SLIMME DEVICES IN PRODUCTIE-OMGEVINGEN BRON VAN ZORG

Security van IoT schiet vaak te kort

Waar uit berichten in de media over cybercrime blijkt hoe belangrijk het beveiligen van IT-systemen is, daar krijgt cybersecurity bij Operationele Technologie veel minder aandacht. Ten onrechte, zeker nu IoT in deze omgevingen een opmars maakt. *Tekst: Mels Dees*

Eigenlijk komt IoT neer op een verbinding van Informatie Technologie (IT) en Operationele Technologie (OT). Het verschil tussen die twee kun je uitleggen aan de hand van de begrippen 'witte'- en 'blauweboordenwerkers'. De eerste groep gebruikt systemen, denk aan office-applicaties, die vooral op software berusten, de tweede hanteert industriële- of productie-omgevingen met een grote hardwarecomponent. IoT zorgt er in de praktijk steeds vaker voor dat IT en OT naar elkaar toegroeien. Steeds meer slimme devices worden ingezet in het OT-domein. Hyperconnectivity, ook met de cloud, komt zo terecht in productieomgevingen. De opkomst van steeds uitdagender cyberbedreigingen maakt verbonden OT-systemen bijzonder kwetsbaar. IoT zorgt er zo voor dat de industriële beveiliging een grotere rol toebedeeld moet worden in de risicoportefeuille van veel organisaties. De OT-beveiliging vertegenwoordigt echter een groeiend punt van zorg voor het management van ondernemingen. Het niveau van beveiliging van IoT-devices is op een lager niveau dan van veel applicaties, wat de kans vergroot op onvoldoende beveiligde devices in het netwerk. Dit gegeven is niet zonder gevaar.

Grote gevolgen

Als met de IT iets fout gaat, dan kost dat in het slechtste geval de kop van de CEO of van de CIO, maar er vallen doorgaans geen doden of gewonden. Wordt een IoT-device binnen een OT-omgeving echter succesvol aangevallen, dan kunnen ongewenste emissies van gassen, schadelijke lozingen van vloeistoffen of explosies het gevolg zijn. Dit kan impact hebben op de natuur, of op het welzijn van mensen. Ook als dergelijke gevolgen uitblijven, zijn OT-gerelateerde beveiligingsincidenten sterk van invloed op de productiviteit en het bedrijfsresultaat van organisaties. Volgens een rapport van security-specialist Fortinet kreeg 93% van alle organisaties met OT-omgevingen de afgelopen 12 maanden te maken met minimaal één succesvolle indringingspoging. 78% kreeg met drie indringers te maken. Bijna de helft van alle getroffen organisaties ondervond hierdoor productiviteitsverlies als gevolg van downtime. In 90% nam het herstel van processen uren of dagen in beslag. Een derde van de respondenten ondervond hierdoor omzetverlies, gegevensverlies, compliance-problemen of imagoschade.

Onduidelijke verantwoordelijkheid

Aan de ene kant heeft de gebleken kwetsbaarheid van IoT binnen OT-omgevingen te maken met het toekennen van verantwoordelijkheid. Binnen het bedrijfsleven is geen sprake van consistente verantwoordelijkheid voor de OT-beveiliging. Volgens het rapport van Fortinet valt het beheer van de OT-beveiliging toe aan professionals in uiteenlopende functies. Veel organisaties beleggen IoT bij de IT-afdeling. Maar niet altijd zijn daar de operationele problemen bekend waarvoor IoT een belangrijke rol kan spelen. Andere organisaties kiezen ervoor deze issues bij het meer algemene management te beleggen. Slechts 15% van de respondenten zegt dat de CISO als security officer verantwoordelijk is voor de OT-beveiliging binnen hun organisatie. Aan de andere kant zien we ook dat de beveiligingsricio's oplopen door een gebrek aan centraal overzicht op de OT-omgevingen en de IoT-oplossingen die er onderdeel van uitmaken. Volgens het onderzoek van Fortinet zorgde slechts 13% van alle respondenten voor centraal overzicht op alle OT-activiteiten. Bovendien is slechts 52% van alle organisaties in staat om deze processen te monitoren vanuit hun security operations center (SOC).

Groot aantal leveranciers

Assetmanagement is echter van groot belang om tot een goede risico-inventarisatie te komen, net als monitoring van IoT-devices - zowel binnen het OT- als binnen het IT-domein. Ook moet de supply chain goed gekend zijn waarvan de onderneming deel uitmaakt. Dit laatste is onder meer relevant om te kunnen bepalen waar gegevens (data) naartoe gaan, als IoT-devices connectie hebben met de cloud. Blijven de data in Nederland, of is ook sprake van verwerking of opslag in het buitenland, en zo ja, zelfs buiten Europa? Lastig is ook het feit dat de overgrote meerderheid van de organisaties oplossingen van twee tot acht leveranciers gebruikt voor de beveiliging van hun industriële apparatuur. Ze hebben tussen de 100 en 10.000 apparaten in gebruik, hetgeen alleen maar aan de complexiteit bijdraagt. "Met elke sensor die aan het IoT wordt toegevoegd, neemt de veiligheid van het netwerk af", stelt beveiligingsexpert en publicist Bruce Schneier uit de VS. Wie zich dat realiseert begrijpt de gevaren van IoT in OT-omgevingen. Volgens Schneier gebeurt het te vaak dat sensoren worden gebouwd op basis van oude techniek. "Er wordt niet bij stilgestaan dat bijvoorbeeld een oude sensor een serieus beveiligingslek kan vormen. Een kwaadwillende die met zijn signaal tot aan de sensor is gekomen, slaagt er meestal in om ook wel verder te komen." ■

> **"Met elke sensor die aan het IoT wordt toegevoegd, neemt de veiligheid van het netwerk af"**

Minimumeisen

Voor de digitale veiligheid van IoT-apparaten komen minimumeisen. Producten die hier niet aan voldoen, zijn vanaf medio 2024 op de gehele EU-markt verboden. Tot de minimumeisen behoort dat deze apparaten niet meer met zwakke, standaard wachtwoorden zijn uitgerust. Ook moeten deze slimme apparaten software-updates ondersteunen, getest zijn op veiligheidslekken, opgeslagen persoonlijke en financiële gegevens afschermen en er moet een mogelijkheid zijn voor de gebruiker om deze data te beheren en te verwijderen. Agentschap Telecom gaat hierop toezien en is bevoegd bij overtredingen op te treden.