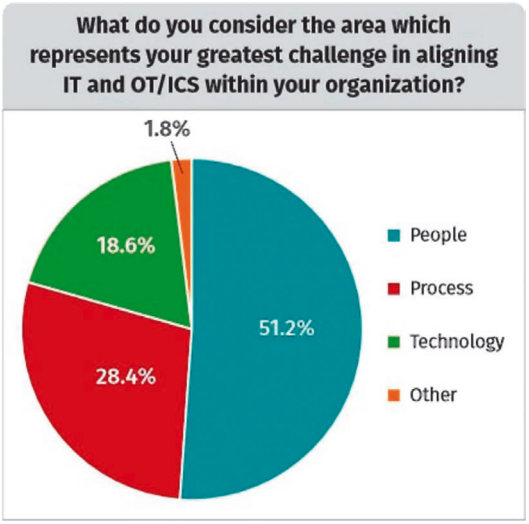
Studie zur Konvergenz von IT und OT: Auch Cybersecurity zusammenführen

Bericht von Trend Micro zeigt große Lücken bei Detection & Response in der OT



Trend Micro, einer der weltweit führenden Anbieter von Cybersicherheitslösungen, veröffentlicht die Ergebnisse eines neuen Reports, aus dem hervorgeht, dass unternehmensinterne Security Operation Center (SOCs) ihre Fähigkeiten auf den OT-Bereich ausweiten. Fehlende Sichtbarkeit und mangelnde Kenntnisse der Mitarbeiter stellen jedoch erhebliche Hindernisse dar.

Security Operation Center

Laut der Studie des japanischen Cybersecurity-Anbieters verfügt mittlerweile die Hälfte der Unternehmen über ein SOC, das ein gewisses Maß an ICS/OT-Transparenz (Industrial Control Systems / Operational Technology, dt. Industrielle Steuerungssysteme / Betriebstechnologie) aufweist. Doch auch bei befragten Unternehmen, die über ein umfassenderes SOC verfügen, speist nur etwa die Hälfte (53 Prozent) ihrer OT-Umgebung Daten für Erkennungszwecke ein.

Dieses Defizit zeigt sich auch in einem anderen Studienergebnis. Demnach ist die Erkennung von Cybervorfällen (63 Prozent) die wichtigste Fähigkeit, die Befragte über IT- und OT-Silos hinweg integrieren wollen. Dem folgen die Bestandsaufnahme der vorhandenen Assets (57 Prozent) sowie das Identitäts- und Zugangsmanagement (57 Prozent). Ereignisse in IT- und OT-Umgebungen übergreifend und frühzeitig zu erkennen, ist für die Ursachenidentifikation und die Bedrohungsabwehr entscheidend.

EDR und NSM

Der Bericht betont die Bedeutung, die Endpoint Detection and Response (EDR) und das interne Network Security Monitoring (NSM) haben, indem sie Daten über die Grundursachen von Cyberangriffen liefern. Allerdings wird EDR nur bei weniger als einem Drittel (30 Prozent) der befragten Unternehmen sowohl auf Engineering-Systemen als auch Produktionsanlagen eingesetzt. NSM kommt auf der Ebene der physischen Prozesse und der grundlegenden Kontrolle in OT-Umgebungen noch seltener (<10 Prozent) zum Einsatz.

Große Herausforderungen

Abgesehen von den Lücken in der Sichtbarkeit zeigt die Studie außerdem, dass die Ausweitung von Security Operations (SecOps) auf IT- und ICS/OT-Umgebungen mit großen personellen und verfahrenstechnischen Herausforderungen verbunden ist. Vier der fünf größten Hindernisse, die von den Befragten genannt wurden, adressieren das Thema Personal:

- Schulung von IT-Mitarbeitern in OT-Security (54 Prozent)
- Kommunikationssilos zwischen relevanten Abteilungen (39 Prozent)
- Einstellung und Mitarbeiterbindung von Cybersecurity-Experten (38 Prozent)
- Schulung von OT-Mitarbeitern in IT (38 Prozent)
- Unzureichende Risikotransparenz zwischen IT- und OT-Bereichen (38 Prozent)

Auch veraltete Technologie bereitet Schwierigkeiten bei der Visibilität: Die technischen Einschränkungen von Altgeräten und Netzwerken (45 Prozent) sowie IT-Technologien, die nicht für OT-Umgebungen konzipiert sind (37 Prozent), kristallisieren sich, neben dem mangelnden OT-Wissen der IT-Mitarbeiter (40 Prozent), als größte Probleme heraus.

Anstrengungen verdoppeln

In Zukunft wollen die Befragten ihre Anstrengungen für eine bessere Security-Konvergenz über IT und OT hinweg verdoppeln und so einen besseren Einblick in OT-Bedrohungen erlangen. Zwei Drittel (67 Prozent) planen, ihr SOC zu erweitern und diejenigen, die bereits EDR einsetzen (76 Prozent), wollen dies in den kommenden 24 Monaten auch auf den ICS/OT-Bereich übertragen. Darüber hinaus planen 70 Prozent der Unternehmen, die bereits NSM-Funktionen eingeführt haben, eine Ausweitung dieser Technologie im gleichen Zeitrahmen.

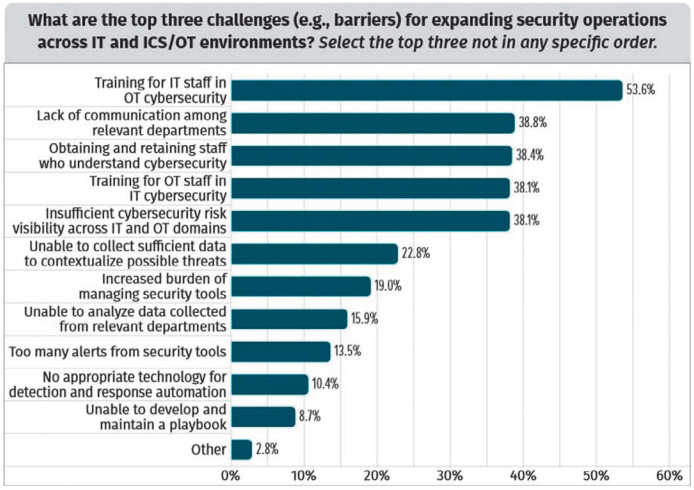
„Die IT-OT-Konvergenz treibt in vielen Industrieunternehmen bereits die digitale Transformation voran. Um Risiken in diesen Umgebungen effektiv zu managen, müssen jedoch auch die IT- und OT-SecOps konvergieren.“, erklärt Udo Schneider, IoT Security Evangelist bei Trend Micro. „OT-Sicherheitsprogramme hinken vielleicht noch hinterher, bieten aber die Gelegenheit, die Transparenz- und Kompetenzlücke zu schließen, indem sie auf einer einzigen SecOps-Plattform wie Trend Vision One konsolidiert werden.“

Weitere Informationen

Den vollständigen Report, Breaking IT/OT Silos With ICS/OT Visibility, finden Sie in englischer Sprache unter: https://resources.trendmicro.com/SANS-ICS-OT-Visibility-Survey.html

Über den Report

Trend Micro beauftragte das SANS Institute, 350 Mitglieder der SANS-Community zu befragen, die in kritischen Infrastrukturbereichen in den USA, Europa und Asien tätig sind. ◄



Trend Micro Deutschland
www.trendmicro.com