Alarmierende Cyber-Sicherheitslücken in der Industrie: Wo stehen wir 2025?

Eine neue Studie enthüllt, dass viele Industrieunternehmen in der Cybersicherheit hinterherhinken, trotz wachsender IoT-Bedrohungen.

Deutschland - Im digitalen Zeitalter sind Cyberbedrohungen in der Industrie längst keine Seltenheit mehr. Die neueste Studie namentlich der Global Industrial Cybersecurity Benchmark 2025, veröffentlicht von Forescout und durchgeführt von Takepoint Research, beleuchtet die aktuelle Lage und zeigt, dass sich viele Unternehmen in der industriellen Automatisierung in einer Zwickmühle befinden.

Interessanterweise geben 44 Prozent der befragten Industrieunternehmen an, über eine effektive Echtzeit-Cyber-Transparenz zu verfügen. Doch fast 60 Prozent können ihre OT-/IoT-Bedrohungserkennung nicht als zuverlässig einstufen. Dies bringt die Diskrepanz zwischen Behauptung und Realität

zur Sprache: Während die eine Hälfte sich sicher fühlt, kämpfen die meisten anderen mit grundlegenden Sicherheitslücken.

Herausforderungen im Cybersecurity-Klima

Der Bericht zeigt, dass die rasante Digitalisierung und die damit verbundene Erhöhung der Konnektivität zwar viele Chancen bringen, aber gleichzeitig auch das Cyberrisiko exponentiell steigern. Über 50 Prozent der Organisationen nehmen Lieferkettenbedrohungen und Cyberkriminalität als größte Sicherheitsherausforderungen wahr. Die Umfrage beleuchtet, dass nur 17 Prozent der Unternehmen von ausgereiften OT-Sicherheitspraktiken berichten können, während 64 Prozent ihre Cybersecurity-Reife als grundlegend kategorisieren, was oft manuelle Prozesse und fragmentierte Sichtbarkeit bedeutet.

Die Studie befragte insgesamt 236 Führungskräfte aus den Bereichen OT und Automatisierung zwischen Januar und März 2025. Dabei fallen einige ernüchternde Zahlen auf: Über 33 Prozent der Unternehmen benötigen mehr als 90 Tage zur Behebung von Bedrohungen, und 63 Prozent benötigen aufgrund unzureichender Metriken und Wartungsbeschränkungen mehr als 30 Tage für das Management ihrer Bedrohungen. Tatsächlich setzen 57 Prozent der Unternehmen mehr als drei verschiedene Tools ein, um ihre IT-, OT- und IoT-Umgebungen zu überwachen.

Laut einer Analyse von Forescout, die die gleichen Befragungsdaten verwendet, spiegelt sich die Überlastung auch in den arbeitsintensiven Aufgaben wider: Fast die Hälfte der Unternehmen gammelt daran, Schwachstellen zu priorisieren (49 Prozent) und Risikominderung zu betreiben (44 Prozent).

Der Blick auf die Zukunft

Die Lage muss ernst genommen werden: Eine andere Umfrage, die in einem OT+IoT Cybersecurity Report 2024 des Cybersicherheitsunternehmens Onekey veröffentlicht wurde,

zeigt, dass die Zahl der vernetzten IoT-Geräte von 12,3 Milliarden im Jahr 2020 auf über 15,1 Milliarden im Jahr 2023 gestiegen ist und bis 2025 auf etwa 27 Milliarden anwachsen soll. Diese rasant wachsende Anzahl an Geräten erhöht nicht nur das Potenzial für Innovation, sondern auch für Cyberangriffe.

Der Schutz dieser Systeme hinkt maßgeblich hinterher. Nur 46 Prozent der befragten IT-Verantwortlichen sind überzeugt, dass die Industrie ausreichend vor Cyberangriffen geschützt ist. Weniger als ein Drittel kennt sich mit den relevanten Vorschriften und Standards zur Cybersicherheit aus. Jan Wendenburg, CEO von Onekey, warnt, dass viele Hersteller Schwierigkeiten haben, rechtliche Anforderungen adäquat zu erfüllen. Dennoch bleibt es unerlässlich, dass Unternehmen alle erforderlichen Maßnahmen zur Gewährleistung ihrer Cybersicherheit implementieren.

Die Herausforderungen sind vielfältig, doch das Bewusstsein für Cyberrisiken in der Industrie ist entscheidend, um den kommenden Bedrohungen wirksam entgegenzutreten. Angesichts der geopolitischen Spannungen wird deutlich, dass integrierte Sicherheitsansätze nicht nur wünschenswert, sondern auch unverzichtbar sind.

Details	
Ort	Deutschland
Quellen	• www.infopoint-security.de • www.forescout.com • www.elektronikpraxis.de

Besuchen Sie uns auf: wom87.de