Cybersecurity

Monitoren van het OT-netwerk geeft inzicht

Voldoet u aan normen, wet- en regelgeving?

Steeds meer organisaties zien de noodzaak om het netwerkverkeer van de Operationele Technologie (OT) te monitoren. Vaak ligt daarbij het zwaartepunt op het detecteren van afwijkingen in het netwerkverkeer. Dergelijke ‘anomaly detection’ alléén is echter niet voldoende. Organisaties verwachten ook andere functionaliteit, zoals inzicht in de kwaliteit van de communicatie en ondersteuning voor asset management. Een goede OT-monitoringoplossing draagt daaraan bij.

‘Anomaly detection’ is een essentieel onderdeel van OT-monitoring. Na het aanmaken van een blueprint van het normale en te verwachten netwerkverkeer binnen de OT-omgeving, wordt al het netwerkverkeer vergeleken met deze blueprint en worden afwijkingen gerapporteerd. Omdat OT-omgevingen vaak statisch zijn, is dit een goede manier om inzicht te krijgen in afwijkingen in het netwerkverkeer.

Meer dan afwijkingen detecteren

Van een professionele OT-monitoringoplossing verwacht men echter meer dan dat. Organisaties willen niet langer alleen afwijkingen in de reguliere communicatie kunnen zien, maar verwachten ook andere functionaliteit. Zo willen bedrijven ook inzicht in de kwaliteit van de communicatie, omdat ze daarmee mogelijke verbindings- of configuratieproblemen kunnen oplossen. Ook verwacht men steeds vaker ondersteuning voor asset management, iets waar een goede OT-monitoringoplossing aan kan bijdragen.

“Het is evident dat een OT-monitoringoplossing de protocollen die specifiek zijn voor een OT-omgeving feilloos moet begrijpen”, zegt Marcel Jutte, managing director van Hudson Cybertec. “Oplossingen die gebouwd zijn voor IT-omgevingen herkennen en verwerken deze OT-protocollen niet, waardoor er ook geen juiste interpretatie van het netwerkverkeer kan plaatsvinden.” Als hele communicatiestromen onbegrepen blijven door de oplossing, ontstaat er natuurlijk een incompleet beeld van juist die assets waar het binnen de OT-omgeving om draait. Een OT-monitoringoplossing dient dan ook alle protocollen te herkennen die binnen de OT-omgeving van een organisatie worden gebruikt. Een oplossing die volledig vanuit OT-perspectief is ontwikkeld, is dan ook essentieel!

Wet- en regelgeving

Bedrijven stellen steeds meer eisen aan OT-monitoring omdat er steeds meer van henzelf wordt gevraagd op gebied van cybersecurity. Wet- en regelgeving omtrent de digitale weerbaarheid van de vitale infrastructuur verandert en wordt aangescherpt. Een voorbeeld hiervan is de Network and Information Security (NIS) Directive, die in Nederland beter bekend staat als de NIB-richtlijn (netwerk- en informatiebeveiliging) en een concrete uitwerking heeft gekregen in de Wbni (Wet beveiliging netwerk- en informatiesystemen). De NIS Directive wordt op dit moment herzien, wat zijn uitwerking zal hebben op de Nederlandse wetgeving. Bedrijven in de vitale infrastructuur zijn aangewezen als AED (Aanbieder Essentiële Diensten) of DSP (Digital Service Provider). Zij hebben een meldplicht voor cybersecurity-incidenten en een zorgplicht voor cybersecurity. Dit betekent simpelweg dat zij hun digitale weerbaarheid aantoonbaar op orde dienen te hebben. Deze organisaties gebruiken vaak normenkaders, zoals de IEC 62443, BIO, VEWIN of CSIR, om zich aan te conformeren. Op deze wijze verzekeren ze zich ervan dat ze cybersecurity op een consistente en verantwoorde wijze managen, de juiste maatregelen treffen om de digitale weerbaarheid te verhogen en aantoonbaar in lijn werken met wet- en regelgeving.

De gamechanger

Een echte gamechanger in het speelveld van OT-monitoring is OT Insight. Deze OT-monitoringoplossing biedt natuurlijk de standaardfunctionaliteit die andere oplossingen bieden. Maar wat deze oplossing zo uniek maakt, is dat het monitoringplatform ook afwijkingen in eerder genoemde normen detecteert en rapporteert aan de asseteigenaar. Jutte legt uit: “Wij hebben vooral klanten in de vitale infrastructuur. Zij moeten voldoen aan deze wet- en regelgeving. OT Insight is voor hen een ideale oplossing. Maar ook bedrijven die niet onder de Wbni vallen zien het belang van deze normen en de grote voordelen van deze oplossing.”

Met OT Insight is in één oogopslag op een overzichtelijk dashboard te zien in welke mate er overeenstemming is met de verschillende normenkaders. Daarnaast kunnen organisaties eenvoudig zien op welke punten niet (of niet langer) aan een kader wordt voldaan en waar actie benodigd is. Men krijgt melding zodra een afwijking wordt geconstateerd, zodat hierop tijdig kan worden geacteerd. Detailinformatie is met een simpele muisklik beschikbaar. Andere unieke eigenschappen zijn dat het een volledig Nederlands-Duitse ontwikkeling is en dat het platform volledig modulair en hardwareonafhankelijk is opgezet. “Voor de beveiliging van de BV Nederland is het van belang dat bedrijven toegang hebben tot een volledig Europese oplossing. Bedrijven mogen voor cybersecurity niet alleen afhankelijk zijn van technologie uit niet-Europese landen”, verduidelijkt Jutte. Deze trend is ook te zien in bijvoorbeeld de telecomsector, waar apparatuur uit bepaalde landen in de ban wordt gedaan om eventuele spionage op het telecomnetwerk te voorkomen.

Integratie van systemen

Bedrijven hebben dus behoefte aan een lokaal gebouwde maatwerkoplossing. Elke organisatie heeft specifieke wensen op het gebied van digitale weerbaarheid. Ook binnen een organisatie hebben verschillende stakeholders verschillende belangen. Een onderhoudsengineer van een OT-omgeving heeft immers behoefte aan heel andere informatie dan een security officer of het managementteam. De juiste informatie wordt door OT Insight op een voor de doelgroep relevante wijze, door middel van specifiek op die functie gemaakte dashboards gepresenteerd.

Een OT-monitoringoplossing als OT Insight helpt organisaties bij hun uitdagingen om de OT-omgeving digitaal weerbaar te maken en te houden. In een omgeving waar integratie van allerlei systemen op het technische netwerk steeds meer toeneemt, is dat zeker geen luxe, maar zelfs een noodzaak geworden. Zeker nu steeds vaker ook gebouwgebonden systemen zoals toegangscontrolesystemen, klimaatbeheersing en zelfs alarmeringssystemen voor brand en inbraak worden ontsloten op hetzelfde netwerk, is het zaak om duidelijkheid te verkrijgen in wat er allemaal gebeurt. En om te weten of al deze verschillende systemen überhaupt op een veilige manier met elkaar kunnen omgaan. Jutte concludeert: “Uiteindelijk draait ook cybersecurity in grote mate om inzicht. Alleen als je weet wat er gebeurt in je OT-omgeving, kun je werkelijk ‘in control’ zijn.”

Meer info over OT Insight:
neem contact op met Hudson Cybertec
via info@hudsoncybertec.com
of kijk op www.hudsoncybertec.com