdelen eisen en verplichtingen voorschrijft.
AT maakt onder meer gebruik van de publicatie van ENISA technical Guideline On Security Measures, om de onderwerpen te bepalen die tijdens de inventarisatie behandeld worden.

Vertrouwensdiensten

De vertrouwensdienstverlener dient met certificering aan te tonen dat zijn dienstverlening conform internationaal erkende normen en standaarden plaatsvindt. N.B. Indien aangetoond wordt dat voldaan is aan de toepasselijke standaarden van ETSI (het Europees Telecommunicatie en Standaardisatie Instituut) dan is vermoedelijk ook voldaan aan de eisen van de eIDAS verordening.

DNB: Uitgangspunt zijn de normenkaders zoals deze door internationale verbanden waarvan DNB uitmaakt, zijn vastgesteld. Dit zijn onder meer: de Bank for International Settlements (BIS), de European Banking Authority (EBA), de European Central Bank (ECB) en de International Organization of Securities Commissions (IOSCO). Voorbeelden hiervan zijn:

- Guidelines on ICT and security risk management (EBA);
- EBA guidelines on outsourcing arrangements (EBA);
- Guidance on cyber resilience for financial market infrastructures (CPMI/IOSCO);

- Cyber resilience oversight expectations (ECB).

Voor onderzoeken binnen deze kaders wordt gebruik gemaakt van de algemene normenkaders zoals NIST (Framework for Improving Critical Infrastructure Cybersecurity), ISO27xxx serie, ITIL, COBIT en het SSM Handboek voor het toezicht op banken. Een voorbeeld van de uitwerking is de DNB Good Practice Informatiebeveiliging (IB) en het Tiber-programma.[11]

IGJ: binnen de sector Zorg is de NEN 7510 de specifieke norm voor informatiebeveiliging en wordt de ISO 27001 gehanteerd als de algemene norm voor informatiebeveiliging.

ILT: Voor de ILT geldt dat binnen de verschillende sectoren daar waar mogelijk sectorale normenkaders worden gehanteerd, dit zijn:

- Voor de sector drinkwatervoorziening: de beveiligingsnorm Procesautomatisering en Rapportagesjabloon (13 februari 2019) met daarin verwijzingen naar de normenkaders ISO/IEC 27001:2017, NIST SP 800-82:2015, NIST SP 800-53:2013, ISA/IEC62443- 3-3:2013.
- Voor de vlucht- en vliegtuigafhandeling: KLM, Schiphol, LVNL, MUAC: NPA 2019-07, met daarin opgenomen EASA RMT.0720 Cybersecurity risks, (EU) IR 202x/xxx on the introduction of requirements for the management of information security risks by organisations involved in civil aviation activity, (EU) IR 2017/373 ATM/ANS.OR.D.010 (per 2/1/2020). EU 202x/xxx zal verwijzingen bevatten naar ISO/IEC 27001:2017, NIST SP 800-53:2013.
- Aanvullend voor Schiphol: IR 139/2014 is beperkt tot Management of aeronautical data and aeronautical information, ISO/IEC 17799:2005, Information technology, Security techniques, Code of practice for information security management; ISO 28000:2007: Specification for security management systems for the supply chain.
- Voor het toezicht op de Koninklijke Marechaussee (KMAR) en Aircraft Fuel Supply (AFS) is nog geen normenkader.
- Voor de scheepvaartafwikkeling werd door de divisie Havenmeester van Havenbedrijf Rotterdam de Baseline Informatiebeveiliging Rijk 2017 en vanaf 1 januari 2019 de opvolger Baseline Informatiebeveiliging Overheid gebruikt.

Daar waar nog geen normenkader wordt gehanteerd, zal de Ministeriële regeling Bbni handvatten bieden. De MR is in 2021 aan de ILT voorgelegd voor een toets op de handhaafbaarheid, uitvoerbaarheid en fraudebestendigheid (de zgn HUF-toets).

Volwassenheidsniveaus
Een aantal van de betrokken toezichthouders hanteren geen volwassenheidsniveaus bij de normenkaders. De ANVS, AT en DNB doen dat wel.

In 2020 is door onderzoek van de ANVS het cybervolwassenheidsniveau per nucleaire organisatie beschikbaar gekomen. In de nabije toekomst zal een gedifferentieerd volwassenheidsniveau per nucleaire organisatie (wellicht ook nader gedifferentieerd naar cybersysteem) worden bepaald. Dit gedifferentieerde volwassenheidsniveau is afhankelijk van het risicoprofiel van de desbetreffende nucleaire organisatie.

[11] https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdfhttps://www.dnb.nl/media/1mdf3lmq/tiber-nl-guide.pdf

AT onderscheidt voor de Wbni sectoren Energie en Digitale infrastructuur vijf volwassenheidsniveaus. Dit geeft vooral een kwalitatief beeld van de mate van beheersing van securityrisico's.

In de DNB Good practice Informatiebeveiliging (IB) wordt gewerkt met de Cobit volwassenheidsniveaus. Ook de Cyber resilience oversight expectations (CROE) van de ECB hanteert volwassenheidsniveaus. Cyber is een structureel onderdeel van het toezicht.

Toetsingskader
ANVS heeft een specifiek toetsingskader voor het toezicht cybersecurity vitale processen opgesteld: een vertaling in concrete maatregelen van de MR beveiliging nucleaire inrichtingen alsmede het DBT Cyber Security (2018).

Ten aanzien van openbare elektronische communicatienetwerken en –diensten hanteert AT geen standaard kader. Voor het uitvoeren van een inspectie of een onderzoek wordt de scope bepaald en daarvoor een kader opgesteld.

Voor vertrouwensdiensten heeft AT zijn toetsingskader gebaseerd op relevante internationaal erkende normen en standaarden (zoals van ETSI, CEN en ISO).

AT hanteert een variabele toolbox met verschillende normenkaders als toetsingskader voor haar toezicht op cybersecurity van de sectoren Energie en Digitale Infrastructuur.

DNB heeft geen afzonderlijk toetsingskader voor toezicht op cybersecurity van vitale processen opgesteld. Hiervoor worden de normenkaders als toetsingskader gehanteerd.

IGJ heeft geen toetsingskader voor informatiebeveiliging opgesteld. De IGJ heeft wel een toetsingskader E-health dat zich in bredere zin richt op toepassing van ICT in de zorg. Informatiebeveiliging is hiervan een vast onderdeel.

IJenV werkt aan de ontwikkeling van een zogenaamd generiek toetsingskader voor toezicht op de digitale vitale aanbieders en processen. Ze zal hierbij zoveel mogelijk aansluiten bij het Bbni-model.

ILT heeft vooralsnog geen toetsingskader voor de vitale sectoren opgesteld.

Context: plannings- en beleidscyclus

In deze paragraaf wordt aangegeven in hoeverre het toezicht op cybersecurity onderdeel is van de plannings- en beleidscyclus.

ANVS: De vergunninghouder formuleert maatregelen op basis van gedane bevindingen en implementeert deze. De ANVS toetst vervolgens of middels dit pakket van maatregelen de vastgestelde risico's gemitigeerd worden.

AT werkt met een flexibele programmering. Dit geldt tevens voor het toezicht op de naleving van de Wbni, Telecommunicatiewet en de eIDAS verordening. Voor het maken van keuzes hanteert zij een werkwijze op basis van risicoperceptie en sturing gevoed door uitgevoerde analyses en informatiesturing. Ze duidt periodiek de maatschappelijke risico's per (sub)domein. Door een werkwijze te hanteren waarbij de prioriteitstelling in het toezicht onderbouwd wordt door scherp de

maatschappelijke risico's in de gaten te houden tracht zij zo effectief mogelijk te zijn.

Het toezicht op cybersecurity door DNB maakt bij de Banken onderdeel uit van het toezicht op de IT-processen. De toezichtactiviteiten worden gebaseerd op de jaarlijkse risicoanalyse, de verplichte melding van toezichtincidenten en de opvolging van acties op basis van eerdere onderzoeken. Cybersecurity is een vast onderdeel van het toezichtprogramma.

Bij IGJ is informatiebeveiliging een aspect van het onderdeel E-health dat opgenomen is in het werkplan van de IGJ; het onderdeel informatiebeveiliging wordt niet specifiek in het werkplan uitgelicht.

IJenV heeft in haar werkprogramma 2021 bij het thema 'een weerbare samenleving' opgenomen dat zij toezicht houdt op de digitale weerbaarheid van vitale en andere kritische processen in het JenV domein. In dat verband voert zij hiertoe het eerste onderzoek uit. Ook voert zij de coördinatie van het toezicht - door verschillende partijen - op de digitale weerbaarheid van cruciale organisaties en vitale processen.

In het begin 2021 verschenen Meerjarenperspectief 2021-2024 geeft de IJenV aan dat digitale veiligheid een vitaal onderdeel is van een organisatie. Daarom richt de IJenV haar toezicht ook op het bevorderen van de weerbaarheid op dit vlak. Dit wordt de komende jaren in de jaarplannen concreet geprogrammeerd.

Bij ILT is toezicht op cybersecurity van de vitale processen nog niet in de planningscyclus opgenomen. Pas nadat het normenkader op basis van de MR Bbni er is, de HUF-toets is afgerond én Beleid de noodzakelijke middelen voor uitvoering van het toezicht beschikbaar heeft gesteld, wordt het toezicht op de uitvoering van de Wbni onderdeel gemaakt van de Plannings- en beleidscyclus.

Context: wet- en regelgeving

Het algemene toezicht dat de betrokken toezichthouders uitvoeren, verrichten zij op basis van verschillende sectorale en in meerdere gevallen internationale wet- en regelgeving. Hieronder valt tevens het algemene toezicht op cybersecurity.

De wettelijke basis voor het toezicht op de beveiliging van netwerk- en informatiesystemen van (per categorie) aangewezen aanbieders van essentiële diensten door ANVS, AT, en ILT is de Wbni.

Op 16 december 2020 presenteerde de Europese Commissie onder andere een herziening van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIB-richtlijn). De herziening van de NIB-richtlijn bevat een verplaatsing van de beveiligingseisen uit de European Electronic Communications Code en de eIDAS-verordening naar de NIB-richtlijn. De herziening zal uiteindelijk in nationale wetgeving worden geïmplementeerd en kan gevolgen hebben voor de wettelijke basis van het toezicht. Bovendien voert de Europese Commissie momenteel een review uit van de eIDAS-verordening. Er is nog geen voorstel gepresenteerd.

De ANVS houdt toezicht op de zorg- en meldplicht op grond van de Ministeriële Regeling beveiliging nucleaire inrichtingen en splijtstoffen. De Wbni heeft een zorgplicht opgelegd voor nucleair.

Agentschap Telecom houdt naast het toezicht op de essentiële Wbni sectoren energie en digitale infrastructuur ook op basis van de Telecommunicatiewet toezicht op de vitale sectoren internet en datadiensten, internettoegang, dataverkeer, spraakdienst, sms en vertrouwensdiensten. De beveiligings- en meldingseisen van de NIB-richtlijn zijn thans niet van toepassing op openbare elektronische communicatienetwerken en –diensten (telecomsector) en verleners van elektronische vertrouwensdiensten, omdat voor die sectoren al bestaande EU-regels gelden.

Voor het toezicht door de DNB wordt in de Wbni verwezen naar de sectorale wet- en regelgeving voor de financiële sector.

De sector gezondheidszorg waar IGJ toezicht op houdt is in het kader van de Wbni niet vitaal verklaard. IGJ houdt dan ook geen toezicht op basis van de Wbni op deze sector, maar houdt toezicht op basis van de Wet kwaliteit, klachten en geschillen zorg (Wkkgz) en de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. In 2021 wordt door VWS een vitaalbeoordelingsanalyse uitgevoerd om te onderzoeken of delen van de gezondheidszorg als vitaal proces aangemerkt dient te worden. Zodra duidelijk is welke processen en/of onderdelen van de zorg eventueel vitaal worden, zal VWS de IGJ tijdig betrekken bij de verdere bespreking hiervan.

IJenV houdt toezicht op de vitaal verklaarde processen ‘communicatie met en tussen hulpdiensten middels 112 en C2000’ en ‘inzet politie’. Deze processen zijn wel vitaal maar niet opgenomen in de Europese NIB-richtlijn en ook niet in de Wbni waardoor er voor deze processen geen AED’s en andere vitale aanbieders zijn aangewezen.

Deze vitale processen vallen onder de verantwoordelijkheid van het ministerie van Justitie en Veiligheid. De wettelijke basis voor het toezicht op cybersecurity bij deze vitale processen door de IJenV is niet expliciet belegd maar wordt afgeleid van wet- en regelgeving voor het generieke toezicht op die processen c.q. betreffende organisaties.

De ILT houdt naast de Wbni ook op basis van de Drinkwaterwet toezicht op de sector drinkwatervoorziening. Daarnaast houdt ILT toezicht op het spoorvervoer en wegtransport. In het kader van de Wbni zijn in deze sectoren nog geen aanbieders van essentiële diensten aangewezen. Het toezicht vindt daardoor ook nog niet plaats op grond van de Wbni. Voor de luchtvaart is de EASA-richtlijn, die voor delen van deze sector, de normen bepalen. De ontwikkeling en het tempo van EASA wordt daarom op de voet gevolgd. Hiermee bepaalt ook de EASA richtlijn, mede de scope van, het toezicht van de ILT.

Context: governance

Het feitelijke toezicht op vitale aanbieders door de betrokken toezichthouders heeft op de volgende organisaties en processen betrekking.

ANVS houdt toezicht op de acht nucleaire organisaties in Nederland. ANVS wisselt intensief informatie uit, over cybersecurity, met Europese partners, zowel op strategisch als op operationeel niveau.

Het AT houdt toezicht op:

- aangewezen (categorieën) AED’s in de sectoren Energie en Digitale Infrastructuur;

- aanbieders van openbare elektronische communicatienetwerken en –diensten;
- verleners van vertrouwensdiensten.

AT werkt veelvuldig nationaal en internationaal samen met andere organisaties en inspecties. AT levert ten aanzien van de Sectoren Energie en Digitale Infrastructuur een bijdrage in Europese werkgroepen (Workstreams) over de implementatie van de NIB-richtlijn.

AT levert de voorzitter van de Europese werkgroep over de implementatie van de NIB-richtlijn ten aanzien van digitale dienstverleners. Verder is AT voorzitter van ECASEC expert group (voormalig artikel 13A werkgroep), het samenwerkingsverband van toezichthouders op het gebied van openbare elektronische communicatienetwerken.

De betrokken toezichthouders hebben verschillende rechtsvormen. De ANVS is een bestuurlijk ZBO en legt verantwoording af aan de minister van IenW. AT is een baten-lasten agentschap en legt verantwoording af aan de staatssecretaris van Economische Zaken en Klimaat (EZK).

DNB is toezichthouder op de bij het besluit van De Nederlandse Bank N.V. aangewezen kredietinstellingen, exploitanten van handelsplatformen, centrale tegenpartijen, afwikkelondernemingen en centrale effecten bewaarinstellingen. Tevens houdt zij toezicht op processen voor het aanbieden en afwikkelen van betalings- en effectenverkeer.

DNB is een NV waarbij de nationale toezichttaken ondergebracht zijn in een ZBO en waarvoor verantwoording wordt afgelegd aan de Minister van Financiën. Voor het Europese bankentoezicht maakt zij deel uit van het Single Supervisory Mechanism (SSM), een zelfstandig onderdeel van de Europese Centrale Bank (ECB).

DNB is onderdeel van het Europees Stelsel van Centrale Banken (ESCB). De basis daarvoor is het verdrag EU en statuten ESCB en ECB.

IGJ houdt toezicht op de kwaliteit en veiligheid in de zorg. De zorg is niet aangewezen als vitale aanbieder (vitaal proces), maar op het terrein van informatiebeveiliging kijkt de IGJ steekproefsgewijs naar ziekenhuizen, GGZ-instellingen, GZ-instellingen, VVT-instellingen, en eerstelijnszorg groepen. In 2020 werd ook gekeken naar de ontwikkelingen in de deelsector jeugd.

IGJ heeft voor de algemene toezichttaak met verschillende internationale partners samenwerkingsafspraken.

IJenV houdt toezicht op de vitale processen ‘communicatie met en tussen hulpdiensten middels 112 en C2000’ en ‘inzet politie’. Deze processen zijn wel vitaal verklaard, maar niet opgenomen in de Europese NIB-richtlijn en ook niet in de Wbni waardoor er voor deze processen geen AED’s en andere vitale aanbieders zijn aangewezen.

Deze vitale processen vallen onder de verantwoordelijkheid van het ministerie van Justitie en Veiligheid. De wettelijke basis voor het toezicht op cybersecurity bij deze vitale processen door de betrokken toezichthouder, i.c. de JenV, is derhalve niet expliciet belegd maar wordt afgeleid van wet- en regelgeving voor het generieke

toezicht op die processen c.q. betreffende organisaties. JenV heeft voor de toezichttaak op de vitale processen geen afspraken met Europese partners.

IGJ en de IJenV zijn rijksinspecties en onderdeel van respectievelijk het ministerie van VWS en van Justitie en Veiligheid. De rijksinspecties hebben conform de Aanwijzingen inzake de rijksinspecties[12] een eigenstandige rol die de politiek verantwoordelijke heeft te respecteren.

ILT is als Rijksinspectie een agentschap van het ministerie IenW. De ILT houdt toezicht op de volgende aangewezen AED's:

- 10 waterleidingbedrijven (aangesloten bij VEWIN);
- Scheepvaartafwikkeling, toezicht alleen op de divisie havenmeester van havenbedrijf Rotterdam;
- Vlucht- en vliegtuigafhandeling, toezicht op KLM, Schiphol, LVNL, MUAC, AFS en KMar.

Meerjarenperspectief

In het laatste onderdeel van dit hoofdstuk wordt beschreven welke ontwikkelingen en ambities er op de lange termijn bij de betrokken toezichthouders op het gebied van het toezicht op cybersecurity zijn.

ANVS

De ANVS werkt aan een meerjarenperspectief op het vlak van cyberinspecties. In dat meerjarenperspectief wordt ingegaan op de noodzakelijke geachte kwantiteit en kwaliteit binnen de ANVS op het vlak van cyberinspecties. Er zal onder meer gekeken worden naar de noodzaak om expertise extern in te huren dan wel intern beschikbaar te hebben. Ook zal worden ingegaan op de mate waarin en wijze waarop het instrument van pentesten denkt te gaan gebruiken.

Aanscherping van het toetsingskader, dit op basis van de veranderingen op het vlak van cyberweerstand, en het actualiseren van desbetreffende volwassenheidsniveaus bij de nucleaire organisaties vormen elementen in dat meerjarenperspectief.

Om te komen tot verdieping van cyberinspecties in de sector Nucleair zal de ANVS nadrukkelijk samenwerking en wederzijdse informatieverstrekking (op strategisch en tactisch niveau) met vergelijkbare inspectiediensten in Nederland en het buitenland nastreven.

De ANVS zoekt actief de samenwerking op met andere toezichthouders en kijkt naar mogelijkheden in de samenwerking. De samenwerking met een aantal andere toezichthouders op het gebied van cybersecurity krijgt momenteel onder meer invulling in en rond het opstellen van het samenhangend inspectiebeeld.

AT

Het toezicht van AT richt zich op de beschikbaarheid, weerbaarheid en security van technische infrastructuren en het vertrouwen in het gebruik en veiligheid van apparaten. Weerbare vitale infrastructuren vormen een van de centrale thema's in ons toezicht. Naast beschikbaarheid van technische infrastructuren wordt het toezicht op de continuïteit en integriteit van netwerken en diensten voortgezet.

[12] Regeling van de Minister-President, Minister van Algemene Zaken van 30 september 2015, nr. 3151041, houdende de vaststelling van de Aanwijzingen inzake de rijksinspecties.

Netwerken dienen zo adequaat mogelijk beschermd te zijn tegen uitval als gevolg van externe factoren, waaronder onbedoeld door menselijke fouten dan wel bedoeld zoals door een hacker. Het kan daarbij bijvoorbeeld gaan om het noodnummer 112, maar ook om de sectoren energie (gas, aardolie en elektra), internetinfrastructuur en digitale dienstverlening. AT zal met betrekking tot de sectoren Energie en Digitale Infrastructuur vanaf 2021 meer thema specials (kennisonderzoeken) gaan uitvoeren, meer publiceren en proactief kennis gaan delen met AED's. Daarnaast professionaliseert en automatiseert AT de komende jaren haar werkzaamheden door het ontwikkelen van tools en instrumenten. Er zijn eerste contacten en overleggen met DNB.

AT ziet toe op de aangescherpte zorgplicht i.h.k.v. telecomsecurity, waaronder de aangescherpte technische maatregelen voor het gebruik van specifieke apparatuur in telecomnetwerken. AT krijgt het toezicht op cyberbeveiligingscertificeringsregelingen en conformiteitsbeoordelingsinstanties vanuit de Cyber Security Act.

DNB
In de Visie op Toezicht 2021-2024 is specifiek genoemd als speerpunt:

"Beveiliging van data en IT-infrastructuur tegen cyberaanvallen vergt continue investering in weerbaarheid. Financiële instellingen, hun (kritieke) dienstverleners en andere vitale sectoren zijn steeds vaker doelwit van cyberaanvallen. Deze trend zet in de coronacrisis onverminderd door. Instellingen en hun dienstverleners moeten kunnen aantonen dat zij hun informatiebeveiliging op orde hebben en moeten regelmatig hun cyberweerbaarheid testen. Verhoging van het kennisniveau van bestuursleden en commissarissen van instellingen op het gebied van IT- en cyberrisico's is nodig om de toenemende risico's te beheersen."

Visie op Toezicht 2021 – 2024, zie https://www.dnb.nl/toezichtprofessioneel/visie-op-toezicht/index.jsp.

Het voorstel van de Europese Commissie voor een verordening "digital operational resilience for the financial sector" (DORA) zal naar alle waarschijnlijkheid leiden tot meer en/of andere samenwerking met Europese financiële toezicht instanties (ESA's – European Supervisory Authorities).

Inspectie JenV
Het toezicht op cyber(security) is sinds 2020 in opbouw en in ontwikkeling. In dit opzicht zal de IJenV de komende jaren met name voor zowel de vitale als niet-vitale processen investeren en inzetten op regulier toezicht.

Naast het regulier toezicht op cybersecurity zal de IJenV, op basis van eigen risico afweging en die van gezaghebbende instanties, jaarlijks een aantal verdiepende en/of intensieve onderzoeken instellen. Deze verdiepende en/of intensieve onderzoeken zullen veelal themagericht plaatsvinden. Daarbij maakt de inspectie een bewuste keuze om al dan niet in de betreffende onderzoeken specifiek in te zoomen op een of meerdere fasen in de beveiligingscyclus, te weten: identificatie, protectie, detectie, response en herstel.

De IJenV maakt voor haar toezicht op cybersecurity, in relatie tot de kwaliteit van de taakuitvoering, gebruik van de ISO normeringen. Daar waar de ISO normeringen tekort schieten zal de IJenV zoveel mogelijk gebruik maken van eigen normeringen

die op basis van eigen inzichten, bepaalde wet- en regelgevingen en/of best practices worden vastgesteld. Ten behoeve van haar onderzoeken maakt de Inspectie (nog) geen gebruik van een expliciet volwassenheid(niveau)model.

Voor wat betreft de coördinerende rol van de Inspectie zal bij meer menscapaciteit ingezet worden op initiatieven die moeten leiden tot de verdere opbouw van kennis en kunde voor alle toezichthouders. Denk hierbij aan onder andere het organiseren van kennissessies, webinars en/of cursussen.

De samenwerking met een aantal andere toezichthouders op het gebied van cybersecurity krijgt momenteel met name invulling in en rond het opstellen van het samenhangend inspectiebeeld.

Het samenhangend inspectiebeeld is een goed instrument om de samenwerking nu en in de toekomst volwassener en intensiever te maken. Dit kan gestalte krijgen in niet alleen kennisuitwisseling maar ook in thema's die in het kader van cybersecurity of weerbaarheid de aandacht moeten krijgen. De kracht in de samenwerking met andere toezichthouders zit tevens in te behalen flexibiliteit van de inzet van specialisten, waarbij toezichthouders de faciliteiten krijgen en gestimuleerd worden om specialisten (tijdelijk) met elkaar uit te wisselen.

Binnen de overheid zijn er nog andere organisaties die audits of toezicht uitvoeren op cybersecurity. Denk hierbij aan de Algemene Rekenkamer (AR) en de Auditdienst Rijk (ADR). Met deze partijen is het vooral van belang om kennis uit te wisselen en elkaar te informeren over (toekomstige) onderzoeken en/of thema's van onderzoeken. Dit vindt al plaats maar wil de Inspectie de komende jaren verder uitbouwen. Dit met respect en behoudt van ieders verantwoordelijkheden en taakstellingen.

ILT

De ILT werkt aan een meerjaren toezichtvisie cybersecurity. De ILT stelt daarom een implementatieplan op waar naast de visie op het toezicht aandacht is voor verschillende thema's. Er volgt in elk geval een beschrijving van de rol en verantwoordelijkheden van de relevante afdelingen binnen ILT in het reguliere toezicht en het te ontwikkelen toezicht in het kader van de Wbni. Ook wordt een beschrijving gegeven van een toezichtsaanpak, waarbij het van belang is om aandacht te hebben om de capaciteit en deskundigheid die nodig zijn voor het uitvoeren van het toezicht in het kader van de Wbni. Daarom start de ILT ook met opleidingstrajecten.

De ILT zoekt daarnaast actief de samenwerking op met andere toezichthouders en kijkt naar mogelijkheden in de samenwerking

II Gebruikte afkortingen

AAVA	Andere aangewezen vitale aanbieder
AED	Aanbieder essentiële dienst
AFS	Aircraft Fuel Supply
ANVS	Autoriteit Nucleaire Veiligheid en Stralingsbescherming
AP	Autoriteit Persoonsgegevens
AT	Agentschap Telecom
AVG	Algemene verordening gegevensbescherming
Bbni	Besluit beveiliging netwerk- en informatiesystemen
BIO	Baseline informatiebeveiliging overheid
BIR	Baseline informatiebeveiliging rijk
CER	Directive on the resilience of critical entities
COBIT	Control objectives for information and related technologies
CSBN	Cybersecuritybeeld Nederland
DDos	distributed-denial-of-service
DNB	De Nederlandse Bank
DSP	Digitale service provider
EECC	Europese Elektronische Communicatie Code
EIDAS	Electronic IDentification Authentication and trust Services
ENISA	Europees Agentschap voor netwerk- en informatiebeveiliging

ETSI	Europees Telecommunicatie en Standaardisatie Instituut
EZK	Ministerie van Economische zaken en Klimaat
FIN	Ministerie van Financiën
FKI	Financiële kerninfrastructuur
IGJ	Inspectie Gezondsheidszorg en Jeugd
IJenV	Inspectie Justitie en Veiligheid
ILT	Inspectie Leefomgeving en Transport
IenW	Ministerie van Infrastructuur en Waterstaat
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	Information technology
LMS	Landelijke meldkamersamenwerking
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NEN	Nederlandse Norm / Stichting Koninklijk Nederlands Normalisatie Instituut.
NIB-richtlijn	Netwerk- en informatieveiligheid richtlijn
NIST	National Institute of Standards and Technology
OT	Operations technology
QSCD	Qualified Signature Creation Device
TIBER	Threat Intelligence Based Ethical Red Teaming
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
Wbni	Wet beveiliging netwerk- en informatiesystemen
Wgmc	Wet gegevensverwerking en meldplicht cybersecurity
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Missie Inspectie Justitie en Veiligheid

De Inspectie Justitie en Veiligheid houdt voor de samenleving, de ondertoezichtgestelden en de politiek en bestuurlijk verantwoordelijken
toezicht op het terrein van justitie en veiligheid
om inzicht te geven in de kwaliteit van de taakuitvoering en de naleving van regels en normen,
om risico's te signaleren
en om organisaties aan te zetten tot verbetering.
Hiermee draagt de Inspectie bij aan een rechtvaardige en veilige samenleving.

Dit is een uitgave van:
Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP Den Haag
Postbus 20301 | 2500 EH Den Haag
Contactformulier | www.inspectie-jenv.nl

Juni 2021