Normen en richtlijnen brengen waterketen naar hoger niveau

‘Watersector is met forse inhaalslag bezig’

Door Pieter van den Brand

De watersector komt van ver, maar is beslist op dreef om de cyberveiligheid naar een hoger niveau te tillen. Handvatten als implementatierichtlijn CSIR worden breed omarmd, stelt cybersecurity-specialist Michael Theuerzeit van Hudson Cybertec. “Zaak is samen de procesautomatisering in de waterketen digitaal weerbaar te maken.”

Een aantal jaren terug kende de procesautomatisering van de watersector lang niet overal een robuust beveiligingsniveau. In het spraakmakende rapport Digitale Dijkbewaking uit 2019 wees de Algemene Rekenkamer op de gebrekkige digitale weerbaarheid van de processystemen voor waterkeringen. Detectiemaatregelen voor cyberaanvallen ontbraken. Veel ‘stand alone’ systemen stamden nog uit de jaren ’80 en ’90 van de vorige eeuw, met verouderde software die in de huidige tijd met omvangrijke computernetwerken verbonden is om bediening op afstand te faciliteren. De kwetsbaarheid daarvan is groot, oordeelde de Rekenkamer.

De afgelopen vijf jaar heeft de watersector echter een forse inhaalslag ingezet om de cyberweerbaarheid van zijn operationele technologie (OT) op niveau te krijgen, weet lead consultant Michael Theuerzeit van Hudson Cybertec. Dit onderdeel van certificeringsinstantie KIWA is in de cybersecurity van OT-omgevingen van bedrijven gespecialiseerd. “De watersector keek altijd al serieus naar cyberveiligheid, maar nu heeft het onderwerp de hoogste aandacht gekregen.”

Als voorbeeld noemt Theuerzeit het wegwerken van de versnipperde en verouderde ICT bij de waterschappen, de erfenis van de fusiegolf van de afgelopen 25 jaar die tot de huidige 21 organisaties heeft geleid. “Er was een bonte mengeling van systemen met aparte onderhoudscontracten bij een veelvoud aan verschillende leveranciers. Met deze consolidatieslag is veel bereikt, ook voor de cyberveiligheid van systemen.”

De waterschappen hebben inzichtelijk wat ze aan automatiseringssystemen in huis hebben, zo ziet Theuerzeit. De volgende stappen zijn de implementatie van veiligheidsmaatregelen, het opvolgen van beleid, richtlijnen en normen, het doen van risicoanalyses en oefeningen en het opleiden van personeel. “Cybersecurity”, benadrukt hij, “draait om het samenspel van mens, organisatie en techniek. Je moet ze alle drie op orde hebben.”

CSIR

Naast de eigen inspanningen om de cyberveiligheid van hun processystemen te verbeteren, kunnen de waterschappen rekenen op de hulp van Rijkswaterstaat. Voor de digitale beveiliging van haar waterinfrastructuur, zoals bruggen, keringen en sluizen, gebruikt de uitvoeringsorganisatie van het ministerie van Infrastructuur en Waterstaat de in eigen huis ontwikkelde Cybersecurity Implementatierichtlijn (CSIR).

IEC 62443: gerenommeerde industriestandaard voor de OT

De IEC 62443 (inclusief voorganger ISA99) geldt al bijna twintig jaar als internationaal normenkader voor cybersecurity van industriële automatiserings- en controlesystemen. Naast procesautomatisering vallen gebouwgebonden installaties onder deze norm; denk aan beheersystemen voor klimaatbehandeling/airconditioning, toegangscontrole en inbraakbeveiliging. Het normenkader bestaat naast de norm zelf uit technische rapporten en gerelateerde informatie en bevat onderdelen voor eindgebruikers, system-integrators en leveranciers, zodat de hele keten hetzelfde normenkader kan gebruiken. Een gremium van experts uit het veld is betrokken bij de verdere ontwikkeling van de norm. Organisaties kunnen zich laten certificeren, om te aan tonen dat ze aan deze OT-cyberveiligheidsnorm voldoen. Hudson Cybertec speelt al jaren een actieve rol in de ontwikkeling van de IEC 62443. Specifiek hiervoor is het trainingsprogramma ‘Cybersecurity voor OT’ ontwikkeld, bedoeld om de norm beter te begrijpen en in de dagelijkse praktijk toe te passen. Daarnaast heeft het bedrijf een praktische workshop opgezet voor bedrijven die aan de slag willen met de CSIR en de BIACS (kort voor Basismaatregelen voor cybersecurity van Industriële Automatisering & Controle Systemen, een opstap naar de complexere CSIR).

Deze richtlijn is afgeleid van de Baseline Informatiebeveiliging Overheid (BIO) en aangevuld met beheersmaatregelen uit industriestandaard IEC 62443 (zie kader), om dekkend te zijn voor de beveiliging van procesautomatisering. Een belangrijk doel van de CSIR is de garantie dat wat Rijkswaterstaat bij de procesautomatisering van objecten aan veiligheidseisen stelt, bij aanbestedingen door ICT-leveranciers wordt geleverd.

Bij versie 3.0 van de CSIR kregen Rijkswaterstaat en Het Waterschapshuis, de ICT-organisatie van de waterschappen, ondersteuning van Hudson Cybertec bij het actualiseren en veralgemeniseren van de richtlijn. “Hierdoor is de CSIR breder inzetbaar en kunnen ook de waterschappen de richtlijn gebruiken om bijvoorbeeld hun waterzuiveringsinstallaties en gemalen digitaal te beveiligen”, zegt Theuerzeit.

De waterschappen hebben volgens de cyberveiligheidsexpert een belangrijke stap gemaakt door expliciet aan te geven dat ze de CSIR gaan hanteren. “Het ene waterschap is daar verder mee dan het andere. Dat is nou eenmaal altijd zo. Toe te juichen is dat deze richtlijn nu breed wordt omarmd. Al moeten er keuzes worden gemaakt. Zoiets kun je niet in één keer doen. Afvalwaterzuiveringen en boezemgemalen zijn belangrijke installaties om te beveiligen, en je ziet dat daar als eerste mee begonnen wordt. Doorgaans is er sprake van langlopende onderhoudscontracten voor systemen tot tien jaar en langer. Die wil je tussentijds niet gaan openbreken, want dan betaal je de hoofdprijs. Pas bij een verlenging of een nieuw contract kun je plek voor de CSIR inruimen.”

Michael Theuerzeit (Hudson Cybertec): “Cybersecurity binnen de OT is echt heel anders dan binnen de IT.”

Waterschappen zullen de richtlijn dan ook geleidelijk aan gaan implementeren, voorziet Theuerzeit, maar steeds meer processystemen zullen op den duur naar een hoger weerbaarheidsniveau toegaan. “Er worden beslist flinke stappen vooruit gezet, maar het blijft een meerjarenplan.”

OT versus IT

Met de CSIR bestaat er nu een cyberbeveiligingskader voor de OT-omgeving van de waterschappen. Onder de vlag van brancheorganisatie Vewin is voor de drinkwatersector eerder de PA-beveiligingsnorm voor procesautomatisering opgesteld, die grotendeels leunt op IT-certificeringsnorm ISO 27001. Theuerzeit wil benadrukken dat bedrijven geen water bij de wijn moeten doen door het bij ISO 27001 te laten. “Essentieel is dat het beveiligingskader zo goed mogelijk aansluit bij het te beschermen belang. Kies een kader dat het beste past. Cybersecurity binnen de OT is echt heel anders dan binnen de IT. Het vraagt om een eigen aanpak met een passend cybersecuritykader.”

Er zijn namelijk belangrijke verschillen, aldus Theuerzeit. “Binnen de IT-omgeving is vertrouwelijkheid van gegevens essentieel, terwijl binnen de OT aspecten als integriteit en beschikbaarheid voorop staan, omdat deze een grote rol spelen bij onder meer gezondheid, veiligheid en milieu. Dit maakt het noodzakelijk om cyberveiligheid integraal vanuit beide domeinen te bekijken.”

Waterketen

Een tweede cruciaal punt, stelt Theuerzeit, is de volledige waterketen cyberweerbaar te maken. Een van de eisen vanuit de Europese cyberveiligheidsrichtlijn NIS2 - medio volgend jaar in ons land van kracht - is ketenaansprakelijkheid. “Gemeenten zijn verantwoordelijk voor het eerste stuk van het rioolstelsel. Dit deel van de infrastructuur met zijn rioolgemalen en pompen is digitaal net zo kwetsbaar als de procesautomatisering van de waterschappen. Aan het eind van de rioolwaterzuivering gaat het gezuiverde afvalwater als effluent naar het oppervlaktewater. De drinkwaterbedrijven gebruiken dat voor hun leidingwaterproductie. Zij worden steeds afhankelijker van oppervlaktewater, aangezien er steeds meer grenzen worden gesteld aan het onttrekken van water uit de bodem. Al deze stappen in de keten sluiten nauw op elkaar aan. Als het bij de gemeenten niet goed zit, kunnen de waterschappen niets meer. Als het bij de waterschappen niet goed zit, is er te weinig betrouwbaar water in de rivieren om voldoende drinkwater te maken. Wat ik vooral wil zeggen is dat er in de hele waterketen op het vlak van cybersecurity goed afgestemd moet worden. Deze drie partijen gebruiken eigen richtlijnen en normen, al zijn er gemeenten die nu ook naar de CSIR kijken. Zaak is samen de processen in de waterketen weerbaar te maken. Cyberveiligheid is zo sterk als de zwakste schakel.”