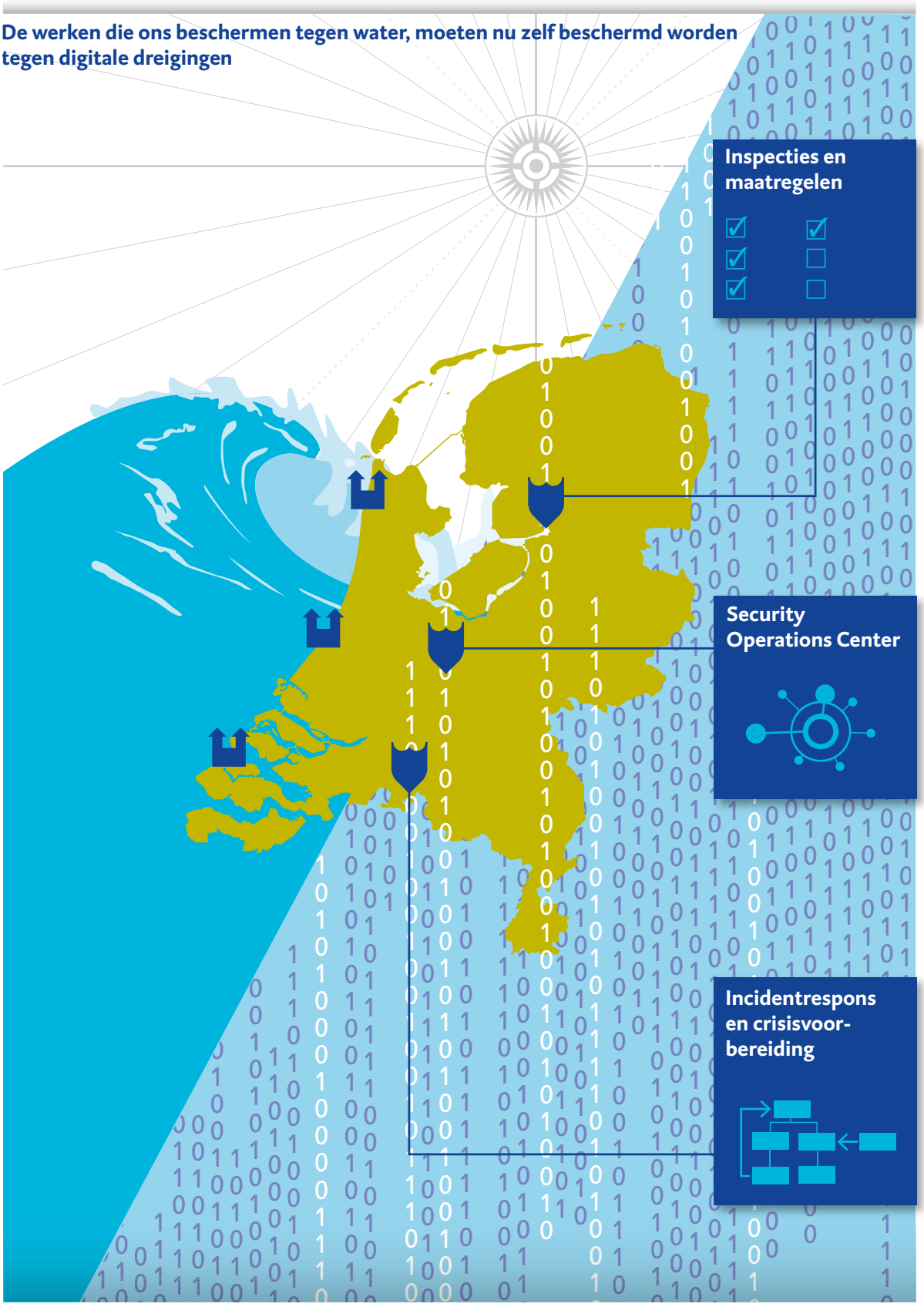
Algemene Rekenkamer

Digitale dijkverzwaring: cybersecurity en vitale waterwerken

2019

Digitale dijkverzwaring: cybersecurity en vitale waterwerken

De tekst in dit document is vastgesteld op 11 maart 2019. Dit document is op 28 maart 2019 aangeboden aan de Tweede Kamer.



Figuur 1 *Oude en nieuwe dreigingen*

Vooraf

De bewoners van de Noordzeedelta worstelen sinds mensenheugenis met het water dat hen omringt. Zij schiepen met terpen, dijken, molens en polders het land dat wij nu Nederland noemen. In de afgelopen eeuwen werden civiele werken van wereldfaam gerealiseerd om het water voor eens en voor altijd de baas te blijven. Miljoenen mensen zijn voor hun veiligheid afhankelijk van de betrouwbaarheid van die waterwerken. Ook de economische en ecologische belangen ervan zijn groot. Het keren en beheren van water is daarom door de overheid als vitale sector aangemerkt: uitval kan leiden tot maatschappelijke ontwrichting en raakt andere vitale sectoren, zoals de distributie van elektriciteit.

De digitale revolutie die zich onder onze ogen voltrekt, brengt ongekende nieuwe mogelijkheden. Tegelijkertijd maakt technologie ons afhankelijk en zijn er cyberdreigingen ontstaan die tot voor kort nog niet bestonden. Spionage, sabotage, terrorisme en criminaliteit hebben zich verplaatst naar de digitale wereld en bedreigen ook de automatisering van waterkeringen. De werken die ons beschermen tegen het water moeten nu zélf beschermd worden tegen digitale dreigingen (figuur 1).

Cybersecurity is iets anders dan informatiebeveiliging. Bij falen van cybersecurity is de schade, anders dan bij falende informatiebeveiliging, potentieel maatschappelijk ontwrichtend. Het gaat om meer dan gelekte persoonsgegevens of verstoorde organisatieprocessen. Bij het keren en beheren van water staat de fysieke veiligheid van Nederland op het spel: in de strijd met het water kan het gaan om leven of dood.

In dit onderzoek hebben we gekeken naar de wijze waarop vitale waterwerken beschermd zijn tegen cyberaanvallen.

Inhoud

1 Samenvatting

1.1 Context: cybersecurity en vitale waterwerken

Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT[1] te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan (NCTV, 2018a). Alles wat hierboven genoemde schade kan veroorzaken, vatten we onder de noemer cyberdreigingen. Sommige sectoren, die bijvoorbeeld zorgen voor de distributie van elektriciteit of drinkwater, zijn zo essentieel voor de Nederlandse samenleving dat ze door de overheid als 'vitaal' zijn aangemerkt.

Dit onderzoek richt zich op de vitale sector Keren en Beheren (van water). De minister van Infrastructuur en Waterstaat (IenW) draagt voor deze vitale sector politieke verantwoordelijkheid. Ook heeft de minister de wettelijke plicht ernstige IT-incidenten in de sector te melden bij het Nationaal Cyber Security Centrum (NCSC). De minister heeft een aantal waterkeringen onder beheer van Rijkswaterstaat aangewezen als vitale onderdelen binnen de sector. Deze waterkeringen noemen we in dit rapport 'vitale waterwerken'. We hebben onderzocht hoe Rijkswaterstaat de vitale waterwerken voorbereidt op cyberdreigingen.

1.2 Voorbereiding op cyberdreigingen

Vitale waterwerken maken voor het aansturen van processen gebruik van automatiseringssystemen die veelal stammen uit de jaren '80 en '90 van de 20e eeuw. Toen was het woord cybersecurity nog geen gemeengoed. Deze systemen functioneerden oorspronkelijk *stand alone* (losstaand) maar zijn in de loop der jaren gekoppeld aan grotere computernetwerken, bijvoorbeeld om bediening op afstand mogelijk te maken. Daardoor is de kwetsbaarheid ervan voor cyberdreigingen toegenomen. Hoe groot de dreiging van een cyberaanval voor de sector Keren en Beheren precies is, is nog niet inzichtelijk.

Risico's wegnemen door de systemen te moderniseren is volgens Rijkswaterstaat technisch uitdagend en kostbaar. De organisatie richt zich daarom met name op de signalering van een cyberaanval (detectie) en een adequate reactie om die aanval onschadelijk te maken (respons). We zien dat Rijkswaterstaat een hoop werk heeft verzet. Echter, zowel op het gebied van detectie als op die van respons moet Rijkswaterstaat, in opdracht van de minister, nog stappen zetten om de aan de eigen doelstellingen voor cybersecurity te voldoen.
We baseren deze hoofdconclusie op drie deelconclusies:

1. Met de uitvoering van het programma Beveiligd Werken Rijkswaterstaat is veel werk verzet, maar nog niet alle gestelde doelen zijn behaald.
2. Met de inrichting van een Security Operations Center (SOC) is de strategie van detectie en respons ingericht, maar deze is qua uitvoering nog niet voltooid.
3. Rijkswaterstaat bereidt zich voor om cyberaanvallen en –crises het hoofd te kunnen bieden, maar belangrijke documentatie blijkt verouderd. Ook test Rijkswaterstaat de maatregelen tegen cyberaanvallen in de praktijk nauwelijks met zogenaamde pentesten.

1.2.1 Vervolg programma Beveiligd Werken Rijkswaterstaat vergt aandacht

Met het programma Beveiligd Werken Rijkswaterstaat (BWR) is een inhaalslag gemaakt op het gebied van cybersecurity. Rijkswaterstaat heeft alle tunnels, bruggen, sluizen, et cetera bezocht en maatregelen vastgesteld om meer weerstand te kunnen bieden tegen een cyberaanval.[2] Wij hebben gekeken naar de BWR-maatregelen voor de vitale waterwerken. We zien dat na afloop van het programma een groot deel van de maatregelen is uitgevoerd (circa 60%) of dat bewust gekozen is het gesignaleerde risico te aanvaarden (20%). De overige maatregelen waren nog in uitvoering (11%) of zijn tot nader order uitgesteld (9%). De resterende maatregelen zijn overgedragen aan de Rijkswaterstaat-regio's. Afgesproken werd dat Rijkswaterstaat centraal overzicht zou houden over de uitvoering van de restpunten. We constateren dat dit centrale overzicht ontbreekt. Ook zien we dat Rijkswaterstaat de ambities om het onderdeel cybersecurity onderdeel te laten zijn van reguliere inspecties nog niet realiseert.

Ondersteunende constateringen uit praktijkonderzoek

Bij de door ons nader onderzochte vitale waterwerken bleek het grootste deel van de BWR-maatregelen te zijn afgerond. Bij één waterwerk bleek een belangrijke openstaande maatregel nog niet uitgevoerd. Bij een ander vitaal waterwerk bleek dat de overdrachtsdocumentatie, waarmee uitvoering van de resterende maatregelen formeel bij de regio waren belegd, niet bekend was.

We zien een aantal oorzaken voor het niet tot uitvoer brengen van alle BWR-maatregelen en het achterblijven van bestendiging van de ingezette lijn:

- Het uitvoeren van maatregelen en deelname aan inspecties die cybersecurity toetsen wordt niet bij de regio's afgedwongen.
- Oude onderhoudscontracten staan het afdwingen van cybersecurityeisen in de weg. Rijkswaterstaat is bezig dit knelpunt op te lossen.
- De financiering voor de resterende maatregelen en borging van cybersecurity in inspecties is niet geregeld, wat voor vertraging in besluitvorming en uitvoering zorgt.

1.2.2 Strategie van detectie en respons nog niet voltooid

Een van de resultaten van het programma BWR was de oprichting van een Security Operations Center (SOC). De belangrijkste taak van het SOC is de detectie van en de reactie (respons) op cyberaanvallen. De ambitie om eind 2017 bij alle vitale waterwerken cyberaanvallen direct te kunnen detecteren was in het najaar van 2018 nog niet gerealiseerd. Hierdoor bestaat het risico dat Rijkswaterstaat een cyberaanval bij een vitaal waterwerk niet of te laat detecteert.

Ondersteunende constateringen uit praktijkonderzoek

Uit een test bij een van de door ons onderzochte vitale waterwerken bleek dat het mogelijk was fysiek toegang te verkrijgen tot het object. Digitale toegang (het aansluiten van een laptop) werd opgemerkt door het SOC van Rijkswaterstaat. Bij dit waterwerk zijn maatregelen getroffen om cyberaanvallen direct te detecteren. Bij een ander vitaal waterwerk dat wij onderzocht hebben, zijn deze maatregelen voor detectie nog niet getroffen.

Sommige regio's zijn terughoudend bij het nemen van maatregelen die directe detectie van cyberaanvallen mogelijk maken bij de objecten die zij in beheer hebben. Dit is een belangrijke oorzaak voor het niet realiseren van dit doel. Het SOC kan het uitvoeren van deze maatregelen niet aan de regio's opleggen.

Het SOC geeft aan over onvoldoende kennis en capaciteit te beschikken om de detectie verder te verfijnen en uit te breiden. Regelmatig wordt met de verantwoordelijk minister gesproken over uitbreiding van het SOC. Tussen vraag en aanbod zien we een kloof. Zolang het dreigingsniveau van de sector nog niet inzichtelijk is, is het moeilijk te beoordelen wat een passende mate van investeren in kennis en capaciteit is.

Daarnaast constateren we dat medewerkers van het SOC worden gescreend op het niveau van een Verklaring Omtrent het Gedrag (VOG), terwijl ze in aanraking komen met gevoelige systeeminformatie van vitale waterwerken. Of dit conflicteert met het dreigingsniveau is, bij gebrek aan inzicht hierin, niet vast te stellen.

1.2.3 Crisisdocumentatie verouderd en geen volwaardige pentesten

Rijkswaterstaat bereidt zich voor op crises, waaronder cybercrises, met een crisismodel. Dit model kent verschillende specifieke crisisscenario's. Voor een door een cyberaanval veroorzaakte crisis blijkt echter geen specifiek scenario te bestaan. Ook is er geen inzicht in de effecten van een cybercrises op andere sectoren (cascade-effecten). We zien verder dat belangrijke documenten bij de bestrijding van een cyberaanval op onderdelen niet actueel

worden gehouden. Actuele informatie kan in een crisissituatie van essentieel belang zijn voor een snelle en adequate reactie.

Organisaties laten zich in een zogenaamde *pentest* bewust hacken door een ingehuurde partij om informatie te verkrijgen over kwetsbaarheden in hun beveiligingssysteem. Rijkswaterstaat voert voor de vitale waterwerken echter nauwelijks pentesten uit omdat dit naar eigen zeggen te risicovol is. Daarmee ontbreekt het de organisatie aan informatie over hoe weerbaar de vitale waterwerken in de praktijk zijn tegen cyberaanvallen.

1.3 Aanbevelingen

Om een goede inschatting te kunnen maken van wat er nodig is om de sector voldoende weerbaar te maken tegen cyberaanvallen bevelen wij de minister van IenW aan:

1. Voer een onderzoek uit naar het actuele feitelijke cybersecurity-dreigingsniveau voor de vitale waterwerken ten behoeve van nadere besluitvorming over allocatie van mensen en middelen.

Ten aanzien van de borging van het afgeronde programma Beveiligd Werken Rijkswaterstaat, bevelen we de minister van IenW het volgende aan:

2. Draag Rijkswaterstaat op centraal en uniform zicht te creëren op de opvolging van de BWR-restpunten die zijn overgedragen aan de regio's en zorg te dragen voor de uitvoering van de resterende maatregelen.
3. Versterk daarnaast waar nodig de instrumenten die in het leven zijn geroepen om de met het programma BWR ingezette lijn voort te zetten (waaronder FIT) met voldoende mensen en middelen.

Om de detectie op cyberaanvallen bij vitale waterwerken te voltooien bevelen we aan:

4. Voltooi de maatregelen die directe detectie van cyberaanvallen mogelijk maken en bouw de monitoring via het SOC uit (op basis van het objectief vastgestelde dreigingsniveau, zie aanbeveling 1).
5. Heroverweeg het niveau van screening voor SOC-medewerkers en de rubricering van gevoelige overzichtsdocumentatie van het SOC (op basis van het objectief vastgestelde dreigingsniveau, zie aanbeveling 1).

Tot slot formuleren wij enkele aanbevelingen om de voorbereiding op cybercrises te optimaliseren:

6. Instrueer Rijkswaterstaat een proces te ontwerpen en te implementeren om de informatie op de crisiskaarten en netwerkoverzichten actueel te houden.
7. Instrueer Rijkswaterstaat een specifiek crisisscenario voor cybersecuritycrises in het crisismodel op te nemen en maak daarbij cascade-effecten inzichtelijk.
8. Maak expliciet welke risico's het doen van volwaardige pentesten op de industriële automatiseringssystemen van de vitale waterwerken in de weg staan en stippel op basis hiervan een route uit om tot een situatie te komen waarin pentesten een integraal onderdeel vormen van de cybersecuritymaatregelen bij vitale waterwerken.

1.4 Reactie minister van Infrastructuur en Waterstaat

In haar reactie schrijft de minister van IenW het als haar verantwoordelijkheid te zien om de digitale veiligheid van de vitale waterwerken goed te organiseren. De minister geeft aan dat ze hierbij onder meer al heeft ingezet op een IenW-brede cybersecuritystrategie en bestuurlijke afspraken over digitale veiligheid in de watersector. De minister ziet onze conclusie als een ondersteuning van de reeds door haar in gang gezette werkzaamheden om de cybersecurity van de watersector verder te verbeteren. Ze onderschrijft onze conclusies en aanbevelingen en geeft aan alle aanbevelingen op te volgen. Zo zal de minister (laten) inzetten op een praktische doorvertaling van de algemene dreigingsbeelden en de aanvullende informatie verkregen vanuit de samenwerking met de diensten naar mogelijke consequenties voor de individuele vitale objecten. De dreigingsbeelden zullen volgens de minister leidend zijn voor de invulling van veel van onze aanbevelingen. In haar reactie geeft de minister eveneens aan dat Rijkswaterstaat ondertussen een flinke inhaalslag heeft gemaakt ten aanzien van de opvolging van de BWR-restpunten.

1.5 Nawoord Algemene Rekenkamer

We constateren dat de minister onze aanbevelingen overneemt. Veel van onze aanbevelingen stelt de minister afhankelijk van opvolging van de eerste aanbeveling: het duiden van het dreigingsniveau. Wij willen de minister er evenwel op wijzen dat een aantal van onze aanbevelingen gaat om het spoedig afronden van maatregelen die al eerder getroffen hadden moeten zijn. We doelen dan bijvoorbeeld op het aansluiten van de vitale waterwerken op het SOC, zodat meer diepgaand en actueel zicht op is op deze waterwerken. Dit had eind 2017 al gerealiseerd moeten zijn en is dus niet afhankelijk van de eerste aanbeveling.

2 Over dit onderzoek

2.1 Wat is er aan de hand?

Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan (NCTV, 2018a). Alles wat deze schade kan veroorzaken (hackers, computervirussen, vandalisme, et cetera) vatten we samen onder de noemer cyberdreigingen. In dit onderzoek ligt de focus op cyberaanvallen: bewuste pogingen om schade te veroorzaken.[3]

De processen binnen vitale sectoren zijn sterk gedigitaliseerd en dus kwetsbaar voor cyberdreigingen. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) meldt in zijn recentste jaarverslag (AIVD, 2018) in toenemende mate activiteiten te signaleren die erop zijn gericht digitale sabotage van vitale infrastructuur in Europa mogelijk te maken. De dreiging van in Nederland actieve beroepscriminelen en buitenlandse mogendheden (statelijke actoren) neemt volgens het Nationaal Cyber Security Center (NCSC) toe; de aanvallen zijn steeds geavanceerder en complexer (NCTV, 2018a). Het NCSC ziet sabotage en verstoring door statelijke actoren als de grootste dreiging voor de nationale veiligheid (NCTV, 2018b).

2.2 Wie is politiek verantwoordelijk?

In 2015 heeft de minister van Veiligheid en Justitie in een brief aan de Tweede Kamer 26 vitale processen benoemd, gekoppeld aan 11 sectoren (VenJ, 2015). Samen vormen deze de vitale infrastructuur van Nederland. Op grond van de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) werden verscheidene ministers verantwoordelijk voor de sectoren en vitale processen.

De Wgmc is eind 2018 vervangen door de Wet beveiliging netwerk- en informatie-systemen (Wbni). Deze wet is de Nederlandse invulling van een Europese richtlijn voor netwerk- en informatiebeveiliging.[4] In die wet wordt een sector ‘Keren en Beheren’ benoemd, met als verantwoordelijke (‘vitale aanbieder’) de minister van Infrastructuur en Waterstaat (IenW).

De minister heeft op grond van de Wbni onverkort de plicht ernstige IT-incidenten bij de door haar aangewezen vitale waterkeringen in de sector, te melden bij het Nationaal Cyber Security Centrum (NCSC).

Bij ministerieel besluit is een aantal waterkeringen binnen de sector aangewezen als vitaal.[5] Deze aangewezen waterkeringen noemen we in dit rapport 'vitale waterwerken'. Ze worden beheerd door Rijkswaterstaat, als uitvoeringsorganisatie van de minister van IenW belast met het beheer van het hoofdwatersysteem (de grote wateren als de zee en de rivieren). De minister van IenW dient zich te verantwoorden over de maatregelen die Rijkswaterstaat treft op het gebied van cybersecurity.

2.3 Wat kenmerkt de sector Keren en Beheren?

In de sector Keren en Beheren wordt naast van kantoorautomatisering gebruik gemaakt van 'industriële automatisering': automatisering voor de bediening van sluizen, gemalen en waterkeringen. Deze industriële automatiseringssystemen in de vitale infrastructuur van Nederland kunnen worden getroffen door spionagesoftware, virussen of *ransomware* (gijzelsoftware). Zo verschenen in 2012 alarmerende berichten in de media naar aanleiding van een kwetsbaarheid in de gemalen van de gemeente Veere.[6] Hackers zouden deze kwetsbaarheid zonder specialistische kennis eenvoudig kunnen misbruiken vanaf het internet en bijvoorbeeld pompen kunnen uitzetten, met overstromingen tot gevolg.

Door automatisering heeft Rijkswaterstaat de afgelopen decennia vitale waterwerken betrouwbaarder en efficiënter gemaakt. De besturing van sluizen, gemalen en keringen werd geautomatiseerd. Daarbij zijn de systemen die voorheen *stand alone* waren, via netwerken benaderbaar gemaakt om bijvoorbeeld bediening en inspectie op afstand mogelijk te maken. Deze ontwikkelingen zijn ingezet in een tijd dat cybersecurity een vrijwel onbekend begrip was. Een van de kenmerken van industriële automatiserings-systemen is dat hun levensduur vele malen langer is dan bijvoorbeeld die van kantoor-automatisering (Agence nationale de la sécurité des systèmes d'information, 2012). Deze combinatie – verouderde technologie die verweven is geraakt met moderne technologie – maakt systemen kwetsbaar voor hedendaagse cyberdreigingen (NCSC, 2016).[7] Gezien de specifieke kenmerken van industriële automatiseringssystemen is het voorkomen van dergelijke aanvallen, kostbaar en technisch uitdagend. Rijkswaterstaat richt zich in zijn strategie vooral op signaleren van en reageren op cyberaanvallen (detectie en respons).

2.4 Wat hebben we onderzocht?

We hebben onderzoek gedaan naar de manier waarop de minister van IenW zich voor-bereidt op cyberaanvallen op de vitale waterwerken die voor haar worden beheerd door Rijkswaterstaat. De volgende vragen stonden daarbij centraal:

1. Welke instrumenten heeft Rijkswaterstaat als beheerder in handen om cyberdreigingen en -aanvallen te detecteren en zich te beschermen tegen cyberdreigingen voor de waterkeringen?
2. In hoeverre werken de instrumenten om cyberdreigingen en -aanvallen te detecteren? En bieden ze voldoende bescherming?
3. Welke scenario's liggen klaar voor wanneer zich een cyberaanval voordoet; met welke maatregelen kan Rijkswaterstaat voorkomen dat andere vitale sectoren ook geraakt worden bij een aanval (cascade-effecten)?
4. Hoe werkt de respons bij detectie van kwetsbaarheden en incidenten bij Rijkswaterstaat?

2.5 Hoe hebben we het onderzoek uitgevoerd?

Voor het beantwoorden van de onderzoeksvragen bestudeerden we in de periode mei tot en met oktober 2018 interne documenten bij het Ministerie van IenW en Rijkswaterstaat, en voerden we gesprekken met betrokkenen. Hierbij keken we naar opzet en bestaan van maatregelen. Daarnaast onderzochten we, voor de tweede onderzoeksvraag, samen met Rijkswaterstaat de werking van maatregelen op locatie bij vitale waterwerken. Bij één van de objecten hebben ethische hackers een test uitgevoerd om de cybersecuritymaatregelen in de praktijk te toetsen. Voor meer informatie kan de methodologische verantwoording in bijlage 1 geraadpleegd worden.

Leeswijzer

In hoofdstuk 3 gaan we in op de inhaalslag die Rijkswaterstaat met een programma voor cybersecurity heeft gemaakt. Dit is van belang omdat dit programma de basis legde voor de detectie van cyberaanvallen en het de stand van zaken op cybersecuritygebied bij Rijkswaterstaat in beeld bracht. Hiermee geven we tevens gedeeltelijk antwoord op de eerste twee onderzoeksvragen.

In hoofdstuk 4 gaan we nader in op de wijze waarop Rijkswaterstaat cyberdreigingen detecteert (eerste twee onderzoeksvragen) en hoe Rijkswaterstaat reageert op gesignaleerde kwetsbaarheden (vierde onderzoeksvraag). In hoofdstuk 5 bekijken we vervolgens de wijze waarop Rijkswaterstaat zich voorbereidt op cyberaanvallen (derde onderzoeksvraag) en reageert op cybersecurity-incidenten (vierde onderzoeksvraag). Hoofdstuk 6 bevat de conclusies en aanbevelingen aan de minister van IenW. In hoofdstuk 7 is de reactie van de minister opgenomen alsmede het nawoord van de Algemene Rekenkamer.

Tussen de hoofdstukken door beschrijven we door ons onderzochte casussen. Deze illustreren onze bevindingen en conclusies. Ze geven bovendien meer inzicht in de werking van cybersecuritymaatregelen in de praktijk (onderzoeksvraag 2).

Vertrouwelijke informatie

Rapporten van de Algemene Rekenkamer zijn in beginsel openbare stukken. De Comptabiliteitswet 2016 legt aan de Algemene Rekenkamer bij de openbaarmaking van onderzoek nauwelijks beperkingen op. Het beleid van de Algemene Rekenkamer is daarbij echter openbaarmaking van onderzoeksbevindingen achterwege te laten als deze onevenredig grote schade aan bepaalde belangen (zouden kunnen) brengen. In het geval van dit onderzoek is er voor gekozen bepaalde informatie alleen vertrouwelijk te delen met de Eerste en Tweede Kamer.

3 Beveiligd Werken Rijkswaterstaat: een inhaalslag

In dit hoofdstuk geven we informatie over de organisatie die de vitale waterwerken in opdracht van de minister beheert en haar meerjarige programma Beveiligd Werken Rijkswaterstaat (BWR), dat was gericht op cybersecurity. Met deze informatie beantwoorden we deels onze eerste en tweede onderzoeksvraag. Daarnaast is deze informatie relevant om de context waarin Rijkswaterstaat opereert beter te begrijpen. Uit het programma BWR volgen ook de doelen die Rijkswaterstaat zichzelf op het gebied van cybersecurity gesteld heeft. Deze vormen deels onze normen om bevindingen aan te toetsen.

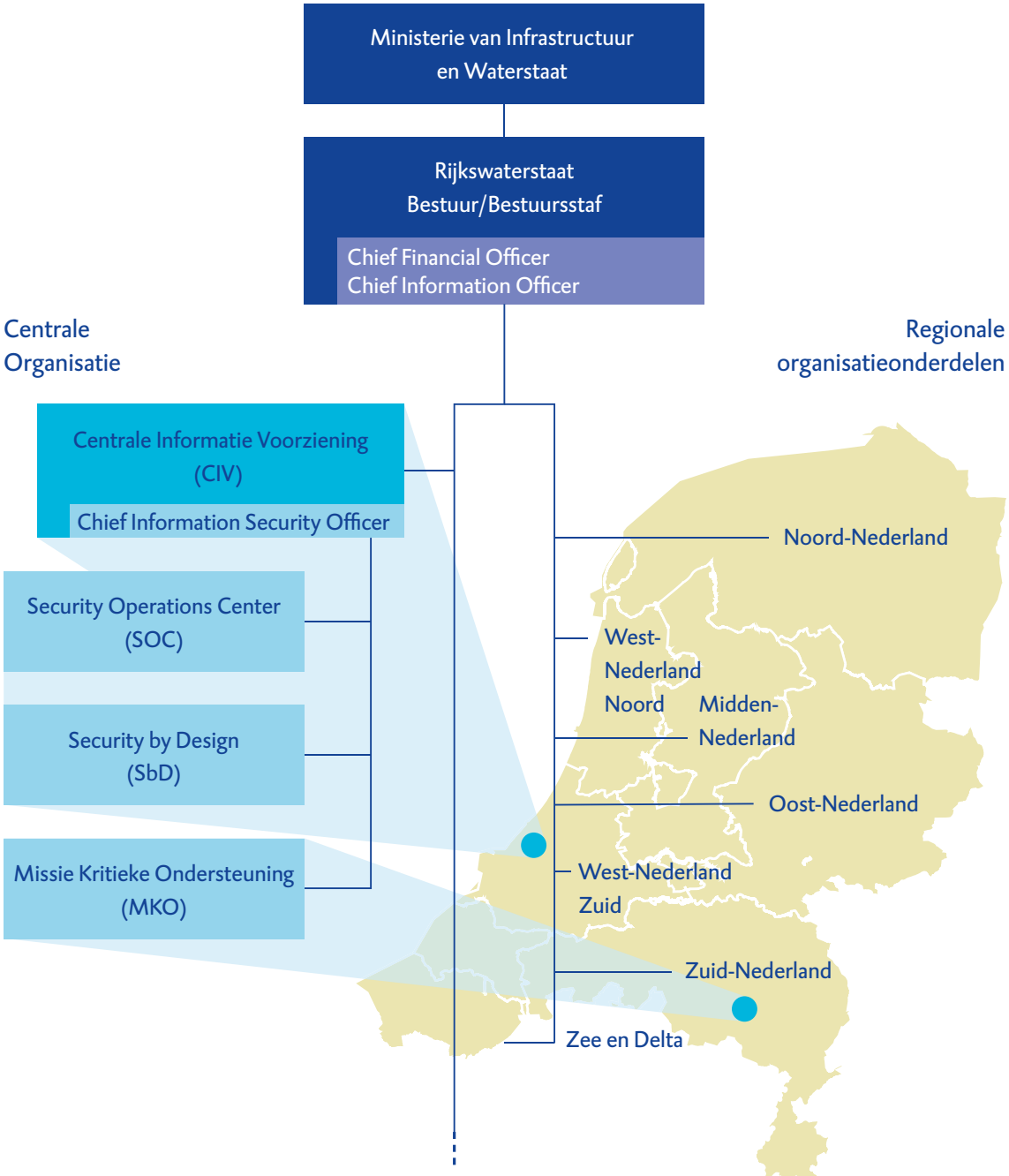
Het hoofdstuk begint met een overzicht van de Rijkswaterstaat-organisatie en de voor cybersecurity meest relevante organisatieonderdelen en rollen. Vervolgens beschrijven we de aanleiding, uitvoering en de drie belangrijkste resultaten van het programma BWR. Resultaat 1, cybersecurity verbetermaatregelen, en resultaat 2, cybersecurityeisen voor waterwerken, hebben we uitgewerkt in dit hoofdstuk. Aan resultaat 3, monitoren van en reageren op cyberdreigingen, is een apart hoofdstuk gewijd.

3.1 Cybersecurity en de organisatie Rijkswaterstaat

Rijkswaterstaat is een agentschap van het Ministerie van IenW en georganiseerd in centrale, landelijke onderdelen en regio's. Boven de centrale afdelingen en de regio's staat het bestuur. De centrale afdelingen stellen kaders en leveren ondersteunende diensten aan de regio's. De regio's verzorgen de aanleg, het beheer en het onderhoud van wegen, vaarwegen en waterwerken. Het bestuur is verantwoordelijk voor het functioneren van de organisatie als geheel. Het accent van het bestuur ligt op de strategische sturing en besluitvorming.

Figuur 2 geeft een overzicht van de organisatie Rijkswaterstaat en de voor dit onderzoek meest relevante actoren.

Centrale landelijke organisatieonderdelen en regio's werken binnen Rijkswaterstaat samen aan cybersecurity



Figuur 2 *De voor cybersecurity meest relevante actoren binnen Rijkswaterstaat*

In het bestuur van Rijkswaterstaat zijn de Chief Financial Officer (CFO) en de Chief Information Officer (CIO) verantwoordelijk voor informatiebeveiliging. Het centrale organisatieonderdeel Centrale Informatie Voorziening (CIV) beheert de IT-netwerken, werkplekken, telefonie, applicaties en data van Rijkswaterstaat. Bij de CIV werken ruim 1.000 mensen. Het organisatiedeel is voor cybersecurity een belangrijke speler:

- De CIO staat aan het hoofd van de CIV.
- De Rijkswaterstaat-breed opererende Chief Information Security Officer (CISO) maakt deel uit van de CIV; hij stelt samen met de CIO het informatiebeveiligingsbeleid op.
- Bij de CIV heeft het team Security by Design (SbD, 7 mensen) als belangrijkste taak om cybersecurityeisen in Rijkswaterstaatprocessen en -contracten met derden op te nemen. Dit komt aan bod in § 3.4.
- Het Security Operations Center (SOC, 11 mensen) opereert vanuit de CIV. Op de rol van het SOC gaan we in hoofdstuk 4 in.
- Missiekritieke Ondersteuning (MKO, 55 mensen) valt ook onder de CIV en is bij Rijkswaterstaat een centrale regisseur voor alle meldingen op het gebied van automatisering, waaronder cyberincidenten. De rol van MKO behandelen we in § 5.1.

De regio's van Rijkswaterstaat zijn verantwoordelijk voor het beheer en onderhoud van de objecten in het land en voeren het beleid van RWS uit in hun eigen regio. Daarbij moeten zij, ook op het gebied van cybersecurity, nauw samenwerken met de CIV. De CIV kan de regio's niet dwingen bepaalde besluiten te nemen op het gebied van cybersecurity. Het bestuur kan dat wel. Rijkswaterstaat heeft er bewust voor gekozen om de CIV een adviserende rol met een beperkt mandaat richting de regio's te geven. Zo wordt volgens Rijkswaterstaat voorkomen dat cybersecurityrisico's op operationeel niveau worden aangepakt en het bestuur niet bereiken. Het is juist de bedoeling dat de risico's naar boven komen zodat er op hoog niveau over dreigingen gepraat wordt. Het bestuur van Rijkswaterstaat kan cybersecuritymaatregelen wel opleggen maar kiest meestal niet voor een top-down benadering. Beheerders van objecten hebben door de kennis van en een betrokkenheid bij 'hun' object een belangrijke stem.

3.2 Het programma BWR; aanleiding, doel en resultaten

Eind 2013 besloot Rijkswaterstaat het programma BWR op te starten. Aanleiding van het programma waren onder andere:

- Problemen met de bediening van de Ketelbrug, die vanaf 2009 regelmatig in het nieuws waren[8].

- Het nieuws over de slechte digitale beveiliging bij de gemeente Veere in 2012[9].
- Een onvolkomenheid[10] die de Algemene Rekenkamer constateerde op het onderdeel informatiebeveiliging tijdens onderzoek over de jaren 2011 en 2012 (AR, 2012), zie het kader.

Eerder onderzoek Algemene Rekenkamer (AR, 2011-–016)

In 2011 constateerden we in ons Verantwoordingsonderzoek dat de informatiebeveiliging bij het toenmalige Ministerie van Infrastructuur en Milieu[11] en Rijkswaterstaat niet op orde was. De informatiesystemen van Rijkswaterstaat waren onvoldoende beschermd en daarmee kwetsbaar voor cyberaanvallen. Naar aanleiding van deze onvolkomenheid heeft Rijkswaterstaat sinds 2012 verbeteringen ingezet, mede met het programma BWR. In 2015 hebben wij geconstateerd dat er bij Rijkswaterstaat genoeg voortgang is geboekt in het oplossen van de eerder geconstateerde problemen. Daarmee is de onvolkomenheid omgezet in een aandachtspunt. In 2016 hebben we ook het aandachtspunt opgeheven. Wel vroegen we nog aandacht voor de overdracht van het programma BWR naar de lijnorganisatie.

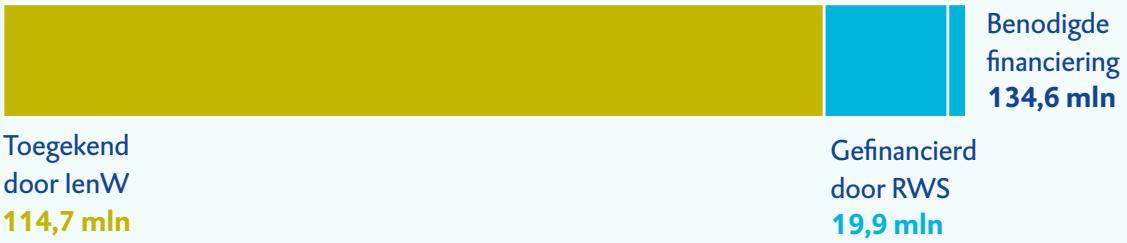
De doelstelling van het programma BWR was ervoor te zorgen dat “de infrastructuur van Rijkswaterstaat betrouwbaar blijft werken en een basaal niveau van beveiliging geïnstalleerd is”. Het programma richtte zich op de drie ‘systemen’ van Rijkswaterstaat: het hoofdwatersysteem (HWS), het hoofdvaarwegennet (HVWN) en het hoofdwegennet (HWN). De objecten (tunnels, bruggen, sluizen, verkeerscentrales, et cetera) en IT-systemen met de grootste risico’s, werden het eerst aangepakt. Naast de objecten en de IT-systemen vielen ook generieke voorzieningen, zoals het netwerk van Rijkswaterstaat (zie § 4.1), onder de reikwijdte van het programma. Ook heeft Rijkswaterstaat gekeken naar de processen voor beheer en onderhoud en naar het personeel dat met de geautomatiseerde systemen werkt.

Uitvoering van BWR grotendeels gefinancierd door de minister van IenW

Voor het gehele programma BWR heeft de minister van IenW bij de start € 114,7 miljoen beschikbaar gesteld. In het voorjaar van 2016 bleek nog € 17,3 miljoen nodig te zijn voor een aantal uitbreidingen van het programma. Het ging om aanvullende objecten en maatregelen voor de fysieke beveiliging. Deze middelen heeft Rijkswaterstaat bijgepast uit de budgetten van de regio's, door de BWR-maatregelen centraal te prioriteren.

Van het aldus totaal beschikbare budget van € 132 miljoen was eind 2017 € 128,2 miljoen besteed. Er restte nog voor € 3,37 miljoen aan verplichtingen, die werden overgedragen aan de regio's. Door extra uitgaven aan het hoofdvaarwegennet zijn de uiteindelijke uitgaven nog € 3 miljoen hoger uitgekomen. Net als de eerder genoemde € 17,3 miljoen, moet Rijkswaterstaat ook dit bedrag uit beschikbare middelen betalen. De prognose van de financiële eindstand van het programma was bij afsluiting derhalve € 134,6 miljoen. Daarvan heeft het Ministerie van IenW € 114,7 miljoen aanvullend gefinancierd en Rijkswaterstaat € 19,9 miljoen uit bestaande budgetten. Figuur 3 geeft een overzicht van de kosten voor het programma BWR.

Het programma BWR werd grotendeels gefinancierd door het ministerie van Infrastructuur en Waterstaat



Figuur 3 *Financiering van het programma BWR*

Voor de cybersecurity van de vitale waterwerken zien we drie belangrijke resultaten van het programma BWR:

1. Rijkswaterstaat heeft, in het deelproject IMPAKT (Impulsprogramma Aanpak Kritieke Technische Infrastructuur), verbetermaatregelen benoemd en uitgevoerd. Om de resultaten van IMPAKT te bestendigen, heeft Rijkswaterstaat het instrument FIT (Functionele Inspecties en Testen) geïntroduceerd (zie § 3.3).
2. Er zijn eisen ontwikkeld om cybersecurity een vast onderdeel te maken van alle processen en contracten rondom het ontwerp, de realisatie en het onderhoud van waterwerken (zie § 3.4).
3. Rijkswaterstaat heeft het Security Operations Center (SOC) opgezet om de waterwerken te beschermen tegen digitale aanvallen (zie hoofdstuk 4).

3.3 IMPAKT: verbetermaatregelen Rijkswaterstaat-waterwerken

3.3.1 IMPAKT-*aanpak: maatregelen op basis van objectbezoeken*

De IMPAKT-aanpak bestond uit een bezoek aan 460 objecten van Rijkswaterstaat door een team van interne en externe experts.[12] Daarbij was cybersecurity het belangrijkste aspect waarop werd getoetst (zie kader). Voor het Hoofdwatersysteem (HWS) ging het om 12 kleine objecten (losse gemalen of aflaatwerken) en 55 grotere complexen, waaronder stormvloedkeringen en sluiscomplexen. De bezoeken aan de waterwerken van het HWS zijn in 2014 en 2015 afgelegd.

Toetsingskader: meerdere aspecten van belang voor cybersecurity

De experts van IMPAKT hebben de locaties beoordeeld aan de hand van een toetsingskader. Naast naar cybersecurity werd ook gekeken naar *asset management* (de beheerprocessen) en fysieke beveiliging (zaken als sleutelbeheer, hekwerk en alarminstallaties). Deze zijn gerelateerd aan cybersecurity. Onder *asset management* valt bijvoorbeeld bijhouden welke softwareversies en updates geïnstalleerd zijn: updates niet uitvoeren kan een cybersecurityrisico met zich meebrengen. Tekortkomingen in de fysieke beveiliging kunnen de continuïteit van de IT ook bedreigen. Niet alleen zou zonder adequate beveiliging iemand zich gericht toegang tot apparatuur kunnen verschaffen, ook ongericht vandalisme kan tot IT-verstoringen leiden. IMPAKT heeft ook gekeken naar functionele veiligheid. Hierbij gaat het om de veiligheid op en rond een Rijkswaterstaat-object, bijvoorbeeld de aanwezigheid van valbescherming en reddingsmateriaal. Omdat dit niet relevant is voor cybersecurity hebben we dit onderwerp buiten beschouwing gelaten. De maatregelen op het vlak van cybersecurity, fysieke beveiliging en *asset management* noemen we in dit rapport de cybersecuritygerelateerde maatregelen.

Op basis van het resultaat van de toets bij het bezoek van de experts werd een pakket van maatregelen voorgesteld voor het object. Voorbeelden van maatregelen zijn[13]:

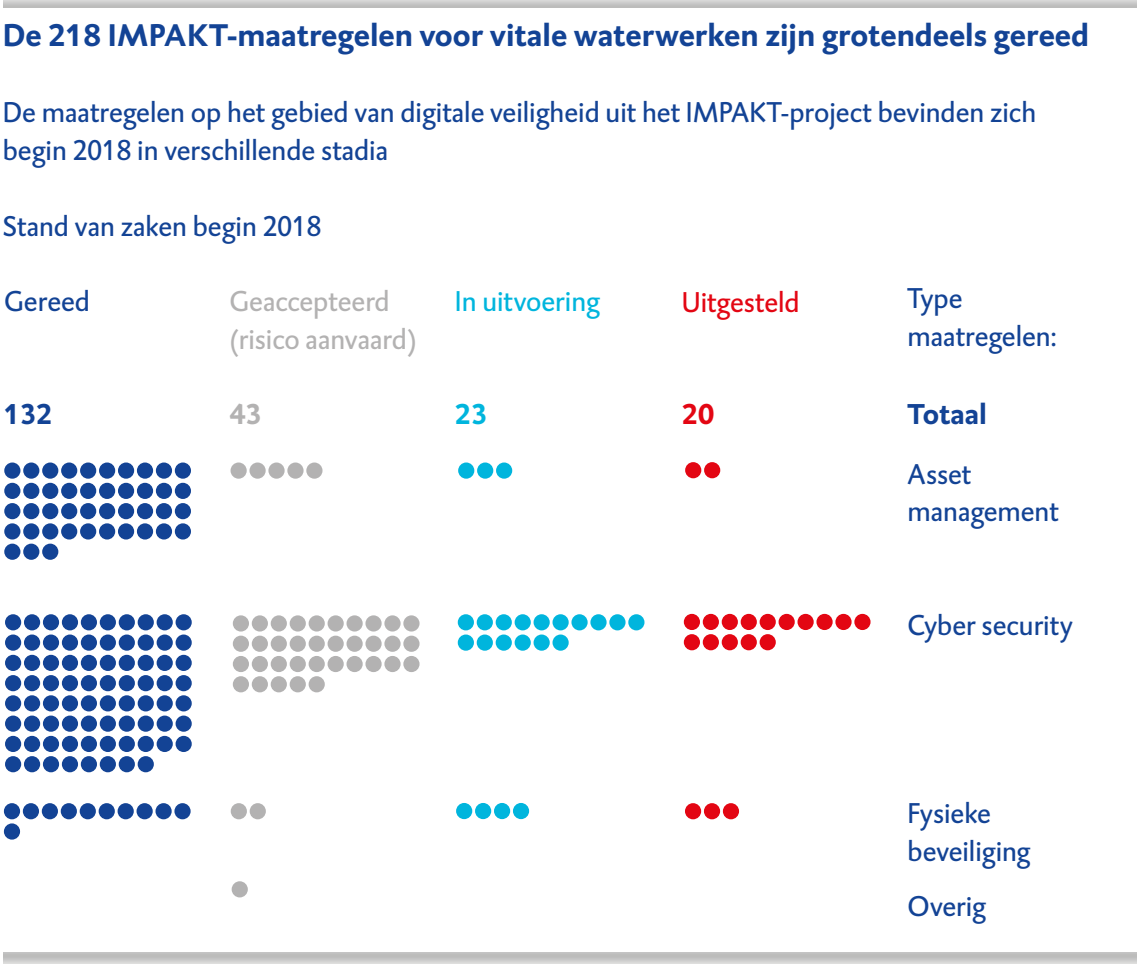
- Voer een upgrade uit op het besturingssysteem van de server naar een versie die versleuteling van gegevens ondersteunt.
- Zorg dat beheer op afstand alleen mogelijk is door een fysieke schakelaar bij het object om te zetten.
- Maak checklists waarop de uitgifte van toegangsmiddelen (sleutels, passen, accounts) wordt bijgehouden en waarop de ontvangers tekenen voor ontvangst.
- Verwijder wachtwoordstickers van alle toetsenborden en schermen.

Voor de uitvoering van de maatregelen waren beheerders van de waterwerken in de regio's verantwoordelijk gesteld. De medewerkers van IMPAKT ondersteunden de beheerders, coördineerden de uitvoering en bewaakten de voortgang.

3.3.2 Ongeveer zestig procent van maatregelen vitale waterwerken uitgevoerd

Wij hebben op basis van de laatste voortgangsrapportage onderzocht in hoeverre Rijkswaterstaat de geplande, cybersecuritygerelateerde, maatregelen heeft uitgevoerd. Deze voortgangsrapportage was begin 2018, kort na beëindiging van het programma BWR, voor het laatst bijgewerkt. Wij hebben ons geconcentreerd op de waterwerken die door de minister van IenW als vitaal zijn aangewezen (zie § 2.2).

Figuur 4 geeft een overzicht van de status van de cybersecuritygerelateerde maatregelen voor vitale waterwerken aan het einde van het programma BWR. Een groot deel van de 218 maatregelen is uitgevoerd (ongeveer 60%). Bij 43 van de voorgestelde maatregelen (20%) is bewust gekozen ze niet uit te voeren en het gesignaleerde risico te aanvaarden. Er waren nog 23 maatregelen in uitvoering (11%) en 20 tot nader order uitgesteld (9%).



Figuur 4 *Cybersecuritygerelateerde maatregelen bij vitale objecten*

Maatregelen zijn om verschillende redenen uitgesteld, nog niet opgestart of bewust geaccepteerd tijdens het programma BWR:

- De onderhoudscontracten met aannemers boden geen ruimte voor de gewenste aanpassingen op cybersecuritygebied, of de benodigde kennis bij die partijen ontbrak.
- De uitvoering bleek afhankelijk te zijn van andere initiatieven. Zo gaven medewerkers van één van de door ons onderzochte vitale waterwerken aan dat de maatregelen voor fysieke beveiliging afhankelijk waren van een lopend project dat zich breder op de fysieke beveiligingsaspecten richtte.
- De kosten bleken niet in verhouding te staan tot het te ondervangen risico. Zo bleek het bij één van de door ons onderzochte vitale waterwerken, gegeven het risico, te duur om verouderde apparatuur aan te passen om sterkere wachtwoorden mogelijk te maken.

De CIV heeft de niet-uitgevoerde maatregelen na afloop van het programma BWR overgedragen aan de beheerders van de waterwerken, de regio's. Hiervoor heeft het de regio's overdrachtsnota's met begeleidende brieven verstuurd. In de overdrachtsnota's is een overzicht opgenomen van de maatregelen die in het kader van IMPAKT waren geïdentificeerd en welke nog uitgevoerd moesten worden. Daarbij is vastgelegd dat de regio verantwoordelijkheid zou dragen voor deze restpunten en de begeleiding vanuit IMPAKT stopt. De financiering van de maatregelen werd bij de regio's gelegd. De nog uit te voeren maatregelen waren niet per definitie maatregelen met een laag risico. Bij één van de waterwerken moest bijvoorbeeld nog een belangrijk netwerkonderzoek uitgevoerd worden, was het sleutelbeheer nog niet op orde en hadden leidinggevenden nog geen cybersecurity-bewustwordingstraining gevolgd.

3.3.3 Geen centraal overzicht resterende maatregelen en geen budget

Het overzicht over de uitvoering van de aan de regio overgedragen maatregelen is een aandachtspunt voor Rijkswaterstaat. De CIO is daar vanaf 2018, na beëindiging van het programma BWR, verantwoordelijk voor. Het overzicht bij de CIV van alle maatregelen en hun status wordt sinds januari 2018, kort na het einde van het programma BWR, niet meer geactualiseerd. Een centraal en actueel overzicht van de manier waarop de regio's de resterende maatregelen hebben opgepakt, ontbreekt. De CIV kan bovendien realisatie van openstaande maatregelen niet afdwingen bij de regio's die de objecten beheren.

Medewerkers van de regio's geven aan dat Rijkswaterstaat er geen rekening mee heeft gehouden dat veel maatregelen structurele kosten met zich meebrengen. Een voorbeeld van zo'n maatregel is het opstellen van toegangsbeleid. Uiteraard vergt uitvoering van de

maatregel een eenmalige inspanning, in dit geval een proces opstellen, formaliseren en implementeren. Daarna moet het beleid echter ook structureel uitgevoerd worden. Dat gaat gepaard met evaluaties en bijstellingen. De regio's hebben hiervoor geen aanvullende middelen gekregen waardoor de financiering van de maatregelen die nog uitgevoerd moeten worden een discussiepunt binnen Rijkswaterstaat.

3.3.4 Voortzetting IMPAKT-aanpak vergt extra aandacht

Om de ervaringen die zijn opgedaan met IMPAKT niet verloren te laten gaan, heeft het bestuur van Rijkswaterstaat het instrument Functionele Inspecties en Testen (FIT) geïntroduceerd. Dit instrument is een aanvulling op bestaande inspecties van Rijkswaterstaat en neemt onder meer cybersecurity onder de loep. Bij de instelling van FIT is gekozen voor een groeimodel. In eerste instantie was FIT gekoppeld aan IMPAKT. Hiervoor ontving FIT budget uit het programma BWR. Het bestuur van Rijkswaterstaat heeft als ambitie uitgesproken FIT na afloop van het programma BWR op te nemen in de inspectie van vrijwel alle objecten met beweegbare delen.

Binnen FIT werken de regio's nauw samen met de CIV en andere centrale organisatieonderdelen. In het eerste jaar van FIT (2017) wilde Rijkswaterstaat het instrument bij "een aantal" objecten laten uitvoeren door de beheerders in de regio en bij zeven objecten door een centraal aangestuurd team van Rijkswaterstaat. Op basis van de ervaringen die hiermee werden opgedaan zou het CIV een voorstel doen voor verdere borging in de lijn. In 2018 zouden de centrale teams 21 objecten bezoeken. De doelstelling was dat uiteindelijk (2020) 470 objecten een jaarlijkse FIT-inspectie zouden ondergaan.

We constateren dat er in 2017 in totaal zeven FIT-inspecties zijn gedaan (door centraal Rijkswaterstaat én objectbeheerders). Daarmee is de ambitie voor 2017 niet volledig waargemaakt. Of het doel van 21 objectbezoeken voor 2018 zou worden gehaald, was ten tijde van ons onderzoek niet zeker. Voor de structurele inzet van FIT na 2017 was bij de introductie nog geen financiële dekking. Sinds de beëindiging van het programma BWR begin 2018 zijn de regio's daarvoor verantwoordelijk. Ook de financiering van FIT is daarmee onderwerp van gesprek tussen het bestuur en de regio's. Een volledige FIT inspectie kost € 25.000. In een brief namens het bestuur zijn de regio's verzocht actief medewerking te verlenen.

3.4 Cybersecurityeisen voor waterwerken van Rijkswaterstaat

3.4.1 Rijkswaterstaat ontwikkelt normen voor industriële automatiseringssystemen

Een tweede voor cybersecurity relevant resultaat van het programma BWR zijn de cybersecurityeisen voor de automatiseringssystemen van objecten die Rijkswaterstaat beheert. De hele sector waterkering en –beheer is van oudsher vooral civiel (bouwkundig) georiënteerd. In de tijd van de eerste automatisering van de waterwerken in de jaren 80 van de vorige eeuw waren de huidige digitale dreigingen nog vrijwel onbekend. In de ontwerpen en onderhoudscontracten van waterwerken is lange tijd nauwelijks rekening gehouden met cybersecurity. Rijkswaterstaat had reeds voor het programma BWR gemerkt dat de bestaande normenkaders voor informatiebeveiliging niet passend waren voor industriële automatiseringssystemen. Op basis van de ISO-standaard voor informatiebeveiliging heeft Rijkswaterstaat daarop een eigen normenkader voor cybersecurity van industriële automatiseringssystemen ontwikkeld: de Cybersecurity Implementatierichtlijn Objecten Rijkswaterstaat (CSIR). De eerste versie hiervan is rond 2012/2013 gebruikt bij de aanleg van de Gaasperdammertunnel. Een van de doelstellingen van het programma BWR was om cybersecurityeisen in onderhoudscontracten vast te leggen. De CSIR is daarvoor verder uitgewerkt en aangevuld. Het team Security by Design (Sbd), onderdeel van de Centrale Informatie Voorziening (CIV), neemt hierin voor alle onderdelen van Rijkswaterstaat het voortouw.

Bij de uitvoering van IMPAKT-maatregelen bleek dat gewenste aanpassingen soms niet binnen de bestaande onderhoudscontracten uit te voeren waren. Ook was kennis bij de onderhoudspartijen contractueel niet verplicht gesteld. Dit sterkte Rijkswaterstaat in de overtuiging dat cybersecurity integraal onderdeel moest uitmaken van alle producten, processen en systemen binnen de organisatie. Zo wordt cybersecurity een vast aandachtspunt gedurende de hele levenscyclus van een object: van eerste ontwerp tot en met het onderhoud, decennia na oplevering. De CSIR vormt hierbij in opzet het uitgangspunt.

3.4.2 Cybersecurityeisen stap voor stap opgenomen in contracten

Met de CSIR heeft Rijkswaterstaat zelf een normenkader voor cybersecurity ontwikkeld. De richtlijn biedt in opzet een basis die breed inzetbaar is bij waterwerken en industriële automatiseringssystemen. Wij hebben kunnen zien hoe de CSIR is opgebouwd en hoe eisen uit de BIR (Baseline Informatiebeveiliging Rijksdienst), het NCSC (Nationaal Cyber Security Centrum) en andere normenkaders hierin hun plek hebben gekregen. Een belangrijke observatie hierbij is dat Rijkswaterstaat alle eisen uit de BIR en de checklist

voor industriële automatiseringssystemen van het NCSC tegen het licht heeft gehouden en, indien relevant, heeft opgenomen in de CSIR.
De normen uit de CSIR worden momenteel stap voor stap opgenomen in alle contracten van Rijkswaterstaat. Hierbij speelt een rol dat de onderhoudscontracten vaak looptijden van 10 tot 20 jaar kennen. Het openbreken van bestaande onderhoudscontracten is juridisch ingewikkeld en kostbaar. Rijkswaterstaat kiest ervoor het einde van contracten af te wachten en bij een nieuw contract de cybersecuritynormen op basis van de CSIR vast te leggen. Zo worden de contracten van alle waterwerken stapsgewijs, in de loop van de komende jaren, 'cyberproof' gemaakt. In de onderhoudscontracten van één van de twee door ons onderzochte vitale waterwerken zijn de cybersecurityeisen volgens Rijkswaterstaat inmiddels geborgd.

3.5 Conclusies

We hebben gezien dat er na afloop van het programma Beveiligd Werken Rijkswaterstaat (BWR) geen centraal overzicht meer was op de voortgang van de resterende maatregelen van IMPAKT. Hierdoor is onvoldoende zicht op het risico dat ze niet worden uitgevoerd. Daarmee komt Rijkswaterstaat niet tegemoet aan haar eigen doelstellingen en bestaat het risico dat kwetsbaarheden bij objecten blijven bestaan. Rijkswaterstaat wil de ervaring met objectbezoeken uit IMPAKT bestendigen met het instrument FIT. We hebben gezien dat dit instrument nog niet conform de ambitie van Rijkswaterstaat wordt ingezet.

Bij beide conclusies signaleren we knelpunten op organisatorisch vlak, op het gebied van kennis en personeel en in de financiering.

Organisatie

De CIV noch het Rijkswaterstaatbestuur dwingt de realisatie van openstaande maatregelen af bij de regio's die de objecten beheren. Hetzelfde geldt voor deelname aan FIT.

Kennis en personeel

De IMPAKT-maatregelen waren niet altijd afdwingbaar omdat onderhoudscontracten met aannemers uitvoering ervan in de weg staan, of omdat de benodigde kennis bij die aannemers ontbreekt.

Rijkswaterstaat neemt de cybersecurityeisen uit de CSIR de komende jaren in alle contracten op. Hoewel dit gezien de looptijd van contracten nog jaren kan duren, is Rijkswaterstaat daarmee op weg om dit knelpunt weg te nemen.

Financiering

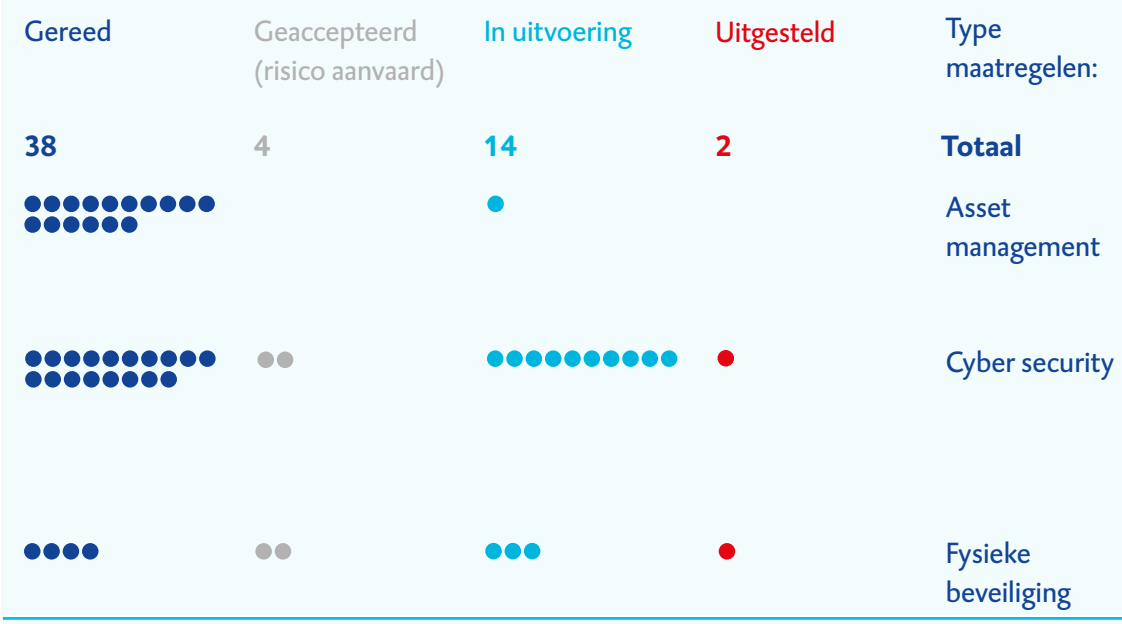
Rijkswaterstaat heeft, na beëindiging van het programma BWR, geen budget beschikbaar voor het uitvoeren van de overgedragen maatregelen. De regio's moeten de nog uit te voeren maatregelen uit bestaand budget herprioriteren. Ook deelname aan het instrument FIT moet uit bestaand budget. Dit leidt tot interne discussies over de financiering en herprioritering en zorgt voor vertraging in besluitvorming en uitvoering.

Onderzoek bij object Alfa

IMPAKT-maatregelen vrijwel afgerond, netwerkonderzoek blijft nodig
Wij hebben in het najaar van 2018 onderzoek gedaan bij object Alfa om de actuele stand van zaken ten aanzien van de IMPAKT-maatregelen in kaart te brengen. Figuur 5 geeft de stand van zaken weer van de maatregelen aan het einde van het programma BWR, zoals die bij Rijkswaterstaat bekend was.

66% van de IMPAKT-maatregelen waren bij Object Alfa uitgevoerd aan het einde van BWR

De maatregelen op het gebied van digitale veiligheid uit het IMPAKT-project bevinden zich begin 2018 in verschillende stadia



Figuur 5 *Status IMPAKT-maatregelen bij object Alfa aan het einde van het programma BWR*

Tijdens ons onderzoek bleek het grootste deel van de IMPAKT-maatregelen inmiddels formeel te zijn afgerond, of zo goed als afgerond. Op een belangrijke openstaande maatregel na. Deze maatregel kon niet binnen IMPAKT gerealiseerd worden. Aangezien er na beëindiging van het programma BWR geen budget meer beschikbaar was, was lange tijd onduidelijk wie de maatregel moest uitvoeren. Hierover ontstond in het najaar van 2018 duidelijkheid.

Kwetsbaarheidstest: hackers komen binnen, SOC detecteert
We hebben samen met Rijkswaterstaat en een extern bedrijf een testopzet gemaakt om de cybersecuritymaatregelen in de praktijk te toetsen bij object Alfa. Met de test zijn drie aspecten getoetst:

1. Het weerstandsniveau waar het gaat om ongeoorloofde toegang tot het object. Hiervoor is geprobeerd fysiek binnen te dringen, als eerste stap van een aanval op de digitale infrastructuur vanaf het terrein.
2. De detectiecapaciteit van het SOC en opvolging op het moment dat er een onbekend apparaat op het netwerk wordt aangesloten. Hiervoor is vanaf het terrein verbinding gemaakt met het netwerk.
3. Mogelijke zwakheden in de infrastructuur. Deze zijn getoetst door een expertreview op netwerkdiagrammen en gesprekken met medewerkers. Bij twijfel over zwakheden is de mogelijkheid om deze uit te buiten met een technische praktijktest gecontroleerd.

Bij het eerste testonderdeel is het het externe bedrijf tot tweemaal toe gelukt toegang te krijgen tot het object door middel van *social engineering* (het misleiden van personeel). De eerste keer hebben de testers toegang tot de controlekamer gekregen en werden zij alleen gelaten bij een open sleutelkast en niet-vergrendelde werkstations. De tweede maal slaagden de testers erin een tijdelijke toegangspas te bemachtigen waarmee zij zich vrijelijk door de locatie konden begeven. Ook bij dit bezoek hadden de testers toegang tot belangrijke onderdelen van de locatie, zoals serverruimtes en opslagruimtes voor kritische onderdelen.

Als tweede onderdeel van de test is vanaf het object een laptop aangesloten op het netwerk. Afgezien van één medewerker was het SOC hiervan uiteraard niet op de hoogte gesteld. De testers hebben zich bij het aansluiten van de laptop technisch gezien op verschillende manieren ‘gedragen’, variërend van zeer verdekt (waarbij geen netwerkverkeer gegenereerd werd) tot vrij opvallend. In alle gevallen werden zij door het SOC gedetecteerd. Normaal gesproken zou dit alle alarmbellen binnen Rijkswaterstaat laten afgaan. Omdat één SOC-medewerker op de hoogte was, is nu eerst contact opgenomen met de beheerders van het object, waarbij bevestigd werd dat het om een test ging.

Tenslotte heeft de externe partij vanuit de expertreview zeven bevindingen geformuleerd. De bevindingen bevestigen het eerder genoemde beeld dat de industriële automatiseringssystemen van vitale waterwerken naar moderne maatstaven kwetsbaar zijn en het nemen van maatregelen technisch complex en kostbaar is.

4 Detectie van cyberaanvallen en kwetsbaarheden

Rijkswaterstaat zet strategisch in op detectie van en respons op cyberaanvallen omdat het meestal niet mogelijk is de industriële automatiseringssystemen te vervangen of volledig te beschermen. Ons onderzoek richt zich daarom op deze elementen van de strategie.

In dit hoofdstuk gaan we in op het derde belangrijke cybersecurityresultaat van het programma BWR (zie hoofdstuk 3): de oprichting van een Security Operations Center (SOC). Hiermee geven we verder antwoord op de vraag welke instrumenten Rijkswaterstaat heeft om cyberdreigingen en -aanvallen te detecteren en in hoeverre deze bescherming bieden (eerste twee onderzoeksvragen). Ook gaan we nader in op de follow-up van detectie (vierde onderzoeksvraag), omdat het SOC ook verantwoordelijk is voor de detectie van kwetsbaarheden.

4.1 Het netwerk van Rijkswaterstaat en de detectiestrategie

4.1.1 Netwerk biedt bescherming, aanvullende strategie van detectie

Rijkswaterstaat beschikt over een eigen glasvezelnetwerk. Dit netwerk werpt al de nodige drempels op voor cyberaanvallen. Daarnaast neemt Rijkswaterstaat aanvullende cybersecuritymaatregelen om cyberaanvallen te detecteren.

Bij ons onderzoek bleek dat het exacte niveau van dreiging, met name dat van buitenlandse mogendheden (statelijke actoren), niet bekend is. De NCTV stelt (NCTV, 2018a) dat de dreiging van beroepscriminelen en statelijke actoren toeneemt en dat aanvallen steeds geavanceerder en complexer zijn. In het Cybersecuritybeeld Nederland 2018 (NCTV, 2018a) worden sabotage en verstoring door statelijke actoren de grootste bedreiging voor de nationale veiligheid genoemd. In het kader van ons onderzoek heeft het SOC ons aangegeven dat het denkbaar is dat geavanceerde aanvallers zich aan de detectie door Rijkswaterstaat kunnen onttrekken. Wat de exacte capaciteiten van aanvallers zijn en hoe groot hun bereidheid is om ze tegen vitale waterwerken in te zetten, is niet vastgesteld.

4.1.2 Niet alle vitale waterwerken in beeld

Voor de detectie en respons (reactie in geval van detectie) heeft Rijkswaterstaat een specialistisch team opgericht: het SOC. Het SOC is tijdens het programma BWR opgezet conform een *best practice* voor de rijksoverheid, opgesteld door experts van de Belastingdienst, het Shared Service Center-ICT (SSC-ICT) en Rijkswaterstaat zelf.

In het kader van detectie en respons is het wenselijk cyberaanvallen bij de vitale waterwerken direct te detecteren. Om directe detectie mogelijk te maken, moet Rijkswaterstaat maatregelen uitvoeren bij de vitale waterwerken.

Doel van Rijkswaterstaat was om eind 2017 bij alle vitale waterwerken cyberaanvallen direct te kunnen detecteren. In het najaar van 2018 was directe detectie bij iets minder dan de helft van de vitale waterwerken mogelijk.

De uitvoering van de maatregelen voor directe detectie bij alle vitale objecten is financieel gedekt. Voor 2018 is in de begroting van IenW een bedrag van € 5,4 miljoen toegekend, waarmee volgens Rijkswaterstaat de kosten van het SOC worden gedekt. De voornaamste reden dat de maatregelen voor directe detectie nog niet bij alle vitale waterwerken zijn uitgevoerd, is dat sommige regio's terughoudend zijn bij het uitvoeren van de maatregelen. Zij zien het uitvoeren van de maatregelen bijvoorbeeld als een risico. Het SOC kan het nemen van de maatregelen niet afdwingen. Doordat directe detectie door het SOC nog niet bij alle vitale waterwerken mogelijk is, is de detectiestrategie nog niet volledig operationeel.

De minister van IenW heeft een wettelijke verantwoordelijkheid om ernstige IT-incidenten te melden. De centrale monitoring van de vitale waterwerken door het SOC is daarin een middel. Zolang deze monitoring niet compleet ingericht is, ontbreekt het aan volledig zicht op de vitale waterwerken.

4.1.3 Detectie en respons door het SOC nog in ontwikkeling

Het SOC analyseert grote hoeveelheden data, uit verschillende bronnen, om hieruit verdachte activiteit te detecteren. Het maakt gebruik van software om de data te analyseren. De software is ingericht om bepaalde situaties en patronen te herkennen en melding te maken wanneer zo'n situatie zich voordoet. Ook categoriseert de software meldingen van 'laag risico' (relatief kleine kans dat er daadwerkelijk iets aan de hand is) tot 'kritiek' (vrijwel zeker sprake van een digitale aanval).

De medewerkers van het SOC beoordelen de meldingen vervolgens door nader onderzoek te doen. Hierbij werkt het SOC risicogestuurd: urgente meldingen krijgen prioriteit boven meldingen met een laag risico. Voorbeelden van verdachte situaties zijn ongewone verbindingen tussen twee computers bij een object, of een plotselinge afwijking in de hoeveelheid data op een deel van het Rijkswaterstaat-netwerk. Dit soort verdachte situaties kunnen duiden op een hack, of poging daartoe. Als het SOC na analyse een (mogelijk)

cyberincident signaleert, wordt de respons hierop in gang gezet door een melding bij het organisatieonderdeel Missie Kritieke Ondersteuning (MKO, zie § 5.1).

Het SOC kampt naar eigen zeggen met een beperkte beschikbaarheid van kennis en personeel. Daardoor is het bijvoorbeeld mogelijk dat de analyse van meldingen van mogelijke dreigingen in het gedrang komt: het SOC zegt dat meldingen met een lage prioriteit meerdere dagen blijven liggen. Het SOC geeft aan de detectie verder te willen verfijnen en professionaliseren. Zo kan de analyse van loggegevens op verdachte patronen bijvoorbeeld doorontwikkeld worden. Om de strategie van respons op basis van detectie verder uit te bouwen is volgens Rijkswaterstaat aanvullende financiering nodig, bovenop de toegekende € 5,4 miljoen voor het jaar 2018. Dit is eind 2017 aangevraagd door Rijkswaterstaat maar door de minister van IenW niet vertaald naar een begrotingsvoorstel aan de Tweede Kamer.

We hebben geconstateerd dat het precieze niveau van dreiging waar de vitale waterwerken mee worden geconfronteerd op terrein van cybersecurity ten tijde van ons onderzoek nog niet inzichtelijk is . Dit maakt de discussie over de allocatie van extra middelen bovenop de aansluiting van de vitale waterwerken een moeilijke. Onduidelijk is wanneer de getroffen maatregelen in lijn zijn met het dreigingsniveau.

4.2 Signalering van dreiging en kwetsbaarheden

Het is een van de taken van het SOC om kwetsbaarheden te signaleren en daarop te reageren (respons). Bij een kwetsbaarheid is nog geen sprake van een cyberaanval, maar gaat het om een gesignaleerd risico dat (mogelijk) aangepakt moet worden. In de eerste plaats verzamelt het SOC hiervoor *intelligence*. Dit staat voor 'inlichtingen', naar analogie van de terminologie bij veiligheidsdiensten. Het SOC verzamelt, analyseert en duidt informatie over cyberdreigingen. Aan de hand van de gesignaleerde dreigingen (*threats*) kan Rijkswaterstaat maatregelen nemen om de dreiging weg te nemen of de gevolgen te beperken.

Bij het verzamelen van *threat intelligence* combineert het SOC eigen informatie en informatie van partners. Hierbij stemt het SOC af met diverse partijen zoals de AIVD, de MIVD en SOC's van andere (overheids-)organisaties. Het NCSC is voor het SOC bijvoorbeeld een externe bron van informatie over kwetsbaarheden. Het gaat dan bijvoorbeeld om industriële apparatuur waarin digitale kwetsbaarheden zijn ontdekt die een hacker zou kunnen uitbuiten.

De medewerker die namens het SOC als liaison in contact komt met partijen als NCSC is AIVD-gescreend (niveau A). Wij constateren dat de overige medewerkers van het SOC alleen beschikken over een Verklaring Omtrent het Gedrag (VOG). Rijkswaterstaat stelt aan die medewerkers geen hogere eisen. Dit bemoeilijkt kennisuitwisseling omdat niet alle van de AIVD afkomstige informatie intern kan worden gedeeld. Daarnaast komen SOC-medewerkers in aanraking met gevoelige systeeminformatie van vitale objecten.

Het SOC controleert ook of er in de organisatie afwijkingen te vinden zijn van het security-beleid van Rijkswaterstaat. Het checkt bijvoorbeeld of apparatuur voorzien wordt van de verplichte updates. Wanneer het SOC een afwijking constateert, adviseert het de regio's over maatregelen om de afwijking op te lossen. Het SOC kan de beheerder van een object niet dwingen om adviezen op te volgen. Het kan bijvoorbeeld zijn dat een regio het risico van de installatie van een update groter vindt dan het risico dat zij loopt door de update niet uit te voeren. In situaties die een acute dreiging veroorzaken, heeft het SOC mandaat om actief in te grijpen. Bijvoorbeeld door kwaadaardige e-mails in quarantaine te plaatsen, risicovolle IP-adressen te blokkeren of ongeautoriseerde apparatuur direct van het netwerk van Rijkswaterstaat te verwijderen. Volgens Rijkswaterstaat is er incidenteel gebruik gemaakt van dit mandaat.

4.3 Conclusies

In dit hoofdstuk zijn we ingegaan op onze onderzoeksvraag over de detectie van en respons op cyberaanvallen. Rijkswaterstaat geeft met het SOC vorm aan een strategie van detectie en respons. Deze strategie is echter nog in ontwikkeling en nog niet voltooid. Niet bij alle vitale waterwerken kunnen cyberaanvallen direct gedetecteerd worden. Daardoor heeft het SOC geen actueel cybersecurity-beeld van alle vitale waterwerken en bestaat het risico dat vitale objecten ongemerkt gehackt kunnen worden. Dit is van invloed op de plicht van de minister om ernstige IT-incidenten in de sector te melden. Of de maatregelen die Rijkswaterstaat treft voldoende zijn, is afhankelijk van het dreigingsniveau. Dit dreigings-niveau is echter niet bekend .

Bij deze conclusies signaleren we knelpunten op organisatorisch vlak, op het gebied van kennis en personeel en in de financiering.

Organisatie

Sommige regio's zijn terughoudend bij het nemen van maatregelen die directe detectie van cyberaanvallen mogelijk maken. Ook zijn regio's niet verplicht de adviezen van het SOC op te volgen. Het SOC kan beide niet afdwingen, het bestuur wel.

Kennis en personeel

We constateren dat de meeste medewerkers van het SOC alleen beschikken over een Verklaring Omtrent het Gedrag (VOG), terwijl ze in aanraking komen met gevoelige systeeminformatie van vitale objecten. Of dit conflicteert met het dreigingsniveau is, bij gebrek aan inzicht hierin, niet vast te stellen.

Financiering

In de begroting is de financiering van het SOC geborgd. Voor de verdere doorontwikkeling van het SOC heeft Rijkswaterstaat naar eigen zeggen niet voldoende (aanvullende) middelen. Inzicht in het dreigingsniveau is nodig om een goede keuze in allocatie te maken.

Onderzoek bij object Bravo

Maatregelen IMPAKT afgerond, overdrachtsdocument niet bekend bij regio
Wij hebben in het najaar van 2018 onderzoek gedaan bij object Bravo om de actuele stand van zaken ten aanzien van de IMPAKT-maatregelen in kaart te brengen. Figuur 6 geeft de stand van zaken weer van de maatregelen aan het einde van het programma BWR, zoals die bij Rijkswaterstaat bekend was.

79% van de IMPAKT-maatregelen waren bij Object Bravo uitgevoerd aan het einde van BWR

De maatregelen op het gebied van digitale veiligheid uit het IMPAKT-project bevinden zich begin 2018 in verschillende stadia

Stand van zaken begin 2018

Gereed	Geaccepteerd (risico aanvaard)	In uitvoering	Uitgesteld	Type maatregelen:
27	6	**0**	**1**	**Totaal**
●●●●●●	●●●●			Asset management
●●●●●●●●●●●●	●●			Cyber security
●			●	Fysieke beveiliging

Figuur 6 *Status IMPAKT-maatregelen bij object Bravo aan het einde van het programma BWR*

Bij ons onderzoek bij object Bravo bleek dat de overdrachtsdocumentatie van IMPAKT, waarmee uitvoering van de resterende maatregelen formeel bij de regio waren neergelegd, niet bekend was. De genoemde maatregelen of hun status werden ook niet alle herkend. Wel waren de maatregelen inmiddels getroffen. Zo is er *hardening* toegepast (het versterken van digitale weerbaarheid door fabrieksinstellingen en standaardwachtwoorden aan te passen en niet-gebruikte IT-onderdelen uit te schakelen) en hebben we gezien dat er op advies van IMPAKT een server is verplaatst naar een afgesloten ruimte. Het IMPAKT-advies om de gegevens op de server te versleutelen is bij object Bravo bewust niet opgevolgd. De regio zegt dat de gegevens nodig kunnen zijn in een noodsituatie en het risico dat ontsleutelen dan niet lukt zwaarder weegt. Dit is een voorbeeld van een risico dat Rijkswaterstaat bewust en onderbouwd heeft geaccepteerd.

Kwetsbaarheidstest: onderdeel *stand alone*, data moeilijk te manipuleren
We hebben een test van een onderdeel van object Bravo meegenomen in dit onderzoek. Speciale aandacht is daarbij uitgegaan naar de externe koppelingen van systemen die betrokken worden bij dit onderdeel.

Bij object Bravo is voor de bediening een conservatieve aanpak gekozen; de bediening is primair handmatig. Deze keuze heeft nu als voordeel dat er minder risico's op het gebied van cybersecurity zijn. Wel beschikt object Bravo over een systeem dat het personeel bij besluitvorming over de bediening van het object ondersteunt en een systeem dat automatische sluiting in werking zet in geval van calamiteiten. Bijvoorbeeld omdat de bediening onbereikbaar is. Beide systemen ontvangen informatie in de vorm van metingen vanuit verschillende bronnen.

Met het oog op ons onderzoek ging onze speciale aandacht uit naar de koppelingen tussen deze systemen en van de systemen met het (openbare) internet. We hebben geconstateerd dat er wel een koppeling is tussen beide systemen; het systeem dat object Bravo in geval van een calamiteit automatisch sluit geeft het ondersteunende systeem aan nog in werking te zijn. Dit is de enige communicatie die tussen beide systemen mogelijk is. Hij kent ook maar een richting: van het sluitende naar het ondersteunende systeem, niet vice versa.

De meetstations die beide systemen cruciale informatie leveren over de waterstand zijn fysiek beveiligd. Bovendien betrekt en vergelijkt het ondersteunende systeem gegevens uit verschillende bronnen; onderling afwijkende gegevens vallen daardoor direct op. Het systeem dat object Bravo sluit in geval van een calamiteit bevindt zich op een aparte, afgesloten locatie. Rijkswaterstaat heeft maatregelen genomen om ongeoorloofde toegang te voorkomen. Bij de test werd het systeem in werking gezet door de meetstations handmatig te beïnvloeden.

Bij object Bravo zijn nog geen maatregelen genomen om directe detectie van cyberaanvallen door het SOC mogelijk te maken. Hierdoor bestaat het risico dat een cyberincident langer dan nodig onopgemerkt blijft.

5 Voorbereiding op cyberincidenten en -crises

Naast detectie is respons een van de centrale elementen in de cybersecurity-strategie van Rijkswaterstaat. In dit hoofdstuk gaan we in op de wijze waarop Rijkswaterstaat zich voorbereidt op cybersecurity-gerelateerde incidenten en crises en reageert op incidenten. Daarmee geven we antwoord op onze derde en vierde onderzoeksvraag.

We beginnen het hoofdstuk door te laten zien hoe Rijkswaterstaat kleine, min of meer geïsoleerde, cyber*incidenten* afhandelt. In de tweede paragraaf beschrijven we de voorbereidingen van Rijkswaterstaat op, grotere en complexere, cyber*crises*. De derde paragraaf gaat in op pentesten.

5.1 Afhandeling cyberincidenten via Missie Kritieke Ondersteuning

Een cyberincident wordt gedefinieerd als een individuele gebeurtenis die schade veroorzaakt, of kan veroorzaken door verstoring, uitval of misbruik van IT, en die mogelijk veroorzaakt wordt door een cyberaanval. Een voorbeeld van een cyberincident is een melding van het SOC dat er vanaf een computer bij een vitaal waterwerk geprobeerd wordt gegevens naar de buitenwereld te sturen. Dit is een melding die onderzocht moet worden omdat er sprake kan zijn van een cyberaanval.

Melding en afhandeling van deze mogelijke cyberincidenten gebeuren binnen het reguliere incidentmanagement van Rijkswaterstaat. De afdeling Missie Kritieke Ondersteuning (MKO) is bij Rijkswaterstaat de centrale regisseur voor alle meldingen over de IT-systemen die voor de missie van Rijkswaterstaat essentieel zijn (missiekritiek). De afdeling MKO neemt de melding van een cyberincident op, registreert die en bewaakt de opvolging. Een medewerker van Rijkswaterstaat die bij een object (brug of sluis) een cyberincident vermoedt, meldt dat via een regionale bediencentrale. Ze vormen de 24-uurs meldkamers van Rijkswaterstaat. Van daaruit wordt het als incident gemeld bij de afdeling MKO.

Ook het SOC kan, zoals eerder geschetst, cyberincidenten signaleren. Op dat moment hoeft men bij het object nog niets te merken. Ook het SOC meldt cyberincidenten bij de afdeling MKO. Voordat dat gebeurt wordt het incident door het SOC nader onderzocht. Ziet het SOC bijvoorbeeld dat er een afwijking is op het IT systeem van een object dan wordt er eerst contact gelegd met de beheerder van dat object. In de praktijk is de afwijking soms het gevolg van (geplande) werkzaamheden van een monteur en gaat het niet om een ongeoorloofde poging om binnen te komen. Het SOC wordt door de objectbeheerders

namelijk niet van te voren op de hoogte gesteld van werkzaamheden. Momenteel moeten medewerkers van het SOC meldingen die de software genereert nog zelf melden bij de afdeling MKO. Rijkswaterstaat wil dit in de toekomst geautomatiseerd doen.

Per maand registreert de afdeling MKO ongeveer 40 cyberincidenten. MKO heeft standaard-werkwijzen voor het afhandelen van cyberincidenten. Eenvoudige gevallen behandelt de afdeling MKO zelf. Hiertoe zijn de MKO-medewerkers opgeleid; het SOC heeft daarvoor het opleidingstraject opgezet.

In complexe gevallen wordt eventueel een zogenoemde oplosgroep geformeerd voor de afhandeling van de melding. Het SOC kan onderdeel uitmaken van een oplosgroep. De oplosgroep onderzoekt de oorzaken van het incident en adviseert over oplossingen en het voorkomen van escalatie. Wanneer een melding niet volgens de standaardwerkwijzen kan worden afgehandeld, volgt opschaling. Vanaf dat moment komt het crisismanagement van Rijkswaterstaat in beeld (§ 5.2).

In gesprekken met het SOC en de afdeling MKO heeft Rijkswaterstaat aangegeven dat alle geconstateerde cyberincidenten ‘vals alarm’ betroffen. Er is tot nu toe volgens Rijkswaterstaat nog geen cyberaanval waargenomen bij een waterkering.

5.2 Voorbereiding op crises

5.2.1 Crisismodel Rijkswaterstaat kent geen cybersecurity-scenario

We spreken van een cybercrisis zodra er een langdurige en/of complexe IT-verstoring optreedt als gevolg van een cyberaanval. Een cyberincident kan zich ontwikkelen tot een cybercrisis: bijvoorbeeld in het geval van *ransomware* die zich vanaf één computer over het gehele netwerk verspreidt.

Opschaling (escalatie) en afschaling zijn belangrijke principes in de omgang met een crisis. Bij op- en afschaling kunnen, afhankelijk van hoe de crisis zich ontwikkelt, verschillende organisaties worden ingeschakeld bij de beheersing en bestrijding. Rijkswaterstaat maakt gebruik van een crisismodel met drie opschalingsfases. Elke fase kent een ander crisisteam. Als een crisisteam er niet in slaagt de situatie beheersbaar te maken, volgt opschaling naar een volgende fase. Het crisismodel beschrijft de werkwijze van de teams en criteria voor opschaling.

Het crisismodel van Rijkswaterstaat kent verschillende scenario's ter voorbereiding op specifieke soorten crises. Voorbeelden van zulke scenario's zijn een aanvaring of oppervlaktewaterverontreiniging. In een crisisscenario zijn onder andere opschalingscriteria uitgewerkt. Rijkswaterstaat heeft geen specifiek scenario voor een cybersecuritycrisis.

Bij cybercrises maakt Rijkswaterstaat gebruik van de zogenaamde Netwerkkaart Cybersecurity. Hierop staat:

- Welke partijen bij een cybersecuritycrisis betrokken zouden moeten zijn;
- Welke partijen met elkaar contact hebben voor inhoudelijke afstemming;
- Welke partijen met elkaar contact hebben voor coördinatie.

De Netwerkkaart Cybersecurity laat wel zien welke netwerkpartners betrokken zijn bij een cybercrisis maar geeft geen beeld van de hiërarchische verhoudingen en de opschalingslijnen tussen de partijen. Dat betekent dat de kaart ook geen inzicht biedt in wat er moet gebeuren tijdens een crisis, de volgordelijkheid daarvan en de verantwoordelijkheden per partij.

Het Ministerie van IenW wordt bij een crisis betrokken als de crisis beleidsoverstijgend is en bijvoorbeeld ook de luchtvaart of het spoor raakt. Het Departementaal Crisis Centrum (DCC) van het ministerie coördineert het hele crisisbesluitvormingsproces binnen IenW en draagt zorg voor de informatievoorziening voor de interdepartementale crisisteams.

Zoals eerder beschreven vloeit er uit de Wet beveiliging netwerk- en informatiesystemen (Wbni) een meldplicht voort. Dit betreft incidenten die zodanig (potentieel) maatschappelijk ontwrichtend van aard zijn, dat ze gemeld moeten worden bij onder meer het NCSC. Deze kan dan het risico van maatschappelijke ontwrichting inschatten en bijstaan in het voorkomen of beperken van die ontwrichting. Verder kan het NCSC tijdig andere vitale sectoren waarschuwen voor potentiele dreiging en zo verdere verspreiding voorkomen.

De drempelwaarden voor melding van incidenten bij het NCSC vallen onder verantwoordelijkheid van de vakministers, in het geval van Keren en Beheren dus de minister van IenW. Een drempelwaarde geeft bijvoorbeeld de maximale tijdspanne weer waarbinnen een melding moet worden gedaan. De voor Rijkswaterstaat relevante drempelwaarden zijn in november 2018 vastgesteld. Tot die tijd was volgens Rijkswaterstaat niet helder wanneer een incident bij een vitaal waterwerk aan de NCSC moest worden gemeld.

5.2.2 Belangrijke crisisdocumentatie bij het SOC deels verouderd

In geval van een calamiteit moet het SOC snel inzicht hebben in de belangrijkste gegevens van de vitale waterwerken. Het SOC gebruikt daarvoor crisiskaarten en netwerkoverzichten.

Crisiskaarten

Op de crisiskaarten staan belangrijke kenmerken van de industriële automatiseringssystemen van de waterwerken. Deze kaarten bevatten onder meer contactgegevens van beheerders, opdrachtnemers en andere stakeholders van een object. Uit de aard van de documenten volgt dat deze informatie juist en volledig moet zijn. We constateren dat de informatie op de crisiskaarten deels verouderd of onvolledig is. Dit betreft bijvoorbeeld de contactgegevens van personen die in geval van een calamiteit moeten worden benaderd. Het risico dat hier uit volgt werd zichtbaar toen het SOC in de zomer van 2018 contact wilde opnemen met een systeemdeskundige van één van de twee door ons onderzochte vitale waterwerken over gesignaleerde uitval van een onderdeel van het netwerk. De op de crisiskaart vermelde medewerker van de regio bleek de dag ervoor met vakantie te zijn gegaan. Het zou beter zijn de contactinformatie te koppelen aan een rol in plaats van aan een persoon. In de oefening bij één van de twee door ons onderzochte waterwerken werd op basis van de crisiskaart contact opgenomen met een medewerker die geen rol had in het oplossen van storingen bij het object.

De crisiskaarten geven een momentopname weer, gemaakt bij de objectbezoeken van IMPAKT, en zijn soms meer dan een jaar oud. Een crisiskaart krijgt pas een update wanneer er iemand van het SOC bij het object langskomt of er bij contact gemerkt wordt dat er een gegeven verouderd is. Op het moment van ons onderzoek bestond er nog geen proces om de crisiskaarten actueel te houden.

Netwerkoverzichten

De netwerkoverzichten waar het SOC gebruik van maakt in tijden van een crisis geven een beeld van de componenten die deel uitmaken van het lokale netwerk van objecten. Ze laten zien hoe de onderdelen met elkaar in verbinding staan, welke poorten openstaan en via welke protocollen over die poorten kan worden gecommuniceerd. De overzichten tonen daarmee de ‘ingangen’ die een hacker zou kunnen gebruiken. Ook laten ze zien hoe de hacker zich verdere toegang tot het netwerk kan verschaffen. Deze overzichten zijn voor veel van de in IMPAKT bezochte objecten gemaakt. Ze bieden een beeld van de situatie ten tijde van IMPAKT. Dit betekent dat de overzichten soms al meerdere jaren oud zijn.

Van de netwerkoverzichten die we hebben gezien, gaf Rijkswaterstaat aan dat de inrichting van het netwerk in de tussentijd nauwelijks tot niet was gewijzigd. Toch bestaat het risico dat er in de regio aanpassingen aan het netwerk zijn gedaan waarvan het SOC niet weet. Na plaatsing van een netwerksensor bij een object heeft het SOC altijd een actueel beeld van het netwerk.

5.2.3 Nog weinig inzicht in cascade-effecten

Een crisis in een vitale sector kan effecten hebben op andere vitale sectoren zoals Vervoer of Energie. Dit noemen we cascade-effecten. Het NCTV richt zich op deze afhankelijkheidsrelaties. Zo wordt momenteel in samenwerking met TNO onderzoek gedaan naar ketenafhankelijkheden binnen meerdere vitale sectoren. Door dit in kaart te brengen kunnen partijen binnen de keten afspraken met elkaar maken en sneller schakelen bij een (dreigende) crisis. In ons onderzoek hebben we bij Rijkswaterstaat op centraal niveau geen document aangetroffen dat inzicht geeft in de mogelijke cascade-effecten vanuit of naar de sector Keren en Beheren.

Op dit moment heeft het SOC wel een samenwerkingsovereenkomst met de waterschappen om tijdig te kunnen reageren op incidenten die effecten kunnen hebben *binnen* de sector. Medewerkers van de waterschappen zijn dagelijks werkzaam bij het SOC. Zo wordt kennis uitgewisseld over securityincidenten en de opvolging daarvan. Voorts zijn op 31 oktober 2018 aanvullende afspraken op het Bestuursakkoord Water uit 2011 bekrachtigd door de minister van IenW (UvW, IPO, Vewin, IenW, VNG, 2018). Onderdeel hiervan is om in 2020 een sectorbrede afhankelijkheids- en kwetsbaarheidsanalyse voor cybersecurity uit te voeren, om onderlinge ketenafhankelijkheden vast te stellen.

5.3 Pentesten bij Rijkswaterstaat

Een penetratietest of kortweg *pentest* is een (door de te testen organisatie zelf) geautoriseerde poging om een beveiligingssysteem te omzeilen of te doorbreken. Op die manier kan een organisatie inzicht krijgen in de effectiviteit van en mogelijke veiligheidsrisico's voor een systeem en hiervoor verbeterpunten vaststellen (GOVCERT, 2010). Rijkswaterstaat kan pentesten gebruiken om de cybersecuritymaatregelen bij vitale waterwerken in de praktijk te testen en deze te verbeteren. Deze testen zouden zo een waardevolle aanvulling zijn in de voorbereiding op cyberaanvallen.

In de praktijk doet Rijkswaterstaat geen pentesten van enige omvang op de industriële automatiseringssystemen. De voor die testen benodigde specialistische software is volgens

Rijkswaterstaat vooral bedoeld voor 'reguliere' IT en niet voor industriële automatiseringssystemen. Rijkswaterstaat geeft aan beperkte kennis te hebben van pentesten op industriële automatiseringssystemen. Daarnaast beschikken lang niet alle objecten over een testomgeving. Volwaardige pentesten op vitale waterwerken terwijl die in werking zijn, zijn niet mogelijk vanwege de daaraan verbonden risico's.

Dat de risico's niet denkbeeldig zijn, illustreert een praktijkvoorbeeld dat in onze contacten met Rijkswaterstaat meerdere keren ter sprake kwam. Bij een test werd een laptop aangesloten op een waterwerk dat in werking was, op volgens de documentatie toegestane wijze. Hierop ontstond een storing in het waterwerk en werd het onbedienbaar. Doordat de noodstop nog wel functioneerde, kon worden ingegrepen. Het is echter niet ondenkbaar dat dit incident had kunnen leiden tot fysieke ongelukken of schade aan het waterwerk.

De Baseline Informatiebeveiliging Rijksdiensten (BIR) schrijft voor dat rijksorganisaties periodiek hun systemen checken met een pentest. Rijkswaterstaat heeft de BIR in de CSIR 'vertaald' voor zijn industriële automatiseringssystemen (zie § 3.4). De verplichting om pentesten te doen heeft het daarbij afhankelijk gemaakt van de beperkingen van deze systemen, en daarmee in feite optioneel. Wat Rijkswaterstaat wel doet en heeft gedaan binnen het project IMPAKT, kunnen we omschrijven als 'kwetsbaarheidsscans'. Daarbij worden wel potentiele ingangen in een systeem blootgelegd, maar worden deze vervolgens niet benut om op het systeem te komen. Doordat Rijkswaterstaat geen pentesten doet ontbreekt het de organisatie aan informatie over hoe weerbaar de vitale waterwerken in de praktijk zijn tegen cyberaanvallen.

5.4 Conclusies

In dit hoofdstuk zijn we ingegaan op onze onderzoeksvragen over de voorbereiding en reactie van Rijkswaterstaat op cyberincidenten en –crises. We hebben gezien dat Rijkswaterstaat geen specifiek cybersecurityscenario heeft binnen het gehanteerde crisismodel, hoewel dit voor vele andere scenario's wel het geval is. Ook bleek dat onderdelen van belangrijke crisisdocumentatie verouderd of onjuist waren en dat er geen proces is om deze regulier bij te werken. In geval van een crisis kan Rijkswaterstaat daardoor niet steunen op volledige, actuele en betrouwbare informatie. Tot slot constateren we dat Rijkswaterstaat geen volwaardige pentesten uitvoert op de industriële automatiseringssystemen en hiermee afwijkt van de BIR.

Bij de voorbereidingen van Rijkswaterstaat op cybercrises zien we knelpunten op twee gebieden.

Organisatie

Op het moment van ons onderzoek had Rijkswaterstaat nog geen proces ingericht om de crisiskaarten en netwerkoverzichten in afstemming met de regio's regelmatig te actualiseren.

Kennis en personeel

Rijkswaterstaat heeft een gebrek aan kennis en expertise om, conform de BIR, pentesten uit te voeren op de automatiseringssystemen van vitale waterwerken. Zonder pentesten kan Rijkswaterstaat de cybersecuritymaatregelen voor objecten niet in de praktijk toetsen.

6 Conclusies en aanbevelingen

Ons onderzoek richtte zich op de vitale sector Keren en Beheren en de vitale waterwerken binnen deze sector. De minister van IenW draagt hiervoor politieke verantwoordelijkheid. Rijkswaterstaat beheert de vitale waterwerken. De minister van IenW moet verantwoording afleggen over de maatregelen die Rijkswaterstaat treft aangaande het vergroten van de cybersecurity (van vitale waterwerken). De gestelde doelen moeten daarbij kunnen worden gerealiseerd met de thans beschikbaar gemaakte mensen en middelen.

In voorgaande hoofdstukken hebben we, uitgaande van onze onderzoeksvragen, laten zien welke maatregelen Rijkswaterstaat heeft getroffen om de waterkering weerbaar te maken tegen cyberdreigingen en hoe dit in de praktijk werkt. Ook hebben we belicht hoe Rijkswaterstaat reageert in geval van cyberincidenten en cybercrises. We hebben uiteengezet dat de automatiseringssystemen van de vitale waterwerken zijn opgezet in een tijd dat cybersecurity nog niet bestond. Door toenemende koppeling van automatiseringssystemen binnen en buiten Rijkswaterstaat, zijn deze kwetsbaarder geworden voor een cyberaanval. Rijkswaterstaat moet met traditionele middelen een traditionele dreiging (het water) het hoofd bieden, terwijl de moderne tijd die traditionele middelen bedreigt. Dat is de opgave anno 2019.

Ondersteunende constateringen uit praktijkonderzoek

In het kader van ons onderzoek heeft een derde partij de automatiseringssystemen van één van de door ons geselecteerde vitale waterwerken onderzocht. Daaruit kwam naar voren dat deze naar moderne maatstaven kwetsbaar zijn.

Rijkswaterstaat richt zich in zijn strategie vooral op detectie van en respons op cyberaanvallen. Het volledig voorkomen van dergelijke aanvallen is namelijk, gezien de specifieke kenmerken van industriële automatiseringssystemen, kostbaar en technisch uitdagend. Onze hoofdconclusie is dat Rijkswaterstaat sinds 2014 een goede inhaalslag heeft gemaakt maar er nog niet in geslaagd is de eigen streefwaarden van beveiliging te halen.

In dit hoofdstuk presenteren we de deelconclusies die dit oordeel ondersteunen en voorzien we deze vervolgens van onze aanbevelingen.

6.1 Inzicht in dreigingsniveau

Hoe groot de dreiging van een cyberaanval voor de sector Keren en Beheren precies is, is op het moment van ons onderzoek nog niet inzichtelijk. Om te kunnen beoordelen of maatregelen 'passend' zijn, is dit inzicht wel nodig. Op basis van dergelijk inzicht kan ook bepaald worden welke allocatie van mensen en middelen voor de passende maatregelen nodig zijn. Dit geldt ook voor het benodigde kennisniveau of de mate van screening van medewerkers. We hebben geconstateerd dat het ontbreken van dit inzicht in de praktijk leidt tot onzekerheden op deze elementen. De eerste aanbeveling aan de minister van IenW is dan ook:

1. Voer een onderzoek uit naar het actuele feitelijke cybersecurity-dreigingsniveau voor de vitale waterwerken ten behoeve van nadere besluitvorming over allocatie van mensen en middelen.

6.2 Afronding programma Beveiligd Werken Rijkswaterstaat

Met het programma Beveiligd Werken Rijkswaterstaat (BWR) is een inhaalslag gemaakt op het gebied van cybersecurity bij de vitale waterwerken. We zien dat na afloop van het programma BWR een groot deel van de voorgestelde maatregelen is uitgevoerd. De resterende maatregelen zijn overgedragen aan de regio's die de objecten in beheer hebben. Centraal overzicht van de status van de maatregelen ontbreekt. Om de met het programma BWR ingezette lijn te bestendigen heeft Rijkswaterstaat het instrument Functionele Inspecties en Testen (FIT) geïntroduceerd. We constateren echter dat Rijkswaterstaat in de uitvoering van FIT de gestelde doelen nog niet haalt.

De CIV kan de regio's het uitvoeren van resterende maatregelen en deelname aan FIT niet opleggen. Het bestuur, dat deze macht wel heeft, laat dit vooralsnog na. De financiering voor de uitvoering van beide is een intern discussiepunt dat besluitvorming en uitvoering vertraagt.

Ondersteunende constateringen uit praktijkonderzoek

Bij de door ons nader onderzochte vitale waterwerken bleek het grootste deel van de maatregelen inmiddels te zijn afgerond. Bij één van de waterwerken bleek een belangrijke openstaande maatregel nog niet uitgevoerd. Na beëindiging van het programma BWR was er geen budget meer beschikbaar. Daardoor was lange tijd onduidelijk wie de maatregel moest uitvoeren. Bij een ander vitaal waterwerk bleek dat de overdrachtsdocumentatie, waarmee uitvoering van de resterende maatregelen formeel bij de regio waren belegd, niet bekend was.

We doen de minister de volgende aanbevelingen:

2. Draag Rijkswaterstaat op centraal en uniform zicht te creëren op de opvolging van de BWR-restpunten die zijn overgedragen aan de regio's en zorg te dragen voor de uitvoering van de resterende maatregelen.
3. Versterk daarnaast waar nodig de instrumenten die in het leven zijn geroepen om de met het programma BWR ingezette lijn voort te zetten (waaronder FIT) met voldoende mensen en middelen.

6.3 Voltooiing strategie van detectie en respons

De belangrijkste taak van het Security Operations Center (SOC) is de detectie van en de reactie (respons) op cyberaanvallen. Om cyberaanvallen bij de door de minister aangewezen vitale waterwerken direct te detecteren is besloten specifieke maatregelen bij de vitale waterwerken te nemen. De ambitie was om dit eind 2017 te hebben gerealiseerd. Dit doel is niet gehaald: in het najaar van 2018 kon Rijkswaterstaat bij iets minder dan de helft van de vitale waterwerken cyberaanvallen direct detecteren. Hierdoor bestaat het risico dat Rijkswaterstaat een cyberaanval bij een vitaal waterwerk niet of te laat detecteert.

Ondersteunende constateringen uit praktijkonderzoek

Uit een test bij een van de door ons onderzochte vitale waterwerken bleek dat het mogelijk was fysiek toegang te verkrijgen tot de controlekamer, een open sleutelkast en niet-vergrendelde werkstations. Digitale toegang (het aansluiten van een laptop) werd opgemerkt door het SOC. Bij dit waterwerk zijn maatregelen getroffen om cyberaanvallen direct te detecteren. Dit laatste is niet aan de orde bij een ander vitaal waterwerk dat wij onderzocht hebben. Daar bestaat dus het risico dat Rijkswaterstaat een cyberaanval niet of te laat opmerkt.

Het SOC gebruikt de beschikbare capaciteit naar eigen zeggen grotendeels voor de analyse van meldingen van mogelijke cyberaanvallen. Daardoor blijven doorontwikkeling en kennisdeling achter. Zolang het dreigingsniveau van de sector nog niet inzichtelijk is, is het echter moeilijk te beoordelen of kennis en capaciteit daarmee in lijn zijn.

Daarnaast constateren we dat medewerkers van het SOC worden gescreend op het niveau van VOG (Verklaring Omtrent het Gedrag). Het is de vraag of dit voldoende is om te werken met gevoelige gegevens over cyberdreigingen.

Om de detectie op cyberaanvallen bij vitale waterwerken te voltooien en, zo nodig, verder te professionaliseren bevelen we de minister aan:

4. Voltooi de maatregelen die directe detectie van cyberaanvallen mogelijk maken en bouw de monitoring door het SOC uit (op basis van het objectief vastgestelde dreigingsniveau, zie aanbeveling 1).
5. Heroverweeg het niveau van screening voor SOC-medewerkers en de rubricering van gevoelige overzichtsdocumentatie van het SOC (op basis van het objectief vastgestelde dreigingsniveau, zie aanbeveling 1).

6.4 Actuele crisisdocumentatie en volwaardige pentesten

Rijkswaterstaat bereidt zich voor op crises, waaronder cybercrises, met een crisismodel. Dit model kent verschillende specifieke crisisscenario's. Voor een door een cyberaanval veroorzaakte crisis blijkt geen specifiek scenario te bestaan. Ook is er op centraal niveau bij Rijkswaterstaat geen inzicht in de cascade-effecten van een cyberaanval op de vitale waterwerken. Daarnaast zien we dat belangrijke documenten bij de bestrijding van een cyberaanval (crisiskaarten en netwerkoverzichten) niet actueel gehouden worden. Het risico bestaat daardoor dat de reactie op een cybercrisis niet tijdig en adequaat is.

Voor de vitale waterwerken worden door Rijkswaterstaat nauwelijks pentesten ingezet om zich voor te bereiden op cyberaanvallen. Daarmee ontbreekt het de organisatie aan informatie over hoe weerbaar de vitale waterwerken in de praktijk zijn tegen cyberaanvallen.

Onze aanbevelingen aan de minister zijn:

6. Instrueer Rijkswaterstaat een proces te ontwerpen en te implementeren om de informatie op de crisiskaarten en netwerkoverzichten actueel te houden.
7. Instrueer Rijkswaterstaat een specifiek crisisscenario voor cybersecuritycrises in het crisismodel op te nemen.
8. Maak expliciet welke risico's het doen van volwaardige pentesten op de industriële automatiseringssystemen van de vitale waterwerken in de weg staan en stippel op basis hiervan een route uit om tot een situatie te komen waarin pentesten een integraal onderdeel vormen van de cybersecuritymaatregelen bij vitale waterwerken.

7 Reactie minister en nawoord Algemene Rekenkamer

De minister van IenW heeft op 5 maart 2019 gereageerd op ons rapport. Hieronder geven we haar reactie samengevat weer. De volledige reactie staat op www.rekenkamer.nl. We sluiten af met ons nawoord.

7.1 Reactie minister van Infrastructuur en Waterstaat

In haar reactie geeft de minister van IenW (verder: de minister) aan onze conclusies te onderschrijven en zich verantwoordelijk te voelen voor de digitale veiligheid van de waterwerken. De minister ziet onze conclusies en aanbevelingen als een ondersteuning van de reeds door haar in gang gezette werkzaamheden om de cybersecurity van de watersector verder te verbeteren. De recent voltooide IenW-brede cybersecuritystrategie geeft daarbij volgens de minister richting aan het maken van de juiste keuzes.
De minister geeft aan onze aanbevelingen allemaal op te pakken. Zo zal de minister (laten) inzetten op een praktische doorvertaling van de algemene dreigingsbeelden en de aanvullende informatie verkregen vanuit de samenwerking met de diensten naar mogelijke consequenties voor de individuele vitale objecten (aanbeveling 1).

De uitkomst van deze analyse van het dreigingsbeeld is volgens de minister van invloed op de opvolging van een deel van onze overige aanbevelingen. Zo zal de minister op basis van het dreigingsniveau de prioritering van de resterende BWR-maatregelen bepalen en versterking van het programma FIT overwegen, waarmee deze ingezette lijn geborgd moet worden (aanbevelingen 2 en 3). Ook geeft de minister aan dat de object-gerelateerde dreigingsinformatie meegenomen wordt in de besluitvorming over normering en hiervoor benodigde inzet van mensen en middelen (aanbeveling 4). Tot slot zal ze op basis van het dreigingsniveau, in overleg met de NCTV, de mogelijkheden laten onderzoeken om het screeningsniveau van de betrokken medewerkers beter aan te laten sluiten (aanbeveling 5).

De minister geeft verder aan ook de aanbevelingen over te nemen op het terrein van respons (aanbeveling 6 en 7). De noodzaak om cascade-effecten inzichtelijk te krijgen heeft de minister opgenomen in het in oktober afgesloten Bestuursakkoord Water. Voor een breder beeld van deze cascade-effecten, sluit het Ministerie van IenW volgens de minister aan bij de aanpak van intersectorale afhankelijkheden van het Ministerie van Justitie en Veiligheid. Ook zal de minister in lijn met onze aanbeveling onderzoeken wat de risico's en mogelijkheden zijn voor invoeren van pentesten bij bestaande systemen (aanbeveling 8).

In haar reactie geeft de minister eveneens aan dat Rijkswaterstaat ondertussen een flinke inhaalslag heeft gemaakt ten aanzien van de opvolging van de BWR-restpunten. Het complete overzicht van de stappen die nog moeten worden gezet om de BWR doelstellingen de halen, is volgens de minister inmiddels beschikbaar.

7.2 Nawoord Algemene Rekenkamer

De minister erkent onze conclusie dat er aanvullende maatregelen uitgevoerd moeten worden voor cybersecurity van de vitale waterwerken. Allereerst om te voldoen aan de eigen doelstellingen en daarnaast om aan te sluiten op het actuele dreigingsniveau nadat dit in kaart is gebracht.

Echter, de uitvoering van onze aanbevelingen maakt de minister afhankelijk van de opvolging van onze eerste aanbeveling: het duiden van het dreigingsniveau. Alhoewel dit logisch lijkt, willen wij de minister er op wijzen dat het ook gaat om het spoedig afronden van maatregelen die al eerder getroffen hadden moeten zijn. We doelen dan bijvoorbeeld op het aansluiten van de vitale waterwerken op het SOC zodat er meer diepgaand en actueel zicht op deze waterwerken is. Dit had eind 2017 al gerealiseerd moeten zijn en is dus niet afhankelijk van de eerste aanbeveling.

De minister wijst in haar reactie verder op de recent vastgestelde IenW-brede cybersecurity-strategie, die ten tijde van ons onderzoek nog niet beschikbaar was. We zullen de voortgang die hiermee ingezet gaat worden met belangstelling volgen evenals de implementatie en uitvoering van toegezegde maatregelen.

Bijlagen

Bijlage 1 Methodologische verantwoording

In dit rapport beantwoorden we de volgende onderzoeksvragen:

1. Welke instrumenten heeft Rijkswaterstaat als beheerder in handen om cyberdreigingen en -aanvallen te detecteren en zich te beschermen tegen cyberdreigingen voor de waterkeringen?
2. In hoeverre werken de instrumenten om cyberdreigingen en -aanvallen te detecteren? En bieden ze voldoende bescherming?
3. Welke scenario´s liggen klaar voor wanneer zich een cyberaanval voordoet; met welke maatregelen kan Rijkswaterstaat voorkomen dat andere vitale sectoren ook geraakt worden bij een aanval (cascade-effecten)?
4. Hoe werkt de respons bij detectie van kwetsbaarheden en incidenten bij Rijkswaterstaat?

Bij beantwoording van deze vragen hebben we ons gebaseerd op (interne) documentatie van met name Rijkswaterstaat en het Ministerie van IenW. Dit betrof naast beleidsstukken en interne memo's ook de concrete informatie over de IMPAKT-bezoeken (scores op de normen van het toetsingskader per bezocht object, duiding van gedetecteerde kwetsbaarheden bij geselecteerde objecten, de maatregelen die daarop werden geformuleerd en de stand van zaken bij beëindiging van het programma BWR).
Verder hebben we veel gesprekken gevoerd met medewerkers van Rijkswaterstaat (zowel van de CIV als van de regio's waar we onze objectonderzoeken hebben uitgevoerd) en van het Ministerie van IenW. Ook spraken we met andere stakeholders: de NCTV, het NCSC, de Unie van Waterschappen en het Watermanagement Centrum. Daarnaast hebben we gesproken met experts op het terrein van cybersecurity, met name ten behoeve van het testen van de werking van maatregelen.

De beantwoording van de onderzoeksvraag naar de werking van maatregelen stond centraal bij de bezoeken aan een aantal geselecteerde vitale waterwerken. Als uitgangspunt voor ons onderzoek daar dienden de IMPAKT-bezoeken en daaruit voortkomende maatregelen. Vervolgens hebben we de werking van die maatregelen in de praktijk bekeken. Bij één van de onderzochte vitale waterwerken hebben we een reguliere test geobserveerd. Bij een ander onderzocht vitaal waterwerk hebben we de effectiviteit van de maatregelen beoordeeld aan de hand van een samen met Rijkswaterstaat georganiseerde pentest.

De selectie van de onderzoeksobjecten was onze keuze, in goed overleg met de gecontroleerde. Criteria die bepalend waren voor de keuze van de objecten waren:

- Waterwerk op de lijst van vitale objecten;
- Wel en niet maatregelen voor directe detectie uitgevoerd;
- Ouderdom van het object;
- Mogelijke cascade-effecten van uitval van het object.

We hebben geconstateerd dat zich nog geen cyberincident heeft voorgedaan bij een waterwerk. Daardoor is de beoogde reconstructie van de respons op een dergelijk incident niet mogelijk geweest. Door te kijken naar in het verleden uitgevoerde oefeningen (bij de onderzochte vitale waterwerken) en door de pentest die we in samenwerking met Rijkswaterstaat en een extern bedrijf bij één van de vitale waterwerken hebben uitgevoerd, hebben we geprobeerd daar toch inzicht in te krijgen.

Bijlage 2 Normen waaraan we toetsen

De minister van Infrastructuur en Waterstaat (IenW) draagt verantwoordelijkheid voor de cybersecurity van de vitale sector Keren en Beheren en daarbinnen voor de door haar aangewezen vitale waterwerken. Onderdeel daarvan is het voldoen aan de meldplicht (waarvoor door de minister een drempelwaarde is bepaald). Rijkswaterstaat beheert de door de minister aangewezen vitale waterwerken en is opdrachtnemer voor de passende maatregelen.

Van belang in ons onderzoek is onze algemene norm aangaande de ministeriële verantwoordelijkheid en doelmatigheid: wanneer derden publiek geld innen, beheren of besteden en/of wanneer zij een publieke taak uitvoeren, moet de verantwoordelijke minister zich er altijd door goed toezicht van vergewissen dat dit rechtmatig en doelmatig gebeurt. De minister van IenW moet altijd (aan de Tweede Kamer) verantwoording kunnen afleggen over de maatregelen die Rijkswaterstaat heeft getroffen en nu nog treft aangaande het vergroten van de cybersecurity (van waterwerken). De minister moet daarvoor onder meer weten welke prestaties Rijkswaterstaat op dit gebeid levert en welke gevolgen deze hebben. De doelen moeten gerealiseerd kunnen worden met de beschikbare mensen en middelen. We verwachten dat de minister van IenW in overleg met Rijkswaterstaat is nagegaan of het beleid uitvoerbaar (ook in tijd) en handhaafbaar is, en of de getroffen maatregelen de beoogde werking zullen hebben.

Naast deze algemene norm hebben we in ons onderzoek vooral normen betrokken die gebaseerd zijn op de doelen die de minister en Rijkswaterstaat zichzelf stellen om de cybersecurity van de vitale waterwerken op orde te brengen. Zo is daar het doel om alle maatregelen die door het programma Beveiligd Werken Rijkswaterstaat (BWR) zijn geïdentificeerd op bestaande kwetsbaarheden tot uitvoering te brengen (of met redenen omkleed het risico van het bestaan er van te accepteren). Het niet uitvoeren van de maatregel (of het niet accepteren van het risico) betekent immers dat de gesignaleerde kwetsbaarheid voor cyberdreigingen blijft bestaan. Dit doel en de daaruit voortvloeiende norm is vooral van toepassing op onze eerste deelconclusie.

Een ander doel, voortvloeiend uit het programma BWR, is het nemen van maatregelen die directe detectie van cyberaanvallen mogelijk maken bij alle vitale waterwerken die door de minister van IenW zijn aangewezen (en om dit voor het einde van 2017 te doen). Deze norm hebben we vooral gerelateerd aan onze tweede deelconclusie. Voorts hebben we hierbij de norm betrokken aangaande de beschikbaarheid van de juiste mensen (kwaliteit,

screenings, taakverdeling en ‘inwisselbaarheid’) voor detectie en opvolging (ontleend aan ISO27002).

Tot slot zijn voor de derde deelconclusie normen betrokken aangaande beschikbaarheid, volledigheid, betrouwbaarheid en actualiteit van standaarden, procedures, plannen en tests inzake onder meer het incident- en crisismanagement. Voorts hebben we voor deze deelconclusie gekeken naar de door Rijkswaterstaat ontwikkelde normen betreffende industriële automatiseringssystemen. We hebben kunnen vaststellen dat Rijkswaterstaat bij de vertaling van de Baseline Informatiebeveiliging Rijk (BIR) naar de eigen normen voor industriële automatiseringssystemen, sommige eisen die de BIR stelt voor zichzelf optioneel heeft gemaakt. Het gaat dan om het uitvoeren van pentesten. Rijkswaterstaat heeft die keuze gemaakt vanwege de karakteristieke eigenschappen (en ouderdom) van zijn systemen.

Bijlage 3 Lijst van afkortingen en Engelstalige begrippen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
Assetmanagement	Het beheren van bedrijfsmiddelen. Assetmanagement is een breed begrip, in de context van dit onderzoek gaat het over het software- en wijzigingsbeheer, processen voor onderhoud en storingen, en de samenwerking met contractpartijen en (onder)aannemers bij vitale waterwerken.
BIR	Baseline Informatiebeveiliging Rijksdienst, een stelsel van algemene beveiligingsmaatregelen die van toepassing is op alle informatie en informatiesystemen bij de rijksoverheid.
BWR	Beveiligd Werken Rijkswaterstaat, een programma dat zich onder meer richtte op cybersecurity binnen Rijkswaterstaat.
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIV	Centrale Informatie Voorziening
CSIR	Cybersecurity Implementatierichtlijn Objecten Rijkswaterstaat
FIT	Functionele Inspecties en Testen, een inspectie van kritieke onderdelen van objecten op onder meer cybersecurity.
HVWN	Hoofdvaarwegennet
HWN	Hoofdwegennet
HWS	Hoofdwatersysteem
IenW	Infrastructuur en Waterstaat
IMPAKT	Impulsprogramma Aanpak Kritieke Technische Infrastructuur, een deelproject van het programma BWR dat (onder andere) cybersecuritymaatregelen definieerde en liet uitvoeren bij Rijkswaterstaat-waterwerken.
ISAC	Information Sharing and Analysis Centre
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NAP	Normaal Amsterdams Peil
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
Pentest	Penetratietest, een 'proefhack' waarmee een organisatie de digitale beveiliging in de praktijk test.

Ransomware	Gijzelsoftware, een chantagemiddel waarmee IT onbruikbaar wordt gemaakt door een aanvaller en de getroffen partij alleen na het leveren van een tegenprestatie (meestal het betalen van geld) weer gebruik kan maken van de IT.
SOC	Security Operations Center
Social engineering	Aanvalsmethode van (ethische) hackers waarbij getracht wordt toegang tot systemen te krijgen door gebruikers te misleiden, bijvoorbeeld door hen hun wachtwoord te ontfutselen.
SSC-ICT	Shared Service Center-ICT
Stand alone	Losstaand, zonder verbindingen en koppelingen naar buiten.
Threat intelligence	Informatie over digitale dreigingen.
VOG	Verklaring Omtrent het Gedrag, een verklaring waaruit blijkt dat het gedrag van een persoon in het verleden geen bezwaar vormt voor het vervullen van een functie of rol.
Wbni	Wet beveiliging netwerk- en informatiesystemen
Wgmc	Wet gegevensverwerking en meldplicht cybersecurity

Bijlage 4 Literatuur

Publicaties

Agence nationale de la sécurité des systèmes d'information (2012). *Managing Cyber-security for Industrial Control Systems*. Parijs: eigen beheer.

Algemene Rekenkamer (2011). *Rapport bij het Jaarverslag 2010 Ministerie van Infrastructuur en Milieu*. Den Haag: eigen beheer.

Algemene Rekenkamer (2012). *Rapport bij het Jaarverslag 2011 Ministerie van Infrastructuur en Milieu*. Den Haag: eigen beheer.

Algemene Rekenkamer (2013). *Rapport bij het Jaarverslag 2012 Ministerie van Infrastructuur en Milieu*. Den Haag: eigen beheer.

Algemene Rekenkamer (2014). *Rapport bij het Jaarverslag 2013 Ministerie van Infrastructuur en Milieu*. Den Haag: eigen beheer.

Algemene Rekenkamer (2015). *Rapport bij het Jaarverslag 2014 Ministerie van Infrastructuur en Milieu*. Den Haag: eigen beheer.

Algemene Rekenkamer (2016). *Rapport bij het Jaarverslag 2015 Ministerie van Infrastructuur en Milieu*. Den Haag: eigen beheer.

[-] 14

GOVCERT (2010). *Pentesten doe je zo*. Den Haag: eigen beheer.

NCSC (2016). *Uw ICS/SCADA- en gebouwbeheersystemen online*. Den Haag: eigen beheer.

NCTV (2018). *Nederlandse Cybersecurity Agenda, Nederland digitaal veilig*. Den Haag: eigen beheer.

NCTV (2018). *Cybersecuritybeeld Nederland 2018*. Den Haag: eigen beheer.

Rijksoverheid (2017). *Vertrouwen in de toekomst: Regeerakkoord 2017–2021*. Den Haag: eigen beheer.

Unie van Waterschappen, IPO, Vewin, IenW, VNG (2018). *Aanvullende Afspraken Bestuursakkoord Water*. Den Haag: eigen beheer.

VenJ (2105). *Brief aan de Tweede Kamer van de minister van Veiligheid en Justitie d.d. 12 mei 2015, over herziening van de Strategie Nationale Veiligheid, herijking vitale infrastructuur en verbetering crisisbeheersing*. Tweede Kamer, vergaderjaar 2014-2015, 30821, nr. 23.

Wet- en regelgeving

Besluit meldplicht cybersecurity. Besluit van 4 december 2017 tot aanwijzing van aanbieders, producten en diensten ten aanzien waarvan een plicht geldt om ernstige ICT-incidenten te melden.[15]

Besluit beveiliging netwerk- en informatiesystemen. Besluit van 30 oktober 2018, houdende regels ter uitvoering van de Wet beveiliging netwerk- en informatiesystemen.

Besluit van Minister van Infrastructuur en Waterstaat van 21-12-2017, met kenmerk Rijkswaterstaat-2017/49666 tot aanwijzing van vitale waterkeringen of onderdelen daarvan in verband met het van kracht worden het Besluit Meldingsplicht Cybersecurity.

Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013). Besluit van de Minister-President, Minister van Algemene Zaken van 1 juni 2013, nr. 3124134, houdende voorschrift informatiebeveiliging Rijksdienst – bijzondere informatie 2013.

Comptabiliteitswet 2016. Wet van 22 maart 2017, houdende regels inzake het beheer, de informatievoorziening, de controle en de verantwoording van de financiën van het Rijk, inzake het beheer van publieke liquide middelen buiten het Rijk en inzake het toezicht op het beheer van publieke liquide middelen en publieke financiële middelen buiten het Rijk.

RICHTLIJN (EU) 2016/1148 VAN HET EUROPEES PARLEMENT EN DE RAAD van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

Wet beveiliging netwerk- en informatiesystemen. Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148.[16]

Wet gegevensverwerking en meldplicht cybersecurity. Wet van 25 juli 2017, houdende regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken.[17]

Bijlage 5 Eindnoten

1 ICT (informatie- en communicatietechnologie) en IT (informatietechnologie) zijn inwisselbare begrippen. In dit rapport gebruiken we het, in onze ogen iets gangbaardere, IT.

2 Cybersecurity was een van de onderdelen van een toetsingskader. Daarnaast werd ook naar andere onderdelen gekeken die nauw verband houden met cybersecurity. Hierop gaan we in § 3.3 nader in.

3 Strikt genomen zijn bijvoorbeeld schade aan een computer door blikseminslag of het per vergissing wissen van gegevens ook cybersecurityrisico's. Dit onderzoek spitst zich toe op dreigingen waaraan bewust menselijk handelen ten grondslag ligt. Merk op dat Rijkswaterstaat niet per se het specifieke doelwit van een cyberaanval hoeft te zijn en er soms 'onschuldige' derden bij betrokken zijn. Een computervirus kan bijvoorbeeld geschreven zijn om willekeurig computers te besmetten en onbewust worden verspreid door een Rijkswaterstaat-medewerker die te goeder trouw is.

4 Het betreft richtlijn (EU) 2016/1148, bekend als de NIB-richtlijn (netwerk- en informatieveiligheid richtlijn).

5 Wij merken op dat het (niet publieke) besluit dat wij hebben ingezien nog verwijst naar de inmiddels vervallen Wgmc en kennelijk nog niet is vervangen door een nieuwe versie.

6 Het programma Eén Vandaag besteedde hier aandacht aan: https://eenvandaag.avrotros.nl/item/sluizen-gemalen-en-bruggen-slecht-beveiligd/ Overigens is het in de reportage geschetste beeld, waarin industriële automatiseringssystemen direct aan het internet zijn verbonden, niet van toepassing op de door Rijkswaterstaat beheerde waterwerken. Die suggestie wordt wel gewekt door de beelden in de reportage van onder andere de Maeslandt- en de Oosterscheldekering.

7 In het document van het NCSC wordt gesproken over ICS/SCADA. Dit is veelgebruikt jargon dat we vermeden hebben in dit rapport; in de praktijk is de term een synoniem voor industriële automatiseringssystemen.

8 Zie bijvoorbeeld: https://www.computable.nl/artikel/ict_topics/security/3814774/1276896/softwarefout-veroorzaakte-ongeluk-ketelbrug.html Het incident bij de Ketelbrug is illustratief voor het belang van goed functionerende industriële automatiseringssystemen en voor de achterblijvende kennis van organisaties daaromtrent.

9 Zie eindnoot 6.

10 De Algemene Rekenkamer spreekt van een onvolkomenheid wanneer een ministerie een bedrijfsvoeringsproces niet goed heeft ingericht of uitgevoerd Om als onvolkomenheid te worden aangemerkt, moet het probleem dat wij constateren meer zijn dan een incident en ook enig (financieel) gewicht hebben.

11 Dit ministerie is van naam veranderd en heet tegenwoordig ministerie van Infrastructuur en Waterstaat (IenW). Voor de leesbaarheid refereren we in de rest van dit rapport aan het ministerie van IenW, ook wanneer het gaat om een moment in de tijd waarop het ministerie nog de oude naam droeg.

12 Naast waterwerken in het HWS (hoofdwatersysteem), ging het ook om objecten in het HVWN en het HWN.

13 De voorbeelden zijn ter illustratie en voor de leesbaarheid niet letterlijk overgenomen en ontdaan van jargon en technische details.

14 In het conceptrapport stond hier de rapportage van de kwetsbaarheidstest bij object Alfa vermeld. Hieruit was op te maken welke partij de test uitvoerde. Dit is vertrouwelijke informatie die uit de definitieve versie van dit rapport is verwijderd.

15 Vervallen per 09-11-2018.

16 Deze wet stond geruime tijd bekend onder de oorspronkelijke citeertitel: Cybersecuritywet.

17 Vervallen per 09-11-2018.

Voorlichting

Afdeling Communicatie
Postbus 20015
2500 EA Den Haag
telefoon (070) 342 44 00
voorlichting@rekenkamer.nl
www.rekenkamer.nl

Omslag

Ontwerp: Corps Ontwerpers
Foto: HH/EyeEm Mobile GmbH

Den Haag, maart 2019