



Customer stories

Watermaatschappij Farys rekent op Orange Cyberdefense om aan de NIS-regelgeving te voldoen en het OT-netwerk te beschermen



- ISO 27001 gecertificeerd
- Meer visibiliteit in het IT- en OT-netwerk
- Meer awareness bij bestuur over belang cybersecurity
- IT wordt gezien als partner, niet als hindernis
- Business is zich meer bewust van het belang van cybersecurity

Essentiële dienst veiligstellen

Farys is een moderne organisatie die activiteiten uitrolt met focus op de drinkwaterbevoorrading van particulieren en bedrijven in Oost en West-Vlaanderen. Daarnaast staat Farys ook in voor afvalwaterbeheer en het beheer van sportinfrastructuur zoals zwembaden in diverse Vlaamse gemeenten. Een kleine duizendtal medewerkers staan garant voor de drinkwatervoorziening bij ongeveer 700.000 gezinnen en bedrijven. In 2020 telde het bijna 668 km toevoerleidingen, 11.733 km distributieleidingen en werd er meer dan 91 miljoen m3 drinkwater geleverd.

Om deze activiteiten in goede banen te leiden, speelt IT een belangrijke rol. Niet alleen op administratief vlak, waar Farys jaarlijks meer dan twee miljoen facturen correct verwerkt en verstuurt. Farys investeerde ook in een online klantenportaal (MyFarys) waar de klanten zelf hun klantenzaken snel kunnen regelen. Denk bijvoorbeeld aan het doorgeven van een

verhuis, het beheer van hun gegevens of het wijzigen van het bedrag van de tussentijdse facturen. “We hebben daarnaast een zeer specifieke OT-technologie nodig waarmee we alle installaties kunnen beheren voor zowel de productie, als het transport en de levering van drinkwater”, vertelt Inge Opreel, directiemanager ICT bij Farys/TMVW. “En IT helpt ook om onze medewerkers op het terrein die volledig mobiel werken aan te sturen. Kortom, IT is voor Farys een cruciaal gegeven.”

Begin 2021 werd Farys aangeduid als een operator van essentiële diensten, wat inhoudt dat Farys aan de NIS-regelgeving dient te conformeren. Samen met alle Vlaamse waterbedrijven heeft Farys beslist om te voldoen aan de strenge ISO 27001-standaard. “De Belgische NIS-wetgeving bepaalt immers dat wanneer je ISO27001 gecertificeerd bent, je automatisch ook voldoet aan de bepalingen in de NIS-wetgeving”, vertelt Inge Opreel. “Uiteraard waren we al intensief met cyberbeveiliging mee bezig. Maar je ziet



dat cybersecurity nu steeds hoger op de agenda komt te staan.”

Niet alleen de NIS-wetgeving was een trigger om meer en meer in cyberbeveiliging te investeren. Andere triggers zijn wat je ziet in de buitenwereld. Verhalen over hacking komen steeds vaker in het nieuws. “Onder andere de hacking van een drinkwatermaatschappij in Florida en de Colonial Pipelines hacking, maakten het gevaar van cybercrime in onze sector zeer zichtbaar voor onze Raad van Bestuur binnen onze organisatie”, aldus Inge Opreel.

De oplossing: risk assessment

De grote uitdaging voor een IT-team in deze sector is de grote geografische spreiding van de diverse drinkwaterinstallaties. “Inzicht in de datastromen binnen het OT-netwerk is cruciaal in het geval van een cyberincident”, verduidelijkt Inge Opreel.

Vanaf het moment dat de NIS-wetgeving in het dossier van de watermaatschappijen ter sprake kwam, heeft Farys samen met Orange Cyberdefense onderzocht welke impact dit voor hen zou kunnen betekenen. Nog vooraleer Farys werd aangeduid als aanbieder van essentiële diensten, werd er gestart met een aantal voorbereidende maatregelen. Daarbij hoorde een volledige risk assessment van Farys als organisatie maar ook van alle installaties. “Hieruit zijn een aantal

actiepunten en maatregelen voortgekomen die geïmplementeerd moesten worden – volgens een uitgestippelde roadmap – om tegen eind 2023 de ISO 27001-certificering te behalen.” De focus voor de komende jaren ligt dus vooral op de implementatie van het Information Security Management System (ISMS)

Naast de technologische en de procesmatige factoren, is voornamelijk de menselijke factor van groot belang. Farys zet daarom volop in op het opleiden van zijn mensen zodat ze niet alleen de juiste procedures leren kennen, maar vooral leren hoe ze op een veilige manier met informatie en de toegang tot systemen moeten omgaan.

Samenwerking

Orange Cyberdefense is al jaren een vertrouwde partner op vlak van IT-security. “Een van de elementen waardoor zij – ten opzichte van andere partijen – eruit springen, is hun expertise en jarenlange ervaring binnen cybersecurity. Bovendien hebben ze een zeer goede kennis van de drinkwatersector, die heel specifieke eisen heeft op vlak van beveiliging”, aldus Inge Opreel.

Het langdurige partnership is ook een meerwaarde volgens de directiemanager ICT. “Ze kennen ons bedrijf door en door, weten hoe we zaken benaderen en passen hun aanpak aan onze specifieke situatie aan. Daarnaast is Orange Cyberdefense

“
Vroeger werd IT door de business gezien als een soort boeman die hen restricties oplegt met maatregelen waar ze weinig van begrijpen. Vandaag beschouwen ze ons als een echte partner.”

Inge Opreel | ICT department manager bij Farys/TMVW



heel pragmatisch ingesteld, en dat appreciëren we. We zijn een bedrijf dat niet alleen in theorie spreekt, maar we willen zien hoe dit praktisch kan worden geïmplementeerd op een snelle en eenvoudige manier.”

Resultaat: reputatie en leveringszekerheid

Het voordeel van de samenwerking met Orange Cyberdefense uit zich in het feit dat de businessmensen bij Farys zich meer bewust zijn van de mogelijke beveiligingsinbreuken die kunnen gebeuren. Dit is helemaal te danken aan de risicoanalyse die Farys samen met Orange Cyberdefense heeft uitgevoerd. “Door een veilige (IT)-omgeving te garanderen, is Farys een gewaardeerde partner en heeft dit proces bijgedragen tot de goede reputatie die wij als organisatie bij onze klanten genieten”, aldus Inge Opreel.

Op vlak van technologie heeft het IT-team nu meer overzicht over het OT-netwerk, wat vroeger ontbrak. ““Het industriële netwerk (OT of Operational Technology) speelt een cruciale rol in de dienstverlening van Farys. Dat OT-netwerk is een van de belangrijkste elementen om te beschermen,

want dit OT-netwerk hebben we nodig om de drinkwatervoorziening te waarborgen. Maar het mooiste voordeel vind ik dat IT hierdoor nauw samenwerkt met de business in een vertrouwensrelatie en niet meer wordt gezien als een soort boeman die hen restricties op de manier van werken oplegt met maatregelen waar ze weinig van begrijpen. We worden nu aanschouwd als een echte partner”, vertelt Inge Opreel fier.

De toekomst

Een van de volgende stappen die Farys wil zetten is de roadmap voor de implementatie van het Information Security Management System (ISMS) verder realiseren. “Daarnaast hopen we ook, in samenwerking met andere bedrijven uit de sector om een Security Operations Center in te richten. Hiermee zouden we 24/7 ons uitgebreid IT- en OT-netwerk kunnen monitoren en proactief waarschuwingen krijgen als er ergens een poging tot hacking of inbraak is. En dan kunnen alle spelers in de sector ook direct actie ondernemen”, besluit Inge Opreel.

Over Orange Cyberdefense

Orange Cyberdefense is de deskundige cybersecurity business unit van de Orange Group. Als Europa's go-to security provider streven zij naar een veiligere digitale samenleving. Zij zijn een threat research en intelligence-driven security provider die ongeëvenaarde toegang biedt tot huidige en nieuwe dreigingen.

Orange Cyberdefense heeft meer dan 25 jaar ervaring op het gebied van informatiebeveiliging, 250+ onderzoekers en analisten, 16 SOC's, 10 CyberSOC's en 4 CERT's verspreid over de hele wereld en verkoop- en dienstenondersteuning in 160 landen. Zij zijn er trots op dat ze met lokale expertise wereldwijde bescherming kunnen bieden en hun klanten gedurende de hele levenscyclus van een bedreiging kunnen ondersteunen.