IT-/OT-NETZWERKE

GRÜNDE FÜR EINE SCHWIERIGE KONVERGENZ

Khobeib Benboubaker
Industry Business Line Manager, Stormshield

Mit Blick auf die Industrie der Zukunft wird in der industriellen Welt derzeit bereits an der Konvergenz der industriellen Netzwerke (OT) und der Computernetzwerke (IT) gearbeitet. Dieses Phänomen verdeutlicht die Besonderheiten dieser Infrastrukturen und offenbart bestimmte Risiken. Das gilt vor allem hinsichtlich der Cybersicherheit.

Vorausschauende Wartung, eine Produktion, die den Erwartungen der Verbraucher so nah wie möglich kommt: Diese Industrie 4.0 macht bei der Konvergenz von Computer- und Industrienetzwerken zahlreiche Versprechungen. Die Zusammenführung dieser beiden sehr unterschiedlichen Infrastrukturen ist jedoch komplexer, als es scheint.

„Die Industrie der Zukunft fügt eine Dimension von Daten hinzu, die von Maschinen oder Benutzern erhoben werden. Durch eine Konvergenz der IT-/OT-Netzwerke können diese genutzt werden, um Wartungszeiten zu reduzieren, Ausfällen vorzugreifen oder Umweltkosten zu senken“, erklärt Stéphane Prévost, Product Marketing Manager bei Stormshield.

ENTWICKLUNG DER IT- UND OT-INFRASTRUKTUREN MIT ZWEI GESCHWINDIGKEITEN

Bereits seit einigen Jahren verschwimmt in der Industrie die Grenze zwischen IT und OT. Die Informationstechnologie, die in den Leitstellen der Werkstätten regelmäßig erneuert wird, wird mit einem Maschinenpark kombiniert, der eine deutlich längere Lebensdauer und deutlich höhere Abschreibungen aufweist. Ein Beispiel ist der USB-RS232-Konverter, mit dem eine Maschine und ihre Sprache (USB für einen PC) von einer anderen Maschine verstanden werden konnte (RS232 für die Industriemaschine). **Für die OT-Teams bestand die Herausforderung darin, diese beiden Welten zu verbinden, die sich in einem unterschiedlichen Tempo entwickeln.** *„Industrielle Werkzeuge haben ihr eigenes Tempo und System, um die verschiedenen aktiven Elemente des Netzwerks zu verbinden: den Feldbus. Er entstand während der zweiten industriellen Revolution und erlaubte die Massenproduktion. Dann überlebte er die dritte industrielle Revolution, welche eine Automatisierung ermöglichte. Die Koexistenz ist im Computerzeitalter jedoch viel komplizierter*", erklärt Stéphane Prévost. Tatsächlich müssen im Zeitalter des Internets die Befehle in industriellen Protokollen, die es in Werkstätten und auf Konsolen noch gibt, nunmehr über TCP/IP übertragen werden.

COMPUTERNETZWERKE UND INDUSTRIELLE NETZWERKE: VON GESTALTUNGSKONTEXTEN ZU GEGENSPIELERN

Die grundlegenden Unterschiede bei der Sicherheit von IT- und OT-Netzwerken können auf ihre Konzeption zurückgeführt werden.

Die Computernetzwerke sind eher für die Übertragung großer Datenmengen ausgelegt. Geboren in einer offenen Umgebung, steht die Interaktion im Mittelpunkt ihrer Funktion, und ihre Protokolle sind abgesichert. Industrielle Netzwerke sind dagegen auf die Weiterleitung von Befehlen ausgerichtet, um die ordnungsgemäße Steuerung des industriellen Prozesses zu gewährleisten. Diese Netzwerke, die in der Regel von einer Werkstatt zur anderen unabhängig konzipiert sind, wurden nicht besonders abgesichert, da sie als isoliert und bereits durch die Sicherheitsrichtlinie der Werke, in denen sie gehostet wurden, als geschützt galten.

„Von Anfang an wurde die IT mit sicheren Datenprotokollen (https für das Surfen im Internet, SMTPS für den E-Mail-Verkehr usw.) ausgestattet, während bei den operativen Netzwerken die Sicherheit nur auf Ebene des Industriestandorts berücksichtigt wurde. So wurde es nicht als sinnvoll erachtet, die in einer engen und sicheren Umgebung entwickelten Netzwerke um eine Schutzschicht zu ergänzen", fügt Stéphane Prévost hinzu.

INDUSTRIELLE NETZWERKE: EINE EINZIGARTIGE VERWALTUNG

Bis vor kurzem brauchte die Industrie die Verwaltung ihrer OT-Infrastruktur nicht zu zentralisieren: Diese Netzwerke, die voneinander unabhängig und aus Sicht der Cybersicherheit wenig exponiert waren, traten dank des Einfallsreichtums der Teams vor Ort *„in Aktion"*!

„Die Einzigartigkeit industrieller Netzwerke erschwert die Einführung einer gemeinsamen Sicherheitsrichtlinie", fasst Stéphane Prévost zusammen.

Schließlich ist die größte Herausforderung bei der Konvergenz von IT- und EO-Netzwerken der Mensch: Wie können IT- und Betriebsteams lernen, sich gegenseitig zu verstehen und sich an ihre jeweiligen Besonderheiten anzupassen? Der Dialog zwischen den IT-Teams mit ihrer Erfahrung in der Cybersicherheit, und den OT-Teams als Spezialisten ihres industriellen Netzwerks ist tatsächlich entscheidend für mehr Sicherheit der globalen Infrastruktur.

Gemeinsam sind sie dafür verantwortlich, Risiken besser zu identifizieren und zu analysieren und die Umsetzung einer globalen IT/OT-Sicherheitsrichtlinie zu unterstützen.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security).

www.stormshield.com