Watermanagement en cybersecurity-management

Cybersecurity is ook voor de waterwereld een belangrijke zaak. Veel waterschappen zijn druk bezig om het cybersecurityniveau omhoog te krijgen. Men moet voldoen aan de BIWA-norm en ook de cybersecuritywet komt in grote vaart op ons af. Hoe gaan waterbedrijven om met cybersecurity?

Hudson Cybertec, wereldwijde cybersecurity solution provider voor de Operationele Technologie (OT), ziet dat veel bedrijven in de watersector nog worstelen met het op orde krijgen van cybersecurity voor de primaire processen. Vaak ontbreekt het aan voldoende kennis over cybersecurity, waardoor er geen afdoende beleid is en OT netwerken vooral nog op functionaliteit gericht zijn. "Cybersecurity wordt nog onvoldoende gemanaged", zegt Marcel Jutte, managing director bij Hudson Cybertec, "We spreken zeer regelmatig met verschillende bedrijven uit de watersector en zien dat er grote behoefte is aan hulp."

Breng structuur

Een gestructureerde aanpak is hierbij noodzakelijk. Zomaar links en rechts wat zaken op gebied van security oppakken en verbeteren brengt geen structuur en is op lange termijn niet te managen. Om een eerste stap te kunnen maken in cybersecurity en verbeteringen door te kunnen voeren, is het van belang te weten waar de organisatie vandaag staat. Een security assessment geeft een duidelijk overzicht van de huidige stand van cybersecurity. Hierbij dienen alle belangrijke factoren te worden meegenomen. Er is dus aandacht nodig voor mens, organisatie en techniek. Jutte: "Wij hebben veel ervaring met security assessments, waarbij gemeten wordt tegen de IEC 62443. Hierbij komen alle drie de factoren uitgebreid aan bod. Klanten zien dat zij, door onze holistische benadering, op meerdere fronten tegelijk een grote slag kunnen maken in het verbeteren van cybersecurity."

IEC 62443

De IEC 62443 is de wereldwijde de facto norm voor cybersecurity voor Industrial Automation & Control Systems (IACS), ofwel het OT domein. Een security assessment uitgevoerd volgens deze norm maakt op eenduidige wijze inzichtelijk op welke vlakken het waterschap maatregelen moet nemen. Zo bracht een assessment, uitgevoerd bij een waterschap, duidelijk naar voren dat er een zeer lage overeenstemming was met de IEC 62443. Op zich niet vreemd omdat de organisatie nog niet bezig was met het normenkader. Wat wel meteen duidelijk werd, was de grote winst die de organisatie kon behalen op alle vlakken, zowel op organisatorisch, als technisch en personeel gebied.

Slimme keuzes

Door het maken van slimme keuzes was het voor het waterschap mogelijk om met een beperkt budget toch een aantal belangrijke stappen te nemen op gebied van cybersecurity. Op advies van Hudson Cybertec is een keuze gemaakt om te beginnen met het actualiseren van het securitybeleid en het toepassen van netwerksegmentatie, volgens het zone & conduit model van de IEC 62443. De komende jaren kunnen nieuwe keuzes worden gemaakt, waarbij eerdere keuzes gemanaged blijven.

Pentest van de OT

Elk bedrijf in de waterwereld is toch weer uniek. Daardoor verschilt ook de aanpak. Bij een ander waterbedrijf werd een combinatie van verschillende pentesten uitgevoerd om aan te tonen hoe kwetsbaar de OT infrastructuur is. Tijdens deze gecontroleerde pentesten, op verzoek van het waterbedrijf uitgevoerd in de live omgeving, werden al heel snel een aantal kwetsbaarheden gevonden. Jutte: "Omdat iedereen binnen de OT organisatie was geïnformeerd en stand-by stond, was het mogelijk om in de productieomgeving zelf te pentesten. Doelstelling was om te zien of binnendringing in de systemen mogelijk was. Daarbij zijn verschillende serieuze kwetsbaarheden gevonden." Op basis daarvan zijn aanbevelingen gedaan en is er direct actie ondernomen om cybersecurity te verbeteren.

IACS forensic readiness

Bedrijven moeten voorbereid zijn voor als een incident gebeurt. Ze dienen te allen tijde inzicht te hebben in wat er op het netwerk aan de hand is. Het belang van forensische data wordt dan ook binnen de IACS (OT) omgeving steeds groter. De aankomende cybersecuritywet maakt het noodzakelijk dat partijen zaken inzichtelijk kunnen maken. Het is belangrijk om daarop voorbereid te zijn. IACS Forensic Readiness zorgt ervoor dat organisaties bij een incident de gegevens die noodzakelijk zijn voor een forensisch onderzoek kunnen veiligstellen. Bijvoorbeeld om de oorzaak van een incident te kunnen vaststellen of eventuele veroorzakers te achterhalen. "Vanuit andere vitale sectoren krijgen we veel vragen om hierbij onze expertise te verlenen" geeft Jutte aan, "Ook in de waterwereld zien we de vraag om forensic readiness nu toenemen." Hierbij valt te denken aan het preventief inrichten, onderhouden en exploiteren van de noodzakelijke infrastructuur voor o.a. incident response, monitoring en detectie, logging en het beheer en onderhoud van back-ups.

Managed services

Hudson Cybertec neemt daarbij zoveel mogelijk zorg uit handen. "Onze opdrachtgevers zijn onze partners. Door onze vertrouwensband met onze partners zijn we in staat ze volledig te ontzorgen", vervolgt Jutte, "Onze managed services hebben tot doel cybersecurity zo toegankelijk en laagdrempelig mogelijk te maken." Bedrijven waarbij watermanagement of drinkwater de core business is, kunnen zo de focus houden op hun primaire proces.

Daarbij profiteren ze van het specialisme van Hudson Cybertec, cybersecurity voor de Industriële Automatisering & Control Systems. Terwijl de vraag vanuit de markt in zijn algemeenheid toeneemt, ziet Jutte ook vanuit de watersector steeds meer behoefte voor specialistische ondersteuning: "Door onze ervaring weten we heel goed wat er speelt binnen de OT omgevingen van de drinkwaterbedrijven en waterschappen, alsook de securityuitdagingen waarmee ze te maken hebben. Dit, gecombineerd met onze expertise in cybersecurity voor het OT domein, zorgt ervoor dat waterbedrijven ons vragen om hen daarbij te helpen. We ontzorgen waterbedrijven door cybersecurity voor hen te managen. Het watermanagement echter, laten we aan hen zelf over."