Optimaal beveiligd waterbeheer met de Cybersecurity Implementatierichtlijn voor Objecten 3.0

Informatieveiligheid is essentieel voor de continuïteit en veiligheid van Nederland. In 2012 werden overheidsorganisaties, waaronder waterschappen, opgeroepen om informatiebeveiliging zelfregulerend te organiseren. Met de Cybersecurity Implementatierichtlijn voor Objecten 3.0 (CSIR), die is ontwikkeld door Rijkswaterstaat en het programma Informatieveiligheid en Privacy van Het Waterschapshuis, is hier invulling aan gegeven. De CSIR biedt waterschappen alle handvatten die nodig zijn om elk object in hun industriële automatiseringsomgeving, van sluizen, gemalen tot zuiveringsinstallaties, zo goed mogelijk te beveiligen tegen digitale gevaren, zowel van binnenuit als van buitenaf. En om aan te tonen dat zij de bescherming van hun objecten op orde hebben.

Rioolwaterzuiveringen, gemalen, rioleringen, stuwen en sluizen zijn in de afgelopen jaren getransformeerd tot complexe informatiesystemen die steeds vaker op afstand bestuurd worden. Dijken zijn ‘slim’ gemaakt en bevatten sensoren die de waterschappen van waardevolle informatie voorzien. Digitale watermeters leveren de stuurinformatie waarmee wateroverlast of juist een tekort wordt voorkomen. Mooie ontwikkelingen waardoor waterschappen steeds sneller en gemakkelijker kunnen reageren op veranderingen in de omgeving en efficiënter kunnen werken. En dus steeds beter kunnen zorgen voor goed waterbeheer.

Maar met de inzet van de hiervoor benodigde ICT-systemen zijn waterschappen ook kwetsbaarder geworden voor ontwrichtende zaken van binnenuit, zoals een datalek, en voor digitale aanvallen van buitenaf. Gabor Verputten, hWh vertelt: “We krijgen elke dag veel aanvallen te verduren en het is nog nooit fout gegaan. Maar de vraag is niet óf het een keer fout gaat, de vraag is wanneer dat gebeurt. En vooral: wat de impact dan is. Stel je voor dat iemand de sluizen open zet. Of ons hele systeem plat legt waardoor we onze zuiveringen niet meer kunnen besturen. Die kans is reëel. We worden regelmatig gewaarschuwd dat ‘statelijke actoren’ (andere landen) actief zijn. Als die ons aanvallen gaan wij dat als waterschappen niet tegenhouden.”

Tot zover het slechte nieuws. Het goede nieuws is dat met de implementatie van de zogenaamde CSIR, de Cybersecurity Implementatierichtlijn 3.0, een grote stap gemaakt wordt naar een veel betere bescherming van onze industriële automatiseringsomgeving. En met goede informatiebeveiliging (cybersecurity) kunnen we de kans op uitval, verstoring en misbruik van ICT-systemen zoveel mogelijk voorkomen.

Van risicoanalyse naar passende beveiligingsmaatregelen
Sinds 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO is een normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. In de BIO staan circa 130 maatregelen die genomen kunnen worden om een object te beveiligen. Alle overheidsorganisaties, ook waterschappen, moeten aan de BIO voldoen.

“Maar de BIO heeft een nadeel”, vertelt Arjen Meijer, hWh “want het is een normenkader dat zich sterk richt op de kantoorautomatisering (KA). De waterschappen moeten daarnaast ook goed kijken naar de beveiliging van hun industriële automatisering (IA), zoals sluizen, bruggen en afvalwaterzuiveringsinstallaties. Voor de IA bestaat ook een norm, de IEC 62443, die veel in de industrie wordt gebruikt en vergelijkbaar is met de BIO. In de IEC staan circa 100 maatregelen en de twee normenkaders overlappen elkaar. Dat maakt het voor de waterschappen niet makkelijker om ze goed toe te passen. Met de CSIR lossen we dat op.”

De Cybersecurity Implementatierichtlijn 3.0 is een soort handleiding die stap voor stap van een risicoanalyse naar passende beveiligingsmaatregelen leidt. De eerste stap is het categoriseren van alle objecten van het waterschap. Wat zijn de kroonjuwelen (bijvoorbeeld een boezemgemaal of een zuiveringsinstallatie) en welke is het minst belangrijk? Met de categoriseringsmethodiek van de CSIR kunnen objecten vervolgens vrij eenvoudig van een score worden voorzien. Hierbij wordt gekeken naar de functie van het object (wat doet het en wat gebeurt er als het uitvalt?) en naar de mate waarin het is geautomatiseerd (het beveiligingsrisico). Hoe hoger de score, hoe belangrijker de beveiliging.

Aan elke classificatie is een set van maatregelen gekoppeld die genomen moeten worden om het betreffende object optimaal te beveiligen. Die set is een selectie van de relevante maatregelen uit de BIO en de IEC 62443. Dus door het uitvoeren van de CSIR weet een waterschap precies voor elk object uit haar industriële automatiseringsomgeving welke beveiligingsmaatregelen het moet nemen.

Het palet aan maatregelen is breed, van de inkoop en afvoer van apparatuur en software tot het in stand houden ervan. Want, in tegenstelling tot bijvoorbeeld een laptop (KA), gaan de objecten in de IA soms wel tot 15 jaar mee. Arjen: “Dat betekent dat in contracten met leveranciers geborgd moet worden dat wat je nu aanschaft ook 15 jaar onderhouden gaat worden door die leverancier. De veiligheid moet geborgd worden voor de looptijd van het contract. We zijn momenteel in samenwerking met inkopers bezig om ervoor te zorgen dat dit goed in contracten wordt opgenomen.”

De risicofactor ‘gedrag’
“De CSIR maakt het makkelijker om passende beveiligingsmaatregelen te identificeren, maar garandeert geen veiligheid”, zegt Rob de Lange, hWh. “Want je kunt er natuurlijk voor kiezen om risico’s laag in te schatten. Of om bepaalde maatregelen niet uit te voeren, bijvoorbeeld omdat je ze te duur te vindt. Alleen als je zorgvuldig en goed overwogen keuzes maakt die passen bij de vastgestelde risico’s, kun je qua veiligheid voldoen aan de norm.”

En dan nog zijn we er niet, want de grootste uitdaging zit bij het gedrag van de mensen die met de apparatuur en software werken. Rob: “Je kunt je huis helemaal beveiligen met materiaal van de beste keurmerken, maar als je bij het weggaan de voordeur open laat staan, loopt die inbreker gewoon naar binnen.” De CSIR bevat dan ook maatregelen die het gedrag van de mensen in een organisatie aangaan. Het naleven van afspraken en procedures is essentieel voor de slagingskans van de informatiebeveiliging.

Bovendien zitten er, naast regels ter voorkoming van schade, in de CSIR ook regels en adviezen over hoe je je ICT-omgeving zo snel mogelijk kunt herstellen. Want hoe goed je je automatisering ook beveiligt, het kán mis gaan. En als dat gebeurt moet je ervoor zorgen dat je zo snel mogelijk weer kunt opbouwen. Daarom is in de CSIR aan alles gedacht, van de inrichting van een goede back-up & restore, het afsluiten van waakvlamcontracten en de opzet van een continuïteitsplanning tot een goed functionerende organisatiestructuur.

Technische, theoretische en praktische haalbaarheid
Belangrijk is dat de CSIR technisch haalbaar is. Dat wil zeggen dat de markt kan leveren wat vanuit het normenkader wordt opgelegd. “En daar zijn we wel een beetje trots op”, vertelt Gabor. “Deze richtlijn is tot stand gekomen in samenspraak met grote marktpartijen, die zich verenigd hebben in de Branche organisatie Techniek Nederland. Dat betekent dat de apparatuur die we adviseren ook echt verkrijgbaar is. We zeggen dus niet zomaar ‘dit moet je doen’, het kan ook echt besteld worden.”

De uitvoering van de CSIR is ook theoretisch haalbaar. Er is door vertegenwoordigers van de waterschappen deelgenomen aan de werkgroep die de CSIR heeft ontwikkeld. Gabor: “Dat wil alleen niet zeggen dat uitvoering van de maatregelen voor iedereen per definitie ook meteen praktisch haalbaar is. Elk waterschap

is zelf verantwoordelijk voor de beveiliging van haar automatiseringsomgeving. Er is weinig sprake van standaardisatie en er zijn veel verschillende ICT-systemen. Ook zijn er grote verschillen in de mate van volwassenheid van de informatiebeveiliging. Als een waterschap jaren niets aan haar informatiebeveiliging heeft gedaan en de organisatie op dit vlak niet goed op orde heeft, dan moet er wellicht eerst nog een heleboel gedaan worden voordat aan de richtlijn kan worden voldaan."

De CSIR verschaft veel duidelijkheid en de verwachting is dat de mensen die met de maatregelen aan de slag moeten er veel profijt van zullen hebben. Ter ondersteuning gaat de werkgroep verder met de ontwikkeling van handreikingen. Daarnaast zijn kennispoules beschikbaar als adviseur en sparring partner en kunnen er vanuit het programma Informatieveiligheid & Privacy naar behoefte kennis- of gebruikersdagen worden georganiseerd.

Toepassing van de CSIR: advies of verplichting?
Jaren geleden maakte Rijkswaterstaat een eerste versie van de CSIR voor intern gebruik, die in de loop van de tijd werd aangescherpt en verbeterd. In 2012 verscheen het Bestuursakkoord Water, waarin werd ingegaan op de samenwerking tussen waterbeherende organisaties. In 2018 werd een addendum ondertekend, waarin het onderwerp informatiebeveiliging aan die samenwerking werd toegevoegd. Er werden nieuwe afspraken gemaakt en er werd gestart met het toepasbaar maken van de CSIR voor waterschappen. Het resultaat is deze vernieuwde versie 3.0.

Rob: "En hij wordt nog verder doorontwikkeld, want hij is nu voor RWS en de waterschappen maar we willen de richtlijn ook geschikt maken voor toepassing door bijvoorbeeld drinkwaterbedrijven, gemeenten en provincies."

Nu de richtlijn klaar is, kan elk waterschap er gebruik van maken. De vraag die echter eerst nog beantwoord moet worden is hoe de richtlijn bij de waterschappen gepositioneerd gaat worden. Is het een advies? Een hulpmiddel? Adopteren de waterschappen deze richtlijn? Of wordt de CSIR zelfs verplicht gesteld? Dat besluit zal nog moeten worden genomen door de bestuurders van de waterschappen.

Voor RWS is de CSIR al sinds de vorige versie 2.0 een verplichte richtlijn. De verwachting is dat de CSIR 3.0 in ieder geval 'de' richtlijn voor de informatiebeveiliging van de industriële automatisering (IA) bij de waterschappen zal worden.

"We hebben het jarenlang best moeilijk gehad om als waterschappen aan te tonen hoe veilig we waren", zegt Rob. "Het ene waterschap zei 'bij ons staat het sein op groen', de ander gaf zichzelf een 7 en de derde had er een letter aan gekoppeld. De CSIR is uniform en toetsbaar. Een organisatie als NOREA (de beroepsorganisatie van IT-auditors in Nederland) is betrokken geweest. Zij kunnen, als onafhankelijke organisatie, de waterschappen hier ook op auditen. Zodra de CSIR als waterschapsrichtlijn is vastgesteld, zal die bij de eerstvolgende audit meegenomen worden. En dat is goed, want dan kunnen waterschappen er niet alleen gemakkelijker voor zorgen dat zij hun informatiebeveiliging goed op orde hebben, maar dat ook aantonen."

Meer informatie?
Meer informatie? Programma Informatieveiligheid & Privacy | Het Waterschapshuis
- Rob de Lange (technisch manager) r.delange@hetwaterschapshuis.nl
- Arjen Meijer (projectleider Industriële automatisering en Risicomanagement) a.meijer@hetwaterschapshuis.nl
- Gabor Verputten (tactisch coördinator CERT WM) g.verputten@hetwaterschapshuis.nl