TECHNOLOGY REVIEW

ONZE EXPERTEN AAN HET WOORD

Convergentie tussen IT- en OT-security is een must

Door Koen Tamsyn
Business Unit Lead Cybersecurity, Inetum

April 2024

inetum

Steeds meer bedrijven integreren informatietechnologie, zoals sensoren en andere IoT-apparaten, in hun operationele systemen. Die convergentie van IT en OT brengt naast heel wat voordelen ook bijkomende veiligheidsrisico's met zich mee. Om die af te dekken hebben bedrijven nood aan zowel een oplossing als een partner die beide domeinen beheersen, zoals de combinatie van Fortinet en Inetum.

De incidenten bij bierproducent Duvel-Moortgat en koffiebranderij Beyers van maart 2024 tonen het nogmaals aan: cybercriminelen mikken meer en meer op productiebedrijven. Daar zit de snelle digitale transformatie van de maakbedrijven voor veel tussen. Gedreven door de eisen en verwachtingen van de business, zetten plantmanagers heel doelgericht in op allerlei nieuwe technologieën die Industrie 4.0 ondersteunen: van IoT tot AI.

Doorgedreven connectiviteit

Centraal in het concept van Industrie 4.0 staat het verzamelen van grote hoeveelheden data via onderling verbonden technologiesystemen. Een diepgaande analyse van al die data moet maakbedrijven toelaten om hun industriële processen te verbeteren. De onderlinge verbondenheid van al die verschillende systemen moet niet alleen een totaalbeeld van de verspreide data helpen creëren, maar ook toelaten om nieuwe verbanden te ontdekken.

"Vroeger waren OT-systemen niet, of in elk geval niet in die mate, met elkaar verbonden", zegt Koen Tamsyn, Business Unit Lead Cybersecurity bij Inetum. Vandaag ligt dat anders. Dat blijkt onder meer uit een studie van SANS Institute. "Daarin geeft bijna de helft van alle bevraagde bedrijven aan dat de connectiviteit van hun operationele controlesystemen sterk is toegenomen."

Daar zijn volgens Koen Tamsyn ook goede redenen voor. "Naast het capteren van de operationele data die ze nodig hebben om hun processen te optimaliseren, willen ze die operationele systemen ook vanop afstand kunnen aansturen en onderhouden."

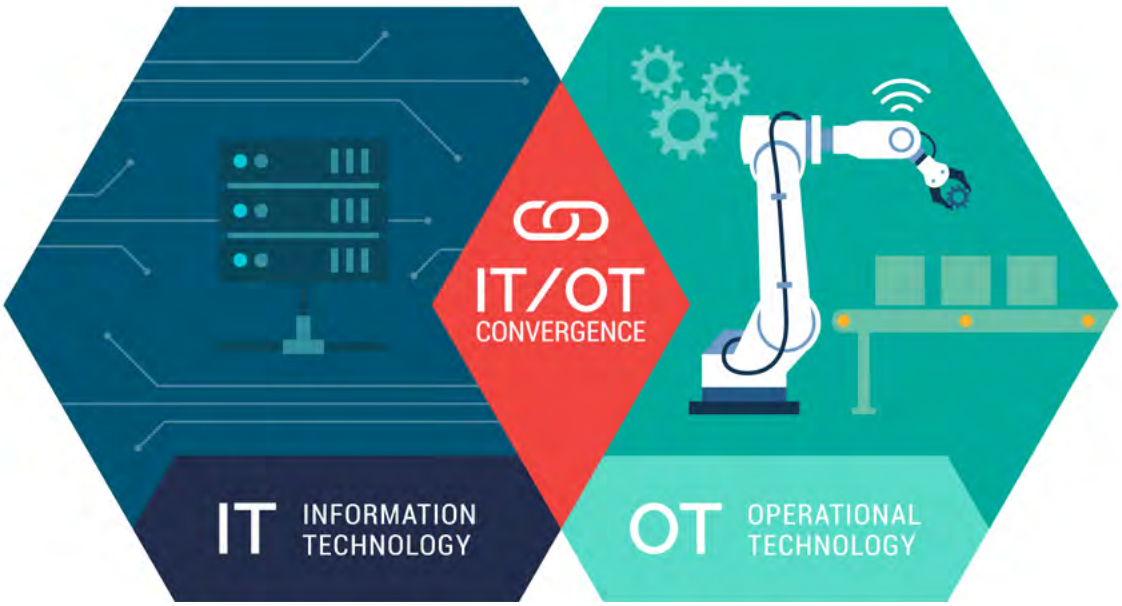
Aanvalsoppervlak vergroot

Die sterke toename van geconnecteerde systemen biedt opportuniteiten voor de business, maar stelt ze tegelijk bloot aan nieuwe risico's. "Het aanvalsoppervlak neemt toe", beklemtoont Koen Tamsyn. "Kritieke operationele systemen, die bijvoorbeeld instaan voor de productie, komen nu in het vizier van cybercriminelen.

Ook langs die weg kunnen zij voortaan inbreken in jouw organisatie. Daarbij komt dat de aangerichte schade voor de meeste maakbedrijven een pak groter is en veel zwaarder doorweegt, precies omdat hun productie zelf nu in het gedrang komt."

Gelukkig komen getroffen bedrijven steeds meer naar buiten met informatie over zulke cyberincidenten. De toegenomen zichtbaarheid van incidenten met een operationele impact draagt vandaag bij tot een verhoogd bewustzijn rond risicobeheer en cyberbeveiliging in operationele omgevingen die daar in het verleden niet of (te) weinig gevoelig voor waren.

Daarbovenop is er de toegenomen druk van allerlei regulering, zoals de NIS2-richtlijn van de EU. "In die richtlijn staat OT-security weliswaar niet expliciet vermeld", geeft Koen Tamsyn aan. "Maar de richtlijn is van toepassing op elk geconnecteerd apparaat, zelfs een koffiemachine, en slaat dus zeker niet op IT-security alleen."



Fundamentele verschillen

Nu ook in maakbedrijven het bewustzijn rond OT-security groeit, moeten Koen Tamsyn en zijn collega's vaststellen dat de kennis en ervaring op dat vlak niet altijd voorhanden zijn. "En net omdat de mogelijke impact van security-ingrepen en -incidenten op zo'n operationele omgeving zoveel groter is, maakt dat de drempel hoger om er zelf werk van te maken." Dan is het zaak om een geschikte partner te vinden die, in het ideale scenario, zowel voor IT-security als OT-security de nodige kennis en ervaring kan voorleggen.

"Niet evident," beseft Koen Tamsyn, "want beide securitydomeinen zijn nu eenmaal fundamenteel verschillend. Om maar iets te noemen: bij OT-security zijn de veiligheid en beschikbaarheid van de operationele systemen cruciale parameters. Werkongevallen wil je tot elke prijs vermijden en je systemen moeten continu blijven draaien. Bij IT-security zijn de integriteit en vertrouwelijkheid van de data dan weer doorslaggevend. Je wilt niet dat iemand je data zomaar kan wijzigen. En je wilt dat enkel de juiste mensen toegang tot die data hebben.

Dat is een totaal andere kijk op security. Die compleet andere mindset maakt ook dat het niet altijd even makkelijk is om IT- en OT-securityspecialisten met elkaar te laten praten."

Doorgedreven segmentering

In dat verband is het goed om te weten dat Inetum niet alleen een erkende leverancier is van IT-securitydiensten. "Wij leggen ons ook al jaren toe op de convergentie van IT en OT. In dat specifieke domein hebben wij, samen met technologiepartner Fortinet, intussen heel wat kennis en ervaring opgebouwd. Zo hebben wij hier ook al enkele grote projecten achter de rug."

Daarbij gaat Inetum steevast tewerk volgens een vast stappenplan. "In een eerste stap creëren we de nodige visibiliteit, zodat je een goed overzicht krijgt van je OT-omgeving. Daarvoor maken we gebruik van tools voor assetinventory en assetmanagement. Stap twee is minstens even belangrijk. Daarin gaan we jouw netwerken op een doorgedreven wijze segmenteren, zodat bij een incident de impact beperkt blijft tot idealiter één segment. Ook het verkeer tussen al die segmenten gaan we controleren. Zo kan je heel granulair je securityregels invoeren en je OT-securitybeleid zorgvuldig opbouwen."

Een volgende stap behandelt authenticatie en de beveiliging van de toegang op afstand tot systemen, met name via MFA. "Ten slotte controleren we je applicaties, waarbij we duidelijk aangeven welke er wel en niet in jouw OT-omgeving mogen draaien, en gaan we je systemen virtueel patchen. Op die manier brengen we de beveiliging van jouw OT-omgeving naar een hoger niveau van maturiteit."

Meer info?

Wenst u uw OT-security naar een hoger niveau te tillen? Ons OT cybersecurity assessment brengt snel duidelijkheid waar de quick wins voor u liggen.

Natuurlijk kan u voor meer info ook altijd terecht bij onze experten of uw vertrouwde contactpersoon.

Bekijk de webinar over hoe Inetum IT- en OT-security op elkaar afstemt met Fortinet!

FORTINET

Inetum
A. Vaucampslaan 42
1654 Huizingen, België
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum