Cyber security speelt bij alle bedrijven en dienstverleners en zeker ook bij waterbedrijven. Het overnemen van gegevens, het manipuleren van procestechnieken en/of sabotage, zijn risico's waar men zeker rekening mee moet houden. Marcel Jutte van Hudson Cybertec monitort dergelijke risico's en adviseert bedrijven en organisaties hoe hier mee om te gaan.

Dreiging cybercriminaliteit bij (drink)waterbedrijven is groot

Cyber Security moet risico's voorkomen

Door Mark Nijveld

''Bij cyber security gaat het er om risico's te onderkennen en te ondervangen binnen alle lagen van het bedrijf. Alle mensen die bij het proces als geheel betrokken zijn doen er toe, van de receptionist tot de CEO en van toeleveranciers tot onderhoudsmonteur. Eén zwakke schakel kan je hele beveiliging te niet doen.''
Het in kaart brengen van (ontbrekende)veiligheidsmaatregelen is de eerste taak die Jutte uitvoert als hij een risico/veiligheidsanalyse opstart. Daarbij hoort onder meer: mensen interviewen, apparatuur controleren en de organisatiestructuur bekijken. ''Het gaat dan om het totale beeld, van (oude)wachtwoorden, beveiliging, toegangspoorten en de bevoegdheden van de storingsmonteur tot de ICT programma's. Maar als eerste komt de vraag aan de orde : is men zich bewust van veiligheidsrisico's. Awareness is één van de belangrijkste punten in de totale beveiliging. Hoe gaat men er mee om, hoe interpreteert men de veiligheidsregels en hoe is iedereen, de schoonmaker, de procesbestuurder en de manager, bij het proces betrokken.''

Geen publiciteit

Maar wat zouden bij waterbedrijven de risico's kunnen zijn? Als we dit aan de Vewin vragen, krijgen we als antwoord dat zij hier niet mee in de publiciteit willen komen. Ook (drink)waterbedrijven willen hierop niet reageren. Jutte: ''Drinkwater wordt door de overheid gekenmerkt als vitale infrastructuur, de dreigingsanalyse is groot en daardoor is het een mogelijk doel ; criminelen, terroristen en hackers kunnen het gebruiken als pressiemiddel. Om risico's als vervuiling, uitschakeling van processen, invoeren van misleidende gegevens en overnemen van informatie te voorkomen, moet je je hele organisatie erbij betrekken. Alleen op die manier kun je alle operationele technologie systemen voldoende beveiligen. Maar dat is ook een doorlopend proces, hackers vinden steeds nieuwe dingen uit, de technologie verandert elke dag en de 'misbruikers' veranderen mee. Het blijft een kat-en-muisspel, en ik kan mij voorstellen dat bedrijven liever niet in het openbaar aangeven hoe hun cyber security op dit moment is geregeld of wat zij nog moeten regelen .




Daarbij wordt het gevaar van hackers die 'voor de lol' het systeem willen saboteren steeds kleiner, maar door het grote afbreukrisico in de waterwereld is de georganiseerde misdaad voor waterbedrijven wél een serieuze bedreiging''

Manipuleren

Als één van de risico's noemt Jutte ook 'het zonder toestemming overnemen van informatie'. ''Bij waterbedrijven wordt veel technische data verzameld en opgeslagen. Bijvoorbeeld aan de hand van de registratie van peilniveau's, stromingen etc. Voor een toeleverancier van de meetapparatuur zou het interessant kunnen zijn om deze gegevens ook te hebben. Het inbouwen van een 'zendertje' in bijvoorbeeld een nieuw geleverde pomp die de gegevens rechtstreeks naar de leverancier stuurt, is niet moeilijk. Het opzetten van een eigen productielijn aan de hand van verkregen gegevens gebeurt steeds vaker. Aan deze vorm van cyber security (ook hier zou ik cybercriminaliteit gebruiken) wordt steeds meer aandacht geschonken, temeer daar er nog een andere mogelijkheid is, namelijk dat de fabrikant of leverancier bewust de meetapparatuur zo manipuleert dat er onjuiste gegevens worden verstrekt. In Amerika, maar ook in Nederland, worden hier steeds vaker voorbeelden van gevonden.
Eén van de maatregelen om dit te voorkomen is het monitoren van alles wat op je netwerk komt, zowel van binnenuit als van buitenaf. "Dat betekent bijvoorbeeld het monitoren van de Process Controle Omgeving door middel van een Intrusion Detection System, specifiek gericht op de process omgeving.''
''Een dergelijk detectie systeem wordt momenteel nog veel te weinig gebruikt terwijl de risico's worden onderschat. Maar het opzetten en uitvoeren van zo'n systeem vraagt ook de nodige kennis. En als je het toe wil passen binnen een complete organisatie, dan moet ook iedereen, van alle afdelingen, dezelfde doelstelling hebben en dezelfde 'taal' spreken. Die vaardigheden proberen wij in te brengen waarbij de kennis van het domein, de techniek en de IT security onze belangrijkste uitgangspunten zijn.'' De noodzaak van cyber security wordt ook door de overheid onderkend die zich onder meer middels regelgeving met de uitvoering en controle begint te bemoeien. Denk aan ISO normering en BIWA (Baseline Information Water) waarbij vooral wordt gekeken naar zaken als vertrouwelijkheid, beschikbaarheid en integriteit.

Security by design

Jutte noemt ook het belang van 'security by design'. Oftewel, bij het opzetten van een nieuw project moet je de security van het begin af aan meenemen. ''Dat zorgt voor een efficiëntere manier van werken, beter resultaat en je bespaart op de kosten. Achteraf een veiligheidssysteem inbouwen kost natuurlijk aanzienlijk meer. Juist de financiering van cyber security schrikt bedrijven soms af, het zijn immers niet alleen de kosten voor onderzoek, ontwerp en implementatie, je moet ook kijken naar onderhoud en beheer. Daarbij moet bovendien verantwoordelijkheid geregeld worden en er moet worden voorzien in een regelmatige toetsing en aanpassing van het systeem waar financieel een prijskaartje aan hangt.''

Hoewel Jutte benadrukt dat alle schakels even belangrijk zijn, licht hij er tot slot toch een punt uit: 'Awareness'. ''Als men niet het belang van cyber security inziet en als je niet constant bewust bent van de risico's, dan werkt een veiligheidsprogramma niet. De mensen moeten het doen, daar kan geen ICT programma tegenop''