PROCESVEILIGHEID VRAAGT ÓÓK OM OT-SECURITY

Procesveiligheid is al decennialang een vanzelfsprekend onderdeel van de industrie. Digitale veiligheid kreeg pas veel later aandacht, terwijl de afhankelijkheid van industriële automatisering sterk toenam. Daarom lijkt het vreemd dat cybersecurity van industriële installaties zich pas relatief laat ontwikkelde.

Tekst: Mels Dees



Marcel Jutte

Foto: Danny Cornelissen



Deze installaties vormen het werkterrein van de operationele technologie (OT). De beveiliging daarvan, OT-security, verschilt fundamenteel van de beveiliging van kantoorautomatisering, zegt Marcel Jutte, voorzitter ad-interim van het Industrieel Platform Cyber Security (IPCS). “Toen ik eind jaren tachtig begon, was security helemaal geen onderwerp. Het uitgangspunt was simpel: het moest werken.”
In 2014 werd daarom het Industrieel Platform Cyber Security (IPCS) opgericht. Het platform brengt inmiddels meer dan zestig organisaties bijeen, variërend van industriële eindgebruikers en leveranciers tot systeemintegratoren, kennisinstellingen en overheden. Anders dan commerciële beveiligingsbedrijven verkoopt IPCS geen producten of adviesdiensten. Het doel is kennis delen en organisaties helpen de digitale weerbaarheid van de Nederlandse industrie te vergroten. “Onze leden concurreren soms met elkaar”, zegt Jutte, “maar binnen IPCS werken ze juist samen aan een gezamenlijk doel: een veiligere industrie.”

NAUW VERWEVEN

De historische achtergrond verklaart volgens hem veel van de uitdagingen waar bedrijven vandaag tegenaan lopen. De besturingssystemen waarmee chemische fabrieken, raffinaderijen, energiecentrales en terminals dagelijks produceren, stammen vaak uit een tijd waarin internet nog geen rol speelde. Cybercriminaliteit speelde simpelweg geen rol bij het ontwerp. “Toen kwam internet eind jaren negentig”, zegt Jutte. “Organisaties wilden hun systemen ook kunnen ontsluiten. Ineens kon je vanuit Nederland een fabriek in Polen monitoren of onderhoud op afstand uitvoeren. Dat leverde enorme voordelen op, maar die installaties waren daar helemaal niet voor ontworpen.”
Veel van die systemen draaien vandaag nog steeds. Daardoor verschilt OT-security van IT-security. Waar kantoorautomatisering draait om informatie en gegevens, staat in de industrie de continuïteit van fysieke processen centraal. “Een IT-storing betekent meestal dat mensen tijdelijk niet kunnen werken”, zegt Jutte. “Een OT-storing kan leiden tot stilstaande fabrieken, milieuschade of zelfs gevaarlijke situaties.”
Voor bedrijven in het Rotterdamse haven- en industriegebied is dat geen theoretisch onderscheid. Chemische bedrijven, energiecentrales, terminals en logistieke ondernemingen vormen samen een industriële cluster. Bedrijven zijn nauw met elkaar verweven. Een cyberincident beperkt zich daardoor lang niet altijd tot één bedrijf. Jutte: “Veel organisaties denken: de IT-afdeling doet OT-security er wel even bij, maar een chemische installatie of een rookgasreiniging is echt iets anders dan een nieuwe printer.”

TWEE WERELDEN

Opmerkelijk genoeg ziet Jutte de grootste kwetsbaarheden lang niet altijd in de techniek. Veel vaker ontstaan ze doordat IT en operationele technologie zich jarenlang vrijwel onafhankelijk van elkaar hebben ontwikkeld. “Het waren twee verschillende werelden. De IT’ers keken een beetje neer op de mannen in de vieze overalls. En andersom werd er op de werkvloer gesproken over die mensen boven in hun overhemden en stropdassen.”
IT-specialisten kijken primair naar de beschikbaarheid van informatiesystemen. Operators en maintenance-afdelingen redeneren vanuit een veilig en stabiel productieproces. Beide perspectieven zijn logisch, maar daardoor ontstond jarenlang een grijs gebied waarin niemand zich echt eigenaar voelde van OT-security.
Volgens Jutte verklaart dat waarom cybersecurity zich veel later ontwikkelde dan procesveiligheid. Veiligheidsprocedures, risicoanalyses


Foto: Danny Cornelissen

en onderhoudsprogramma's kregen volop aandacht, terwijl digitale veiligheid vaak bleef steken in losse technische maatregelen zonder duidelijke verantwoordelijkheid. Pas onder invloed van digitalisering en regelgeving, zoals de Europese richtlijn voor cybersecurity NIS2, verschuift OT-security van de serverruimte naar de bestuurskamer.

EEN DURE KROONSTEEN

Jutte geeft een praktijkvoorbeeld: "Een industrieel bedrijf besloot de productieomgeving beter af te schermen van het kantoornetwerk. Er werd een firewall besteld, de inkoopafdeling handelde de bestelling af en leverde de apparatuur af bij de IT-afdeling. Daar hoorde een firewall immers thuis." Toen Jutte later een eerste security assessment uitvoerde, bleek dat de investering nauwelijks iets had opgeleverd. "Die firewall stond gewoon op 'allow all'. Eigenlijk was het een dure kroonsteen."
De hardware functioneerde uitstekend. Alleen had niemand de configuratie daadwerkelijk ingericht. De IT-afdeling ging ervan uit dat de specialisten uit de fabriek dat zouden doen. Operations dacht juist dat dit vanzelfsprekend onder IT viel. "Dit laat zien waar OT-security werkelijk begint. Niet bij firewalls of antivirussoftware, maar bij heldere verantwoordelijkheden."
Organisaties investeren wel in techniek, weet Jutte, maar hebben vaak onvoldoende zicht op hun eigen omgeving. Oude PLC's blijken nooit te zijn geïnventariseerd, leveranciers beschikken nog over remote toegang en niemand weet precies welke systemen met internet communiceren. "Je kunt niet beschermen wat je niet kent."

GEEN LOSSE EILANDEN

Juist in een industriecluster als Europoort en de Botlek krijgt OT-security volgens Jutte een extra dimensie. Chemische bedrijven, raffinaderijen, energiecentrales en terminals functioneren niet als losse eilanden. Bij de bouw of modernisering van een installatie zijn vaak tientallen partijen betrokken.
Systeemintegrators ontwerpen de besturing, leveranciers leveren PLC's en andere componenten, gespecialiseerde bedrijven verzorgen software en onderhoud. Al die partijen beschikken over kennis en informatie die essentieel is voor het functioneren van de installatie. "Als hun engineeringomgeving of de ontwerpbestanden onvoldoende zijn beveiligd, ontstaat alsnog een risico. Uiteindelijk ben je als fabriek ook afhankelijk van de digitale veiligheid van je leveranciers."

IPCS ONDERDEEL VAN HSD

Sinds 2024 is het secretariaat en de communicatie van het Industrieel Platform Cyber Security (IPCS) ondergebracht bij de Haagse Security Delta (HSD), het nationale veiligheidscluster waarin overheden, bedrijven en kennisinstellingen samenwerken aan innovatieve veiligheidsoplossingen. Deze samenwerking heeft IPCS organisatorisch versterkt en de verbinding met het bredere cybersecurity-ecosysteem verstevigd, aldus Marcel Jutte. Het platform blijft groeien en vertegenwoordigt inmiddels meer dan zestig aangesloten organisaties. Ook werkt het samen met partnerorganisaties, zo is Cyberweerbaarheidscentrum Maakindustrie onlangs ook aangesloten als samenwerkingspartner. Jutte: "Met name op het vlak van cybersecurity is samenwerken essentieel."

Volgens Jutte verdient de beveiliging van de keten daarom veel meer aandacht. Cybersecurity moet niet pas ter sprake komen wanneer een installatie wordt opgeleverd, maar al tijdens aanbestedingen en contractonderhandelingen. Bedrijven moeten leveranciers aantoonbare beveiligingseisen opleggen, periodiek controleren of daaraan wordt voldaan en kritisch kijken naar de manier waarop remote toegang wordt ingericht.

BEGIN NIET MET TECHNIEK

Juist omdat investeringsbudgetten onder druk staan, krijgt Jutte regelmatig de vraag waar bedrijven het beste kunnen beginnen. Zijn antwoord is steevast hetzelfde: "Begin met de kroonjuwelen." Daarmee bedoelt hij de processen waarvan de continuïteit van de onderneming afhankelijk is. Welke installaties mogen nooit uitvallen? Welke systemen beschermen mens, milieu en productie? Welke onderdelen bepalen uiteindelijk of een fabriek na een incident binnen enkele uren weer draait of wekenlang stil ligt?
Volgens Jutte wordt die vraag nog te weinig gesteld. Organisaties investeren vaak in losse beveiligingsmaatregelen zonder eerst vast te stellen welke processen werkelijk kritiek zijn. Dat vraagt volgens hem om een andere manier van denken. Niet de techniek staat centraal, maar het productieproces. Vanuit dat vertrekpunt ontstaat vanzelf een prioriteitenlijst.

KLEINE WIJZIGINGEN, GROTE GEVOLGEN

Dat het mis kan gaan door ogenschijnlijk onschuldige veranderingen, heeft Jutte vaker gezien. Hij vertelt over een bedrijf waar een nieuwe telefooncentrale werd aangesloten op het netwerk. Voor de IT-afdeling leek dat een gewone infrastructuurwijziging. "Niemand had voorzien dat daardoor ook verbindingen met de productieomgeving werden beïnvloed. Een aanzienlijk deel van de fabriek viel uit."
Voor Jutte is dat illustratief voor de manier waarop IT en OT elkaar steeds vaker raken. Een wijziging die in een kantooromgeving nauwelijks gevolgen heeft, kan in een productieomgeving onverwacht grote impact hebben. Daarom vindt hij het ook gevaarlijk wanneer organisaties ervan uitgaan dat ervaren IT-beheerders OT-security 'er wel even bij doen'.

VAN COMPLIANCE NAAR WEERBAARHEID

Nieuwe wetgeving zoals NIS2 heeft het onderwerp nadrukkelijk op de agenda van bestuurders gezet. Dat is volgens Jutte een positieve ontwikkeling, maar tegelijk waarschuwt hij dat compliance geen synoniem is voor veiligheid. "Een wet maakt een organisatie niet veiliger."
De echte uitdaging begint volgens hem pas nadat aan wettelijke verplichtingen is voldaan. Cyberweerbaarheid vraagt om investeringen in mensen, processen en samenwerking. IT, operations, maintenance, engineering en directie moeten gezamenlijk verantwoordelijkheid nemen voor de veiligheid van de productieomgeving.
Juist voor bedrijven in het Rotterdamse haven- en industriegebied is dat volgens hem een belangrijk uitgangspunt. De onderlinge verwevenheid van installaties, leveranciers en logistieke ketens maakt dat de digitale weerbaarheid van één organisatie steeds vaker afhankelijk is van die van een ander.
Volgens Jutte is dat de reden waarom het Industrieel Platform Cyber Security (IPCS) werd opgericht. Niet om producten te verkopen of organisaties te adviseren, maar om een plek te creëren waar bedrijven, overheden, leveranciers en kennisinstellingen open ervaringen kunnen uitwisselen. "Tijdens een verkoopgesprek vertellen organisaties zelden waar het echt misging. Binnen een onafhankelijk platform gebeurt dat wel. Juist daar leren bedrijven van."