Cybersecurity wordt steeds serieuzer genomen in water- en infrasector

Waterschap moet zich wapenen tegen cybercrime

Door Joeri van der Kloet

Naar aanleiding van de recente problemen met de digitale beveiliging bij het Amsterdamse Waternet, heeft minister Van Nieuwenhuizen maatregelen genomen om de cybersecurity in de watersector te verbeteren. Cybersecurityspecialist voor de OT Hudson Cybertec constateert dat cybersecurity meer aandacht krijgt in de water- en infrasector. Ook komen er steeds meer certificeringen. Daar staat tegenover dat het voor de gemiddelde zolderkamerhacker nog nooit zo makkelijk was om aan effectieve cybercrimetools te komen.

Eén van de meest in het oog springende ontwikkelingen op het gebied van cybersecurity is de toenemende aandacht voor certificering. Naast het feit dat steeds meer bedrijven het belang van de internationale IEC62443-norm inzien, is er ook nationaal steeds meer aandacht voor cybersecurity.

Marcel Jutte: “De Cybersecurity Implementatierichtlijn krijgt steeds meer vorm en wordt ook steeds breder geadopteerd.”

“Zo zien we dat in Nederland de Cybersecurity Implementatierichtlijn steeds meer vorm krijgt en ook steeds breder wordt geadopteerd”, vertelt Marcel Jutte, managing director bij Hudson Cybertec, marktleider op het gebied van cybersecurity in de operationele technologie.
De Cybersecurity Implementatierichtlijn (CSIR) is oorspronkelijk door Rijks-

waterstaat opgesteld voor zijn eigen weg- en waterinfra. In de richtlijn werd aan opdrachtnemers inzichtelijk gemaakt wat er van de partijen verwacht werd op het gebied van cybersecurity op het gebied van de operationele technologie (OT). De CSIR ontstond omdat de richtlijn vanuit de Rijksoverheid, de BIR (Baseline Informatievoorziening Rijksoverheid) zich beperkte tot de kantoorautomatisering. De BIR is inmiddels vervangen door de BIO (Baseline Informatievoorziening Overheid), maar deze heeft dezelfde focus op IT.

Nieuwe versie

Omdat de BIR overging in de BIO, is de Cybersecurity Implementatierichtlijn ook toe aan vernieuwing. De nieuwe versie van de CSIR voor Rijkswaterstaat is er inmiddels. Jutte: “Hudson heeft actief bijgedragen aan de totstandkoming van de CSIR. In de CSIR zijn onderdelen van IEC 62443 opgenomen, maar ook van andere internationale normen. Deze versie van de CSIR is voor Rijkswaterstaat geschreven, om bij grote infraprojecten de cybersecurity in het OT-domein te kunnen waarborgen, bijvoorbeeld bij de grote renovatie van de technische infrastructuur op de Afsluitdijk. “Maar denk ook aan de nieuwe aansluiting op de A15 en de Blankenburgtunnel: allemaal grote projecten waarbij men veel te maken heeft met OT-objecten.”

Veralgemenisering

Nu de CSIR voor Rijkswaterstaat gereed is, gaan er steeds meer stemmen op om die richtlijn ook voor andere toepassingen te gaan inzetten. Bijvoorbeeld binnen het Bestuursakkoord Water (BAW): in het BAW zijn partijen als Rijkswaterstaat, de waterschappen, de provincies, de gemeenten en de drinkwaterbedrijven vertegenwoordigd. Michael Theuerzeit, lead consultant bij Hudson Cybertec: “Het doel van de veralgemenisering van de CSIR is om die geschikt te maken voor andere partijen dan alleen die van Rijkswaterstaat. Net zoals IEC 62443 nu breed geaccepteerd wordt, zou het goed zijn als ook de CSIR op een bredere acceptatie kan rekenen. We richten ons nu nog vooral op de waterschappen, maar op korte termijn zouden ook andere BAW-partners kunnen aansluiten.” Voor de procesindustrie wordt de CSIR relevant op het moment dat bedrijven de verwerking van afvalwater uitbesteden aan een partij die onder de CSIR valt.

Compleet beeld

De CSIR is niet simpelweg een nationale vorm van de reeds bestaande IEC 62443. Theuerzeit: “Het zijn twee verschillende dingen. De IEC 62443 is een norm die beschrijft dat je bepaalde zaken met betrekking tot cybersecurity moet regelen. Er staat in wat je moet doen, maar niet hoe je dat precies moet doen. In de CSIR wordt er gesproken over maatregelensets: er staat heel concreet in omschreven hoe je maatregelen moet doorvoeren. Naast technische eisen en proceseisen worden er op een aantal risicogebieden concrete maatregelen voorgeschreven. Daarnaast bevat de CSIR ook richtlijnen met ‘best practices’. De CSIR geeft dus een concrete invulling voor cybersecuritymaatregelen.”
Vanuit wetgeving hoeven bedrijven formeel nog niet te voldoen aan IEC 62443. Theuerzeit: “We hebben in Nederland een digitale zorgplicht, zoals is vastgelegd in de Wbni (Wet beveiliging netwerk en informatiesystemen, red.). Die wet is een afgeleide van de Europese NIS-directive (Directive on security of Network and Information Systems, red.). Je ziet nu dat Europa die NIS actualiseert en op korte termijn met een zwaardere NIS2 zal komen. Je moet dan als organisatie kunnen aantonen dat je voldoet aan de eisen in die NIS2. Dat kun je aantoonbaar maken met een normenkader als de IEC 62443, maar ook de CSIR biedt een heel mooie operationele uitwerking, waarmee je kunt laten zien dat je de zorgplicht uit de NIS2 serieus neemt.”

Op de agenda

Maar er zijn meer trends waar te nemen. Met enige regelmaat wordt in de media verslag gedaan van geslaagde hacks, nieuwe vormen van cybercriminaliteit en constateringen over de mate van cybersecurity van bepaalde sectoren. “Onlangs konden we nog in de media lezen dat veel Nederlandse gemeenten niet voorbereid zijn op cyberaanvallen”, vertelt Theuerzeit. “Als je dat soort berichten leest, zou je kunnen denken dat het er slecht voorstaat als het om cybercrime gaat, maar de werkelijkheid ligt wat genuanceerder.”

Theuerzeit constateert een toename van bewustzijn met betrekking tot cybercrime. “Tot in de boardroom staat het onderwerp cybersecurity nu beduidend vaker op de agenda dan een aantal jaren geleden. En dat komt

Hudson Cybertec en Kiwa

Onlangs nam Kiwa een belang in Hudson. Kiwa is een zogenaamde TIC company, wat staat voor testen, inspecteren en certificeren. Allerlei soorten apparatuur die wordt gebruikt in industriële, watertechnische, utilitaire en andersoortige toepassingen, worden door Kiwa aan diverse tests onderworpen. “Kiwa was op zoek naar een partij met veel expertise in OT-cybersecurity”, vertelt Theuerzeit. “Wij hebben door dit belang van Kiwa ineens vijfduizend collega’s er bij gekregen. Voor Kiwa betekent het dat ze ineens de beschikking hebben over OT-cybersecurity expertise. “Er ontstaat nu een soort van one-stop-shop waar bedrijven terecht kunnen op het gebied van cybersecurity.” Daarbij speelt het feit dat zowel Kiwa als Hudson Nederlandse ondernemingen zijn een grote rol. “Vooral in de infra, de watersector en overige vitale infrastructuur is het natuurlijk uitermate belangrijk dat ze zoiets belangrijks als cybersecurity, van nulmeting tot certificering, kunnen neerleggen bij Nederlandse bedrijven als Kiwa en Hudson Cybertec.”

Verhogen van de digitale weerbaarheid bij waterschappen

Hudson Cybertec helpt verschillende waterschappen om hun digitale weerbaarheid te vergroten. “We kijken bij die waterschappen hoe ze er technisch en organisatorisch voorstaan op het gebied van cybersecurity in de vorm van een assessment”, vertelt Theuerzeit. “Daarbij gebruiken we zowel de IEC 62443, De CSIR, als de BIO.” Na het assessment worden concrete stappen voorgesteld waarmee de digitale weerbaarheid op orde kan worden gebracht. “Dat betekent dat er soms beleid moet worden geactualiseerd, of dat de netwerksegmentatie op orde moet worden gebracht. Of misschien moet er iets op het gebied van patch-management worden gedaan. We nemen zelfs de keten onder de loep.” Sommige maatregelen zijn ingrijpender en kostbaarder dan anderen. “Het op orde krijgen van het beleid is meestal vrij goed en vlot uit te voeren”, vertelt Theuerzeit. “Maar als je netwerksegmentatie niet op orde is, kost dat meer tijd en vooral ook meer geld.”

Ook op het gebied van gedrag valt er vaak vooruitgang te boeken. Door de toenemende awareness in de watersector voor de valkuilen van cybersecurity wordt het spreekwoordelijke USB-stickje op de parkeerplaats vaak niet meer achteloos ingeplugd, maar Theuerzeit komt wel andere onvolkomenheden tegen. “Ik zie regelmatig dat er bij een afvalwaterzuiveringsinstallatie een mooi groot hek om het terrein staat, maar als je dan eenmaal binnen dat hek bent, zijn veel deuren van gebouwen niet afgesloten, omdat werknemers het vervelend vinden om elke keer weer die sleutel te moeten gebruiken. En bij de engineering workstations zie je hetzelfde: gebruikers loggen zichzelf niet uit en ben je dan als kwaadwillende bij dat workstation, kan je heel wat schade berokkenen.”

dus, let wel, onder andere juist door die berichten in de media. De CEO’s van grote bedrijven lezen die berichten ook en willen dan weten hoe hun eigen organisatie ervoor staat qua digitale weerbaarheid.”

Zolderkamerhacker

Diverse onderzoeksbureaus rapporteren een forse toename in het aantal cyberaanvallen in coronatijd. Een onderzoek van Mimecast heeft het zelfs over een toename van bijna vijftig procent. Theuerzeit is daar niet verbaasd over: “Tot een paar jaar geleden moest je echt wel wat kunnen om een cyberaanval uit te voeren. Tegenwoordig zijn tools en kennis breed verkrijgbaar, ook voor de zolderkamerhacker. Het wordt daardoor steeds makkelijker om een cyberaanval uit te voeren. Je kunt nu de broncode van Stuxnet gewoon downloaden, deze eenvoudig aanpassen en dan kan je sommige installaties al vrij gemakkelijk stilleggen.”

Daarnaast worden technieken steeds moderner en makkelijker beschikbaar. Bijvoorbeeld voor ‘social engineering’, dat vaak voorafgaat aan serieuze cyberaanvallen. Het is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken. “Je kunt bij social engineering bijvoorbeeld gebruikmaken van deep fakes, waarbij videobeelden gemanipuleerd worden en het lijkt alsof je met een vertrouwd persoon in een video-call zit. De technieken worden steeds geavanceerder. Een phishing-mailtje van vroeger zag je van mijlenver aankomen. Tegenwoordig moet je echt goed kijken of het nu echt of fake is.”

Monitoring

Als het lastiger wordt om aanvallers buiten de deur te houden, wordt het belangrijker om maatregelen te nemen die ervoor zorgen dat je ziet als een aanvaller is binnengedrongen, en die de schade daarvan minimaliseren. “Dat moet je dan wel doen op een manier die past bij jouw situatie”, verduidelijkt Theuerzeit. “Bijvoorbeeld met onze monitoringoplossing ‘OT Insight’, juist gebouwd voor de OT-omgeving. Monitoring in een OT-systeem vraagt namelijk om heel andere tools dan monitoring in een IT-systeem.”

Er komt in de watersector ook steeds meer aandacht voor ‘compliance monitoring’. Theuerzeit: “Vooral als je deel uitmaakt van de vitale infrastructuur en je dus moet voldoen aan allerlei wet- en regelgeving, is compliance monitoring een zeer praktische methode om te kunnen bewaken en aan te tonen dat je aan die regelgeving voldoet.” OT Insight is in staat om ook op compliance te monitoren. Aan de basis van compliance monitoring staat een audit, waarna de oplossing in staat is om complianceafwijkingen te detecteren en te rapporteren.

Michael Theuerzeit: “Tot in de boardroom staat het onderwerp cybersecurity nu beduidend vaker op de agenda dan een aantal jaren geleden.”