Samenhangend inspectiebeeld cybersecurity vitale processen

2021-2022

Inhoud

Voorwoord

Digitalisering is in de vitale sectoren en processen in Nederland niet meer weg te denken. Je moet er niet aan denken dat een vitaal proces – zoals energie- en drinkwatervoorziening, communicatie tussen de hulpverleningsdiensten, financieel verkeer – door een cyberincident uitvalt of wordt verstoord. Het is dan ook heel belangrijk dat deze sectoren en processen weerbaar zijn tegen cyberdreigingen en aanvallen. Toenemende dreigingen van statelijke actoren en cybercriminelen, de toegenomen (digitale) verwevenheid van systemen en organisaties en de daaruit voortvloeiende ketenafhankelijkheden maken dat we als toezichthouders alert zijn op de digitale weerbaarheid van onze vitale infrastructuur. De bij dit inspectiebeeld betrokken toezichthouders willen met dit inspectiebeeld in gezamenlijkheid bijdragen aan een digitaal veilige vitale infrastructuur.

In dit tweede samenhangend inspectiebeeld geven de betrokken toezichthouders inzicht in de huidige stand van de cybersecurity bij de vitale sectoren en processen in Nederland. Alhoewel de beelden per onderscheidenlijke vitale sector naar inhoud verschillen, is het de betrokken inspecteurs gelukt om door onderling overleg en uitwisseling van praktijkervaring een aantal gemeenschappelijke rode draden en trends te signaleren. Hierdoor biedt dit inspectiebeeld een inzicht in sectoren waar al goede resultaten worden geboekt en die als voorbeeld kunnen dienen voor andere sectoren. Ik hoop dat dit alle organisaties, vitaal en niet-vitaal, prikkelt om voortdurend te werken aan een betere digitale weerbaarheid. Dreigingen veranderen immers continu en daarmee ook de risico's. In dit inspectiebeeld geven we daarom vanuit een gezamenlijke benadering een aantal belangrijke aanbevelingen bij de verbetering van het risicomanagement ten aanzien van cybersecurity.

Tot slot wil ik nog even vooruit kijken. Want met de nieuwe Europese regelgeving op het gebied van digitalisering zoals de NIB2-richtlijn, zal het aantal vitale sectoren en organisaties sterk worden uitgebreid. Dat zal grote gevolgen hebben voor die organisaties, maar ook voor ons eigen toezicht. Daarom wijs ik er bij het uitbrengen van dit gezamenlijke beeld nog maar eens op dat het van belang is dat regelgeving, ook die vanuit Europa, voldoende aandacht heeft voor de uitvoerbaarheid van het toezicht.

Mede namens alle betrokken collega's,

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

Loopt u bij lezing tegen onbekende cybersecuritybegrippen aan, kijkt u dan eens in het cybersecurity woordenboek, een gratis beschikbare uitgave van Cyberveilig Nederland en de Cybersecurity Alliantie.

Samenvatting

De digitale wereld biedt geweldige kansen voor onze samenleving en economie. Dat vraagt om een adequate cybersecurityaanpak en goed en effectief toezicht hierop. De samenwerkende toezichthouders bieden een samenhangend inspectiebeeld van de cybersecurity van de vitale processen in Nederland.

De samenwerkende toezichthouders zijn Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS), Autoriteit Persoonsgegevens (AP), Agentschap Telecom (AT), De Nederlandsche Bank (DNB), Inspectie Gezondheidszorg en Jeugd (IGJ), Inspectie Justitie en Veiligheid (IJenV) en de Inspectie Leefomgeving en Transport (ILT).

Dit beeld bevat de huidige staat per toezichtveld, distilleert enkele rode draden en signaleert een aantal trends in relatie tot het toezicht. De individuele beelden per toezichtveld zijn terug te lezen in de bijlagen van dit inspectiebeeld. Het hoofddocument beschrijft een aantal rode draden die op basis van bespreking van de praktijkervaring en de individuele beelden tussen de toezichthouders is benoemd. De trends geven blik op een tweetal uitdagingen bij het houden van zicht op digitale risico's.

De belangrijkste rode draad richt zich op het onderwerp *risicomanagement*. Op basis van toezichtresultaten zien we dat risicomanagement in algemene zin de aandacht krijgt, ook op bestuurlijk niveau. Op het inrichtingsniveau vraagt implementatie van een Information Security Management Systeem (ISMS) nog aandacht. Daarom doen de toezichthouders op risicomanagement gezamenlijk de volgende *aanbeveling* met de belangrijkste aandachtspunten waarop ingezet zou moeten worden bij de verbetering van risicomanagement:

- het verder integreren van integrale beveiliging in het overkoepelende risicomanagement raamwerk;
- het actualiseren van scenario's op het snel veranderende dreigingsbeeld;
- het meten van de effectiviteit van mitigerende maatregelen;
- het inregelen van het risicomanagementproces rondom leveranciers.

Twee andere rode draden liggen in de toezichtpraktijk. De ene ziet op het nut van de beschikbaarheid van passende standaarden of best practices. Dit in verband met regelgeving waarin wordt gewerkt met open normen, ook wel doelregelgeving genoemd. In de praktijk komen toezichthouders voor de IT-omgeving vaak de ISO 27001 tegen of in de zorg specifiek de NEN7510. Maar denk ook aan normen op het gebied van OT, zoals de IEC 62443. Een passend aanbod van normen biedt de noodzakelijke handvatten om invulling te kunnen geven aan de verschillende beveiligingsdoelen die bedrijven wensen te halen.

De andere rode draad ziet op vorm en plaats van interventies. Gewenst gedrag ten aanzien van cybersecurity kan vaak het best worden bereikt met een mix van informele methoden en formele of sanctionerende interventies. Daarnaast is het voor toezichthouders relevant om op systeemniveau naar de risicovraagstukken in hun sector te kijken, waardoor mogelijk effectieve interventies zichtbaar worden die niet per definitie zijn gericht op de vitale dienstverlener zelf.

Terugkijkend op het vorige Inspectiebeeld zijn stappen vooruit gezet in de samenwerking en de toezichthouders kijken tevens alweer vooruit naar komende Europese regelgeving op het gebied van digitalisering zoals de NIB2-richtlijn en leveren daar ook actief bijdragen aan. Gezien de omvangrijke uitvoeringsvraag die bij de implementatie van de nieuwe wetgeving komt kijken, blijft samenwerking een aandachtspunt. Zo wordt vanuit de Inspectieraad ook samengewerkt, met de inzet van een brede groep van meer dan 20 rijksinspecties, markttoezichthouders en onderzoeksinstituten op het thema Artificial Intelligence (AI) als voorbeeld.

Tot slot wijzen we in dit beeld op twee trends met invloed op risico's in cybersecurity. De eerste trend richt zich op vernauwing van scope bij risicomanagement, door te veel te focussen op bepaalde soorten dreigingen, bijvoorbeeld criminele actoren. Deze scopevernauwing draagt in zichzelf weer een risico met zich mee voor de continuïteit van dienstverlening. De andere trend richt zich op de ontwikkeling van digitale ecosystemen, waardoor risico's duiden vanuit de klassieke supply chain benadering voor zowel toezichthouders als vitale dienstverleners en andere bedrijven een complexere uitdaging wordt. Sectoren en dienstverleners worden actief in meer verbanden en raken daardoor op steeds meer lagen en lijnen verbonden, waarmee risico's ook verbonden raken.

1 Inleiding

1.1 Aanleiding

Het coalitieakkoord onderkent als gevolg van de digitale revolutie geweldige kansen voor onze samenleving en economie, maar de coalitie geeft ook aandacht aan de noodzaak voor een adequate cybersecurityaanpak en goed en effectief toezicht hierop. Een aantal in het oog springende kwetsbaarheden, waaronder Log4J en niet in de laatste plaats de oorlog in Oekraïne en de daarbij genoemde risico's van cyberaanvallen op vitale infrastructuur blijven nieuwe dreigingen opleveren. Dit heeft weerslag op de digitale veiligheid in Nederland. Nederlandse organisaties kunnen bijvoorbeeld in hun ketenafhankelijkheden geraakt worden als gevolg van digitale aanvallen in relatie tot de oorlog in Oekraïne. Zo hebben eerdere aanvallen door Russische actoren geleid tot nevenschade.[1]

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 van bijlage 'Totaaloverzicht toezicht op cybersecurity'. De aanbieders van een groot deel van deze processen zijn tevens op basis van de Wbni als vitaal aangewezen.

In lijn met het versterken van samenwerking en samenhang tussen de diverse toezichthouders stelden de verschillende toezichthouders in 2021 het eerste samenhangend inspectiebeeld samen. Het beeld liet zien dat er op het gebied van digitaal weerbare vitale processen en aanbieders de nodige stappen zijn gezet. Maar het liet ook 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 voortdurend alertheid, adequaat handelen en scherpte nodig.
De toezichthouders maken de doorontwikkeling van het toezicht hierop inzichtelijk en leveren jaarlijks een staat van de cybersecurity van de vitale processen en aanbieders op in een samenhangend inspectiebeeld.

In het eerste samenhangend inspectiebeeld hanteerden we een beschrijving voor het begrip cybersecurity, deels ontleend aan het Cybersecurity Woordenboek, een publicatie van Cyberveilig Nederland:

"Alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of herstellen als die toch is ontstaan. Voorbeelden van schade zijn dat men niet meer in een computersysteem kan komen wanneer men dat wil. Of dat de opgeslagen informatie bij anderen terecht komt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen."

Specifiek in de Wet beveiliging netwerk- en informatiesystemen (Wbni), die voor een aantal toezichthouders bepalend is, wordt verwezen naar de Europese NIB richtlijn, waarin de volgende definitie wordt gegeven:

"Beveiliging van netwerk- en informatiesystemen: het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen."

[1] Digitale aanvallen oorlog Oekraïne | Nationaal Cyber Security Centrum (ncsc.nl).

1.2 De betrokken toezichthouders

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

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

Alhoewel de Wbni een heel duidelijk wetgevend kader voor cybersecurity van essentiële dienstverleners vormt, hebben niet alle bij dit beeld betrokken toezichthouders daarmee te maken. Dat kan zijn vanwege een ander wettelijk kader dan de Wbni, bijvoorbeeld in het geval van de Telecomsector of de Financiële sector. Of het komt doordat er simpelweg nog geen essentiële diensten in een bepaalde sector zijn aangewezen. Hieronder volgt in het licht van bovenstaande een korte duiding.

De sector gezondheidszorg waar de IGJ toezicht op houdt, is wel benoemd in de Europese NIB-richtlijn, maar in het kader van de Wbni zijn daar tot op heden nog geen vitale organisaties benoemd en ook geen essentiële diensten in de zin van de NIB 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. De term vitaal wordt in dit rapport breed toegepast en heeft dus ook betrekking op de sector gezondheidszorg en IGJ. De IGJ houdt nu al toezicht op de wettelijke verplichtingen van zorginstellingen op het gebied van informatiebeveiliging op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

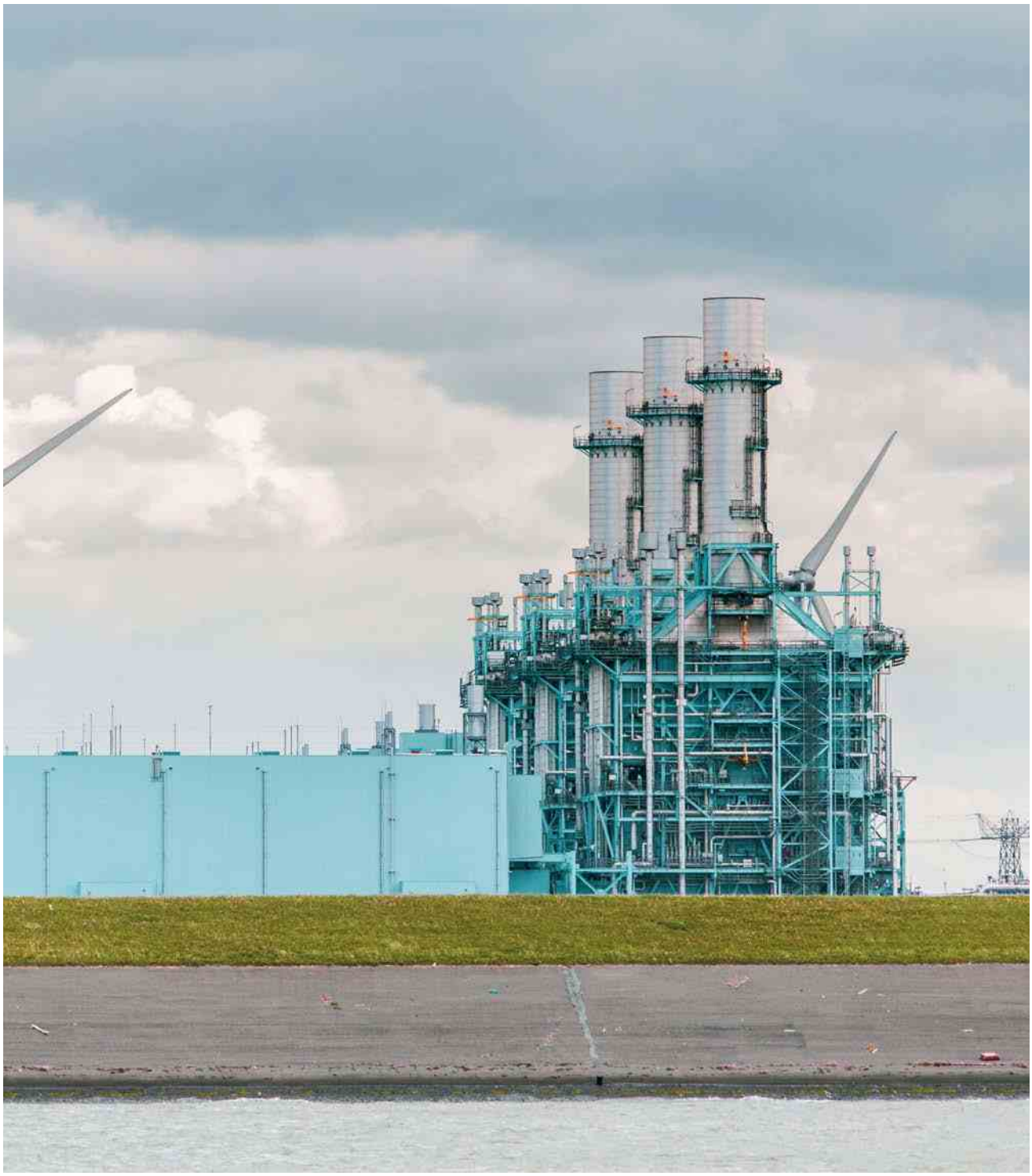
Met betrekking tot vitale processen is de IJenV geen toezichthouder in de zin van de Wbni. Wel houdt de IJenV toezicht op de vitaal verklaarde processen ‘communicatie met en tussen hulpdiensten middels 112 en C2000’ en ‘inzet politie’ binnen de sector OOV. Deze processen zijn wel vitaal maar niet opgenomen 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.

De AP is ook een van de betrokken toezichthouders, maar heeft een ander perspectief 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.

Zoals gezegd, houden de betrokken toezichthouders behalve op grond van de Wbni, ook toezicht op grond van diverse andere wettelijke kaders. Door deze verschillende invalshoeken kan het zo zijn dat verschillende toezichthouders dezelfde aanbieders van vitale processen onder toezicht hebben maar voor verschillende aspecten. Zo houdt de ANVS toezicht op situaties waarbij ioniserende straling vrij kan komen en stralingsbronnen kunnen voorkomen. Toepassingen komen bijvoorbeeld voor in ziekenhuizen. Deze partijen vallen ook onder het toezicht van de IGJ waardoor zij met meerdere toezichthouders te maken krijgen. Deze samenhang laat zien dat samenwerking tussen de verschillende toezichthouders geen optie, maar een noodzakelijk gegeven is.

1.3 Leeswijzer

In hoofdstuk 2 zijn de uitkomsten van het toezicht op de cybersecurity van de vitale processen per toezichthouder beschreven. Daarnaast zijn een aantal rode draden geïdentificeerd op inhoudelijk vlak en op het gebied van de doorontwikkeling van het toezicht. In hoofdstuk 3 is de doorontwikkeling samenhangend inspectiebeeld beschreven. Hierbij is gekeken naar de verbeterpunten uit het voorgaande inspectiebeeld, is de ambitie voor de komende jaren toegelicht en wordt ingegaan op de trends rondom Risk Management en Supply Chain Management.



2 Rode draden vanuit toezicht

2.1 Inleiding

Dit hoofdstuk bevat de rode draden op basis van de inspectieresultaten en over de toezichthouders zelf. De rode draden zijn gebaseerd op de inspectiewerkzaamheden die zijn uitgevoerd in 2021 en begin 2022 door de betrokken toezichthouders op het gebied van cybersecurity bij de verschillende vitale dienstverleners en processen. De focus van de inspectiewerkzaamheden richtte zich zowel op de Information Technology (IT) als de *Operational Technology (OT)*. In de bijlage is een gedetailleerd overzicht van de toezichtresultaten per toezichthouder opgenomen.

OT of IACS
Met de term OT wordt veel verwezen naar op ICT-gebaseerde meet-en regelsystemen die gebruikt worden voor het aansturen van productieprocessen. Voorbeelden van dit soort processen zijn het openen van bruggen en sluizen, het verwerken van nucleair materiaal en het distribueren van energie. Een andere term die ook vaak wordt gebruikt voor dit soort systemen is IACS, wat staat voor Industrial Automation and Control Systems. Meer achtergrond is bijvoorbeeld te vinden in een drietal webinars over dit onderwerp.

2.2 Risicomanagement als speerpunt in cybersecurity

Alle toezichthouders besteedden in 2021 aandacht aan risicomanagement. Het onderwerp was onderdeel van een brede analyse op het gebied van digitale weerbaarheid, kwam in sommige gevallen terug in diepgaande inspecties en werd besproken op bestuursniveau, aangezien de aandacht voor het onderwerp daar dient te beginnen. Een belangrijke basis hiervoor werd veelal gelegd door de opzet van een Information Security Management Systeem (ISMS). Risicomanagement kwam in het toezicht ook vaak terug in combinatie met het specifieke onderwerp van risico's in de toeleverantieketen.

2.2.1 Risicomanagement en het belang van een goed ISMS

Toezicht genietende organisaties zijn in het licht van dit inspectiebeeld de organisaties die vitale diensten aanbieden, al gaat die beschrijving niet 100% op voor sommige bij dit beeld betrokken toezichthouders, zoals toegelicht in paragraaf 1.2 van dit beeld. In het kader van de NIB richtlijn en de Wbni wordt in plaats van vitaal ook gesproken over Aanbieders van Essentiële Diensten (AED's). Voor meer achtergrond hierover verwijzen we naar het eerste Samenhangend Inspectiebeeld, waar uitgebreider werd ingegaan op de door elkaar gehanteerde begrippen vitaal en essentieel. In dit beeld hanteren we in het vervolg de term vitale dienstverleners.

Een ISMS borgt het risicomanagement proces op basis van een plan-do-check-act cyclus. Uit de analyses van de toezichthouders blijkt, dat de meeste *toezicht genietende organisaties* continu aandacht besteden aan hun Information Security Management Systeem (ISMS). Nagenoeg alle vitale dienstverleners hanteren de ISO 27001[2] als leidraad voor een ISMS. Een deel van de vitale dienstverleners heeft zich hiervoor ook laten certificeren. Alhoewel in algemene zin kan worden gezegd dat een basisniveau voor cybersecurity aanwezig is, is het ook zo dat nog niet alle organisaties de implementatie van hun ISMS al volledig adequaat hebben ingericht.

[2] Of de daarmee vergelijkbare NEN 7510 voor de sector gezondheidszorg.

Los van de individuele verschillen, menen de toezichthouders dat het goed is dat de gehele klas het gemiddeld aardig doet, maar dat derhalve ook ruimte bestaat om het gemiddelde van diezelfde klas omhoog te brengen.

In het algemeen onderkennen de vitale organisaties uit de verschillende sectoren overigens dat verbeteringen in de governance ten aanzien van risico's moeten worden doorgevoerd. Mede als gevolg van de inspectiewerkzaamheden kregen verbetertrajecten een extra stimulans en raakt het bestuursniveau steeds meer betrokken bij dit onderwerp.

Zoals eerder benoemd, hebben alle toezichthouders op verschillende manieren aandacht gegeven aan risicomanagement in hun toezicht. Zo zijn in een aantal gevallen ook diepgaande inspecties uitgevoerd, waarbij specifiek aandacht is gegeven aan dit thema. In deze gevallen maakten de toezichthouders specifieke afspraken met de betreffende vitale organisaties over verbeteringen en/of vervolgstappen.

Binnen het overkoepelende risicomanagement draagt een ISO 27001 certificering bij aan de IT en OT governance van vitale dienstverleners. Het toont aan dat maatregelen continue worden gemonitord en waar nodig verder worden verbeterd. Uit de inspectiewerkzaamheden blijkt dat vitale dienstverleners snel reageren op kwetsbaarheden. In enkele gevallen leveren kwetsbaarheden echter onvoorziene scenario's op waar organisaties niet goed op zijn voorbereid. Zo bleek bijvoorbeeld dat het vaststellen van de impact voor de LOG4J kwetsbaarheid complex was als gevolg van het ontbreken van inzicht in de kwetsbare applicaties. Op basis van lessons learned dient aanscherping in processen plaats te vinden.

AANBEVELING

Zoals hierboven benoemd, menen de toezichthouders dat er ruimte is om het gemiddelde van de klas omhoog te krijgen en hechten er daarom waarde aan dat de risicomanagementcyclus gericht op integrale beveiliging over het algemeen naar een hoger niveau wordt getild. De belangrijkste aandachtspunten waarop ingezet zou moeten worden zijn:

- het verder integreren van integrale beveiliging in het overkoepelende risicomanagement raamwerk;
- het actualiseren van scenario's op het snel veranderende dreigingsbeeld;
- het meten van de effectiviteit van mitigerende maatregelen.

2.2.2 Risicomanagement bij leveranciers

Dit risico komt tevens naar voren in het Cybersecurity Beeld Nederland en wordt wereldwijd gezien als een belangrijk risico. Bedrijven zorgen zelf voor een adequaat niveau van cybersecurity, waardoor kwaadwillenden uitwijken naar de toeleveranciers, om via die weg alsnog binnen te komen op het netwerk van de vitale organisatie. Bekende voorbeelden zijn Citrix en Solarwinds. Voor meer achtergrond verwijzen we naar een onderzoek dat TNO in februari 2021 heeft afgerond in opdracht van het NCSC.[3]

Dit risico wordt specifiek door de toezichthouders vanuit de praktijk onderkend als uitdaging voor de vitale dienstverleners. Op deze leveranciers kan door de toezichthouder zelf namelijk geen actief toezicht worden gehouden.

AANBEVELING

- Het inregelen van het risicomanagementproces rondom leveranciers behoeft gezien het bovenstaande specifiek aandacht van de vitale organisaties.

2.2.3 Risicomanagement als middel om te sturen op veranderende dreigingen

Digitale weerbaarheid is complex en continu aan verandering onderhevig. Het onderwerp zit verweven in een samenspel tussen mensen, techniek en processen. Het vraagt daarom een gestructureerde aanpak én commitment van het bestuur. Om deze reden vinden de toezichthouders een adequaat risicomanagement een belangrijk speerpunt in toezicht op cybersecurity.

[3] TNO 2021 R10245 - Vraagstukken en perspectieven voor ICT SCRM – een initiële verkenning.

Risicomanagement is de basis van de digitale weerbaarheid van organisaties. Het is een continu proces dat risico's identificeert. Door het inschatten van de impact en kans van het optreden van de risico's, kunnen de juiste beheersmaatregelen worden getroffen. Dit hele stelsel belegt verantwoordelijkheden, geeft inzicht en stelt organisaties in staat om proactief op risicobeheersing te sturen.

Diensten van vitale dienstverleners ondervinden steeds meer het effect van digitalisering, gewild en soms ook ongewild vanuit de aanbodzijde van toeleveranciers. Dit zal de komende jaren naar verwachting toenemen. De digitale infrastructuur in de maatschappij en dus ook die van vitale dienstverleners is steeds vaker doelwit van cyberaanvallen.[4] Dit kan leiden tot maatschappelijke ontwrichting. Een goed ingericht en actief toegepast risicomanagementproces draagt bij aan het waarborgen van de continuïteit van vitale en essentiële diensten.

2.2.4 Meldingen van cybersecurity incidenten

Er gelden vanuit verschillende wettelijke regimes diverse meldplichten voor incidenten bij de toezichthouders, waaronder de meldplicht voor incidenten onder de Wbni. Vitale dienstverleners onder de Wbni zijn verplicht om alle incidenten die aanzienlijke gevolgen hebben voor de continuïteit van de dienstverlening en/of een specifieke drempelwaarde overschrijden, onverwijld te melden bij de toezichthouder en het NCSC. Naar aanleiding van incidenten kan de toezichthouder nader onderzoek uitvoeren om te kijken of het noodzakelijk is om de kwaliteit van de digitale weerbaarheid te verhogen en het lerend vermogen te stimuleren. In dit beeld gaan de toezichthouders niet uitgebreid in op meldingen. Er zijn in 2021 namelijk geen incidenten gerapporteerd die aan de verplichte drempels raakten.

De Autoriteit Persoonsgegevens ontvangt zoals bekend elk jaar veel meldingen, waarover zij rapporteert in de Datalekkenrapportage.[5] Een observatie vanuit deze rapportage is dat de Autoriteit Persoonsgegevens in 2021 28 cyberaanvallen bij ICT-leveranciers heeft gesignaleerd. Deze incidenten hebben impact op tenminste 1.800 klanten van deze ICT-leveranciers. Zonder analyse is hier verder geen verband te benoemen met vitale dienstverlening, maar deze observatie onderstreept wel het eerdere genoemde belang van risicomanagement richting toeleveranciers.

Een breder inzicht in digitale incidenten wordt overigens ook geproduceerd op Europese schaal. Dit wordt bijvoorbeeld gedaan door het Europese agentschap voor cybersecurity; ENISA. Zij verzamelen vanuit de verschillende lidstaten de gerapporteerde incidenten onder de NIB-richtlijn, de eIDAS-verordening en de Telecomsector en rapporteren hierover.[6]

2.3 Uitdagingen in het toezicht

Het samenhangend inspectiebeeld helpt ook het toezicht op cybersecurity verder te professionaliseren door het belichten van gemeenschappelijke uitdagingen en vraagstukken. Het gaat om vraagstukken over de wisselwerking tussen wet- en regelgeving, normen, kaders en systemen die binnen de verschillende terreinen, sectoren en aanbieders gebruikelijk zijn. Of vraagstukken over de effectieve inzet van het gehele toezichtinstrumentarium om vitale dienstverleners in beweging te krijgen of risico's ten aanzien van het gehele systeem te beperken. Vraagstukken als deze zorgen voor dynamiek en vragen tegelijkertijd om inzicht in samenhang van het blikveld van de toezichthouders. Hieronder volgen een aantal inzichten uit de gezamenlijke toezichtpraktijk.

2.3.1 Doelregelgeving en het nut van standaarden, guidelines en best practices

In diverse soorten regelgeving, zoals de NIB-richtlijn of de Telecommunicatiewet, worden open formuleringen gebruikt om zorgplichten voor cybersecurity of continuïteit van dienstverlening te benoemen. Open formuleringen, ook vaak open normen genoemd, benoemen vaak doelen en dit biedt een voordeel voor bedrijven om zo binnen hun eigen bedrijfsvoering te bepalen hoe zij dergelijke doelen invullen. Deze invullingsruimte biedt bijvoorbeeld voordelen in termen van level playing field, waarbij risicomanagement een belangrijk principe vormt, dat mede bepaalt hoe die invulling wordt gedaan. In een digitaal snel veranderend risicolandschap past deze open benadering goed.

[4] Cybersecuritybeeld Nederland 2021 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl).
[5] Datalekkenrapportage_ap_2021.pdf (autoriteitpersoonsgegevens.nl).
[6] Incident Reporting — ENISA (europa.eu).

Maar de open formulering van regelgeving vraagt in de praktijk ook om verduidelijking. Organisaties, waaronder ook vitale dienstverleners, zoeken naar uitleg en interpretatie van de normen, aangezien zij die in de praktijk benutten om aan te tonen hoe zij aan de norm voldoen. De toezichthouders geven binnen hun sector op verschillende manieren richting en interpretatie bij de wettelijke normen, omdat het (detail)niveau daarbij niet vooraf bepaald of bekend is en de mate van behoefte bovendien per sector of toezicht genietende organisatie (grote) verschillen kent. Maatwerk is een vereiste. Immers, een open norm waar onvoldoende handvatten voor bestaan, kan tot gevolg hebben dat aan de norm niet wordt voldaan, waardoor grote maatschappelijke risico's ontstaan. Te gedetailleerde interpretatie of invulling kan echter weer het effect sorteren dat aan het doel van de norm voorbij wordt gegaan.

Standaarden, guidelines en best practices
Een standaard of een norm is een document met bepaalde erkende afspraken of specificaties ten aanzien van producten, diensten of processen. Het feit dat de afspraken erkend zijn geeft ze waarde. Hoe breder de erkenning, bijvoorbeeld in een branche of zelfs internationaal op een bepaalde techniek of vakgebied, hoe groter de waarde. Standaarden kunnen bedrijven helpen om gestructureerd invulling te geven aan doelen die ze willen bereiken op het gebied van bijvoorbeeld veiligheid of kwaliteit.

Guidelines geven in een gestructureerde vorm niet bindende aanbevelingen, gebaseerd op een combinatie van informatie uit bepaalde standaarden, best practices of andere goede praktijkvoorbeelden.

Een best practice is een bepaalde techniek, werkmethode of activiteit die in de praktijk heeft bewezen effectief te zijn. Sommige best practices kunnen vanwege hun bewezen waarde later weer terug komen in standaarden.

De toezichthouders zien in dit licht een groot belang in de ontwikkeling van het handvat van passende (internationale) standaarden, guidelines en best practices. De praktijkervaring van toezichthouders kan daarin een waardevolle factor zijn bij de ontwikkeling, beschikbaarheid of stimulans van dergelijke handvatten. De doorontwikkeling en beschikbaarheid van de standaarden en normen is daarbij even belangrijk als het bestaan ervan. We zien bijvoorbeeld in de inspectiebeelden van ILT, AT en IGJ dat de standaarden en normen voor informatiebeveiliging – zoals de ISO 27000-familie of de in de zorg gehanteerde NEN 7510 – een belangrijke rol spelen. En niet alleen voor IT, ook op het snijvlak van IT en OT is de ontwikkeling van relevante standaarden voor cybersecurity, zoals de IEC-62443, zeer belangrijk.

Deze standaarden kunnen – evenals guidelines en best practices – een doelmatige oplossing bieden om concrete, erkende maatregelen te kunnen treffen en processen in te kunnen richten, die zoveel mogelijk aansluiten en passend zijn bij de doestelling van open regelgeving. De mogelijkheden om de standaarden, normen, etc., aan te passen of bij te werken indien dat nodig is, zijn ruimer en flexibeler dan dit bij wet- en regelgeving het geval is.

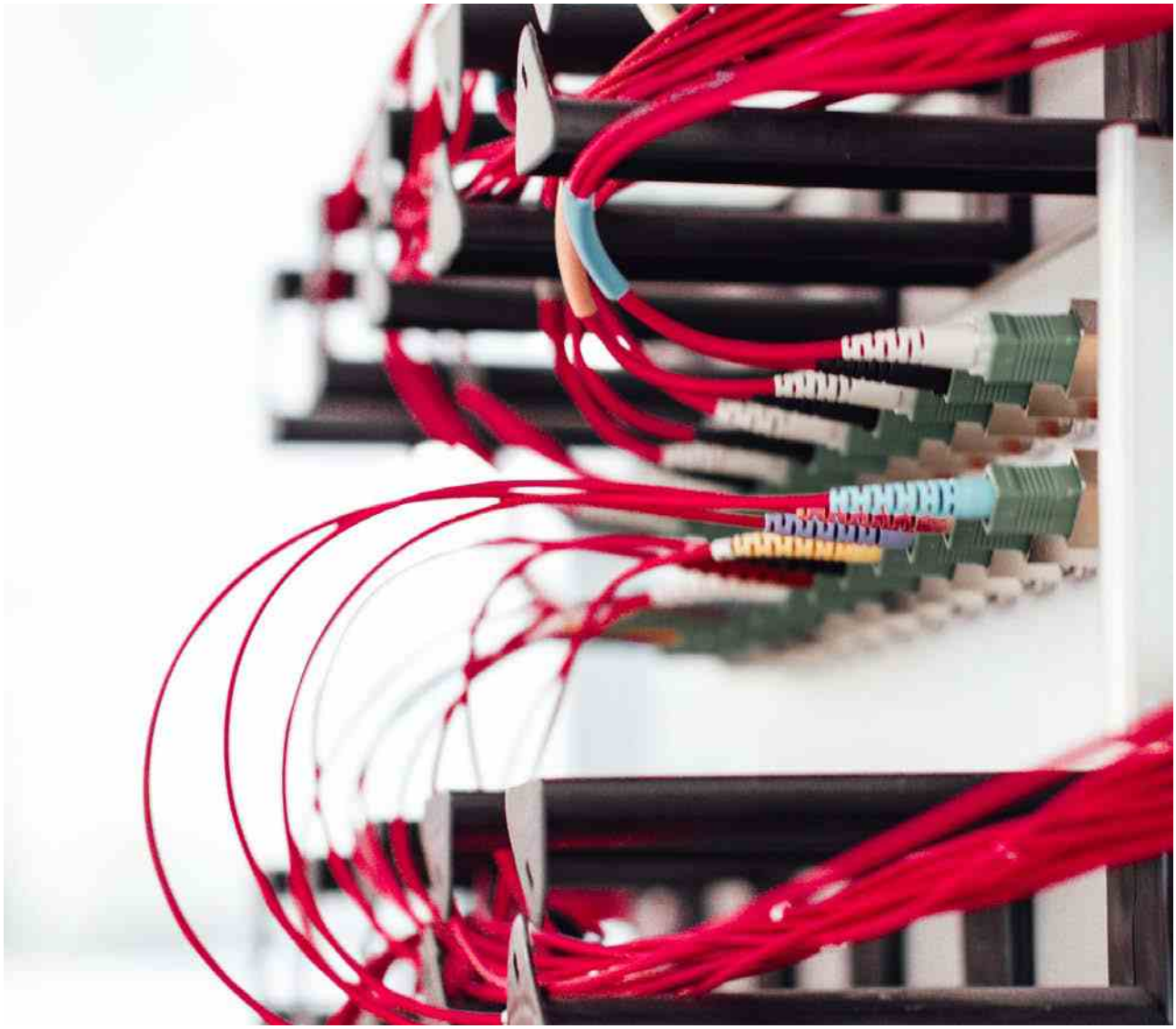
2.3.2 Interventies effectief door te kijken naar de vorm en de plek in de gehele keten

Een toezichttaak vergt een wettelijke grondslag en biedt vervolgens interventie- en handhavingsinstrumenten die de toezichthouder bij de uitvoering van zijn taak ondersteunen. De instrumenten zijn er in velerlei soorten en maten. Van (informele) interventies als educatieve of normatieve communicatie tot het handhavingsmiddel bestuurlijke boete. De keus voor één specifieke interventie is niet altijd eenvoudig en vanuit gedragsoptiek is het ook de vraag in welke vorm of mix interventies een juiste prikkel geven om nakoming van cybersecurity zorg- en meldplichten te stimuleren.

Het samenhangend inspectiebeeld laat onder meer zien dat informele interventies in positieve zin leiden tot verbeteringen of verbetertrajecten. Dit is zichtbaar in de individuele beelden in de bijlage, bijvoorbeeld bij ANVS, AT, IGJ en ILT. De essentie ligt hier vaak in het creëren van de juiste prikkel om de passende en voortdurende aandacht te hebben voor cybersecurity. Dit leidt tot motivatie, bestendigheid en het nemen van eigen verantwoordelijkheid.

Het voorgaande zegt iets over de vorm van een interventie richting een vitale dienstverlener vanuit het toezicht. Maar een vitale dienstverlener is niet alleen. Hij maakt bijvoorbeeld gebruik van diensten van anderen of maakt onderdeel uit van een breder stelsel of ecosysteem. Het is voor een toezichthouder aan te bevelen om breder te kijken naar aanwezige knelpunten in de omgeving van de vitale dienstverlener of op systeemniveau. Deze knelpunten kunnen wezenlijke risico's of juist oplossingen in het kader van de cybersecurity met zich mee dragen. Dit biedt kans om op andere manieren dan direct richting de vitale dienstverlener beweging te creëren en gedrag te beïnvloeden. Als het gaat om cybersecurity en vitale processen kunnen derden namelijk ook een grote rol spelen. Dit kunnen partijen zijn zoals certificerende instellingen, maar bijvoorbeeld ook leveranciers van apparatuur of diensten. Deze derden zijn formeel vaak geen onder toezicht staande organisatie, maar de toezichthouder heeft of kan met zo'n instelling of leverancier te maken hebben bij de uitvoering van de toezichttaak.

Interventies op of in het systeem kunnen dus nuttig zijn, maar ook een uitdaging, omdat in veel gevallen geen directe wettelijke basis bestaat om jegens derden naleving van concrete regels af te dwingen. De effecten van (gedrag van) derden op compliance door aanbieders kunnen echter wel groot zijn, bijvoorbeeld omdat een in de keten belangrijke bijdrage van een derde van dusdanige kwaliteit is dat risico's daarmee beter opgevangen kunnen worden. Derde partijen kunnen dus bijdragen aan het wegnemen van knelpunten of maatschappelijke risico's, al dan niet hier toe gestimuleerd door de toezichthouder die hier vanuit zijn maatschappelijke opgave of systeemrol zorgvuldig laveert tussen wat formeel mag en informeel kan. Ook in een dergelijke ketenaanpak kan het toezicht op cybersecurity zich verder ontwikkelen en het samenhangend inspectiebeeld kan hieraan bijdragen.



3 Doorontwikkeling samenhangend inspectiebeeld

3.1 Inleiding

Het Samenhangend Inspectiebeeld 2021 sloot vorig jaar af met een aantal aandachtspunten en een schets van een aantal onderwerpen waarin de ambitie voor doorontwikkeling voor de komende jaren werd gevat. In deze paragraaf blikken we terug op de aandachtspunten van vorig jaar en kijken we naar de doorontwikkelingspunten, die zich richten op het ontwikkelen van gedeelde indicatoren, toezicht langs een gezamenlijk thema en het opzetten van een platform voor toezichthouders.

3.2 Terugblik aandachtspunten 2021 en vooruitblik

In dit inspectiebeeld van 2022 brengen de samenwerkende toezichthouders het belang van risicomanagement naar voren. Niet voor niets één van de vijf hoofdmaatregelen, zoals opgenomen in de bijlage bij het Besluit beveiliging netwerk- en informatiesystemen,[7] als nadere uitwerking van de zorgplicht in de Wbni. Vorig jaar lag de focus in de concluderende aandachtspunten van het inspectiebeeld op supply-chain management, business continuity management en de opkomst van nieuwe technologie, zoals AI.

Terugkijkend bleken die aandachtspunten goed gekozen en van groot belang. Risico's in ketenafhankelijkheden bleken onverminderd groot, met Log4J als zeer zichtbaar voorbeeld. Ook business continuity management bleek een belangrijk aandachtspunt, gezien het toenemende risico van ransomware aanvallen, waarvan een deel ook de media haalden.

Verder werd gesignaleerd dat Europese regelgeving op het gebied van digitalisering de komende jaren een flinke impact op de aard en omvang van de regelgeving en onderliggende sectoren in Nederland en daarmee dus ook een impact op de uitvoeringskracht van betrokken toezichthouders. Het gaat onder andere om nieuwe regelgeving in de financiële sector (DORA), op het gebied van cybersecurity certificering (CSA) en regelgeving gericht op de vitale infrastructuur en essentiële diensten (NIS2 en CER).[8] Zo valt te voorzien dat onder de nieuwe NIB-richtlijn het soort en aantal vitale of essentiële dienstverleners gaat toenemen. Vanwege de verwachte omvang van de uitvoeringsopgave houden toezichthouders in Nederland ondertussen op verschillende manieren rekening met deze Europese ontwikkelingen. Zo is er actieve betrokkenheid vanuit de werkgroep toezichthouders van dit inspectiebeeld bij het proces dat loopt rond de herziening en implementatie van de nieuwe Europese NIB-richtlijn. De uitdaging ligt niet alleen op nationaal niveau, aangezien de regelgeving een Europese basis heeft en de aanbieders en eventuele derde partijen vaak ook actief zijn in meerdere EU-lidstaten. Steeds meer is de uitvoering van de toezichttaak daarom gebaat bij nationale én internationale afstemming en samenwerking.

[7] Besluit beveiliging netwerk- en informatiesystemen.

[8] DORA, Digital Operational Resilience Act, betreft regelgeving voor digitale weerbaarheid in de financiële sector. CSA, Cyber security Act, introduceert een Europees certificeringstelsel voor IT producten, -diensten, en processen. NIS2 betreft regelgeving voor de digitale weerbaarheid van diverse essentiële en belangrijke sectoren. CER, Critical Entities Resilience, regelgeving gericht op de algemene weerbaarheid van kritieke diensten.

3.3 Doorontwikkeling samenhangend inspectiebeeld 2021 en vooruitblik

Bij de totstandkoming van het Inspectiebeeld 2021-2022 bleek het in gezamenlijkheid opzetten van gedeelde indicatoren of het uitvoeren van een gezamenlijk opgezet thema een stap te vroeg te komen. De tijd die nodig is om de voorafgaande analyse uit te voeren en de noodzakelijke capaciteit te prioriteren bleek te kort. Dit stond eraan in de weg om deze ambitie mee te nemen in de individuele programmering bij de verschillende toezichthouders. Inhoudelijk heeft dit enerzijds te maken met verschillen in sectorale risico's en kaders en daarmee verschil in prioriteiten en anderzijds in organisatorische zin met een beperkte inzetbare capaciteit aan geschikte inspecteurs en de verschillen in tempo bij de cycli die de toezichthouders in hun programmering hanteren.

Dat doet niet af aan de ambitie, het belang van gezamenlijk optrekken wordt onderkend. In 2022 is daarom in het werkproces rond het samenhangend inspectiebeeld tijdig ruimte gemaakt om te komen tot gezamenlijke indicatoren voor de sectorale toezicht-programma's voor 2023.[9] Een volgende stap kan daarna liggen in de doorontwikkeling naar een gezamenlijk onderzoeksthema.

Op nationaal niveau werken de bij dit inspectiebeeld betrokken toezichthouders al enkele jaren samen rond cybersecurity van vitale processen, maar ook op andere niveaus werken toezichthouders steeds meer samen vanwege digitale ontwikkelingen en ontwikkelingen op het gebied van digitale ecosystemen. Vanuit de door de Inspectieraad ingestelde portefeuille digitalisering[10] wordt werk gemaakt van een inventarisatie van de voor de toezichthouders relevante Europese digitale regelgeving om zo te kunnen anticiperen op de mogelijke gevolgen voor het toezicht. Ook wordt werk gemaakt van de noodzaak tot verdere professionalisering van het digitale toezicht. De toezichthouders zetten in op het starten van een analyse om de kwalitatieve en kwantitatieve behoeften in kaart te brengen op dit terrein.

Een andere doorontwikkelingsfunctie die vorig jaar werd genoemd, is gelegen in een platformfunctie voor toezichthouders. Op dagdagelijks en operationeel niveau weten de toezichthouders die werken aan het samenhangend inspectiebeeld elkaar te vinden. Een bredere platformfunctie is voor toezichthouders echter ook een nuttig instrument om elkaar te vinden en van elkaar te leren.

Een goed voorbeeld van een dergelijke platformfunctie is het spoor *toezicht op AI* in de portefeuille digitalisering van de Inspectieraad. Onder deze beweging heeft zich ondertussen een grote werkgroep van rijksinspecties, markttoezichthouders en onderzoeksinstituten verzameld. Ook onder het spoor cybersecurity heeft zich een werkgroep gevormd die breder is dan de deelnemende toezichthouders aan dit samenhangend inspectiebeeld. Vanuit het bureau Inspectieraad worden de werkgroepen ondersteund en is een kennisplatform ingericht. Op deze wijze worden toezichthouders in staat gesteld elkaar te vinden op deze onderwerpen en kennis en methodieken uit te wisselen.

3.4 Trends: Risk Management en Supply Chain Management

Een goed verstaander van nieuws rond digitale incidenten en dreigingen begrijpt waar de focus moet zitten. Het kwam ook al naar voren in paragraaf 2.1 in de rode draden vanuit het toezicht. Generiek gaat het om Risk Management, specifiek gaat het om Supply Chain Management. Het zijn risicogebieden, waarbij het interessant is om ze vanuit het toezicht tegen het licht te houden van een achterliggende trend. Dit levert inzichten op voor toezicht in de toekomst.

3.4.1 Een breed perspectief op Risk Management

Voor het generieke Risk Management is de zaak helder: ontwikkelingen in de samenleving dwingen af dat risico's eerder onderkend worden, dat er meer op gestuurd wordt ze te mitigeren en dat risico's die tot een calamiteit leiden ruiterlijk erkend en deugdelijk onderzocht worden om collectief stappen te kunnen zetten in het verhogen van de cyberveiligheid van essentiële diensten.

[9] Een voorbehoud bij deze doorontwikkeling dient in dit kader te worden gemaakt voor toezichthouders die niet volledig zelfstandig kunnen besluiten over de inzet en verdeling van hun capaciteit en toezichtmiddelen, zoals bijvoorbeeld DNB.

[10] De Inspectieraad heeft een portefeuille digitalisering ingesteld, waarin verschillende aspecten van digitalisering in het toezicht samen komen. De portefeuille richt zich op vier sporen, te weten:
(1) toezicht met behulp van AI, (2) toezicht op AI, (3) Cybersecurity en (4) databewustzijn.

Een achterliggende trend die men in het kader van digitale dreigingen zou kunnen benoemen, betreft de focus op actieve dreigingen, bijvoorbeeld die vanuit criminele en statelijke actoren. En dat is begrijpelijk, aangezien het daarbij gaat om het toenemende belang van aansprekende dreigingen op economisch gebied en sinds het voorjaar van 2022 zelfs heel zichtbaar, op politiek gebied. Het zijn die ontwikkelingen die met steeds grotere nadruk duidelijk maken dat Risk Management in iedere organisatie hoog op de agenda moet staan. Niet alleen omdat dienstverlening uit kan vallen, maar – belangrijker nog – omdat vertrouwen in leveringszekerheid en afgedekte veiligheid onherstelbaar geschaad kunnen worden. Waar toezichthouders vanuit hun praktijkervaring echter op willen wijzen in het kader van risk management, is de all-hazard benadering in digitale weerbaarheid of cybersecurity. Met all-hazard bedoelen we alle oorzaken die voor uitval, storing of misbruik van ICT kunnen zorgen, niet alleen oorzaken die vanuit een doelgerichte of bewuste actor komen. Een observatie die de WRR bijvoorbeeld ook al deed in 2019.[11]

Waarom dan de focus op deze trend? Vanwege het feit dat het volgen van een trend met focus op actieve dreigingen, zomaar kan leiden tot een blinde vlek in de scope die bedrijven hanteren in hun risicomanagement. Onbewust selecteren op risico's uit actieve dreigingen, kan inherent leiden tot het negeren van meer voor de hand liggende ICT risico's met een wellicht evenzo groot effect op de continuïteit van de dienstverlening. Een objectieve kijk op het gehanteerde perspectief is derhalve raadzaam.

3.4.2 Van supply chains naar ecosystemen

Alhoewel in dit inspectiebeeld aandacht wordt gegeven aan verhoogde volwassenheid op het gebied van Supply Chain Management, valt ook hier een achterliggende trend te benoemen. Die trend zit hier in de ontwikkeling van digitale ecosystemen. Het is daardoor niet langer voldoende enkel de toeleverantieketens van de eigen organisatie te bezien.

Door allerlei nieuwe technologische ontwikkelingen en digitalisering van de economie volstaat het niet meer om enkel in klassieke van-A-naar-B-ketens te denken. De waarde die producten en diensten in maatschappelijk of economisch perspectief vervullen, komt steeds vaker tot stand in coöperatief verband met inzet van afwisselende partijen. Die partijen worden betrokken op basis van hun specifieke rol, kennis of expertise en digitalisering speelt daarin een belangrijke rol. Zo vormt zich een digitaal ecosysteem waarin de specifieke multidisciplinaire combinatie van verschillende digitale diensten van verschillende aanbieders een waarde toevoegt in de economie of maatschappij. Partijen kunnen hun specifieke waarde bovendien inzetten in verschillende digitale ecosystemen. Hierdoor kan het aantal leveranciers en onderleveranciers, in wisselende samenstellingen, in hoog tempo toenemen.

Voornoemde trend kan worden bezien in combinatie met de eerder in dit beeld benoemde nieuwe digitale regelgeving, zoals die vanuit Europa. Het aantal als essentiële dienst benoemde organisaties gaat daardoor toenemen, evenals het aantal digitale leveranciers dat die organisaties weer bedient. De geschetste trend brengt met zich mee dat er een toenemende kans bestaat dat dienstverleners en hun toeleveranciers of partners actief zijn in meerdere digitale ecosystemen die aan meerdere sectoren raken.

Eerder schetsten we in dit inspectiebeeld dat het voor de cybersecurity van vitale dienstverleners nodig is om dieper te kijken dan de dienst zelf. We stelden dat het noodzakelijk is dat vitale dienstverleners zich goed rekenschap geven van de keten die hen bedient, want Supply Chain Management is een wezenlijk onderdeel van cybersecurity. Tevens schetsten we de daarbij de uitdaging voor toezichthouders om op een dieper niveau in de keten actief toezicht uit te oefenen, ook al worden daar risico's gezien. Door de geschetste trend wordt die uitdaging complexer als de gelaagdheid van onderliggende dienstverlening toeneemt en zich daarbij tevens uitspreidt over meerdere ecosystemen en daarmee sectoren. Dan kan een relatief klein incident bij één partij meerdere cruciale processen elders en zelfs andere sectoren raken.

Het vanuit het toezicht detecteren en adresseren van zich snel ontwikkelende en manifesterende risico's in het perspectief van deze trend is de uitdaging voor de komende jaren. Het dwingt toezichthouders niet alleen zelf inzicht en overzicht te krijgen over ketens, maar ook om samen te werken met elkaar en sterker de verbinding te zoeken met publieke en private stakeholders. Een goede samenwerking draagt bij aan het mitigeren van risico's in een snel veranderende wereld.

[11] Wetenschappelijke Raad voor het Regeringsbeleid, *Voorbereiden op digitale ontwrichting*, p.19, Den Haag 2019.

Bijlage:
Toezichtresultaten per toezichthouder

Toezichthouder: Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Geen		Nucleaire sector	Regeling beveiliging nucleaire inrichtingen en splijtstoffen	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligingsbeheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
X	X	X	X	X
Aanleiding:	Alle bedrijven die onder toezicht staan van de ANVS binnen de Nucleaire sector hebben op basis van de eerder uitgevoerde analyse van de digitale weerbaarheid (in 2020) verbeterplannen opgesteld. Doel van deze verbeterplannen is het versterken van de onderliggende processen en het aantonen en/of verbeteren van de praktijkwerking (validatie, testen, oefenen). Hiermee moet het optreden van kwetsbaarheden zoveel als mogelijk worden voorkomen en het moet leiden tot een toename van de (gemeten) digitale weerbaarheid in 2021. Deze wordt uitgedrukt in volwassenheids-niveaus. Deze activiteiten betreffen alle domeinen van het NIST framework.			
Status onderzoek:	De ANVS heeft alle verbeterplannen beoordeeld en houdt toezicht op de voortgang en implementatie van deze plannen. Het onderzoek is afgerond.			
Algemeen beeld:	De ANVS heeft drie fysieke inspecties en vijf administratieve inspecties uitgevoerd (in verband met Corona restricties waren fysieke inspecties niet mogelijk). Vijf inspecties hebben geen doorgang kunnen vinden in verband met Corona restricties en bezetting. Het algemene beeld van de ANVS is dat voortdurend verbeteren wordt toegepast. Bij een aantal bedrijven is de digitale weerbaarheid aantoonbaar significant toegenomen. Uitdagingen die door sector worden ervaren zijn onder meer gekwalificeerd personeel werven en behouden en externe leveranciers; het beveiligen van de informatie en het beheersen van de toegang tot deze informatie.			
Interventie:	Gebleken is dat het uitvoeren van inspecties leidt tot verbeteringen. Naar aanleiding van de bevindingen en de gesprekken zijn processen en maatregelen aangescherpt of verbetert alle onder toezichtstaanden voldoen aan het wettelijk kader en daarmee aan hun zorgplicht. Er zijn geen interventies gedaan.			
Relatie met andere toezichthouder:	Niet van toepassing in 2021, in het komende jaar 2022 gaat de ANVS samenwerken met het Agentschap Telecom bij de Kerncentrale Borssele (deze is naast nucleair bedrijf ook energieleverancier wat onder de WBNI valt).			

Toezichthouder: Agentschap Telecom (AT)				
Vitaal proces:		**Sector:**		**Grondslag:**
• Landelijk en regionaal transport en distributie elektriciteit • Gasproductie, landelijk en regionaal transport en distributie gas • Olievoorziening • Internettoegang en datadiensten		Energie en Digitale Infrastructuur		NIB
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatie-beveiligingsbeheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Alle beheers-maatregelen	Alle beheers-maatregelen	Alle beheers-maatregelen	Alle beheers-maatregelen	Alle beheersmaatregelen
Aanleiding:	Iedere 2 jaar wordt de reguliere inspectie uitgevoerd bij deze AED's. Hiervoor vult de AED een self assessment gebaseerd op de ISO27001 in inclusief een volwassenheidsscore. De self assessment raakt alle beheersmaat-regelen voor de 5 domeinen van het Bbni. Hiermee wordt een totaalinzicht omtrent de digitale weerbaarheid van de sector verkregen. Agentschap Telecom toetst of de self assessment juist en volledig is ingevuld.			
Status onderzoek:	Afgerond.			
Algemeen beeld:	In 2021 is voor het eerst de self assessment uitgezet bij 10 AED's. De AED's hebben in de self assessment 44 beheersdoelstellingen toegelicht en voorzien van een volwassenheidsniveau. Middels een deelwaarneming op 5 van de 44 beheersdoelstellingen valt het op dat de self assessments kritisch en grotendeels juist en volledig door de AED's zijn ingevuld. Daar waar nodig zijn reeds verbetertrajecten gestart. Dit betreft enkele beheers-doelstellingen per sector en over het algemeen is de opzet van beheersmaatregelen gedocumenteerd en worden deze op gestructureerde en geformaliseerde wijze uitgevoerd.			
Interventie:	Agentschap Telecom heeft tijdens haar inspecties de resultaten besproken met de AED's. Dit heeft geleid tot aanscherpingen en verbeteringen in de verantwoording in de self assessments. De deelwaarneming heeft geen bevinding van overtreding van de zorgplicht opgeleverd. De inhoudelijke resultaten van de self assessments gebruikt AT voor de verdere invulling van haar toezicht. Dit betekent onder meer dat verbeteringen worden gemonitord in accountgesprekken en dat de resultaten worden verwerkt in de analyses voor de prioritering in komende inspecties.			
Relatie met andere toezichthouder:	ACM.			

Toezichthouder: Agentschap Telecom (AT)				
Vitaal proces:		**Sector:**		**Grondslag:**
• Productie van elektriciteit		Energie		Wbni (NIB)
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Alle beheersmaatregelen	Alle beheersmaatregelen	Alle beheers-maatregelen	Alle beheers-maatregelen	Alle beheersmaatregelen
Aanleiding:	Sinds 1 juni 2021 zijn 22 elektriciteitsproducenten aangewezen als Aanbieder van een Essentiële Dienst (AED). Direct na de zomer is AT gestart met de toezichtcyclus. De eerste stap daarin is het voeren van kennismakings-gesprekken met deze partijen. Het doel is om inzicht te krijgen wat voor een organisatie het is, wat de toekomst-visie van AED op ontwikkelingen binnen de energiemarkt is en hoe op bestuursniveau met cybersecurity wordt omgegaan. Aanvullend vindt op basis van een tweetal vragenlijsten en een interview een verdieping plaats. Doel hiervan is meer begrip van het bedrijf te krijgen en te inventariseren hoe de organisatie omgaat met de beveiliging van netwerk- en informatiesystemen in het kader van de zorgplicht. Dit geeft een eerste indruk van de weerbaar-heid van de desbetreffende elektriciteitsproducent.			
Status onderzoek:	Naar verwachting in Q2 2022 afgerond dit vanwege vertragingen van afspraken door Covid.			
Algemeen beeld:	Na de aanwijzing door MinEZK is Agentschap Telecom in september 2021 gestart met de inventarisatie van de elektriciteitsproducenten onder andere door kennismakingsgesprekken te voeren op directie -en bestuursniveau met de AED's. Deze gesprekken zijn goed verlopen. Tijdens de gesprekken is de waardering uitgesproken dat Agentschap Telecom als toezichthouder proactief op locatie gesprekken gevoerd heeft en dat er constructieve dialoog gevoerd wordt. Vervolgens zijn verdergaande inventarisatiegesprekken gevoerd met verantwoordelijke personen op het gebied van cybersecurity. De gesprekken vonden plaats op basis van een tweetal opgestelde vragenlijsten. De eerste indruk van de gevoerde gesprekken tot op heden is dat het belang van cybersecurity bevestigd wordt door de diverse AED's. De aangewezen elektriciteitsproducenten verschillen onderling van elkaar zowel in omvang, maar ook in besturing. Dit varieert van zelfstandige tot internationale besturing vanuit het moederbedrijf uit het buitenland. Daarnaast constateren we dat de AED's in deze categorie verschillende strategieën hanteren als het gaat om beheersing van processen en diensten. Waarbij sommige zelf zoveel mogelijk in beheer willen hebben of dat ze juist zoveel mogelijk willen uitbesteden aan derden. Een aantal AED's beschikken op dit moment nog niet over een Information Security Management Systeem (ISMS) maar hebben de plannen toegelicht om dit op korte termijn te implementeren. Enkele AED's die internationaal opereren vallen ook in andere landen onder de kaders van de NIB richtlijn en staan onder toezicht van buitenlandse collega-toezichthouders. Dit werpt de noodzaak voor internationale afstemming en samenwerking op.			
Interventie:	De kennismaking- en inventarisatiefase heeft geleid tot een breed risicobeeld van deze categorie AED's. Zij hebben laten zien welke verbeteringen en aandachtspunten de nieuwe wetgeving met de zorgplicht voor hen heeft geïntroduceerd. Dit heeft reeds geleid tot de start van diverse projecten, het aanwijzen van projectleiders, gap-analyses en diverse verbeteracties. Hiermee is het eerste effect van het toezicht van AT via de Wbni in beeld. Uit de gesprekken wordt nogmaals bevestigd het belang van de onderwerpen als riskmanagement en supply chain management. In 2022 gaat AT ook aan de hand van thema toezicht aandacht besteden aan de onderwerp supply chain management. Agentschap Telecom neemt de inhoudelijke resultaten uit deze fase mee als input voor de invulling van de risico-gerichte toezichtprogrammering voor deze categorie.			
Relatie met andere toezichthouder:	ANVS (voor Kerncentrale Borssele). Buitenlandse toezichthouders (internationale AED's). O.a. DE en DK.			

Toezichthouder: Agentschap Telecom (AT)				
Vitaal proces:		**Sector:**		**Grondslag:**
• Spraakdienst en SMS • Internet en dataverkeer		ICT/Telecom Digitale Infrastructuur		Tw (EECC)
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Risicomanagement	-	Detectie, Logging en Monitoring	Incidenten-beheer	Incidentenonderzoek
Aanleiding:	Telecom Security (bereikbaarheid 112), Incidentonderzoek, samen met IGJ en IJenV. AT heeft in zijn reguliere toezicht bij KPN de voortgang van het actieplan en de implementatie van de aanbevelingen uit het onderzoek “Onbereikbaarheid van 112 op 24 juni 2019” gemonitord.			
Status onderzoek:	Afgerond.			
Algemeen beeld:	KPN heeft aangegeven dat alle aanbevelingen zijn overgenomen en grotendeels zijn uitgevoerd. Een deel hiervan is vertraagd als gevolg van Covid en andere prioriteiten. AT constateert op basis hiervan dat er belangrijke stappen zijn gezet om de robuustheid van het 112- en telefonienetwerk verder te bevorderen en de kans op herhaling van de telefoniestoring van 24 juni 2019 verder te minimaliseren. Afgesproken is met KPN dat zij de invulling van nog de openstaande aanbevelingen en het actieplan verder oppakt. AT heeft dit in zijn reguliere toezicht in het voorjaar van 2022 opnieuw gemonitord. KPN heeft aangegeven de nog openstaande aanbevelingen en het actieplan verder te hebben ingevuld. Een deel is geïmplementeerd, voor het overige deel loopt dit nog i.v.m. de benodigde langere doorlooptijden. Hiermee is voor AT het specifieke monitoringstraject van het onderzoek afgerond. AT blijft in zijn periodieke toezichtsgesprekken met KPN de verdere implementatie monitoren.			
Interventie:	Gesprek met KPN over de voortgang van de implementatie van de aanbevelingen.			
Relatie met andere toezichthouder:	In dit onderzoek is samengewerkt met IJenV en IGJ waarbij iedere toezichthouder vanuit zijn eigen toezichtdomein heeft gehandeld. IJenV was de trekker van het onderzoek. De drie inspecties hebben in het verleden vaker gezamenlijk onderzoeken uitgevoerd.			

Toezichthouder: Agentschap Telecom (AT)				
Vitaal proces:		**Sector:**		**Grondslag:**
• Spraakdienst en SMS • Internet en dataverkeer		ICT/Telecom Digitale Infrastructuur		Tw
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Risicomanagement	BBGT	Detectie, Logging en Monitoring	Incidenten-beheer	Incidentenonderzoek
Aanleiding:	Telecom Security (Bevoegd aftappen). Naar aanleiding van berichtgeving in de Volkskrant van 17 april 2021 dat een leverancier in 2010 ongeautoriseerde toegang zou hebben tot systemen van KPN doet Agentschap Telecom onderzoek bij deze telecomaanbieder.			
Status onderzoek:	Lopend.			
Algemeen beeld:	Agentschap Telecom doet onderzoek naar mogelijk ongewenste toegang tot de aftapvoorziening van KPN. Alle systemen en processen die een bijdrage leveren aan de tapvoorziening bij KPN, waaronder de kern van het mobiele netwerk, vallen binnen de focus van het onderzoek. Agentschap Telecom heeft relevante documentatie geanalyseerd en systemen onderzocht. Ook zijn inspecties uitgevoerd bij meerdere datacenters en heeft Agentschap Telecom onder meer aspecten als fysieke beveiliging, logische toegangsbeveiliging, logging en monitoring nader onderzocht. Aan dit onderzoek verleent KPN volledige medewerking. De technische complexiteit en het belang van een zorgvuldig proces maken dat de afronding van dit onderzoek nog enige tijd vraagt.			
Interventie:	-			
Relatie met andere toezichthouder:	-			

Toezichthouder: Agentschap Telecom (AT)				
Vitaal proces:		**Sector:**		**Grondslag:**
• Identificatie en authenticatie van burgers en bedrijven		Vertrouwensdiensten		NIB / eIDAS
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
-	-	Detectie, Logging en Monitoring	-	-
Aanleiding:	Sinds 2020 is identificatie op afstand (IoA) is niet meer weg te denken uit het ecosysteem van vertrouwensdiensten. In lijn met de digitale transformatie, nog versterkt door de Covid-crisis, is de behoefte aan slimme technologische identificatie-methoden, al dan niet voorzien van een AI component, alleen maar toegenomen. Naar een bijzondere toepassing van AI-technologie binnen een operationele IoA-oplossing is in 2021 een specifiek onderzoek gestart. Met deze casus heeft AT concrete ervaring opgedaan in het opstellen van regulering- en toezichtkaders en kan vaardigheid en kennis hierover worden uitgebouwd.			
Status onderzoek:	Afgerond			
Algemeen beeld:	Steeds meer aanbieders melden wijzigingen in hun vertrouwensdiensten t.g.v. de inzet van IoA.			
Interventie:	Elke casus wordt op zijn eigen merites beoordeeld a.d.h.v. de eIDAS-eisen, het regulering- en toezichtkader en EU-erkende technische standaarden.			
Relatie met andere toezichthouder:	Toezichthouders Vertrouwensdiensten in Lidstaten waar de betreffende aanbieder eveneens actief is.			

Toezichthouder: De Nederlandsche Bank (DNB)				
Vitaal proces:		**Sector:**		**Grondslag:**
• Betalings- en effectenverkeer		Financiële sector		NIB / eIDAS
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Art. 1:24 Wet Financieel Toezicht (Wft) NIB / Wbni**
Operationele en IT risico's	Operationele en IT risico's	Operationele en IT risico's	Operationele en IT risico's	Operationele en IT risico's
Aanleiding:	Cyberrisico's staan hoog op de agenda van de belangrijkste instellingen voor de vitale processen betalings- en effectenverkeer (samen 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 gestructureerde vragenlijsten, onderzoeken, inspecties, en gesprekken 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. Daarnaast bestaat er een beeld van de cyber beheersing bij instellingen via gestructureerde vragenlijsten over IT risico's die jaarlijks door instellingen worden ingevuld. DNB voert tevens zelfstandig, alsmede ten behoeve van het Single Supervisory Mechanism (SSM) van de ECB, inspecties uit bij onder toezicht staande instellingen. Voor de periode 2022-2024 heeft de ECB een werkprogramma vastgesteld voor het toezicht op IT risico's waarin DNB sterk betrokken is. Cyber security krijgt hierin een hoge prioriteit. Tevens coördineert DNB cyber resilience surveys die door de ECB uitgezet zijn bij Europese Financial Market Infrastructures voor wat betreft de Nederlandse instellingen.			
Status onderzoek:	Surveys en questionnaires worden elk jaar opgevraagd bij instellingen. De informatie hieruit wordt ingezet voor risico gebaseerd toezicht en kan tevens een aanleiding vormen voor gerichte onderzoeken of inspecties die doorlopend van aard zijn.			
Algemeen beeld:	Uit de uitgevoerde onderzoeken zijn een drietal hoofdthema's naar voren gekomen. **1. Risicomanagement gericht op informatiebeveiliging behoeft verbetering.** De risicomanagementcyclus gericht op informatiebeveiliging kan doorgaans verbeterd worden omdat: I) zij geen onderdeel uitmaakt van het overkoepelende risicomanagement raamwerk van de instelling, II) de gebruikte scenario analyses niet langer aansluiten op het snel veranderende dreigingsbeeld, en III) de effectiviteit van de mitigerende maatregelen moeilijk meetbaar is. Een positieve connotatie hierbij is dat cyberrisico's steeds vaker als belangrijk risico worden onderkend op bestuursniveau van financiële instellingen. **2. Beheersen van informatiebeveiliging in ketens vereist meer aandacht.** Instellingen moeten aantoonbaar controleren, monitoren en meten in hoeverre dienstverleners en onderaannemers hun afspraken nakomen op het gebied van informatiebeveiliging, cybersecurity en business continuïteit. Gebleken is dat niet alle instellingen de juiste risicomanagementprocessen hebben ingeregeld rondom hun dienstverleners. Daarnaast is vastgesteld dat het bij de onderzochte instellingen soms ontbreekt aan een volledig inzicht in de beheersmaatregelen bij dienstverleners en eventuele onderaannemers die zijn betrokken in de uitbestedingsketen. Deze waarnemingen kunnen cyberrisico's opleveren voor instellingen, immers door uitbesteding worden instellingen blootgesteld aan het aanvalsoppervlak van de dienstverlener. Steeds vaker blijkt dat gerichte cyberaanvallen op organisaties en bedrijven starten bij een dienstverlener van de financiële instelling. **3. De weerbaarheid tegen cyberaanvallen moet worden versterkt.** Enerzijds zien we verbeteringen onder andere door goede processen en procedures maar anderzijds zijn er nog veel risico's op het gebied van cyber hygiëne zoals I) volwassenheid van vulnerability & patch management, II) beheersing van End-Of-Life systemen, en cyber resilience: III) testen op basis van een risico analyse om zwakheden op te sporen. Ten aanzien van vulnerability & patch management is inzicht in mogelijke kwetsbaarheden in IT-systemen, en de risico inschatting van deze kwetsbaarheden, een proces dat meer aandacht verdient. In veel gevallen is hierbij sprake van het niet hebben van een goed overzicht van de belangrijkste IT-middelen (IT-assets) of een goed inzicht in de mogelijke (cyber)kwetsbaarheden daarvan. Een connotatie hierbij is dat wanneer er kwetsbaarheden naar buiten komen met een zeer hoog risicoprofiel, zoals bij de Log4J kwetsbaarheid, instellingen weliswaar zeer snel reageerden maar het tegelijkertijd complex was om vast te stellen hoe kwetsbaar zij waren als gevolg van onduidelijkheid rondom de aanwezigheid van Log4J in actieve IT-assets.			

Toezichthouder: De Nederlandsche Bank (DNB)	
	Ten aanzien van het testen is het voor instellingen van belang om periodiek de cyberweerbaarheid te testen op basis van een risicoanalyse en actuele cyberdreigingen met als doel zwakheden op te sporen en de mogelijke impact inzichtelijk te maken. Het TIBER-NL programma van DNB dat al enkele jaren in samenwerking met de financiële sector deze testen faciliteert is hier een voorbeeld van. Tenslotte blijft response en recovery een blijvend aandachtsgebied voor de financiële sector in het kader van weerbaarheid tegen cyberaanvallen. Reguliere business continuity en recovery plannen die zijn opgezet om zeer snel te kunnen herstellen van scenario's zoals stroomuitval of brand zullen door instellingen wellicht uitgebreid moet worden om effectief te kunnen zijn bij grootscheepse cyberaanvallen zoals een ransomware aanval.
Interventie:	De uitkomsten van surveys en questionaires worden o.a. gebruikt om aanvullende toezichtinstrumenten zoals gerichte inspecties en onderzoeken in te zetten. Bevindingen van een onderzoek of inspectie worden in een rapport aan het bestuur van een instelling gecommuniceerd. Voor de opvolging van bevindingen wordt van instellingen verwacht een plan met acties en daaraan gekoppelde tijdslijnen te overleggen. De opvolging van een dergelijk actieplan wordt gemonitord middels voortgangsgesprekken via regulier toezicht.
Relatie met andere toezichthouder:	DNB werkt in de uitvoering van haar toezicht actief samen met de Europese Centrale Bank (ECB), nationale toezichthouders in Europa inzake het toezicht op financiële instellingen, alsmede met de Autoriteit Financiële Markten (AFM).

Toezichthouder: Inspectie Gezondheidszorg en Jeugd (IGJ)				
Vitaal proces:		**Sector:**		**Grondslag:**
• Zorg		Ziekenhuiszorg Verpleeghuiszorg Geestelijke gezondheidszorg		Wet kwaliteit klachten en geschillen zorg; Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
-	Inrichting van een managementsysteem voor informatiebeveiliging	-	-	-
Aanleiding:	De IGJ ziet dat zorgaanbieders steeds afhankelijker worden van ICT. Er komen steeds meer ICT-toepassingen die de zorg ondersteunen (e-health). Behalve dat vrijwel alle zorgaanbieders gebruik maken van een elektronisch patiëntendossier, speelt ook elektronische gegevensuitwisseling een belangrijke rol. Ook andere toepassingen nemen een vlucht, waardoor zorg op afstand mogelijk wordt. Denk aan elektronische consulten, monitoring op afstand of dossierinzage via patiëntportalen. De IGJ besteedt al enige tijd aandacht aan deze ontwikkelingen, omdat goede zorg vereist dat zorgaanbieders ook bij inzet van e-health zorgen voor de juiste randvoorwaarden. Een van die randvoorwaarden is informatiebeveiliging. Zorgaanbieders zijn op basis van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg verplicht om een managementsysteem voor informatiebeveiliging in te richten conform NEN 7510. De afgelopen jaren voerde de IGJ inspectiebezoeken uit in meerdere deelsectoren van de zorg, waarbij de mate van voldoen aan de NEN 7510 een van de aandachtspunten was. Het gaat o.a. om ziekenhuizen, verpleeghuizen en aanbieders van geestelijke gezondheidszorg.			
Status onderzoek:	In 2020 heeft de inspectie over deze inspectiebezoeken een drietal factsheets gepubliceerd. De inspectie blijft ook in de toekomst aandacht besteden aan de toepassing van e-health in de zorg, waaronder het aspect informatie-beveiliging.			
Algemeen beeld:	De IGJ bezocht tussen 2017 en 2021 voor dit thema 22 ziekenhuizen, 14 ggz-instellingen en 10 V&V-instellingen. Daarbij vroeg de inspectie naar een recente onafhankelijke beoordeling van het managementsysteem voor informatiebeveiliging, die op grond van de norm NEN 7510 met regelmaat moet worden uitgevoerd. Zonder een objectieve controle op de werking van de maatregelen is de informatiebeveiliging niet geborgd. Alle ziekenhuizen hebben een vorm van informatiebeveiligingsbeleid en hebben beveiligingsmaatregelen ingezet. Echter, de meerderheid van de bezochte ziekenhuizen kon op het *moment van het inspectiebezoek* niet duidelijk maken hoe effectief het informatiebeveiligingsbeleid was en hoe gewerkt werd aan verbetering. Ziekenhuizen die op het moment van het inspectiebezoek hun informatiebeveiliging niet op orde hadden, konden na het uitvoeren van verbeterplannen alsnog aantoonbaar aan de NEN7510 norm voldoen. Wel kon het na het inspectiebezoek soms lang duren voordat een ziekenhuis voldoende verbeteringen had doorgevoerd om dit te bereiken. Meer dan de helft van de ziekenhuizen had of haalde na het inspectiebezoek een certificaat van een onafhankelijke partij. Dit betekent dat een onafhankelijke deskundige deze ziekenhuizen regelmatig controleert op de naleving van de norm voor informatiebeveiliging. De inspectie ziet in de ggz vaker zorgaanbieders met een NEN-7510-certificaat dan in andere sectoren. Ruim de helft van de bezochte zorgaanbieders had op het moment van het inspectiebezoek al een certificaat. Er zijn echter als het gaat om informatiebeveiliging net als bij ziekenhuizen grote verschillen in niveau tussen zorgaanbieders in de ggz. Ongeveer een derde van de bezochte zorgaanbieders in de ggz had nog geen onafhankelijke beoordeling van de informatiebeveiliging. Het kostte deze partijen na het bezoek langer dan een jaar om hun informatiebeveiliging op voldoende niveau te krijgen. Soms bestond het informatiebeveiligingsbeleid ten tijde van het inspectiebezoek nog vooral op papier. Geen van de zorgaanbieders in de verpleeghuiszorg had bij het inspectiebezoek al een onafhankelijke beoordeling van het managementsysteem voor informatiebeveiliging. Daarmee was het beeld in deze sector minder goed dan bij ziekenhuizen of in de ggz. Nadat (na de inspectiebezoeken) alsnog een onafhankelijke beoordeling was gedaan, bleek vaak dat de zorgaanbieder de eigen risico's niet genoeg in beeld had. Ook moesten de meeste zorgaanbieders nog veel beveiligingsmaatregelen invoeren of verbeteren. Alle bezochte zorgaanbieders wisten na het inspectie-bezoek duidelijke verbeteringen door te voeren. Daarbij richtten zij aantoonbaar een kwaliteitscyclus in. Een aantal zorgaanbieders haalde zelfs een certificaat. Als het onderwerp voldoende aandacht krijgt, kan een zorgaanbieder op dit punt dus sterk verbeteren.			

Toezichthouder: Inspectie Gezondheidszorg en Jeugd (IGJ)	
Interventie:	Bij zorgaanbieders die niet beschikten over een onafhankelijke beoordeling van het managementsysteem voor informatiebeveiliging, vroeg de inspectie de zorgaanbieder hiervoor alsnog te zorgen. Indien uit de resultaten bleek dat de informatiebeveiliging onvoldoende op orde was, vroeg de inspectie de zorgaanbieder om een verbeterplan, gevolgd door een nieuwe onafhankelijke beoordeling. Dit leidde in alle gevallen tot aantoonbare verbetering, al was hier bij zorgaanbieders die nog veel beheersmaatregelen moesten inrichten wel veel tijd voor nodig (in meerdere gevallen langer dan een jaar).
Relatie met andere toezichthouder:	De Autoriteit Persoonsgegevens houdt in het kader van de Algemene Verordening Gegevensbescherming ook toezicht op de informatiebeveiliging en hanteert hierbij eveneens de NEN 7510 als uitgangspunt. De focus ligt hierbij op bescherming van persoonsgegevens, terwijl de IGJ vooral naar informatiebeveiliging kijkt vanuit het perspectief van kwaliteit en continuïteit van zorg. AP en IGJ hebben een samenwerkingsovereenkomst en wisselen zo nodig informatie uit.

Toezichthouder: Inspectie Justitie en Veiligheid (IJenV)				
Vitaal proces:		**Sector:**		**Grondslag:**
• Communicatie met en tussen hulpdiensten middels 112 en C2000.		Openbare orde en veiligheid		Wet beveiliging netwerk- en informatie-systemen, VIR, BIO.
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken.**
-	Het inrichten en borgen van risicomanagement op de informatiebeveiliging van meldkamersystemen	-	-	-
Aanleiding:	De meldkamer is het eerste contact met de hulpdiensten van de brandweer, ambulance, politie en de Koninklijke Marechaussee (KMar) voor mensen die 112 bellen. Andersom krijgen de hulpdiensten via de meldkamers informatie over een incident waar hun hulp bij wordt gevraagd. Meldkamers zijn ook cruciaal bij rampenbestrijding, crisisbeheersing, opsporing en handhaving van de openbare orde. Het is dan ook van belang dat zij onverminderd bereikbaar blijven en dat ze goed beschermd blijven tegen toenemende digitale aanvallen. Hierbij schakelen criminelen computersystemen uit en eisen losgeld. Goede beveiliging zorgt ervoor dat hulpverleners bij informatie in de meldkamersystemen kunnen komen wanneer ze dat willen, dat de informatie klopt en dat de informatie niet bij anderen terecht komt. Dan kan het gaan om informatie over meldingen en van hulpdiensten die onderling met elkaar in contact zijn. Het is dan ook van essentieel belang dat het bestuur van de Landelijke meldkamersamenwerking (LMS) door risicomanagement de digitale risico's voor de meldkamersystemen inschat om deze tot een aanvaardbaar niveau te reduceren.			
Status onderzoek:	Afgerond			
Algemeen beeld:	Uit het onderzoek van de Inspectie JenV blijkt dat de landelijke meldkamersamenwerking nog onvoldoende in staat is om digitale risico's te signaleren en tot een aanvaardbaar niveau te reduceren. De LMS is hierdoor onvoldoende weerbaar tegen de toenemende dreiging van verstoring. Dit is een risico voor de veiligheid van de meldkamersystemen en daarmee voor de continuïteit van de meldkamers als onderdeel van de vitale infrastructuur van Nederland. Vanwege de ernst van de situatie is een strakke aansturing nodig. Meldkamers moeten hun beveiliging aanscherpen uit voorzorg tegen digitale aanvallen. Wanneer de systemen van meldkamers verstoord raken, zijn de hulpdiensten niet goed bereikbaar. De Inspectie JenV concludeert dat de hulpverlening, crisisbeheersing en opsporing dan gevaar lopen. Volgens de Inspectie JenV moet het bestuur van de meldkamers prioriteit geven aan het in kaart brengen van cyberrisico's en hoe die aan te pakken. Volgens de Inspectie JenV is het daarom van belang dat meldkamers voortdurend op de hoogte blijven van de specifieke risico's voor hun computersystemen en de mogelijke gevolgen hiervan. Hoewel de ICT-afdeling beveiligingsmaatregelen treft, gebeurt dat nu niet op basis van een zo volledig mogelijk en actueel inzicht in de digitale risico's. Het bestuur van de meldkamers moet daarom serieus de beveiliging van de meldkamersystemen gaan aansturen. Het ministerie van Justitie en Veiligheid moet samen met de meldkamers goed kijken naar de verantwoordelijkheden voor de meldkamersystemen. Dit zodat de beveiliging in de praktijk beter uitvoerbaar wordt. De Inspectie JenV vindt de continuïteit van de meldkamers al jarenlang een zorgpunt. Ook in 2021 vroeg zij, samen met Agentschap Telecom, aandacht hiervoor.			
Interventie:	Onderzoek met rapportage, aansluitend bestuurlijk gesprek. Op basis daarvan zijn de volgende maatregelen toegezegd: • Het Bestuurlijk meldkamerberaad zal risicomanagement op de informatiebeveiliging van de meldkamersystemen inrichten en toepassen en dit onderbrengen binnen het eigen normenkader. • Het Bestuurlijk meldkamerberaad stelt hiertoe een uitvoeringsplan op met herkenbare stappen. De Inspectie en het AT gaan toezien op het uitvoeren van de gedane toezeggingen voor verbetering. • De Inspectie monitort de voortgang en het toepassen van het uitvoeringsplan in de periodieke gesprekken van de hoofdinspecteur met de directeur Veiligheidsregio's, crisisbeheersing en meldkamers.			
Relatie met andere toezichthouder:	Agentschap Telecom.			

Toezichthouder: Inspectie Leefomgeving en Transport (ILT)				
Vitaal proces:		**Sector:**		**Grondslag:**
Drinkwatervoorziening		Drinkwater		Wbni (en drinkwaterwet)
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
X	X	X	X	X
Aanleiding:	In 2021 heeft de ILT 'verkennende inspecties' uitgevoerd bij alle drinkwaterbedrijven (m.u.v. Waternet). Doel van deze inspecties was/is om een eerste beeld op te bouwen in hoeverre alle deelonderwerpen zoals benoemd in de Ministeriele Regeling I&W afgedekt worden. De MR dekt alle hierboven benoemde thema's af. Daarnaast is er ook gekeken hoe op bestuursniveau invulling is gegeven aan de besturing van cybersecurity (besturingstoezicht). Scope van de inspecties is de procesautomatisering voor de levering en kwaliteit drinkwater.			
Status onderzoek:	Begin 2022 zijn de laatste inspecties afgerond.			
Algemeen beeld:	In 2021 hebben er inspecties plaatsgevonden bij de drinkwaterbedrijven. De sector is zich bewust van het belang van de beveiliging van dergelijke systemen. De sector heeft zelf (al eerder) een normenkader opgesteld (PA-norm) om de beveiliging van de procesautomatisering drinkwater te vergroten. Er wordt hard gewerkt om dit opgestelde normenkader te implementeren/verbeteren. De ILT heeft daarnaast ook gekeken naar aspecten uit de MR die niet door de PA-norm zijn afgedekt. Nog niet alle drinkwaterbedrijven hebben hun implementatie van een ISMS op orde. Daar waar dit schort ziet de ILT wel verbetertrajecten omdat men zelf de tekortkomingen al geïdentificeerd heeft. Veel bedrijven hanteren de ISO27K als leidraad voor een ISMS waarvan enkelen er ook naar streven hiertegen formeel ge-audit te worden. Een ander aandachtspunt is monitoring/ detectie/incident-response. De sector kijkt hier of bijvoorbeeld een gezamenlijk water-SOC toegevoegde waarde heeft. Over het algemeen kan worden gesteld dat er veel maatregelen zijn geïmplementeerd, maar dat bij individu-ele drinkwaterbedrijven er nog wel verbeterpunten zijn. Borging/vastlegging/beschrijving van maatregelen is een aandachtspunt. Deze individuele aandachtspunten zullen waar nodig worden meegenomen in de inspecties voor 2022.			
Interventie:	Er hebben geen interventies plaatsgevonden. De uitkomsten van deze inspectieronde (en eventuele verbeteringen) zullen worden gebruikt bij de inspecties in 2022.			
Relatie met andere toezichthouder:	Niet van toepassing.			

Toezichthouder: Inspectie Leefomgeving en Transport (ILT)				
Vitaal proces:		**Sector:**		**Grondslag:**
Drinkwatervoorziening		Drinkwater		Wbni (en drinkwaterwet)
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
X	X	X	X	X
Aanleiding:	Begin 2021 heeft de ILT Waternet onder verscherpt toezicht gesteld i.v.m. tekortkomingen in cybersecurity en de aansturing daarop. Tijdens dit toezicht wordt gemonitord of Waternet de benodigde verbeteringen daadwerkelijk realiseert.			
Status onderzoek:	Lopend.			
Algemeen beeld:	In de afgelopen periode heeft Waternet hard gewerkt om diverse tekortkomingen weg te nemen. Waternet heeft een ambitieus verbeterprogramma opgestart en uit de voortgangsrapportages blijkt dat er iedere maand progressie wordt geboekt. Tegelijkertijd wordt ook door de ILT geconstateerd dat er nog veel moet gebeuren, zowel voor het volledig in control komen op de cybersecurity als voor het verbeteren van doeltreffendheid van besturing. In de komende tijd worden nog belangrijke stappen gezet ten aanzien van de (cybersecurity)beheers-maatregelen en het aantonen van de werking (effectiviteit) hiervan.			
Interventie:	Waternet staat onder verscherpt toezicht naar aanleiding van het ILT-onderzoek uit Q4 ’20 , verbeteringen worden periodiek gemonitord. Vanuit de ILT vindt dit plaats door o.a. maandelijkse voortgangsbesprekingen met de directie Waternet, incidentele verdiepingssessies waarbij op (de toestand van) specifieke verbeterthema’s ingegaan wordt en gesprekken met het AGV-bestuur.			
Relatie met andere toezichthouder:	Niet van toepassing.			

Bijlage:
Totaaloverzicht toezicht op cybersecurity

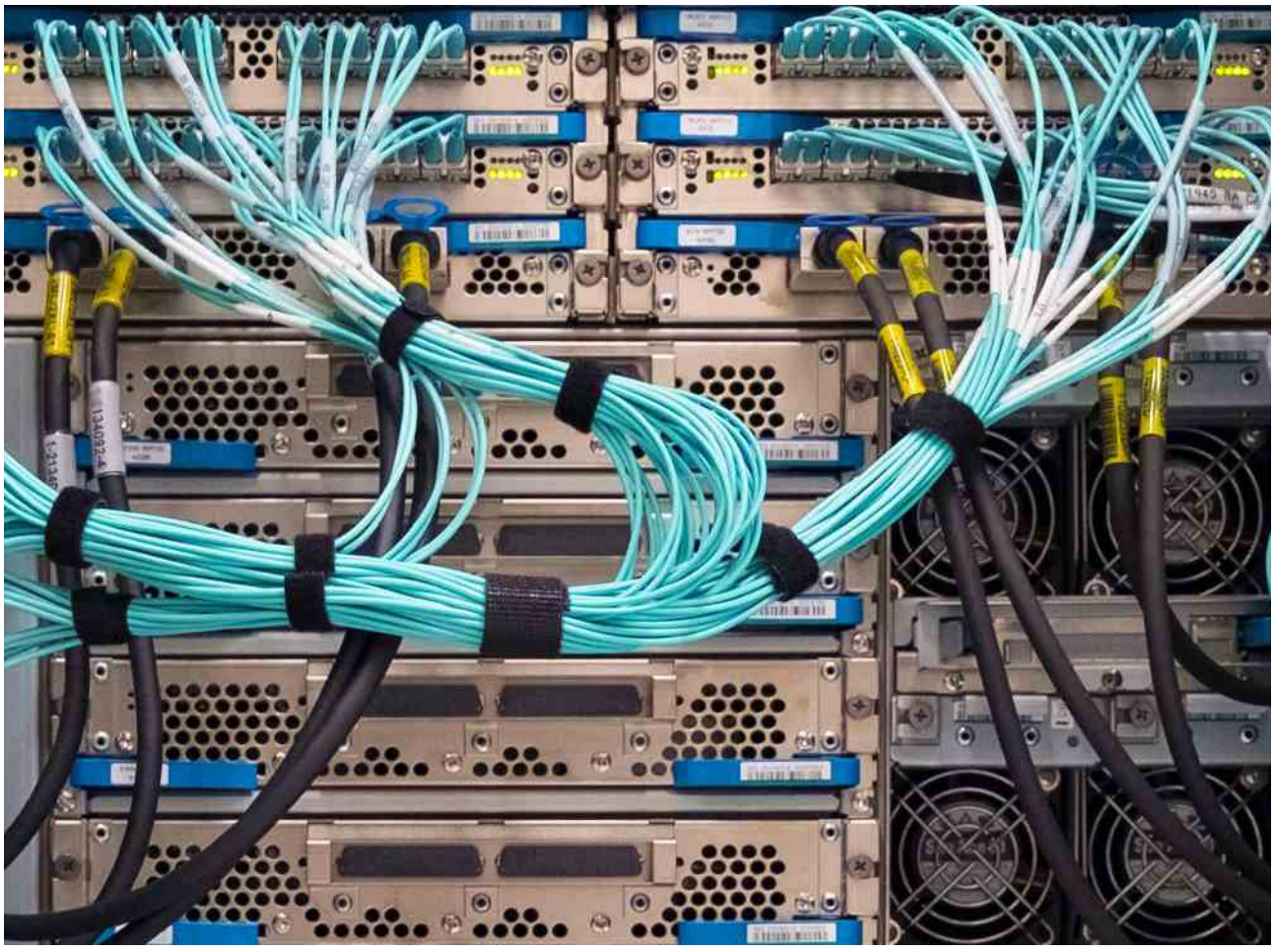
In dit samenhangend inspectiebeeld wordt het begrip 'vitaal' in brede zin toegepast: het gaat hierbij om processen die door vakdepartementen als vitale processen zijn aangemerkt. Een overzicht van deze processen is opgenomen in Tabel A. De aanbieders van een groot deel van deze processen zijn tevens op basis van de Wbni als vitaal aangewezen.

Tabel A. *Totaaloverzicht toezicht op cybersecurity*

Vitaal proces	Sector	Grondslag			Toezichthouder
		NIB	Wbni		
			AED[12]	AAVA[13]	
Landelijk transport en distributie elektriciteit	Energie	X	X		AT
Regionale distributie elektriciteit	Energie	X	X		AT
Gasproductie, landelijk transport en distributie gas	Energie	X	X		AT
Regionale distributie gas	Energie	X	X		AT
Olievoorziening	Energie	X	X		AT
Internet en datadiensten	ICT/Telecom	X	X		AT
Internettoegang en dataverkeer	Digitale infrastructuur	EECC			AT
Spraakdienst en SMS	ICT/Telecom	EECC			AT
Plaats- en tijdsbepaling middels GNSS					-
Drinkwatervoorziening	Drinkwater	X	X		ILT
Keren en beheren waterkwantiteit	Water			X	-[14]
Vlucht- en vliegtuigafhandeling	Transport	X	X		ILT
Scheepvaartafwikkeling		X	X		ILT
Vervoer van personen en goederen over (hoofd)spoorweg-infrastructuur	Transport	X			ILT[15]
Vervoer over (hoofd)wegennet	Transport	X			ILT[16]
Grootschalige productie/verwerking en/of opslag (petro) chemische stoffen	Chemie				Nnb[17]
Opslag, productie en verwerking nucleair materiaal	Nucleair			X	ANVS
Toonbankbetalingsverkeer	Financieel	X	X	X	DNB
Massaal giraal betalingsverkeer	Financieel	X	X	X	DNB
Hoogwaardig betalingsverkeer tussen banken	Financieel	X	X	X	DNB

[12] AED: Aanbieder Essentiële Dienst. Hiervoor geldt de Wbni-zorgplicht en -meldplicht waarop toezicht wordt gehouden.
[13] AAVA: Andere Aangewezen Vitale Aanbieder. Hiervoor geldt alleen een Wbni-meldplicht bij het NCSC en hierop wordt geen toezicht gehouden.
[14] Nog geen toezichthouder aangewezen.
[15] Deze processen zijn (inmiddels) door het betrokken vakdepartement als vitaal aangemerkt; daarbinnen worden de AED's aangewezen. Dit vindt plaats in 2022.
[16] Deze processen zijn (inmiddels) door het betrokken vakdepartement als vitaal aangemerkt; daarbinnen worden de AED's aangewezen. Dit vindt plaats in 2022.
[17] Chemie: Omgevingsdiensten zijn toezichthouder, ILT is tweedelijns toezichthouder. Voor cybersecurity is echter (nog) geen toezichthouder aangewezen.

Vitaal proces	Sector	Grondslag			Toezichthouder
		NIB	Wbni		
			AED[12]	AAVA[13]	
Effectenverkeer	Financieel	X	X	X	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	Vertrouwensdiensten	eIDAS			AT
Inzet defensie	Defensie				-
Gezondheidszorg[18] (**geen** vitaal proces in NL)		X			IGJ



[18] 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.

Dit is een uitgave in opdracht van de werkgroep toezichthouders cybersecurity vitale processen

Voor meer informatie over deze uitgave:

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat
Postbus 450 | 9700 AL | Groningen
communicatie@agentschaptelecom.nl
T +31 (0)50 587 74 44 (ma t/m vrij 8.30 - 17.00)

Juni 2022