Auteur: Henriëtte van Norel

Tunnels hangen vol met digitale systemen die zorgen voor de veiligheid van de tunnelgebruikers.

Digitale componenten cyberveilig ontwikkelen

Cybersecurity in de keten

Bij het cyberveilig maken van een organisatie wordt veelal gedacht aan het cyberweerbaar maken van administratieve omgevingen. Dit is echter nog maar de helft van het werk. Minstens zo belangrijk is het volgens Lead Consultant Michael Theuerzeit van Hudson Cybertec en Jean-Paul Sablerolle, Managing Director bij Hudson Cybertec, om ervoor te zorgen dat ook alle digitaal gekoppelde componenten op het OT-netwerk cyberveilig zijn ontwikkeld, geïnstalleerd en geconfigureerd. Ofwel dat de juiste organisatorische en technische maatregelen zijn genomen conform deel 4-1 en 4-2 van de IEC62443, een internationaal normenkader voor cybersecurity in de industriële OT-omgeving (lees: Operationele Technologie) en CSIR voor natte en droge infra.

Sablerolle: “Fabriekseigenaren en de grotere toeleveranciers in de (petro-)chemie, de olie- en gaswereld en de wereld van infra (lees: waterbouwkundige bewegingswerken, bruggen en sluizen en verkeerssystemen) werken al geruime tijd conform de IEC62443 of de CSIR (Cyber Security Implementatie Richtlijn), omdat zij vanuit NIS al langere tijd moeten voldoen aan de op komst zijnde NIS2-wetgeving die binnenkort voor veel meer bedrijven van toepassing is. Als geen ander weten deze grote organisaties welke organisatorische en technische maatregelen er genomen dienen te worden om te allen tijde te kunnen aantonen dat zij digitaal weerbaar zijn. Zo wordt in deze norm onder andere beschreven hoe risico-analyses dienen te worden uitgevoerd, welke eisen er gesteld dienen te worden aan ‘system integrators’ waarmee zij nauw samenwerken en waaraan de producten van componentleveranciers moeten voldoen. Denk daarbij

aan leveranciers van industriële automatiseringscomponenten en andersoortige elektronische componenten die op enigerlei wijze digitaal gekoppeld zijn aan OT-netwerken in bedrijven, bijvoorbeeld leveranciers van SCADA- en PLC-systemen. Ook dergelijke componenten moeten cyberveilig worden ontwikkeld."

'Monitoring is 'key"

Installateurs

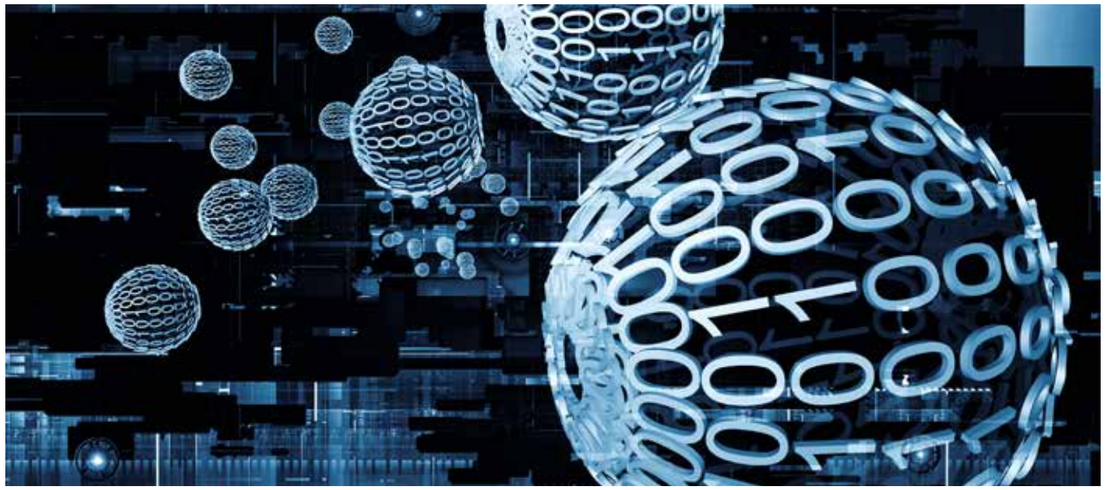
Wat al 'normaal' is voor fabriekseigenaren en grotere toeleveranciers op het gebied van cyberveilig ontwikkelen, dat geldt zeker nog niet voor 'system integrators' en installateurs. Volgens Theuerzeit ontbreekt het zeker de laatstgenoemde groep, de installateurs, vaak aan kennis op bovengenoemd gebied. "Ze gebruiken dan wel IEC62443-gecertificeerde componenten, maar dat is nog geen garantie dat deze op de juiste wijze zijn geïnstalleerd en geconfigureerd. Zo komen in de praktijk ook gebouwgebonden systemen, camerasystemen, sprinklerinstallaties en alarminstallaties vaak allemaal terecht op het OT-netwerk, waar ook de rest van een fabriek of infrasysteem op draait. Als dat niet goed wordt gesegmenteerd en niet digitaal weerbaar in elkaar wordt gesleuteld, dan worden daar lekken geïntroduceerd en dus problemen." Omdat het op dat gebied nog regelmatig mis gaat, is het volgens Theuerzeit noodzaak voor installateurs om een certificatiesysteem op te zetten. Hij maakt de vergelijking met autogordels. "Een voertuig kan dan wel uitgerust zijn met gecertificeerde autogordels. Deze gordels zijn pas veilig als ze ook daadwerkelijk op de juiste wijze worden bevestigd. Met cybersecurity werkt het eigenlijk op exact dezelfde manier."

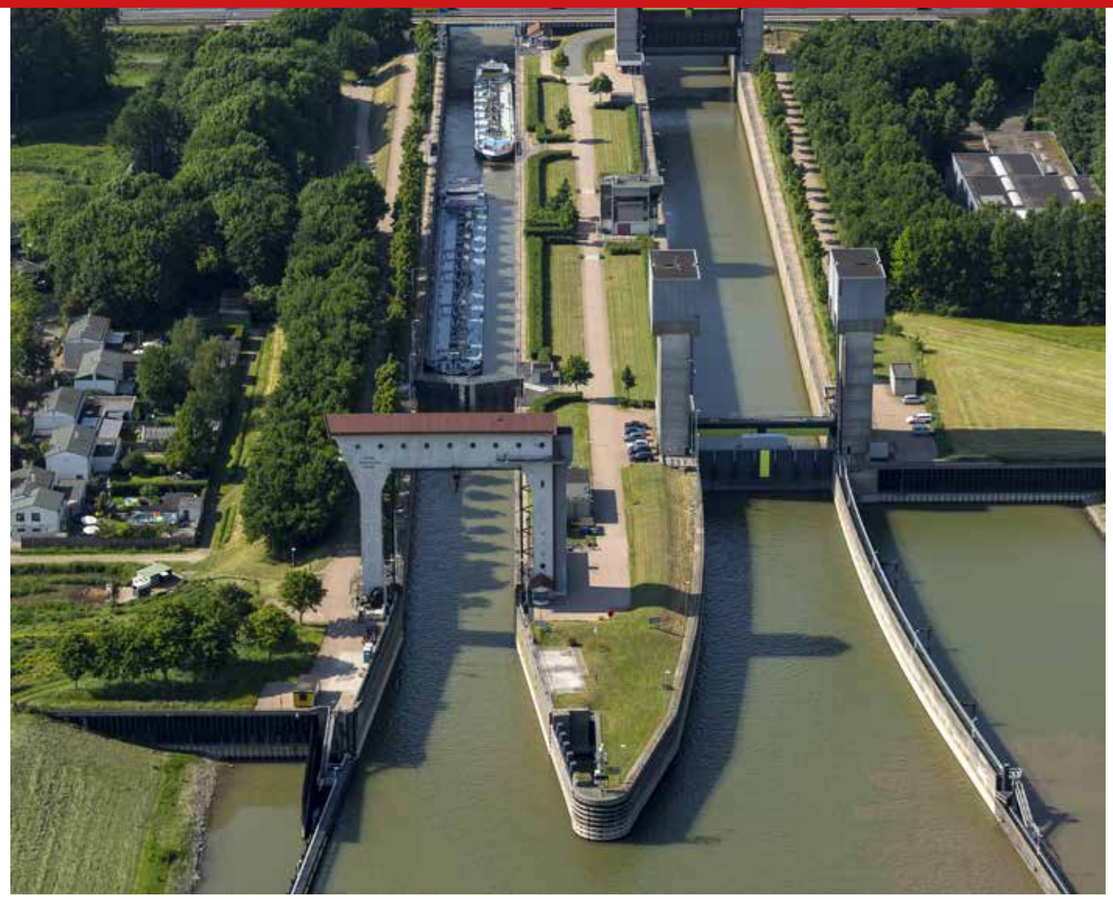
Keurmerk installateurs

Michael Theuerzeit, Lead Consultant bij Hudson Cybertec en lid van de OT-werkgroep van het Centrum voor Criminaliteitsbestrijding en Veiligheid (CCV): "Om het bovenstaande probleem te ondervangen is CCV momenteel druk doende met het opzetten van een keurmerk. Een keurmerk in het bijzonder voor MKB'ers, zodat ook kleinere installateurs kunnen aantonen dat ze vakvolwassen zijn en cyberveilig kunnen installeren. Bovengenoemde werkgroep bestaat uit 'asset owners' (vertegenwoordigers van (petro-)chemische bedrijven) die al langere tijd bezig zijn met OT-security in hun fabrieken, leveranciers van componenten als PLC's en SCADA-systemen, 'system integrators' en consultancypartijen zoals Hudson Cybertec. In totaal zo'n 20-tal mensen uit de praktijk. Het doel van deze werkgroep is om eind volgend jaar een keurmerk te lanceren voor enerzijds de installateurs en anderzijds de kleine maakindustrie. Met dit keurmerk kunnen deze partijen aantonen dat ze alle noodzakelijke technische en organisatorische basismaatregelen hebben genomen en dus voldoen aan het keurmerk, zodat ze daarmee bijvoorbeeld korting kunnen krijgen op een cybersecurity-verzekering.

Geopolitieke omstandigheden

Een keurmerk in het leven roepen en het afsluiten van een cybersecurity-verzekering zijn zeker gezien de geopolitieke spanningen die er momenteel zijn in de wereld geen overbodige luxe meer. Denk maar eens aan de Russen, andere statelijke actoren zoals China en Noord-Korea en de zogeheten 'frenemies' (lees: landen die ons goed gezind zijn, maar toch stiekem bij andere landen in de keuken willen kijken). Een illustratief voorbeeld hiervan was Belgacom een aantal jaren geleden, toen Engeland België bespioneerde. Infra is zeker met deze geopolitieke omstandigheden een interessante plek om te zijn. Het is namelijk dé manier bij uitstek om een land te ontwrichten, verkeerspleinen en stoplichten plat te leggen, bruggen open te zetten en tunnels af te sluiten. Kortom





Sluiscomplexen zijn een cruciale schakel in het waterbeheer en moeten digitaal weerbaar zijn.

om een verkeersinfarct te creëren. Het is een illusie om te denken dat de statelijke actoren niet reeds in onze systemen zitten. Cruciaal om dit in de grip te houden is dus om het goed te monitoren. Blijf derhalve goed in de gaten houden welke bewegingen er op het OT-netwerk zijn en welke afwijkingen er zijn in het normale digitale verkeer. In een OT-omgeving is dit vaak makkelijker te zien, vanwege een zekere mate van voorspelbaarheid. Denk maar eens aan tunnelsystemen, brand- en verlichtingsinstallaties, slagbomen etc. Niet voor niets heeft Rijkswaterstaat (RWS) een overkoepelend netwerk waarop zij 24/7 met een 'security operation center' (SOC) toezichthouden. De snelweg in Nederland is namelijk opgedeeld in delen. Sommige delen zijn eigendom van RWS, andere delen zijn in handen van de provincie of de gemeente. Voor het beheer en het onderhoud werken al deze eigenaren met eigen systemen, die wel door RWS allemaal gemonitord worden.

Ieders verantwoordelijkheid

Sablerolle vult aan: "Dat laat maar weer eens duidelijk zien dat iedereen in een organisatie verantwoordelijk is voor cybersecurity. Ook als je een tunnel, brug of fabriek ontwerpt. In alle gevallen is het essentieel om reeds in een vroeg stadium maatregelen op te nemen die ervoor zorgen dat het uiteindelijke bouwwerk digitaal weerbaar is, zodat alle partijen in de keten hun verantwoordelijkheid daarin kunnen nemen. Is een fabriek of waterbouwkundig bewegingswerk eenmaal in gebruik genomen, dan is het zaak dat de operators hun verantwoordelijkheid op dit gebied nemen. In alle gevallen is het dus cruciaal om bij elk nieuw project alle betrokkenen te informeren over de rol die ze hierin hebben en de dreigingen die op de loer liggen, zodat iedereen in de keten zijn/haar verantwoordelijkheid kan nemen. Iedereen een bewustwordingstraining laten volgen is dan ook zeker aan te bevelen."

Bewustwordingstraining

Op de vraag voor wie zo'n bewustwordingstraining dan interessant is, antwoordt Theuerzeit: "Eigenlijk voor iedereen, van het topmanagement tot de operator en de schoonmaker op de werkvloer. Het is voor iedereen belangrijk om te weten wat digitale weerbaarheid is binnen de operationele technologie en om te begrijpen hoe zij daar als persoon een rol in spelen. Hoewel veel grote ondernemingen hiermee reeds gestart zijn, is het van belang dat ze dit ook blijven doen en dat ook kleinere ondernemingen hiermee aan de slag gaan. In alle gevallen dient te worden voorkomen dat componenten op afstand gemanipuleerd kunnen worden. Of het nu gaat om een waterbouwkundig bewegingswerk of een fabriek. Als al deze partijen in de nabije toekomst een certificaat van CCV hebben of op een andere wijze kunnen aantonen dat ze vakvolwassen zijn, dan is dat een goede stap op weg naar het cyberveiliger maken van Nederland."