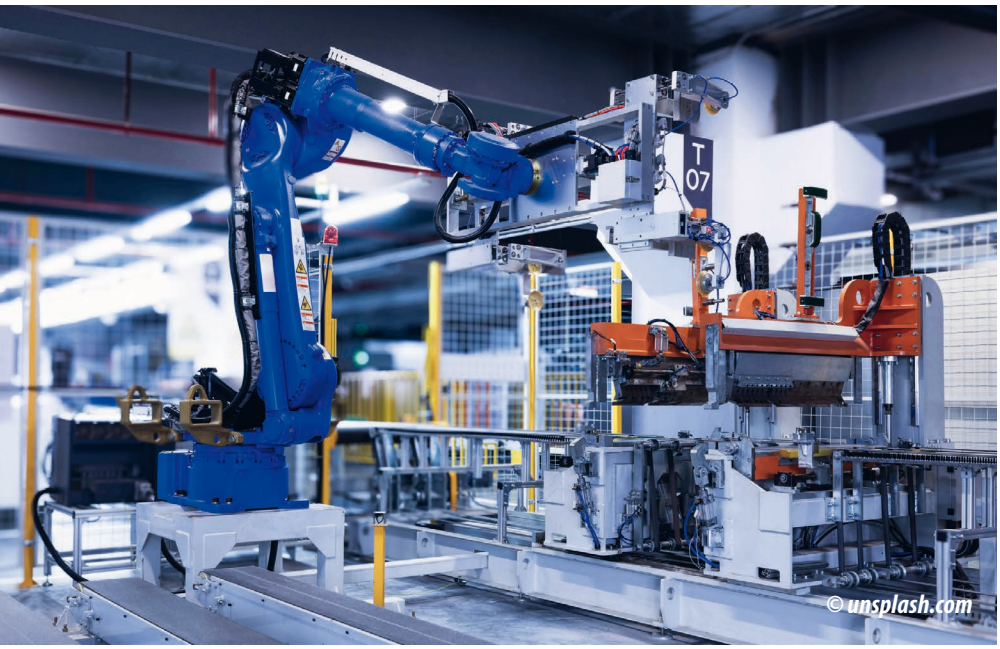
Zero Trust in der Industrie: Zukunft oder Buzzword?

Zwischen Fernwartung, Cloud-Anbindung und vernetzten Produktionsanlagen



© unsplash.com

Die Bedrohungslage im Cyberraum verschärft sich kontinuierlich. Im aktuellen Lagebericht des Bundesamts für Sicherheit in der Informationstechnik werden im Durchschnitt 119 neue Schwachstellen pro Tag registriert – ein Anstieg von 24 Prozent gegenüber dem Vorjahr [1]. Gleichzeitig verfügen noch immer fast die Hälfte der KRITIS-Betreiber über kein System zur Angriffserkennung [2]. Die wirtschaftlichen Schäden durch Cyberangriffe summierten sich in Deutschland zuletzt auf rund 289 Milliarden Euro pro Jahr [3]. Während sich diese Zahlen häufig auf klassische IT beziehen, rückt ein Bereich zunehmend in den Fokus: die industrielle Produktion. Mit der fortschreitenden Digitalisierung der Fabrikhalle verschwimmen die Grenzen zwischen IT und OT (Operational Technology). Maschinen kommunizieren über Netzwerke, Produktionsdaten werden analysiert und Wartungszugriffe erfolgen remote. Damit wird die Produktion Teil der globalen Angriffsfläche – mit erheblichen Konsequenzen. Denn im Gegensatz zur IT steht in der OT nicht die Vertraulichkeit, sondern die anhaltende Verfügbarkeit im Mittelpunkt. Ein ungeplanter Stillstand einer Fertigungslinie kann innerhalb kürzester Zeit hohe wirtschaftliche Schäden verursachen.

Früherer Einstieg zu Zero Trust

Vor diesem Hintergrund gewinnt das Konzept Zero Trust zunehmend an Bedeutung – und die Frage, ob es sich hierbei um ein echtes Architekturprinzip oder nur um ein modisches Buzzword handelt.

Zero Trust sagt: Vertrauen wird nicht vorausgesetzt, sondern muss bei jedem Zugriff neu überprüft werden. Selbst wer bereits im Firmennetz ist, gilt nicht automatisch als vertrauenswürdig. Jeder einzelne Zugriff muss sich ausweisen, jede Kommunikation wird geprüft. Dieses Prinzip ist besonders relevant, wenn Büro-IT und Produktion zusammenkommen, Fernwartung durchgeführt wird oder Cloud-Dienste angebunden werden. Die Industrie steht damit an einem Punkt, an dem sie entscheiden muss: Ist Zero Trust ein notwendiger Schritt zur zukunftsfähigen OT-Security, oder bleibt es eine theoretische Idee, die unter Produktionsbedingungen nicht funktioniert?

Architektur statt Schlagwort

Das Konzept „Zero Trust“ wird oft als Trendbegriff diskutiert. Tatsächlich ist es aber ein grundlegendes Architekturprinzip, das eine zentrale Annahme der klassischen IT-Sicherheit umkehrt. Im traditionellen Modell galt als vertrauenswürdig, wer einmal im Netz war. Zero Trust kippt diese Logik und verlangt, dass jeder Zugriff neu authentifiziert und geprüft wird. Nicht Vertrauen, sondern Verifikation ist der Ausgangspunkt. Gerade in hybriden Infrastrukturen, in denen Büro-IT, Produktionssysteme, Cloud-Dienste und externe Dienstleister miteinander agieren, gewinnt dieser Ansatz an Bedeutung. Allerdings lässt sich das Konzept nicht eins zu eins auf alle Bereiche der OT übertragen. Viele Produktionsprozesse sind darauf ausgelegt, dass Wartungszugriffe schnell und unkompliziert erfolgen können. Zu restriktive Zugriffskontrollen könnten hier die Betriebsabläufe beeinträchtigen. In der Praxis entsteht daher ein hybrider Ansatz. Zero Trust wird vor allem an den Schnittstellen zwischen IT und OT sowie bei externen Zugriffen umgesetzt, während im inneren Produktionsnetz weiterhin auf bewährte, stabilitätsorientierte Konzepte gesetzt wird.

Mehrschichtige Sicherheit statt Einzelmaßnahme

Das Konzept Defense in Depth gehört zu den etablierten Grundprinzipien der Cybersicherheit. Die Idee ist einfach: Sicherheit wird nicht durch eine einzelne Maßnahme gewährleistet, sondern durch mehrere aufeinander abgestimmte Schutzschichten. Ein häufig genutztes Bild ist das der mittelalterlichen Burg mit Graben, Mauer und innerem Kern. Selbst wenn eine Verteidigungslinie überwunden wird, verhindern weitere Ebenen ein vollständiges Eindringen.


© VIDEC Data Engineering GmbH

Autor:
Ruben Bay
Leiter Technik & Schulung
Videc BU OT Networks & OT Security
VIDEC Data Engineering
www.videc.de

In industriellen Netzwerken wird dieses Prinzip häufig durch Zonenkonzepte umgesetzt, etwa nach IEC 62443. Produktionsbereiche werden in eigene Sicherheitszonen unterteilt, um die Ausbreitung von Angriffen zu begrenzen und frühzeitig zu detektieren. Genau hier spielt Transparenz eine entscheidende Rolle. Die passive Analyse der Netzwerkkommunikation ermöglicht es, Anomalien frühzeitig zu erkennen und die Sichtbarkeit innerhalb von OT-Netzwerken deutlich zu erhöhen.

Es gibt Programme, die genau hier ansetzen, indem sie die Lösung industrieller Kommunikationsbeziehungen passiv sichtbar machen und Auffälligkeiten im laufenden Betrieb erkennen, ohne in Produktionsprozesse einzugreifen. Nur wer weiß, welche Systeme miteinander kommunizieren, kann Risiken realistisch bewerten. Zero Trust und Defense in Depth sind keine Gegensätze, sondern ergänzen sich: Zero Trust regelt die Zugriffe an den Schnittstellen, Defense in Depth sorgt für mehrschichtige Verteidigung im Anlagenkern. Ein realistischer OT-Security-Ansatz kombiniert beides.

Grenzen im industriellen Umfeld

In klassischen IT-Umgebungen ist Endpoint Security ein zentraler Bestandteil der Sicherheitsstrategie. Schutzsoftware wird direkt auf Endgeräten installiert, um Bedrohungen frühzeitig zu erkennen und abzuwehren. In der Produktion stößt dieses Konzept jedoch schnell an seine Grenzen. Viele Steuerungen und industrielle Systeme sind proprietär und lassen keine nachträgliche Installation zusätzlicher Software zu. Zudem können Eingriffe in die Systeme deren Stabilität gefährden. In Bezug auf Zero Trust ist dieses Prinzip ebenfalls relevant: Wenn Endpunkte nicht aktiv geschützt werden können, muss die Kontrolle über Zugriffe und Kommunikation anders gewährleistet werden – etwa durch Netzwerkanalyse und strenge Zugriffskontrollen an den Übergängen.

Transparenz als Schlüssel zur Sicherheit

Unabhängig vom gewählten Sicherheitsansatz zeigt sich ein zentrales Problem in vielen Industrieunternehmen: mangelnde Transparenz. Häufig existiert keine vollständige Übersicht über alle vernetzten Geräte, Steuerungen und Kommunikationsbeziehungen.

Ohne diese Grundlage bleibt die tatsächliche Angriffsfläche weitgehend unbekannt. Für Zero Trust ist Transparenz nicht nur hilfreich, sondern unverzichtbar. Das Prinzip basiert darauf, jeden Zugriff kontextbezogen zu bewerten und kontinuierlich zu überprüfen. Ohne Kenntnis darüber, welche Systeme vorhanden sind, welche Kommunikationsbeziehungen bestehen und welches Verhalten als normal gilt, lässt sich diese Bewertung nicht verlässlich durchführen. Sichtbarkeit wird damit zur Grundlage jeder Zero-Trust-Strategie in industriellen Netzwerken.

Sicherheit als Teil der Produktionsstrategie

Neben technischen Herausforderungen steigt auch der regulatorische Druck. Mit der NIS2-Richtlinie und dem IT-Sicherheitsgesetz 2.0 sind Unternehmen zunehmend verpflichtet, ihre Sicherheitsmaßnahmen nachweisbar zu gestalten. OT-Security wird damit zur Managementaufgabe und zum Bestandteil der Unternehmensstrategie. Ein entscheidender Erfolgsfaktor ist dabei die Praxistauglichkeit der eingesetzten Lösungen. In der Produktion sind es häufig nicht spezialisierte IT-Sicherheitsexperten, sondern Ingenieure, Instandhalter oder Anlagenverantwortliche, die Systeme überwachen. Sicherheitslösungen müssen daher verständlich, übersichtlich und in den Arbeitsalltag integrierbar sein. Anomalie-Erkennungsprogramme wie IRMA adressieren genau diesen Punkt mit einer visualisierten Darstellung von Bedrohungsstatus und Kommunikationsbeziehungen, damit auch Mitarbeitende ohne tiefes Security-Know-how Risiken schneller einordnen können. Strategisch entwickelt sich OT-Security zunehmend von einer technischen Disziplin zu einem unternehmerischen Erfolgsfaktor. Zero Trust trägt dazu bei, Risiken bei der Vernetzung von Produktionssystemen kontrollierbar zu machen und gleichzeitig regulatorische Anforderungen besser zu erfüllen. Damit wird das Konzept zu einem wichtigen Baustein für resiliente und zukunftsfähige Produktionsumgebungen.

Evolution statt Buzzword

Zero Trust ist mehr als ein Schlagwort. Die Grundidee, Vertrauen nicht vorauszusetzen, sondern kontinuierlich zu überprüfen, entspricht den Anforderungen moderner Industrieumgebungen mit vernetzten Anlagen, Fernwartungszugängen und Cloud-Anbindungen.

Zwar lässt sich das Konzept nicht uneingeschränkt auf jede Produktionsumgebung übertragen, doch als Architekturprinzip an den Schnittstellen zwischen IT und OT bietet es einen praxisnahen Ansatz, um Sicherheitsrisiken nachhaltig zu reduzieren. Die industrielle Produktion wird auch in Zukunft zunehmend vernetzt sein. Damit wächst nicht nur ihre Effizienz, sondern auch ihre Verwundbarkeit. Unternehmen, die Sicherheit frühzeitig strategisch verankern und an die spezifischen Bedingungen der OT anpassen, schaffen die Grundlage für stabile Prozesse und langfristige Wettbewerbsfähigkeit. Die entscheidende Frage lautet daher nicht, ob Zero Trust in der Industrie relevant wird, sondern wie Unternehmen das Prinzip so umsetzen können, dass Sicherheit, Verfügbarkeit und Effizienz gleichermaßen gewährleistet bleiben.

Links für Referenzen

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2025_Achtseiter.pdf?__blob=publicationFile&v=7

[2] https://medien.bsi.bund.de/lagebericht/de/index.html

[3] https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf

Wer schreibt:

Ruben Bay ist Leiter Technik & Schulung Videc BU OT Networks & OT Security bei der VIDEC Data Engineering GmbH

Als Experte für OT Security im Bereich industrieller Netzwerke unterstützt Herr Bay Kunden der kritischen Infrastruktur in Zonenkonzepten, Monitoring und Systeme zur Angriffserkennung.

VIDEC Data Engineering begleitet Unternehmen in regulierten und energieintensiven Industrien, aus ihren Anlagendaten einen strategischen Wettbewerbsvorteil zu machen – und ihre Produktionsumgebungen wirksam zu schützen. Die Lösungen des Unternehmens machen Menschen handlungsfähig: Anlagen effizient und sicher zu betreiben, regulatorische Anforderungen wie NIS2 zu erfüllen. ◄