Bescherm industriële netwerken pro-actief tegen cyberaanvallen met behulp van IPS-technologie of whitelisting controle.

Tekst *Johan Debaere* | **Beeld** *Technolec/Moxa*

INDUSTRIËLE NETWERKEN PRO-ACTIEF BESCHERMEN TEGEN CYBERBEDREIGINGEN

Cyberaanvallen, al dan niet bewust, leggen de laatste tijd wel vaker de infrastructuur van bedrijven plat en zorgen voor veel schade. De creatie van afzonderlijke zones in de industriële netwerkarchitectuur kan de schade beperken, maar cybersecurity experts stellen ook pro-actievere maatregelen voor om industriële netwerken te beschermen, met name door een industrieel Intrusion Prevention System (IPS), dat inbraken effectief kan tegengaan en de impact ervan kan verminderen.

Om operationele efficiëntie en beschikbaarheid na te streven, is het altijd belangrijk om rekening te houden met cyberbeveiliging. Men kan industriële netwerken beter beveiligen door een veilige funderingsvriendelijke netwerkinfrastructuur, waardoor geautoriseerd verkeer naar de juiste plaatsen kan stromen, of door kritieke assets te identificeren en deze gelaagde, proactieve bescherming te bieden, zoals een industriële IPS en whitelisting controle.

Industriële IPS

Een IPS detecteert en blokkeert geïdentificeerde bedreigingen door netwerken voortdurend te monitoren, op zoek te gaan naar mogelijke kwaadaardige cyberincidenten en informatie daarover te loggen. Het beschikt over Deep Packet Inspection (DPI) technologie, verbetert de zichtbaarheid van de netwerkbeveiliging, helpt uiteindelijk de risico's te beperken en industriële netwerken te beschermen tegen beveiligingsbedreigingen. De IPS kan voor kritieke assets, zoals PLC's en HMI's, geplaatst worden om de netwerkbeveiliging te verbeteren en de beschikbaarheid van het netwerk te garanderen, terwijl die assets tegen manipulatie door kwaadwillige actoren beschermd worden. Het doel is tweeledig: kwaadaardig verkeer blokkeren en het probleem beperken als het zich toch voordoet.

Rekening houden met bewerkingsvereisten

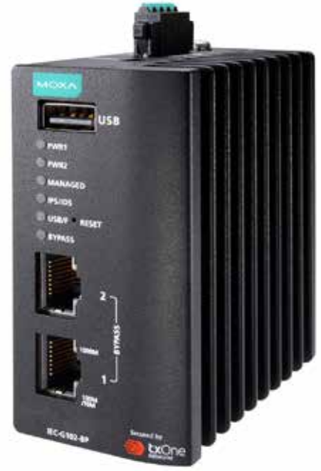
"Hoewel IPS-technologie al een tijdje heel goed werkt op IT-netwerken, is het moeilijk om een IPS rechtstreeks in OT-netwerken in te zetten. De eerste prioriteit van OT-netwerken is immers beschikbaarheid en prestaties, terwijl bij IT-cyberbeveiliging vertrouwelijkheid op de eerste plaats komt. Als men bij de implementatie van een IPS in OT-netwerken geen rekening houdt met de dagelijkse bewerkingsvereisten van OT-ingenieurs, kunnen belangrijke besturingsopdrachten voor de productie geblokkeerd worden en de bedrijfsvoering verstoord", stelt Karel Mus van Technolec. "Om te voldoen aan de OT-cyberbeveiligingsvereisten, is het essentieel om OT-gecentreerde DPI-technologie te gebruiken. Die kan immers meerdere industriële protocollen identificeren en specifieke functies zoals lees- of schrijftoegang toestaan of blokkeren. Op basis van het geïdentificeerde protocol kan een industriële IPS vervolgens ongeautoriseerde protocollen of functies voorkomen, waardoor het verkeer op industriële netwerken vertrouwd en niet schadelijk is."

'Onze bedrijven worden steeds vaker het slachtoffer van al dan niet doelgerichte cyberaanvallen'

Whitelisting controle

Een andere mogelijkheid is 'whitelisting controle', waarbij alleen toegang verleend wordt tot de geautoriseerde apparaten, service, protocolindeling en besturingsopdrachten van een geautoriseerde lijst, de zogenaamde witte lijst. Op die manier worden alle netwerkactiviteiten op industriële netwerken geautoriseerd en kunnen netwerkexploitanten gedetailleerde toegangscontroles op verschillende niveaus definiëren, afhankelijk van operationele vereisten. "OT-ingenieurs kunnen een witte lijst van apparaten en services of IP-poorten definiëren die toegang hebben tot het gehele of een deel van het netwerk. Ze kunnen ook het geautoriseerde protocolformaat definiëren om te voorkomen dat onbevoegde commando's door de netwerken gaan en zelfs definiëren welke besturingsopdrachten door het netwerk kunnen gaan om menselijke fouten te verminderen die gepaard gaan met het verzenden van een verkeerde besturingsopdracht", licht de zaakvoerder van Technolec toe. "Dankzij dergelijke controle op een witte lijst wordt de kans op een DoS-aanval door OT-trojans aanzienlijk verminderd."

Een industriële IPS detecteert en blokkeert geïdentificeerde bedreigingen.



Moxa introduceert de Industrial Cybersecurity Solution. De industriële IPS van Moxa beschermt kritieke assets tegen cyberaanvallen.

OT-IT Integrated Security van Moxa

Als reactie op de toenemende cyberdreigingen introduceert Moxa, dat al langer beveiligde netwerkapparatuur, zoals routers en Ethernet switches ontwikkelt, zijn Industrial Cybersecurity Solution. Mus van officieel verdeler Technolec sluit af: "Door OT- en IT-technologieën effectief te integreren, beschermt de industriële IPS van Moxa uw kritieke assets tegen de nieuwste cyberbeveiligingsbedreigingen en helpt het de transitie van de industriële wereld naar veilige automatiseringsarchitecturen te versnellen." ■