EINE PUBLIKATION VON SMART MEDIA

SMART.

Infrastruktur 2030



November '26

Peter Körte

Peter Körte erklärt, wie industrielle KI und intelligente Energieinfrastruktur Europas Chance für technologische Souveränität und eine führende Rolle im globalen Wettbewerb werden können.

Lesen Sie mehr auf **fokus.swiss**

»Der Schutz der OT-Umgebungen entscheidet über die Versorgungssicherheit«

Die Vernetzung von IT und Operational Technology (OT) stellt Betreiber kritischer Infrastrukturen vor neue Herausforderungen. Gleichzeitig erhöhen NIS2 und die KRITIS-Regulierung den Handlungsdruck. Christopher Gasteier, Teamleiter Business Development Operational Technology bei Controlware, erläutert, wie sich industrielle Anlagen schützen lassen, ohne den Betrieb zu gefährden.



Christopher Gasteier
Teamleiter Business Development Operational Technology

Herr Gasteier, warum rückt die Sicherheit industrieller Anlagen gerade jetzt in den Fokus?
Energieversorger, Stadtwerke und Industrieunternehmen vernetzen ihre Anlagen zunehmend mit klassischen IT-Systemen, um Prozesse effizienter zu steuern und zu überwachen. So entstehen aber neue Angriffsflächen – zumal viele OT-Umgebungen über Jahrzehnte gewachsen sind und Systeme umfassen, die gar nicht für eine Vernetzung konzipiert wurden. Während die klassische IT Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Diensten schützt, stehen in OT-Umgebungen der sichere und zuverlässige Anlagenbetrieb sowie die Integrität der industriellen Prozesse im Fokus.

Wie können Betreiber ihre OT-Umgebungen schützen, ohne den Betrieb zu gefährden?
Der erste Schritt ist Transparenz. Betreiber kritischer Infrastrukturen müssen wissen, welche Systeme vorhanden sind, wie diese kommunizieren und wo ihre Schwachstellen liegen. Ein bewährter Ansatz ist ein etabliertes Risikomanagement. Sicherheitsmaßnahmen müssen auf die betrieblichen Anforderungen abgestimmt, vorab geprüft und stets so umgesetzt werden, dass Betriebsrisiken minimiert werden. Controlware setzt hier auf ganzheitliche Sicherheitsarchitekturen, kontinuierliches Monitoring und klare Prozesse. Unser modularer OT-Leitstand führt Betriebs- und Sicherheitsinformationen aus vielen Systemen in einem zentralen Lagebild zusammen. Dabei verbinden wir technische Betriebsunterstützung, strukturierte Service-Prozesse und OT-spezifisches Know-how. Betriebs- und Sicherheitsinformationen werden zusammengeführt, um Auffälligkeiten zu bewerten und fundierte Entscheidungen vorzubereiten. Die Betriebsverantwortung verbleibt jedoch bei den Betreibern. Eingriffe erfolgen auf Grundlage vereinbarter Zuständigkeiten und Freigabeprozesse.

Welche Anforderungen ergeben sich aus NIS2 und den KRITIS-Vorgaben?
Die Pflichten hängen davon ab, wie ein Unternehmen eingeordnet ist und welche branchenspezifischen Vorgaben gelten. Gerade NIS2 betrifft nicht nur klassische KRITIS-Betreiber: Es geht darum, Cyberrisiken systematisch zu bewerten, angemessene Schutzmaßnahmen umzusetzen und auf Sicherheitsvorfälle vorbereitet zu sein. Hinzu kommen abgestufte Registrierungs-, Melde- und Nachweispflichten für die Geschäftsleitung.

Diese Vorgaben sind jedoch nicht nur auf dem Papier zu erfüllen: Die Maßnahmen müssen regelmäßig überprüft und angepasst werden – unter Berücksichtigung der besonderen Anforderungen des laufenden OT-Betriebs.

Neben Technologie geht es dabei um klare Verantwortlichkeiten, belastbare Prozesse und qualifizierte Fachkräfte. Gerade diese sind oft knapp. Umso wichtiger sind Betriebsmodelle, die internes Wissen sichern und bei Bedarf externe Spezialist:innen einbinden. Die Verantwortung für die Compliance verbleibt jedoch beim Unternehmen.

Wie unterstützt Controlware konkret bei der Absicherung der Infrastrukturen?
Wir begleiten Kunden bei der Bestandsaufnahme, Konzeption und Implementierung geeigneter Sicherheitsarchitekturen. Dabei verzahnen wir unsere OT-Expertise mit Managed Cyber Defense Services: Unsere Spezialist:innen überwachen IT-Infrastrukturen rund um die Uhr, erkennen und bewerten Aktivitäten und unterstützen bei der Reaktion auf Sicherheitsvorfälle. Im Zusammenspiel mit dem OT-Leitstand entsteht ein ganzheitliches Sicherheits- und Betriebsmodell. So können Betreiber kritischer Infrastrukturen ihre Cyberresilienz stärken und die Einhaltung regulatorischer Vorgaben unterstützen, ohne alle Spezialkompetenzen und Kapazitäten vorhalten zu müssen.

Weitere Informationen unter:
controlware.de

controlware