Ministerie van Infrastructuur
en Waterstaat

Programma Versterken Cyberweerbaarheid in de Watersector 2019-2022

Rapportage Haalbaarheidsstudie harmonisatie standaarden voor de Cybersecurity van Industrial Control Systems (ICS) in het kader van het Bestuursakkoord Water (BAW)

Rapportage Haalbaarheidsstudie harmonisatie standaarden voor de Cybersecurity van Industrial Control Systems (ICS) in het kader van het Bestuursakkoord Water (BAW)

Opdrachtgever: Directoraat-generaal Water en Bodem
Programma versterken cyberweerbaarheid in de watersector

Opgesteld door: Jessica Maes, I-Control Company
10 november 2020

Versie 1.2

Managementsamenvatting

In oktober 2018 hebben de waterpartners (Het Rijk, de Vereniging van Nederlandse Gemeenten (VNG), het Interprovinciaal Overleg (IPO), de Unie van Waterschappen (UvW) en de Vereniging van waterbedrijven in Nederland (Vewin)) aanvullende afspraken gemaakt op het Bestuursakkoord Water. Het addendum bevat onder anderen afspraken over de verdere samenwerking op het terrein van risico's van digitale dreigingen.

Om in de toekomst beter voorbereid te zijn op cyberaanvallen is voor en door de watersector het programma Versterken Cyberweerbaarheid in de Watersector opgezet. Het ministerie van Infrastructuur en Waterstaat en partijen in de watersector werken in dit programma samen in diverse projecten, die met name gericht zijn op operationele technologie. Denk aan een verdere invoering van het basisniveau informatiebeveiliging (baselines), maar ook aan de ontwikkeling van aanvullende eisen voor procesautomatisering, zodat de informatiebeveiliging in 2021 op orde is.[1]

Binnen de sector operationele technologie zijn Industriële controlesystemen (ICS) belangrijk. Deze systemen worden gebruikt om industriële processen te bewaken en te besturen. Dit rapport beschrijft de mogelijkheden om te komen tot een gemeenschappelijke standaard voor ICS Security binnen de BAW-ketenpartners. Om dit te beoordelen is een aantal onderzoekvragen beantwoord. Ook is een vergelijking gemaakt met internationale normen en de meest gebruikte normen binnen de waterketenpartners. Uit analyse, op basis van documentanalyse, interviews en een expert workshop, blijkt dat er voldoende inhoudelijke overeenkomsten en draagvlak is om tot een gemeenschappelijke standaard te komen. Ook biedt deze analyse inzicht in de toegevoegde waarde hiervan voor andere organisaties.

Normen

In het algemeen is de Baseline Informatiebeveiliging Overheid (BIO)[2] (gebaseerd op de ISO27000 serie) voor veel organisaties nog de basis van cybersecurity in ICS-omgevingen, aangevuld met de IEC 62443 en de NIST-800-82. Bijna alle waterketenpartners maken gebruik van een (mix) van deze normen.

Er zijn twee maatwerknormen in gebruik:

1. De Cyber Security Implementatie Richtlijn objecten (CSIR) van Rijkswaterstaat (Rijkswaterstaat).
2. De Proces Automatisering (PA)-beveiligingsnorm van de drinkwaterbedrijven.

Aan het einde van 2020 komt er een nieuwe, actuele versie van de CSIR, die enkele jaren geleden is opgesteld door Rijkswaterstaat. Deze norm heeft zich al bewezen in de praktijk, de adoptiegraad is hoog bij ketenpartners van Rijkswaterstaat. Uit een vergelijking op basis van beschikbare informatie blijkt dat er in de normenset van de CSIR en de PA-beveiligingsnorm waarschijnlijk veel overeenkomsten te vinden zijn. Beide normen gebruiken dezelfde basis, aangevuld met de IEC 62443 en de NIST-800-82.

De PA-beveiligingsnorm en CSIR kunnen als uitgangspunt dienen voor een gemeenschappelijke standaard. Bestuurlijk gezien is het de wens om een sectorale standaard op te stellen, blijkt onder andere uit de rapportage van de Cyber Security Raad[3]. Dit kan veel synergie in kennisdeling realiseren.

Randvoorwaarden:

- Het verminderen van bestuurlijke en administratieve lasten, ook in relatie tot de implementatie van de Wbni en Bbni;
- De mogelijkheid om uit te kunnen gaan van een groeipad, omdat volwassenheidsniveaus binnen de organisaties verschillend zijn;
- Het gebruiken van risicomanagement als integraal onderdeel van de standaard;
- Het integreren van ICS Cybersecurity tot een integraal cybersecurity managementsysteem binnen de organisaties. De risico's en maatregelen van ICS Cybersecurity zouden niet separaat binnen de cybersecurity organisatie moeten worden toegepast maar integraal aan de hand van het Cyber Security Management Systeem (CSMS).

Uit een inventarisatie met de BIO-werkgroep, bestaande uit alle organisaties die de BIO toepassen, blijkt een verbinding met de documentatie van de BIO, bijvoorbeeld in de vorm van een handreiking, mogelijk. Een gestandaardiseerde norm kan beter gedeeld worden en is mogelijk van toegevoegde waarde voor andere organisaties die ICS toepassen.

[1] De drinkwatersector heeft aangegeven dat zij géén onderdeel van de betreffende afspraak uit het BAW zijn. Zij hebben in het kader van de Wbni reeds een eigen normenset voor beveiliging van de PA opgesteld.

[2] https://bio-overheid.nl

[3] https://www.cybersecurityraad.nl/010_Actueel/cyberweerbaarheid-iacs-in-nederland-onvoldoende-op-orde.aspx

Inhoudsopgave

Inleiding

1. Cybersecurity Problematiek van ICS

Het Rijk, de Vereniging van Nederlandse Gemeenten (VNG), het Interprovinciaal Overleg (IPO), de Unie van Waterschappen (UvW) en de Vereniging van waterbedrijven in Nederland (Vewin) sloten in 2011 het Bestuursakkoord Water (BAW). Daarin is afgesproken om de doelmatigheid van het waterbeheer te vergroten. Minder bestuurlijke drukte, heldere verantwoordelijkheden, slim en kosteneffectief samenwerken staan centraal in deze afspraken, die lopen tot 2021. In oktober 2018 hebben de waterpartners aanvullende afspraken gemaakt op het BAW. Het addendum (BAW+) bevat nieuwe en hernieuwde afspraken, onder anderen over de risico's van digitale dreigingen.

Het programma

In het programma Versterken Cyberweerbaarheid in de Watersector is onder meer afgesproken om de samenwerking verder te verstevigen. Ook wordt gestreefd naar een verdere invoering van het basisniveau informatiebeveiliging (baselines) en ontwikkeling van aanvullende eisen voor procesautomatisering, zodat de informatiebeveiliging in 2021 op orde is. Op deze manier kunnen de betreffende organisaties voldoen aan de zorgplicht. De zorgplicht is vastgelegd in de Wet beveiliging netwerk- en informatiesystemen (Wbni), dit zal in het volgende hoofdstuk worden toegelicht. De drinkwaterbedrijven geven invulling aan hun zorgplicht door middel van de eisen uit de drinkwaterregelgeving en de beveiligingsnorm voor de procesautomatisering. Deze zijn door de sector opgesteld, door TNO positief beoordeeld en moet door de minister van Infrastructuur en Waterstaat worden goedgekeurd.

Doel

Het doel van dit project is onderzoeken of een geharmoniseerde standaard voor ICS binnen de afspraken van het BAW+ van toegevoegde waarde is. Daarbij moet worden aangetekend dat vanaf 1 januari 2019 de Baseline Informatiebeveiliging Overheid (BIO) van kracht is. De BIO vervangt de bestaande baselines (zoals BIG, BIR, IBI en BIWA) voor het Rijk, gemeenten (VNG), waterschappen en provincies. Hiermee ontstaat één basisniveau voor informatiebeveiliging binnen de gehele overheid. De BIO is dus niet van toepassing voor de waterleidingbedrijven. Het normenkader is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002), aangevuld met specifieke maatregelen en heeft risicomanagement als uitgangspunt.

Voor de cybersecurity van ICS-omgevingen voldoet de BIO niet geheel; de BIO is een generiek normenkader dat in principe voor elk vraagstuk onvoldoende specifiek is. De baseline biedt een goede basis, maar aan de hand van risicomanagement moeten de precieze ICS-maatregelen ingevuld worden. Cybersecurity van ICS heeft namelijk te maken met specifieke problematiek. Wat deze problematiek inhoudt, wordt eerst beschreven. Vervolgens wordt de bestaande wet- en regelgeving toegelicht. Daarna volgt een beschrijving van de onderzoeksaanpak en als laatste de analyse met de beantwoording van de onderzoeksvragen.

Naamgeving

Binnen de gehele waterketen wordt veel gebruik gemaakt van de termen ICS en SCADA-systemen (Supervisory Control And Data Acquisition). Dit zijn meet- en regelsystemen die voor de primaire aansturing van vitale processen binnen deze keten worden ingezet. ICS staat voor Industrial Control Systems ofwel industriële controlesystemen. SCADA-systemen zijn de systemen die de meetgegevens uitwisselen. Hiernaast worden ook termen als IACS (Industrial Automation and Control Systems), Operationele Techniek (OT), Procesautomatisering (PA) of Cyber-Physical Systems gehanteerd. De termen zijn inhoudelijk niet volledig hetzelfde, maar wel vergelijkbaar. Voor het gemak wordt in dit document de verzamelnaam ICS gebruikt.

2. Wet- en regelgeving

Cybersecurity van ICS kent een specifieke problematiek ten opzichte van kantoorautomatiserings-omgevingen. Waar het bij ICS veelal gaat om fysieke processen, gaat kantoorautomatisering meer over administratieve processen. De risico's moeten dan ook anders worden ingeschat. Een cyberincident in een organisatie waar veel ICS wordt gebruikt, kan al snel een grote impact hebben. De kans dat er een incident plaatsvindt, neemt toe. Daarnaast zijn er bij ICS andere technische uitdagingen van toepassing. Dit zal verder toegelicht worden.

1.1 Risico's

Het dreigingslandschap binnen de fysiek aangestuurde ketens, zoals de waterketen waarin ICS wordt toegepast, heeft zich anders ontwikkeld in vergelijking met traditionele IT-systemen. Zie bijvoorbeeld een citaat uit het rapport 'Digitale dijkverzwaring: Cybersecurity en vitale waterwerken' van de Algemene Rekenkamer (maart 2019)[4]: "*ICS-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. 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.*"

Ook de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) beschrijft in zijn meest recente jaarverslag dat digitale sabotage van vitale infrastructuur in Europa steeds vaker voorkomt. De kwetsbaarheid van ICS voor cybercriminaliteit of sabotage lijkt dan ook toegenomen. Het 'Cyber Security Beeld 2020' van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), en het Nationaal Cyber Security Centrum (NCSC)[5] stelt dat er een compleet en scherp beeld ontbreekt van de digitale weerbaarheid van Nederlandse vitale processen. Ook beschrijft dit rapport dat de eerste specifiek op ICS gerichte ramsomware in 2020 is gesignaleerd, het werk van een criminele actor. De impact van dergelijke incidenten kan verstrekkende gevolgen hebben voor de gehele maatschappij. "*Statelijke actoren hebben in het verleden meermaals laten zien over de capaciteit en intentie te beschikken om digitale aanvallen uit te voeren op de vitale infrastructuur of toeleveranciers van (ICS-)systemen die daarin worden gebruikt.*"

1.2 Technische uitdagingen

Naast de toegenomen risico's zijn er uitdagingen op technisch vlak. De gemiddelde levensduur van ICS is 15 tot 20 jaar, terwijl traditionele ICT-systemen 3 tot 5 jaar mee gaan. Hierdoor zijn de huidige ICT-systemen al veel meer aangepast op de mogelijkheden en dreigingen die het internet kan bieden. Ook houden de huidige systemen meer rekening met cybersecurity, denk aan security by design. Bij ICS heeft de aandacht voor cybersecurity-maatregelen zich pas het afgelopen decennium sterk ontwikkeld.

Ook het gebruik van de generieke ICT-middelen binnen ICS-omgevingen levert risico's op. Deze zijn in de loop der jaren meer gekoppeld aan computernetwerken om onder andere bediening op afstand mogelijk te maken. Door deze directe of indirecte aansluiting op het internet, staan ICS ook steeds meer bloot aan dezelfde dreigingen als reguliere ICT-systemen. Waar bij reguliere ICT-systemen beschikbaarheid niet altijd als het grootste probleem wordt gezien, is dat bij ICS juist wel zo. Indien een vitaal proces uitvalt, kan dit direct een maatschappelijk effect hebben, of het nu gaat om drinkwatervoorzieningen, gemalen, bruggen of sluizen. Deze afhankelijkheid van beschikbaarheid heeft ook gevolgen voor onderhoudsprocessen. Een ICS-omgeving kan niet zomaar stil gelegd worden om een nieuwe patch toe te passen, omdat het een complexe legacy omgeving betreft. Dit geeft meer problematiek dan bij kantoorautomatisering. Men is dus minder snel geneigd om grote wijzigingen in de systemen aan te brengen. Het hoge risico dat er dan iets niet meer juist functioneert, maakt dat patchen niet vanzelfsprekend is. Organisaties maken daarom vaak een expliciete risico-afweging tussen het patchen van hun legacy systemen en de kans dat hun vitale proces langere tijd stil kan liggen doordat de patch niet functioneert als beoogd.

Als laatste moet niet onderschat worden dat procesautomatisering specifieke expertise vereist. Experts zijn schaars en vaak op een andere technisch vlak geschoold, omdat het gaat om meet- en regelsystemen. In opdracht van het NCSC is door TNO in 2019 onderzocht wat organisatorische succesfactoren zijn voor het inbedden van OT-cybersecurity[6]. Dit onderzoek maakt duidelijk welke specifieke cybersecurity-problematiek van toepassing is in organisaties die veel ICS gebruiken en welke factoren het meeste succes opleveren bij het borgen van een goede cybersecurity.

[4] https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken

[5] https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020, pagina 16 en 19

[6] https://www.ncsc.nl/documenten/publicaties/2019/november/26/onderzoek-ics-tno

3. Analyse

ICS en vitale processen krijgen ook steeds meer bestuurlijke aandacht. Dit blijkt onder andere ook uit het feit dat er inmiddels cybersecurity-regelgeving is gemaakt voor organisaties met maatschappelijk relevante vitale processen:

- **Wet beveiliging netwerk- en informatiesystemen (Wbni)**: per 9 november 2018 geldt de Wbni. Deze wet streeft naar de digitale weerbaarheid van Nederland te vergroten. In het bijzonder van aanbieders van essentiële diensten (AED's) en andere aangewezen vitale aanbieders (AAVA's[7]), Rijksoverheid en digitale dienstverleners. De wet is erop gericht de gevolgen van cyberincidenten bij die groepen te beperken en zo ook maatschappelijke ontwrichting te voorkomen. Dat doet de wet door AED's te verplichten maatregelen te nemen om hun ICT te beveiligen tegen incidenten (de zogenoemde zorgplicht). Voor inbreuken en incidenten met (potentieel) significante gevolgen voor de continuïteit van de dienstverlening geldt bovendien een meldplicht voor vitale aanbieders bij het NCSC. AED's melden ook bij de sectorale toezichthouder.
- **Besluit beveiliging netwerk- en informatiesystemen (Bbni)**: samen met de Wbni is ook het Bbni in werking getreden. Hierin worden onder meer de vitale aanbieders aangewezen die onder de reikwijdte vallen van de verplichtingen van de Wbni. Op dit moment ligt er een wijziging van de Bbni voor ter consultatie. Deze wijziging vult de aanwijzing aan van AED's en andere vitale aanbieders. Daarnaast stelt dit besluit, met behulp van een aparte bijlage, sector overstijgende nadere regels over de door AED's te nemen beveiligingsmaatregelen (uitwerking van artikelen 7 en 8 Wbni). De vakminister kan bij Ministeriele Regeling nadere regels stellen over de zorgplicht.

In april 2020 heeft de CSR (Cyber Security Raad)[8] een advies uitgebracht over de digitale veiligheid van Industrial Automation en Control Systems (IACS). Volgens dit rapport is er beperkt inzicht in de risico's en afhankelijkheden tussen overheid en bedrijfsleven in de verschillende vitale sectoren. Ook is er onvoldoende voorbereid op de gevolgen van IACS. De CSR adviseert om over sectorale IACS-controleraamwerken te beschikken. Hierop zou de (sectorale) toezichthouder kunnen toetsen en reflecteren, zodat er een continue verbetercyclus ontstaat. Hiermee kan het toezicht binnen de wettelijke kaders van de Wbni een actieve invulling krijgen.

[7] AAVA's hebben alleen een meldplicht

[8] https://www.cybersecurityraad.nl/010_Actueel/cyberweerbaarheid-iacs-in-nederland-onvoldoende-op-orde.aspx

Sector	Standards	Good practices
Drinking water supply and distribution	• ISO 27001 Information technology - Security techniques - Information security maganement systems - requirements • ANSI/ISA, series 'ISA-62442: security for industrial automation and control system'	• ANSI/AWWA G430-09/'Security practices for operations and management

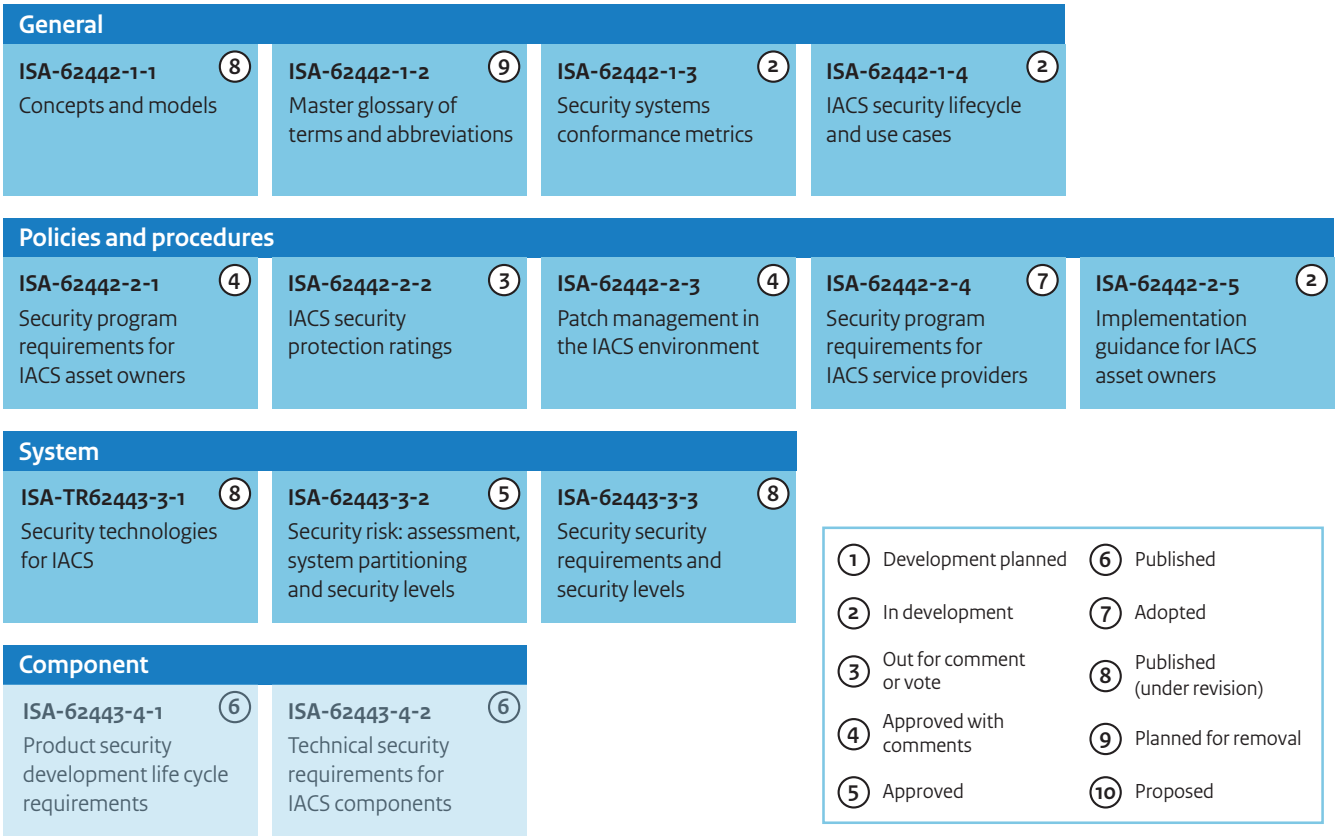
International standards and good practices specific to the drinking water supply and distribution sector

3.1 Doel en onderzoeksvragen

Het doel van dit onderzoek is het doen van een haalbaarheidsstudie naar een mogelijke gemeenschappelijke ICS-standaard(norm) voor de waterketenpartners die aangesloten zijn bij het BAW. Dit levert een bijdrage aan de verdere invoering van het basisniveau informatiebeveiliging (baselines) en concretiseert aanvullende eisen voor procesautomatisering.

Om deze haalbaarheid in kaart te brengen worden de volgende onderzoeksvragen beantwoord:

1. Is het mogelijk en wenselijk voor alle BAW-ketenpartners om te komen tot een gemeenschappelijke standaard voor ICS Cybersecurity binnen de waterketen?
2. a. Zo ja: hoe zou deze eruit kunnen zien? Rekening houdend met de reeds ontwikkelde of spoedig op te leveren normensets in de waterketen en best practices in het internationale ICS-werkveld.
   b. Op welke manier kunnen apart ontwikkelde normensets toch bijdragen aan een uniform minimum beveiligingsniveau? Wat zijn hierin de gemeenschappelijke elementen en de gaps (fit/gap analyse)?
3. Welke globale cybersecuritynormen in het ICS-domein kunnen een rol spelen bij de harmonisatie?
4. Voor welke andere systemen/processen/sectoren zou een



Overzicht 62443 onderdelen (bron: ISA.org/ISA99)

dergelijke gemeenschappelijke standaard of gemeenschappelijke elementen van toegevoegde waarde kunnen zijn?

Aanpak
Om de onderzoeksvragen te kunnen beantwoorden, zijn de volgende vier stappen doorlopen:

SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means
SL3	Protection against intentional violation using sophisticated means
SL4	Protection against intentional violation using sophisticated means with extended resources

1. *Documentenonderzoek*
In dit documentenonderzoek is de gemeenschappelijke basis van de nu gebruikte normen binnen de waterketen geanalyseerd. Het betreft:
- De algemene normenset van de BIO;
- De richtlijn met maatregelen die is opgesteld door Rijkswaterstaat; de CyberSecurity Implementatierichtlijn objecten Rijkswater (CSIR). Deze norm, versie 1.4, dateert van 4 augustus 2015. In Q3 2020 wordt een update verwacht. Helaas is deze update niet gereed bij afronding van dit onderzoek;
- De vertaling van zowel de BIO als de CSIR in het stappenplan implementatie BIO IA voor decentrale overheden. Dit stappenplan is opgesteld door het kennisplatform CROW, als onderdeel van het programma iCentrale.

Naast deze kaders is er een PA-beveiligingsnorm opgesteld door de drinkwatersector in 2018. Deze bevat beheersmaatregelen geselecteerd op basis van een risicoanalyse. Dit is (tezamen met de eisen uit de Drinkwaterwet- en besluit) de sectorale basis voor invulling van de zorgplicht uit de Wbni door de tien drinkwaterbedrijven. De norm is destijds positief getoetst door TNO. Vewin, de Vereniging van waterbedrijven in Nederland, heeft aangegeven dat dit een vertrouwelijk document is. Daarnaast heeft Vewin aangegeven geen onderdeel te zijn van de afspraak om te komen tot een gemeenschappelijk kader voor procesautomatisering. Om toch te kunnen leren van de ervaringen die zijn opgedaan in het komen tot deze uitvoeringsnorm, is er een presentatie gegeven om uit te leggen hoe de norm tot stand is gekomen en wat de ervaringen en geleerde lessen zijn tot nu toe. Waar deze ervaringen en lessons learned relevant en niet vertrouwelijk zijn, worden deze ervaringen wel meegenomen in dit onderzoek.

2. *Interviews*
Met 6 medewerkers, werkzaam bij een ketenpartner die onderdeel is van de waterketen, zijn interviews uitgevoerd. Vragen voor deze interviews zijn opgesteld op basis van het documentenonderzoek.

3. *Fit/gap*
Op basis van de eerste twee stappen is er een fit/gap zichtbaar geworden. Deze is gebruikt om een aantal stellingen te formuleren die voorgelegd zijn in een 'expert- workshop'. Voor iedere groep van betrokkenen in het BAW (provincie, gemeente, Rijkswaterstaat en waterschappen) is er een expert aangeschoven. Deze workshop is voorafgegaan door de hiervoor genoemde presentatie van de PA-beveiligingsnorm van de drinkwatersector. In totaal hebben 13 experts meegedaan aan deze workshop. Doel was om te komen tot een gemeenschappelijke visie en mogelijke beantwoording van de hoofdvraag.

4. *Afstemmings-sessie*
Uit de eerste drie stappen bleek dat er veel samenhang is met de BIO. Hierdoor ontstond de behoefte om ook een afstemmings-sessie te beleggen met de BIO-werkgroep. Deze wordt voorgezeten door het ministerie van BZK. Uitgelegd is het doel van het onderzoek en specifiek de fit/gaps die te maken hebben met de aansluiting bij de BIO. Dit heeft weer geleid tot waardevolle aanvullende inzichten die in deze rapportage zijn verwerkt.

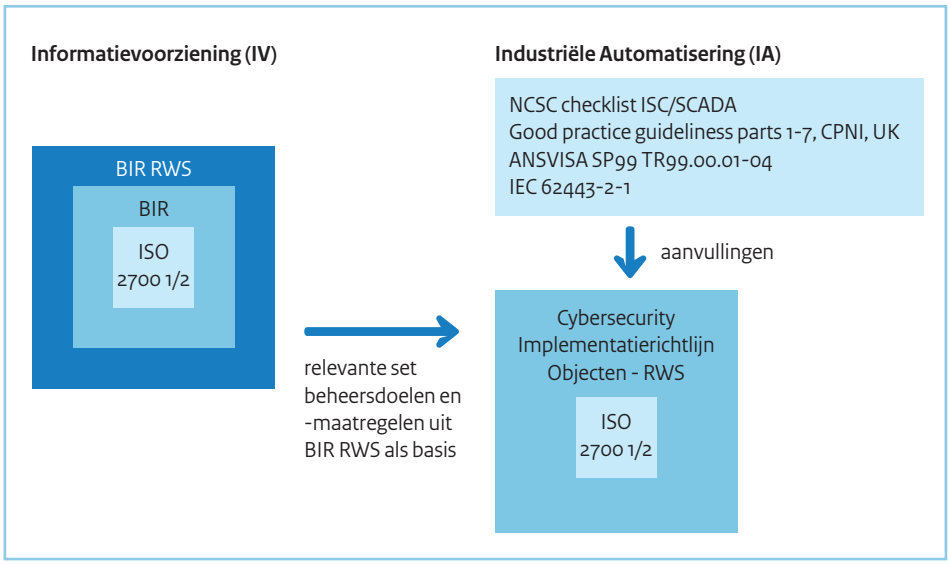
3.2 Normenanalyse
In deze paragraaf is uiteengezet welke raamwerken of normenkaders er in gebruik zijn voor ICS en dan specifiek voor de watersector. Eerst wordt dit vanuit internationaal perspectief beschreven, daarna wordt in detail beschreven wat er in gebruik is bij de ketenpartners van het BAW.

3.2.1 Internationale normen
Uit een publicatie van ENISA is gebleken dat, volgens de Europese drinkwaterbedrijven[9], de meest gebruikte standaarden voor de sector de ISO27001 en de ISA/IEC 62443 zijn. De ISO27001 is grotendeels vertaald naar maatregelen voor de overheid in de BIO en generiek van aard, de ISA/IEC 62443 is specifiek voor I(A)CS.
Uit dit overzicht blijkt ook dat de AWWA (American Waterworks Association) een set van security practises heeft die van toegevoegde waarde kunnen zijn. Ook al wordt specifiek gesproken over drinkwaterbedrijven, we gaan er hieronder vanuit dat deze normen relevant kunnen zijn voor alle vitale processen die binnen de waterketen van het BAW vallen. Hieronder worden deze standaarden, samen met de NIST-800-82 waarvan bekend is dat deze ook veel gebruikt wordt, toegelicht. In de fit/gap analyse hierna wordt geanalyseerd welke normen precies in welke mate gebruikt worden door de BAW keten-partners.

ISA/IEC 62443

[9] https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/

De ISA/IEC 62443 is een raamwerk dat meer dan 10 jaar geleden is ontwikkeld. De ISA/IEC 62443-reeks (vanaf nu: IEC 62443) is ontwikkeld door de ISA99-commissie en goedgekeurd door de International Electrotechnical Commission (IEC) in de Verenigde Staten. Dit uitgebreide raamwerk is niet openbaar beschikbaar en bestaat uit een aantal categorieën: “General, Policies and Procedures, System, and Component” (zie de tabel hieronder). Een aantal onderdelen binnen deze categorieën is nog in ontwikkeling.



Structuur CSIR
Bron: CSIR Versie 1.4

Ketenpartner	Algemene normen		Maatwerk normen		Internationale normen (eventueel verwerkt in maatwerknorm)		
	BIO	ISO27000-serie	PA-beveiligingsnorm	CSIR	IEC 62443	NIST-800-82	AWWA Good practises
Gemeenten	+	+	-	*o*	*o*	-	-
Provincies	+	+	-	+	*o*	-	-
Waterschappen	+	+	-	+	+	*o*	-
Rijkswaterstaat	+	+	-	+	+	*o*	-
Drinkwaterbedrijven	*nvt*	+	+	-	+	+	-

Gebruikte normen bij BAW ketenpartners

Legenda:
+ wordt veel gebruikt
o wordt af en toe of deels gebruikt
- wordt (nagenoeg) niet gebruikt

De IEC 62443 gaat uit van een aantal securitylevels. Afhankelijk van het securitylevel dat benodigd is, kunnen de bijbehorende maatregelen geselecteerd worden.

Als eerste organisatie in de watersector in Nederland heeft het hoogheemraadschap van Rijnland in 2020 een aantal operationele systemen gecertificeerd conform de IEC 62443.

NIST-800-82

De NIST-800-82 is een "Guide to ICS Security", opgesteld door het National Institute of Standards and Technology in de Verenigde Staten. Het adresseert globaal de volgende onderwerpen:

- Risicobeheer en de beoordeling van ICS;
- De ontwikkeling en implementatie van een ICS-beveiligingsprogramma;
- Aanbevelingen voor het integreren van beveiliging in netwerkarchitecturen die doorgaans voorkomen in ICS, met de nadruk op netwerksegregatie;
- Samenvatting van de beheer-, operationele en technische controles.

Omdat het een "guide" is, heeft dit document een iets ander karakter dan bijvoorbeeld de IEC 62443. Het is breder georiënteerd, openbaar en voldoet ook als naslagwerk.

Water Sector Cybersecurity Risk Management Guide

Hoewel het niet een op zichzelf staand raamwerk of normenkader is, is het de moeite waard om deze Water Sector Cybersecurity Risk Management Guide te noemen. Deze guide is speciaal ontwikkeld voor de watersector in de Verenigde Staten (American Waterworks Association-AWWA). In de eerdergenoemde studie van ENISA wordt verwezen naar deze good practice.

Deze AWWA Cybersecurity Risk Management Guidance (AWWA Guidance) en bijbehorende AWWA Cybersecurity Assessment Tool (AWWA Assessment Tool), is een sectorspecifieke aanpak voor de toepassing van het NIST Cybersecurity Framework. Het oorspronkelijke doel van deze AWWA-leidraad was om eigenaren/exploitanten van waterbedrijven een consistent en herhaalbare beoordelingstool en aanbevolen richtlijnen te bieden om de kwetsbaarheden voor cyberaanvallen te verminderen.

Conclusie

Een panel van materiedeskundigen identificeerde de meest urgente cyberveiligheidsproblemen waarmee waterbedrijven vandaag de dag worden geconfronteerd. Op basis van deze risicoanalyse zijn deze cybersecurityrichtlijnen ontwikkeld. Deze beschrijven de maatregelen die als het meest kritisch worden beschouwd voor het verkleinen van cyberrisico's in de watersector. Het betreft een set van 99 maatregelen voor Cybersecurity die zodanig zijn georganiseerd dat de implementatie is gekoppeld aan uitvoerbare taken.

Elke maatregel heeft een prioriteitsniveau toegewezen gekregen, onderverdeeld in prioriteiten 1, 2, 3 en 4, waarbij prioriteit 1 de hoogste is. Dit zijn de basismaatregelen die het minimale beveiligingsniveau weergeven. Prioriteit 4 maatregelen zijn complexer en bedoeld om ook bescherming te geven tegen meer geavanceerde aanvalstechnieken. De management guide is openbaar[10].

3.2.2 Zelf ontwikkelde normenkaders bij de BAW-ketenpartners

Nu duidelijk is welke internationale normen het meest gangbaar zijn, is het relevant om te analyseren welke van deze internationale normen binnen de BAW-ketenpartners worden toegepast in een eventueel zelf samengestelde norm.

PA-beveiligingsnorm voor de drinkwatersector

Zoals eerdergenoemd heeft Vewin aangegeven dat zij geen onderdeel zijn van de afspraak om te komen tot een gemeenschappelijk kader voor procesautomatisering. Daarnaast is de inhoud van de door henzelf samengestelde norm en het rapportage sjabloon vertrouwelijk. In dit document zal dan ook niet de inhoud van de beheersmaatregelen benoemd worden. Wel is het van toegevoegde waarde om de informatie over de opzet en totstandkoming van deze norm te beschrijven. Dit kan immers helpen om te bepalen of er gemeenschappelijke elementen te ontdekken zijn over de raamwerken heen.

De PA-beveiligingsnorm bestaat grotendeels uit maatregelen uit de ISO27001. Daarnaast zijn er aanvullende normen geselecteerd. Het raamwerk is tot stand gekomen op basis van een risicoanalyse om vooral díe risico's te beheersen die als kritiek beschouwd worden.

Bij het uitwerken en beschrijven van de ISO27001 maatregelen is een koppeling gemaakt met de technische maatregelen uit de NIST SP 800-82:2015 en de IEC 62443:2013. Aan de hand van een risico-acceptatie mag er (beargumenteerd) deels van afgeweken worden. Er is hiermee direct inzichtelijk welke relatie er is tussen de ISO27001, NIST en IEC normen. Eénmaal per 4 jaar vindt een externe audit plaats naar de PA-norm, de resultaten worden bij het leveringsplan gevoegd en aan de toezichthouder voorgelegd.

De Cybersecurity Implementatie Richtlijn Objecten van Rijkswaterstaat

Rijkswaterstaat heeft op het gebied van informatiebeveiliging voor industriële automatisering met de Cyber Security Implementatie Richtlijn (CSIR) een praktische invulling van de BIR, de voorloper van de BIO, voor industriële automatisering uitgewerkt. Rijkswaterstaat past deze al een aantal jaren in de praktijk toe. Deze aanpak is generiek van opzet en daardoor ook bruikbaar voor andere overheden. Om de cybersecurityaanpak van Rijkswaterstaat ook toepasbaar en praktisch werkbaar te maken voor gemeenten en provincies, is door het CROW (kennnisplatform) een aanvullende handreiking gemaakt op basis van deze CSIR[11] en de BIO, het huidige basisniveau voor informatiebeveiliging binnen de gehele overheid. Deze handreiking van CROW helpt om de CSIR te implementeren in samenhang met de BIO, hiermee wordt niet automatisch voldaan aan de BIO. Deze handreiking met hierin opgenomen de CSIR is openbaar.

De huidige CSIR-versie is versie 1.4. Deze dateert uit augustus 2015. Er is op dit moment een grote wijziging voorzien. Deze moet voor het einde van 2020 gerealiseerd zijn. Deze versie zal verder in lijn worden gebracht met de huidige BIO. Omdat nog niet geheel duidelijk is hoe deze nieuwe versie samengesteld zal zijn, wordt beschreven hoe de 1.4 versie is opgebouwd. Volgens Rijkswaterstaat is het waarschijnlijk dat de structuur van de nieuwe versie in grote lijnen hetzelfde blijft.

De CSIR is ooit tot stand gekomen omdat bij de uitvoeringstaken van Rijkswaterstaat veel inzet van ICS-systemen nodig is. Deze zijn van zo'n belangrijke aard dat extra eisen en maatregelen nodig bleken naast de toen geldende BIR om zo beveiligingsrisico's in het eigen werkveld te kunnen mitigeren. Deze samenhang is door Rijkswaterstaat in onderstaand schema weergegeven. Ook hier is de ISO27001/2 de basis met daarop aanvullingen vanuit onder andere de NIST SP800-82 en de IEC 62443. Daarnaast is nog de checklist van het NCSC en de Good Practise guidelines van het CPNI (Center for the Protection of National Infrastructure) van het Verenigd Koninkrijk gehanteerd.
De CSIR werkt met een zogenaamde cyber-classificatie die leidt tot een cybersecurity weerstandsniveau. Voor een object met een weerstandniveau 4 wordt een zwaarder maatregelpakket voorgeschreven dan voor een object met een weerstandsniveau 3. De maatregelen zijn ingedeeld naar categorie, zoals logische toegang, fysieke toegang, logging en monitoring etc. Daarnaast wordt een onderscheid gemaakt in het type maatregelen: mens, procedures en organisatie en techniek.

De huidige versie van de CSIR is mede gericht op de Opdrachtgever-Opdrachtnemer relatie. Dit omdat Rijkswaterstaat veel werkt met aannemers die onderhoud of

[10] https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960

[11] https://www.crow.nl/downloads/pdf/verkeer-en-vervoer/verkeersmanagement/verkeersregelinstallaties/stappenplan-implementatie-bio-ia_web.aspx

Infographic CSBN 2020

implementaties doen op objecten. Veel aannemers zijn daarom ook bekend met de CSIR. Er is veel overleg en samenwerking met de waterschappen in de PA-werkgroep. Hier wordt onder andere over de toepassing van de CSIR gesproken. De waterschappen hebben recentelijk een "nulmeting" uitgevoerd. Een subwerkgroep die met objectclassificatie bezig is, gaat de review doen op de nieuwe versie van de CSIR. Ook is de CSIR in het vizier bij een aantal provincies en wordt daar ook (deels) toegepast. De huidige CSIR heeft dus een hoge adoptiegraad.

3.2.3. Fit/Gap analyse

Om een beeld te krijgen van de raamwerken of normen die de grootste "fit" hebben en te kunnen bepalen of harmonisatie mogelijk is, is in de tabel op de volgende pagina een vergelijking gemaakt van het gebruik van de normen binnen de waterketenpartners.
In het algemeen is de BIO/ ISO27000 serie voor veel organisaties nog de basis van Cybersecurity in ICS-omgevingen, aangevuld met de IEC 62443 en de NIST-800-82.

Daarnaast zijn er de twee maatwerk normenkaders die gebruikt worden; de PA-beveiligingsnorm en de CSIR.

- De gemeenten gebruiken grotendeels de BIO nog als raamwerk voor ICS-security. Enkele gemeenten oriënteren zich op het gebruik van de CSIR, anderen kijken hierbij ook naar de IEC 62443.

Deze brochure is een uitgave van:

Ministerie van Infrastructuur en Waterstaat
Postbus 20901 | 2500 EX Den Haag
T 070 456 00 00

November 2020