Wendy Kloeg, divisiemanager Bedrijfsvoering en Klant Dunea.

ISIDOOR in de praktijk: Dunea

Zelfde cyberdreiging kan voor elk drinkwaterbedrijf anders uitpakken

Drinkwaterbedrijf Dunea deed voor de derde keer mee met ISIDOOR. Divisiemanager Bedrijfsvoering en Klant Wendy Kloeg vertelt hoe de oefening verliep en welke lessen zijn geleerd.

Kloeg: 'Organisaties kunnen op verschillende niveaus meedoen aan ISIDOOR. Wij hebben voor het niveau 'Goud' gekozen, omdat je dan kunt meedenken over het scenario en je eigen oefendoelen kunt bepalen. Op die manier kan ieder bedrijf eruit halen wat ze zelf willen oefenen.'

Het oefenscenario

'In onze casus waren er wereldwijd in diverse systemen kwetsbaarheden ontdekt in software voor procesautomatisering (PA), die waarschijnlijk via malware waren verspreid. Volgens het oefenscenario waren er de afgelopen tijd problemen in onze eigen PA, waardoor de aanname was dat ook onze PA-systemen waren besmet. We hebben daarom geoefend wat het betekent om de procesautomatisering op alle Dunea-locaties opnieuw in te richten.'

'Tijdens de oefening hadden we intensieve afstemming met vele betrokken partijen, zoals Vewin, het Water Information Sharing and Analysis Center (WaterISAC), het Nationaal Cyber Security Centrum (NCSC) en de Incident Response Board (IRB). Vanuit deze organisaties lopen ook communicatielijnen met de nationale crisisstructuur.'

Eigen oefendoelen bepalen

'Omdat de situatie bij elk drinkwaterbedrijf anders is, hebben wij nadrukkelijk onze eigen specifieke oefendoelen bepaald. Zo wilden wij nauwkeurig in kaart brengen hoe in een (dreigende) crisissituatie de onderlinge samenwerking is tussen de collega's van de procesautomatisering en de uitvoerders van onze primaire productieprocessen.'

‘Ook wilden we onze back-upsystemen testen en oefenen met het installeren van nieuwe software en opstarten van de processen vanaf verschillende devices. Het gaat daarbij niet alleen om voldoende ICT-kennis, maar ook of alle betrokken collega’s voldoende weten van het proces van drinkwaterproductie. De kennis van dit primaire proces is essentieel, zeker als je bijvoorbeeld over moet gaan op handbediening, omdat alle automatisering is uitgeschakeld.’

‘Onze medewerkers hebben voor deze situaties uitgebreide draaiboeken en protocollen, die ze nauwkeurig volgen. Dit wordt tijdens de oefening gevolgd door neutrale auditors, die een evaluatie opstellen van wat zij zien en horen. Wat daarbij opviel, is dat het nog niet eenvoudig is om richting externe crisispartners in begrijpelijke taal te beschrijven wat er eigenlijk in het primaire proces gebeurt en wat de gevolgen daarvan kunnen zijn voor de continuïteit van de drinkwatervoorziening.’

Hoe verliep de samenwerking binnen de drinkwatersector en met externe partijen, zoals het NCSC?
Kloeg: ‘De samenwerking met de andere drinkwaterbedrijven verliep prima. Ook de formele communicatie- en informatielijnen met de overheid functioneerden goed. De ondersteuning vanuit het NCSC was duidelijk beter dan in het verleden.’

Sectorbeeld

‘We hebben deze keer geoefend om snel een sectorbreed beeld boven water te krijgen over wat er speelde, in nauwe samenwerking met Vewin en het WaterISAC. Zo vergroten we de cyberweerbaarheid, omdat snel duidelijk is of bepaalde problemen elders wel of niet spelen en in welke mate de drinkwaterbedrijven elkaar kunnen helpen, bijvoorbeeld met steunleveringen. Verder maken wij als Dunea gebruik van een extern Security Operations Center (SOC), dat onze netwerken permanent monitort en bepaalde opvallende zaken rondom het dataverkeer met ons deelt. Hiermee kunnen we de aard en omvang van een hack beter en sneller duiden.’

‘IEDER DRINKWATERBEDRIJF HEEFT ZIJN EIGEN DRINKWATERSYSTEEM’

‘Elk drinkwaterbedrijf heeft andere systemen en kent andere maatregelen om op bepaalde gebeurtenissen te reageren. Wat voor de één grote gevolgen kan hebben, kan voor de ander nauwelijks een probleem vormen. Dit heeft te maken met de inrichting van het productieproces en van de procesautomatisering. Bijvoorbeeld omdat het ene bedrijf drinkwater maakt van oppervlaktewater en het andere van grondwater. Ook de precieze manier waarop de procesautomatisering is georganiseerd, op basis van welke concepten en systemen, speelt natuurlijk een rol.’

Wat waren de leerpunten bij Dunea?
Kloeg: ‘Belangrijke les bij ons was – zoals gezegd – dat het nog best lastig is om richting externe crisispartners in heldere (niet al te technische) taal uit te leggen hoe het concept van onze procesautomatisering in de praktijk werkt, wat er eventueel fout kan gaan (of juist niet) en wat daarvan de gevolgen zijn. Daar moeten we nog meer rekening mee houden in bijvoorbeeld de externe communicatieplannen. Een aandachtspuntje daarbij zijn ook de vele – vaak Engelstalige – afkortingen, die het voor anderen niet makkelijk maken om te snappen wat we bedoelen.’

‘We hebben gezien dat – als je goed wil oefenen – er voldoende capaciteit moet zijn gereserveerd, zowel qua menskracht als qua hardware. Dat moet dus goed zijn vastgelegd in de jaarplannen.’

‘De oefening betrof deze keer een combinatie van ransomware en datadiefstal. Wij hebben wederom vastgesteld dat het noodzakelijk is om goed op de hoogte te blijven van deze nieuwe vormen (of combinaties) van cybercriminaliteit, en onze maatregelen continu te actualiseren.’

‘KENNIS VAN DE PRIMAIRE PROCESSEN IS ESSENTIEEL’

Oefent Dunea ook zelf op het gebied van cybersecurity, los van deze landelijke oefeningen?
Kloeg: ‘Wij hebben een kalender voor alle mogelijke crisisoefeningen, waaronder uiteraard cyberveiligheid. Bepaalde cybersecurityoefeningen, zoals rondom handbediening en proceskennis, doen we elk jaar. Daarnaast hebben we voor de gehele organisatie een permanent awareness-programma op het gebied van cybersecurity. Ook hebben de drinkwaterbedrijven samen met het ministerie van IenW een serious game ontwikkeld, waarin we meerjarig verschillende scenario’s kunnen oefenen, op alle lagen binnen het bedrijf.’

Hebben jullie nog wensen als het gaat om oefenen met de overheid?
Kloeg: ‘Wij vinden het belangrijk dat de verschillende overheidspartners weten dat ieder drinkwaterbedrijf anders is. Eenzelfde cyberdreiging kan voor elk drinkwaterbedrijf anders uitpakken. Zonder gedegen en specifieke informatie van alle partijen generieke conclusies trekken is daarom niet productief. We zouden graag zien dat dit aspect in de oefeningen nog meer naar voren komt. Ook oefenen van ketenafhankelijkheden tussen de verschillende vitale sectoren zou wat ons betreft vaker mogen gebeuren, ook omdat het speelveld snel verandert – en daarmee de uitdagingen en de risico’s. Wij zijn dan ook een groot voorstander van het jaarlijks herhalen van ISIDOOR.’