De beveiliging van SCADA systemen binnen waterschappen

Gerrald van Oene

Titel:	De beveiliging van SCADA systemen binnen waterschappen
Auteur:	Gerrald van Oene
Eerste beoordelaar:	Dhr. G.H. Melching
Tweede beoordelaar:	Mevr. A. Bastiaansen
Praktijkbegeleider:	Dhr. P. Westerveld
Datum:	4 april 2016
Plaats:	Deventer
Opleiding:	Integrale veiligheidskunde, Saxion Hogeschool

Inhoudsopgave

Inleidende begrippenlijst

Inleiding

Hieronder ziet u de inleidende begrippenlijst voor het onderzoek naar de mogelijkheid tot het opstellen van een uniform analysemodel voor de beveiliging van SCADA systemen binnen waterschappen. In het onderzoek kunnen begrippen voorkomen waar niet iedereen al eerder van gehoord heeft. De begrippenlijst biedt een overzicht van termen die niet voor iedereen bekend zijn. Dit geeft de lezer inzicht in de specialistische kennis die nodig is om de informatie in dit onderzoek te begrijpen.

Begrippenlijst

Computervirus: Een computervirus is een computerprogrammatje dat zichzelf kan verspreiden en de computer waar hij zich op bevindt kan aanpassen. Vaak met negatieve bedoelingen. Een virus kan zich verspreiden door middel van internet en het kan verstopt zitten in andere bestanden, downloads en websites. (Microsoft, 2016)

Cybersecurity: Om duidelijk te kunnen stellen wat wel en niet als cybersecurity aangeduid kan worden zal de definitie van de Nationaal Coördinator Terrorisme en Veiligheid worden gebruikt. Deze definitie luidt: “Cyber security is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT (informatie en communicatie technologie) of door misbruik van ICT” (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2015). Met deze definitie wordt duidelijk gemaakt dat de mate van veiligheid afhangt van de mogelijkheid tot het aanrichten van gevaar of schade door middel van ICT.
Beschikbaarheid, integriteit en vertrouwelijkheid van systemen of aantasting van de vertrouwelijkheid van informatie vormen de factoren waardoor binnen de ICT onveiligheid kan ontstaan.

- Beschikbaarheid gaat om de tijd waarin data bereikbaar is.
- Integriteit geeft aan hoe correct en betrouwbaar de data is.
- Vertrouwelijkheid geeft aan dat alleen bepaalde personen de data mogen bereiken. (Taskforce Bestuur & Informatieveiligheid Dienstverlening, 2014)

Hacking: Het gebruik maken van, aanpassen van of toegang tot verkrijgen tot een systeem waarvan het niet de bedoeling is dat het systeem op die manier bereikt en gebruikt wordt. (Mashable, 2016)

IT: Information Technology. Hiermee wordt alles bedoeld dat te maken heeft met computers en netwerken. Hierbij valt te denken aan het beheer van computers, servers en software. In veel organisaties heeft IT een eigen plek gekregen en is het onderdeel van de organisatie. (TechTerms, 2016)

Netwerk: Met een netwerk wordt een verzameling computers bedoeld die aan elkaar gekoppeld zijn door middel van werkstations, servers, routers en software. Binnen bedrijven en organisaties waar meerdere apparaten tegelijk gebruikt moeten worden wordt gebruik gemaakt van netwerken. (NLDIT Computer Kennis, 2016)

PLC’s/RTU’s: Programmable Logic Controllers en Remote Terminal Units worden binnen een SCADA netwerk gebruikt om opdrachten te verwerken en door te geven aan apparaten.

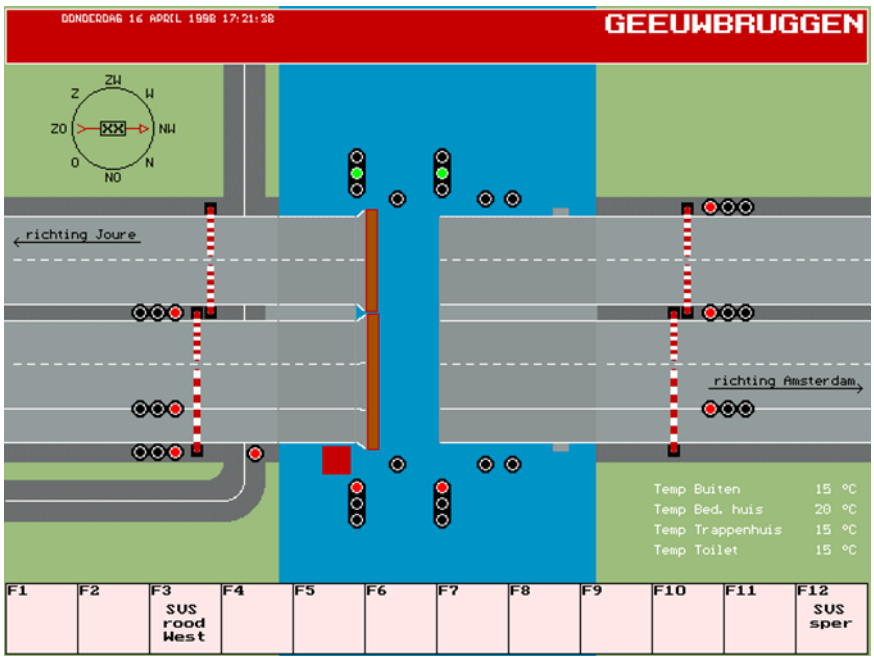
Het verschil tussen RTU's en PLC's is dat RTU's over langere afstanden gebruikt kunnen worden. (Soullié, Industrial Control Systems Pentesting PLCs 101, 2014)

Figuur 1: Nautische centrale in Zeeland (Controlroomdesign, 2015)

Security: Security is de mate waarin de organisatie, de processen, de techniek en de mensen beschermd zijn tegen opzettelijke en onopzettelijke dreigingen van personen binnen of buiten de organisatie en tegen dreigingen van groepen of andere organisaties. Een groot verschil tussen safety en security is de oorsprong van de onveiligheid, bij security heeft deze een menselijke oorsprong.

SCADA

SCADA, voluit Supervisory Control and Data Aquisition is een systeem waarmee verschillende mechanische processen worden aangestuurd. SCADA is onderdeel van de Industrial Control Systems binnen een productielijn (Taskforce Bestuur & Informatieveiligheid Dienstverlening, 2014). SCADA wordt gebruikt in productie, industrie, infrastructuur, de energie sector en soort gelijke toepassingen waarbij meerdere taken tegelijk of in serie moeten worden uitgevoerd. Het wordt gebruikt om systemen te monitoren of om de onderdelen binnen het systeem opdrachten te geven (Schellevis, 2012). SCADA en de Programable Logic Controllers die er op aangesloten zijn hebben voor organisaties een groot voordeel omdat ze aan te sluiten zijn op internet. Het voordeel hiervan is dat het niet nodig is dat er iemand fysiek aanwezig is op de locatie waar een bepaalde handeling uitgevoerd moet worden. Binnen de industrie kunnen meerdere processen worden aangestuurd door middel van een Human-Machine Interface (HMI). Hierdoor wordt informatie over verschillende processen binnen het systeem zichtbaar op één bedieningspaneel waar een persoon alles kan monitoren en aansturen. In de figuren hiernaast zijn de beeldweergaves van SCADA systemen zichtbaar.



Figuur 2: Human Interface Machine weergave van de Geeuwbruggen (Leiden Scientific B.V. Industriële automatisering)

Sensoren binnen de productielijn zorgen ervoor dat signalen zoals temperatuur, snelheid en druk worden gesignaleerd. Actuators kunnen juist opdrachten doorgeven aan de onderdelen van de productielijn. Het openzetten van ventielen en kleppen en het inschakelen van pompen zijn hier voorbeelden van. De sensoren en actuators worden aangestuurd door middel van Programmable Logic Controllers (PLC) of Remote Terminal Units (RTU). RTU's worden vaker gebruikt bij toepassingen op grotere afstanden en zijn voorzien van een eigen stroomtoevoer. Ook maken RTU's vaker gebruik van draadloze communicatie. PLC's bevinden zich vaker binnen bedrijven en inrichtingen. PLC's en RTU's staan in verbinding met een Human Machine Interface (HMI) (Leverett, 2011). Op de HMI kan het bedienend personeel zien wat er op het moment gebeurt binnen de productielijn. De informatie van de RTU's en PLC's wordt niet alleen weer gegeven op de HMI, maar ook opgeslagen op een data historian. De data historian is een computer die de data uit het systeem opslaat. (Soullié, Industrial Control Systems Pentesting PLCs 101, 2014)

Uniform analysemodel: In de probleemstelling wordt gesproken over een uniform analysemodel. Als uniform analysemodel wordt een analysemodel bedoeld dat vaker toepasbaar is op meerdere gelijksoortige casussen. Door het opstellen van een uniform analysemodel wordt het mogelijk om de analyse van de beveiliging van SCADA systemen op een gestandaardiseerde wijze aan te pakken. Dit betekent dat er bij verschillende casussen gebruik gemaakt kan worden van één en dezelfde aanpak die er op toeziet dat het onderzoek op dezelfde wijze wordt uitgevoerd.
Een groot voordeel hiervan is dat er van te voren duidelijk is welke stappen doorlopen moeten worden om te komen tot een duidelijke conclusie en een serie aanbevelingen.
Na het doorlopen van de aanbevelingen uit het analysemodel kan bijvoorbeeld de conclusie getrokken worden dat het nodig is dat er aanvullende maatregelen getroffen worden. Op basis van die conclusie kunnen vervolgens maatregelen worden geformuleerd die er op toezien dat de beveiliging van het systeem verbetert.

Hoofdstuk 1: Inleiding

1.1 Aanleiding

Veiligheidsvraagstukken blijven verschuiven en veranderen. Dat geldt ook voor de continue veranderende omgeving van cybersecurity. Criminelen, fraudeurs en andere kwaadwillenden zullen altijd nieuwe manieren zoeken om veiligheidsmaatregelen te omzeilen. Ook kan personeel onbedoeld fouten maken. Omdat steeds meer personen, bedrijven en organisaties verbonden zijn met het internet verplaatst ook veiligheid en onveiligheid zich naar cyberspace. “The Internet of Things” speelt hierbij een grote rol. The Internet of Things verwijst volgens Kevin Ashton naar een situatie waarin informatie kan worden verzameld door het internet zelf. Dit betekent dat het internet sensoren krijgt waardoor het in staat is om zelf informatie te verzamelen. (Ashton, 2009)
Toen Ashton deze uitspraak voor het eerst deed was dit nog niet zo. Toen was de mens de sensor van het internet en voerde de mens zelf informatie in.
Het gevolg van dit fenomeen is dat het internet steeds meer sensoren krijgt. Dit betekent ook dat het internet steeds verder reikt en er steeds meer apparaten online zijn en dus in verbinding met elkaar.

Dit brengt risico’s en gevaren met zich mee omdat deze apparaten niet alleen door andere apparaten bereikt kunnen worden, maar ook door personen. Door verbinding met het internet zijn apparaten en informatie beschikbaar, maar het gevaar hiervan is dat het gebruik minder exclusief kan worden. Dit betekent dat personen of organisaties bij informatie en systemen zouden kunnen komen waarvan dat niet de bedoeling is.

Ook apparaten die gebruikt worden bij waterschappen staat in verbinding met internet. Hier wordt vaak gebruik gemaakt van SCADA systemen [1]. In de praktijk is gebleken dat SCADA systemen kwetsbaar zijn voor cyberaanvallen. Er zijn meerdere voorbeelden bekend van systemen en installaties die door hacking of virussen zijn misbruikt of zelfs vernield.

Enkele voorbeelden van virussen zijn slammer worm en het bekendere Stuxnet.
De nucleaire energie centrale Davis-Besse in Ohio werd besmet met een slammer worm die in 2003 het Safety Parameter Display systeem van de Davis-Besse energie centrale onbruikbaar maakte (Leverett, 2011). Het Safety Parameter Display systeem zorgt ervoor dat data over de centrale wordt verzameld en weergegeven. Dit systeem kan geen opdrachten geven aan de energie centrale. (Instep, 2015)

Een bekender en meer destructief voorbeeld van een virus is Stuxnet. Stuxnet richtte in 2010 schade aan in Iraanse kerncentrales door centrifuges en drukventielen te overbelasten (Langner, 2013). Het ingenieuze aan Stuxnet is dat het de opdracht heeft om te zoeken naar centrifuges van de merken Vacon en Fararo Paya (Haes, 2010). Stuxnet is vervolgens in staat om het systeem te observeren en vervolgens fysiek te overbelasten zonder dat dit zichtbaar is op de Human-Machine Interface. Het is op dat moment dus niet mogelijk om te zien wat het systeem aan het doen is. Stuxnet heeft op die manier het Iraanse nucleaire programma vertraagd zonder dat uitsluitend kan worden bewezen wie de verantwoordelijke is.

[1] Zie inleidende begrippenlijst

Twee interessante aanvallen van hackers op SCADA systemen zijn het inschakelen van waterpompen door een ex medewerker in Maroochyshire in Australië en het per ongeluk gebruiken van op een SCADA aangesloten laptop voor het gebruik ervan in een game netwerk.
(Leverett, 2011)

Vrij recentelijk, op 21 december 2015, bleek dat Iraanse hackers het beheer van een dam in Washington over konden nemen. Dit gebeurde in 2013. (Chiacu, 2015)

Naast deze gevallen blijkt uit onderzoek van de Universiteit van Cambridge dat een groot aantal niet afgeschermde industriële en infrastructurele apparaten is te bereiken door middel van Shodan. De website Shodan is voor iedereen met internet gratis en legaal bereikbaar. (Leverett, 2011)
Het is duidelijk dat door de groei van The Internet of Things de mogelijkheden onbegrensd zijn en de risico's mogelijk ook.

Waterschappen zijn kwetsbare belangrijke instanties en zij hebben belangrijke taken waarvan de uitvoering van belang is voor de maatschappij. Het niet functioneren van bruggen is een bedreiging voor het verkeer en de scheepvaart. Daarnaast blijkt dat terroristische organisaties zoals IS en sympathisanten van IS zich ook steeds meer op internet bevinden.
Door deze actuele grote incidenten is het van belang dat adviseurs en waterschappen een middel krijgen om de mate van veiligheid van hun systemen beter te kunnen waarborgen.

1.2 Context

Het aansluiten van infrastructurele objecten aan internet levert risico's op. De systemen waar gebruik van gemaakt wordt zijn vaak oud en technische beveiligingsmaatregelen zijn daardoor vaak niet geïntegreerd. Ook is het zo dat dergelijke systemen niet worden gepatcht of onderhouden door de leveranciers. Onderhoud van dergelijke systemen is voor operators en werknemers vaak niet uit te voeren omdat zij hier niet voor opgeleid en getraind zijn. Zij zijn er enkel voor getraind om met het systeem te werken. Dit levert voor waterschappen problemen op.
Er is daardoor een vraag naar kennis en kunde van professionals die de beveiliging van SCADA kunnen begeleiden. Sincerus levert consultants die zich hier op kunnen focussen.

1.3 Betrokkenen en belanghebbenden

Belanghebbende: ***Sincerus Consultancy***
De opdracht is afkomstig van Sincerus Consultancy. Sincerus Consultancy adviseert organisaties op het gebied van informatiebeveiliging met als doel het creëren van veiligere omstandigheden voor (kwetsbare) informatie. Hierbij wordt er gelet op de technische factoren, organisatorische factoren, procesmatige factoren en menselijke factoren die kunnen leiden tot onveiligheid of kwetsbaarheid. Daarnaast levert Sincerus services om systemen "realtime" te kunnen monitoren en services om kwetsbaarheden op het gebied van informatiebeveiliging binnen bedrijven op te sporen. Het is voor Sincerus interessant om te kijken wat het kan betekenen voor organisaties die gebruik maken van SCADA systemen. De risico's en gevaren van SCADA systemen zijn relatief nieuw en onbekend binnen het cybersecurity vakgebied. Uitkomsten van dit onderzoek kunnen bruikbaar zijn voor Sincerus bij het formuleren en leveren van nieuwe producten en services aan een nieuwe groep belanghebbenden. Het analyseren van SCADA systemen kan makkelijker worden door middel van dit model.

Belanghebbende: ***Waterschappen***

Waterschappen zijn erg afhankelijk van SCADA systemen. SCADA zorgt er bij waterschappen voor dat meerdere bruggen, sluizen en pompen vanaf één locatie kunnen worden aangestuurd en gemonitord. De bouwwerken die worden aangestuurd door waterschappen worden aangemerkt als vitale infrastructuur. Dit betekent dat het uitvallen van deze bouwwerken maatschappelijke of economische ontwrichting kan veroorzaken. (NCTV, 2010)

Het aansluiten van SCADA systemen binnen waterschappen op internet levert andere risico's op dan voorheen. Het is daarom voor waterschappen van belang wat zij kunnen doen voor de beveiliging van hun systemen en welke kosten dit met zich mee brengt.

Belanghebbende: ***Ingelanden***

Waterschappen zijn verantwoordelijk voor het welzijn van grote groepen burgers. De burgers die profijt hebben van de bescherming van het waterschap en daarvoor belasting betalen worden de ingelanden genoemd. Het niet of in beperkte mate van beschikbaar zijn van de diensten van het waterschap kan grote gevolgen voor hen hebben. Het niet functioneren van bruggen leidt tot verkeersbelemmeringen op autowegen en vaarwegen. Wanneer sluizen niet werken heeft dit gevolgen voor de waterstand in een bepaald gebied, dit zijn enkele gevolgen voor ingelanden. Ingelanden hebben baat bij de werkzaamheden van waterschappen en dus bij de beveiliging van de SCADA apparatuur binnen die waterschappen.

Hoofdstuk 2: Probleemstelling

2.1 Doelstelling

Het uiteindelijke doel van dit onderzoek is het opstellen van een uniform analysemodel[2] dat gebruikt kan worden om de mate van beveiliging van de SCADA apparatuur binnen een waterschap te bepalen. Een uniform analysemodel is herhaalbaar en toepasbaar op meerdere gelijksoortige casussen. Het uniforme analysemodel moet zicht geven in de factoren die bijdragen aan de mate van beveiliging in relatie tot de risico's die SCADA omgevingen lopen.
Sincerus Consultancy kan dit uniforme analysemodel gebruiken om de beveiligingssituatie bij klanten te toetsen. Op basis van de uitkomsten van de analyse die met het model zijn uitgevoerd moet Sincerus Consultancy aanbevelingen kunnen doen die erop toezien dat de beveiliging van de SCADA omgeving verbeterd.

2.2 Probleemstelling

Om het doel zoals hierboven geformuleerd te behalen is er een probleemstelling opgesteld. Het is van belang dat die probleemstelling de kwaliteit en doelmatigheid van het onderzoek waarborgt. Daarom is de volgende probleemstelling opgesteld:

"Is het mogelijk om een uniform analysemodel op te stellen waarmee de mate van SCADA beveiliging kan worden aangetoond? Zo ja, uit welke onderdelen zou een uniform analysemodel waarmee de mate van beveiliging van SCADA systemen bij waterschappen kan worden aangetoond moeten bestaan?"

Het uniforme analysemodel moet een middel zijn om de beveiligingssituatie van een SCADA systeem te kunnen analyseren. Dit model moet meerdere keren toepasbaar zijn op verschillende gelijksoortige casussen. Het model richt zich op de factoren die SCADA beveiliging beïnvloeden en voorziet in maatregelen tegen risico's die voor SCADA apparatuur relevant zijn.

2.3 Onderzoeksvragen

Om de probleemstelling zoals die hierboven is geformuleerd te kunnen beantwoorden zijn de volgende onderzoeksvragen opgesteld:

- Welke risico's lopen waterschappen die gebruik maken van SCADA systemen?
- Welke maatregelen worden er voorgesteld door de operationele handreiking Taskforce Bestuur en Informatieveiligheid Dienstverlening en in de baseline informatiebeveiliging waterschappen?
- Hoe verhouden de vastgestelde middelen uit de operationele handreiking Taskforce Bestuur en Informatieveiligheid Dienstverlening en de baseline informatiebeveiliging waterschappen zich tot de vastgestelde bedreigingen?

[2] Zie inleidende begrippenlijst

Hoofdstuk 3: Theoretisch kader

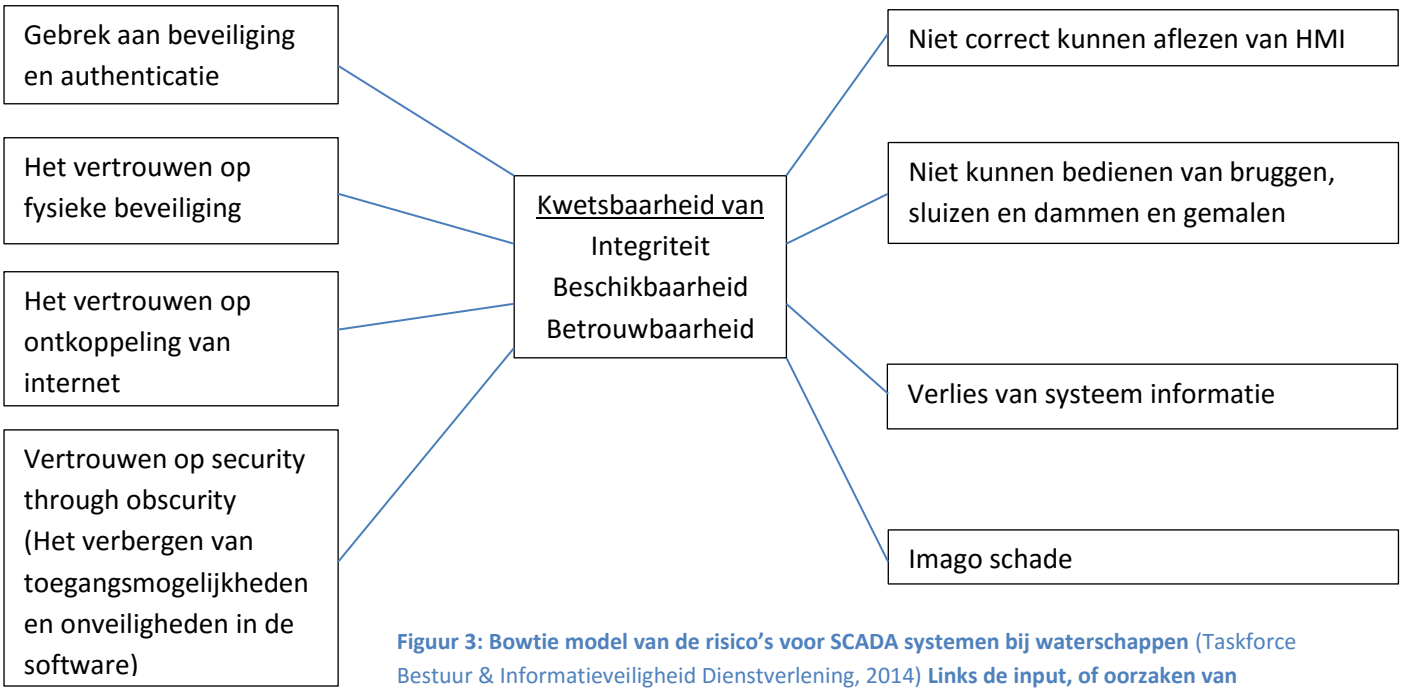
3.1 Theoretische ondersteuning

In dit hoofdstuk zullen de in het onderzoek gehanteerde theorieën worden besproken. Het is van belang dat duidelijk is omschreven welke stappen zijn gezet om te komen tot de conclusie zoals die is. Hiermee wordt de mogelijkheid tot het herhalen van het onderzoek bevorderd.

3.2 Worst case scenario thinking

"Worst case scenario thinking" gaat er vanuit dat er een situatie is die voorkomen moet worden. Er wordt daarom terug geredeneerd naar de oorzaken die die situatie kunnen veroorzaken. Door deze manier van redeneren is het beter mogelijk om een doelstelling te formuleren die te behalen is. Er wordt gericht gezocht naar oplossingen voor een al vastgesteld veiligheidsprobleem. Een gefocuste en doelgerichte aanpak van de problematiek is het gevolg. (Van Mil, Berenschot, Dijkzeul, & van der Pennen, 2006)

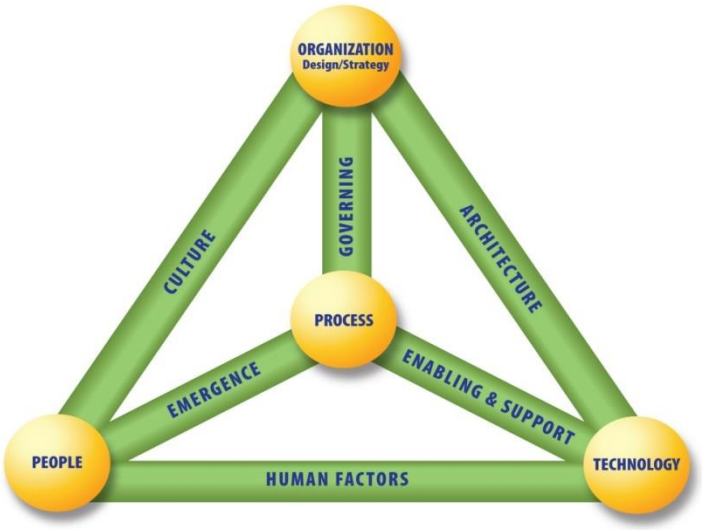
Het doel van dit onderzoek is het creëren van een analysekader op basis waarvan er aanbevelingen kunnen worden gedaan met betrekking tot de beveiliging van SCADA systemen. De systemen zullen moeten voldoen aan de criteria betrouwbaarheid, beschikbaarheid en vertrouwelijkheid. Deze situatie moet worden gehandhaafd en is dus de doelstelling. Het scenario dat moet worden voorkomen is in het geval van SCADA het beïnvloeden van het systeem door ongeautoriseerde personen of software, waardoor het systeem niet of in mindere mate doet wat het moet doen. Het niet functioneren van het systeem of het uitvoeren van onbedoelde handelingen door het systeem in dit geval de scenario's die voorkomen moeten worden. Er zal voor dit onderzoek dan ook gezocht worden naar mogelijke gevaren die dit scenario kunnen veroorzaken. Op basis daarvan is het mogelijk om aanbevelingen te doen die het optreden van de ongewenste situatie kunnen verminderen.



Figuur 3: Bowtie model van de risico's voor SCADA systemen bij waterschappen (Taskforce Bestuur & Informatieveiligheid Dienstverlening, 2014) **Links de input, of oorzaken van kwetsbaarheid. Rechts de gevolgen daarvan.**

3.3 Business Model For Information Security

Omdat security niet alleen afhankelijk is van technologie moeten ook de rollen en verantwoordelijkheden van de organisatie, processen en personen worden meegenomen. Deze verhoudingen zijn vastgelegd in het Business Model for Information Security. (ISACA, 2009)
Het model legt uit dat de basis voor informatiebeveiliging wordt gelegd door middel van vier factoren. De factoren kunnen volgens het model worden verbonden in een drie dimensionale vierzijdige piramide. De vier hoeken zijn organisatie, personen, processen en technologie.



Figuur 4: The business model for information security (ISACA, 2009)

Hieronder zal worden uitgelegd wat er verstaan moet worden onder de vier factoren.

- *Organisatie*
  De organisatie is de verzameling van mensen, middelen en processen binnen een netwerk die door middel van samenwerking een gemeenschappelijk doel willen behalen.
  Het behalen van het gemeenschappelijke doel wordt gedaan door middel van een strategie waarin is geformuleerd hoe de organisatie wordt ingezet om haar doelen te behalen. In de strategie is ook vastgelegd welke normen en waarden hierbij van belang zijn.
  De vormgeving van de strategie wordt het design genoemd.

- *Personen*
  Het eerder genoemde ontwerp slaat voor een deel op de manier waarop de personen binnen de organisatie zich tot elkaar verhouden. Dit zijn de medewerkers. Dit kan hiërarchisch zijn, maar ook meer flexibel. De personen binnen de onderneming zijn de belangrijkste middelen. In het model wordt onder de term mensen de mens als middel binnen de organisatie beschouwd. Ook de (on)veiligheid die zij kunnen veroorzaken binnen de organisatie valt onder deze term. Een belangrijk onderdeel van de factor personen is de plaats waar zij zich bevinden in het ontwerp van de organisatie. Hier is namelijk ook de mate van verantwoordelijkheid op gebaseerd.

- *Processen*
  Het behalen van het doel van de organisatie en de subdoelen die tussen de huidige situatie en de doelstelling zitten, worden behaald doormiddel van het proces. Het proces is de interactie van het personeel en de middelen om tot een verandering van vorm of omstandigheid te leiden. Een proces bestaat vaak uit meerdere stappen die elk een bepaalde bijdrage hebben die leiden tot een gewenste uitkomst.

- *Technologie*
  Als technologie binnen een organisatie worden alle technieken beschouwd die als bedoeling hebben om de processen sneller te laten verlopen. Hieronder vallen applicaties, hulpmiddelen en infrastructuren binnen de organisatie. Technologie bevindt zich in een snel veranderende omgeving. Doordat technologische ontwikkelingen nieuwe mogelijkheden bieden die processen sneller en efficiënter kunnen laten verlopen is het een belangrijk, kritiek en kwetsbaar punt binnen organisaties. Een zwakte die nog vaak voorkomt binnen organisaties is het overdadig vertrouwen op technologie. Hierdoor is personeel zich niet altijd bewust van de gevaren.

In het model zijn geen hiërarchische verhoudingen tussen de vier factoren. Ze zijn dus even belangrijk en afhankelijk van de onderlinge relaties.
Hierdoor zijn alle vier de factoren met elkaar verbonden door middel van zes verbindingen: Cultuur, governing, noodzaak, menselijke factoren, architectuur en inschakeling en ondersteuning.
Beïnvloeding van deze verbindingen leidt tot een verandering van de waarde van de factoren. De invloed ervan op de mate van cybersecurity kan dus toenemen of afnemen. De verbindingen kunnen positief maar ook negatief beïnvloed worden.
De verbindingen zullen hieronder worden besproken en toegelicht. Voor de duidelijkheid wordt er ook toegelicht tussen welke factoren deze verbindingen zich bevinden.

- *Governing* [Organisatie ←→ processen]
  Governing geeft aan hoe de sturing van de organisatie eruit ziet. Dit is te benoemen als de strategie van de organisatie. Deze strategie begrenst het opereren van de organisatie. Dit wordt gedaan door resultaten en kaart te brengen en activiteiten te beschrijven. Eén van de doelen van de strategie die voor cybersecurity interessant is, is het voorkomen dat de organisatie risico's loopt die het niet kan of wil lopen.

- *Cultuur* [Organisatie ←→ personen]
  Cultuur is de houding van het personeel ten opzichte van bepaalde onderwerpen. De cultuur is te typeren aan de hand van geloof, aannames, houdingen, gedrag en de manier waarop er gehandeld word binnen de organisatie. Groepscultuur is het resultaat van wat er in de omgeving van de groep gebeurt. Cultuur is hier een reactie op. Op basis van bepaalde gebeurtenissen zullen dus ook andere responses ontstaan binnen de groep. Deze respons wordt hetzelfde naarmate meer mensen dezelfde ervaringen hebben. Cultuur heeft veel invloed op hoe mensen met elkaar, leidinggevenden en veranderingen omgaan.

- Architectuur [Technologie ←→ organisatie]
  De security architectuur is de betrekking van hoe de organisatie (en alle losse onderdelen daarbinnen) omgaat met de aanwezige technologie. Het is echter ook van belang dat de juiste technologie bij de juiste organisatie past. Architectuur is daarom geen eenzijdige verhouding van organisatie tot technologie, maar ook van technologie tot organisatie.

- *Inschakeling & ondersteuning* [Processen ←→ technologie]
  Inschakelen in het aanzetten van personen tot het uitvoeren van bepaalde handelingen, ondersteuning is de mate waarin zij worden voorbereid en getraind in het uitvoeren van de

handelingen. Door positieve beïnvloeding van inschakeling & ondersteuning ontstaat er een situatie waarin de medewerkers die het proces beïnvloeden bewust worden van hoe er met de technologie binnen dat proces moet worden omgegaan. Door het installeren van beveiligingsmaatregelen en het instellen van procedures wordt de kans op fouten kleiner. inschakeling & ondersteuning ondervinden vaak weerstand vanuit de organisatie omdat het volgens werknemers de efficiëntie van hun werkzaamheden negatief beïnvloed. Duidelijkheid en een goede onderbouwing van de maatregel kan dan helpen om acceptatie onder het personeel te bevorderen.

- *Noodzakelijkheid* [Processen ←→ personen]
  Noodzakelijkheid verwijst naar de verwachting van het personeel ten aanzien van maatregelen. Incidenten zijn niet altijd te voorzien en de gevolgen zijn voor personeel vaak vaag en onduidelijk. Er wordt daarom niet altijd vanuit gegaan dat deze incidenten zich voor gaan doen. Maatregelen worden daardoor niet altijd als noodzakelijk gezien. Noodzakelijkheid slaat dus op de mate waarin personeel zich bewust is van risico's en het gedrag met betrekking op deze risico's. Persoonlijke beleving is hier een belangrijk onderdeel.

- *Menselijke factoren* [Personen ←→ technologie]
  De mate waarin mensen invloed hebben op technologie worden menselijke factoren genoemd. Wanneer er voor personeel ruimte is om onbewust of bewust fouten te maken tijdens het werken met systemen, valt dit onder menselijke factoren.
  Menselijke factoren lijken op inschakeling & ondersteuning, maar richten zich meer op de factoren die er toe leiden dat personen fouten maken. Er kunnen op het gebied van inschakeling & ondersteuning richtlijnen opgesteld worden die gevolgd moeten worden. Wanneer werknemers geen noodzaak zien om deze te volgen hebben ze alsnog nauwelijks tot geen effect. Dit laatste wordt beïnvloed door menselijke factoren. (ISACA, 2009)

3.4 Onderzoeksobject en onderzoeksvariabelen

Onderzoeksobject en variabelen
Om de onderzoeksvraag *"Is het mogelijk om een uniform analysemodel op te stellen waarmee de mate van SCADA beveiliging kan worden aangetoond? Zo ja, uit welke onderdelen zou een uniform analysemodel waarmee de mate van beveiliging van SCADA systemen bij waterschappen kan worden aangetoond moeten bestaan?"* te kunnen beantwoorden moeten de variabelen en de onderzoeksobjecten duidelijk worden.

Het onderzoeksobject is dat waar onderzoek naar gedaan wordt. Dit kan gezien worden als het onderwerp. Dit onderwerp is vast en dus niet aan verandering onderhevig zoals de onderzoeksvariabele. Het onderzoeksobject is goed herkenbaar en duidelijk afgebakend.
Het onderzoeksobject binnen dit onderzoek is het uiteindelijke uniforme analysemodel dat moet toezien op het verbeteren van de beveiliging van SCADA systemen binnen waterschappen.

De onderzoeksvariabele is het fenomeen of de gebeurtenis waar het onderzoeksobject aan onderhevig is. In dit geval wordt het onderzoeksobject gedefinieerd door de onderdelen van het model die de mate van beveiliging van SCADA systemen beïnvloeden.

De onderdelen van het analysemodel worden in dit geval dan ook aangemerkt als de onderzoeksvariabelen.

3.5 Onderzoeksdesign en operationalisatie

In deze paragraaf zal worden beschreven hoe het onderzoek zal worden uitgevoerd. Het onderzoek zal worden verklaard aan de hand van een stappenplan waarin wordt uitgelegd hoe de verschillende stadia van het onderzoek zich tot elkaar verhouden.

1) Het formuleren van de verwachtingen van het eindproduct

Er moet worden vastgesteld hoe een ideale SCADA beveiliging is vormgegeven. De mate van beveiliging is van twee zaken afhankelijk. Ten eerste situaties of risico's die voorkomen moeten worden. Ten tweede op welke wijze deze risico's beïnvloed kunnen worden.

De risico's moeten in kaart worden gebracht. Doormiddel van een literatuur onderzoek wordt er uitgezocht welke risicovolle situaties zich voordoen met betrekking tot SCADA installaties. Er zal vanuit de variabelen: Taken, kwetsbaarheden en bedreigingen gekeken worden naar de risico's. Elk van deze variabelen is herkenbaar aan een aantal indicatoren waaraan de variabele te herkennen is. De indicatoren zijn herkenbaar en vastgelegd.

Naast de risico's moet er ook gekeken worden naar de factoren die de mate van die risico's beïnvloeden. Uit de theoretische ondersteuning is gebleken dat de beveiliging van technologische systemen, zoals SCADA, zich richt op vier factoren. Deze factoren zijn organisatie, processen, personen en technologie. Sturing op het gebied van SCADA beveiliging vindt op deze gebieden plaats. Wanneer deze twee onderdelen worden samengevoegd ontstaat een ideale wenselijke situatie. Wanneer SCADA op de juiste manier zou zijn beveiligd dan zouden de maatregelen gericht zijn op het verminderen van de risico's door middel van sturing binnen de vier factoren. Door deze vaststelling kunnen maatregelen die geen invloed hebben op de factoren of bijdragen aan het verminderen van de risico's worden geschrapt.

Onderzoeksvraag	Variabelen	Methode	Meetinstrument	Indicatoren
Welke risico's lopen waterschappen die gebruik maken van SCADA systemen?	Taken van waterschappen	Deskresearch	Welke taken voeren waterschappen uit?	• Beheer • Onderhoud • Kwaliteitszorg
	Kwetsbaarheden		Op welke punten is de SCADA binnen waterschappen kwetsbaar?	• Organisatie • Technologie • Personeel • Processen
	Bedreigingen		Welke middelen hebben bedreigingen van SCADA bij waterschappen?	• Intern • Extern • Tools

2) Vaststelling van middelen

Middelen die waterschappen op dit moment hebben om de beveiliging van SCADA systemen te toetsen zijn de Operationele handreiking Bestuur en Informatieveiligheid Dienstverlening (hierna te noemen operationele handreiking BID) en de Baseline Informatiebeveiliging Waterschappen (hierna te noemen BIWA).

In de operationele handreiking BID wordt een proces beschreven dat erop toe moet zien dat de mate van beveiliging van SCADA systemen toeneemt. In één van de stappen de handreiking BID wordt toegelicht dat een analyse op basis van maatregelen in de BIWA kan worden uitgevoerd om te kijken waar de beveiliging kan worden verbeterd. In de BIWA zijn maatregelen vastgelegd die toezien op de beveiliging van informatie binnen waterschappen.

De volgende stap in het onderzoek is het inventariseren van de inhoud van de BIWA. Deze zal bekeken worden op basis de vier factoren in het Business model for Information Security. In de BIWA zijn maatregelen genomen op verschillende gebieden. Deze zijn verdeeld in hoofdstukken die ingaan op de aard van de maatregel. Deze hoofdstukken kunnen gezien worden als deelonderwerpen van de beveiliging. Van deze hoofdstukken wordt gekeken hoe die aansluiten bij de vier factoren van het Business model for Information Security. Dit wordt gedaan doormiddel van determinatie. De tekst wordt beoordeeld op basis van de hieronder vastgestelde indicatoren. Die indicatoren zijn opgesteld om te kunnen beoordelen bij welke van de vier factoren een bepaald deelonderwerp hoort.

De indicatoren die zijn gebruikt voor het beoordelen van de inhoud van de BIWA zijn hieronder weergegeven. Door deze stap wordt duidelijk op welke onderdelen en beveiligingselementen de BIWA zich richt. In Bijlage 1 is de indeling van de deelonderwerpen uit de BIWA dik gedrukt.

Onderzoeksvraag	Variabelen	Methode	Meetinstrument	Indicatoren
Welke maatregelen worden er voorgesteld door de handreiking Taskforce BID en in de baseline informatiebeveiliging waterschappen?	Organisatorisch	Deductief deskresearch	Welke organisatorische maatregelen bieden de handreiking en de taskforce aan?	• Betrokkenheid • Doelstelling • Verantwoording • Externe actoren • Beoordeling
	Technologisch		Welke technologische maatregelen bieden de handreiking en de taskforce aan?	• Monitoring • Wachtwoordbeheer • Hardening • Ontkoppeling • Firewalls • Fuzz- en pentesting • Fysieke beveiliging • Toegangsbeveiliging
	Persoonlijke beveiliging		Welke persoonlijke beveiligingsmaatregelen bieden de handreiking en de taskforce aan?	• Eisen en voorwaarden • Gedrag • Opleiding • Bewustwording • Controle • Disciplinaire maatregelen • Werving en ontslag
	Procesmatig		Welke procesmatige maatregelen bieden de handreiking en de taskforce aan?	• Procedures • Beleid • Beheer

3) Beoordeling van aangeboden middelen

De toetsing van de maatregelen in de eerder geïnventariseerde deelonderwerpen vindt plaats op basis van determinatie. Deze keer vindt de determinatie niet plaats op basis van de factoren, maar op basis van de eigenschappen van eerder vastgestelde bedreigingen.

Om deze indicatoren vast te stellen zal er een onderzoek naar de dreigingen uitgevoerd moeten worden. Onderstaand zijn de methode en de indicatoren vastgelegd waarmee de maatregelen gedetermineerd zijn. Een volledige uitwerking van de bedreigingen is te vinden in hoofdstuk 4. In Bijlage 1 is terug te zien hoe de maatregelen uit de BIWA gedetermineerd zijn.

Onderzoeksvraag	Variabelen	Methode	Meetinstrument	Indicatoren
Hoe verhouden de vastgestelde middelen uit de BIWA zich tot de vastgestelde bedreigingen en beveiligingsfactoren?	Organisatorisch	Deductief deskresearch	Welke organisatorische maatregelen uit de BIWA zijn gepaste maatregelen tegen bedreigingen en risico's?	• <u>Geautoriseerd intern</u> Monteurs Werknemers Bezoekers Leveranciers • <u>Ongeautoriseerd intern</u> Inbrekers Indringers "Mystery guests" • <u>Geautoriseerd extern</u> Ex werknemers Bezoekers met insider informatie Derde partijen Ex leveranciers • <u>Ongeautoriseerd extern</u> Bedrijfsspionnen Buitenlandse veiligheidsdiensten Hackers Activisten
	Technologisch		Welke technologische maatregelen uit de BIWA zijn gepaste maatregelen tegen bedreigingen en risico's?	
	Persoonlijke beveiliging		Welke persoonlijke beveiligingsmaatregelen maatregelen uit de BIWA zijn gepaste maatregelen tegen bedreigingen en risico's?	
	Procesmatig		Welke procesmatige beveiligingsmaatregelen zijn gepaste maatregelen tegen bedreigingen en risico's?	

Hoofdstuk 4: Methodieken en instrumenten

4.1 Waarborg betrouwbaarheid

Om te waarborgen dat het onderzoek op een kwalitatief goede manier zal worden uitgevoerd zullen in dit paragraaf de dataverzamelingsmethoden worden weergegeven. Door na te denken over de manier van dataverzameling wordt de kwaliteit van het onderzoek gewaarborgd en kunnen eisen gesteld worden om op die manier de betrouwbaarheid van de informatie te waarborgen.

Zo zal van bronnen de auteur worden gecheckt en zal er gekeken worden of de bron betrouwbaar is. Er zal worden gekeken of informatie te vinden is bij verschillende bronnen. Het vaker tegenkomen van dezelfde informatie is een belangrijke indicator om de betrouwbaarheid van een bron mee vast te stellen.

4.2 Literatuur onderzoek

Voor het onderzoek naar technische systemen en voor meer inzicht in de aanbevolen maatregelen wordt gebruik gemaakt van een literatuur onderzoek. Door inzicht te verschaffen door middel van informatie van experts op het gebied van technologie kan de kwaliteit gewaarborgd worden. Het is voor onderzoekers zonder technische expertise en verstand van informatica een grote uitdaging om zelf expertise op te bouwen met betrekking tot SCADA systemen. Daarom zal er een beroep worden gedaan op de inzichten van experts op het gebied van deze techniek.
Op het internet is deze informatie vrij te verkrijgen. Doordat de informatie zo specifiek van aard is, is ook vak literatuur goed te raadplegen. Vakliteratuur is onder andere te vinden op de sites van overheidsorganisaties. Ook zijn relevante bronnen, checklists en analysemodellen te vinden op de site van de informatie beveiligingsdienst. Deze kunnen helpen met het in beeld brengen van de huidige en gewenste situatie binnen waterschappen. Van overige bronnen zal worden gecheckt of de auteur als betrouwbaar mag worden beschouwd.

Literatuur onderzoek zal voornamelijk worden gebruik voor het in kaart brengen van de theorieën die er zijn rond de factoren die meespelen met betrekking tot SCADA systemen. Ook het onderzoek naar bedreigingen en risico's berust op literatuur onderzoek.

4.3 Deductief deskresearch

Om een goed analysemodel op te kunnen stellen is het nodig dat er voldoende informatie over het onderwerp te vinden is. Een kwalitatief onderzoek is daarvoor geschikt. Het stelt de onderzoeker in staat om veel details over een bepaald object of een bepaalde situatie te verkrijgen. De onderzoeker kan vervolgens een analyse op deze details uitvoeren en op basis daarvan conclusies trekken en aanbevelingen doen. In dit geval zal er door middel van een kwalitatief onderzoek onderzocht worden wat er allemaal bijdraagt aan de mate van beveiliging van SCADA systemen bij waterschappen.

Deductief deskresearch is de onderzoeksmethode die wordt gebruikt voor het analyseren van grotere stukken informatie. Hierbij worden stukken tekst getoetst aan de hand van bestaande vooraf gestelde theorieën (Verhoeven, 2011). Deze methode leent zich goed voor het toetsen van de maatregelen uit de Baseline Informatie Beveiliging Waterschappen en de operationele handreiking van de BID. Aan de hand van de theorieën kunnen indicatoren worden opgesteld die kunnen dienen als code. Vervolgens wordt de inhoud van de BIWA en de operationele handreiking getoetst aan die codes.

Hoofdstuk 5: Welke risico's lopen waterschappen die gebruik maken van SCADA systemen?

5.1 Waar waterschappen zich mee bezig houden

In Nederland zijn waterschappen verantwoordelijk voor het waterbeheer. Waterbeheer houdt in dit geval watersysteembeheer, zuiveringsbeheer en het beheer van vaarwegen in.
Watersysteembeheer gaat over de kwantiteit en kwaliteit van het water in een bepaald gebied. De hoeveelheid water wordt door het waterschap gecontroleerd, dit mag niet teveel en niet te weinig zijn. Met zuiveringsbeheer wordt bedoeld dat het waterschap verantwoordelijk is voor het zuiveren van afvalwater. (Het waterschapshuis, 2016) Sommige waterschappen zijn ook verantwoordelijk voor het beheren van vaarwegen. (Rijksoverheid, 2016)

Voor het uitvoeren van deze taken wordt gebruik gemaakt van apparatuur die kan worden aangestuurd met SCADA systemen. Het beheren van vaarwegen wordt bijvoorbeeld gedaan door het bedienen van bruggen en sluizen. Ook bij waterzuiveringsinstallaties wordt van SCADA gebruik gemaakt. Bij grotere systemen wordt hiervoor gebruik gemaakt van SCADA apparatuur.

5.2 Bedreigingen

Er is onderzoek gedaan naar waar de meeste bedreigingen van SCADA omgevingen van afkomstig is. De British Columbia Institute of Technology en de PA consulting groep hebben hier onderzoek naar gedaan. Zij hebben 41 cases tussen 1995 en 2003 naast elkaar gelegd en geanalyseerd.
Uit grafieken is duidelijk af te lezen dat het aantal aanvallen tussen 2000 en 2001 ineens toenemen. In de periode 1995 – 2000 komen er jaarlijks niet meer dan drie gedocumenteerde aanvallen per jaar in beeld. In de periode na 2000 stijgt het aantal aanvallen. Zo zijn er in 2001 al vier aanvallen, 2002 al zes en in 2003 is het aantal al opgelopen naar tien aanvallen per jaar.
(Byres & Lowe, 2004)

Ook Thales cyberassurance deed in 2013 een gelijksoortig onderzoek. In het onderzoek werd uitgegaan van vier dreigingscategorieën. Personeel, aanvallen vinden dan plaats als insider attacks. Fysieke aanvallen, indringers en overvallers vallen hieronder. Cyber, het gebruik van hacking en malware. Omgeving, brand en water overlast en andere natuurlijke bronnen.
Tussen de categorieën fysiek en cyber kan enige overlap plaatsvinden omdat ook hackers gebruik kunnen maken van middelen die fysiek in de organisatie aanwezig moeten zijn. (Thales Cyberassurance, 2013)

Ook stelde Thales enkele mogelijke daders op. Dit zijn de volgende:

- Externe partijen: Hiermee worden bijvoorbeeld monteurs van leveranciers bedoeld. Deze personen zijn niet altijd op de hoogte van de geldende omgangsregeling met de systemen op locatie. Daardoor kan het zijn dat zij handelingen uitvoeren die een risico kunnen vormen en daarom niet uitgevoerd mogen worden.
- Bedrijfsspionnen: Andere bedrijven in dezelfde branche kunnen interesse hebben in de informatie en systemen binnen de organisatie. Het kopiëren van technieken is daardoor een gevaar. Ook kunnen dit soort bedrijven bij aanbestedingen in een bevooroordeelde positie komen omdat zij hun offertes kunnen aanpassen op die van de tegenpartij.

- Criminelen: Criminelen hebben vaak financieel gewin als doel. Inbraken zijn risico's die zij kunnen veroorzaken. Het ontbreken van apparatuur en informatie is gevaarlijk voor de bedrijfscontinuïteit van de organisatie.
- Werknemers: Werknemers kunnen het belang van veiligheidsprocedures niet altijd inschatten. Daardoor kunnen zij proberen de maatregelen te omzeilen, dit kan beveiligingsrisico's opleveren. Het kan ook zo zijn dat zij voldoende op de hoogte zijn van de maatregelen. Dit kan ook risico's opleveren.
- Kwaadwillende werknemers: Werknemers met wraakmotieven, financiële problemen, belangen die niet met die van de organisatie overeenkomen of omkoopbaar zijn.
- Buitenlandse veiligheidsdiensten: Buitenlandse veiligheidsdiensten hebben uiteenlopende en vergaande middelen om aan informatie te komen. Ook informatie over infrastructuur kan hun doelwit zijn.
- Hackers: Hackers hebben verschillende motieven om in te breken in systemen. Overheden, criminaliteit, maar ook nieuwsgierigheid kunnen hen motiveren. Via de juiste sites, zoals Shodan, kunnen zij apparaten benaderen via internet. Inbreuk in SCADA apparatuur kan vergaande gevolgen hebben.
- Bezoekers: Bezoekers kunnen de mogelijkheid hebben om informatie in te zien die zij niet zouden mogen zien. Ze kunnen ook de mogelijkheid hebben om te kijken in accounts die toevallig ingelogd wanneer er bezoekers zijn.
- Activisten (hacktivisten): Zijn traditionele activisten die gebruik maken van digitale middelen. Dit doen zij om hun eigen doelen te behalen. Politieke en maatschappelijke motivaties spelen een grote rol in hun handelen. Radicale activisten kunnen hierbij serieuze schade veroorzaken. Ook kunnen zij gebruik maken van traditionele middelen zoals bedreiging, intimidatie, blokkades en protesten.
- Terroristen: Terroristen hebben vaak als doel het verspreiden van angst om op die manier een politieke of maatschappelijke verandering te bewerkstelligen. Digitale toegang en bediening tot infrastructurele objecten kan een manier zijn om angst te zaaien.

Uit het onderzoek van the British Columbia Institute of Technology en de PA consulting groep bleek dat de bron van SCADA gerelateerde aanvallen is verschoven. Uit de studie is gebleken dat tussen 1982 en 2000 het grootste deel van de SCADA gerelateerde incidenten afkomstig was uit interne bron. Dat wil zeggen dat het grootste aantal incidenten veroorzaakt werd door werknemers. Opvallend is dat het percentage onopzettelijke incidenten kleiner is dan het aantal opzettelijke incidenten.

Tussen 2001 en 2003 veranderde deze verhouding. Het grootste aantal aanvallen was afkomstig van een externe bron en een heel klein deel was afkomstig van interne bron. Er wordt vastgesteld dat SCADA systemen nu vooral aangevallen worden door externe bronnen en dat deze trend zich zal voortzetten.

Uit voorgenoemde informatie blijkt dat de aanvaller geautoriseerd of ongeautoriseerd kan zijn. Daarmee wordt bedoeld of hij binnen de organisatie mag of mocht zijn of dat hij helemaal niks binnen de organisatie te zoeken heeft. Daarnaast wordt ook gekeken naar de afkomst van de aanval. De plaats van opereren kan intern of extern zijn. Hierbij kan ook gedacht worden aan de termen fysiek of technologisch. Als een aanval intern plaats vindt, dan is er fysieke toegang tot het systeem

of de apparatuur nodig. Een inbreker kan alleen schade veroorzaken als hij fysiek aanwezig is. Wanneer de aanval van een externe bron afkomstig is, dan is die technologisch van aard. Een hacker hoeft niet fysiek aanwezig te zijn om schade te veroorzaken.
Op de volgende pagina is een model weergegeven dat de verschillende dreigingsprofielen toelicht. In het model zijn de bedreigingen zoals die zijn omschreven door Thales ingevuld om enkele voorbeelden te geven van mogelijke bedreigingen die in die categorie vallen.

	Plaats van opereren – extern/intern (technisch/fysiek)	
(on)geautoriseerd	Geautoriseerd - Intern - Monteurs van leveranciers - Werknemers - Bezoekers	Geautoriseerd – Extern - Ex werknemers - Bezoekers met insider informatie - Derde partijen - Leveranciers
	Ongeautoriseerd – Intern - Inbrekers - Indringer - “Mystery guests”	Ongeautoriseerd – Extern - Bedrijfsspionnen - Buitenlandse veiligheidsdiensten - Hackers - Activisten - Terroristen

Figuur 5: Profilering van bedreigingen voor SCADA systemen.

5.3 Profilering

In het model zijn de bedreigingen voor SCADA systemen geselecteerd op hun eigenschappen. Door profielen te schetsen van de groepen wordt duidelijk via welke weg zij schade kunnen aanrichten binnen de organisatie. Tegen het aanrichten van die schade moeten vervolgens maatregelen worden geformuleerd. Ook moet er bekeken worden hoe die maatregelen gehandhaafd kunnen worden.

Geautoriseerd – intern

Onder geautoriseerde interne bedreigingen vallen monteurs, werknemers en bezoekers. Zij hebben gemeenschappelijk dat niemand hun aanwezigheid wantrouwt. Personen die in dit profiel passen hebben daardoor toegang tot op zekere hoogte toegang tot de organisatie. Bezoekers hebben toegang tot plekken waar zij anders niet zouden moeten kunnen komen. Zij hebben over het algemeen geen expertise over apparaten en software en zijn niet op de hoogte van richtlijnen en procedures. Sommige werknemers hebben volledige toegang tot kwetsbare apparaten van de organisatie. Monteurs en leveranciers hebben daarnaast ook kennis van systemen en worden snel vertrouwd op hun expertise. Externe monteurs zijn echter niet altijd op de hoogte van de richtlijnen die door de organisatie gesteld kunnen worden. Dit kan risico’s opleveren met betrekking tot het handhaven van beveiligingsnormen.

Ongeautoriseerd – Intern

Inbrekers en indringers hebben gemeenschappelijk dat zij vaak met kwade bedoelingen de organisatie binnendringen. Inbrekers hebben vaak een financieel motief en zijn bereid om schade te veroorzaken. Indringers horen simpelweg niet in de organisatie thuis en kunnen, wanneer onopgemerkt, stelen en vernielen. Dit veroorzaakt schade. Van inbrekers en indringers is vaak ook al snel duidelijk dat zij niet in de organisatie thuis horen. Dit is een verschil met mystery guests. Mystery guests zijn personen die doen alsof zij binnen de organisatie thuis horen maar dat eigenlijk

niet horen. Zij kunnen doen alsof zij bezoekers, monteurs of zelfs medewerkers zijn. Dit kan gebeuren door vertrouwen op te wekken door het gebruik van nagemaakte pasjes of uniformen. Mystery guests worden vaak gebruikt door consultancy bureaus die de veiligheid binnen een organisatie willen aantonen. Het is niet ondenkbaar dat kwaadwillenden dezelfde methode gebruiken.

Geautoriseerd – Extern
Geautoriseerde externe personen kunnen ex werknemers zijn die nog kunnen inloggen in het systeem of externen met toegangsinformatie, zoals wachtwoorden. De man die de hack in Maroochy Shire veroorzaakte was bijvoorbeeld werkzaam bij een bedrijf dat SCADA apparatuur plaatste in rioleringen. (Hale, 2010)
Het is van belang dat niet alle personen bij kwetsbare informatie kunnen en dat de personen die dat wel hebben betrouwbaar zijn.

Ongeautoriseerd – Extern
Ongeautoriseerde externe bedreigingen zijn de daders die geen toegang tot de organisatie hebben en die toegang ook niet nodig hebben voor het uitvoeren van hun acties. Zij kunnen opereren op afstand. Hiervoor wordt vooral gebruik gemaakt van hacking. Bij hacking word het systeem zo gemanipuleerd dat het dingen doet die het niet zou moeten doen. Dit gebeurt doormiddel van zwakheden in de software. Leukfeldt en de Jong geven aan dat hacking voldoet aan drie kenmerken. Het is illegaal, simpel maar doordacht en het vereist aanzienlijke technische kennis. In de praktijk blijkt dat vooral het laatste niet altijd waar is. Op internet zijn voldoende hulpmiddelen en sites te vinden die het makkelijker maken voor een hacker. (Leukfeldt & Stol, 2012)

5.4 Toegang tot de SCADA omgeving

Uit het onderzoek van the British Columbia Institute of Technology en de PA consulting group gaat ook in op de wijze waarop hackers toegang kunnen krijgen tot SCADA. Dit is uitgezocht voor incidenten uit interne bron en voor incidenten uit externe bron.
Er is gebleken dat bij interne incidenten de toegang voornamelijk door het bedrijfsnetwerk tot stand kwam. Dit betekent dat personen uit de kantooromgeving van de organisatie via hun netwerk contact kunnen maken met de SCADA apparaten in het industriële netwerk. Het tweede grootste toegangspunt was de Human Machine Interface. Via de HMI worden de processen schematisch inzichtelijk gemaakt voor medewerkers. Hieruit blijkt dat de mate van veiligheid van het netwerk sterk afhankelijk is van het personeel. Als één na laatste blijkt dat fysieke toegang tot apparaten een bron van onveiligheid is. Als laatste bleek dat laptops een toegangspunt vormen bij interne incidenten.

Bij externe incidenten blijkt dat een groot deel van de incidenten plaats vindt door middel van internet. Ook dail up verbindingen vormen een grote voedingsbron voor incidenten. Bij een dail up verbinding wordt er verbinding gemaakt tussen een computer en een modem door de computer op te bellen. Deze netwerkverbinding wordt niet heel veel meer gebruikt. (EasySwitch, 2016)

Een interessant gegeven is dat veel externe incidenten zich voortdoen door middel van verbindingen die voorzien in remote access. Remote access zorgt ervoor dat een derde partij, bijvoorbeeld een provider of een onderhoudsmonteur, kan werken in het systeem. Voor deze toegang worden er

externe verbindingen aangelegd in de vorm van VPN verbindingen en vertrouwde derde partij remote access verbindingen.

Belangrijke middelen die hackers gebruiken voor het hacken van SCADA zijn programma's de vrij op internet te vinden zijn. Thales beschrijft dat hackers objecten kunnen opzoeken door middel van shodan. Vervolgens kunnen zij een verbinding maken via een TOR netwerk, TOR geeft gebruikers de mogelijkheid om anoniem op internet te bewegen. Hackers kunnen exploits (zwakte punten in een programma) kunnen vinden via de kwetsbaarheden scanner Metasploit en die benutten op het object dat ze hebben gevonden.

Eerder is de verdeling gemaakt tussen geautoriseerde en ongeautoriseerde bedreigingen en interne en externe aanvallen. Uit het onderzoek van Thales kan opgemaakt worden dat er verschil is in de toegangswegen van interne en externe aanvallen. Deze kunnen als volgt weergegeven worden. Achter het punt is het percentage gegeven dat het aanvalspunt deel uitmaakt van het totale aantal aanvallen.

Interne aanvalspunten:

- Zakelijke netwerkomgeving/IT omgeving (43%)
- Human Machine Interface (29%)
- Fysieke toegang tot apparaten (21%)
- Laptops (7%)

Externe aanvalspunten:

- Internet (36%)
- Dial-up modem verbindingen (20%)
- Op afstand met onbekende bron (12%)
- VPN connecties (8%)
- Op afstand draadloos (8%)
- Op afstand Telco netwerk (8%)
- Op afstand SCADA netwerk (4%)
- Op afstand vertrouwelijke leveranciers toegang (4%)

Binnen beide lijsten kan er vervolgens gekeken worden welke maatregelen er nodig zijn om misbruik door geautoriseerd en ongeautoriseerde aanvallers te beperken. Hiervoor zal er in het volgende hoofdstuk gekeken worden naar de maatregelen die de baseline informatiebeveiliging waterschappen en de operationele handreiking BID aanbevelen.

Hoofdstuk 6: Welke maatregelen worden er voorgesteld door de handreiking Taskforce Bestuur en Informatieveiligheid Dienstverlening en in de Baseline Informatiebeveiliging Waterschappen?

Voordat er gezocht kan worden naar maatregelen voor SCADA systemen zal er gekeken worden welke maatregelen al voorhanden zijn. Deze maatregelen zijn vastgelegd in de handreiking van de BID en in de BIWA.
In dit hoofdstuk zullen de maatregelen per document in kaart worden gebracht. Er zal worden gekeken onder welke factor van het business model zij vallen. Er zijn vier factoren waar de maatregel deel van uit kan maken: Organisatorisch, technologisch, persoonlijke en procesmatig. Vervolgens zullen de maatrelen kort uitgelegd worden.

6.1 Operationele handreiking Bestuur en Informatieveiligheid Dienstverlening

Er zal van de stappen in de handreiking van de taskforce worden benoemd onder welke factor ze vallen in het business model for information security van ISACA. De maatregelen worden gecategoriseerd onder een van de vier factoren.
Per factor wordt besproken welke maatregelen uit de operationele handreiking BID hier deel van uit maakt.

Organisatorisch

Inzichtelijk maken van processen in de organisatie waarbij van SCADA gebruikt wordt gemaakt
Het doel van dit actiepunt is het verduidelijken van:

- De toepassing en taken van SCADA op een locatie
- Prioritering en mate van belangrijkheid van het proces waarbinnen SCADA gebruikt wordt
- Fysieke locaties waar SCADA aanwezig is
- Netwerk locaties die invloed kunnen hebben op SCADA

Op basis van deze informatie kunnen vervolg stappen worden gezet voor het afstemmen van beleid en verantwoordelijkheden.

Toetsing aan baselines en GAP analyse
Er wordt aangeraden om de organisatie te toetsen aan de baseline informatiebeveiliging waterschappen. In deze baseline worden op verschillende gebieden maatregelen aangeraden die geïmplementeerd zouden moeten worden. De maatregelen richten zich op beveiligingsbeleid, de organisatie van informatiebeveiliging, het beheer van bedrijfsmiddelen, personele beveiliging, fysieke beveiliging, het beheer van communicatie- en bedieningsprocessen, toegangsbeveiliging, verwerving en ontwikkeling en onderhoud van informatiesystemen, het beheer van informatiebeveiligingsincidenten en bedrijfscontinuïteitsbeheer ook wordt er in gegaan op de naleving van maatregelen.
De maatregelen richten zich op veel van de factoren uit het business model for information security.

Inrichten van de organisatie van ICS/SCADA organisatie
Deze inrichting stuurt op de rol van de organisatie en het management met betrekking tot informatiebeveiliging. Hierdoor wordt informatiebeveiliging niet slechts een taak van de organisatie, maar een onderdeel van het beleid. Management en directie worden verantwoordelijk gesteld voor de doelen en middelen die binnen de organisatie gebruikt mogen worden.

Implementatie aanbevolen maatregelen uit GAP analyse
De implementatie van de aanbevolen maatregelen uit de GAP analyse zorgt ervoor dat de gevonden kwetsbaarheden worden verminderd.

Technisch

Pentesting
Het testen van het systeem is enkel een technisch aspect. Door middel van pentesting wordt het systeem getest op kwetsbaarheden die de onveiligheid kunnen veroorzaken. Het eenmalig uitvoeren van pentesten is enkel goed voor de korte termijn en als er op basis van de test maatregelen worden toegepast. Software kan exploits bevatten en deze kunnen niet altijd al ontdekt zijn. Dit betekent dat deze exploits nog ontdekt kunnen worden en dat ze bij een hack of een volgende test wel naar voren kunnen komen. Bij een hack kan een exploit een risico op leveren.

Monitoring SCADA omgeving
De monitoring van een SCADA omgeving is een technische maatregel. Door de monitoring wordt er inzichtelijk gemaakt wat er in het systeem gebeurt. Verdachte autorisatie verzoeken kunnen meteen onderzocht worden en in realtime worden bekeken. Monitoring is een belangrijk onderdeel van structurele verbetering. Wel is het van belang dat het wordt toegepast samen met sluitend beleid dat ongewenste autorisatie kan voorkomen, anders is het slechts symptoombestrijding.

Verbetering van remote access
Remote access zorgt ervoor dat systemen vanaf een andere locatie te besturen zijn. Het is van belang dat verbindingen waarbij gebruik wordt gemaakt van verbindingen via internet goed beveiligd zijn. Deze beveiliging kan tot stand komen door middel van firewalls, VPN verbindingen en monitoring.

Toegangsbeveiliging
Toegangsbeveiliging ziet erop toe dat niet alle personen bij alle informatie kunnen. Niet iedereen hoeft toegang te hebben tot alle informatie en systeemonderdelen dus dienen hier verantwoordelijkheden voor gesteld te worden. Autorisatie en verdeling van bevoegdheden zijn hierbij van belang.

Moeilijker maken van wachtwoorden
Het is volgens de taskforce van belang dat er een beleid wordt opgesteld omtrent het gebruik van verschillende wachtwoorden. Binnen organisaties die gebruik maken van SCADA wordt gebruik gemaakt van verschillende systemen. Het is dan ook noodzakelijk dat er een beleid komt dat erop toeziet dat er verschillende wachtwoorden worden gebruikt die veilig zijn, maar ook goed te onthouden.

Hardening
Hardening beschrijft dat systemen niet onnodig gecompliceerder uitgevoerd worden dan nodig is. Wanneer systemen uitgebreider zijn dan nodig, zullen de systemen ook kwetsbaarder worden. Het

wordt lastiger om het systeem in kaart te brengen en te beveiligen. Hardening zorgt ervoor dat de processen die binnen de organisatie plaats vinden niet verstoord kunnen worden door technologische achterstand.

Ontkoppeling
IT en SCADA omgevingen dienen zoveel mogelijk van elkaar te worden gescheiden. Hierdoor wordt het lastiger om vanuit een IT omgeving in een SCADA omgeving te komen. Netwerkscheiding is van groot belang.

Fuzz testen
Fuzz testen laat zien hoe kwetsbaar het systeem is. Dit wordt gedaan door onjuiste en onverwachte data op het systeem los te laten. Hierdoor kunnen kwetsbaarheden naar voren komen. Fuzz testen lijkt te maken te hebben met het inzichtelijk maken van het systeem en richt zich slechts op de technologie in de organisatie.

Persoonlijk
In de operationele handreiking wordt niet ingegaan op maatregelen die onder de categorie persoonlijke maatregelen vallen. Wel wordt er aan geraden om de maatregelen uit de BIWA uit te voeren. Deze kunnen zich wel richten op de menselijke factoren de meespelen in de beveiliging van SCADA systemen.

Procesmatig
Verantwoordingen in kaart brengen
Op basis van de aanwezige technologie en de vormgeving van de organisatie kan in kaart gebracht worden wie verantwoordelijk is of zou moeten zijn, dit heet verantwoording. Op basis van verantwoordelijkheden kan organisatiebeleid opgesteld worden. Het gedrag van mensen heeft invloed op de technologie, maar technologie heeft voor een deel ook invloed op het gedrag van mensen. Door verantwoordelijkheden duidelijk te verdelen kan de (negatieve) invloed van mensen op de technologie worden beperkt.

Ontwikkelen organisatiebeleid ten aanzien van SCADA
Het ontwikkelen van organisatiebeleid zorgt ervoor dat er afgesproken wordt hoe er gehandeld wordt in bepaalde situaties. Dit is de verbindende schakel tussen processen en organisatie. Er wordt beschreven hoe de strategieën die de organisatie heeft worden ingezet om bepaalde processen uit te voeren. De vereiste processen worden vormgegeven op basis van wat er in de organisatie van belang is.

Conclusie
Op de volgende pagina is een overzicht te vinden van de maatregelen uit de operationele handreiking. In de tabel zijn de maatregelen en actiepunten onder de factor ingedeeld waar ze op basis van de in de operationalisatie vastgestelde indicatoren horen.

Beveiligingsmaatregelen BID	
Organisatorisch	
	Inzichtelijk maken van processen in de organisatie waarbij van SCADA gebruikt wordt gemaakt
	Toetsing aan baselines en GAP analyse
	Inrichten van de ICS/SCADA organisatie
	Implementatie aanbevolen maatregelen uit GAP analyse
Technologisch	
	Pentesting
	Monitoring SCADA omgeving
	Remote acces verbeteren
	Moeilijker maken van wachtwoorden
	Hardening
	Ontkoppeling
	Fuzz testen
Persoonlijk	
Procesmatig	
	Verantwoordingen in kaart brengen
	Ontwikkelen van organisatiebeleid ten aanzien van ICS/SCADA

6.2 Baseline Informatiebeveiliging Waterschappen

Er zal van de stappen in de BIWA worden benoemd onder welke factor ze vallen in het business model for information security van ISACA. De maatregelen worden gecategoriseerd onder een van de vier factoren.
Per factor wordt besproken welke maatregelen uit de BIWA hier deel van uit maakt.

Organisatorische maatregelen

Informatiebeveiligingsbeleid

Bij reguliere informatie en communicatie voorzieningen wordt de meeste waarde gehecht aan vertrouwelijkheid,vervolgens aan integriteit en als laatste aan beschikbaarheid. Deze prioritering ziet er voor SCADA omgevingen heel anders uit. Hier wordt het meeste belang gehecht aan integriteit, vervolgens aan beschikbaarheid en als laatste aan de vertrouwelijkheid van het systeem.

De bedoelingen van organisatiebeveiligingsbeleid zijn het borgen van betrouwbare dienstverlening, het aantoonbaar kunnen maken dat het beleid voldoet aan de relevante wet en regelgeving van informatiebeveiliging, bevorderen dat alle partners zich kunnen vinden in de voorstellen en als laatste het voortzetten van de belangrijkste bedrijfsprocessen tijdens calamiteiten en incidenten.
Het is nodig dat informatiebeveiligingsbeleid wordt toegepast als integriteit, betrouwbaarheid en beschikbaarheid gebrekkig zijn. beveiligingsbeleid wordt gemaakt door de maatregelen en procedures die er in vastgelegd zijn.
Het is belangrijk dat beleidsdocumenten voor de hele organisatie inzichtelijk zijn en periodiek op de inhoud worden geëvalueerd.

Organisatie van informatiebeveiliging

De bedoeling van het organiseren van informatiebeveiliging is het betrekken van de hele organisatie in het beveiligingsproces. Het evalueren en updaten van beleidsplannen is dan ook een indicatie die laat zien dat de organisatie belang hecht aan veiligheid.

- De top van de organisatie ziet het belang van informatiebeveiliging. Het management spreekt wensen en eisen uit en kent de verantwoordelijkheden voor informatiebeveiliging.
- Taken voor verbetering van de informatiebeveiliging zijn ondergebracht bij vertegenwoordigers uit onderdelen van de organisatie.
- Verantwoordelijkheden zijn duidelijk bij betrokken personeel.
- Nieuwe apparaten worden goedgekeurd volgens een proces.
- Er zijn eisen voor geheimhouding en deze worden periodiek geëvalueerd.
- Er worden contacten met overheidsorganisaties onderhouden betreft informatiebeveiliging.
- Er worden contacten met overige actoren onderhouden betreffende informatiebeveiliging.
- Er is periodieke evaluatie van beleidsdocumenten.
- Bij samenwerking met externe partijen zijn de risico's geëvalueerd.
- Bij toegangsverlening aan klanten wordt er beoordeeld of voldaan kan worden aan beveiligingseisen.
- Bij toegangsverlening aan overige partijen wordt beoordeeld of er voldaan kan worden aan de beveiligingseisen.

Technische beveiliging

Fysieke beveiliging

De fysieke beveiligingsmaatregelen moeten voorkomen dat onbevoegden toegang hebben tot of schade kunnen aanbrengen aan het terrein of systeem van de organisatie. Dit kan inhouden dat er barrières worden opgeworpen in de vorm van muren, omheiningen, toegangscontroles en recepties. In de BIWA zijn omschrijvingen gegeven van de situaties die binnen waterschappen voor kunnen komen en welke maatregelen daarop van toepassing zijn. Specifieke maatregelen tegen gevaren van natuurlijke oorsprong zijn niet meegenomen in het analyse model.

- Er zijn barrières tussen ICT en SCADA voorzieningen.
- Er is toegangsbeveiliging die erop toeziet dat alleen bevoegd personeel toegang heeft.
- Kantoren, ruimten en faciliteiten zijn fysiek beveiligd.
- Er is bescherming tegen risico's van menselijke en natuurlijke oorsprong.
- De organisatie heeft richtlijnen voor het werken in beveiligde ruimten.
- Toegangspunten van het bedrijf zijn afgeschermd van ICT voorzieningen.
- Apparatuur wordt geplaatst en beschermd en verminderd het risico op schade en onbevoegde toegang.
- Apparatuur is beschermd tegen storingen en uitval.
- Bekabeling is beschermd tegen beschadiging en ongewenste manipulatie.
- Apparatuur wordt onderhouden om beschikbaarheid te bevorderen.
- Apparatuur buiten het terrein wordt beveiligd tegen risico's die op die locatie relevant zijn.
- Apparatuur waarop informatie kan worden opgeslagen wordt gecontroleerd voordat de apparatuur wordt verwijderd of vervangen.
- Zonder voortijdige toestemming wordt er geen apparatuur van de locatie meegenomen.

Toegangsbeveiliging

Indringers worden door Thales aangemerkt als bedreiging voor SCADA systemen. Indringers kunnen schade veroorzaken of spullen meenemen. Toegangsbeveiliging zoals aangeraden is in de BIWA is daarom van belang. Bij toegangsbeveiliging moet gedacht worden aan technische maatregelen die worden aangevuld moet procedurele maatregelen.

- Beheersen van toegang tot informatie.
- Toegang voor onbevoegden voorkomen.
- Voor het registreren van gebruikers zijn procedures opgesteld.
- Het gebruik van speciale bevoegdheden wordt beheerst.
- Wachtwoorden uitgeven gebeurt door middel van een formeel beheersproces.
- Het management beoordeelt de toegangsrechten van gebruikers door middel van een formeel proces.
- Onbevoegde toegang, beschadiging en diefstal worden voorkomen.
- Gebruikers maken gebruik van goede beveiligingsgewoontes bij het instellen van wachtwoorden.
- Gebruikers zorgen ervoor dat onbeheerde apparatuur passend beschermd is.
- Er wordt gebruik gemaakt van een clear screen en clean desk beleid.
  Dit houdt in dat personeel nooit zichtbaar informatie achter kan laten terwijl hij niet aanwezig is.
- Onbevoegde toegang tot netwerkdiensten wordt voorkomen.
- Alleen specifieke bevoegdheid geeft gebruikers toegang tot diensten.
- Er zijn authenticatie middelen om toegang op afstand te beheersen.
- Er wordt overwogen om automatische identificatie van apparaten op bepaalde locaties toe te staan.
- Fysieke en logische toegang tot poorten voor diagnose en configuratie worden beheerst.
- Verschillende systemen op netwerken moeten worden gescheiden.
- Wanneer verbindingen moeten worden opgezet die de grenzen van de organisatie overschrijden moeten de toegangsmogelijkheden worden beperkt.
- Netwerken zijn voorzien van beheersmaatregelen voor netwerkroutering.
- Onbevoegde toegang tot besturingssystemen wordt voorkomen.
- Er is een procedure voor het verkrijgen van toegang tot besturingssystemen.
- Gebruikers hebben elk een unieke identificatiecode. De identiteit van de gebruiker wordt door middel van een geschikte techniek bewezen.
- Wachtwoordkeuze wordt beïnvloed door interactief wachtwoordbeheer.
- Hulpprogrammatuur waarmee beheersmaatregelen kunnen worden gepasseerd moet zo min mogelijk worden toegepast.
- Niet actieve inlogsessie worden na een vastgestelde periode uitgeschakeld.
- De duur waarop een verbinding met een toepassing met een verhoogd risico in stand mag worden gehouden is beperkt.
- Er wordt voorkomen dat onbevoegden toegang hebben tot informatie in toepassingssystemen.
- Niet alle gebruikers hebben toegang tot alle informatie of alle functies van het systeem.
- Gevoelige systemen hebben een eigen vaste omgeving.

- Informatie op draagbare apparaten en computers is beveiligd.
- Er is formeel beleid omtrent heb treffen van beveiligingsmaatregelen voor het tegen gaan van risico's van draagbare computers.

Ontwikkeling en onderhoud van informatiesystemen
Op informatiesystemen kan gevoelige en belangrijke informatie worden opgeslagen en verlies daarvan kan schadelijk zijn voor de organisatie. SCADA systemen zijn een ander soort systeem dan informatiesystemen. SCADA systemen zijn niet bedoeld voor het opslaan van grote hoeveelheden informatie. Voor SCADA is koppeling met een informatiesysteem niet nodig en zelfs gevaarlijk.
Er zal daarom geen verdere uitwerking over de ontwikkeling en het onderhoud van informatiesystemen toegevoegd worden in het uniforme analyse model.

<u>Persoonlijke beveiligingsmaatregelen</u>
Beheer van bedrijfsmiddelen
Het is van belang dat de bescherming van bedrijfsmiddelen op een adequaat niveau is en dat dit niveau wordt gehandhaafd. Een inventarisatie van bedrijfsmiddelen kan laten zien welke middelen wel of niet op een bepaalde locatie in de organisatie mogen zijn. Ook kan de aanwezigheid van bedrijfsmiddelen gecontroleerd worden door en beheersmaatregel.

- Er is een inventaris van alle belangrijke bedrijfsmiddelen en deze wordt actief bijgehouden.
- Bedrijfsmiddelen zijn eigendom van een organisatie onderdeel.
- Gebruik van bedrijfsmiddelen vindt alleen plaats volgens vooraf opgestelde regels.
- Informatie wordt geclassificeerd naar waarde, wettelijke eisen gevoeligheid en onmisbaarheid.
- Volgens de classificatie zijn er procedures opgesteld die worden gehandhaafd voor het gebruik van informatie.

Personele beveiligingsmaatregelen
De bedoeling van persoonlijke beveiligingsmaatregelen is om ervoor te zorgen dat personen binnen de organisatie geschikt zijn om hun taken uit te voeren. Zij moeten geschikt zijn voor hun taak, hun verantwoordelijkheden kennen en geen risico vormen voor de organisatie. Trainingen en opleidingen moeten aansluiten op de vastgestelde rollen en verantwoordelijkheden.

- Rollen en verantwoordelijkheden zijn verdeeld en vastgelegd
- Gegevens over (mogelijke) medewerkers worden geverifieerd en beoordeeld in relatie tot de mogelijke risico's die iemand kan vormen.
- In arbeidsvoorwaarden zijn verantwoordelijkheden vastgelegd.
- Er wordt verwacht dat iedereen die binnen de organisatie komt zich gedraagt volgens de opgestelde procedures.
- Personen binnen de organisatie worden periodiek getraind.
- Er zijn disciplinaire maatregelen voor medewerkers die inbreuk hebben gemaakt op informatiebeveiliging.
- Er is een procedure voor het beëindigen van het dienstverband van een medewerker.
- Bedrijfsmiddelen worden ingeleverd wanneer het dienstverband eindigt of er van functie wordt gewisseld.
- De toegang tot het systeem wordt ontnomen na beëindiging van het dienstverband.

Beheer van beveiligingsincidenten
Het beheer van beveiligingsincidenten zorgt ervoor dat tastbaar is welke gebeurtenissen er plaats vinden en welke zwakheden daaruit naar voren komen. Op basis daarvan kunnen corrigerende maatregelen worden genomen. Voor SCADA is dit van belang zodat er tijdens evaluaties gekeken kan worden hoe de beveiliging aangescherpt kan worden. Voor een goede en zo compleet mogelijke documentatie van beveiligingsincidenten is het wel nodig dat er wordt ingezet op detectie van incidenten. Monitoring kan daar bijvoorbeeld een onderdeel van zijn.

- Incidenten met betrekking tot informatiebeveiliging moeten zo snel mogelijk worden gerapporteerd.
- Alle personen binnen de organisatie zijn verplicht om gevonden zwakheden te rapporteren en door te geven.
- Verantwoordelijken reageren op informatiebeveiligingsincidenten volgens een vaste procedure.
- De aard, omvang en kosten van een informatiebeveiligingsincident kunnen worden gekwantificeerd en gecontroleerd.
- Er wordt bewijs verzameld volgens de voorschriften.

Naleving van voorschriften
In de BIWA wordt er aandacht gegeven aan de naleving van voorschriften. Omdat de BIWA ook gericht is op beveiligen van informatie wordt er veel ingegaan op de wetgeving omtrent de aard van die informatie. Zo hebben de opslag van intellectueel eigendomsrecht en privacy gevoelige informatie procedurele gevolgen voor de organisatie.
SCADA systemen slaan dit soort informatie niet op dus zal hier geen verder inhoud aangegeven te worden.

Procesmatig
Beheer van communicatie en bedieningsprocessen
Het is van belang dat er wordt vastgelegd hoe de bedieningsprocessen van de aanwezige SCADA systemen eruit zien. In het bedieningsproces is vastgelegd welke handelingen wel en niet mogen worden uitgevoerd en wanneer bepaalde handelingen moeten worden uitgevoerd.
Er is gebleken dat een deel van de incidenten een interne afkomst heeft. Hier valt ook onbedoeld handelen tussen. Het moet daarom voor iedereen in de organisatie duidelijk zijn wat zij wel en niet mogen doen.

- Bedieningsprocessen zijn vastgelegd en beschikbaar voor personeel.
- Wijzigingen in systemen worden gecontroleerd en vastgelegd.
- Verantwoordelijkheden zijn verdeeld zodat misbruik wordt voorkomen.
- Er zijn duidelijke scheidingen aangebracht in netwerken en organisatie onderdelen om risico’s te voorkomen.
- Wanneer een externe partij werkzaamheden komt verrichten is die partij verplicht om de regels die vastgelegd zijn in de overeenkomst na te leven.
- Opgeleverde stukken van externe partijen worden regelmatig gecontroleerd en beoordeeld.
- Wanneer de externe partij haar dienstverlening wijzigt, dan moet dit worden vastgelegd en moet de impact hiervan worden onderzocht.

- De capaciteit van apparaten wordt afgestemd met de vereiste prestaties die geleverd moeten worden.
- Tegen virussen worden duidelijke maatregelen getroffen in de vorm van detectie, preventie, voorlichting en herstel.
- “Mobile code” wordt wanneer nodig gebruikt volgens het vastgestelde beveiligingsbeleid.
- Er worden periodiek back-ups gemaakt van informatie en programma’s.
- Netwerken worden beschermd en beheerst.
- In elke overeenkomst omtrent netwerkdiensten zijn beveiligingskenmerken en niveau’s opgenomen.
- Voor verwijderbare media is een beheersprocedure.
- Wanneer opslagapparaten niet langer nodig zijn, worden ze verwijderd volgens procedures.
- Behandeling en opslag van informatie vindt volgens een procedure plaats.
- Onbevoegden hebben geen toegang tot systeemdocumentatie.
- Vertrouwelijke informatie is niet vrij toegankelijk.
- Wanneer informatie op welke manier dan ook moet worden uitgewisseld zijn er beschrijvingen van hoe dit mag plaatsvinden.
- In overeenkomsten is vastgelegd voor de uitwisseling van informatie tussen de organisatie en externe partijen.
- Media die informatie bevatten moeten worden beschermd tegen onbevoegden en misbruik.
- Digitale informatie verspreiding moet worden beschermd.
- Het koppelen van systemen die bedrijfsinformatie bevatten moet gebeuren volgens vastgestelde procedures.
- Informatie die fraude gevoelig is en bereikbaar is via openbare netwerken moet worden beschermd tegen fraudegevoelige activiteiten.
- Online transacties en informatie die daarop van toepassing is, moet worden beschermd tegen duplicatie, openbaar making, wijziging en onvolledige overdracht.
- Modificatie die beschikbaar wordt gesteld mag niet worden aangepast door onbevoegden.
- Activiteiten en netwerkgebeurtenissen worden opgeslagen in logbestanden die worden bewaard voor een bepaalde periode.
- Het gebruik van IT voorzieningen wordt gecontroleerd middels vastgestelde procedures.
- Logbestanden worden beschermd tegen modificatie.
- Activiteiten van administratoren worden vastgelegd in logbestanden.
- Storingen worden vastgelegd in logs.
- Tijden worden op alle apparaten gesynchroniseerd en komen met elkaar overeen.

Bedrijfscontinuïteitsbeheer

Bedrijfscontinuïteit is de mate waarin de organisatie tijdens een grote storing in staat is om de primaire bedrijfsactiviteiten voort te zetten. Bedrijfscontinuïteit is geen preventiemaatregel, maar meer gericht op nazorg. Maatregelen die vallen onder bedrijfscontinuïteit kunnen niet voorkomen dat SCADA voorzieningen uitvallen. Bedrijfscontinuïteitsbeheer zal daarom buiten het uniforme analysemodel vallen.

Conclusie

Hieronder is een overzicht gemaakt van de maatregelen uit de BIWA. In de tabel zijn de maatregelen en actiepunten onder de factor ingedeeld waar ze op basis van de in de operationalisatie vastgestelde indicatoren horen.

Beveiligingsmaatregelen BIWA	
Organisatorisch	
	Informatiebeveiligingsbeleid
	Organisatie van informatiebeveiliging
Technologisch	
	Fysieke beveiliging
	Toegangsbeveiliging
	Ontwikkeling en onderhoud
Persoonlijk	
	Beheer van bedrijfsmiddelen
	Personele beveiliging
	Beheer van beveiligingsincidenten
	Naleving van voorschriften
Procesmatig	
	Beheer van communicatie en bedieningsprocessen
	Bedrijfscontinuïteitsbeheer

Hoofdstuk 7: Hoe verhouden de vastgestelde middelen uit de operationele handreiking Taskforce Bestuur en Informatieveiligheid Dienstverlening en de Baseline Informatiebeveiliging Waterschappen zich tot de vastgestelde bedreigingen?

In dit hoofdstuk wordt er gekeken naar de maatregelen die SCADA kunnen beveiligen tegen de eerder vastgestelde bedreigingen. Deze bedreigingen zijn verdeeld in vier categorieën. Het is van belang dat er voor al deze vier categorieën maatregelen zijn die voortkomen uit de vier factoren uit het businessmodel for information security. Welke maatregelen onder welke categorie vallen is in hoofdstuk 6 uitgezocht en beschreven

7.1 SCADA relevante maatregelen uit de operationele handreiking Bestuur en Informatieveiligheid Dienstverlening

In de operationele handreiking BID worden actiepunten gepresenteerd waardoor organisaties zicht kunnen krijgen op de risico's die hun SCADA organisatie loopt. Wanneer gebruik wordt gemaakt van de operationele handreiking is het nodig dat er eerst inzichtelijk wordt gemaakt welke processen binnen de organisatie gebruiken maken van SCADA. Ook moet er een GAP analyse worden uitgevoerd. Deze moet uitgevoerd worden op basis van de maatregelen die de BIWA aanbeveelt.

Van actiepunten is niet vast te stellen op welke van de bedreigingen er een oplossing wordt geformuleerd. De actiepunten uit de operationele handreiking beschrijven een proces dat doorlopen moet worden om inzicht te verkrijgen in de kwetsbaarheden binnen de organisatie en het SCADA systeem binnen de organisatie. Er zal alleen van de geboden maatregelen uit de handreiking worden beoordeeld op welke van de bedreigingen ze zich richten. Deze maatregelen zijn:

- Pentesting
- Monitoring van de SCADA omgeving
- Verbetering van remote acces
- Vervangen en moeilijker maken van wachtwoorden
- Hardening
- Ontkoppeling
- En fuzz testen

Deze maatregelen zijn allemaal technologisch van aard. In de tabel hieronder is inzichtelijk gemaakt tot welke bedreigingen deze maatregelen zich richten.

Maatregel	Geautoriseerd intern	Ongeautoriseerd intern	Geautoriseerd extern	Ongeautoriseerd extern
Pentesting				X
Monitoring			X	X
Verbetering Remote acces			X	X
Moeilijker maken wachtwoorden				X
Hardening				X
Ontkoppeling				X
Fuzz testen				X

Wat opvalt is dat alle maatregelen volledig van technologische aard zijn en zich alleen richten op bedreigingen van externe aard. Eerder is vastgesteld dat bedreigingen die een herkomst hebben buiten de organisatie altijd van technologische aard zijn.
De maatregelen die de operationele handreiking biedt geven goed weer welke technische mogelijkheden er zijn om de mogelijkheid tot het uitvoeren, maar zijn niet voldoende om een volledige bescherming van het systeem te kunnen garanderen.

7.2 SCADA relevante maatregelen uit de Baseline Informatiebeveiliging Waterschappen

Voor de maatregelen uit de BIWA is hetzelfde gedaan. De maatregelen zijn gedetermineerd aan de hand van de eerder opgestelde indicatoren.
Hieronder is inzichtelijk gemaakt hoeveel maatregelen er bij de groepen maatregelen zijn gedetermineerd. Naast de vier bedreigingen zijn ook de kolommen “borgende maatregelen” en “niet van toepassing op SCADA” te zien. Borgende maatregelen geven vooral maatregelen aan die dienen ter evaluatie. De maatregelen die hiermee zijn aangemerkt, kunnen niet ingezet worden om de dreigingen in de andere categorieën te verminderen.
In de laatste kolom zijn alle maatregelen gedetermineerd die niet toepasselijk zijn op SCADA systemen. Enkele voorbeelden hiervan zijn maatregelen die toezien op de beveiliging van persoonsgegevens, SCADA systemen hebben niks te maken met het opslaan van persoonsgegevens. Deze maatregelen kunnen dus buiten beschouwing gelaten worden tijdens de selectie van maatregelen voor het uniforme analyse model.
Een volledig overzicht van de maatregelen uit de BIWA en de wijze hoe ze gedetermineerd zijn is te vinden in [BIJLAGE].

Factoren	**Maatregel groep**	Geautoriseerd intern	Ongeautoriseerd intern	Geautoriseerd extern	Ongeautoriseerd extern	Borgende maatregelen	Niet van toepassing op SCADA
Organisatorisch	Informatiebeveiligingsbeleid	-	-	-	-	2	-
	Organisatie van informatiebeveiliging	1	-	4	-	6	2
Technologisch	Fysieke beveiliging	6	26	1	3	1	5
	Toegangsbeveiliging	19	10	33	19	-	1
Persoonlijk	Beheer van bedrijfsmiddelen	17	7	4	1	2	4
	Beheer van beveiligingsincidenten	-	-	-	-	16	-
Procesmatig	Beheer van communicatie en bedieningsprocedures	19	18	6	36	13	16

De cijfers geven aan hoeveel maatregelen van toepassing zijn op bepaalde dreigingen. Wat opvalt is dat er bij het beheer van beveiligingsincidenten alleen maar maatregelen zijn die zijn aangemerkt als borgende maatregelen. Dit komt doordat deze maatregelen dienen ter evaluatie van het

informatiebeveiligingsbeleid. Sommige maatregelen zijn meegeteld onder verschillende categorieën omdat ze kunnen worden ingezet tegen meerdere soorten bedreigingen.

Hoofdstuk 8: Conclusie

Er is in dit onderzoek gezocht naar een antwoord op de vraag: *"Is het mogelijk om een uniform analysemodel op te stellen waarmee de mate van SCADA beveiliging kan worden aangetoond? Zo ja, uit welke onderdelen zou een uniform analysemodel waarmee de mate van beveiliging van SCADA systemen bij waterschappen kan worden aangetoond moeten bestaan?"*

Om antwoord te krijgen op deze vraag is eerst gekeken naar de bedreigingen van SCADA systemen. Deze bedreigingen kunnen geautoriseerd of ongeautoriseerd zijn ten opzichte van de organisatie en intern of extern opereren. Hierdoor ontstaan enkele profielen waar rekening mee gehouden moet worden tijdens het formuleren van het uniforme analyse model.

De operationele handreiking van de BID raadt aan om technische maatregelen te implementeren. Deze maatregelen zijn:

- Pentesting
- Monitoring van de SCADA omgeving
- Verbetering van remote acces
- Vervangen en moeilijker maken van wachtwoorden
- Hardening
- Ontkoppeling
- En fuzz testen

Technische verbetering is echter vaak van tijdelijke aard. Daarom raadt de BID ook aan om maatregelen uit BIWA te gebruiken. Deze maatregelen richten zich naast techniek ook op de organisatie, menselijke factoren en de vormgeving van processen. Niet alle maatregelen uit de BIWA zijn echter van toepassing op SCADA netwerken. De maatregelen die toepasbaar zijn, zijn weergegeven in Bijlage 1 en gemarkeerd onder de risico's die de maatregel kan verminderen. Deze maatregelen dienen gecombineerde te worden met de aanbevelingen uit de operationele handreiking BID. Met behulp van deze maatregelen kan de mate van SCADA beveiliging binnen waterschappen getoetst worden. Wanneer blijkt dat de beveiliging niet voldoende is dan kunnen er met behulp van de geselecteerde maatregelen ook aanbevelingen worden gedaan tot het invoeren van aanvullende maatregelen.

Hoofdstuk 9: Aanbeveling

Om SCADA systemen zo goed mogelijk te beveiligen wordt aangeraden om de technische aanbevelingen uit de operationele handreiking te combineren met de toepasselijke aanbevelingen uit de BIWA. De technische maatregelen geven inhoud aan de beveiliging van het SCADA systeem. Er wordt daarnaast aangeraden om een analyse uit te voeren op basis van de maatregelen die de BIWA geeft. Om deze analyse op een voldoende manier uit te voeren moeten de maatregelen zoals die zijn geselecteerd in de bijlage van dit onderzoek worden gebruikt.

Het is mogelijk om te kijken of genoemde aanbevelingen kunnen worden omgezet in een online quickscan die waterschappen zelf online kunnen invullen zodat zij zelf een beeld hebben van de mate waarin zij hun SCADA beveiliging voor elkaar hebben. Op basis daarvan kan het analyse model een nog praktischere functie krijgen.

Bibliografie

Ashton, K. (2009, juni 22). *That 'Internet of Things' Thing*. Opgeroepen op september 30, 2015, van RFID Journal: http://www.rfidjournal.com/articles/view?4986

Byres, E., & Lowe, J. (2004). *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems.* Berlijn: VDE.

Chiacu, D. (2015, 12 21). *Iranian hackers infiltrated computers of small dam in NY: WSJ*. Opgeroepen op 1 4, 2016, van Reuters: http://www.reuters.com/article/us-cybersecurity-dam-iran-idUSKBN0U41MD20151221

Controlroomdesign. (2015). *Projecten*. Opgeroepen op 12 21, 2015, van Controlroomdesign: http://www.controlroomdesign.nl/Projecten/NautischecentralesRijkswaterstaat.html

EasySwitch. (2016, maart 21). *Dial Up Internet*. Opgeroepen op maart 21, 2016, van EasySwitch: https://www.easyswitch.nl/internet/internet-begrippen/dial-up-internet/

Haes, A. U. (2010, november 20). *Vijf bewijzen dat Stuxnet kerncentrale saboteerde*. Opgeroepen op september 30, 2015, van Webwereld: http://webwereld.nl/beveiliging/1012-vijf-bewijzen-dat-stuxnet-kerncentrales-saboteerde

Hale, G. (2010, September 22). *Classic Hacker Case: Maroochy.* Opgeroepen op maart 21, 2016, van Industrial Safety and Security Source: http://www.isssource.com/classic-hacker-case-maroochy-shire/

Het waterschapshuis. (2016, maart 21). *Watersysteembeheer*. Opgeroepen op maart 21, 2016, van HetWaterschapshuis: http://www.hetwaterschapshuis.nl/pagina/producten/watersysteembeheer/watersysteembeheer.html

Instep. (2015). *Safety Parameter Display System*. Opgeroepen op september 30, 2015, van Instep: http://www.instepsoftware.com/solutions/nuclear-applications/safety-parameter-display-system

ISACA. (2009). *An Introduction to the Business Model for Information Security.* Rolling Meadows: ISACA.

ISO27001. (2010, december 31). Opgeroepen op september 30, 2015, van ISO27001 Informatiebeveiliging begint met beleid: http://www.iso27001.nl/nieuwe-norm/

Langner, R. (2013). *To Kill a Centrifuge.* Arlington, Hamburg, Munich: The Langner Group.

Leiden Scientific B.V. Industriële automatisering. (sd). *Schermafdrukken van LSAnimate 7.0 (DOS)*. Opgeroepen op 12 21, 2015, van Leiden Scientific : http://www.leidenscientific.nl/scada/scada_a.php

Leukfeldt, E., & Stol, W. (2012). *Cybeer Safety: An Introduction.* Den Haag: Boom uitgevers.

Leverett, É. P. (2011). *Quantitatively Assessing and Visualising.* Cambridge: University of Cambridge.

Mashable. (2016). *Hacking*. Opgeroepen op januari 4, 2016, van Mashable: http://mashable.com/category/hacking/

Microsoft. (2016). *What is a computer virus*. Opgeroepen op januari 4, 2016, van Microsoft: https://www.microsoft.com/security/pc-security/virus-whatis.aspx

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2015). *Cyber security*. Opgeroepen op Oktober 1, 2015, van Nationaal Coördinator Terrorismebestrijding en Veiligheid: https://www.nctv.nl/onderwerpen/cybersecurity/

Nationaal Cyber Security Centrum. (2012). *Beveiligingsrisico's van on-line SCADA systemen.* Ministerie van Veiligheid en Justitie.

Nationaal Cyber Security Centrum. (2012). *Checklist beveiliging van ICS/SCADA systemen.* Ministerie van Veiligheid en Justitie.

NCTV. (2010, februari 22). *Analyse bescherming vitale infrastructuur.* Opgeroepen op 12 23, 2015, van Rijksoverheid: https://www.rijksoverheid.nl/documenten/rapporten/2010/02/26/analyse-bescherming-vitale-infrastructuur

NLDIT Computer Kennis. (2016). *Nadeel en voordelen van Netwerk Computers*. Opgeroepen op januari 4, 2016, van NLDIT Computer Kennis: http://www.nldit.com/netwerken/other-computer-networking/201309/78997.html

Rijksoverheid. (2016, maart 21). *Rijksoverheid*. Opgeroepen op maart 21, 2016, van Provincies: https://www.rijksoverheid.nl/onderwerpen/provincies/vraag-en-antwoord/wat-is-een-waterschap

Schellevis, J. (2012, januari 30). *Scada-beveiliging: een structureel probleem*. Opgeroepen op september 30, 2015, van tweakers: http://tweakers.net/reviews/2465/3/scada-beveiliging-een-structureel-probleem-direct-aan-het-internet.html

Soullié, A. (2014, september). Industrial Control Systems Pentesting PLCs 101. *Industrial Control Systems Pentesting PLCs 101*. Solucom management & IT consulting.

Soullié, A. (sd). Industrial Control Systems Pentesting PLCs 101. *Industrial Control Systems Pentesting PLCs 101*. Solucom management & IT consulting.

Taskforce Bestuur & Informatieveiligheid Dienstverlening. (2014). *ICS/SCADA.* Taskforce Bestuur & Informatieveiligheid Dienstverlening.

TechTerms. (2016). *IT*. Opgeroepen op Januari 4, 2016, van TechTerms: http://techterms.com/definition/it

Thales Cyberassurance. (2013). *Cyber Security for SCADA systems.* Basingstoke: Thales.

Van Mil, B., Berenschot, Dijkzeul, A., & van der Pennen, R. (2006). *Zicht op risico's handboek Risicoanalysemethodieken.* Utrecht.

Verhoeven, N. (2011). Wat is onderzoek? In N. Verhoeven, *Wat is onderzoek?* (p. 302). Den Haag: Boom Lemma.

Zijlstra, W. (2008, oktober 8). *ISO 27001 of ISO 27002 als norm voor uw informatiebeveiliging*. Opgeroepen op september 30, 2015, van ZBC kennisbank: http://zbc.nu/algemeen/archief-management/iso-27001-of-iso-27002-als-norm-voor-uw-informatiebeveiliging/

Bijlage 1:
Analyse Baseline Informatiebeveiliging Waterschappen

Factor	Maatregel	Geautoriseerd intern	Ongeautoriseerd intern	Geautoriseerd extern	Ongeautoriseerd extern	Borgende maatregel	NVT
Organisatorisch	**Informatiebeveiligingsbeleid**						
	Er is beleid voor informatiebeveiliging door het Dagelijks Bestuur vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritieke bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.					X	
	Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.					X	
	Organisatie van informatiebeveiliging						
	Er is een goedkeuringsproces voor zowel nieuwe informatievoorzieningen als wijzigingen in informatievoorzieningen.					X	
	Nieuwe medewerkers dienen bij in dienst treden de ambtseed af te leggen, respectievelijk een geheimhoudingsverklaring te tekenen. Dit geldt ook indien het een externe medewerker betreft.	X		X			
	Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.					X	

	Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.					X	
	Het informatiebeveiligingsbeleid wordt minimaal één keer in de drie jaar geëvalueerd en desgewenst bijgesteld					X	
	Periodieke beveiligingsaudits worden uitgevoerd in opdracht van directie.					X	
	Over het functioneren van de informatiebeveiliging wordt, conform de P&C cyclus, jaarlijks gerapporteerd aan het lijnmanagement.					X	
	Informatiebeveiliging is aantoonbaar, op basis van een risicoafweging, meegewogen bij het besluit een externe partij wel of niet in te schakelen.	X		X			
	Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang, fysiek, netwerk of tot gegevens, de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.	X		X			

	Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie (bijv. risicoklasse II van WBP of de vertrouwelijkheidklasse) heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.						X
	Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt.	X					
	Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkerovereenkomst (conform WBP artikel 14) afgesloten.						X
	Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd. (zie ook 6.2.3.3). Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.	X					
	Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.	X					

	Alle noodzakelijke beveiligingseisen worden op basis van een risicoafweging vastgesteld en geïmplementeerd, voordat aan gebruikers toegang tot informatie op bedrijfsmiddelen wordt verleend.	X					
	Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow (broncodedeponering) en reviews geregeld worden.	X					
	In contracten met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.	X					
	In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.	X					
	Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid en integriteit.	X		X			
	In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.	X					
	Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.	X					

	De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.	X					
Technologisch	**Fysieke beveiliging**						
	Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.		X				
	De fysieke locaties van een waterschap en de omtrek worden ingedeeld in verschillende zoneringen.		X				
	Voor voorzieningen (binnen of buiten het gebouw) zijn duidelijke beveiligingsgrenzen bepaald.		X				
	Gebouwen bieden voldoende weerstand (bepaald op basis van een risicoafweging).		X				
	Voor toegang tot speciale ruimten is een doelbinding vereist, dat wil zeggen dat personen op grond van hun werkzaamheden toegang kan worden verleend. (bijvoorbeeld Beheer, BHV).	X	X				
	Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.		X				
	Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.		X				

	De beveiligingszones en toegangsbeveiliging daarvan zijn ingericht conform het toegangsbeleid.		X				
	De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afhankelijk van de zone van een bepaald toegangsmiddel.		X				
	De uitgifte van toegangsmiddelen wordt geregistreerd.		X				
	Niet uitgegeven toegangsmiddelen worden opgeborgen in een beveiligd opbergmiddel.		X				
	Apparatuur en bekabeling buiten computerruimtes moeten aan dezelfde beveiligingseisen voldoen als apparatuur daarbinnen.		X				
	Er vindt minimaal één keer per half jaar een periodieke controle/ evaluatie plaats op de autorisaties voor fysieke toegang.		X				
	Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.		X				
	Papieren documenten en mobiele gegevensdragers die vertrouwelijke informatie bevatten worden beveiligd opgeslagen.		X				
	Er is actief beheer van sloten en kluizen met procedures voor wijziging van combinaties door middel van een sleutelplan, ten behoeve van opslag van gerubriceerde informatie.		X				
	Serverruimtes, datacenters en daar aan gekoppelde bekabelingsystemen zijn ingericht in lijn met daarvoor geldende best practices.		X				
	Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast.						X

	Er behoren richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.	X					
	Medewerkers die zelf niet geautoriseerd zijn mogen alleen onder begeleiding van bevoegd personeel en als er een duidelijke noodzaak voor is toegang krijgen tot fysiek beveiligde ruimten waarin IT voorzieningen zijn geplaatst of waarin met vertrouwelijke informatie wordt gewerkt.	X	X				
	Beveiligde ruimten (zoals een serverruimte of kluis) waarin zich geen personen bevinden zijn afgesloten en worden regelmatig gecontroleerd.		X				
	Zonder expliciete toestemming mogen binnen beveiligde ruimten geen opnames (foto, video of geluid) worden gemaakt.	X					
	Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT voorzieningen, om onbevoegde toegang te voorkomen.		X				
	Er bestaat een procedure voor het omgaan met verdachte pakketten en brieven in postkamers en laad- en losruimten.		X				
	Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.		X				

	Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningsbeveiliging.						X
	Standaard accounts in apparatuur worden gewijzigd en de bijbehorende standaard leveranciers wachtwoorden worden gewijzigd bij ingebruikname van apparatuur.				X		
	Gebouwen zijn beveiligd tegen de gevolgen van blikseminslag.						X
	Eten en drinken zijn verboden in computerruimtes.	X					
	Een informatiesysteem dient te voldoen aan de hoogste classificatieeisen, conform de informatie die voor kan komen op het informatiesysteem bij het verwerken ervan. Indien dit niet mogelijk is wordt een gescheiden systeem gebruikt voor de informatieverwerking waaraan hogere eisen gesteld worden						X
	Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.						X
	Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd.		X				
	Reparatie en onderhoud van apparatuur (hardware) vindt op locatie plaats door - bevoegd personeel, reparatie op locatie uitsplitsen tenzij er geen data op het apparaat aanwezig of toegankelijk is.		X				

	Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.		X				
	Alle apparatuur buiten de terreinen wordt beveiligd met fysieke beveiligingsmaatregelen zoals bijvoorbeeld sloten en cameratoezicht die zijn vastgesteld op basis van een risicoafweging.		X				
	Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.				X		
	Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd op basis vna risicoafweging.	X					
	Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode.				X		

	Hergebruik van apparatuur buiten de organisatie is slechts toegestaan indien de informatie is verwijderd met een voldoende veilige methode.			X			
	Toegangsbeveiliging						
	Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.	X		X			
	Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.	X		X			
	Op basis van een risicoafweging wordt bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	X		X			
	De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.	X					
	De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.				X		

	Wachtwoorden worden nooit in originele vorm (onversleuteld) opgeslagen of verstuurd. • Ten aanzien van wachtwoorden geldt: • Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker). • Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord. • Gebruikers bevestigen de ontvangst van een wachtwoord. • Wachtwoorden zijn alleen bij de gebruiker bekend. • Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken. • Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden.		X		X		
	Het management behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.	X		X			
	Toegangsrechten van gebruikers worden periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het toegangsbeleid en is bepaald op basis van het risiconiveau.	X		X			
	Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en ICT-voorzieningen. Gebruik van wachtwoorden	X		X			

	Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.	X		X			
	Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende: • Wachtwoorden worden niet opgeschreven. • Gebruikers delen hun wachtwoord nooit met anderen. • Wachtwoorden mogen niet opeenvolgend zijn. • Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde. • Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).	X		X			
	Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.	X					
	Er behoort een ‘clear desk’-beleid voor papier en verwijderbare opslagmedia en een ‘clear screen’-beleid voor ICT-voorzieningen te worden ingesteld.		X				
	In het clear desk beleid staat minimaal dat de gebruiker geen vertrouwelijke informatie op het bureau mag laten liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).		X				
	Bij afdrukken van gevoelige informatie wordt, wanneer mogelijk, gebruik gemaakt van de functie ‘beveiligd afdrukken’ (pincode verificatie).						X

	Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.		X				
	Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.		X				
	Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.			X			
	Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.			X			
	Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authentiseren.			X			
	Alleen geïdentificeerde en geauthentiseerde apparatuur kan worden aangesloten op een vertrouwde zone. Eigenapparatuur (BringYourOwn Device) wordt niet aangesloten op een vertrouwde zone.			X			
	De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.			X	X		
	Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten.			X	X		
	Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.				X		

	Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.				X		
	De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.				X		
	Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.				X		
	Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.				X		
	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).				X		
	Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen			X	X		

	Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.			X	X		
	Netwerken zijn voorzien van beheersmaatregelen voor routering gebaseerd op mechanismen ter verificatie van bron en bestemmingsadressen.			X	X		
	Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.		X		X		
	Toegang tot bedrijfskritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie.		X		X		
	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.		X		X		
	Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.	X		X			
	Bij uitgifte van authenticatiemiddelen wordt minimaal de identiteit vastgesteld evenals het feit dat de gebruiker recht heeft op het authenticatiemiddel.	X		X			

	Bij het intern gebruik van IT voorzieningen worden gebruikers minimaal geauthenticeerd op basis van wachtwoorden.	X					
	Applicaties mogen niet onnodig en niet langer dan noodzakelijk onder een systeemaccount (een privileged user zoals administrator of root) draaien. Direct na het uitvoeren van handelingen waar hogere rechten voor nodig zijn, wordt weer teruggeschakeld naar het niveau van een gewone gebruiker (een unprivileged user).	X					
	Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.	X		X			
	Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (o.a. voldoende sterke wachtwoorden 8, regelmatige wijziging, directe wijziging van initieel wachtwoord).	X		X			
	Wachtwoorden hebben een geldigheidsduur zoals beschreven bij 11.2.3. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.	X		X			
	Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.				X		

	De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Hierbij geldt het volgende: • Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthenticeerd. • Ter voorkoming van typefouten in het nieuw gekozen wachtwoord is er een bevestigingsprocedure.	X		X			
	Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd behoort te worden beperkt en behoort strikt te worden beheerst.				X		
	Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.		X				
	De periode van inactiviteit van het gebruik van een informatiesysteem is vastgesteld op maximaal 15 minuten. Daarna wordt de sessie afgebroken.		X				
	Bij remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.			X			
	De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.			X			
	De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis een wijzigingsverzoek of storingsmelding.			X			
	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.	X					

	Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.				X		
	Bedrijfskritieke systemen behoren een eigen vast toegewezen (geïsoleerde) computeromgeving te hebben. Isoleren kan worden bereikt door fysieke of logische methoden.				X		
	Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.			X			
	Het mobiele apparaat is zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ("zero footprint"). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens. Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.			X			
	Er zijnvoorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen. Bij melding van verlies of diefstal wordt de communicatiemogelijkheid met de centrale applicaties afgesloten.			X			
	Er behoort beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.			X			

	Er wordt een beleid met gedragsregels en een geschikte implementatie van de techniek opgesteld t.a.v. telewerken.			X			
	Er wordt beleid vastgesteld met daarin de uitwerking welke systemen niet en welke systemen wel vanuit de thuiswerkplek of andere telewerkvoorzieningen mogen worden geraadpleegd.			X			
	De telewerkvoorzieningen zijn waar mogelijk zo ingericht dat op de werkplek (thuis of op een andere locatie) geen bedrijfsinformatie wordt opgeslagen (“zero footprint”) en mogelijke malware vanaf de werkplek niet in het vertrouwde deel terecht kan komen.			X			
	Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.				X		
Persoonlijk	**Beheer van bedrijfsmiddelen**						
	Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.	X	X				
	Waterschap specifieke maatregel Er is een actuele registratie van bedrijfsmiddelen die voor de organisatie een belang vertegenwoordigen zoals informatie(verzamelingen), software, hardware, diensten, mensen en hun kennis/vaardigheden. Van elk middel is de waarde voor de organisatie, het vereiste beschermingsniveau en de verantwoordelijke lijnmanager bekend.	X	X				

	Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie	X					
	Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijke lijnmanager benoemd.	X					
	Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen.	X					
	Gebruikers hebben kennis van de regels.	X					
	Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. De toestemming kan generiek geregeld worden in het kader van de functieafspraken tussen manager en medewerker.	X					
	Informatiedragers worden dusdanig gebruikt dat vertrouwelijke informatie niet beschikbaar kan komen voor onbevoegde personen.		X				
	Informatie behoort te worden geclassificeerd om bij het verwerken van de informatie de noodzaak, prioriteiten en verwachte graad van bescherming te kunnen aangeven.						X
	Waterschap specifieke maatregelDe organisatie heeft classificatierichtlijnen opgesteld.						X

	In overeenstemming met hetgeen in het WBP is vastgesteld, dient er een helder onderscheid te zijn in de herleidbare (klasse II/III) en de niet herleidbare (klasse 0 en I) gegevens.						X
	De lijnmanager heeft maatregelen getroffen om te voorkomen dat niet-geautoriseerden kennis kunnen nemen van geclassificeerde informatie.		X		X		
	De opsteller van de informatie doet een voorstel tot classificering en brengt deze aan op de informatie. De goedkeurder van de inhoud van de informatie stelt tevens de classificering vast.						X
	Personele beveiligingsmaatregelen						
	De taken en verantwoordelijkheden van een medewerker zijn opgenomen in de functiebeschrijving en worden onderhouden. In de functiebeschrijving wordt minimaal aandacht besteed aan: • uitvoering van het informatiebeveiligingsbeleid • bescherming van bedrijfsmiddelen • rapportage van beveiligingsincidenten • expliciete vermelding van de verantwoordelijkheden voor het beveiligen van persoonsgegevens	X					

	Alle vaste en ingehuurde medewerkers krijgen bij hun indiensttreding hun verantwoordelijkheden ten aanzien van informatiebeveiliging ter inzage. De schriftelijk vastgestelde en voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging, welke zij bij de vervulling van hun functie hebben na te leven, worden op een toegankelijke plaats ter inzage gelegd. Overeenkomstige voorschriften maken deel uit van de contracten met externe partijen. Ook voor hen geldt de toegankelijkheid van geldende regelingen en instructies.	X					
	Indien een medewerker speciale verantwoordelijkheden heeft t.a.v. informatiebeveiliging dan is hem dat voor indiensttreding (of bij functiewijziging), bij voorkeur in de aanstellingsbrief of bij het afsluiten van het contract, aantoonbaar duidelijk gemaakt.	X					
	De algemene voorwaarden van het arbeidscontract of de aanstelling van medewerkers bevatten de wederzijdse verantwoordelijkheden ten aanzien van informatiebeveiliging. Het is aantoonbaar dat medewerkers bekend zijn met hun verantwoordelijkheden op het gebied van informatiebeveiliging.	X					
	Bij de aanstelling worden de gegevens die de medewerker heeft verstrekt onder andere over zijn identiteit, arbeidsverleden en scholing geverifieerd.	X					

	Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd.	X					
	De directie heeft een strategie ontwikkeld en geïmplementeerd om blijvend over specialistische kennis en vaardigheden van waterschapsambtenaren en ingehuurd personeel (onder andere die kritieke bedrijfsactiviteiten op het gebied van IB uitoefenen) te kunnen beschikken.					X	
	De directie bevordert dat waterschapsambtenaren, ingehuurd personeel en (waar van toepassing) externe gebruikers van interne systemen, algemene beveiligingsaspecten toepassen in hun gedrag en handelen conform vastgesteld beleid.	X		X			
	Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.	X		X			
	Alle medewerkers van de organisatie worden regelmatig attent gemaakt op het beveiligingsbeleid en de beveiligingsprocedures van de organisatie, voor zover relevant voor hun functie.					X	

	Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de informatiebeveiliging hebben gepleegd.	X					
	Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het informatiebeveiligingsbeleid	X					
	Voor ambtenaren is in de ambtseed of belofte vastgelegd welke verplichtingen ook na beëindiging van het dienstverband of bij functiewijziging nog van kracht blijven en voor hoe lang. Voor ingehuurd personeel (zowel in dienst van een derde bedrijf als individueel) is dit contractueel vastgelegd. Indien nodig wordt een geheimhoudingsverklaring ondertekend.			X			
	Het lijnmanagement heeft een procedure vastgesteld voor beëindiging van dienstverband, contract of overeenkomst waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten, innemen van bedrijfsmiddelen en welke verplichtingen ook na beëindiging van het dienstverband blijven gelden.			X			
	Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.		X				

	Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst, of behoort na wijziging te worden aangepast.		X				
	De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en ICT-voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.		X				
	Beheer van beveiligingsincidenten						
	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.					X	
	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen vastgesteld.					X	
	Er is een procedure waarin wordt beschreven hoe met een aangemeld beveiligingsincident wordt omgegaan.					X	
	Er is een procedure voor communicatie met het centrale aanspreekpunt voor incidenten bij de waterschappen.					X	
	Er is een contactpersoon aangewezen voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.					X	

	Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan het centrale aanspreekpunt voor incidenten bij de waterschappen.					X	
	Vermissing of diefstal van apparatuur of media die gegevens van het waterschap kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.					X	
	Informatie over de beveiligingsrelevante handelingen, bijvoorbeeld loggegevens, foutieve inlogpogingen, van de gebruiker wordt regelmatig nagekeken. De CISO bekijkt periodiek – bij voorkeur maandelijks - een samenvatting van de informatie.					X	
	Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en –diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.					X	
	Er is een procedure om eenvoudig en snel beveiligingsincidenten en zwakke plekken in de beveiliging te melden.					X	
	Er behoren verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.					X	
	Er zijn procedures voor rapportage van gebeurtenissen en escalatie. Alle medewerkers behoren op de hoogte te zijn van deze procedures.					X	

	Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.					X	
	De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren. (PDCA Cyclus).					X	
	Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.					X	
	Er is een procedure voor het verzamelen van bewijsmateriaal vastgelegd.					X	
Procesmatig	**Beheer van communicatie en bedieningsprocedures**						
	Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.	X					
	Bedieningsprocedures bevatten informatie over opstarten, afsluiten, backup- en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging.	X					

	Er zijn procedures voor de behandeling van digitale media die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging.				X		
	1. In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: 2. het administreren van significante wijzigingen 3. impactanalyse van mogelijke gevolgen van de wijzigingen 4. goedkeuringsprocedure voor wijzigingen 5. Instellingen van informatiebeveiligingsfuncties (b.v. security software) op het koppelvlak tussen vertrouwde en niet vertrouwde netwerken, worden automatisch op wijzigingen gecontroleerd.				X		
	Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.		X				
	Niemand in een organisatie of proces mag op uitvoerend niveau rechten hebben om een gehele cyclus van handelingen in een bedrijfskritiek informatiesysteem te beheersen. Dit in verband met het risico dat hij of zij zichzelf of anderen onrechtmatig bevoordeelt of de organisatie schade toe brengt. Dit geldt voor zowel informatieverwerking als beheeracties.		X				

	Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.		X				
	Vóór de verwerking van gegevens die de integriteit van kritieke informatie of kritieke informatie systemen kunnen aantasten worden deze gegevens door een tweede persoon geïnspecteerd en geaccepteerd. Van de acceptatie wordt een log bijgehouden.		X				
	Verantwoordelijkheden voor beheer, wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.		X				
	Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.				X		
	Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test en/of Acceptatie en Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet.				X		

	Gebruikers hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test en/of Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt.		X				
	Indien er een experimenteer of laboratorium omgeving is, is deze fysiek gescheiden van de productieomgeving.				X		
	Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.	X					
	De uitbestedende partij blijft verantwoordelijk voor de betrouwbaarheid van uitbestede diensten.	X					
	Uitbesteding is goedgekeurd door de voor het informatiesysteem verantwoordelijke lijnmanager.	X					
	De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.	X					
	Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer.	X					

	De in dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld middels audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem).	X					
	Er zijn voor beide partijen eenduidige aanspreekpunten.	X					
	Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.					X	
	Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.					X	

	De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheid eis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.					X	
	Er worden beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke middelen, zodat een enkele gebruiker (of systeem) niet meer van deze middelen kan opeisen dan nodig is voor de uitvoering van zijn of haar taak en daarmee de beschikbaarheid van systemen voor andere gebruikers (of systemen) in gevaar kan brengen.	X					

	In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om aanvallen te signaleren en hierop te reageren. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is.			X	X		
	Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.					X	
	1. Van acceptatietesten wordt een log bijgehouden.					X	
	2. Er zijn acceptatiecriteria vastgesteld voor het testen van de beveiliging.					X	
	Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.				X		
	Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.						X

	Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, (automatisch) plaats.						X
	In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur antivirusprogrammatuur van verschillende leveranciers toegepast.				X		
	Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken				X		
	Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.				X		
	Op mobile devices wordt antivirus software toegepast				X		
	Als gebruik van 'mobile code' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.				X		
	Mobile code wordt uitgevoerd in een logisch geïsoleerde omgeving (sandbox) om de kans op aantasting van de integriteit van het systeem te verkleinen. De mobile code wordt altijd uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet wordt aangetast.	X					
	Een gebruiker moet geen extra rechten kunnen toekennen aan programma's (bijv. internet browsers) die mobile code uitvoeren.	X					

	Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-up beleid.					X	
	Er zijn periodiek geteste procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.					X	
	Back-upstrategieën zijn vastgesteld op basis van het soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.					X	
	Van back-upactiviteiten en de verblijfplaats van de media wordt een registratie bijgehouden, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie.		X		X		
	Back-ups worden bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up.		X		X		
	De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.		X		X		

	Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.				X		
	Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau komt.				X		
	Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.			X			
	Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast.			X			
	Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast.			X			
	Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	X					
	Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.					X	

	Er zijn procedures opgesteld en geïmplementeerd voor opslag van vertrouwelijke informatie voor verwijderbare media. Voetnoot: toepassen van encryptie bij usb sticks				X		
	Verwijderbare media met vertrouwelijke informatie mogen niet onbeheerd worden achtergelaten op plaatsen die toegankelijk zijn zonder toegangscontrole.		X		X		
	Informatie die langer beschikbaar moet zijn dan de levensduur van de media waarop hij is opgeslagen behoort te worden gekopieerd wanneer 75% van de levensduur van het medium is verstreken.						X
	Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.						X
	Er zijn procedures vastgesteld en in werking voor verwijderen van vertrouwelijke data en de vernietiging van verwijderbare media. Verwijderen van data wordt gedaan met een gecertificeerde methode voor wissen van data, afhankelijk van classificering van data 6 voor apparaten waar dit mogelijk is. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt.				X		
	Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.				X		
	Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang.				X		

	Systeemdocumentatie die vertrouwelijke informatie bevat is niet vrij toegankelijk.				X		
	Wanneer de eigenaar er expliciet voor kiest om gerubriceerde systeemdocumentatie buiten het waterschap te brengen, doet hij dat niet zonder risicoafweging.				X		
	Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.				X		
	Het meenemen van geclassificeerde informatie buiten het waterschap vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is.			X	X		
	Medewerkers zijn geïnstrueerd om zodanig om te gaan met (telefoon) gesprekken, e-mail, faxen, ingesproken berichten op antwoordapparaten en het gebruik van de diverse digitale berichtendiensten dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt.				X		
	Medewerkers zijn geïnstrueerd om zodanig om te gaan met mobiele apparatuur en verwijderbare media dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt. Hierbij wordt ten minste aandacht besteed aan het risico van adreslijsten en opgeslagen boodschappen in mobiele telefoons.		X		X		
	Medewerkers zijn geïnstrueerd om geen vertrouwelijke documenten bij de printer te laten liggen.		X				

	Er zijn maatregelen getroffen om het automatisch doorsturen van interne e-mail berichten naar externe e-mail adressen te voorkomen.						X
	Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.	X					
	Er zijn afspraken gemaakt over de beveiliging van de uitwisseling van gegevens en software tussen organisaties waarin de maatregelen om betrouwbaarheid - waaronder traceerbaarheid en onweerlegbaarheid - van gegevens te waarborgen zijn beschreven en getoetst.	X					
	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, alsmede procedures over melding van incidenten.	X					
	Het eigenaarschap van gegevens en programmatuur en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van programmatuur zijn vastgelegd.	X					
	Indien mogelijk wordt binnenkomende programmatuur (zowel op fysieke media als gedownload) gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de leverancier via een gescheiden kanaal geleverde checksum of certificaat.		X				

	Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.			X	X		
	Om vertrouwelijke informatie te beschermen worden maatregelen genomen, zoals: • versleuteling • bescherming door fysieke maatregelen, zoals afgesloten containers of archief verzegeling • gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • persoonlijke aflevering • opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes				X		
	Informatie die een rol speelt bij elektronisch berichtenverkeer behoort op geschikte wijze te worden beschermd.						X
	Digitale documenten binnen het waterschap waar eindgebruikers rechten aan kunnen ontlenen maken gebruik van bijvoorbeeld PKI Overheid certificaten voor tekenen en/of encryptie.						X
	Er is een (spam) filter geactiveerd voor e-mail berichten.						X
	Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.						X

	Er zijn richtlijnen met betrekking tot het bepalen van de risico's die het gebruik van waterschaps informatie in kantoorapplicaties met zich meebrengen en richtlijnen voor de bepaling van de beveiliging van deze informatie binnen deze kantoorapplicaties. Hierin is minimaal aandacht besteed aan de toegang tot de interne informatievoorziening, toegankelijkheid van agenda's, afscherming van documenten, privacy, beschikbaarheid, back-up en in voorkomend geval cloud diensten.						X
	Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie.						X
	1. Conform verplichting wordt gebruik gemaakt van en voldaan aan de eisen van de authentieke basisregistraties en aangewezen voorzieningen van de overheid gebruikt.						X
	Informatie die een rol speelt bij onlinetransacties behoort te worden beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen.						X

	Een transactie wordt bevestigd (geautoriseerd) door een elektronische handtekening of een andere vorm van wettelijk geldige authenticatie.						X
	De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem behoort te worden beschermd om onbevoegde modificatie te voorkomen.						X
	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.	X			X		
	Er dient een procedure te zijn hoe wordt omgegaan met logging.					X	
	Van logbestanden worden rapportages gemaakt die periodiek worden beoordeeld. Deze periode dient te worden gerelateerd aan de mogelijkheid van misbruik en de schade die kan optreden. De GBA logging kan bijvoorbeeld dagelijks nagelopen worden, evenals financiële systemen, controle van het Internet gebruik kan bijvoorbeeld per maand of kwartaal.					X	

	Een log-regel bevat minimaal: 4. Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID 5. De gebeurtenis (zie 10.10.2.1) 6. Waar mogelijk de identiteit van het werkstation of de locatie 7. Het object waarop de handeling werd uitgevoerd 8. Het resultaat van de handeling 9. De datum en het tijdstip van de gebeurtenis 10. In een log-regel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).		X		X		
	Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden. Controle op opslag van logging: het vol lopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).					X	
	Er behoren procedures te worden vastgesteld om het gebruik van IT voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.		X		X		

	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore. • gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases). • handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels. • beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services). • verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen). • logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren aangesloten op een Security Information and Event Management Systeem 7 waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.		X		X		

	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.		X		X		
	Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.	X					
	Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.		X		X		
	De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.						X