Cyberrisico's nog onderschat

MEER BEWUSTWORDING IS NODIG

Bedrijven hebben nog altijd te weinig aandacht voor het beveiligen van OT-systemen, signaleren Marcel Jutte en Chris van den Hooven van Hudson Cybertec. En dat terwijl de dreiging allerminst is teruggelopen. "Elk groot bedrijf in de haven van Rotterdam wordt aangevallen."


Marcel Jutte


Chris van den Hooven

Het in Den Haag gevestigde Hudson Cybertec geldt als een onafhankelijke cybersecurity-specialist met specifieke expertise in het beveiligen van Operationele Technologie (OT). Wat dit laatste precies is, legt Chris van den Hooven uit, senior cybersecurity consultant bij Hudson Cybertec. "Als ik op een verjaardag vertel dat ik thuis ben in het beveiligen van OT, kijken mensen mij meestal wat glazig aan. Dan noem ik het voorbeeld van een bierbrouwerij. Als de IT daar is gehackt, kan de brouwer geen facturen meer sturen. Is de OT gehackt, dan kan het geen bier meer leveren. Meestal doet dit het kwartje vallen."

Kwetsbaarheid

"Regelmatig halen incidenten het nieuws waarbij bedrijven slachtoffer zijn van een cyberaanval", ziet managing director Marcel Jutte van Hudson Cybertec. "Desondanks wordt het beveiligen van OT nog altijd onderschat. Bij vrijwel elke klant waar we voor het eerst komen, is dit een ondergeschoven kindje. Tegelijkertijd neemt de kwetsbaarheid toe. Systemen die vroeger autonoom draaiden, zijn nu aan elkaar gekoppeld, zelfs met systemen van andere bedrijven. Veel voorkomend zijn oudere systemen ('legacy') waar bij het ontwerp geen rekening is gehouden met cybersecurity. Dat zie je aan de componenten en de manier van koppelen." Van den Hooven heeft wel een verklaring waarom de beveiliging van OT niet actiever wordt opgepakt: "In de regel moeten OT-systemen vooral doen waarvoor het bedoeld is. Zorgen dat de productiecontinuïteit gewaarborgd is. Je kunt daar niet zomaar aan sleutelen zonder de bedrijfsprocessen stil te zetten. Daarbij komt dat het voor bedrijven niet altijd helder is welke acties ze moeten nemen."

Tijdig reageren

De grootste winst zit hem vooral in bewustwording, vindt Jutte. "Bedrijven hebben onvoldoende in kaart wat voor gevolgen een digitaal incident kan hebben. Je merkt dat een incident als bij VDL helpt de ogen te openen. Dan komt de dreiging ineens wel erg dichtbij en ontstaat er awareness. Wel 'mosterd na de maaltijd'. De mosterd is dan ook veel kostbaarder." Van den Hooven noemt het voorbeeld van een bedrijf dat onlangs een

“Elk groot bedrijf in de haven van Rotterdam wordt aangevallen; wees dus voorbereid”
Marcel Jutte

“Als een bedrijf zijn OT-installatie laat certificeren op de IEC 62443, toont het aan dat het aan de wet voldoet”
Chris van den Hooven

Foto Danny Cornelissen

risicoanalyse had uitgevoerd. Dit was volgens hem 'heel net' gedaan, alleen schortte er toch iets aan: "Het risico was voor elke component afzonderlijk bepaald. Per component werd in kaart gebracht wat er gebeurt als het uitvalt. Maar bij een cyberaanval valt niet één component uit, maar alles tegelijk. Wat doe je dan?" Hudson Cybertec helpt bedrijven om de cyberrisico's te vertalen naar wat er kan gebeuren. De reputatie van een bedrijf kan een deuk krijgen als een hack in het nieuws komt. Maar er kunnen ook gewonden of doden vallen. Jutte: "Soms is een bedrijf niet eens doelwit, maar wordt het slachtoffer van 'collateral damage'. Dat overkwam APM/Maersk bijvoorbeeld. Elk groot bedrijf in de haven van Rotterdam wordt aangevallen. Wees dus voorbereid. Neem maatregelen om te voorkomen dat de schade groot uitvalt. Ook helpt monitoring. Als je ziet dat er iets afwijkends gebeurt, kun je tijdig reageren."

Digitale bom

Naast ransomware is cyberspionage een reële dreiging, zeggen Jutte en Van den Hooven. "In tegenstelling tot ransomware doen cyberspionnen er alles aan om niet te worden ontdekt. Ze maken geen lawaai en willen zo lang en zo onopvallend mogelijk in een netwerk aanwezig zijn. Hun doel is bedrijfsgevoelige informatie vergaren, al is het niet ondenkbaar dat ze een digitale bom plaatsen. Je komt er moeilijk achter. Als je dit ontdekt, is het de vraag hoe lang ze er al zitten en of je alles te pakken hebt. Veelal zijn het 'nation states' die aan cyberspionage doen", vertelt Van den Hooven, die in zijn loopbaan een aantal keer met cyberspionage te maken heeft gehad. Jutte: "Alle vitale infrastructuur in Nederland ligt onder vuur. Rotterdam is het grootste industriële complex, waar veel schade kan worden berokkend. Energie is geopolitiek; er is geen twijfel over mogelijk dat energiebedrijven doelwit zijn van nation states als China, Rusland en andere landen. Hierbij geldt opnieuw dat awareness van zeer groot belang is, ook bij bedrijven waar men denkt dat er niets te halen valt. Ook zij zijn doelwit."

'CYBERCRIMINELEN NIET VERNIEUWEND'

"Cybercriminelen hoeven over het algemeen verrassend weinig vernieuwend te zijn", zegt Chris van den Hooven van Hudson Cybertec. "Ze proberen het eerst op de gemakkelijke, voor hen bekende manier. Jammer genoeg lukt dat vaak. Waarom zouden ze dan geld steken in het ontwikkelen van nieuwe methodes? Het is een kosten-/batenafweging. Bij cyberspionage speelt mee dat het gebruik van iets nieuws de kans vergroot dat dit wordt ontdekt. Voor nation states is het heel vervelend als ze daarmee in het nieuws komen."

Enige oplossing

Nu steeds meer bedrijven - vaak in een klant-/leverancierrelatie - met elkaar zijn verbonden, ziet Jutte de ketenaansprakelijkheid toenemen. "Op allerlei niveaus zijn er koppelingen, wat het aanvalsoppervlak voor cyberaanvallen vergroot. Omdat bedrijven zelf geen zeggenschap hebben over het netwerk van hun leverancier, is de enige oplossing het inbouwen van ketenaansprakelijkheid. Een leverancier mag bijvoorbeeld alleen leveren als niet alleen het product, maar ook de cybersecurity aan de eisen van de afnemer voldoet. Die trend is duidelijk ingezet en zal zeker doorzetten." Volgens Van den Hooven kunnen bedrijven ook niet anders. Hij waarschuwt dat het opleggen van eisen alleen niet helpt. "Kleinere bedrijven zijn niet altijd in staat om hun IT of OT te beveiligen. Je ziet dat grotere ketenpartners hen daarbij helpen."

Compliance monitoring

"Tegelijkertijd zit de wetgever niet stil. In de aankomende Europese NIS2 [Network and Information Security, red.] Directive worden meer sectoren als vitaal beschouwd dan in de huidige NIS. Dit betekent dat meer bedrijven moeten aantonen dat ze aan de richtlijn voldoen. Dit kunnen ze doen door een auditor dit te laten beoordelen of door monitoring. Alles grijpt dus in elkaar. De dreiging neemt toe, net als de noodzaak om iets te doen en de wetgever onderneemt actie", aldus Jutte. "Maar hoe handhaaf je de NIS en straks de NIS2? Dit kun je doen met behulp van het normenkader IEC 62443. Dit is een internationale set cybersecuritynormen die speciaal is ontwikkeld voor het beveiligen van OT. Als een bedrijf zijn OT-installatie laat certificeren op de IEC 62443, toont het aan dat het aan de wet voldoet. Dit gaan we meer zien", verwacht Van den Hooven. Compliance monitoring - een van de diensten die Hudson Cybertec aanbiedt - kan daarbij van nut zijn. "Hierbij wordt gemonitord in hoeverre een bedrijf aan de eigen eisen of andere, zoals de 62443, voldoet. Een audit vindt maar één keer per jaar plaats, terwijl monitoring continu gebeurt. Daardoor is het een heel krachtige tool. We zien de vraag hiernaar toenemen en verwachten dat dit voorlopig zal aanhouden", zegt Jutte.

HUDSON CYBERTEC

Het voornaamste doel van Hudson Cybertec is het digitaal weerbaar maken én houden van de primaire processen bij zijn klanten. Dit doet de cybersecurity-expert op verschillende manieren, legt Marcel Jutte van Hudson Cybertec uit. "We bieden consultancy aan, waarbij we kijken waar bedrijven nog een stapje kunnen zetten. Denk een zowel technische als organisatorische assessments, die uiteenlopen van een quickscan tot een complete audit. Ook onderzoeken we waar verbetering mogelijk is. We voeren daarvoor risicoanalyses uit, waarbij we de IEC 62443 toepassen. Verder bieden wij netwerk- en compliancemonitoring aan, verzorgen wij, samen met NEN, internationaal gespecialiseerde cybersecurity trainingen en kunnen wij voor klanten de gehele cybersecurity op ons nemen."