Cybersecurity binnen OT: geen water bij de wijn

Door Michael Theuerzeit, lead consultant Hudson Cybertec

Nederland heeft als waterland een aantal evidente belangen: hoe houden we onze voeten precies droog genoeg, hoe zuiveren we afvalwater zodat het schoon genoeg is om opgenomen te worden in de natuur, hoe zorgen we voor veilige waterwegen en hoe borgen we voldoende en veilig drinkwater? Vier compleet verschillende vraagstukken die voortkomen uit verschillende ketens, maar toch een heleboel verbinding met elkaar hebben. Niet alleen binnen de waterketen zelf, maar ook op het gebied van cybersecurity.

Rijkswaterstaat, waterschappen en drinkwaterbedrijven worstelen elk met hun unieke uitdagingen met betrekking tot het water. Net als provincies en gemeenten die hierin ook een eigen rol hebben. In de uitdagingen waarvoor ze staan op het gebied van hun digitale weerbaarheid, is er echter een grote overlap. Ze hebben te maken met dezelfde dreigingsactoren, wet- en regelgeving en alle kennen cybersecurityrisico's met een mogelijk grote impact op de samenleving.

Cybersecuritywetgeving

Hudson Cybertec ondersteunt als cybersecurityspecialist voor de Operationele Technologie (OT) veel van deze partijen en ziet dat de digitale weerbaarheid van de objecten binnen deze organisaties ook serieus wordt genomen. Deze organisaties hebben een focus op de cybersecurity van hun OT. Met de aanscherping van de NIS2 die vanuit Europees verband de cybersecurityteugels aantrekt, wordt het steeds belangrijker te voldoen aan de cybersecuritywetgeving. Het draait daarbij niet alleen om het melden van incidenten, maar juist ook om het aantoonbaar 'in control' te zijn - de zorgplicht uit de NIS2.

Om eenvoudig aan te kunnen tonen dat een organisatie in control is, is het van belang cybersecurity op gestructureerde wijze te managen. Cybersecuritynormen en richtlijnen helpen hierbij. Zo kent Rijkswaterstaat al zo'n tien jaar de Cybersecurity Implementatierichtlijn Objecten (CSIR), welke onlangs samen met Hudson Cybertec nog volledig werd geactualiseerd, zodat deze weer volledig aansluit bij de actualiteit. Inmiddels hebben ook waterschappen afgesproken zich te gaan conformeren aan de CSIR en is er ook vanuit provincies en gemeenten steeds meer interesse voor dit kader. Hudson Cybertec hiervoor heeft een training ontwikkeld.

Normenkader

Daarnaast is er natuurlijk de IEC 62443, de internationale norm voor cybersecurity van industriële automatisering en controlesystemen. Dit normenkader is specifiek ontwikkeld voor de OT en kent delen voor eindgebruikers, system integratoren en leveranciers, zodat de hele keten hetzelfde normenkader kan gebruiken. Welk kader een organisatie ook kiest, het is essentieel dat dit aansluit bij het te beschermen belang. Doe als organisatie nooit water bij de wijn door een kader te kiezen dat eigenlijk niet past, zoals bijvoorbeeld de ISO 27000, simpelweg omdat men deze al binnen de kantooromgeving gebruikt. Cybersecurity binnen OT is echt anders dan binnen IT. Het vraagt om een eigen aanpak, met specialisten uit de OT én met een passend cybersecuritykader.

www.hudsoncybertec.com