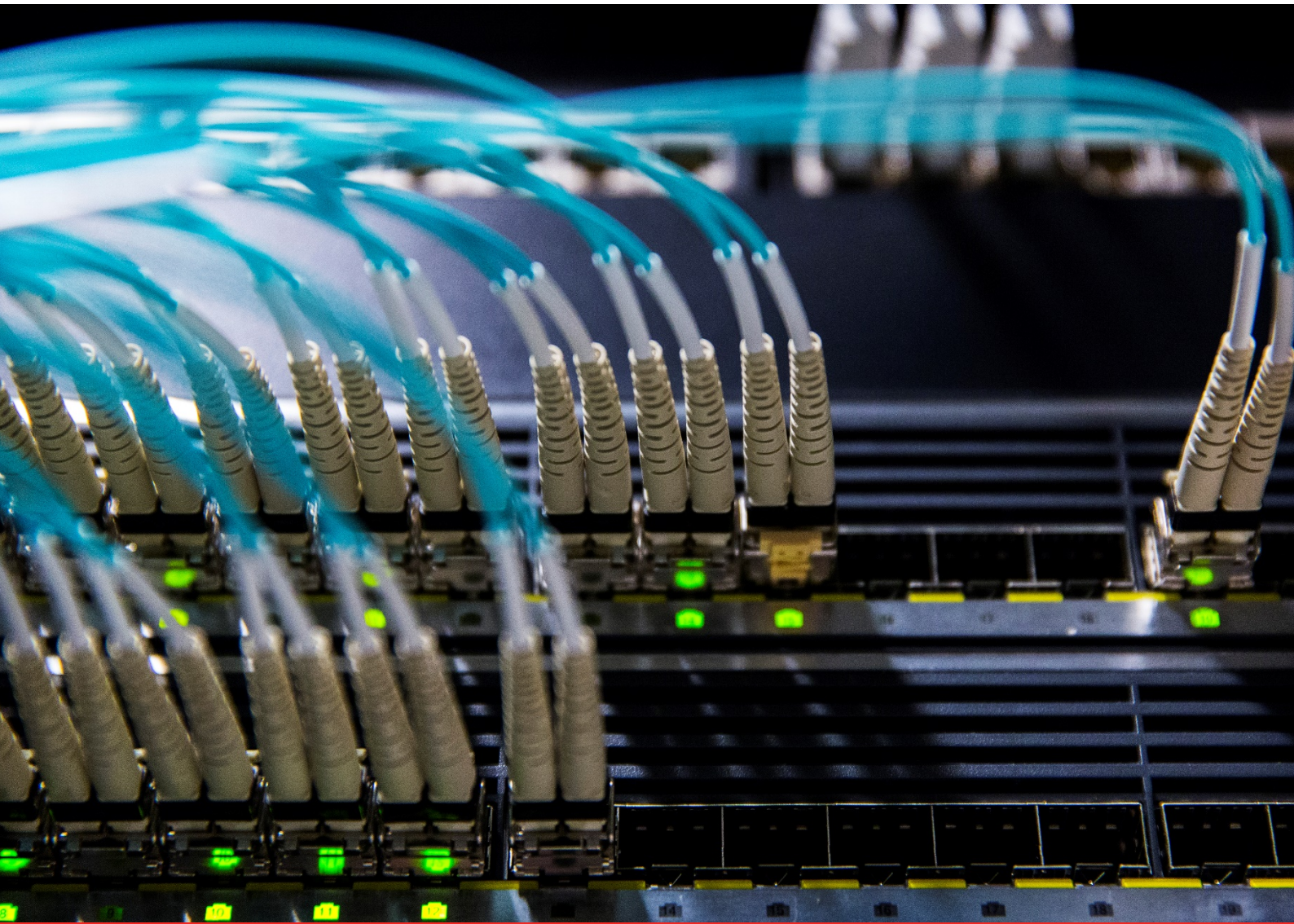
Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

Onderzoeksrapport Stichting Waternet

Onderzoek naar de toestand van de cybersecurity en besturing bij Stichting Waternet in het kader van de leveringszekerheid en kwaliteit van drinkwater



Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

Onderzoeksrapport Stichting Waternet

Onderzoek naar de toestand van de cybersecurity en besturing bij Stichting Waternet in het kader van de leveringszekerheid en kwaliteit van drinkwater

Datum 31 maart 2021

Colofon

Uitgegeven door

Inspectie Leefomgeving en Transport
Directie Publieke instituties en control
Afdeling Toezicht publieke instellingen
Vakgroep Drinkwater

Postbus 16191, 2500 BD Den Haag

088 489 00 00
www.ilent.nl

Inhoud

Colofon—5

Inhoud—7

Samenvatting—9
Stichting Waternet—9

1 Inleiding—11
1.1 Stichting Waternet—11
1.2 Aanleiding—11
1.3 Doelstelling en vraagstelling onderzoek—11
1.4 Onderzoeksaanpak—11
1.5 Reikwijdte van onderzoek—12

2 Cybersecurity—13
2.1 Inleiding—13
2.2 Afhankelijkheid van PA—13
2.3 Zorgplicht—14
2.3.1. Status implementatie BIO—15
2.3.2. Status implementatie PA-norm—16
2.3.3. Onderwerpen nader onderzocht—17
2.4 Meldplicht—21
2.5 Conclusies cybersecurity—22

3 Besturing en waarborging drinkwatertaak—24
3.1 Inleiding—24
3.2 Inrichting en functioneren van de bestuurlijke structuur—24
3.2.1. Inrichting van de bestuurlijke structuur—24
3.2.2. Functioneren van de bestuurlijke structuur—26
3.2.3. Conclusies inrichting en functioneren van de bestuurlijke structuur—27
3.3 Aansturing en waarborgen drinkwatertaken en IT—29
3.3.1. Werking organisatie nader in beeld—29
3.4 Conclusies aansturing drinkwatertaken en IT—31
3.5 Cultuur—32
3.6 Conclusie cultuur—33

4 Conclusie risico's kwaliteit en leveringszekerheid drinkwater—34

Bijlage A Onderzoeksproces—35

Bijlage B Onderzoekskader cybersecurity—36

Bijlage C Onderzoekskader besturing en waarborging drinkwater—39

Bijlage D Overzicht geconstateerde tekortkomingen—41

Samenvatting

Stichting Waternet

Stichting Waternet is een organisatie die taken uitvoert voor de gehele waterkringloop. In Amsterdam en omgeving levert Stichting Waternet drinkwater en beheert de riolering. In het gebied van Waterschap Amstel Gooi en Vecht beheert Stichting Waternet de waterpeilen en dijken en zorgt voor zuivering van afvalwater. Daarnaast bedient Stichting Waternet bruggen en sluizen.

Aanleiding en doel

In de media is in september en november 2020 het signaal naar voren gekomen dat de cybersecurity bij Waternet niet op orde zou zijn en dat de besturing bij Waternet verbeteringen ten aanzien van cybersecurity zou belemmeren. Dit signaal, in combinatie met de uitkomst van een bestuurlijk gesprek met Stichting Waternet over dit signaal, was voor de Inspectie Leefomgeving en Transport (ILT) reden om een onderzoek naar de cybersecurity en de besturing bij Waternet in te stellen.

Het doel van dit onderzoek is vast te stellen in hoeverre er sprake is van risico's voor de waarborging van de kwaliteit en leveringszekerheid van drinkwater. De drinkwaterproductie is sterk afhankelijk van geautomatiseerde processen. Cybersecurity is dus van vitaal belang.

De ILT heeft de praktijk bij Waternet getoetst aan het wettelijk kader voor de zorgplicht en de meldplicht[1] voor de cybersecurity. De Drinkwatersector heeft een eigen norm opgesteld voor de procesautomatisering (PA-norm) om invulling te geven aan de zorgplicht. De ILT heeft de onderdelen van deze PA-norm meegenomen in haar onderzoek.

Daarnaast heeft het onderzoek tot doel zicht te krijgen of er sprake is van een doeltreffende sturing op cybersecurity en drinkwater.

Conclusies cybersecurity en besturing

Waternet heeft zowel op bestuurlijk als organisatorisch niveau onvoldoende grip op de cybersecurity. Dit wordt veroorzaakt door tekortkomingen in de uitvoering van wettelijke zorgplicht en meldplicht en in de besturing van de organisatie. De belangrijkste tekortkomingen in de zorgplicht zijn: onvoldoende risicomanagement, onvoldoende evaluatie en verbeterprocessen, en beperkingen in detectie en incident-response. Daarnaast doet de ILT in dit rapport vele constateringen op onderdelen van de PA-norm of meer algemeen op het gebied van cybersecurity bij Waternet.

Voor wat betreft de meldplicht is te verwachten dat daadwerkelijke incidenten, die boven de drempelwaarde uitstijgen, volgens de juiste procedure gemeld zullen worden. Waternet heeft nog geen procedure voor het tweede onderdeel van de meldplicht, het melden van ICT-inbreuken die aanzienlijke gevolgen voor de

[1] De Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) is per 9 november 2018 in werking getreden. Deze wet regelt een zorgplicht (treffen van beveiligingsmaatregelen) en een meldplicht van incidenten. De Minister van Infrastructuur en Waterstaat is voor de sectoren Vervoer en Levering en distributie van drinkwater aangewezen als bevoegde autoriteit. In het Besluit beveiliging netwerk- en informatiesystemen (Bbni) worden onder meer de vitale aanbieders aangewezen die onder de reikwijdte van de verplichtingen van de Wbni vallen. De Drinkwaterbedrijven zijn binnen de Bbni aangewezen als vitale aanbieders.

continuïteit van de levering van drinkwater kunnen hebben. Als gevolg daarvan kan het mogelijk langer duren voordat incidenten opgelost zijn en kunnen de gevolgen van incidenten onnodig groter worden.

Naast de tekortkomingen in de zorgplicht en meldplicht voor cybersecurity, vormen ook de tekortkomingen in de besturing een risico voor de waarborging van kwaliteit en leveringszekerheid van drinkwater. De ILT constateert dat de besturing niet doeltreffend genoeg is, terwijl dit een belangrijke voorwaarde is voor het waarborgen van de drinkwatertaak en de cybersecurity. Borging van drinkwaterprocessen vindt vooral op operationeel niveau (op de werkvloer) plaats. Op strategisch niveau (hiermee wordt het bestuurlijk niveau bedoeld, waaronder directie en stichtingsbestuur) is waarborging van de drinkwatertaak en de cybersecurity nog niet genoeg aanwezig. In het ontwerp van de bestuurlijke structuur ontbreekt integraal toezicht op de drinkwatertaak. Er is nog geen gestructureerd risicomanagement en evaluatie en bijsturing vinden nog niet genoeg plaats.

Risico's van de tekortkomingen

De ILT is van oordeel dat Waternet, ten tijde van het ILT-onderzoek, onvoldoende 'in control' is over haar cybersecurity. Hierdoor is een verhoogd risico aanwezig op een cyberincident met mogelijke gevolgen voor de kwaliteit en/of de continuïteit van drinkwater.

Hoeveel groter de kans of impact voor het drinkwater is, laat zich niet eenvoudig kwantificeren. De beveiliging van cybersecurity leunt niet op één maatregel; maatregelen werken aanvullend op elkaar en verhogen als geheel de weerstand tegen cyberaanvallen of verkleinen als geheel de impact. Hoe groot het negatief effect van een of enkele ontbrekende of niet optimaal werkende maatregelen daadwerkelijk is, is niet exact aan te geven.

De tekortkomingen in de besturing vormen een oorzaak van de risico's die op het gebied van cybersecurity en de (overige) voorwaarden voor waarborging van de drinkwatertaak zijn geconstateerd. Dit toont het belang van verbetering van de besturing ten behoeve van waarborging van de drinkwatertaak.

Vervolg

Waternet heeft inmiddels al een aantal stappen gezet ter verbetering van de tekortkomingen in de uitvoering van de wettelijke zorgplicht en meldplicht. Tevens evalueert Waternet het besturingsmodel. De ILT vindt dit een positieve ontwikkeling, maar benadrukt het belang om zo snel mogelijk voldoende grip te hebben op het uitvoeren van verbeteringen, hier voldoende inzicht in te hebben en indien nodig tijdig bij te sturen.

De ILT stelt Waternet de komende periode onder verscherpt toezicht en gaat toezien op de verbetering van de uitvoering van de wettelijke zorgplicht en meldplicht en de besturing.

1 Inleiding

1.1 Stichting Waternet

Stichting Waternet is een organisatie die taken uitvoert voor de gehele waterkringloop. In Amsterdam en omgeving levert Stichting Waternet drinkwater en beheert de riolering. In het gebied van Waterschap Amstel Gooi en Vecht beheert Stichting Waternet de waterpeilen en dijken en zorgt voor zuivering van afvalwater. Daarnaast bedient Stichting Waternet bruggen en sluizen.

1.2 Aanleiding

De ILT houdt toezicht op de leveringszekerheid, kwaliteit en doelmatigheid van de openbare drinkwatervoorziening. De Drinkwaterwet en de Wet beveiliging netwerk- en informatiesystemen zijn daarvoor een belangrijk uitgangspunt.

In de media is in september en november 2020 het signaal naar voren gekomen dat de cybersecurity bij Waternet niet op orde zou zijn en dat de besturing bij Waternet verbeteringen ten aanzien van cybersecurity zou belemmeren. Dit signaal, in combinatie met de uitkomst van een bestuurlijk gesprek met Stichting Waternet over dit signaal, was voor de Inspectie Leefomgeving en Transport (ILT) reden om een onderzoek naar de cybersecurity en de besturing bij Waternet in te stellen.

1.3 Doelstelling en vraagstelling onderzoek

Het doel van dit onderzoek is vaststellen of er risico's zijn voor de kwaliteit en leveringszekerheid van drinkwater. Hiervoor is een kader vastgelegd in de Drinkwaterwet (DWW) en het Drinkwaterbesluit (DWB). Het wettelijk kader voor cybersecurity, vastgelegd in de Wet beveiliging netwerk- en informatiesystemen (Wbni), geeft de mogelijkheid te toetsen aan de zorgplicht en de meldplicht. Een ander doel van dit onderzoek is zicht krijgen op de inrichting en het functioneren van de besturing bij Waternet, en daarmee op waarborging van de cybersecurity en de drinkwatertaak.

Bij de uitvoering van het onderzoek staan 2 onderzoeksvragen centraal:

1) Voldoet Stichting Waternet aan de verplichtingen die de Wet bescherming netwerk- en informatiesystemen stelt?

2) Hoe is de besturing bij Waternet ingericht? En is een doeltreffende sturing op cybersecurity en drinkwater zichtbaar?

1.4 Onderzoeksaanpak

De ILT heeft dit onderzoek uitgevoerd in de periode van 24 november 2020 tot 5 februari 2021. Het betreft een kwalitatief onderzoek, op basis van documentenanalyse en interviews.

Bij het raadplegen van documenten heeft de inspectie gebruikgemaakt van de Verstoringsrisicoanalyse (VRA) en het Leveringsplan, beleidsplannen, managementrapportages, notulen van diverse overlegvergaderingen, auditrapporten, rapportages van uitgevoerde veiligheidstesten en van de uitkomsten

van eerder uitgevoerde externe onderzoeken. In totaal heeft zij 150 documenten ontvangen en bestudeerd.

De ILT heeft bij Stichting Waternet gesproken met de onafhankelijk voorzitter en het bestuurslid die tevens Dijkgraaf is bij het Waterschap Amstel, Gooi en Vecht (AGV), 5 directeuren (waaronder de algemeen directeur, secretaris-directeur, directeur financiën en control, directeur dienstverlening en directeur assets en operatie), 5 afdelingshoofden, de chief information security officer (CISO), de manager PA beheer en ontwikkeling, de security coördinator PA, de systeem architect PA/OT, de IT-manager, de regievoerder digitalisering, de adviseur risicomanagement, een business controller, de kwartiermaker SOC en een extern adviseur die via het stichtingsbestuur is ingehuurd.

Bij de gemeente Amsterdam heeft de ILT gesproken met de stedelijk directeur, de CISO en de bestuursadviseur van de wethouder.

1.5 Reikwijdte van onderzoek

Het onderzoek richt zich op de toestand van de cybersecurity, van de procesautomatisering van de drinkwatervoorziening, en op de besturing bij Waternet.

Cybersecurity
De kwaliteit van de procesautomatisering is een belangrijke voorwaarde voor de kwaliteit en leveringszekerheid van het drinkwater door Waternet. Als er geen of onvoldoende scheiding tussen de procesautomatisering en kantoorautomatisering is aangebracht, dan maken risico's die dat met zich meebrengt onderdeel uit van de scope van het onderzoek.

De volgende zaken vallen buiten de scope van het toezicht van de ILT:
- activiteiten riolering;
- waterbeheer;
- het bedienen van bruggen en sluizen.

Het onderzoek richt zich vooral op de inrichting van maatregelen die Waternet heeft getroffen rondom de zorgplicht en meldplicht binnen de Wbni. Het functioneren (de werking) van maatregelen is door de beperkte onderzoektijd slechts incidenteel en exemplarisch onderzocht.

In dit onderzoeksrapport zijn wel bevindingen opgenomen over de werking van maatregelen zoals de ILT die tijdens de uitvoering van het onderzoek, in rapporten en interviews, is tegengekomen. Dit geeft echter (voor zover al mogelijk) geen allesomvattend beeld van de werking van alle maatregelen die vallen onder de cyberbeveiliging bij Waternet.

Besturing en waarborging drinkwatertaak
Om een beeld te kunnen vormen van de besturing, richt het onderzoek zich op de inrichting en het functioneren van de bestuurlijke structuur van Waternet. Daarbij is gekeken naar de inrichting en het functioneren van de taak- en verantwoordelijkheidsverdeling rondom de drinkwatervoorziening tussen de gemeente Amsterdam, het stichtingsbestuur en de algemeen directeur van Waternet. Ook is gekeken naar de wijze waarop Waternet de drinkwatertaak heeft georganiseerd.

In bijlagen B en C staat een toelichting op het in dit onderzoek gehanteerde kader.

2 Cybersecurity

2.1 Inleiding

Om de toestand van de cybersecurity binnen Waternet te kunnen bepalen en te beoordelen, heeft de ILT een onderzoekskader (bijlage B) opgesteld. De Wbni en de Bbni zijn als vertrekpunt gehanteerd. Deze hebben tot doel de cybersecurity bij de aanbieders van essentiële diensten (AED's), waaronder de drinkwaterbedrijven, op een voldoende niveau te brengen en te houden.

In dit hoofdstuk staat de beantwoording van de eerste onderzoeksvraag centraal:

Voldoet Waternet aan de verplichtingen die de Wet bescherming netwerk- en informatiesystemen stelt?

De beantwoording van de onderzoeksvraag loopt langs de volgende deelvragen:

- In welke mate is Waternet afhankelijk van de procesautomatisering (hierna PA) voor haar leverings- en kwaliteitsverplichtingen ten aanzien van drinkwater?
- Voldoet Waternet aan de verplichtingen ten aanzien van de zorgplicht zoals beschreven in de Wbni? Zo nee, welke tekortkomingen doen zich voor? En zijn er op dit moment ongewenste grote risico's?
- Voldoet Waternet aan de verplichtingen ten aanzien van de meldplicht, zoals beschreven in de Wbni? Zo nee, welke tekortkomingen doen zich voor? En zijn er op dit moment ongewenste grote risico's?

2.2 Afhankelijkheid van PA

PA zorgt ervoor dat processen volcontinu (7x24x365) functioneren en kostenefficiënt, betrouwbaar en veilig uitgevoerd kunnen worden. Een correct functionerende PA is noodzakelijk om veilig drinkwater te kunnen leveren.

Het is noodzakelijk om beheersmaatregelen te treffen die ervoor zorgen dat de PA bij verstoringen blijft functioneren. Wanneer de PA toch uitvalt, dan moeten de gevolgen van de restrisico's worden beperkt.

Het Leveringsplan 2020-2024[2] van Waternet bevat een beschrijving van te nemen maatregelen om de leveringszekerheid en kwaliteit van drinkwater zoveel mogelijk te borgen. Deze maatregelen moeten worden gebaseerd op een Verstoringsrisicoanalyse (VRA). In de VRA van 2019 onderkent Waternet afzonderlijk de gevaren en de bedreigingen die haar processen en/of PA zouden kunnen verstoren. Voor de onderkende gevaren van cybersecurity is Waternet van mening dat deze geen effect hebben op de waterkwaliteit en waterkwantiteit. De kans daarop wordt onwaarschijnlijk tot zeer onwaarschijnlijk ingeschat. Veel gevaren en bedreigingen (inclusief cyberrisico's) scoren laag[3]. De kans is laag en/of het effect is beperkt. Dit heeft te maken met weerstand verhogende maatregelen

[2] In een Leveringsplan moet door de drinkwaterorganisatie worden aangegeven op welke wijze aan de uitvoering van de op grond van de voor hem geldende verplichtingen ten aanzien van de leveringszekerheid, de dekking van de toekomstige behoefte aan drinkwater en de levering van nooddrinkwater en noodwater, wordt voldaan (art. 37 DWW). ILT-vergunningverlening beoordeelt het Leveringsplan op de wettelijke eisen. ILT-toezicht ziet toe op de uitvoering van het Leveringsplan. Het college van B&W van de gemeente Amsterdam is in geval van Waternet verantwoordelijk voor het horizontaal toezicht op de Do, Check en Act als het gaat om uitvoering van het Leveringsplan.

[3] Op het inschatten van cyberrisico's wordt in paragraaf 2.3 nog nader ingegaan.

(proactieve en preventieve maatregelen) die Waternet in het drinkwaterproces heeft getroffen.

Getroffen weerstands-verhogende of impact verkleinende maatregelen ten aanzien van de PA zijn onder andere:
- er is redundantie[4] aanwezig van de meeste installaties op de productielocaties;
- aanwezigheid van noodstroomvoorzieningen;
- redundantie van netwerkverbindingen;
- overname van productie door een andere locatie in geval van uitval;
- indien de PA van een installatie uitvalt zal deze installatie blijven produceren met de laatst bekende instellingen[5]; en
- het op de hand bedienbaar blijven van alle essentiële installaties.

Uitval van netwerkcommunicatie of uitval van de PA leiden tot het moeten overgaan op handbediening op locatie. Op 15 december 2020 heeft Waternet een test uitgevoerd - in aanwezigheid van een ILT inspecteur -, met als doel vast te stellen wat er met de PA gebeurt bij uitval van de communicatie/verbinding op één productielocatie/installatie. Daarbij is ook getest of het vervolgens mogelijk is om lokaal de bediening van een installatie over te nemen. Dit bleek inderdaad mogelijk. Het betrof een beperkte test waarbij uitval gedurende korte tijd en in delen werd beproefd.

De ILT heeft ten aanzien van het testen van de essentiële installaties de volgende bevindingen:
- er is geen integraal testplan voor het testen van de gehele (PA) infrastructuur;
- er is (nog) geen testkalender op basis waarvan de gehele (PA) infrastructuur planmatig wordt getest;
- tijdens de uitgevoerde test op 15 december 2020 is één scenario getest: volledige uitval van communicatie. Er zijn ongetwijfeld ook andere scenario's denkbaar om in het testprogramma op te nemen. Deze scenario's heeft de ILT niet aangetroffen;
- tijdens de test op 15 december 2020 is niet langdurig (enige uren) getest. Waternet toont daarbij niet aan of het mogelijk is de handbediening, voor langere tijd, vol te blijven houden.

Conclusie
Waternet heeft maatregelen genomen om de kans en impact van uitval van de PA te beperken. Een belangrijke impact-beperkende maatregel is dat de organisatie bij uitval van de PA kan overschakelen op handbediening. Deze maatregel wordt jaarlijks getest. De door de ILT geobserveerde test was echter maar beperkt. Er is daarmee op dit moment onvoldoende zekerheid dat deze maatregel daadwerkelijk en gedurende een langere periode door Waternet uitgevoerd kan worden.

2.3 Zorgplicht

Ten tijde van het ILT-onderzoek is er nog geen nadere uitwerking van de zorgplicht beschikbaar. Om toch te kunnen bepalen of Waternet aan de vereisten van de zorgplicht voldoet, is onderzocht wat de status van de implementatie van de normen is, die Waternet voor zichzelf hanteert:

[4] Technische systemen kunnen zowel op component- als systeemniveau redundant worden uitgevoerd. Dit houdt in dat bepaalde onderdelen dubbel, of nog vaker, aanwezig zijn, zodat het geheel goed blijft functioneren wanneer een onderdeel uitvalt.
[5] Bijvoorbeeld dosering, klepstand, toerental pomp, etc.

1) Status implementatie Baseline Informatiebeveiliging Overheid (hierna BIO)[6]
2) Status implementatie PA-norm

Daarnaast heeft de ILT ervoor gekozen een aantal onderwerpen uit de BIO en PA-norm nader te onderzoeken. Dit zijn onderwerpen die ook terugkomen in de ministeriële regeling die ten tijde van dit onderzoek in voorbereiding was.

2.3.1. Status implementatie BIO

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO is de vervanger van eerdere baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. De BIO is een baseline van maatregelen met een beoogd beschermingsniveau tot en met Basis Bescherming Niveau 2 (BBN2)[7]. Dit niveau gaat er van uit dat een actor over beperkte middelen, kennis en tijd beschikt om een aanval uit te voeren. Voor bescherming tegen geavanceerde actoren (zoals cybercriminelen en statelijke actoren) zullen, op basis van een adequate risicoanalyse, aanvullende maatregelen getroffen moeten worden.

In het Cyber Security Beeld Nederland 2020 stelt de NCTV, dat de dreiging in Nederland vooral afkomstig is van statelijke actoren en criminelen. Voor Waternet geldt dus ook, dat naast de BIO, aanvullende maatregelen noodzakelijk zijn. Bovendien geldt dat de BIO niet gericht is op beveiliging van PA, maar op de beveiliging van kantoorautomatisering (KA)[8]. Daarom heeft de sector drinkwater zelf aanvullend een PA-norm opgesteld.

Voor dit onderzoek is het van belang om te weten in welke mate Waternet aan de BIO voldoet, omdat de toegang tot de PA-drinkwater loopt via de KA. Eventuele kwetsbaarheden in de KA kunnen daarmee impact hebben op de PA-drinkwater.

In 2020 zijn er 2 onderzoeken geweest naar de toestand van de BIO-implementatie. Uit het eerste onderzoek komt naar voren dat Waternet maar ten dele aan de BIO voldoet (45%). Er zijn onder andere tekortkomingen geconstateerd op het vlak van patch- en kwetsbaarhedenmanagement, configuratiemanagement, eigenaarschap van data, systemen en applicaties, classificatie van systemen en data en een standaard maatregel set.

Het tweede onderzoek heeft een BIO volwassenheidsscore opgeleverd van gemiddeld 1,54 (op een schaal van 1-5). Daarbij staat een waarde 1 voor initieel/reactief en een waarde 2 voor herhaalbaar/ad-hoc. Dit lage volwassenheidsniveau verklaart (deels) de moeite die de organisatie heeft met implementatie en verbeteringen van maatregelen.

Volgens het tweede onderzoek scoort de volwassenheid van de PA-omgeving hoger dan het overall Waternet gemiddelde. De score wordt echter niet nader gekwantificeerd.

[6] Een gedeelte van de cybersecurity beheersmaatregelen binnen Waternet is generiek en behelzen zowel de generieke ICT/kantoorautomatisering (KA) alsook de procesautomatisering (PA). Denk bijvoorbeeld aan de taken en verantwoordelijkheden van de CISO, security beleid of risicomanagement. Dat rechtvaardigt een bredere blik op de organisatie en dus ook op relevante onderwerpen uit de BIO.
[7] Bron: www.bio-overheid.nl
[8] De BIO is bedoelt voor Informatie Technologie (IT), waar de kantoorautomatisering (KA) onder valt, en is gericht op het beschermen van de vertrouwelijkheid van informatie. Binnen de Operationele Technologie (OT), waar de procesautomatisering (PA) onder valt, ligt de nadruk op de beschermen van letsel aan mens en omgeving.

In meerdere interviews die de ILT heeft gehouden, blijkt dat er erg op individuele kwaliteit van medewerkers wordt vertrouwd. De vastlegging van ICT, PA en security werkprocessen is beperkt.

Conclusie
De lage volwassenheids-score duidt op een zeer reactieve organisatie. Kwaliteit en herhaalbaarheid van werkzaamheden/processen is in het algemeen beperkt geborgd. De organisatie vertrouwt sterk op de individuele kwaliteiten van medewerkers. Waternet vindt zelf dat zij, als organisatie behorende tot de vitale infrastructuur, minimaal gemiddeld een 3 (gedefinieerd/proactief) zou moeten behalen.

Waternet heeft zelf inzicht in de maatregelen die ze nog moet nemen om BIO-compliant te worden. Het management is zich ervan bewust dat er nog veel werk moet worden verricht. Een planning voor het bereiken van BIO-compliance is echter niet aangetroffen. Het is evenmin vast te stellen in hoeverre bepaalde verbeteringen al gerealiseerd zijn.

NB: De plicht om te voldoen aan de BIG (de voorganger van de BIO) en vervolgens de BIO, dateert (al) uit 2013.

Het voldoen aan de BIO betekent nog niet dat de informatiebeveiliging op orde is, omdat de BIO slechts een baseline betreft. Aanvullende beheersmaatregelen, zoals bijvoorbeeld de PA-norm, zullen op basis van een risicoanalyse moeten worden vastgesteld.

2.3.2. Status implementatie PA-norm

De PA-norm is een door de drinkwatersector zelf opgesteld. Het doel is om de beveiliging van de PA te verhogen. De maatregelen zijn gericht op het voorkomen van ongewenste toegang tot de PA of het snel detecteren van ongewenste toegang.

Het Leveringsplan 2020-2024 bevat resultaten van een uitgevoerde audit naar de opzet en het bestaan van de 42 maatregelen in de PA-norm. Uit de audit van 2020 blijkt dat Waternet aan 34 van de 42 maatregelen voldoet. 8 maatregelen voldoen deels. Het betreffen maatregelen op het terrein van:

1) Back-ups (ten tijde van het ILT-onderzoek bleek dit inmiddels opgelost)
2) Event-logging & monitoring
3) Verantwoordelijkheden en procedures, rapportages en opvolging van informatie beveiligingsgebeurtenissen.
4) Continuïteit en zonering

Naar aanleiding van deze audit heeft Waternet een verbeterplan opgesteld. Per verbetervoorstel is een planning, een verantwoordelijke en een uitvoerder aangewezen. De actuele status van dit verbeterplan en de individuele toestand/implementatiestatus van verbeteringen was ten tijde van het onderzoek niet beschikbaar. Wel heeft Waternet aangegeven dat nog niet alle verbeterpunten zijn geïmplementeerd. Als reden hiervoor wordt aangegeven dat dit, onder meer, te maken heeft met de hectiek die ontstond na een aantal media-publicaties.

De ILT vraagt zich af of door het afwijkende karakter[9] van Waternet ten opzichte van de andere drinkwaterbedrijven het gehanteerde risicoprofiel representatief is.

[9] Waternet heeft als enige uit de sector naast drinkwater ook taken op het vlak van waterbeheer, waterzuivering en objectbediening. Waternet is daarmee mogelijk een aantrekkelijker doelwit dan andere

De audit heeft zich, in overeenstemming met de afspraken van de sector voor de invoering van de PA-norm, alleen gericht op de opzet en het bestaan. Het is daarmee nu niet duidelijk of de werking en de effectiviteit van de maatregelen afdoende is[10].

Conclusie
Een heel groot deel van de maatregelen uit de PA-norm heeft Waternet geïmplementeerd. Hierdoor is bijvoorbeeld de kans op ongeautoriseerde toegang tot de PA verkleind.

Echter, een deel van de nog niet opgeloste, geconstateerde tekortkomingen zijn relatief zwaar. Want zij kunnen leiden tot het niet, of te laat, detecteren van ongewenste acties of aanvallen op de systemen binnen de PA. Daarnaast leiden de beperkingen ten aanzien van incidentmanagement er mogelijk toe, dat kwetsbaarheden niet of onvoldoende worden verholpen.

NB: Waternet heeft bovenstaande onderkend. Er is een kwartiermaker aangesteld, die een Security Operations Center (SOC) aan het opzetten is. Een SOC kan de benoemde tekortkomingen aanpakken.

2.3.3. Onderwerpen nader onderzocht

De ILT heeft een aantal onderwerpen uit de BIO en PA-norm nader onderzocht. Dit zijn onderwerpen die ook terugkomen in de ministeriële regeling die ten tijde van dit onderzoek in voorbereiding was. Het betreft de volgende onderwerpen:

- Risicoanalyse;
- Verbeter- en evaluatie proces;
- Lifecycle management;
- Zonering / kennis van systemen / CMDB;
- Patchmanagement;
- Derden-Overeenkomsten;
- Logische toegangsbeveiliging;
- Logging/monitoring & response.

Risicoanalyse
Het ontbreekt binnen Waternet momenteel aan een ingericht risicomanagement-proces (conform een erkende standaard of industry recommended practice). Daar waar cyberrisico's ingeschat zijn wordt onvoldoende rekening gehouden met de dreiging door geavanceerdere actoren (staten, criminelen); zie ook paragraaf 2.3.1. Er vindt onvoldoende toetsing plaats of de maatregelen uit de PA-norm ook voor Waternet afdoende zijn[11].

In augustus 2020 heeft Waternet een risicomanager a.i. aangesteld. Hij heeft tot taak het risicomanagement organisatie breed in te richten.

drinkwaterbedrijven. Bovendien beschikt Waternet over minder productielocaties dan andere drinkwaterbedrijven. De impact van de verstoring van 1 van die productielocaties, kan daardoor een grotere impact hebben, dan een verstoring bij een drinkwaterbedrijf met meerdere productielocaties. Daarnaast speelt schaalgrootte en de locatie mogelijk een rol. Waternet bedient met haar drinkwatervoorziening een metropool en is daardoor mogelijk aantrekkelijker voor een aanval dan een ander drinkwaterbedrijf.
[10] Om de werking te kunnen beoordelen zullen de maatregelen ook enige tijd actief moeten zijn gewet.
[11] Vanwege het reeds eerder benoemde, complexere profiel van Waternet ten opzichte van de rest van de drinkwatersector.

Conclusie
De volledigheid van te onderkennen risico's, alsmede het effect/werking van genomen maatregelen wordt niet geborgd. Er is daarmee geen aantoonbaar inzicht in de cybersecurityrisico's voor relevante assets.

Verbeter- en evaluatie proces
Waternet beschikt niet over een (intern controle) proces waarmee de opzet, bestaan en werking/effectiviteit van beheersmaatregelen periodiek worden getoetst. Dit openbaart zich op meerdere gebieden:

- penetratietesten worden ad-hoc uitgevoerd. Aan de uitvoering liggen geen planning of andere systematiek ten grondslag. Eventuele ontdekte securityproblemen worden (vooral) ad-hoc opgelost. Deze worden niet gebruikt om van te leren of structurele verbeteringen door te voeren;
- technische bevindingen uit penetratietesten worden onvoldoende vertaald naar bedrijfsrisico's. Dit heeft tot gevolg dat prioriteitstelling niet adequaat verloopt;
- bij de uitgevoerde audits is tot op heden in hoofdzaak gekeken naar opzet en bestaan van maatregelen. De beoordeling of de maatregelen doen wat ze moeten doen, en daarmee het beoogde effect realiseren (de werking), vindt niet tot nauwelijks plaats;
- het ontbreekt aan samenhangende verbeterprogramma's met een planmatige aanpak. Er is ten tijde van het onderzoek geen overzicht/dashboard van verbetertrajecten, of de status ervan aangetroffen. De sturing op verbeteringen is onduidelijk en gefragmenteerd;
- er vindt geen structurele rapportage van de verbetercyclus plaats. Daardoor worden problemen niet zichtbaar gemaakt voor het management.

Over de werking van specifieke security-maatregelen of processen wordt niet gerapporteerd. Zo heeft de ILT voor bijvoorbeeld patchmanagement[12] geen periodiek overzicht, van al dan niet doorgevoerde patches aangetroffen (zie tevens verderop).

Het risicomanagement is niet voldoende ontwikkeld. Er is ook geen informatie over de werking/effectiviteit van maatregelen beschikbaar. Hierdoor is er ook onvoldoende overzicht van eventuele risico's en noodzakelijke verbeteringen op centraal niveau.

Conclusies
Voor het doorvoeren van verbeteringen wordt vaak gewerkt volgens de PDCA-cyclus[13]. Bij Waternet zijn de Check en Act stappen minder goed ontwikkeld. Daarom zal procesverbetering worden afgeremd: na implementatie wordt dan onvoldoende getoetst of de implementatie effectief is en/of de gehanteerde norm (bijv. kritieke prestatie-indicatoren[14] (kpi's)) realistisch is. Doordat bovendien een integraal beeld op cybersecurity ontbreekt, lijkt ook de koppeling tussen Plan en Do te ontbreken.

Waternet is tot nu toe beperkt in staat gebleken om verbeteringen systematisch en planmatig te realiseren. Een generiek proces voor het oppakken en monitoren (dashboards) van verbeteringen is niet aangetroffen.

[12] Patchmanagement is het proces dat zorgt voor het verwerven, testen en installeren van patches (wijzigingen ter opheffing van bekende beveiligingsproblemen in de code) op (verschillende softwarecomponenten van) een computersysteem.
[13] Uit de Plan-Do-Check-Act cyclus volgens William Edwards Deming (1950).
[14] Met kritieke prestatie-indicatoren kunnen prestaties worden gemeten.

Mogelijke input voor verbeterprocessen, bijvoorbeeld de resultaten van penetratietesten, worden niet als zodanig gebruikt. Daardoor wordt de effectiviteit van maatregelen mogelijk niet voldoende bijgestuurd.

Lifecycle management
Lifecycle management is nog onvoldoende ingevoerd vooral in het KA-domein; Waternet heeft daar een (te) groot aantal applicaties in bedrijf. Deze applicaties zijn ook vaak verouderd. Bij de proceseigenaren is een beperkt besef van de levensduur van applicatieondersteuning. Voor de eventueel verouderde en niet meer ondersteunde applicaties betekent dat ook dat kwetsbaarheden mogelijk niet meer kunnen worden gemitigeerd[15] en dat er onevenredig veel capaciteit en geld aan onderhoud moet worden besteed.

Conclusie
Door het nog in bedrijf hebben van niet meer door leverancier ondersteunde applicaties en/of systemen kunnen kwetsbaarheden niet meer worden verholpen. Eventuele kwetsbare systemen/applicaties, bijvoorbeeld binnen de KA kunnen dan mogelijk ook dienen als 'springplank' voor een aanval op andere systemen[16].

Zonering / kennis van systemen / CMDB
Waternet hanteert een zonering en scheiding van netwerken en systemen. Zo zijn de KA en PA van elkaar gescheiden. In het geval van een relevante aanvalsdreiging, kan de PA drinkwater worden losgekoppeld van de andere netwerken. Deze PA kan dan in 'eilandbedrijf' functioneren.

Binnen de PA is aanvullende scheiding/zonering aangebracht. Daarbij zijn de verschillende functionaliteiten waaronder drinkwater, objectbediening en afvalwater ook van elkaar gescheiden.

Een deel van de netwerkscheiding binnen de PA-beheer is virtueel/logisch uitgevoerd. Dit geeft beperkingen in de mogelijkheden om gecontroleerd netwerk uitval-scenario's te kunnen testen[17].

Het ontbreekt aan een volledig en compleet assetoverzicht. Bijvoorbeeld vastgelegd in een Configuratie Management DataBase (CMDB) en classificatie. De ILT heeft (netwerk)tekeningen aangetroffen. Deze zijn echter op detailniveau niet altijd meer up-to-date.

Conclusie
Op dit moment is er afdoende scheiding tussen de PA (drinkwater) en de overige PA en KA. Daardoor hoeft het compromitteren (in gevaar brengen) van een specifieke zone niet direct een dreiging voor een andere zone in te houden. Anders gezegd: eventuele security problemen binnen de KA zijn geen directe dreiging voor de PA drinkwater.

NB. Met de toenemende digitalisering is het de vraag of deze strikte scheiding gehandhaafd kan blijven en of de organisatie zich voldoende bewust is van de eventuele risico's die hieraan vastzitten.

[15] Voorkomen of reduceren van de negatieve gevolgen van kwetsbaarheden.
[16] De ILT heeft geen onderzoek gedaan of er binnen de PA kwetsbare systemen aanwezig waren.
[17] Bij een virtuele scheiding lopen er meerdere (logische) netwerken over dezelfde fysieke verbinding en apparatuur. Bij het testen van een netwerkuitval-scenario in een fysieke omgeving kan een fysieke verbinding worden losgekoppeld om te zien wat er gebeurt. Bij het loskoppelen van een fysieke verbinding in een virtuele scheiding valt er meer uit dan het netwerk dat men wil testen; namelijk alle virtuele netwerken die van deze verbinding gebruikmaken. In dat geval is er mogelijk niet alleen sprake van uitval van de PA-drinkwater, maar wellicht ook van PA-waterzuivering of PA-peilbeheer.

Patchmanagement
Waternet heeft voor de PA drinkwater patchmanagement ingericht. Waternet scant daarnaast ook periodiek de eigen omgeving op mogelijke kwetsbaarheden en/of gemiste patches. Eventuele omissies worden op operationeel niveau (de werkvloer) verholpen. Er wordt echter geen managementrapportage gegenereerd die inzicht geeft in de algehele patch-/kwetsbaarhedenstatus; en die mogelijk input kan vormen voor een verbeterproces.

Conclusie
In de praktijk lijkt patchmanagement op orde. Eventuele omissies met betrekking tot missende patches worden ad-hoc opgelost. Er wordt hierover niet gerapporteerd. Daardoor kunnen eventuele tekortkomingen van het patchmanagementproces niet gedetecteerd en bijgestuurd worden.

Derden-Overeenkomsten
Daar waar werkzaamheden door derden worden uitgevoerd, vindt dit altijd onder begeleiding van, en met toestemming van Waternet-medewerkers plaats.

Waternet neemt bij het verlenen van opdrachten de cybersecurity(-eisen) onvoldoende mee (nieuwbouw, vervanging, onderhoud). Daardoor voldoen systemen/projecten bij oplevering niet altijd aan de security-eisen.

Conclusie
Er is onvoldoende borging in het meenemen van security-eisen bij werkzaamheden door derden. Daardoor doet het risico zich voor dat er systemen in gebruik zijn die niet aan alle security-eisen voldoen.

Logische toegangsbeveiliging
Waternet hanteert 1-factor authenticatie (gebruikersnaam en wachtwoord) voor toegang tot de PA-omgeving. Toegang tot de PA verloopt altijd vanuit de KA via de demilitarized zone[18] (DMZ). Tijdens twee recente onderzoeken/testen is gepoogd om vanuit de KA ongeautoriseerd toegang te verkrijgen tot (systemen binnen) de PA. Dit is in beide gevallen niet geslaagd. Hierbij maken we wel de kanttekening dat deze testen maar beperkt[19] waren.

Waternet hanteert processen voor het toekennen en evalueren van toegangsrechten. Dit proces verloopt echter (grotendeels) handmatig. Hierdoor is een risico op vervuiling van de rechten aanwezig. Hierdoor behouden ex-medewerkers, of mensen die een andere functie gaan bekleden, onbedoeld rechten.

Conclusie
Het 'hacken' van gebruikers binnen de KA leidt niet direct, en zeker niet eenvoudig, tot toegang tot de PA. De ILT merkt hierbij wel op dat nooit kan worden uitgesloten dat een zeer 'skilled' aanvaller, met veel tijd en middelen, wel een succesvolle 'hack' zou kunnen uitvoeren.

Logging/monitoring & response
Binnen de PA drinkwater is een gespecialiseerd Intrusion Detection System (IDS) ingericht. Dit systeem kan onder andere onbedoelde procesmanipulatie, aanvallen en andere ongeregeldheden detecteren. Er wordt binnen PA drinkwater gelogd op security-gerelateerde gebeurtenissen. Het controleren van deze logging, of opvolging van meldingen vanuit deze IDS-systemen, vindt echter niet volcontinue

[18] Dit is een netwerksegment dat zich tussen twee netwerken bevindt.
[19] Beperkt in tijdsduur en gebruikte technieken. Het valt niet uit te sluiten dat een aanvaller met veel meer tijd en de mogelijkheid om alle technieken (bijvoorbeeld social engineering) in te zetten wel kan slagen.

(24/7) plaats. Het 'virtuele Security Operations Center (SOC)', dat deze meldingen afhandelt, is tijdens werkdagen (9ux5) actief. Het betreft een virtueel SOC; geen vaste groep medewerkers. De medewerkers die in het virtuele SOC participeren hebben vooral ook andere taken/prioriteiten. Tijdige opvolging van eventuele alerts kan dus een aandachtspunt zijn.

Logging/detectie binnen de KA is ook nog te beperkt ingericht. Hierdoor kunnen ook aanvallen op de PA via de KA mogelijk niet, of te laat worden opgemerkt.

Er zijn meerdere documenten over het melden van incidenten aangetroffen. Deze documenten geven echter geen invulling aan het behandelen, analyseren, oplossen, rapporteren en evalueren van security-incidenten.

Conclusie
Eventuele aanvallen, of pogingen daartoe, worden mogelijk te laat opgemerkt. Hierdoor is het risico aanwezig, dat aanvallen niet gestopt worden en/of ongemerkt plaatsvinden. Door het ontbreken van voldoende uitgewerkte incident-response processen, is er het risico dat te ad-hoc gewerkt wordt en dat het doen van meldingen, in het kader van de meldplicht, over het hoofd wordt gezien.

NB: Waternet heeft het gemis van bovenstaande punten onderkend. Waternet is bezig dit te verbeteren door het opzetten van een SOC.

2.4 Meldplicht

Melden incident met aanzienlijke gevolgen voor continuïteit levering drinkwater
Incidenten met aanzienlijke gevolgen voor de continuïteit van de levering van drinkwater leiden tot het (getrapt) opschalen van de Waternet-crisisorganisatie (NB: dat betreft dus niet alleen cyberincidenten). De 'leider operationeel team' van de crisisorganisatie is ook verantwoordelijk voor het doen van de melding naar de toezichthouder. Geïnterviewden spreken de verwachting uit dat hiermee meldingen in categorie 'incidenten met aanzienlijke gevolgen' van de Wbni zijn afgedekt.

Geïnterviewden geven aan dat er ten aanzien van dit deel van de meldplicht, niet formeel en expliciet, processen zijn geregeld of vastgelegd. Externe onderzoeken[20] bevestigen dat incident-managementprocessen nog niet (afdoende) zijn ingericht.

Bij een deel van de geïnterviewden is de drempelwaarde waarvoor een melding moet worden gedaan niet bekend.

Melden inbreuk die aanzienlijke gevolgen kan hebben voor continuïteit levering drinkwater
Een inbreuk in de ICT/PA die aanzienlijke gevolgen kan hebben voor de continuïteit van de levering van drinkwater, zal niet leiden tot het opschalen van de crisisorganisatie. Hierdoor wordt het signaleren van het al of niet moeten uitvoeren van een melding, niet door de crisisorganisatie ingevuld. Cybersecurity gerelateerde ICT/PA incidenten zullen via de security- organisatie (ISO/CISO) worden afgehandeld. Een eventuele melding zal hierbij ad-hoc worden gedaan.

Conclusie
Het is te verwachten dat daadwerkelijke incidenten, die boven de drempelwaarde uitstijgen, via het Departementaal Coördinatiecentrum Crisisbeheersing (DCC) van

[20] Bijvoorbeeld de onderzoeken naar BIO-implementatie en PA-norm.

het ministerie van Infrastructuur en Waterstaat bij de ILT gemeld zullen worden via de procedures binnen de dan actieve crisisorganisatie.

Door het ontbreken van formele procedures is het aannemelijk dat een inbreuk op de beveiliging, die aanzienlijke gevolgen kan hebben voor de continuïteit van drinkwater, niet gemeld zal worden. Procedures voor incident-management, en het eventueel moeten melden van inbreuken bij het Nationaal Cyber Security Centrum (hierna NCSC), zijn niet opgesteld.

2.5 Conclusies cybersecurity

Hieronder staan de meest zwaarwegende bevindingen (tekortkomingen). Deze tekortkomingen maken dat de ILT van oordeel is dat Waternet, ten tijde van het ILT-onderzoek, onvoldoende 'in control' is over haar cybersecurity.

Tekortkomingen zorgplicht

Risicomanagement
Waternet heeft risicomanagement onvoldoende ingericht. Daarmee is er onvoldoende zicht op:
- daadwerkelijke (cyber)risico's,
- of er passende maatregelen zijn getroffen,
- of er voldoende maatregelen zijn getroffen en
- of eventuele restrisico's[21] bewust geaccepteerd zijn.

Waternet schat veel cyber-gerelateerde risico's laag in (lage kans of lage impact[22]). Zo houdt zij ook onvoldoende rekening met dreiging door geavanceerde actoren[23]. Daarmee is er onvoldoende zekerheid dat er afdoende maatregelen getroffen zijn.

Evaluatie/verbeterprocessen
Door het ontbreken van een structurele en periodieke toetsing op bestaan en werking/effectiviteit van maatregelen, ontbreekt het aan inzicht of maatregelen afdoende zijn. Daarnaast ontbreekt hierdoor ook belangrijke input voor risicomanagement.

Door het ontbreken van structurele (management)rapportages/dashboards over cybersecurity, ontbreekt het aan noodzakelijk inzicht. Door tekortkomingen in de PDCA-cyclus worden eventuele verbeteringen ad-hoc doorgevoerd. Daardoor vindt er onvoldoende sturing op voortgang en resultaat plaats.

Detectie & incident response
Door de nu nog beperkte opsporingsmogelijkheden, in combinatie met een mogelijk niet tijdige afhandeling van incidenten, bestaat het risico dat (pogingen tot) aanvallen te laat (of niet) worden opgemerkt.

Door beperkingen in de incident-response procedures bestaat het risico dat het oplossen van incidenten (te) laat start of langer duurt dan noodzakelijk.
Waternet is nog onvoldoende toegerust om incidenten tijdig op te sporen en/of af te handelen.

[21] Een restrisico is een risico dat overblijft na het treffen van beheersmaatregelen en bewust geaccepteerd wordt. Bijvoorbeeld omdat de impact verlaagd is tot een acceptabel niveau.
[22] Inschatting op basis van getroffen beheersmaatregelen
[23] Daders met veel kennis, tijd, motivatie en/of geld zoals statelijke actoren, criminelen etc.

Tekortkoming meldplicht

Het ontbreken van procedures voor de meldplicht, in geval van ICT-inbreuken aan het NCSC vindt de ILT ongewenst. Waternet meldt daardoor mogelijk niet of te laat waardoor het niet tijdig ondersteuning krijgt vanuit het NCSC. Als gevolg daarvan duurt het langer om incidenten op te lossen en kunnen de gevolgen van incidenten onnodig groter worden.

3 Besturing en waarborging drinkwatertaak

3.1 Inleiding

In dit hoofdstuk wordt de tweede onderzoeksvraag beantwoord:

Hoe is de besturing bij Waternet ingericht? En is een doeltreffende sturing op cybersecurity en drinkwater zichtbaar?

In bijlage C is het gehanteerde kader opgenomen.

3.2 Inrichting en functioneren van de bestuurlijke structuur

In deze paragraaf wordt ingegaan op de inrichting van de bestuurlijke structuur van Stichting Waternet en op de wijze waarop de bestuurlijke structuur in het kader van de leveringszekerheid en kwaliteit van drinkwater functioneert. De eerste subparagraaf (3.2.1.) bevat de bevindingen met betrekking tot de inrichting van de bestuurlijke structuur. De tweede subparagraaf (3.2.2.) bevat de bevindingen en conclusies met betrekking tot het functioneren van de bestuurlijke structuur. De derde paragraaf (3.3.3.) bevat de conclusies.

3.2.1. Inrichting van de bestuurlijke structuur

In onderstaande figuur is de mandatering en verantwoording tussen het Stichtingsbestuur Waternet, het Waterschap AGV en de gemeente Amsterdam schematisch weergegeven.



Figuur: Structuur stichting en mandatering-verantwoording (bron: Stichting Waternet)

Het college van B&W van de gemeente Amsterdam heeft de algemeen directeur van Waternet gemandateerd voor de uitvoering van de drinkwatertaak. De

verantwoordelijkheid en bevoegdheid voor beslissingen over de drinkwatertaak ligt bij het college van B&W van de gemeente Amsterdam.

Waternet is voor wat betreft de drinkwatertaak te zien als een uitvoeringsorganisatie van de gemeente Amsterdam. De gemeente Amsterdam is eigenaar van alle installaties voor de drinkwatervoorziening. Vanuit Waternet wordt voor de drinkwatertaak beleid voorbereid voor de gemeente Amsterdam.

De algemeen directeur is volgens de statuten, het directiereglement[24] en de samenwerkingsovereenkomst[25] tussen de gemeente en Waternet, eindverantwoordelijk voor de voorbereiding en uitvoering van de aan de directie opgedragen taken. De algemeen directeur vervult niet een rol van dagelijks bestuurder bij Waternet[26]. De algemeen directeur legt over het uitvoeren van de drinkwatertaken verantwoording af aan het college van B&W.

De gemeenteraad controleert het college van B&W op de drinkwatertaak die onder verantwoordelijkheid van het college van B&W door Waternet wordt uitgevoerd. De gemeenteraad heeft volgens de figuur op de vorige pagina het toezicht belegd bij het college van B&W, maar is bevoegd het college van B&W te controleren. Het extern toezicht op de uitvoering van de drinkwatertaak ligt bij de ILT.

De verdeling van de bevoegdheden tussen de algemeen directeur, het stichtingsbestuur, de gemeente Amsterdam en het Waterschap AGV zijn nader uitgewerkt in statuten, het directiereglement en de samenwerkingsovereenkomst.

In de bepalingen uit de statuten en uit de samenwerkingsovereenkomst inclusief toelichtingen die daarover zijn ontvangen, valt het volgende op:

- De bestuurlijke verantwoordelijkheid voor beleidsrealisatie van de drinkwatertaak en de bevoegdheid om besluiten te nemen over de drinkwatertaak, ligt bij het college van B&W. De drinkwatertaak (beleidsrealisatie) wordt alleen op het niveau van het college van B&W besproken. Dat gebeurt niet in het stichtingsbestuur. In interviews is toegelicht dat er geen vermenging van verantwoordelijkheden mag plaatsvinden. De bedrijfsvoering wordt alleen op het niveau van het stichtingsbestuur besproken. Besluitvorming over de bedrijfsvoering kan namelijk alleen in gezamenlijkheid met het waterschap worden bepaald. Hierdoor is er geen bestuurstafel waarop bedrijfsvoeringaspecten en de drinkwatertaak in hun samenhang worden besproken.

- Het toezicht op de interne organisatie[27] van Waternet is belegd bij het stichtingsbestuur. Het stichtingsbestuur heeft volgens de samenwerkingsovereenkomst een verantwoordelijkheid om toezicht te houden op afspraken uit de samenwerkingsovereenkomst en de algemene gang van zaken bij Waternet. Er is geen nadere uitwerking aanwezig over de wijze waarop het stichtingsbestuur hier invulling aan geeft. Volgens de statuten heeft het stichtingsbestuur de bevoegdheid om de stichting te besturen. Dit wekt de indruk dat het stichtingsbestuur volledig verantwoordelijk zou zijn voor het bestuur. De bevoegdheid voor beslissingen over de drinkwatertaak ligt echter

[24] Bron: Statuten 2010, Directiereglement 2020.
[25] Samenwerkingsovereenkomsten gemeente Amsterdam, Waterschap AGV en Stichting Waternet (1997, 2005 en 2010, de samenwerkingsovereenkomst uit 2005 betreft de drinkwatertaak).
[26] Door de algemeen directeur is toegelicht dat voor zover van een dagelijks bestuur van Waternet kan worden gesproken, die rol ligt bij de gezamenlijke directie bestaande uit zes directeuren.
[27] Uit interviews blijkt dat met interne organisatie de bedrijfsvoering wordt bedoeld, wat hier onder valt is niet gedocumenteerd maar wel in interviews toegelicht.

niet bij het stichtingsbestuur maar bij het college van B&W. Dit geeft onduidelijkheid over de precieze verantwoordelijkheid van het stichtingsbestuur.

- Taken die vanuit het stichtingsbestuur aan de algemeen directeur zijn opgedragen zijn niet nader uitgewerkt. Met uitzondering van het benoemen, schorsen en ontslaan van directieleden.

De bedrijfsvoering en het primaire proces (uitvoering van de drinkwatertaak) raken elkaar bij het treffen van beveiligingsmaatregelen binnen de PA. Die maatregelen moeten bijdragen aan de leveringszekerheid en de kwaliteit van het drinkwater. Ook de IT en de inrichting en werking van risicomanagement zijn van belang, om zicht te hebben op de uitvoering en waarborging van de drinkwatertaak.

3.2.2. Functioneren van de bestuurlijke structuur

Verantwoording aan het stichtingsbestuur
De algemeen directeur legt verantwoording af over de bedrijfsvoering aan het stichtingsbestuur. Dit doet hij onder andere door 3 keer per jaar een bestuursrapportage toe te sturen. Het stichtingsbestuur komt 4 keer per jaar tijdens vergaderingen bij elkaar.

Vertragingen in de voorgang van de digitalisering,[28] worden door de algemeen directeur aan het stichtingsbestuur gemeld. De ILT ziet een reflectie op de oorzaken en de gevolgen van de vertraging en het treffen van corrigerende maatregelen niet terug.

Diverse personen geven in de interviews met de ILT aan, dat in de informatievoorziening over de voortgang van de digitalisering en de cyberveiligheid een goede duiding ontbreekt. Een toelichting op knelpunten, die ontstaan als gevolg van het niet tijdig realiseren van geplande verbeteringen, geeft de organisatie niet. Concrete informatie over de kwaliteit en ontwikkeling van de PA van de drinkwatervoorziening heeft de ILT in deze rapportages niet aangetroffen.

Informatie over de werking van risicomanagement (zowel organisatiebreed als specifiek op drinkwater) ontbreekt in de verantwoording.

Toezicht door het stichtingsbestuur
Uit notulen van de afgelopen jaren blijkt dat het stichtingsbestuur slechts een beperkt aantal kritische vragen stelt over de ontvangen rapportages. Deze vragen hebben onder meer betrekking op het niet tijdig realiseren van verbeteringen in de digitalisering. Er is geen informatie aangetroffen over de opvolging van de gestelde vragen. Toezicht op de drinkwatertaak vindt niet plaats door het stichtingsbestuur.

De waarborging van drinkwater door middel van veilige PA krijgt vanuit het stichtingsbestuur géén aandacht; de drinkwatertaak valt als bestuurlijk thema onder toezicht van het college van B&W.

Verantwoording aan de gemeenteraad via het college van B&W
De algemeen directeur legt verantwoording af over de uitvoering van de drinkwatertaak aan het college van B&W. Vervolgens legt het college van B&W hierover verantwoording af aan de gemeenteraad. Deze verantwoording bestaat uit de financiële resultaten en enkele kritieke prestatie-indicatoren[29].

[28] Bron: notulen overleg stichtingsbestuur, 5 februari 2020.
[29] Kpi's bij drinkwater waarover het college van B&W verantwoordingsinformatie geeft aan de gemeenteraad, zijn: voldoen aan wettelijke kwaliteitsnorm, aantal geplande ondermaatse leveringsminuten,

Onderwerpen zoals drinkwaterveiligheid, doelmatigheid, waarborgen van leveringszekerheid, cyberveiligheid, en de voortgang van de verbeteringen in de beleidsuitvoering, ontbreken in de verantwoording. Ook legt de algemeen directeur geen verantwoording af over de werkwijze en de resultaten van het toezicht door het stichtingsbestuur. Daardoor kan de gemeenteraad haar controlerende rol niet goed uitvoeren.

Bestuurlijke verantwoordelijkheid en toezicht college van B&W
Uit het onderzoek blijkt dat het toezicht van het college van B&W op de uitvoering van de drinkwatertaak zich beperkt tot de beleidsrealisatie en thema's zoals loodproblematiek en medicijnresten in drinkwater. Wat betreft de uitvoering van de drinkwatertaak is er vooral betrokkenheid bij financiële onderwerpen (onder andere onderdelen voor de gemeentelijke begroting en jaarrekening, investeringen voor drinkwater en tariefbepaling) en een aantal kritieke prestatie-indicatoren zoals het aantal aansluitingen en klanttevredenheid. De ILT heeft niet waargenomen dat het college van B&W om meer informatie vraagt, bijvoorbeeld over de inrichting van risicomanagement. Toezicht op de leveringszekerheid en de drinkwaterveiligheid, vindt op bestuurlijk niveau niet of nauwelijks plaats. Het college van B&W zag tot voor kort het belang van cyberveiligheid voor de drinkwatervoorziening niet als bestuurlijk thema. Maar als onderdeel van bedrijfsvoering belegd bij het stichtingsbestuur. Het college van B&W pakt hierbij haar rol als toezichthouder beperkt op.

3.2.3. Conclusies inrichting en functioneren van de bestuurlijke structuur

- Er is geen integraal toezicht. Op bestuurlijk niveau is er geen centrale aansturing van de drinkwatertaak:
  - bedrijfsvoering komt op tafel bij het stichtingsbestuur;
  - beleidsrealisatie drinkwatertaak ligt bij college van B&W en de gemeenteraad.

  Hierdoor is er op geen van de bestuurlijke niveaus (college van B&W en het stichtingsbestuur) een integraal beeld van de wijze waarop het bestuur de drinkwatertaak borgt. Een risico hiervan is dat er niet voldoende inzicht beschikbaar is en dat belangrijke risico's gemist worden. Het college van B&W onderkende tot voor kort niet dat cyberveiligheid van groot belang is voor de drinkwatervoorziening. Het college van B&W zag dit als onderdeel van bedrijfsvoering, niet als essentieel beleidsonderwerp voor de drinkwatervoorziening en dus ook niet als een bestuurlijk thema. Ook het stichtingsbestuur had geen aandacht voor de waarborging van de drinkwatertaak door middel van cyberveiligheid en veilige PA. Aan het stichtingsbestuur is geen rol toebedeeld om toezicht te houden op de drinkwatertaak. Het toezicht op de waarborging van de drinkwatertaak is niet centraal belegd. De ILT ziet dit als een ontwerpfout in de bestuurlijke structuur.

- In de statuten en de samenwerkingsovereenkomst staan tegenstrijdigheden over de verantwoordelijkheid van het stichtingsbestuur. Hierdoor is onduidelijk wat de verantwoordelijkheid van het stichtingsbestuur is.

- De verantwoording aan het college van B&W en het stichtingsbestuur is niet volledig. Toezicht op de waarborging van de drinkwatertaak kan daardoor onvoldoende inhoudelijk plaatsvinden. Onderwerpen als de voortgang van de

aantal m3 drinkwater, aantal aansluitingen, klanttevredenheid (bron: jaarrekening 2019 gemeente Amsterdam).

beleidsuitvoering, drinkwaterveiligheid, leveringszekerheid en cyberveiligheid moeten duidelijker in de verantwoording naar voren komen. Monitoring, evaluatie en bijsturing moeten een prominente plek innemen in de verantwoording.

- Zowel het college van B&W als het stichtingsbestuur geven beperkt uitvoering aan hun taken als het gaat om drinkwater:

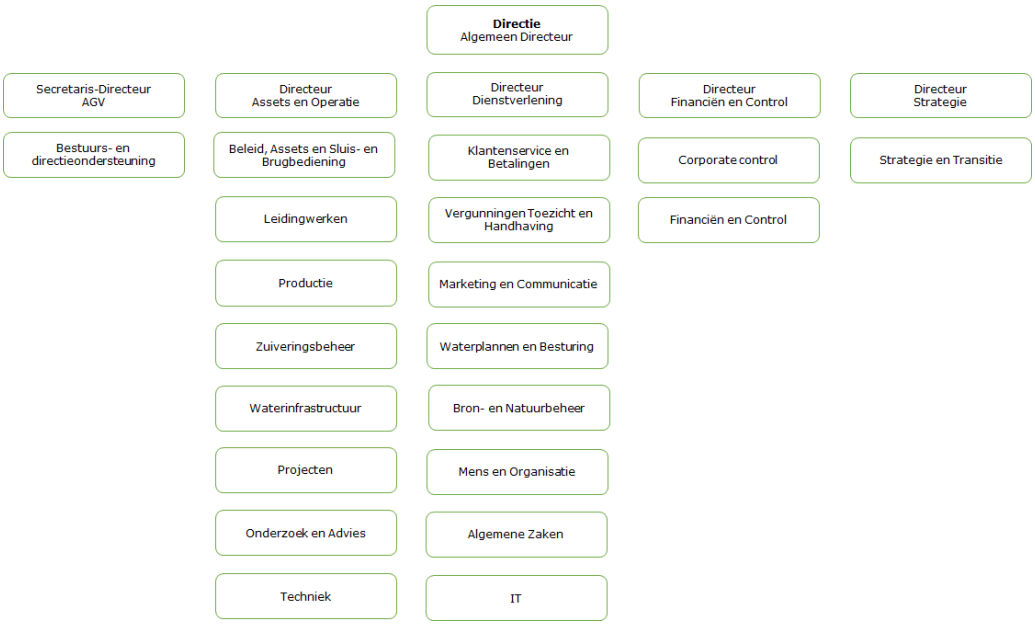
  Het college van B&W is opdrachtgever en bestuurlijk verantwoordelijk voor de drinkwatertaak. Uit het onderzoek blijkt dat het college van B&W beperkt verantwoording ontvangt en vraagt over de drinkwatertaak. Het betreft voornamelijk financiële gegevens. Er vindt niet of nauwelijks toezicht plaats op leveringszekerheid en drinkwaterveiligheid. Daardoor kan de gemeenteraad haar controlerende rol niet goed uitvoeren.

  Het stichtingsbestuur stelt zich wel kritisch op ten opzichte van de ontvangen rapportages. Ook is zichtbaar dat vragen worden gesteld over het niet op tijd realiseren van verbeteringen in de digitalisering. Maar opvolging op de kritische vraagstelling ontbreekt. De ILT is van mening, dat het stellen van een aantal kritische vragen alleen, onvoldoende invulling is van de toezichtstaak.

3.3 Aansturing en waarborgen drinkwatertaken en IT

Bij Waternet is in 2018 gekozen voor een functioneel directiemodel. Het uitgangspunt bij dit directiemodel is het tegengaan van verkokering in de organisatie[30]. De directie, bestaande uit zes directeuren (inclusief de algemeen directeur), stuurt de organisatie gezamenlijk aan.

Een overzicht van directeuren en afdelingen is in onderstaand schema opgenomen. De operationele drinkwatertaken vallen onder de Directie Assets en Operatie, waaronder ook de andere uitvoerende taken van Waternet vallen.



Figuur: Schematisch overzicht directie en afdelingen Waternet

3.3.1. Werking organisatie nader in beeld

De directie functioneert collegiaal; bij besluitvorming wordt naar eenstemmigheid gestreefd. De eindverantwoordelijkheid van de algemeen directeur houdt in dat hij hiervan kan afwijken[31]. De algemeen directeur ziet zijn rol als eindverantwoordelijke vooral als een bevoegdheid om voorstellen in de directie af te wijzen of te laten aanpassen. De ILT beschouwt dit als (relatief) beperkt regie nemen ten aanzien van de inhoud.

De afdelingshoofden worden aangestuurd door de directie als geheel. Een individuele directeur stuurt zijn of haar afdelingshoofden op hun functioneren en presteren aan.

In een deel van de interviews is aangegeven dat met dit model een grotere afstand tussen het strategische, tactische en operationele niveau is ontstaan. Hierdoor is het risico aanwezig dat op strategisch niveau niet genoeg inzicht is in datgene wat op

[30] Bron: brief van algemeen directeur aan het stichtingsbestuur van 19 juni 2018, waarin is aangegeven dat een tot dan gehanteerde vaste indeling in sectoren verkokering in de hand werkt en werken over sectorgrenzen belemmert. De sectorgrenzen worden nu losgelaten, er wordt gekozen voor een hybride organisatie met uniforme aansturing vanuit portefeuilles, de genoemde verwachting is dat dit integraliteit en uniform procesgericht werken bevordert.
[31] Bron: directiereglement, december 2020.

operationeel niveau (de werkvloer), bij de uitvoering van de drinkwatertaken, plaatsvindt.

Sinds de invoering van het directiemodel in 2018 voert de directeur Assets en Operatie wekelijks lijn- en matrix-overleggen met alle afdelingshoofden die werkzaam zijn in de assetmanagementprocessen.

De algemeen directeur heeft op 27 november 2020 in een brief aan het stichtingsbestuur aangegeven dat beleid vanuit de directie onvoldoende door het middenkader wordt geïmplementeerd en dat de hiërarchische aansturing dichter naar het operationele proces moet worden gebracht.

De directie bespreekt in de vierjaarlijkse cyclus het Leverings- en Drinkwaterplan. De ILT verwacht dat na bespreking in de planfase, ook de uitvoering, de monitoring en de bijsturing van deze plannen aan de orde komen aan de directietafel.

De directie geeft aan dat het jaarplan/prestatieplan van de afdeling drinkwaterproductie met haar wordt besproken en door haar wordt vastgesteld. De stand van zaken over de uitvoering van de drinkwatertaak wordt op hoofdlijnen aan de directie gerapporteerd. Afwijkingen van planning en prognoses komen aan de orde in bilateraal overleg.

De directierapportage[32] bevat in hoofdzaak financiële informatie, vrijwel geen informatie over behaalde prestatiedoelen, knelpunten of over de werking van risicobeheer. De toelichtingen over drinkwater zijn erg algemeen. Doordat de informatievoorziening beperkt is, bestaat het risico dat niet of niet tijdig door de directie op ontbrekende onderwerpen kan worden bijgestuurd.

De afdelingen die betrokken zijn bij de uitvoering van de drinkwatertaak,[33] werken met elkaar samen in de vorm van een 'matrixstructuur'. In interviews wordt aangegeven dat deze structuur als voorbeeld wordt gezien voor de overige onderdelen van de organisatie die een primair proces uitvoeren. In deze structuur vervult het afdelingshoofd Productie Drinkwater de rol van waardeketenregisseur, die supervisie voert over de drinkwaterketen.

Binnen Waternet is een crisisorganisatie ingericht voor de afhandeling van incidenten binnen het gehele proces van drinkwater. Het afdelingshoofd productie drinkwater is één van de vier operationeel leiders die leiding geven aan het operationeel team crisisorganisatie, waaraan ook PA-beheer en IT-beheer deelnemen.

In 2019 heeft Waternet van twee verschillende onderzoeksbureaus de aanbeveling gekregen om duidelijkheid aan te brengen in rollen en verantwoordelijkheden, zowel in de bestuurlijke structuur als in de Waternet organisatie. De directie herkent op dat moment het signaal dat de organisatie nog te veel onduidelijkheid ervaart als het gaat om verantwoordelijkheden en besluitvorming en geeft aan dat dit in de komende maanden verder vorm krijgt binnen Waternet en binnen het digitaliseringsprogramma. In 2020 is een uitwerking hiervan echter niet opgesteld bij Waternet.

De directie neemt voltallig deel in een stuurgroep data en digitalisering. Onder deze stuurgroep functioneren een aantal regiegroepen voor de domeinen: klant,

[32] Bron: directierapportage januari t/m oktober 2020, met daarin bijvoorbeeld informatie over verwachte over- of onderschrijdingen van de begroting.
[33] Hieronder zijn alle afdelingen in het assetmanagementproces betrokken.

medewerkers en assets. Deze regiegroepen hebben tot taak gebruikerswensen vanuit de organisatie te bespreken en hiervoor digitale oplossingen te realiseren. Twee directeuren zijn voorzitter van de regiegroepen.

De directie ontvangt daarnaast ook informatie van de CISO, over de voortgang op het gebied van cyberveiligheid en over kritische aandachtspunten waar verantwoordelijke actoren op moeten handelen.

Daarmee mag worden verwacht dat de directie, voor wat betreft de digitalisering, over een goede informatiepositie beschikt. In interviews geven enkele directieleden aan dat evaluatie en bijsturing op basis van deze informatie niet genoeg plaatsvindt.

Knelpunten in personele capaciteit bij de PA van de drinkwatervoorziening, komen wel bij de directie op tafel, maar worden niet aan het stichtingsbestuur gerapporteerd.[34]

Afdelingen die IT-gerelateerde werkzaamheden uitvoeren, vallen onder aansturing van meerdere directeuren[35]. Over deze verdeelde aansturing wordt eind 2020 door een extern adviseur[36] geconstateerd, dat dit leidt tot te weinig centraal inzicht in het beheer en onderhoud van de digitale processen. Er is meer centrale aansturing nodig. In interviews met directeuren wordt deze analyse onderschreven.

Waternet heeft nog geen organisatiebreed risicomanagement-systeem ingericht. Waternet heeft in augustus 2020 een extern adviseur risicomanagement aangesteld. Begin 2021 wordt gestart met het opstellen van een risicoprofiel en met een afweging van prioritering van risico's en maatregelen.

3.4 Conclusies aansturing drinkwatertaken en IT

- Een combinatie van factoren maakt de besturing en daarmee de borging van de drinkwatertaak kwetsbaar:
  - het functioneel directiemodel - waarbij de afstand tussen het strategisch en operationeel niveau (de werkvloer) als te groot wordt ervaren,
  - beperkte verantwoordingsinformatie,
  - nog geen gestructureerd risicomanagement voor de gehele organisatie,
  - een niet goed werkende PDCA-verbetercyclus
  - en een (relatief) beperkte regierol van de algemeen directeur.

- Ten aanzien van de samenwerking, in de uitvoering op de werkvloer, is het beeld positiever. Alle afdelingen in het assetmanagementproces werken met elkaar samen in de vorm van een 'matrixstructuur'. In interviews wordt aangegeven dat deze structuur, waarbij het afdelingshoofd Productie Drinkwater de rol van waardeketenregisseur vervult, als goed voorbeeld wordt gezien voor de overige onderdelen van de organisatie die een primair proces uitvoeren.

- De uitvoering van de drinkwatertaak, is in sterke mate afhankelijk van IT (incl. PA). Zowel in de sturing van de drinkwatertaak als de IT-organisatie zijn

[34] In het jaarplan/prestatieplan 2020 van de afdeling productie drinkwater worden vier belangrijke aandachtspunten genoemd, waaronder het beheer en veiligheid van procesautomatisering op orde brengen en houden. Als knelpunt in dit plan voor de productie van drinkwater wordt genoemd dat er onvoldoende kwantiteit en kwaliteit van personeel is bij de afdeling Techniek.
[35] Tot medio februari 2021 vielen IT (incl. PA) werkzaamheden onder de directeur assets en operatie (de procesautomatisering), onder de directeur dienstverlening (de kantoorautomatisering), onder de directeur strategie (het programma digitalisering) en onder de directeur financiën & control (de CISO)
[36] Memo van extern adviseur aan het Stichtingsbestuur | 24-11-2020 | Versie 2.5 | Vertrouwelijk

kwetsbaarheden geconstateerd. Belangrijke voorwaarden voor waarborging van de drinkwatertaak zijn daardoor niet voldoende aanwezig.

Recente ontwikkelingen:
Waternet heeft in december 2021 besloten dat vanaf februari 2021 de afdelingen, programma's en regiegroepen die IT-taken uitvoeren (PA, KA, programma regievoering digitalisering, en de regiegroepen digitalisering) onder een nieuw aan te stellen CIO komen te vallen.

Tot december 2020 had de CISO geen bevoegdheid om in stuurgroep data en digitalisering besluiten af te dwingen. Uit de ontvangen informatie blijkt, dat deze bevoegdheid inmiddels aan de CISO toegekend.

Begin 2021 is een interventieteam opgericht, met als doel in de eerste drie maanden van 2021 op een rij te zetten wat er moet gebeuren op basis van de verbeterpunten uit beschikbare IT-rapporten. De ILT vindt dit een positieve ontwikkeling, maar benadrukt het belang om ook op de langere termijn voldoende grip te hebben op het uitvoeren van verbeteringen. Om hier voldoende inzicht in te hebben en tijdig bij te sturen indien nodig.

3.5 Cultuur

In de eerste media-publicatie werd aan de orde gesteld dat er binnen Waternet '(…) een bedrijfscultuur heerst waarbij waarschuwingen van veiligheid officers structureel worden genegeerd en veiligheid ondergeschikt is gemaakt aan gebruiksgemak en ingesleten gewoontes (…) Bij de security-afdeling zou een angstcultuur zijn ontstaan. Kritiek wordt niet gewaardeerd en als je tegen bepaalde managers in gaat, volgen er represailles (…)[37]'. Vanwege dit signaal heeft de ILT ervoor gekozen het onderwerp cultuur mee te nemen in het onderzoek. Met name in de interviews. Er is dus geen sprake van een diepgaand cultuuronderzoek. Wel van een beeld dat redelijk consistent terug kwam in de interviews.

Dat beeld houdt in, dat personeel ervaart, dat aanspreekbaarheid en openheid meer aandacht nodig hebben. Het blijkt binnen Waternet een gewoonte om, in geval van problemen, niet direct een leidinggevende te benaderen. Als reden hiervoor wordt een cultuur van vakmanschap genoemd; men lost problemen graag zelf op. Ook wordt een cultuur genoemd van polderen (lang met elkaar spreken zonder snel een besluit te nemen) en situaties te rooskleurig inschatten. In interviews komen termen naar voren als: 'men ziet vooral de halfvolle kant van het glas', 'medewerkers minder taakvolwassen dan gedacht', 'familiecultuur' en een 'impliciete cultuur'.

Het expliciet aanspreken op situaties en consequenties lijkt men ongemakkelijk te vinden. Concreet is zichtbaar dat er twee externe publicaties nodig waren, voor de directie en het stichtingsbestuur, om meer urgentie en versnelling in de door de CISO in gang gezette verbeteringen te brengen en verbeteringen in de aansturing vanuit de directie op te starten.

Daarnaast komt in interviews naar voren dat er in de organisatie sprake is van 'eilandvorming'. Dit vanwege grote verschillen in taakgebieden en fusies in het verleden en dat samenwerking met andere afdelingen, of teams hierdoor niet altijd vanzelf gaat. Eén van de doelstellingen die Waternet met de invoering van het functioneel directiemodel voor ogen had, was meer samenwerking en het voorkomen van eilandvorming. Dat doel lijkt nog niet bereikt.

[37] Bron: Digitale beveiliging Waternet zo 'lek als een mandje', Follow the Money, 20 september 2020

Uit de interviews, op strategisch, tactisch en operationeel niveau, blijkt dat mensen het geschetste beeld van een angstcultuur niet herkennen.

3.6 Conclusie cultuur

Met betrekking tot de cultuur constateert de ILT een aantal aandachtspunten. Binnen Waternet lijkt het de gewoonte om niet expliciet te bespreken welke problemen aan de orde zijn. Daardoor is een risico aanwezig dat men te lang met problemen blijft rondlopen en problemen niet tijdig worden opgepakt. Dat aanspreekbaarheid en openheid meer aandacht nodig hebben wordt door betrokkenen op alle niveaus erkend: operationeel, tactisch en strategisch.

In het volgende hoofdstuk volgt een samenvattende conclusie.

4 Conclusie risico's kwaliteit en leveringszekerheid drinkwater

In dit hoofdstuk komen de conclusies uit het onderzoek naar de cybersecurity (zie paragraaf 2.5) en uit het onderzoek naar besturing (zie paragraaf 3.2, 3.4 en 3.6) samen, om daarmee een samenhangend beeld te geven van de risico's die de ILT constateert in de waarborging van de kwaliteit en leveringszekerheid van drinkwater door Waternet.

Risico's tekortkomingen in zorgplicht en meldplicht cybersecurity

Door de geconstateerde tekortkomingen ten aanzien van de zorg- en meldplicht zal zowel de kans als de impact van een eventueel cyberincident, met mogelijke gevolgen voor de kwaliteit en/of de continuïteit van drinkwater, groter zijn dan in een situatie waarin volledig aan de Wbni wordt voldaan.

Hoeveel groter die kans of impact is, laat zich niet kwantificeren. Door de gehanteerde 'defense in depth' aanpak leunt de beveiliging niet op één maatregel. Er geldt dat maatregelen aanvullend op elkaar werken en als geheel de weerstand tegen cyberaanvallen verhogen. Het negatief effect van ontbrekende of niet optimaal werkende maatregelen is daarmee niet aan te geven.

Waternet geeft ook aan dat bij incidenten, die leiden tot uitval van de PA drinkwater, de impact beperkt wordt door diverse redundantiemaatregelen en daarnaast ook terug te kunnen vallen op handbediening. Echter omdat de maatregel handbediening niet grootschalig is getest én omdat er geen testprogramma is voor crisismanagement, is de ILT van oordeel dat er momenteel onvoldoende zekerheid is dat die maatregel bij grootschalige uitval toegepast kan worden. Daarmee zijn de risico's voor kwaliteit en continuïteit voor levering van drinkwater momenteel met onvoldoende zekerheid beheerst.

Risico's tekortkomingen in de besturing

De ILT constateert kwetsbaarheden in de besturing, de besturing is niet genoeg doeltreffend. Dit vormt een ongewenst risico voor waarborging van de drinkwatertaak.

In het ontwerp van de bestuurlijke structuur ontbreekt integraal toezicht op de drinkwatertaak. In de uitvoering ontbreekt effectieve aansturing op waarborging van de drinkwatertaak. Er is geen integrale informatievoorziening op bestuurlijk niveau. Evaluatie en bijsturing vinden onvoldoende plaats. Op directie en bestuurlijk niveau is er nog geen integrale inschatting en afweging van risico's gemaakt. Deze kwetsbaarheden vormen een risico voor de waarborging van kwaliteit en leveringszekerheid van drinkwater. Ze zijn een grondoorzaak van de tekortkomingen die op het gebied van cybersecurity zijn geconstateerd.

In bijlage D staat een samenvattend overzicht van de geconstateerde tekortkomingen op het gebied van cybersecurity en besturing.

Naar aanleiding van dit onderzoeksrapport maakt de ILT met Waternet afspraken om tot verbetering te komen en ziet toe op de realisatie van deze verbetering.

Bijlage A Onderzoeksproces

Onderzoeksfasering

Het onderzoek is in een aantal fasen uitgevoerd:



Initiatie

- Risicosignalering;
- Verkennend gesprek;
- Aankondigen onderzoek.

Vooronderzoek

- Informeren directie Waternet over de onderzoeksopzet;
- Uitvoeren documentanalyse. Bij het onderzoek is gebruik gemaakt van beleidsdocumenten, voortgangsrapportages, verslagen van overleggen, uitgevoerde onderzoeken door derden, etc.

Veldwerk

- Houden interviews, verzorgen verslagging en validatie door geïnterviewden;
- Opvragen aanvullende documenten waar nodig en uitvoeren documentanalyse.

Analyse

- Verwerken en analyseren uitkomsten documentonderzoek en interviews.

Rapportage

- Bespreken en voorleggen concept rapportage;
- Afspraken over vervolgtoezicht

Bijlage B Onderzoekskader cybersecurity

Deze bijlage gaat nader in op het gebruikte toetsingskader ten behoeve van de op cybersecurity gerichte onderzoeksvragen.

Wbni en Bbni

Per 9 november 2018 is de Wet beveiliging netwerk- en informatiesystemen (Wbni) van kracht. De Wbni is de vertaling van de Europese Netwerk- en Informatiebeveiliging Richtlijn, de NIB-Richtlijn. Deze richtlijn heeft tot doel Europa digitaal veiliger te maken door de digitale weerbaarheid te vergroten en de gevolgen van cyberincidenten te verkleinen. Alle Europese lidstaten nemen daarom in nationale wetgeving verplichtingen op rond cybersecurity en de continuïteit van dienstverlening.

De Wbni streeft ernaar de digitale weerbaarheid van Nederland, en in het bijzonder van:
- Vitale aanbieders, bestaande uit aanbieders van een essentiële diensten (AED's) en Andere aangewezen vitale aanbieders (AVA's);
- Rijksoverheid;
- Digitale dienstverleners, te vergroten.

In de Bbni zijn de drinkwaterbedrijven aangewezen als aanbieder van een essentiële dienst (een AED). De bevoegde autoriteiten zijn belast met de handhaving (toezicht en sancties) van de Wbni en het Bbni. Door de Minister van Infrastructuur en Waterstaat, de bevoegde autoriteit voor onder andere de drinkwaterbedrijven, is de ILT als de toezichthoudende dienst aangewezen.

De Wbni stelt aan de AED een zorgplicht en een meldplicht.

Vereisten zorgplicht

De zorgplicht richt zich op het beheersen van risico's en het voorkomen van incidenten en het beperken van de gevolgen van incidenten.

Artikel 7 (risico's beheersen) van de Wbni verplicht de AED passende en evenredige technische en organisatorische maatregelen te nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. De maatregelen moeten, gezien de stand van de techniek, zorgen voor een niveau van beveiliging dat is afgestemd op de risico's die zich voordoen.

Artikel 8 (incidenten voorkomen en gevolgen van incidenten beperken) van de Wbni verplicht de AED passende maatregelen te nemen om incidenten die de beveiliging van de voor de verlening van de betrokken dienst gebruikte netwerk- en informatiesystemen aantasten, te voorkomen en de gevolgen van dergelijke incidenten zo veel mogelijk te beperken, teneinde de continuïteit van die dienst te waarborgen.

De zorgplicht zoals omschreven in de Wbni is onvoldoende concreet om duidelijke handvatten te bieden wat daar onder verstaan wordt. Op dit moment is er wel een Ministeriele Regeling (MR) in voorbereiding die meer handvatten gaat bieden wat er onder de zorgplicht verwacht wordt. Om toch al een kader te hebben voor het door de ILT uitgevoerde onderzoek is er een pragmatische aanpak gekozen.

Hierbij is gekeken naar (de toestand van) de door Waternet gehanteerde normenkaders. Dat zijn er 2:
1) De Baseline Informatiebeveiliging Overheid (BIO)[38]
2) Een door de drinkwatersector zelf opgestelde Proces Automatiseringsnorm (PA-norm)

Daarnaast heeft de ILT ervoor gekozen een aantal onderwerpen uit de BIO en PA-norm nader te onderzoeken. Dit zijn onderwerpen die ook terugkomen in de ministeriële regeling die ten tijde van dit onderzoek in voorbereiding was.

Bij het bepalen van de onderwerpen, heeft de ILT gebruikgemaakt van de elementen die onderdeel uitmaken van een Cyber Security Management System (CSMS):
A) Risico Analyse, het identificeren, classificeren en onderzoeken van risico's passend bij de organisatie;
B) Security policies/procedures die het CSMS ondersteunen, inbedding in de organisatie, bewustwording, juiste scoping van het CSMS;
C) Keuze van passende securitymaatregelen die de risico's geïdentificeerd in de risico analyse afdoende mitigeren. Deze maatregelen kunnen worden ingedeeld in de volgende groepen; personele security, netwerkzonering/segmentering, Access-control (authenticatie, autorisatie, administratie);
D) Implementatie van de security maatregelen; worden de juiste maatregelen geselecteerd, worden de maatregelen planmatig/projectmatig geïmplementeerd, wordt patch- & change- management toegepast, back-up & restore, life-cycle management toegepast, Incident-Response ingericht (inclusief monitoring & detectie);
E) Monitoren (en verbeteren/evalueren) van het CSMS (en de maatregelen. Worden er periodiek audits uitgevoerd die toetsen op aanwezigheid en juiste werking en effectiviteit van (technische) maatregelen, policies & procedures. Zijn /worden de risico's nog steeds afdoende gemitigeerd.

Deze elementen heeft de ILT vertaalt naar de volgende nader te onderzoeken onderwerpen:
- Risicoanalyse;
- Verbeter- en evaluatie proces;
- Lifecycle management;
- Zonering / kennis van systemen / CMDB;
- Patchmanagement;
- Derden-Overeenkomsten;
- Logische toegangsbeveiliging;
- Logging/monitoring & response.

Vereisten meldplicht

De meldplicht omvat twee soorten meldingen:

1. De Wbni verplicht de AED een incident met aanzienlijke gevolgen voor de continuïteit van de door hem verleende dienst bij de sectorale toezichthouder (in dit geval ILT, via DCC) te melden.

[38] Een gedeelte van de cybersecurity beheersmaatregelen binnen Waternet is generiek en behelzen zowel de generieke ICT/kantoorautomatisering (KA) alsook de procesautomatisering (PA). Denk bijvoorbeeld aan de taken en verantwoordelijkheden van de CISO, security beleid of risicomanagement. Dat rechtvaardigt een bredere blik op de organisatie en dus ook op relevante onderwerpen uit de BIO.

2. De Wbni verplicht de AED een inbreuk op de beveiliging van netwerk- en informatiesystemen, die aanzienlijke gevolgen kan hebben voor de continuïteit van de door hem verleende dienst, bij het NCSC te melden.

Voor wat verstaan wordt onder een incident met aanzienlijke gevolgen is door de minister een (vertrouwelijke) drempelwaarde vastgesteld.

Bijlage C Onderzoekskader besturing en waarborging drinkwater

Vereisten drinkwaterwet (DWW) en Drinkwaterbesluit (DWB)

De DWW en het DWB geven wettelijke vereisten voor de openbare drinkwatervoorziening. Een hiervan is het wettelijk vereiste om de leveringszekerheid en kwaliteit van drinkwater te waarborgen (art. 7, 8 en 32 DWW) en zorg te dragen voor een doelmatige drinkwatervoorziening (onder meer art. 3 en 11 en DWW). Op basis van dat vereiste draagt een eigenaar verantwoordelijkheid voor het waarborgen van de drinkwatertaak. Het voldoen aan de zorgplicht en meldplicht voor het borgen van de cybersecurity (zie bijlage B) wordt beschouwd als voorwaarde voor het waarborgen van de drinkwatertaak.

Aanvullend op dit wettelijk vereiste staat in art. 7 DWW dat de eigenaar van een drinkwaterbedrijf concreet tot taak heeft (betreft geen uitputtend overzicht):
- het tot stand brengen en in stand houden van een duurzame en doelmatige openbare drinkwatervoorziening;
- het tot stand brengen en in stand houden van de infrastructuur die noodzakelijk is voor de productie en distributie van drinkwater;
- het borgen van de kwaliteit en duurzaamheid van het productie- en distributieproces en het geleverde drinkwater.

Toelichting begrip 'eigenaar' bij Waternet
Stichting Waternet is een gekwalificeerd rechtspersoon, aan welke het in 2005 door de toenmalige minister is toegestaan dat de uitvoering van de drinkwatertaak door de gemeente Amsterdam aan Waternet wordt gemandateerd[39]. Het college van B&W is verantwoordelijk voor de realisatie van de drinkwatertaak en bevoegd om beslissingen met betrekking tot drinkwater te nemen, het stichtingsbestuur heeft deze bevoegdheid niet. De gemeente Amsterdam is te beschouwen als eigenaar van de drinkwatertaak, de gemeenteraad heeft een controlerende rol.

Kaders voor intern toezicht

In de parlementaire geschiedenis bij de DWW is vermeld wat er van een RvC als intern toezichthoudend orgaan bij een drinkwaterbedrijf wordt verwacht: het houden van toezicht op het bestuur en het geven van adviezen, het benoemen van bestuurders, het goedkeuren van belangrijke voorstellen en besluiten van het bestuur, en waar nodig ingrijpen in het besturingsproces.

In de DWW wordt in algemene zin uitgegaan dat drinkwaterbedrijven een vennootschappelijke rechtspersoon zijn. Waarin publiekrechtelijke bestuursorganen aandeelhouder zijn en via die weg invloed uitoefenen op een drinkwaterbedrijf, zoals het benoemen van leden van een RvC. Waternet is een verbonden partij van de gemeente Amsterdam en heeft geen RvC. Desondanks verwacht de ILT dat voor een goede waarborging van de drinkwatertaak, de intern toezichthoudende taken op een

[39] In de parlementaire geschiedenis is beschreven dat in de regio Amsterdam in 2005 het eerste waterketenbedrijf in Nederland, Waternet, is opgericht. De verantwoordelijk Minister ondersteunde destijds de wens om te komen tot waterketenbedrijven, waarin drinkwatervoorziening, riolering en afvalwaterzuivering in één bedrijf worden geïntegreerd, zoals verwoord in de Rijksvisie waterketen. Voor wat betreft de rechtsvorm van Waternet bleek er bij de betrokken overheden een grote voorkeur voor een stichting was; dit mede vanwege het feit dat riolering en afvalwaterzuivering reeds enige jaren in deze vorm samenwerkten. Dit heeft ertoe geleid om ook het gemeentelijke drinkwaterbedrijf in deze rechtsvorm onder te brengen.

vergelijkbare wijze zichtbaar zijn in de bestuurlijke structuur bij Waternet en dat hierbij algemeen aanvaardbare principes voor goed bestuur worden toegepast.

Kaders voor besturing

Naast wettelijke kaders maakt de ILT gebruik van principes in de Nederlandse Corporate Governance Code[40] en de Code voor publieke dienstverleners[41]. Omdat drinkwaterbedrijven een vitale functie hebben verwacht de ILT dat deze organisaties vanuit het waarborgen van hun publieke taak streven naar een goede besturing en basisprincipes uit deze code ter harte nemen.

Kaders voor besturing zijn onder meer vindbaar in:

- Drinkwaterwet: onder andere art. 8 en 32, waarborgen kwaliteit en leveringszekerheid drinkwater, dit is een wettelijke verantwoordelijkheid voor drinkwaterbedrijven en uitvoerders van drinkwatertaken. De ILT verwacht dat de drinkwatervoorziening op operationeel, tactisch, strategisch en bestuurlijk niveau voldoende wordt gewaarborgd.
- Nederlandse Corporate governance code: onder andere principe 1.2 en 1.4 (risicobeheersing), 2.4 (besluitvorming), 2.4.7 (waarborgen informatievoorziening) en 2.5.1 (cultuur).
- Code goed bestuur publieke dienstverleners: onder andere principe 3.7 (zorg dragen voor goede informatievoorziening), principe 4 (zorg dragen voor toetsen van prestaties en functioneren van bestuur) en principe 5 (risicomanagement en interne beheersing).

Duiding bij het wettelijke begrip waarborging drinkwatertaak

Om nadere duiding te geven aan het wettelijke vereiste om de leveringszekerheid en kwaliteit van drinkwater te waarborgen, maakt de ILT mede gebruik van algemene kaders voor goed bestuur. Het uitgangspunt is dat een doeltreffende besturing nodig is om de drinkwatertaak te kunnen waarborgen.

Voor een doeltreffende besturing is nodig: het evalueren van bestuur en intern toezicht, een onafhankelijk werkende tegenkracht (intern toezicht), ruimte voor een kritische reflectie, duidelijkheid over verantwoordelijkheden, een goed werkend risicomanagement en een goede informatievoorziening op basis waarvan effectieve evaluatie en bijsturing plaatsvindt.

[40] Deze code is wettelijk verplicht voor beursgenoteerde bedrijven met als doel de belangen te beschermen van aandeelhouders en andere belanghebbenden. Bron: https://www.rijksoverheid.nl/onderwerpen/corporate-governance/corporate-governance-code
[41] Bron: Code Goed Bestuur Publieke Dienstverleners 2015_Definitief (publiekverantwoorden.nl)

Bijlage D Overzicht geconstateerde tekortkomingen

Tekortkomingen zorgplicht en meldplicht cybersecurity

1) Tekortkomingen in testen van noodscenario's bij uitval PA drinkwater
   a) Beperkte omvang
   b) Beperkte scenario's
   c) Beperkte tijdsduur
   d) Geen periodieke testkalender
2) Implementatie BIO (incl opzet, bestaan en werking getoetst)
3) Implementatie PA-norm t.b.v. drinkwater (opzet, bestaan en werking)
4) Gebreken eventlogging & monitoring
5) Gebreken incident response
6) Onvoldoende inrichting & uitvoering risicomanagement inclusief te beperkte risicoanalyse m.b.t. te verwachten dreigingen/actoren t.a.v. cyber
7) Gebreken t.a.v. verbeter- en evaluatieprocessen
   a) ontbrekende rapportages/dashboards
   b) geen samenhang in verbeterprogramma's, geen goede PDCA cyclus
   c) geen audits op werking van maatregelen
   d) (penetratie)testen ad-hoc uitgevoerd. Verbeteringen worden ad-hoc doorgevoerd
8) Gebreken patchmanagement
9) Gebreken werkzaamheden derden
10) Verbeterpunten logische toegangsbeveiliging
11) Gebreken meldplicht; meldingen naar NCSC
12) Verbeterpunten asset & lifecyclemanagement

Tekortkomingen en kwetsbaarheden in de besturing

Bestuurlijke structuur:
1) Op bestuurlijk niveau geen integraal beeld van de wijze waarop de drinkwatertaak wordt geborgd.
2) Toezicht op de waarborging van de drinkwatertaak is niet centraal belegd.
3) Bestuurlijke verantwoording en de interne informatievoorziening aan de directie is niet volledig.
4) Toezicht op het feit of de leveringszekerheid en drinkwaterveiligheid mogelijk in gevaar komt, vindt op bestuurlijk en strategisch niveau niet of nauwelijks plaats.
5) Het stichtingsbestuur stelt zich wel kritisch op ten opzichte van de ontvangen rapportages, maar opvolging op de kritische vraagstelling ontbreekt.

Aansturing:
6) In de organisatie wordt de afstand tussen het strategisch en operationeel niveau als te groot ervaren.
7) Beperkte regie en aansturing op strategisch en bestuurlijk niveau.
8) Onvoldoende integrale inrichting en uitvoering van risicomanagement.
9) Een niet goed werkende PDCA-cyclus en informatievoorziening.

Cultuur:
10) Aanspreekbaarheid en openheid verdienen meer aandacht.

Dit is een uitgave van de

Inspectie Leefomgeving en Transport

Postbus 16191 | 2500 BD Den Haag
088 489 00 00

www.ilent.nl

@inspectieLenT

Maart 2021