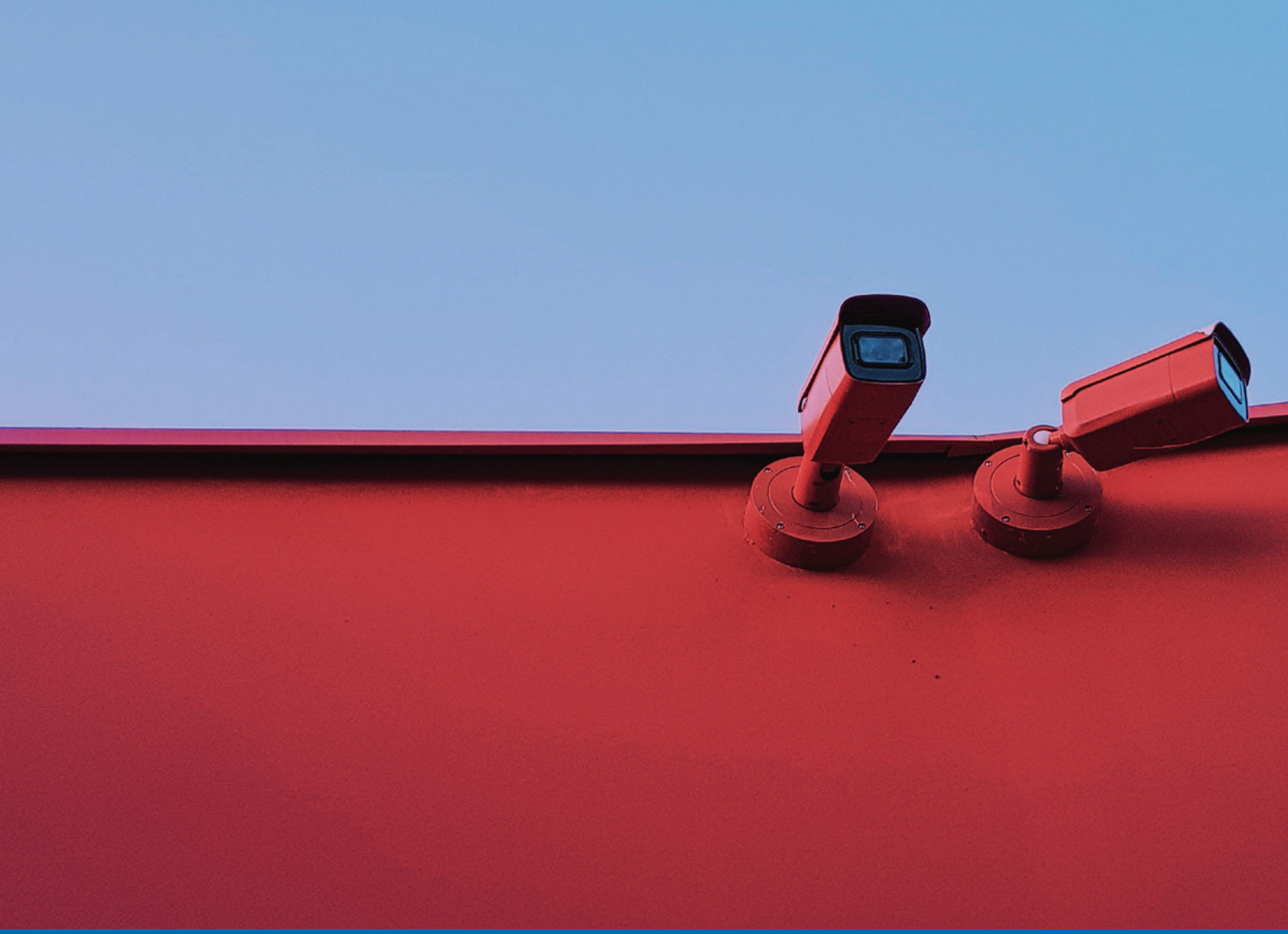


Samenhangend Inspectiebeeld cybersecurity vitale processen

2023

Inhoud

Voorwoord 3

Samenvatting 4

Summary 6

1 Inleiding 8
- 1.1 Aanleiding 9
- 1.2. De betrokken toezichthouders 10
- 1.3. Leeswijzer 12

2 Rode draden vanuit toezichtresultaten 13
- 2.1. Inleiding 14
- 2.2. Risicomanagement blijft speerpunt in cybersecurity 14
  - 2.2.1. Risicomanagement en het belang van een goed ISMS 14
  - 2.2.2 Risicomanagement bij logische toegangsbeveiliging 16
  - 2.2.3 Risicomanagement als middel om te sturen op veranderende dreigingen 19
- 2.3. Meldingen van cybersecurity-incidenten 19

3 Uitdagingen in het toezicht 20
- 3.1. Inleiding 21
- 3.2. Nieuwe Europese richtlijnen voor digitale en fysieke weerbaarheid 21
- 3.3. Samenwerking tussen toezichthouders 23

4 Doorontwikkeling Samenhangend Inspectiebeeld 24
- 4.1. Inleiding 25
- 4.2. Basis voor doorontwikkeling ligt in het jaar 2021 25
- 4.3. Risicomanagement als thema voor 2023 25

bijlage 1 Toezichtresultaten per toezichthouder 26

bijlage 2 Bronnen 41

Voorwoord

Een voorrecht en een uitdaging. Zo ervaar ik toezichthouden op de cybersecurity van essentiële diensten in de samenleving. Een voorrecht omdat het maatschappelijk belang er zo nadrukkelijk mee gediend is. Ook in 2022 hebben wij als bij dit inspectiebeeld betrokken toezichthouders gemotiveerd onze expertise daarop ingezet.

De cybersecurity van de vitale diensten is van cruciaal belang voor een veilige samenleving. Daarbij moet voldoende ruimte zijn voor innovatie en groei. De uitdagingen zijn groot: de ontwikkelingen op het gebied van digitalisering en cybersecurity zijn omvangrijk en voltrekken zich razendsnel. Ook de cyberdreigingen zijn talrijk en nemen snel toe. Dat maakt ons kwetsbaar. Onderdelen van de vitale dienstverlening staan daardoor onder druk.

Toenemende digitalisering en verknoping van digitale diensten bieden ook veel kansen. Tegelijkertijd vragen deze kansen meer van de verschillende partners in het ecosysteem. De ene keer in de rol van afnemer en dan weer in de rol van toeleverancier. Het vraagt een volwassen manier van omgaan met risicomanagement. Zowel in de eigen organisatie als in de supply chain. Geen sinecure, met al die verschillende, digitaal verbonden partners in het systeem. Het Samenhangend Inspectiebeeld 2023, dat gaat over de inspectieresultaten van 2022, geeft daarom een aantal belangrijke aandachtspunten waar organisaties mee aan de slag kunnen om hun risico's beter te beheersen. Een voorbeeld hiervan is de noodzakelijke aandacht voor cyberhygiëne in organisaties.

Ik ben ook blij te zien dat wij als samenwerkende toezichthouders de stap hebben gezet naar een gezamenlijk thema in onze programmering voor 2023, gebaseerd op een meerjarig thema van risicomanagement. Door samen te kijken naar vergelijkbare vraagstukken, in plaats van die apart te benaderen, zetten we een stap in de versterking van gezamenlijk digitaal toezicht. Deze stap is onontbeerlijk in de ontwikkeling van samenwerkend digitaal toezicht de komende jaren. Zeker gezien de aankomende en brede digitale Europese regulering, onder meer op het gebied van AI, data en cybersecurity. Laat de concrete samenwerking van toezichthouders van diverse pluimage rond dit Samenhangend Inspectiebeeld daarin een mooi voorbeeld zijn.

Met vriendelijke groet,
mede namens alle betrokkenen,

Angeline van Dijk
Inspecteur-generaal
Rijksinspectie Digitale Infrastructuur

Samenvatting

De digitale revolutie biedt geweldige kansen voor de samenleving en economie, maar brengt ook risico's voor de vitale infrastructuur van Nederland. Dit vraagt om een adequate cybersecurityaanpak en goed en effectief toezicht hierop. Jaarlijks maken de toezichthouders die sinds de invoering van de NIS en de Wbni samenwerken de ontwikkelingen in het toezicht inzichtelijk in het Samenhangend Inspectiebeeld. Dit document gaat over de inspectieresultaten over het jaar 2022.

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

Dit inspectiebeeld omschrijft de huidige staat per toezichtveld. Het destilleert enkele rode draden vanuit de toezichtresultaten en gaat in op de uitdagingen in het toezicht. Ook wordt ingegaan op de doorontwikkeling van het Samenhangend Inspectiebeeld. De individuele beelden per toezichtveld zijn opgenomen in de bijlage van dit document.

De belangrijkste rode draad op basis van de inspectieresultaten en bevindingen van de toezichthouders is het onderwerp *risicomanagement*. Net als in het jaar 2021 besteedden alle toezichthouders in 2022 aandacht aan dit onderwerp. Mede als gevolg van de inspectiewerkzaamheden kregen verbetertrajecten bij vitale aanbieders een extra stimulans en raakten de organisaties ook op bestuursniveau steeds meer betrokken bij dit onderwerp. Ook zien de toezichthouders dat steeds meer vitale aanbieders zich laten certificeren. Terugkijkend op de aanbevelingen in het voorgaande Samenhangend Inspectiebeeld constateren de toezichthouders dat vitale aanbieders meer aandacht hebben voor bijvoorbeeld de steeds complexere digitale dreigingen in de leverancierskketens.

De toezichthouders zien dat er ruimte is om de cyberhygiëne verder te verbeteren en dat vitale aanbieders hun risicomanagementproces naar een hoger niveau tillen. De toezichthouders hebben gezamenlijk de volgende aandachtspunten vastgesteld voor het verbeteren van risicomanagement:

- het onafhankelijk laten beoordelen van de effectiviteit van het ISMS;
- het verder ontwikkelen en implementeren van beveiligingstesten;
- het zorgdragen voor risicobeheersing binnen het ISMS van het complete ecosysteem van samenwerking en uitbesteding.

De belangrijkste rode draad op basis van de inspectieresultaten en bevindingen van de toezichthouders is het onderwerp risicomanagement.

Risicomanagement kwam in het toezicht ook vaak terug in combinatie met het specifieke onderwerp van risico's in de logische toegangsbeveiliging. Op dit onderwerp gaat de aandacht bij vitale aanbieders vooral uit naar het buitenhouden van onbevoegden in informatiesystemen. Op basis van incidenten en bevindingen in het afgelopen jaar wordt verder ingegaan op een aantal aanvullende onderwerpen binnen het onderwerp logische toegangsbeveiliging: toegang voor eigen medewerkers, toegang voor leveranciers en identificatie van klanten. Vanuit het NCSC wordt in dit inspectiebeeld guidance gegeven over hoe organisaties logische toegangsbeveiliging kunnen versterken.

Met de introductie van de Europese CER- en NIS2-richtlijnen komen de toezichthouders voor verschillende uitdagingen te staan. Voor een aantal toezichthouders en sectoren betekent de komst van de CER dat de reikwijdte van het toezicht zal uitbreiden naar toezicht op de bescherming van fysieke risico's. Onder de NIS2 zal het aantal sectoren en daarmee het aantal entiteiten dat onder toezicht valt, uitbreiden. Tevens komt er een aantal toezichthouders bij die onder de eerste NIS-richtlijn nog geen toezicht hielden. De nieuwe richtlijnen verlangen herinrichting van het toezicht. Tegelijkertijd is sprake van uitbreiding van het takenpakket met als bijkomende uitdaging de krapte op de arbeidsmarkt. Ten tijde van het opstellen van dit inspectiebeeld is het echter nog niet volledig duidelijk hoe (toekomstige) vitale aanbieders aan de gestelde eisen in de richtlijnen kunnen voldoen. Dit geldt ook voor de inrichting van het toezicht.

Mede vanwege de komst van de Europese richtlijnen is de uitvoering van de toezichtstaak steeds meer gebaat bij nationale én Europese afstemming en samenwerking. De NIS2 stelt dat NIS2-toezichthouders nationaal en binnen de EU nauw met elkaar moeten samenwerken, waarbij het belang wordt benadrukt van effectieve samenwerking en informatie-uitwisseling tussen de verschillende toezichthouders. Daarnaast zijn aanbieders en eventuele derde partijen vaak actief in meerdere EU-lidstaten en kunnen incidenten meerdere wettelijke normen raken en daarmee meerdere toezichthouders.

Vooruitkijkend naar het komende jaar hebben de toezichthouders afspraken gemaakt over het uitvoeren van een gezamenlijk thema risicomanagement. Gezamenlijk is de scope en aanpak bepaald voor een eenduidige analyse. Het doel is om, ondanks de verschillende aanpak vanwege beschikbare tijd en capaciteit en uiteenlopende sectorale risico's, kaders en prioriteiten, een meer eenduidig en diepgaander beeld te schetsen op basis van de inspectiewerkzaamheden.

Summary

The digital revolution offers tremendous opportunities for society and the economy. At the same time, however, it also carries risks for the Netherlands' critical infrastructure. It is therefore important to have an appropriate cybersecurity approach in place, accompanied by proper and effective monitoring of it. Each year, the supervisory authorities who have worked together since the introduction of the NIS Directive and the national Network and Information Systems Security Act (Wet beveiliging netwerk- en informatiesystemen, 'Wbni') review the developments in supervision in the Inspection Overview. This document presents the inspection results for 2022.

The collaborating supervisory authorities are: the Authority for Nuclear Safety and Radiation Protection (ANVS), the Dutch Data Protection Authority (DPA), De Nederlandsche Bank (DNB), the Health and Youth Care Inspectorate (IGJ), the Inspectorate of Justice and Security (IJenV), the Human Environment and Transport Inspectorate (ILT) and the Dutch Authority for Digital Infrastructure (RDI), formerly: Radiocommunications Agency Netherlands (AT)).

caused the organisations to become increasingly engaged with this issue, including at board level. The supervisory authorities also observe an increased commitment toward certification among growing numbers of critical providers. Looking back at the recommendations in the previous Inspection Overview, the supervisory authorities note that critical providers are focusing more attention on increasingly complex digital threats in supply chains, for example.

The supervisory authorities conclude that there is scope for further improving cyber hygiene and see that critical providers are taking their risk management process to the next level. The supervisory authorities jointly identified the following focal areas for improving risk management:

- provide for independent assessment of the effectiveness of the ISMS;
- further develop and implement security testing;
- ensure risk management within the ISMS encompassing the entire ecosystem of collaboration and outsourcing.

The principal common theme emerging from the inspection results and findings of the supervisory authorities is that of risk management.

This inspection overview describes the current situation for each area of supervision. It distils several common themes from the supervision results and addresses the challenges in supervision. The further development of the Inspection Overview is also discussed. The individual overviews for each area of supervision are included in the annex to this document.

The principal common theme emerging from the inspection results and findings of the supervisory authorities is that of risk management. As in 2021, all the supervisory authorities paid attention to this issue in 2022. The inspection activities also had the effect of giving an additional impetus to improvement processes at critical providers and

Risk management was also frequently evident in supervision in combination with the specific matter of risks in logical access security. Critical providers' focus with regard to this issue is mainly directed at keeping unauthorised persons out of information systems. Based on incidents and findings in the past year, we discuss in further detail a number of additional issues in relation to the subject of logical access security: access for own staff, access for suppliers and customer identification. This inspection overview includes guidance from the NCSC on how organisations can strengthen logical access security.

The introduction of the CER and NIS2 Directives presents supervisory authorities with a range of different challenges. For a number of supervisory authorities and sectors, the arrival of the CER Directive means that the scope of supervision will expand to include supervision of the protection of physical risks. Under the NIS2 Directive, the number of sectors – and hence the number of entities subject to supervision – will expand. This Directive also sees the addition of a number of supervisory authorities that did not exercise any supervision under the NIS1 Directive. The new Directives will require a reassessment and reorganisation of supervision. At the same time, the range of tasks will expand, accompanied by the additional challenge of a tight labour market. At the time of preparing this inspection overview, however, it is not yet fully clear how critical providers, both now and in the future, can meet the requirements set out in the Directives. The same also applies to how supervision is to be organised.

The introduction of the new European Directives makes it clear that the implementation of the supervisory task increasingly benefits from national as well as European coordination and cooperation. The NIS2 Directive states that NIS2 supervisory authorities should work closely together both nationally and within the EU, with emphasis being given to the importance of effective cooperation and information sharing between different supervisory authorities. In addition, providers and any third parties often operate in multiple EU Member States and incidents can involve several legal standards, and hence several supervisory authorities.

Looking ahead to the coming year, the supervisory authorities have agreed to conduct a joint risk management undertaking. The scope and approach have been jointly determined for an unambiguous analysis. The aim is that, despite different approaches due to available time and capacity and varying sectoral risks, frameworks and priorities, a more unambiguous and in-depth picture be presented based on the inspection activities.

1 Inleiding

foto: Evert-Jan Daniels

1.1 Aanleiding

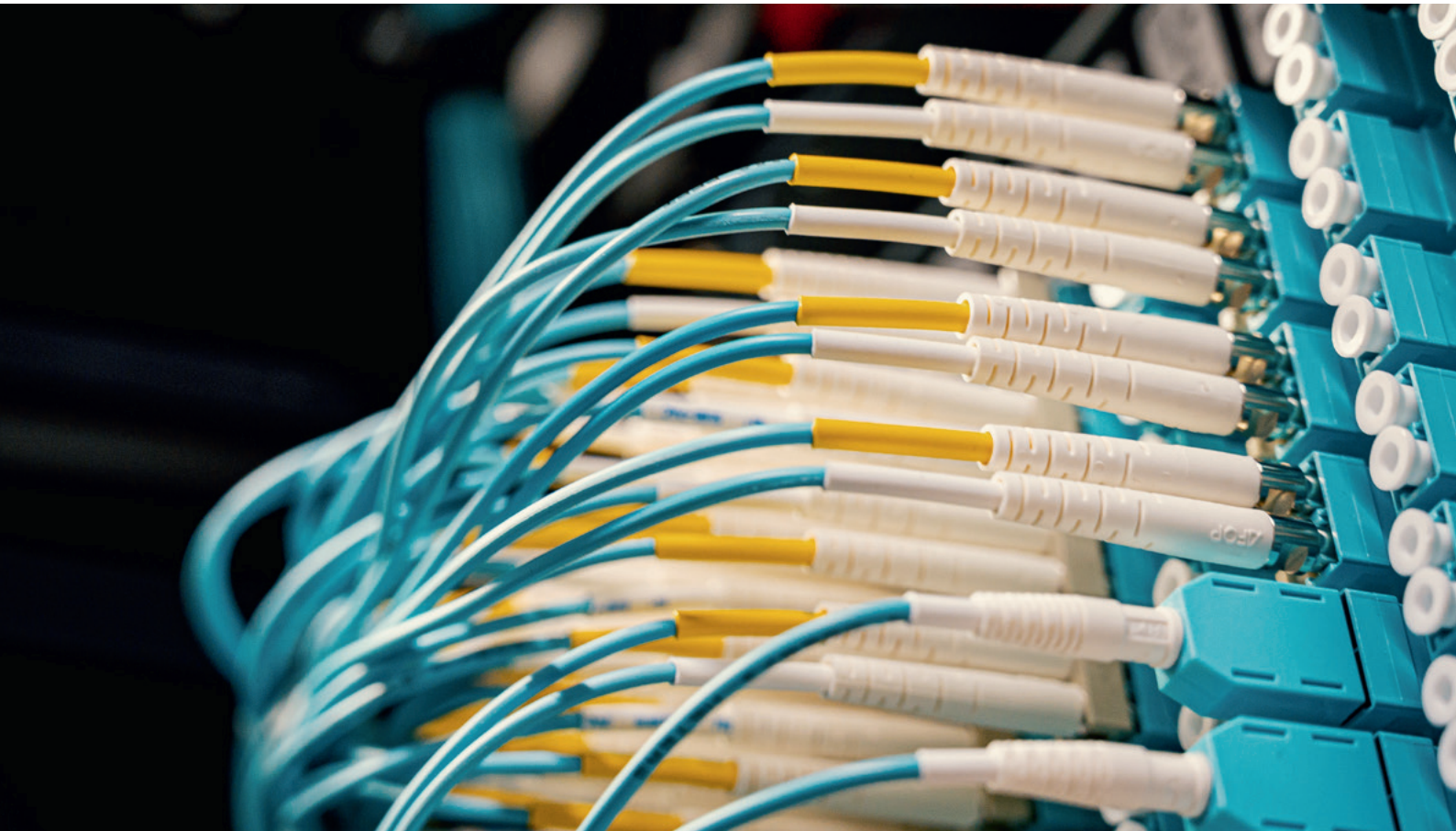
Het huidige coalitieakkoord onderkent dat de digitale revolutie geweldige kansen biedt voor onze samenleving en economie. Tegelijkertijd is er de noodzaak voor een adequate aanpak van cybersecurity en een effectief toezicht hierop. Voortdurend komen kwetsbaarheden in onze digitale systemen naar voren. Geopolitieke ontwikkelingen, zoals de oorlog in Oekraïne, bedreigen de vitale infrastructuur onophoudelijk. Dit heeft zijn weerslag op de digitale veiligheid in Nederland.

Continue alertheid, adequaat handelen en scherpte zijn noodzakelijk als het gaat om cybersecurity. De toezichthouders die sinds de invoering van de Europese netwerk- en informatieveiligheid-richtlijn (NIS, ook wel bekend als NIB)[1] en de Wet beveiliging netwerk- en informatiesystemen (Wbni)[2] samenwerken, maken de doorontwikkeling van het toezicht hierop jaarlijks inzichtelijk in het Samenhangend Inspectiebeeld. Het inspectiebeeld weerspiegelt de staat van de cybersecurity van vitale aanbieders en vitale processen aan de hand van de inspectieresultaten en bevindingen van de betrokken toezichthouders. Dit document gaat over de inspectieresultaten over het jaar 2022. Het Samenhangend Inspectiebeeld wordt jaarlijks gepubliceerd.

Vitaal

Dit Samenhangend Inspectiebeeld past het begrip 'vitaal' in brede zin toe: vitale processen zijn de processen die zo essentieel zijn voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid[3]. Vitale aanbieders zijn partijen die een dienst aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. De vakdepartementen zijn beleidsmatig verantwoordelijk voor de vraag welke aanbieders beschouwd moeten worden als vitaal[4]. De aanbieders van een groot deel van deze processen zijn tevens op basis van Wbni als vitale aanbieder aangewezen.

Onder toezicht staande organisaties zijn in het licht van dit inspectiebeeld de organisaties die vitale diensten aanbieden, al gaat die beschrijving niet 100 procent op voor sommige bij dit beeld betrokken toezichthouders, zoals toegelicht in paragraaf 1.2 van dit beeld. In het kader van de NIS 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. Daarin wordt uitgebreider ingegaan op de door elkaar gebruikte begrippen vitaal en essentieel. Dit inspectiebeeld hanteert de term vitale aanbieders[5].



De inspectiebeelden van de afgelopen jaren laten zien dat de sectoren voortdurend hard werken aan de versterking van de digitale weerbaarheid.

In lijn met het versterken van de samenwerking en samenhang tussen de toezichthouders stelden zij in 2021 het eerste Samenhangend Inspectiebeeld op over het jaar 2020. De inspectiebeelden van de afgelopen jaren laten zien dat de sectoren voortdurend hard werken aan de versterking van de digitale weerbaarheid. De toezichthouders concentreerden zich hierbij op het meerjarenthema risicomanagement. Tegelijkertijd loopt men tegen sectorspecifieke uitdagingen aan. Ook zijn er onderlinge afhankelijkheden tussen sectoren en kunnen dezelfde dreigingen meerdere sectoren raken. In dit inspectiebeeld laten de toezichthouders zien dat deze lijn van doorontwikkeling en uitdagingen zich voortzet.

Cybersecurity

In lijn met de eerdere inspectiebeelden wordt de volgende beschrijving van het begrip cybersecurity gehanteerd:
"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 te 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[6]."

1.2. De betrokken toezichthouders

Dit Samenhangend Inspectiebeeld is opgesteld door de toezichthouders die sinds de invoering van de NIS en de Wbni samenwerken. Dit betreffen:

- Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)
- Autoriteit Persoonsgegevens (AP)
- De Nederlandsche Bank (DNB)
- Inspectie Gezondheidszorg en Jeugd (IGJ)
- Inspectie Justitie en Veiligheid (IJenV)
- Inspectie Leefomgeving en Transport (ILT)
- Rijksinspectie Digitale Infrastructuur (RDI), voorheen Agentschap Telecom (AT)

Niet alle bij dit inspectiebeeld betrokken toezichthouders vallen onder de Wbni. Soms geldt een ander wettelijk kader, zoals in het geval van de telecomsector of de financiële sector. Soms zijn simpelweg nog geen vitale aanbieders in een bepaalde sector aangewezen. Hieronder volgt in het licht van bovenstaande een korte duiding.

De sector gezondheidszorg waar de IGJ toezicht op houdt, wordt in de NIS expliciet benoemd. In het kader van de Wbni zijn tot op heden nog geen vitale aanbieders benoemd. Ook zijn er geen vitale processen in de zin van de NIS aangewezen. Met de implementatie van de nieuwe NIS2-richtlijn (NIS2)[7] komt hier naar verwachting verandering in[1]. Het is nog niet duidelijk welke consequenties dat heeft voor het toezicht van de IGJ. De term vitaal wordt in dit rapport breed toegepast en heeft daarmee 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.

Voor 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

1 Er wordt in hoofdstuk 3 'Uitdagingen in het toezicht' uitgebreid ingegaan op de NIS2-richtlijn.

112 en C2000[II]' en 'inzet politie' binnen de sector Openbare Orde en Veiligheid (OOV). Deze processen zijn wel vitaal maar niet opgenomen in de Europese NIS-richtlijn en ook niet in de Wbni. Daarom zijn voor deze processen geen vitale aanbieders aangewezen. De vitale processen binnen OOV vallen onder de verantwoordelijkheid van het ministerie van Justitie en Veiligheid. De IJenV sluit zoveel mogelijk aan bij de risicogebaseerde aanpak en werkwijze van de toezichthouders die wel toezicht houden in het kader van de Wbni.

De AP heeft een ander perspectief dan de andere bij dit inspectiebeeld betrokken toezichthouders. De AP houdt namelijk geen toezicht op specifieke organisaties, op een specifieke sector of op een vitaal proces zelf. De AP houdt toezicht krachtens de Algemene Verordening Gegevensbescherming (AVG)[8] op alle publieke en private organisaties 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 cybersecurity, maar vormt het adequaat beveiligen van persoonsgegevens een belangrijk vereiste voor AVG-conforme gegevensverwerking. Bij incidenten met persoonsgegevens werkt de AP nauw samen met de in dit inspectiebeeld betrokken toezichthouders.

Zoals gezegd houden de betrokken toezichthouders toezicht op basis van de Wbni, maar ook vanuit andere wettelijke kaders. Hierdoor kunnen verschillende toezichthouders dezelfde aanbieders van vitale processen onder toezicht hebben voor uiteenlopende aspecten. Zo houdt de ANVS toezicht op situaties waarbij ioniserende straling kan vrijkomen en stralingsbronnen kunnen voorkomen. Deze toepassingen komen bijvoorbeeld voor in ziekenhuizen. Deze partijen vallen ook onder het toezicht van de IGJ. Daardoor spelen meerdere toezichthouders een rol. Deze samenhang laat zien dat samenwerking tussen de verschillende toezichthouders geen optie, maar noodzaak is.

II C2000 is het communicatiesysteem voor de hulpdiensten. Politie, brandweer, ambulancediensten, onderdelen van het ministerie van Defensie en daaraan gekoppelde organisaties gebruiken het digitale systeem voor hun mobiele communicatie.

1.3. Leeswijzer

Hoofdstuk 2 beschrijft de uitkomsten van het toezicht op de cybersecurity van de vitale processen. Op basis van de inspectieresultaten zijn een aantal rode draden geïdentificeerd. Hoofdstuk 3 schetst de uitdagingen en ontwikkelingen die de betrokken toezichthouders zien in het toezicht. Hoofdstuk 4 beschrijft de doorontwikkeling van het Samenhangend Inspectiebeeld. Hierbij is gekeken naar de verbeterpunten uit het voorgaande inspectiebeeld. Tevens is de ambitie voor de komende jaren toegelicht.

2 Rode draden vanuit toezichtresultaten

foto: Remco Zwinkels

2.1. Inleiding

Dit hoofdstuk schetst de rode draden op basis van de inspectieresultaten van de betrokken toezichthouders. Deze rode draden zijn gebaseerd op de inspectiewerkzaamheden die door de toezichthouders in 2022 zijn uitgevoerd. Op basis van de rode draden hebben de toezichthouders conclusies en aanbevelingen gedefinieerd. Een gedetailleerd overzicht van de resultaten per toezichthouder is opgenomen in de bijlage van dit inspectiebeeld.

2.2. Risicomanagement blijft speerpunt in cybersecurity

Net als in 2021 besteedden alle toezichthouders in 2022 aandacht aan risicomanagement. Veelal vond dat plaats binnen de reguliere inspectiewerkzaamheden. Indien nieuwe sectoren en vitale aanbieders zijn aangewezen vanuit de Wbni is het onderwerp risicomanagement door de toezichthouders besproken met het bestuur en andere verantwoordelijken binnen de desbetreffende organisaties. De verantwoordelijkheid van het bestuur kent een belangrijke basis in de opzet van een Information Security Management System (ISMS)[III]. Risicomanagement kwam in het toezicht ook vaak terug in combinatie met het specifieke onderwerp van risico's in de logische toegangsbeveiliging.

Risicomanagement

Risicomanagement is een continu proces waarbij bedrijfsrisico's voortdurend worden bewaakt. Onderdelen van dit proces zijn bijvoorbeeld het identificeren, evalueren en prioriteren van risico's en het nemen van maatregelen. Bijvoorbeeld door risico's te mitigeren of te accepteren. Door middel van risicoanalyses krijgen organisaties inzicht in deze risico's[9].

2.2.1. Risicomanagement en het belang van een goed ISMS

Een ISMS borgt het risicomanagementproces op basis van een plan-do-check-act-cyclus. Door deze cyclus besteden vitale aanbieders continu aandacht aan cybersecurityrisico's van hun organisatie. Nagenoeg alle vitale aanbieders hanteren de standaard ISO 27001 als leidraad. Een deel van de vitale aanbieders is hiervoor gecertificeerd. Het aantal vitale aanbieders dat zich laat certificeren blijft groeien.

Een adequaat ISMS bevat een basisniveau voor cybersecurity. Uit de toezichtwerkzaamheden blijkt dat vitale aanbieders een lichte stijging in de blootstelling aan cybersecurityrisico's laten zien. Zo hadden vitale aanbieders in 2022 veel aandacht voor geopolitieke dreigingen. Vermindering van deze risico's vraagt effectievere beheersmaatregelen op het gebied van cybersecurity. Mede als gevolg van de inspectiewerkzaamheden kregen verbetertrajecten bij vitale aanbieders een extra stimulans en raakten de organisaties ook op bestuursniveau steeds meer betrokken bij dit onderwerp.

Terugkijkend op de aanbevelingen in het voorgaande Samenhangend Inspectiebeeld signaleren de toezichthouders dat vitale aanbieders steeds meer aandacht hebben voor de steeds complexere digitale dreigingen in leveranciersketens. Organisaties maken voor hun dienstverlening steeds meer gebruik van verschillende leveranciers, die op hun beurt weer gebruik maken van andere leveranciers[10]. Zo ontstaat een keten aan leveranciers. De vitale aanbieders brengen steeds vaker hun ketens in kaart en houden dit overzicht actueel. Gezien de dreiging van cyberaanvallen op vitale aanbieders is bewaking van de effectiviteit van beheersmaatregelen in de gehele keten essentieel. Op deze manier houden organisaties grip op de dreigingen die samenhangen met uitbestedingstrends. Een bekend voorbeeld daarvan is de aanval met een Mimecast-certificaat op Microsoft 365 accounts[11].

III Een ISMS is een managementsysteem voor de beveiliging van informatie. Met dit systeem bewaakt men het proces van informatiebeveiliging.

Operationele Technologie

Operationele Technologie of Operational Technology (OT) is een verzamelnaam voor verschillende systemen die worden gebruikt voor het beheer van operationele processen in de fysieke wereld, zoals het aansturen en monitoren van (industriële) apparatuur. Het kan dan gaan om het uitlezen van sensoren of het inschakelen van een pomp of schakelaar op basis van een bepaalde conditie. OT speelt een grote rol in verschillende industrieën en sectoren. Het komt veel voor in de maakindustrie, olie- en gasindustrie, waterschappen en in de transport- en energiesector[12].

Binnen het overkoepelende risicomanagement draagt een ISO 27001 certificering bij aan de governance van vitale aanbieders. Ook komt de IEC 62443 (cybersecurity for industry) als aanvullende standaard voor OT steeds vaker in beeld. Het toont aan dat maatregelen continu worden aangevuld, gemonitord en verbeterd.

Cybersecurity-standaarden

Standaarden helpen bedrijven om gestructureerd invulling te geven aan doelen die ze willen bereiken op het gebied van bijvoorbeeld veiligheid of kwaliteit. Hiertoe kunnen organisaties zich laten certificeren. Veel gebruikte standaarden bij de vitale aanbieders zijn onder andere:

ISO 27001: Deze standaard biedt vereisten voor organisaties die een informatiebeveiligingsbeheersysteem willen opzetten, implementeren, onderhouden en voortdurend verbeteren. Dit raamwerk dient als richtlijn voor het voortdurend beoordelen van de veiligheid van informatie.

IEC 62443: Deze standaard biedt een systematische en praktische aanpak die elk aspect van cyberbeveiliging voor industriële systemen omvat. De standaard is bedoeld om Industrial Automation & Control Systems (IACS) te beveiligen.

NEN 7510: Deze norm is gebaseerd op de ISO 27001 en is in Nederland de wettelijke norm voor informatiebeveiliging bij zorgaanbieders. De norm houdt rekening met specifieke kenmerken van de zorgsector.

Uit de inspectiewerkzaamheden blijkt dat vitale aanbieders adequaat reageren op nieuwe dreigingen[IV]. Echter, bij succesvolle digitale aanvallen wordt regelmatig gebruik gemaakt van zwakke plekken in de beveiliging. Goede cyberhygiëne[V] kan dit risico verkleinen. Door evaluatie en documentatie van ervaringen vindt aanscherping van processen plaats.

De toezichthouders zien dat er ruimte is om de cyberhygiëne verder te verbeteren. Zij hechten er daarom waarde aan dat de vitale aanbieders hun risicomanagementproces naar een hoger niveau tillen. De belangrijkste verbeterpunten zijn:

- het onafhankelijk laten beoordelen van de effectiviteit van het ISMS;
- het verder ontwikkelen en implementeren van beveiligingstesten;
- het zorgdragen voor risicobeheersing binnen het ISMS van het complete ecosysteem van samenwerking en uitbesteding.

Onafhankelijke beoordeling

Het onafhankelijk laten beoordelen van een ISMS geeft organisaties aanvullende zekerheid over de werking hiervan. Interne of externe auditors kunnen hierbij een rol vervullen. Ook certificering kan toegevoegde waarde leveren.

Beveiligingstesten

Beveiligingstesten maken zichtbaar of aan de beveiligingsvereisten van een toepassing wordt voldaan. Aanvallen kunnen bijvoorbeeld worden gesimuleerd door het uitvoeren van penetratietesten of door het inzetten van mystery guests. Een voorbeeld van een geavanceerde cyberweerbaarheidstest binnen de Nederlandse financiële sector is voor de meest kritieke partijen het programma Threat Intelligence Based Ethical Red-teaming (TIBER-NL). Binnen dit programma testen financiële instellingen hoe weerbaar ze zijn tegen geavanceerde cyberaanvallen, waarbij de tactieken, technieken en procedures van hackersgroepen worden nagebootst[13].

IV Meer informatie over dreigingen van statelijke actoren is terug te vinden in het 'Dreigingsbeeld Statelijke Actoren' van november 2022. Dit betreft een gezamenlijke analyse van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Militaire inlichtingen- en Veiligheidsdienst (MIVD) en de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV).

V Cyberhygiëne is dat wat minimaal nodig is om een informatienetwerk te beveiligen. Bijvoorbeeld het automatisch vergrendelen van een digitaal systeem als het een bepaalde tijd niet gebruikt wordt, meerfactorauthenticatie, het maken van back-ups, het gebruik van antivirussoftware en het aansturen op veilig gedrag van personeel.

Van ketens naar ecosystemen

Door nieuwe technologische ontwikkelingen en digitalisering van de economie volstaat het niet meer om in klassieke ketens te denken. Producten en diensten komen steeds vaker tot stand in coöperatief verband met inzet van wisselende partijen. Die partijen worden betrokken op basis van hun specifieke rol, kennis of expertise. Digitalisering speelt daarin een belangrijke rol. Zo ontstaat er een digitaal ecosysteem van veel verschillende partijen. Zij kunnen hun specifieke waarde bovendien inzetten in verschillende digitale ecosystemen. Hierdoor kan het aantal leveranciers en toeleveranciers, in wisselende samenstellingen, in hoog tempo toenemen[VI]. Een adequaat functionerend ISMS houdt rekening met deze ontwikkeling rondom digitale ecosystemen om het risicomanagementproces optimaal te ondersteunen.

2.2.2 Risicomanagement bij logische toegangsbeveiliging

Bij logische toegangsbeveiliging gaat de aandacht bij vitale aanbieders vooral uit naar het buitenhouden van onbevoegden. Dat blijft belangrijk omdat diefstal of gijzeling van gegevens nog steeds één van de meest concrete cyberdreigingen is. Het wordt toegejuicht dat vitale aanbieders bewust bezig zijn met dreigingen van buitenaf en daar voldoende maatregelen op blijven nemen. Op basis van incidenten en bevindingen in het afgelopen jaar verdienen een aantal aanvullende onderwerpen binnen het onderwerp logische toegangsbeveiliging meer aandacht.

Toegang voor eigen medewerkers

Ongeautoriseerde inzage in dossiers of onnodige toegang tot systemen binnen de eigen organisatie, ook wel bekend als insider threat, leidde het afgelopen jaar tot meerdere incidenten. Regelmatig bleken zowel preventie (bijvoorbeeld accuraat rollen- en rechtenbeheer) als detectie (zoals logging en auditing) onvoldoende te zijn ingericht. Meer aandacht voor de toegang tot systemen door eigen medewerkers is essentieel voor de veiligheid van persoonsgegevens en gevoelige informatie. Ook ongeautoriseerde toegang met het risico op manipulatie van OT-systemen moet worden voorkomen.

Toegang voor leveranciers

Veel vitale aanbieders maken gebruik van complexe digitale infrastructuur. Om inrichtings- of beheerstaken te kunnen uitvoeren, krijgen leveranciers of onderaannemers regelmatig (op afstand) toegang tot delen van deze infrastructuur. Bij uitgebreide leverancierssketens of bij leveranciers van buiten Europa, levert dit extra risico's op. Diverse incidenten en bevindingen laten zien dat vitale aanbieders op dit punt onvoldoende in beeld hebben waartoe leveranciers toegang hebben en welke activiteiten daar plaatsvinden.

VI Verder lezen over ketenafhankelijkheden: 'Ketenafhankelijkheden' (deitauditor.nl).

foto: Ivo Vranckena

Sinds de coronaperiode heeft geautomatiseerde identiteitsvaststelling een vlucht genomen.

Identificatie van klanten

Identificatie op afstand

De term identificatie op afstand wordt voor meerdere zaken gebruikt. In dit inspectiebeeld wordt met identificatie op afstand bedoeld: de innovatieve manier voor het vaststellen van de identiteit aan de hand van een identiteitsbewijs, zonder dat daarvoor een fysieke afspraak op locatie nodig is. Een voorbeeld hiervan is identificatie door middel van een app die een identiteitsbewijs uitleest en vergelijkt met live-beelden van het gezicht van de persoon die zich identificeert.

Smart Mobility

Met smart mobility wordt de digitalisering en automatisering van de mobiliteit bedoeld. Hierbij worden op een slimme manier informatie- en communicatietechnologieën en data gebruikt om de mobiliteitsopgaven op te lossen. Het kan gaan om gedigitaliseerde diensten die vervoer of transport op maat aanbieden. Ook zijn er apps waarmee openbaar vervoer, taxi's, deelauto's, deelscooters en/of deelfietsen kunnen worden gereserveerd en betaald.

Organisaties in diverse sectoren identificeren en autoriseren hun klanten voor toegang tot hun diensten door hun identiteit op afstand met hoge zekerheid vast te stellen. Dit is gebruikelijk in de financiële dienstverlening, bij elektronische toegangs- of vertrouwensdiensten en bij smart mobility. Soms is dit wettelijk vereist. Sinds de coronaperiode heeft geautomatiseerde identiteitsvaststelling een vlucht genomen. Identificatie op afstand gebeurt veelal door middel van applicaties die gebruik maken van kunstmatige intelligentie (AI-technologie). Organisaties hebben de risico's van deze innovatie niet altijd voldoende in beeld. Er kleven risico's aan gegevensverwerking in leverancierskетens die zich uitstrekken tot buiten Europa. Een ander belangrijk risico zijn aanvallen op nieuwe identificatieprocessen, waarbij de aanvallers vaak even innovatief zijn als de gebruikte applicaties.

Logische toegangsbeveiliging

Guidance vanuit het Nationaal Cyber Security Centrum (NCSC)

Logische toegangsbeveiliging controleert wie, wanneer, op welke wijze en met welke rechten toegang krijgt tot bepaalde digitale informatie, informatiesystemen en netwerken. Voor toegangscontrole is Identity and Access Management (IAM) nodig. Dit bestaat uit:

- Identificatie: Een persoon of entiteit moet herkend kunnen worden aan een digitale identiteit of een account. Accounts die zijn gebonden aan een persoon bieden meer controle dan accounts die worden gedeeld.

- Authenticatie: Om aan te tonen dat je de rechtmatige gebruiker bent van een account, heb je een authenticatiemiddel zoals een wachtwoord, vingerafdruk, smartcard of gebruik je een systeem als DigiD. Om fraude en misbruik te voorkomen worden meerdere soorten bewijzen gevraagd. Dit heet multifactorauthenticatie[14].

- Autorisatie: Aan accounts worden rechten verleend. Er wordt vastgelegd waartoe precies toegang mogelijk is, en of bepaalde informatie en configuraties ingezien, gecreëerd, bewerkt en/of verwijderd mogen worden. Een beheerder kan autoriseren, maar rechten kunnen bijvoorbeeld ook automatisch verleend worden aan de hand van de functie van een medewerker. Voor goede beveiliging en om onbedoelde acties te voorkomen worden niet meer rechten dan nodig verleend. Dit heet het principle of least privilege[15].

- Accounting: Systemen en netwerken kunnen loginformatie genereren om toegang en acties van accounts te registreren. Dit is van belang voor het detecteren en corrigeren van ongewenste situaties en afwijkingen[16].

Logische toegangsbeveiliging kan verder versterkt worden door bijvoorbeeld toegangscontrole na verloop van tijd te herhalen om te controleren of de actieve gebruiker nog steeds de geautoriseerde persoon is. Ook kan een netwerk gesegmenteerd worden waardoor toegang nauwkeuriger bepaald kan worden, en waardoor problemen geïsoleerd kunnen worden in een deel van het netwerk[17].

Logische toegangsbeveiliging is essentieel voor cybersecurity. De basismaatregelen van het NCSC zijn hier nadrukkelijk op gericht[18]. Het NCSC adviseert organisaties daarnaast om risicomanagement toe te passen door aan de hand van de te beschermen belangen, dreigingen en de weerbaarheid van de betreffende organisatie te bepalen of aanvullende maatregelen nodig zijn.

2.2.3 Risicomanagement als middel om te sturen op veranderende dreigingen

Digitale weerbaarheid is complex en continu aan verandering onderhevig. Het is een nauw samenspel tussen mensen, processen en technologie. Digitale weerbaarheid verlangt daardoor een gestructureerde aanpak én commitment van het bestuur van organisaties. Om deze reden vinden de toezichthouders adequaat risicomanagement een belangrijk speerpunt in toezicht op digitale weerbaarheid.

Risicomanagement is de basis van de digitale weerbaarheid van organisaties. Het is een continu proces dat risico's identificeert. Door de risico's en de mogelijke impact daarvan in te schatten, kunnen de juiste beheersmaatregelen worden getroffen.

Dit hele stelsel belegt verantwoordelijkheden, geeft inzicht en stelt organisaties in staat om proactief op risicobeheersing te sturen.

Vitale aanbieders ondervinden in toenemende mate effecten van geopolitiek en digitalisering. De digitale infrastructuur in de maatschappij groeit en is steeds vaker doelwit van cyberaanvallen. Dit kan leiden tot maatschappelijke ontwrichting. Bijzondere aandacht dient uit te gaan naar identificatie op afstand en aanvallen op (toe) leveranciers. Een goed ingericht en actief toegepast risicomanagementproces draagt bij aan de continuïteit van vitale processen.

2.3. Meldingen van cybersecurity-incidenten

Naast de meldplicht van incidenten onder de Wbni, gelden er ook andere wettelijke meldplichten voor een aantal vitale aanbieders. Onder de Wbni zijn vitale aanbieders verplicht om alle incidenten die aanzienlijke gevolgen hebben voor de continuïteit van de dienstverlening, onmiddellijk te melden bij het NCSC. Bij overschrijding van een specifieke drempelwaarde wordt dit tevens gemeld bij de toezichthouder. De toezichthouder kan 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 2022 zijn geen incidenten gerapporteerd aan de toezichthouders die de drempelwaarde overschreden.

3 Uitdagingen in het toezicht

3.1. Inleiding

Dit hoofdstuk schetst de uitdagingen en ontwikkelingen in het toezicht. Er wordt ingegaan op de uitdagingen die samenhangen met de introductie van verschillende Europese regelgeving. Daarnaast wordt het belang van samenwerken in het toezicht onderstreept.

3.2. Nieuwe Europese richtlijnen voor digitale en fysieke weerbaarheid

De afgelopen jaren hebben diverse ontwikkelingen de stabiliteit van onze maatschappij en economie in toenemende mate onder druk gezet. Daarom is er sinds 2020 vanuit de Europese Unie (EU) gewerkt aan twee richtlijnen, de Critical Entities Resilience richtlijn (CER)[19] en de NIS2-richtlijn. Samen moeten deze richtlijnen leiden tot een verbeterde bescherming van de lidstaten en van de interne markt. Beide richtlijnen helpen de Europese lidstaten om hun fysieke, digitale en economische weerbaarheid te vergroten.

De CER richt zich op de bescherming tegen fysieke risico's zoals de gevolgen van natuurrampen, gezondheidscrises en terroristische misdrijven. De NIS2 richt zich op digitale risico's zoals cyberbeveiligingsrisico's. De NIS2 moet bijdragen aan een hoger niveau van cybersecurity, mede door meer harmonisatie van de cyberwetgeving van de lidstaten. De richtlijn is de opvolger van de eerste NIS-richtlijn, die in 2016 is vastgesteld en vervolgens is geïmplementeerd in de Wbni. De lidstaten hebben tot eind 2024 de tijd om de richtlijnen te implementeren in nationale wet- en regelgeving.

Reikwijdte CER

De CER richt zich op kritieke entiteiten die essentiële diensten verlenen binnen de volgende sectoren: energie, drinkwater, vervoer, digitale infrastructuur, levensmiddelenindustrie, gezondheidszorg, infrastructuur voor de financiële markt, afvalwater, overheidsdiensten, bankwezen en ruimtevaart.

De ministers die verantwoordelijk zijn voor deze sectoren gaan beoordelen welke organisaties als kritieke entiteit onder de CER worden aangewezen. Daarbij zal worden gekeken naar de mate waarin een organisatie een dienst verleent die cruciaal is voor de instandhouding van maatschappelijke functies en economische activiteiten. Organisaties die al eerder door de overheid zijn aangewezen als 'vitale aanbieder' in één van de genoemde sectoren, zullen onder de CER worden aangewezen als kritieke entiteit.

Voor een aantal toezichthouders en sectoren betekent dit dat de reikwijdte van het toezicht zal uitbreiden naar toezicht op de bescherming tegen fysieke risico's. De reikwijdte is niet langer beperkt tot netwerk- en informatiesystemen.

Reikwijdte NIS2

De reikwijdte van de NIS2 is verruimd. Sectoren die zowel onder de eerste als tweede NIS-richtlijn vallen zijn de energiesector, het bankwezen, de financiële marktinfrastructuren, de digitale infrastructuur, digitale dienstverleners, het vervoer, de drinkwatervoorziening en de gezondheidszorg. Onder de NIS2 vallen daarnaast organisaties die behoren tot sectoren als afvalwater, overheidsdiensten, ruimtevaart, post- en koeriersdiensten, afvalstoffenbeheer, levensmiddelen, chemische stoffen, onderzoek, beheer van ICT-diensten en de maakindustrie.

Voor de toezichthouders van vitale processen betekent dit een uitbreiding van het aantal sectoren en daarmee het aantal entiteiten dat onder hun toezicht valt. Tevens komen er een aantal toezichthouders bij die onder de eerste NIS-richtlijn nog geen toezicht hielden. De toezichthouders zien zich mede hierdoor voor grote uitdagingen gesteld in 2023 in de voorbereiding van het toezicht en vanaf 2024 en verder in het uitvoeren ervan. De nieuwe richtlijn verlangt herinrichting van het toezicht. Tegelijkertijd is sprake van uitbreiding van het takenpakket. Een bijkomende uitdaging is de krapte op de arbeidsmarkt, waardoor toezichthouders moeite hebben met het invullen van vacatures.

NIS1

- Energie
- Transport
- Bankwezen
- Infrastructuur financiële markten
- Gezondheidszorg
- Drinkwater
- Digitale infrastructuur
- Digitale dienstverleners

NIS2

- Energie
- Transport
- Bankwezen
- Infrastructuur financiële markten
- Gezondheidszorg
- Drinkwater
- Digitale infrastructuur
- Digitale dienstverleners
- Afvalwater
- Overheidsdiensten
- Ruimtevaart
- Post- en koeriersdiensten
- Afvalstoffen-beheerder
- Levensmiddelen
- Chemische stoffen
- Onderzoek
- Vervaardiging/ Manufacturing
- ICT Service Management

Een belangrijk verschil met de eerste NIS is dat organisaties automatisch onder de NIS2 vallen als zij actief zijn in één van de bovenstaande sectoren en van een bepaalde grootte zijn.

Micro- en kleine bedrijven uit de bovenstaande sectoren vallen – op een aantal uitzonderingen na – niet automatisch onder de NIS2[VII]. De verantwoordelijke vakministers moeten deze bedrijven alsnog aanwijzen als deze bedrijven voldoen aan bepaalde criteria uit de NIS2-richtlijn. Een voorbeeld van een criterium is als hun dienstverlening van bijzonder of cruciaal belang is voor de Nederlandse economie of maatschappij.

De NIS2 maakt onderscheid tussen twee verschillende typen organisaties: 'essentiële' entiteiten en 'belangrijke' entiteiten. Van essentiële entiteiten wordt over het algemeen aangenomen dat de uitval van hun diensten veel meer ontwrichtende impact heeft op de economie en samenleving, dan uitval bij belangrijke entiteiten. Essentiële entiteiten vallen daarom onder een intensiever regime van toezicht. Lidstaten kunnen ervoor kiezen om belangrijke entiteiten aan te wijzen als essentiële entiteit, bijvoorbeeld als hun dienstverlening van bijzonder of cruciaal belang is voor de economie of maatschappij.

Verplichtingen uit de CER en de NIS2

De kaders die beide richtlijnen neerzetten, vertonen grote gelijkenissen. Beide richtlijnen schrijven een zorgplicht voor. Deze zorgplicht moet ervoor zorgen dat organisaties op basis van een risicobeoordeling passende maatregelen nemen om de continuïteit, integriteit en vertrouwelijkheid van hun diensten te waarborgen. Bij de CER zijn deze maatregelen gericht op fysieke dreigingen en bij de NIS2 op dreigingen voor de beveiliging van netwerk- en informatiesystemen.

Ten tijde van het opstellen van dit inspectiebeeld is het nog niet volledig duidelijk hoe (toekomstige) vitale aanbieders aan de gestelde eisen in de richtlijnen kunnen voldoen. Dit wordt duidelijk zodra de richtlijnen zijn omgezet in nationale wet- en regelgeving. Ook voor de nog aan te wijzen of aangewezen toezichthouders geldt dat nog niet geheel duidelijk is hoe het toezicht onder de CER en NIS2 moet worden ingericht. Dit zal mede volgen uit de keuzes in de nationale implementatiewetgeving. Daarbij bepaalt de NIS2 dat de nationale toezichthouders bepaalde bevoegdheden krijgen,

VII Indien micro- en kleine bedrijven actief zijn als aanbieder van vertrouwensdiensten, als register voor topleveldomeinnamen, verleners van domeinnaamregistratiediensten of als aanbieder van openbare elektronische-communicatienetwerken of van openbare elektronische-communicatiediensten, dan vallen zij wel automatisch onder de NIS2-richtlijn. Ditzelfde geldt voor overheidsinstanties.

waaronder bevoegdheden die vooralsnog in deze context nieuw zijn in het Nederlands (bestuurs) recht en waar toezichthouders in die gevallen nog geen ervaring mee hebben. De ministeries werken aan eenduidige externe communicatie over de implementatie van de NIS2 en de CER om zo alle betrokken partijen op de hoogte te houden van de laatste ontwikkelingen.

NIS2 ten opzichte van NIS

Naast de grotere reikwijdte en het onderscheid tussen essentiële en belangrijke entiteiten brengt de NIS2 ook nog een aantal andere belangrijke wijzigingen met zich mee.

1. Beveiligingseisen in de NIS2 zijn inhoudelijk aangescherpt ten opzichte van de huidige NIS. De beveiliging van de leveranciersketen moet worden aangepakt, rapportage- en registratieverplichtingen zijn gestroomlijnd en aangescherpt en er wordt een vorm van bestuursverantwoordelijkheid geïntroduceerd. Aan de bestuursverantwoordelijkheid zijn ook verplichtingen ten aanzien van opleiding over informatiebeveiliging verbonden.

2. Verder stelt de NIS2 dat voor een aantal typen entiteiten geldt dat de lidstaat van de hoofdvestiging jurisdictie heeft. De dienstverlening van deze entiteiten is meestal grensoverschrijdend. Dit geldt met name voor entiteiten die actief zijn binnen de sectoren digitale infrastructuur, beheer van ICT-diensten en digitale aanbieders. Voorheen gold dit alleen voor digitale dienstverleners. Om de verplichtingen voor deze partijen te harmoniseren binnen de EU, zal de Europese Commissie nadere regels stellen over de zorg- en meldplicht van deze partijen.

3. Ten slotte bepaalt de NIS2 in veel verdergaande mate de specifieke bevoegdheden waar toezichthouders over dienen te beschikken, waaronder vergaande nieuwe bevoegdheden.

3.3. Samenwerking tussen toezichthouders

Steeds meer is de uitvoering van de toezichtstaak gebaat bij nationale en Europese afstemming en samenwerking. Vitale aanbieders en eventuele derde partijen zijn vaak actief in meerdere EU-lidstaten. Bovendien kunnen cyberincidenten meerdere wettelijke normen raken en daarmee meerdere toezichtdomeinen.

De NIS2 stelt dat NIS2-toezichthouders nationaal en binnen de EU nauw met elkaar samenwerken en elkaar ondersteunen. Ook kunnen zij gezamenlijke toezichtacties uitvoeren. De samenwerking met toezichthouders onder andere regelgeving wordt ook in de NIS2 aangehaald, waaronder de CER, de Digital Operational Resilience Act (DORA)[20], de AVG en andere sectorale regelgeving. De NIS2 benadrukt daarbij het belang van effectieve samenwerking en informatie-uitwisseling tussen de verschillende toezichthouders. Tevens wordt in de Nederlandse Cybersecurity Strategie 2022-2028 (NLCS) benadrukt dat toezichthouders op nationaal niveau, maar ook Europees en internationaal intensiever zullen samenwerken met partners[21].

In Europees verband wordt door Europese toezichthouders samengewerkt in verschillende workstreams onder de Europese NIS Cooperation Group. De Workstream Supervision is recentelijk opgericht om de samenwerking tussen toezichthouders verder te intensiveren in de aanloop naar de implementatie van de NIS2. Nederland vervult samen met Ierland het voorzitterschap. Op het moment van schrijven van dit inspectiebeeld wordt aan de precieze invulling van deze workstream gewerkt.

Op nationaal niveau werken de bij dit inspectiebeeld betrokken toezichthouders samen in het Overleg Toezichthouders cybersecurity vitale processen. De toezichthouders wisselen ervaringen uit, stellen gezamenlijke producten op en delen ervaringen uit de toezichtpraktijk met de ministeries ten behoeve van de implementatie van de NIS2. Deze samenwerking zal de komende periode verder intensiveren. Tevens zal dit overleg op korte termijn worden gecombineerd met de samenwerking op digitalisering in de Inspectieraad[22].

Het geheel overziend zal de introductie van de NIS2 een grote impact hebben op de aard en reikwijdte van de nationale regelgeving en de vitale sectoren in Nederland. Dit beïnvloedt de invulling van het toezicht door de betrokken toezichthouders. Vanwege de verwachte omvang van de uitvoeringsopgave houden toezichthouders in Nederland op verschillende manieren rekening met deze ontwikkelingen. Zo is er actieve betrokkenheid bij de implementatie van de NIS2 vanuit het Overleg Toezichthouders. De daadwerkelijke impact wordt de komende maanden duidelijker.

4 Doorontwikkeling Samenhangend Inspectiebeeld

4.1. Inleiding

Het vorige Samenhangend Inspectiebeeld over het jaar 2021 sloot af met de ambitie om het inspectiebeeld verder door te ontwikkelen. Deze ambitie werd aan de hand van een aantal onderwerpen uitgewerkt. In dit hoofdstuk kijken we vooruit naar het komende jaar waarin we het inspectiebeeld verder willen ontwikkelen, met toezicht langs een gezamenlijk thema waarbij de samenwerking tussen de toezichthouders wordt geïntensiveerd.

4.2. Basis voor doorontwikkeling ligt in het jaar 2021

Risicomanagement vormt het meerjarenthema voor het Samenhangend Inspectiebeeld. In het vorige Samenhangend Inspectiebeeld lag de focus al bij risicomanagement, waarbij specifiek ingezoomd werd op risicomanagement bij leveranciers. Ook in dit inspectiebeeld is risicomanagement weer het hoofdthema. Dit is in lijn met het Besluit beveiliging netwerk- en informatiesystemen (Bbni) als nadere uitwerking van de zorgplicht in de Wbni. Risicomanagement wordt als één van de vijf hoofdmaatregelen genoemd in het Bbni.

Bbni

In het Bbni staat dat een aanbieder van een essentiële dienst ten minste de volgende maatregelen neemt en deze maatregelen periodiek evalueert en bijstelt ten aanzien van een risicogebaseerde aanpak:

De aanbieder heeft een actueel overzicht van de netwerk- en informatiesystemen die zijn essentiële dienst ondersteunen. De aanbieder stelt een risicoanalyse op waarin hij de risico's met betrekking tot de beveiliging beschrijft en ingaat op de wijze waarop hij de risico's naar een passend niveau verkleint. Hij motiveert daarbij waarom dit niveau volgens hem proportioneel en aanvaardbaar is. In die motivering gaat hij in ieder geval in op de organisatiespecifieke en sectorspecifieke risico's, het maatschappelijke belang van zijn essentiële dienst en de stand van de techniek. Hij legt de resultaten van de risicoanalyse schriftelijk vast en verwerkt de resultaten in beveiligings- en beheersmaatregelen.

Terugkijkend blijken die aandachtspunten goed gekozen en blijft dit thema van groot belang. Risico's in ketenafhankelijkheden blijven onverminderd groot. Geopolitieke spanningen spelen een steeds grotere rol in de dreiging. Cyberaanvallen door andere landen zijn het nieuwe normaal geworden. Dit heeft een verdere impuls gekregen door de oorlog in Oekraïne.

4.3. Risicomanagement als thema voor 2023

In 2022 maakten de toezichthouders afspraken over het uitvoeren van een gezamenlijk opgezet thema risicomanagement. Gezamenlijk is de scope en aanpak bepaald voor een eenduidige analyse. Op basis van deze uitwerking nemen de toezichthouders het thema op in hun programmering. Door het uitvoeren van een gezamenlijk opgezet thema zijn de toezichthouders in staat om hun inhoudelijke inspectiewerkzaamheden over het jaar 2023 op onderdelen inhoudelijk op elkaar af te stemmen en een eenduidiger beeld te schetsen op basis van de inspectiewerkzaamheden.

Niet alle toezichthouders hebben dezelfde tijd en capaciteit beschikbaar. Dit hangt samen met uiteenlopende sectorale risico's, kaders en prioriteiten. Er zijn organisatorische verschillen waardoor programmering van inspecties bij de toezichthouders een andere cyclus doorloopt. Daarbij zijn inspecteurs niet onbeperkt inzetbaar. Ondanks deze verschillen is afgesproken intensiever samen te werken aan de doorontwikkeling van het gezamenlijke onderzoeksthema in 2023.

bijlage 1
Toezichtresultaten per toezichthouder

Toezichthouder: Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Niet van toepassing		Nucleaire sector	Regeling beveiliging nucleaire inrichtingen en splijtstoffen	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Van toepassing	Van toepassing	Van toepassing	Van toepassing	Van toepassing
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. De ANVS controleert de voortgang van deze plannen.			
Status onderzoek:	Doorlopend tot alle verbeterplannen zijn afgerond			
Algemeen beeld:	Het algemene beeld van de ANVS is dat de vergunninghouders de verbeterplannen goed oppakken en dat voortdurend verbeteringen worden toegepast.			
Interventie:	De onder toezicht staanden blijven verbeteren en voldoen aan het wettelijk kader. Er zijn geen interventies gedaan.			
Relatie met andere toezichthouder:	RDI (voor Kerncentrale Borssele, dit is naast nucleair bedrijf ook energieleverancier hetgeen onder de Wbni valt).			

Toezichthouder: Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Niet van toepassing		Nucleaire sector	Regeling beveiliging nucleaire inrichtingen en splijtstoffen	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Van toepassing	Van toepassing	Van toepassing	Van toepassing	Van toepassing
Aanleiding:	De ANVS heeft aan de hand van enkele thema-inspecties een verkenning gedaan om tot een verbeterde en gestructureerde toezichtstrategie te komen. Deze inspecties zullen ook in 2023 uitgevoerd worden, en aan de hand van de bevindingen zal dit eind 2023 leiden tot een hernieuwd toezicht beleid.			
Status onderzoek:	Doorlopend in 2023			
Algemeen beeld:	Het algemene beeld van de ANVS is dat de vergunninghouders de nieuwe aanpak als constructief en transparant hebben ervaren.			
Interventie:	De onder toezicht staanden voldoen aan het wettelijk kader. Er zijn geen interventies gedaan.			
Relatie met andere toezichthouder:	RDI (voor Kerncentrale Borssele, dit is naast nucleair bedrijf ook energieleverancier hetgeen onder de Wbni valt).			

Toezichthouder: Autoriteit Persoonsgegevens (AP)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Niet van toepassing		Overheid	AVG	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Impactvolle datalekken binnen dit thema	Onrechtmatige inzage in persoonsgegevens door overheidspersoneel	Logging en systematische controle van de logging	-	-
Aanleiding:	Thema: onrechtmatige inzagen in dossiers door overheidspersoneel De AP ontvangt – ten opzichte van andere sectoren – een beperkt aantal meldingen over dit thema. Het probleem is dat persoonsgegevens van burgers geraadpleegd kunnen worden door overheidsmedewerkers, zonder dat dit zichtbaar wordt voor de organisatie en getroffen burger. Dat maakt dat het niet mogelijk is voor burgers en overheden om zich weerbaar te maken tegen dit probleem. In januari 2023 gaat een project binnen de afdeling Eerstelijns Onderzoek van start om extra toezicht te houden binnen dit thema.			
Status onderzoek:	Start januari 2023			
Algemeen beeld:	In 2022 hebben een aantal incidenten binnen dit thema plaatsgevonden. De betrokken organisaties blijken acties van medewerkers niet of onvoldoende te loggen. Bovendien ontbreekt controle van de loggegevens vaak. Meestal gaat het om het raadplegen van persoonsgegevens van burgers. Als dit bij meer overheden het geval is, dan kan dat een verklaring zijn voor het (relatieve) lage aantal datalekmeldingen.			
Interventie:	Interventie zal gericht zijn op aanscherping van beveiligingsmaatregelen (logging en controle op de logging).			
Relatie met andere toezichthouder:	Niet van toepassing.			

Toezichthouder: De Nederlandsche Bank (DNB)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Betalings- en effectenverkeer		Financiële sector	Art. 1:24 Wet Financieel Toezicht (Wft) Wbni	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
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:	DNB geeft invulling aan haar toezicht op de belangrijkste instellingen voor het betalings- en effectenverkeer (samen de Financiële Kerninfrastructuur FKI) door middel van verschillende toezichtsinstrumenten. Enkele van deze instrumenten zijn: onderzoeken, inspecties ter plaatse, analyses van incidenten en gesprekken met instellingen om voortgang van bevindingen uit onderzoeken te monitoren en om nieuwe risico's te identificeren. Daarnaast bestaat er een beeld van de cyber beheersing bij instellingen via gestructureerde vragenlijsten over IT-risico's die jaarlijks door instellingen worden ingevuld. Op basis van al deze bronnen ontstaat een geaggregeerd beeld van de beheersing van IT en operationele risico's bij onder toezicht staande instellingen. DNB voert tevens zelfstandig, alsmede ten behoeve van het Single Supervisory Mechanism (SSM) van de Europese Centrale Bank (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. Cybersecurity krijgt hierin een hoge prioriteit. Tevens is DNB betrokken bij cyber resilience surveys die uitgezet zijn bij Europese Financial Market Infrastructures. Daarnaast maakt DNB deel uit van de European Cyber Resilience Board en het Europees crisisoverleg voor financiële marktinfrastructuren die beiden worden voorgezeten door de Europese Centrale Bank.			
Status onderzoek:	De toezichtsinstrumenten die DNB inzet, zoals onderzoeken, inspecties ter plaatse, analyses van incidenten en gesprekken met instellingen zijn doorlopend van aard. Daarnaast worden periodiek surveys en questionnaires opgevraagd bij instellingen. De informatie uit alle genoemde toezichtsinstrumenten wordt ingezet voor risicogebaseerd toezicht en kan tevens aanleiding vormen voor gerichte onderzoeken of inspecties die doorlopend van aard zijn.			
Algemeen beeld:	Het algemene beeld is dat instellingen meer en blijvend aandacht hebben voor de risico's op het gebied van IT en cybersecurity. Uit onze toezichtonderzoeken en analyses van gestructureerde zelfbeoordelingen blijkt dat instellingen hun weerbaarheid tegen cyberaanvallen verbeterden, maar dat verdere aanscherping nodig is, onder andere voor het op orde houden van de cyberhygiëne, de frequentie van beveiligingstesten, het zicht op de uitbestedingsketen en risicomanagement. Uit de onderzoeken blijkt onder andere dat instellingen een lichte stijging in de blootstelling aan IT-risico's laten zien. Om deze stijging in risico blootstelling te mitigeren zijn effectievere beheersingsmaatregelen op het gebied van cybersecurity nodig. De effectiviteit van dergelijke beheersmaatregelen kan verbeterd worden aan de hand van onderstaande vier rode draden: **1. Op orde houden van cyberhygiëne met beheersmaatregelen** Uit de uitgevoerde toezichtonderzoeken blijkt dat de volwassenheid van de cyberhygiëne voor sommige beheersmaatregelen achterblijft bij het gestegen dreigingsniveau, onder meer bij Patch[I] - en Vulnerability[II] Management en Lifecycle Management.			

I Patch is een nieuwe versie van software. In deze nieuwe versie heeft de leverancier kwetsbaarheden in het systeem hersteld.

II Vulnerability (kwetsbaarheid) is een fout in een digitaal systeem waardoor een aanvaller in het systeem kan komen. De aanvaller kan vervolgens bij informatie of toepassingen in het systeem komen terwijl hij dat niet mag.

Algemeen beeld:	**2. Frequentie en dekkingsgraad van beveiligingstesten** Bijna alle onder toezicht staande instellingen voeren beveiligingstesten zoals red team testen en penetratietesten uit, maar hierin is ruimte voor verbetering. Onder andere in de frequentie van beveiligingstesten en in het betrekken van derde partijen in de uitvoering van deze testen. **3. Zicht op de uitbestedingsketen** Uit gestructureerde zelfbeoordelingen komt het beeld naar voren dat de volwassenheid van de beheersmaatregelen op dit gebied vrijwel ongewijzigd is. Er is dus geen sprake van een significante verbetering of verslechtering ten opzichte van de vorige meting. Vorig jaar heeft DNB gerapporteerd dat "niet alle instellingen de juiste risicomanagement-processen hebben ingeregeld rondom hun dienstverleners en dat het soms ontbreekt aan een volledig inzicht in de beheersmaatregelen bij dienstverleners en eventuele onderaannemers in de uitbestedingsketen." Aandacht voor uitbesteding blijft onverminderd nodig omdat uitbesteding blijft toenemen. Gezien de dreiging van cyberaanvallen die zich meer en meer richten op dienstverleners van financiële instellingen is het van belang oog te hebben voor de effectiviteit van beheersmaatregelen in de uitbestedingsketen. **4. Risicomanagement** In het vorige Samenhangend Inspectiebeeld 2021-2022 is aangegeven dat de toezichthouders in algemene zin ruimte zien voor verbetering van de risicomanagementcyclus gericht op integrale beveiliging. Vier aandachtsgebieden zijn daarbij specifiek genoemd: I) de integratie van beveiliging in het overkoepelende risicomanagement raamwerk; II) het actualiseren van scenario's op het snel veranderende dreigingsbeeld; III) het meten van de effectiviteit van mitigerende maatregelen en IV) het inregelen van het risicomanagementproces rondom leveranciers. Aandachtsgebied IV is reeds behandeld onder kopje 3 in dit kader: de awareness bij instellingen met betrekking tot risicomanagement rondom uitbesteding is gestegen, maar daarnaast zijn er nog verbeteringen mogelijk door meer inzicht te verkrijgen in de effectiviteit van beheersmaatregelen in de uitbestedingsketen. Voor wat betreft de aandachtsgebieden onder I, II en III ziet DNB in de uitvoering van haar toezichtwerkzaamheden dat cyberrisico's voldoende aandacht krijgen, maar dat de volwassenheid van beheersmaatregelen niet in gelijke mate meegroeit met het stijgende dreigingsniveau. Voor de bovenstaande vier aandachtsgebieden is extra aandacht benodigd, zowel vanuit onder toezicht staande instellingen als vanuit toezichthouders. De komst van de Digital Operational Resilience Act (DORA) kan hier ondersteunend bij zijn.
Interventie:	De uitkomsten van surveys en questionnaires worden onder andere 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 door 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) en Rijksinspectie Digitale Infrastructuur (RDI).

Toezichthouder: Inspectie Gezondheidszorg en Jeugd (IGJ)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Niet van toepassing; zie algemene opmerkingen onder tabel bij (*)		Particuliere klinieken voor medisch specialistische zorg	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz; hieruit volgt de verplichting te voldoen aan de NEN 7510)	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
-	Werking van het ISMS	-	-	-
Aanleiding:	In 2021 en het voorjaar van 2022 heeft de IGJ 10 particuliere klinieken voor medisch specialistische zorg bezocht om te zien hoe zij digitale zorg bieden. Hierbij zijn grote, landelijk werkende organisaties met meerdere locaties en een breed zorgaanbod, maar ook kleinere aanbieders met een focus op een specifiek zorgaanbod bezocht. Informatiebeveiliging was één van de thema's binnen dit onderzoek. Particuliere klinieken moeten op grond van de Wabvpz aantoonbaar zorgen voor een managementsysteem voor informatiebeveiliging (ISMS) dat voldoet aan de wettelijke norm NEN 7510. Hiervoor moet minimaal een onafhankelijke beoordeling aanwezig zijn van het ISMS.			
Status onderzoek:	Afgerond (afgezien van nog lopende verbeterplannen)			
Algemeen beeld:	Alle bezochte klinieken hadden maatregelen genomen op het gebied van informatiebeveiliging. Drie klinieken waren gecertificeerd volgens de NEN 7510-norm. Hoewel certificering wettelijk niet verplicht is, vindt de inspectie dit wel wenselijk. Certificering is een extra middel om informatiebeveiliging blijvend te borgen in de organisatie. Bij de meeste bezochte klinieken bleek het informatiebeveiligingsbeleid nog niet voldoende geborgd in de organisatie. Zo ontbrak bij 7 klinieken op het moment van het bezoek een recente, onafhankelijke beoordeling van het managementsysteem voor informatiebeveiliging. Daarmee was niet helder of de klinieken een effectief werkende aanpak van informatiebeveiliging hadden.			
Interventie:	Bij particuliere klinieken 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.			
Relatie met andere toezichthouder:	Zie algemene opmerking onder (**).			

(*) in het kader van de Wbni zijn vooralsnog geen zorgaanbieders aangewezen. Met de komst van de Europese NIS2-richtlijn gaat dat veranderen.

(**) De AP houdt in het kader van de AVG 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 Gezondheidszorg en Jeugd (IGJ)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Niet van toepassing (*)		Zorgaanbieders in de sector gehandicaptenzorg	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (verplichting te voldoen aan de NEN 7510)	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
-	Werking van het ISMS	-	-	-
Aanleiding:	In de periode 2017-2022 bezocht de IGJ 13 zorgaanbieders voor gehandicaptenzorg voor een thematisch toezicht op het gebied van e-health/digitale zorg. Hierbij was de inrichting van de informatiebeveiliging één van de thema's. Ook organisaties voor gehandicaptenzorg moeten op grond van de Wabvpz aantoonbaar zorgen voor een ISMS dat voldoet aan de wettelijke norm NEN 7510. Hiervoor moet minimaal een onafhankelijke beoordeling aanwezig zijn van het ISMS.			
Status onderzoek:	Afgerond (afgezien van nog lopende verbeterplannen)			
Algemeen beeld:	Alle bezochte zorgaanbieders hadden maatregelen genomen op het gebied van informatiebeveiliging. Twee zorgaanbieders waren gecertificeerd volgens de NEN 7510-norm of de ISO 27001-norm (die aan de NEN 7510 ten grondslag ligt). Sommige zorgaanbieders hadden creatieve werkwijzen gevonden om het personeel bewust te maken van het belang van informatiebeveiliging. Zo had een zorgaanbieder hiervoor een speciale thematische escape room ingericht. Bij de meeste bezochte zorgaanbieders bleek het informatiebeveiligingsbeleid echter nog niet voldoende geborgd in de organisatie. Zo ontbrak bij de meeste aanbieders op het moment van het bezoek een recente, onafhankelijke beoordeling van het managementsysteem voor informatiebeveiliging. Daarmee was niet helder of de zorgaanbieders een effectief werkende aanpak van informatiebeveiliging hadden.			
Interventie:	Bij de 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. Zorgaanbieders die nog veel beheersmaatregelen moesten inrichten, hadden hier wel veel tijd voor nodig (in meerdere gevallen langer dan een jaar).			
Relatie met andere toezichthouder:	Zie algemene opmerking onder (**).			

(*) in het kader van de Wbni zijn vooralsnog geen zorgaanbieders aangewezen. Met de komst van de Europese NIS2 richtlijn gaat dat veranderen.

(**) De AP houdt in het kader van de AVG 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 Gezondheidszorg en Jeugd (IGJ)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Niet van toepassing (*)		Ziekenhuizen	Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (verplichting te voldoen aan de NEN 7510)	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
-	Werking van het ISMS	-	-	-
Aanleiding:	In 2022 heeft de IGJ aan alle ziekenhuizen waarvan de actuele status van het ISMS niet bekend was schriftelijk vragen gesteld over de mate waarin het ISMS aantoonbaar voldeed aan de wettelijke norm NEN 7510. Hierbij is tevens gevraagd om onderbouwend bewijsmateriaal. Het ging om 51 ziekenhuizen. Met alle betrokken ziekenhuizen zijn daarna vervolgafspraken gemaakt, die erop gericht zijn dat de ziekenhuizen uiterlijk eind 2023 aantoonbaar kunnen voldoen aan de wettelijke norm. Daarnaast doet de IGJ sinds 2018 in geval van grootschalige ICT-storingen bij ziekenhuizen stelselmatig navraag naar aard, verloop en gevolgen hiervan. Deze storingen blijken overigens in het algemeen niet het gevolg van beveiligingsproblematiek, maar de norm voor informatiebeveiliging gaat wel degelijk in op aspecten die ook invloed hebben op het ontstaan en verloop van storingen, zoals wijzigingsprocedures.			
Status onderzoek:	Niet afgerond; zal naar verwachting worden afgerond in 2023.			
Algemeen beeld:	Bij de betrokken ziekenhuizen was eind 2022 al duidelijke voortgang te zien in de implementatie van de NEN 7510 en de inrichting van een plan-do-check-act-cyclus die op basis van de NEN 7510 vereist is. Een deel van de ziekenhuizen bevond zich in een formeel certificeringstraject of had dit zojuist afgerond. Een ander deel was bezig met de uitvoering van een verbeterplan naar aanleiding van een in 2022 uitgevoerde onafhankelijke beoordeling. Tenslotte was er een groep die weliswaar maatregelen had genomen op het gebied van informatiebeveiliging, maar hiervoor na 2022 nog een eerste onafhankelijke beoordeling moest laten uitvoeren. Verbetermaatregelen hadden veelal te maken met het inrichten van de check- en actfases van de volgens NEN 7510 vereiste plan-do-check-act-cyclus, zodat het informatiebeveiligingsbeleid in de praktijk ook daadwerkelijk gemonitord en verbeterd wordt.			
Interventie:	Bij de ziekenhuizen 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 traject was eind 2022 nog niet afgerond.			
Relatie met andere toezichthouder:	Zie algemene opmerking onder (**)			

(*) in het kader van de Wbni zijn vooralsnog geen zorgaanbieders aangewezen. Met de komst van de Europese NIS2 richtlijn gaat dat veranderen.

(**) De AP houdt in het kader van de AVG 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:**	
NCTV Categorie B Vitale Processen - Communicatie met en tussen hulpdiensten middels 112 en C2000		OOV	Baseline Informatiebeveiliging Overheid (BIO)	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Risicomanagement	-	-	-	-
Aanleiding:	**In haar rapport van februari 2022 stelt de IJenV dat het bestuur van de meldkamers prioriteit moet geven aan het in kaart brengen van cyberrisico's en hoe die aan te pakken. De meldkamers moeten meer werk maken van het inschatten van risico's op digitale aanvallen op hun systemen. Wanneer de systemen van meldkamers verstoord raken, zijn de hulpdiensten niet goed bereikbaar. De hulpverlening, crisisbeheersing en opsporing lopen dan gevaar.** In 2022 heeft de Inspectie en de RDI een toetsingskader opgesteld voor het toezicht op de continuïteit van de meldkamers. Met dit toetsingskader wordt de basis gelegd voor het toezicht op de meldkamers. Het toetsingskader is gebaseerd op de Regeling beleid en beheer meldkamers en de toezeggingen die de minister aan de Tweede Kamer heeft gedaan om de continuïteit van de meldkamers te waarborgen. ***Toezicht op de informatiebeveiliging C2000*** C2000 is het communicatiesysteem voor de hulpdiensten. Politie, brandweer, ambulancediensten, onderdelen van het ministerie van Defensie en daaraan gekoppelde organisaties gebruiken het digitale systeem voor hun mobiele communicatie. Sinds 2015 heeft het ministerie van Justitie en Veiligheid en de Nationale Politie ingezet op de vernieuwing van de (centrale) IT infrastructuur C2000 en het C2000 telecommunicatienetwerk.			
Status onderzoek:	Het rapport risicomanagement meldkamers is afgerond. De meldkamers en C2000 worden in 2023 via regulier toezicht gemonitord.			
Algemeen beeld:	Blijkens diverse documenten en gesprekken is in opzet de nodige aandacht voor informatiebeveiliging C2000, door zowel het ministerie van Justitie en Veiligheid alsook door de nationale politie. Een nog uit te voeren nulmeting naar de staat van cybersecurity en cyberweerbaarheid van C2000 moet in 2023 meer (in)zicht gaan verschaffen in de feitelijke getroffen beheers- en beveiligingsmaatregelen.			
Interventie:	Geen			
Relatie met andere toezichthouder:	RDI			

Toezichthouder: Inspectie Leefomgeving en Transport (ILT)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Drinkwatervoorziening		Drinkwater	Wbni & Drinkwaterwet	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
-	-	-	Van toepassing	-
Aanleiding:	In 2021 heeft de ILT een eerste inspectieronde in het kader van de Wbni uitgevoerd binnen de sector. Eén van de uitkomsten was dat actieve monitoring – ofwel detectie en respons – nadere aandacht behoeft. Voor 2022/2023 wordt daarom op dit thema verdiepend geïnspecteerd.			
Status onderzoek:	Inspecties lopen. Afronding in het derde kwartaal van 2023.			
Algemeen beeld:	Alle 10 drinkwaterbedrijven worden aan deze inspectie onderworpen. Omdat de inspecties nog niet afgerond zijn, is nog geen algemeen beeld voor de sector vast te stellen.			
Interventie:	Er hebben geen interventies plaatsgevonden.			
Relatie met andere toezichthouder:	Niet van toepassing			

Toezichthouder: Inspectie Leefomgeving en Transport (ILT)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Drinkwatervoorziening		Drinkwater	Wbni & Drinkwaterwet	
	Organisatie van netwerk- en informatiebeveiligings-beheer	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Van toepassing	Van toepassing	Van toepassing	Van toepassing	Van toepassing
Aanleiding:	Begin 2021 heeft de ILT Waternet onder verscherpt toezicht gesteld in verband met tekortkomingen in haar cybersecurity en de aansturing daarop. Tijdens dit verscherpte toezicht wordt gemonitord of Waternet de benodigde verbeteringen daadwerkelijk realiseert.			
Status onderzoek:	Afgerond. In december 2022 is besloten dat per 1 januari 2023 Waternet weer valt onder het reguliere toezichtregime.			
Algemeen beeld:	De eerder geconstateerde tekortkomingen zijn door Waternet opgelost. De organisatie heeft laten zien 'in control' te zijn ten aanzien van cybersecurity. Het gaat hierbij om de ICT-systemen (procesautomatisering) ten behoeve van levering en kwaliteit van het drinkwater.			
Interventie:	Beëindiging verscherpt toezicht: terug naar regulier toezicht.			
Relatie met andere toezichthouder:	Niet van toepassing			

Toezichthouder: Inspectie Leefomgeving en Transport (ILT)				
Vitaal proces:		**Sector:**	**Grondslag:**	
Vlucht- en vliegtuigafhandeling		Vervoer	Wbni	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Van toepassing	Van toepassing	Van toepassing	Van toepassing	Van toepassing
Aanleiding:	De ILT is in het vierde kwartaal van 2021 gestart met het voorbereiden en uitvoeren van inspecties binnen deze sector. Doel van deze inspecties is om een eerste beeld op te bouwen in hoeverre alle deelonderwerpen zoals benoemd in de Ministeriële Regeling IenW (MR) afgedekt worden bij de vitale aanbieders. De MR dekt alle 5 hierboven benoemde thema's af. Daarnaast wordt rekening gehouden met komende EASA-regelgeving ten aanzien van cybersecurity. Het onderzoek wordt uitgevoerd middels een begeleid self assessment. Governance op cybersecurity is ook onderdeel van de inspectie.			
Status onderzoek:	In het vierde kwartaal van 2022 is de eerste inspectieronde bij 5 van de 6 vitale aanbieders afgerond.			
Algemeen beeld:	De sector laat een divers beeld zien. Mede veroorzaakt door de soms totaal verschillende aard van de onderzochte vitale aanbieders. Voor de meeste vitale aanbieders) geldt dat ze in opzet grotendeels voldoen aan de Wbni / MR. Met name inbedding van de meldplicht in de organisatie-procedures vraagt hier en daar nog aandacht (dat kan de OTS relatief eenvoudig en snel realiseren). Voor een vitale aanbieder geldt dat ten aanzien van de zorgplicht en de meldplicht enkele tekortkomingen zijn geconstateerd. De benodigde verbeteringen zijn inmiddels geïdentificeerd en in gang gezet. Voor een andere vitale aanbieder geldt dat de inspectie nog niet formeel is afgerond. Door het ontbreken van informatie konden nog niet alle systemen die vallen binnen de Wbni worden geïnspecteerd.			
Interventie:	De ILT volgt in 2023 de voortgang van de benodigde verbeteringen. Voor de nog ontbrekende informatie levert de betreffende vitale aanbieder de resterende informatie zo spoedig mogelijk op. Voor de overige vitale aanbieders waren geen interventies.			
Relatie met andere toezichthouder:	Niet van toepassing			

Toezichthouder: Rijksinspectie Digitale Infrastructuur (RDI) - Telecom				
Vitaal proces:		**Sector:**	**Grondslag:**	
Spraakdienst en SMS Internet en dataverkeer		ICT/Telecom Digitale Infrastructuur	Telecomwet	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Risicomanagement	Besluit beveiliging gegevens telecommunicatie (BBGT)	Detectie, Logging en Monitoring	Incidentenbeheer	Incidentenonderzoek
Aanleiding:	Telecom Security (Bevoegd aftappen/beveiliging) 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 de RDI een onderzoek bij deze telecomaanbieder.			
Status onderzoek:	Afgerond			
Algemeen beeld:	Uit het onderzoek blijkt dat de beveiliging niet op alle onderdelen aan de wettelijke vereisten voldeed. John Derksen, hoofd Toezicht van Agentschap Telecom: ''Het onderzoek laat zien dat KPN 'de voordeur' tot haar systemen voldoende beveiligd heeft. Niemand anders dan KPN bepaalt wie er toegang krijgt tot de systemen. Het onderzoek laat echter ook zien dat een beperkte groep systeembeheerders die toegang had tot de systemen, niet over de vereiste Verklaring omtrent het Gedrag (VOG) en een geheimhoudingsverklaring beschikte. Deze personen hadden bovendien geen persoonlijk account. Daardoor konden hun individuele handelingen niet goed worden gevolgd en geregistreerd.'' KPN heeft tijdens het onderzoek maatregelen genomen om de veiligheid van het aftapsysteem op het vereiste niveau te brengen. KPN heeft aangegeven dat het autorisatieproces inmiddels is verbeterd en dat alle beheerders nu over de vereiste documenten beschikken. De RDI heeft essentiële delen van de verbeteringen gezien en de overige verbeteringen worden gecontroleerd in het reguliere inspectieproces onder de aangescherpte zorgplicht.			
Interventie:	KPN is een boete opgelegd van 450.000 euro.			
Relatie met andere toezichthouder:	Niet van toepassing.			

Toezichthouder: Rijksinspectie Digitale Infrastructuur (RDI) - Telecom				
Vitaal proces:		**Sector:**	**Grondslag:**	
Spraakdienst en SMS Internet en dataverkeer		ICT/Telecom Digitale Infrastructuur	Telecomwet	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Risicomanagement	Rvit	Detectie, Logging en Monitoring	Incidentenbeheer	Incidentenonderzoek
Aanleiding:	Telecom Security (Rvit) De Regeling veiligheid en integriteit telecommunicatie (hierna: Rvit) omvat nadere regels voor de netwerken van de drie mobiele netwerkaanbieders KPN, T-Mobile en Vodafone (hierna: de netwerkaanbieders). Hiermee wordt de weerbaarheid van hun netwerken verhoogd tegen actuele dreigingen als spionage of misbruik.			
Status onderzoek:	Gestart			
Algemeen beeld:	Met ingang van 1 oktober 2022 moeten de netwerkaanbieders aan de beheersmaatregelen hebben voldaan. In aanloop naar 1 oktober 2022 heeft de RDI gesprekken met hen gevoerd. Daarnaast is de netwerkaanbieders per brief van 1 september 2022 verzocht de stand van zaken per 1 oktober 2022 aan te leveren in de vorm van een self assessment. Zij hebben tijdig de gevraagde informatie aangeleverd.			
Interventie:	Begin 2023 zal de RDI een beeldvormende inspectie bij hen uitvoeren. Hierin wordt het (administratieve) beeld van de netwerkaanbieders met hen besproken en op onderdelen geverifieerd. Naast de beeldvormende inspecties zal de RDI vanaf 2023 ook thematische inspecties gaan uitvoeren op de implementatie van de beheersmaatregelen uit de Rvit en de zorgplicht uit hoofdstuk 11a van de Tw. Deze inspecties zullen risicogericht vormgegeven worden en vormen een onderdeel van het reguliere toezicht dat de RDI zal gaan uitvoeren op het gebied van de Rvit in de komende jaren.			
Relatie met andere toezichthouder:	Niet van toepassing.			

Toezichthouder: Rijksinspectie Digitale Infrastructuur (RDI) - Vertrouwensdiensten				
Vitaal proces:		**Sector:**	**Grondslag:**	
Vertrouwensdiensten		Digitale Infrastructuur	eIDAS verordening en Telecomwet	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
Risico op identiteitsfraude	Procesbeheer Leveranciersbeheer	Governance, (AI) risico beheersing	Registratie en analyse	-
Aanleiding:	Vertrouwensdiensten vormen in veel gevallen de link tussen een natuurlijke- of rechtspersoon en een digitale transactie. Vandaar dat de vaststelling van de identiteit van de natuurlijke persoon of vertegenwoordiger van de rechtspersoon die de dienst afneemt een essentieel onderdeel is van een vertrouwensdienst. Naast identiteitsvaststelling bij fysieke aanwezigheid zien we sinds 2020 een sterke groei in zogenaamde Identificatie op Afstand (IoA). Hierbij wordt bijvoorbeeld via een videoverbinding of door middel van geautomatiseerde toepassingen (apps) de identiteit van de afnemer vastgesteld zonder fysiek contact. Met name bij het gebruik van geautomatiseerde toepassingen ziet de RDI een sterke opmars van AI-technologie. Deze opmars is in lijn met de digitale transformatie, en wordt nog versterkt door de Covid-crisis. Het is de verwachting dat deze opmars de komende jaren alleen maar zal toenemen. Het gebruik van IoA, en met name het gebruik van AI-technologie introduceert nieuwe systemen met nieuwe leveranciers-ketens, en vooral nieuwe risico's in het ecosysteem van vertrouwensdiensten. Gezien het belang van identificatie binnen vertrouwensdiensten, zag RDI de noodzaak tot nader onderzoek en sturing op de beheersing van deze risico's binnen de kaders van bestaande wet- en regelgeving.			
Status onderzoek:	De RDI heeft bij gekwalificeerde verleners van vertrouwensdiensten die IoA gaan gebruiken een afzonderlijk onderzoek ingesteld.			
Algemeen beeld:	Over het algemeen zien we dat vertrouwensdienstverleners stimulans vanuit de markt ondervinden om innovatieve IoA toepassingen in te zetten. Ook vanuit economische overwegingen (bijvoorbeeld een krappe arbeidsmarkt) is er druk op de inzet van geautomatiseerde oplossingen en het gebruik van AI. Daarbij bestaat er bij vertrouwensdienstverleners over het algemeen een sterk besef van hun rol en aansprakelijkheid in het voorkomen van veiligheidsincidenten in hun vertrouwensdiensten. We zien dat vertrouwensdienstverleners zoekende zijn in deze belangenafweging en naar partijen die hen daarbij kunnen ondersteunen. Daarbij komen met name leveranciers van innovatieve oplossingen in beeld. Onder de nieuwe leveranciers van IoA toepassingen, met name bij gebruik van AI, zijn veel innovatieve pioniers. De sterk georganiseerde risicobeheersing die gebruikelijk is in het ecosysteem van (gekwalificeerde) vertrouwensdienstverleners hebben zij (nog) niet altijd eigen gemaakt. . Andersom kunnen de vertrouwensdienstverlening nog meer ervaring opdoen met het beheersen van specifieke risico's rond de inzet van AI-toepassingen in hun processen. Als gevolg hiervan zien we op meerdere plaatsen in de keten verbetermogelijkheden in verstrekking van de juiste informatie, niveau van risicoanalyse en verantwoordelijkheid voor beheersmaatregelen. Het ontbreken van specifieke wet- en regelgeving en Europese normen waarmee de beheersing van AI toepassingen kan worden vormgegeven vormt een uitdaging. Hoewel de RDI deze situatie herkent en heeft aangekaart bij beleidsmakers en normeringsinstanties, staat een verantwoorde inzet van innovatieve toepassingen voorop. Een vertrouwensdienstverlener die de keuze maakt IoA met AI in te zetten dient samen met haar leveranciersketen tot een complete risicoafweging en passende beheersmaatregelen te komen. Dit is ook binnen de kaders van bestaande wet- en regelgeving een vereiste.			
Interventie:	Tot nu toe worden vereiste reparaties en herstelmaatregelen door partijen goed en binnen gestelde termijnen opgepakt.			
Relatie met andere toezichthouder:	RDI werkt samen met de andere Europese toezichthouders op vertrouwensdiensten in FESA, het forum voor Europese toezichthouders op het gebied van elektronische handtekeningen. Binnen FESA wordt intensief kennis en ervaring uitgewisseld over de onderwerpen IoA en AI binnen vertrouwensdiensten. Daarnaast wordt gebruik gemaakt van ondersteuning door het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) voor de organisatie van EU-breed onderzoek en conferenties met stakeholders.			

Toezichthouder: Rijksinspectie Digitale Infrastructuur (RDI) - Wbni				
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	Wbni	
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Gevolgen van incidenten beperken**
-	-	-	-	Business Continuity Management (BCM)
Aanleiding:	Het is onvermijdelijk dat er situaties ontstaan die zijn veroorzaakt door grote verstoringen of andere dreigende situaties zoals een pandemie of grootschalig kwetsbaarheid. Organisaties dienen in deze gevallen voorbereid te zijn om de impact van die gebeurtenissen op de essentiële dienst te beperken. BCM is daarom een belangrijk onderwerp. RDI hanteert onderstaande definitie voor BCM: "De managementprocessen die de continuïteit van de kritische processen van een organisatie waarborgen. De processen zijn erop gericht om de impact van een verstoring te beperken en zo snel mogelijk weer een acceptabel dienstenniveau te bereiken."			
Status onderzoek:	Naar verwachting in januari 2023 afgerond.			
Algemeen beeld:	***Netbeheer*** Binnen het netbeheer is continuïteit van dienstverlening en het verhelpen van storingen van oudsher een kerntaak om de beschikbaarheid te borgen. Dit verklaart waarom inspecteurs in alle gevallen een veerkrachtige crisisorganisatie hebben aangetroffen. De sector heeft invulling gegeven aan het onderwerp BCM. Hierbij hebben zij inzicht gekregen in hun kritische processen, dreigingen en afhankelijkheden voor de essentiële dienst. Op basis hiervan zijn maatregelen getroffen, zoals bijvoorbeeld het opstellen van continuïteitsplannen en het inrichten van crisisstructuren. Organisaties maken betrokkenen bewust van de risico's en de processen. Dit bewustzijn wordt versterkt door het regelmatig oefenen met scenario's. Voor BCM gebruiken de organisaties verschillende methodieken en best practices. ***Digitale Infrastructuur*** Zoals bij netbeheer ligt ook bij DI de focus van BCM op de continuïteit van de dienstverlening en het verhelpen en herstellen van storingen. De sector heeft op diverse wijzen invulling gegeven aan BCM. Hierbij zijn de processen over het algemeen niet volgens bekende internationale BCM-normen opgezet, maar sommige organisaties hebben hier wel plannen voor. De BCM-plannen worden door alle organisaties ontwikkeld op basis van een risicoanalyse en deze worden dan ook regelmatig bijgewerkt naar de actuele risico's.			
Interventie:	Diverse organisaties hebben naar aanleiding van (bevindingen uit) de inspectiewerkzaamheden verbeteringen onderkend en opgepakt.			
Relatie met andere toezichthouder:	Niet van toepassing			

bijlage 2
Bronnen

foto: Rob Poelenjee

1 Richtlijn (EU) 2016/1148, via https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016L1148&qid=1680093737005

2 Wet beveiliging netwerk- en informatiesystemen, via https://wetten.overheid.nl/BWBR0041515/2022-12-01

3 'Vitale Infrastructuur', NCTV, https://www.nctv.nl/onderwerpen/vitale-infrastructuur

4 'Vitale aanbieders', NCTV, https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni/vitale-aanbieders

5 'Samenhangend Inspectiebeeld cybersecurity vitale processen 2021-2022', toezichthouders op cybesecurity van vitale processen, https://www.rijksoverheid.nl/documenten/rapporten/2022/07/06/tk-bijlage-samenhangend-v-cybersecurity-vitale-processen-21-22

6 'Cybersecurity Woordenboek 2021', Cybersecurity Alliantie, https://www.cybersecurityalliantie.nl/ecp_images/2021/12/Cybersecurity-Woordenboek-2021_ZonderSpreads.pdf

7 Richtlijn (EU) 2022/2555, via https:/eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32022L2555&qid=1680094478347

8 Verordening (EU) 2016/679, via https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679&qid=1680094520396

9 'Cybersecurity Woordenboek 2021', Cybersecurity Alliantie, https://www.cybersecurityalliantie.nl/ecp_images/2021/12/Cybersecurity-Woordenboek-2021_ZonderSpreads.pdf

10 'Start een ketensamenwerking, handreiking', NCSC, https://www.digitaltrustcenter.nl/sites/default/files/bestanden/website/NCSC%20Handreiking%20ketensamenwerking.pdf

11 'Mimecast-certificaat gebruikt bij aanval op Microsoft 365-accounts', Security.nl, 12 januari 2021, https://www.security.nl/posting/685744/Mimecast-certificaat+gebruikt+bij+aanval+op+Microsoft+365-accounts

12 'Operational Technology', Digital Trust Centre, https://www.digitaltrustcenter.nl/informatie-advies/operational-technology#:~:text=Operational%20Technology%20(OT)%20is%20een,monitoren%20van%20(industri%C3%ABle)%20apparatuur

13 'TIBER-NL', DNB, https://www.dnb.nl/voor-de-sector/betalingsverkeer/tiber-nl/

14 'Multifactorauthenticatie', NCSC, https://www.ncsc.nl/onderwerpen/multifactorauthenticatie

15 'Toegang', NCSC, https://www.ncsc.nl/onderwerpen/toegang

16 'Loginformatie', NCSC, https://www.ncsc.nl/onderwerpen/loginformatie

17 'Netwerksegmentatie', NCSC, https://www.ncsc.nl/onderwerpen/netwerksegmentatie

18 Basismaatregelen cybersecurity, NCSC, https://www.ncsc.nl/onderwerpen/basismaatregelen

19 Richtlijn (EU) 2022/2557, via
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32022L2557&qid=1680095388684

20 Verordening (EU) 2022/2554, via
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32022R2554&qid=1680096148067

21 'Nederlandse Cybersecuritystrategie 2022-2028', NCTV,
https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/nlcs-2022/NLCS_2022_19.pdf

22 'Nieuwe technologieën en nieuwe samenwerkingen', Inspectieraad,
https://www.rijksinspecties.nl/onderwerpen/programma-innovatie-toezicht/nieuwe-technologieen-en-nieuwe-samenwerkingen

Dit is een uitgave in opdracht van het Overleg Toezichthouders cybersecurity vitale processen

Voor meer informatie over deze uitgave:

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat
Postbus 450 | 9700 AL | Groningen

communicatie@rdi.nl
T: +31 (0) 88 041 60 00 (ma t/m vrij 8.30 – 17.00)

Mei 2023