Cybersecurity

Update Cybersecurity Implementatierichtlijn

De watersector wordt digitaal weerbaar

Door Annemarie Jansen

De watersector is zich de afgelopen jaren steeds bewuster geworden van het belang van digitale weerbaarheid. Daarbij is niet alleen aandacht voor de IT-aspecten die een weerslag hebben op de kantoorautomatisering, maar juist ook in toenemende mate voor de weerbaarheid van de procesautomatisering.

De uitdagingen waarmee de verschillende organisaties in de watersector te maken krijgen, zijn heel divers en in grote mate afhankelijk van de wijze waarop de procesautomatisering (PA) is ingericht en hoe deze is gescheiden van de kantoorautomatisering (KA). Beide domeinen kennen hun eigen specifieke uitdagingen en vragen daardoor om een andere aanpak en oplossingen. Dat begint al bij het beveiligingskader dat wordt toegepast.

Meerdere kaders

Sinds een aantal jaren kent de overheid de Baseline Informatiebeveiliging Overheid (BIO). Voor waterschappen was dit de vervanger van de Baseline Informatiebeveiliging Waterschappen (BIWA). Waar deze kaders uitstekend helpen om de digitale weerbaarheid voor de KA op gestructureerde wijze te managen, voorzien ze niet in de specifieke behoeften van de PA.
Zo'n tien jaar geleden ontwikkelde Rijkswaterstaat daarom een eigen kader om in die specifieke behoefte te voorzien. Dit kader is de Cybersecurity Implementatierichtlijn (CSIR). De CSIR had zijn oorsprong in de Baseline Informatiebeveiliging Rijk (BIR), die net als de BIWA en ook de BIG (Baseline Informatiebeveiliging Gemeenten) en IBI (Interprovinciale Baseline Informatiebeveiliging) zijn opgegaan in de BIO. Om de CSIR te laten aansluiten bij de vereisten uit de BIO en deze volledig te updaten, heeft Rijkswaterstaat nauw samengewerkt met Hudson Cybertec, cybersecurity solution provider voor de Operationele Technologie. Michael Theuerzeit, lead consultant bij Hudson Cybertec: "Tegelijk met de actualisatie ten aanzien van de BIO, zijn ook maatregelen uit de IEC 62443 meegenomen en is gezorgd dat ook andere kaders geborgd zijn. Zo hebben we samen met Rijkswaterstaat ervoor gezorgd dat de CSIR weer helemaal actueel is."

Cybersecurity Implementatierichtlijn

Dit heeft geleid tot versies 2.0 en 2.4 van de CSIR voor Rijkswaterstaat. Beide versies zijn opgebouwd rondom een set van proces- en systeemeisen. Deze eisen zijn integraal onderdeel van de 2.0-versie en onderdeel van de contracteisen bij de 2.4-versie, zodat opdrachtnemers deze kunnen implementeren als onderdeel van eenopdracht. Daartoe zijn de eisen ook opgenomen in de Inkoopeisen Cybersecurity Overheid Wizard (ICO Wizard). Beide versies bevatten de maatregelensets die zijn gebouwd rond de tien thema's, met daarbij een aantal bijlagen die een nadere 'best practice'-uitwerking geven op specifieke onderdelen.

Sinds enige tijd zijn er zelfs de CSIR 3.0 en 3.4 die de watersector helpen om de digitale weerbaarheid van de PA-omgeving op gestructureerde wijze te managen. Deze versies zijn een doorontwikkeling van de Rijkswaterstaatversies, geschikt gemaakt voor een breder publiek. Bij de ontwikkeling van versie 3.x heeft het Waterschapshuis de expertise van Hudson Cybertec ingeroepen en is met Rijkswaterstaat en de waterschappen samengewerkt om te komen tot een breed gedragen versie, die voor alle partijen leesbaar, begrijpelijk en toepasbaar is.

Sinds de afronding van de laatste versie wordt er gewerkt aan een toelichting op de CSIR, met daarin een operationele uitwerking van verschillende thema's. In deze toelichting worden voor een aantal thema's invulling van cybersecurity en operationele beheerprocessen uitgewerkt en toegelicht.

Dit maakt het makkelijker voor de betrokken partijen om de CSIR toe te passen binnen hun organisatie.

Laaghangend fruit

Zowel Rijkswaterstaat als waterschappen kennen een groot areaal van objecten, die in verschillende fasen van hun levenscyclus zitten. Sommige objecten zijn net nieuw, terwijl andere objecten al jaren worden gebruikt en bijna aan de beurt komen voor groot onderhoud en een technologie-update. Hoe langer het nog duurt voordat een bestaand onderhoudscontract voor een object afloopt, hoe lastiger het is om nu al alle maatregelen te nemen om het object volledig in lijn te brengen met de vereisten uit de CSIR.

"Het is van belang te focussen op die maatregelen die wel alvast redelijk eenvoudig kunnen worden doorgevoerd, het zogenaamde laaghangend fruit", geeft Theuerzeit aan. "Vaak zijn dit maatregelen van organisatorische oorsprong, waarmee procedureel zaken worden afgedwongen, maar soms ook technische maatregelen die geen directe impact hebben op het primaire proces."

Tweeledige opzet

Zo helpt de toelichting met operationele werkwijzen de waterschappen enerzijds met het toepassen van de CSIR vóóraf. Anderzijds helpt de toelichting met het geven van concrete invulling aan operationele beheerprocessen.
Een van de belangrijke thema's die hierbij besproken wordt, is het managen van kwetsbaarheden. Hierbij wordt een uniforme aanpak besproken, waarmee organisaties meteen uit de voeten kunnen. Het hele proces wordt uitgebreid behandeld en kan kant en klaar worden geïmplementeerd.

Digitaal weerbaar

Met de nieuwe CSIR-versies hebben, naast Rijkswaterstaat en de waterschappen, ook andere partijen een cybersecuritykader specifiek voor de PA in handen. Michael Theuerzeit besluit: "De CSIR helpt hen om de kwetsbare PA-omgevingen risicogestuurd digitaal weerbaar te maken."

Meer weten over de CSIR?

www.hudsoncybertec.com/trainingen/csir-workshop/