WHITEPAPER

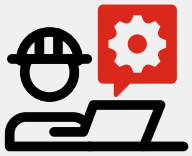
Zero-Trust für OT einfach erklärt

Starker Schutz für Betriebstechnologie (OT) mit fortschrittlicher Sicherheit

Zusammenfassung

Vor nicht allzu langer Zeit waren Netzwerke für Betriebstechnologie (OT) in Produktionsstandorten oder von kritischen Infrastrukturen nicht mit dem Internet verbunden. Die Zeiten, in denen IT und OT getrennte Wege gingen, sind jedoch vorbei: Durch die Digitalisierung sowie neue Arbeitsmodelle wie Remote- und Hybrid-Working wachsen beide Bereiche zunehmend zusammen. Diese Konnektivität zwischen IT und OT kann die Produktivität dank gemeinsamer Datenbestände und neuer cloudbasierter Tools verbessern und Unternehmen interessante Geschäftsvorteile eröffnen. Einer der größten Nachteile der IT-OT-Konvergenz ist jedoch, dass nun hochkomplexe, dynamische Cyberbedrohungen leichter in bislang abgeschottete OT-Umgebungen gelangen können – und so die Vorteile dieser Integration aufs Spiel setzen.

Besonders anfällig sind betriebstechnische Anlagen und Systeme. Denn zum Zeitpunkt ihrer Entwicklung gab es kein Sicherheitsproblem: Da OT-Systeme früher durch ein Air Gap vollkommen von der digitalen Außenwelt abgeschirmt wurden, sind sie so konzipiert, dass sie alles und jedem in ihrer Umgebung vertrauen. Dieses Sicherheitsdefizit lässt sich mit einem Zero-Trust-Cybersecurity-Modell lösen, das ständig die Vertrauenswürdigkeit von Benutzern und Geräten überprüft und gleichzeitig den Netzwerkzugang anhand kontextbezogener Informationen kontrolliert.



„Über IT-Umgebungen werden oft nicht nur OT-Geräte konfiguriert und verwaltet, sondern auch wichtige Daten erfasst, normalisiert, verarbeitet und in Berichten zusammengestellt, damit das Unternehmen seine OT-Ressourcen effektiv verwalten kann. Dieser Brückenschlag zwischen verwaltungstechnischen und industriellen Netzwerken ist geschäftlich sinnvoll, stellt aber völlig neue Anforderungen an die Cybersecurity von Betriebstechnologie, da immer mehr IT-Ressourcen in cloudbasierte Umgebungen verlagert werden.“[1]

Drei Viertel der OT-Unternehmen meldeten im Vorjahr mindestens einen Sicherheitsvorfall: Illegale Netzwerkzugriffe durch Malware (56 %) und Phishing (49 %) waren die häufigsten Angriffsformen – und fast ein Drittel der Befragten war Opfer von Ransomware.[5]

Hintergrund: Warum ist Betriebstechnologie so „vertrauensselig“?

Früher konnten sich Entwickler, Konstrukteure, Hersteller und Betreiber von industriellen Automatisierungs- und Steuerungssystemen (IACS, Industrial Automation and Control Systems) darauf verlassen, dass ein System nichts ausführte, was für die Belegschaft oder die Produktionsanlage gefährlich war. Die meisten IACS-Technologien basierten auf dem hypothetischen Konzepts des impliziten Vertrauens: Alle Verbindungen innerhalb des OT-Perimeters, der durch Air-Gapping von der digitalen Außenwelt abgeschottet war, galten automatisch als sicher. Als Sicherheitsstrategie funktionierte dieser Vertrauensvorschuss meistens gut, da Betriebstechnologie vom öffentlich zugänglichen Internet isoliert war und so automatisch vor Cyberbedrohungen geschützt wurde, mit denen der IT-Bereich seit langem zu kämpfen hatte.

Darüber hinaus ist industrielle Steuerungstechnik (ICS) in der Regel auf Langlebigkeit ausgelegt und eingesetzte Technologien können 20 Jahre oder länger funktionsfähig bleiben. Neben Aspekten wie Arbeitsschutz und Zuverlässigkeit sprechen oft auch wichtige geschäftliche Gründe für den weiteren Betrieb älterer ICS-Ausrüstung.[2] Und dass irgendwann einmal externe Verbindungen zu OT-Systemen unverzichtbar sein würden, hatte bei der Entwicklung heutiger Legacy-Geräte niemand ernsthaft in Betracht gezogen.

Mittlerweile werden betriebstechnische Umgebungen allerdings zunehmend mit IT-Netzwerken verbunden (auch als „IT/OT-Konvergenz“ oder „Industrie 4.0“ bezeichnet). Das kann neue strategische Vorteile bringen, wie z. B. cloudnative Funktionen oder bessere, informiertere Entscheidungen dank Daten aus IT- und OT-Systemen.[3] Diese Konvergenz kann auch den Platzbedarf für die Aufstellung von Hardware reduzieren (oder physische Hardware überflüssig machen), Bereitstellungszeiten verkürzen, Kostensenkungen ermöglichen, die Leistung steigern und die Zusammenarbeit zwischen IT- und OT-Teams fördern.[4] Das Problem ist jedoch: Durch das Zusammenwachsen von OT und IT wird der Air-Gap durchlässig und OT-Systeme sind nicht mehr von der Außenwelt isoliert.
Das implizierte Vertrauen und die Vorstellung einer ICS-Security by Design sind damit nicht mehr tragfähig.

Warum sich Zero-Trust bei der Cybersecurity durchsetzt

Wortwörtlich übersetzt bedeutet Zero-Trust „null Vertrauen“, also das Gegenteil des implizierten Vertrauens. Dahinter steckt eine Art permanente Alarmbereitschaft nach dem Motto: „Ohne Überprüfung gilt nichts und niemand als vertrauenswürdig“.

In der Praxis wird Zero-Trust mit einem Sicherheitsmodell umgesetzt, bei dem Benutzern und Geräten nicht mehr abhängig vom Netzwerkstandort automatisch Zugang gewährt wird (z. B. alle Benutzer, die sich aus der Niederlassung Aachen beim Netzwerk anmelden, sind immer vertrauenswürdig). Stattdessen wird die Vertrauenswürdigkeit pro Transaktion bewertet. Welche Zugriffsrechte dann verifizierte Benutzer und Geräte erhalten, hängt von den Kontextfaktoren im Zusammenhang mit der Anfrage ab. Eine erneute Überprüfung oder Neubewertung von Berechtigungen kommt bei Zero-Trust häufig vor.

Die Ansätze zur Implementierung eines Zero-Trust-Modells können sich stark unterscheiden und selbst einige der gebräuchlichen Abkürzungen für Lösungen sind ohne detaillierte Definitionen oft verwirrend, wie z. B. der Unterschied zwischen ZTA und ZTNA:

- **Zero-Trust-Access (ZTA):** Bei einer ZTA-Lösung liegt der Schwerpunkt auf der Identifizierung und Überwachung der Anwender und Geräte, die auf das Netzwerk zugreifen. Da immer mehr Benutzer außerhalb des Unternehmens arbeiten und IIoT-Geräte (Industrial Internet of Things) vermehrt in OT-Umgebungen eingesetzt werden, sollte der Anwendungs- und Datenzugriff aller Benutzer und Geräte ständig überprüft werden.
- **Zero-Trust Network Access (ZTNA):** Eine ZTNA-Lösung bezieht sich auf den Anwendungszugriff. Ohne korrekte Anmeldedaten wird keinem Benutzer oder Gerät der Zugriff auf eine Anwendung gewährt. Der Zero-Trust-Network-Access wird oft als logische Weiterentwicklung von VPN-Tunneln (Virtual Private Network) beschrieben. Die Unterschiede sind jedoch erheblich: Bei einem VPN gilt alles als vertrauenswürdig, was die Netzwerkkontrollen passiert hat. Im Gegensatz dazu erweitert ein ZTNA das Zero-Trust-Modell über das Netzwerk hinaus und reduziert die Angriffsfläche, indem Anwendungen vor dem Internet verborgen werden.

In den USA stieg das Interesse an der Umsetzung von Zero-Trust-Prinzipien, nachdem das Weiße Haus 2021 angeordnet hatte, dass in allen Behörden grundlegende Sicherheitspraktiken vorhanden sein müssen und die US-Bundesregierung auf eine Zero-Trust-Architektur umgestellt werden soll.[6]

Welche Probleme lassen sich mit Zero-Trust lösen?

Eine effektive Zero-Trust-Implementierung kann mehrere dringende Anforderungen an die Cybersecurity erfüllen, mit denen Unternehmen heute konfrontiert sind:

- Ermöglichung einer uneingeschränkten Mobilität für Mitarbeiter, ohne den normalen Betrieb zu stören oder geltende Zugangskontrollrichtlinien zu schwächen
- Vereinheitlichung der unternehmensweiten Sicherheitsstrategie für Benutzer, Assets und (indirekt) Anwendungen, unabhängig von deren Standort
- Prävention und Abwehr von Cyberbedrohungen, die sich quer im Unternehmensnetzwerk verbreiten, durch ständige Identitäts- und Profilüberprüfungen von Benutzen und Geräten pro Sitzung

Herausforderungen bei der Implementierung von Zero-Trust für Betriebstechnologie

Die Umstellung vom impliziten Vertrauen zu einer ständigen Überprüfung ist nicht ohne Hürden und Komplikationen. Um eine wirksame Zero-Trust-Lösung wie ZTA in einer OT-Umgebung zu implementieren, müssen Security-Verantwortliche zuerst einige Fragen zur Funktionsweise von Steuerungstechnik in der OT-Umgebung sowie sicherheitsrelevante Aspekte klären, wie z. B.:

1. Gibt bei eingesetzten Automatisierungslösungen eine begrenzte oder beschränkte Garantie für bestimmte Netzwerkkonstellationen oder -vorgänge? Dies ist ein relativ häufiges Problem, das im Vorfeld umfassend geprüft werden sollte.
2. Sind die ZTA-Technologien mit den älteren Technologien in OT-Umgebungen kompatibel? Die Langlebigkeit von Steuerungstechnik mit Lebenszyklen von über 20 Jahren muss stets berücksichtigt werden.
3. Produktionsstandorte sind bei der Integration und Inbetriebnahme häufig auf Systemintegratoren und Erstausrüster (OEM) angewiesen. Sind die Zuständigen auf die Einführung von ZTA-Technologien vorbereitet, die zu Störungen bei integrierten Subsystemen führen könnten?
4. OEM-Anbieter und Systemintegratoren können in den Garantiebedingungen oder in Betriebs- und Wartungsverträgen mit Dritten einen Fernzugriff verlangen.
5. Der Großteil der ICS/OT-Technologie hat keine eigene Steuerung, was Benutzerinteraktionen unmöglich macht. Da oft statische IP-Adressen verwendet werden, lassen sich Verbindungen zu solchen Headless-Geräten ohne eine Benutzeroberfläche nicht ständig neu authentifizieren. Unterstützt die ZTA-Lösung diese einzigartige Einschränkung von OT-Umgebungen?
6. Da OT-Umgebungen früher durch Air-Gapping geschützt waren, sind manchmal statische Passwörter notwendig statt Passwörter, die in Active Directory (AD) mit sicheren Richtlinien für das Anmeldedaten-Management verwaltet werden können.
7. Einige OT-Komponenten – wie speicherprogrammierbare Steuerungen [SPS] oder Mensch-Maschine-Schnittstellen [MMS] – unterstützen womöglich nicht die nötigen Technologien oder Protokolle für eine vollständige ZTA-Integration. Daher ist ein ZTA-Ansatz für einige OT-Geräte oder -Systeme vielleicht nicht machbar oder zu kompliziert.
8. Zur OT-Umgebung können ICS-Technologien für Sicherheitsabläufe oder Schutzfunktionen gehören, die zeitnah und ununterbrochen auf Systeme zugreifen können müssen. Die ZTA-Implementierung für solche Steuerungstechnik darf auf keinen Fall Sicherheitsaspekte der Infrastruktur beeinträchtigen.

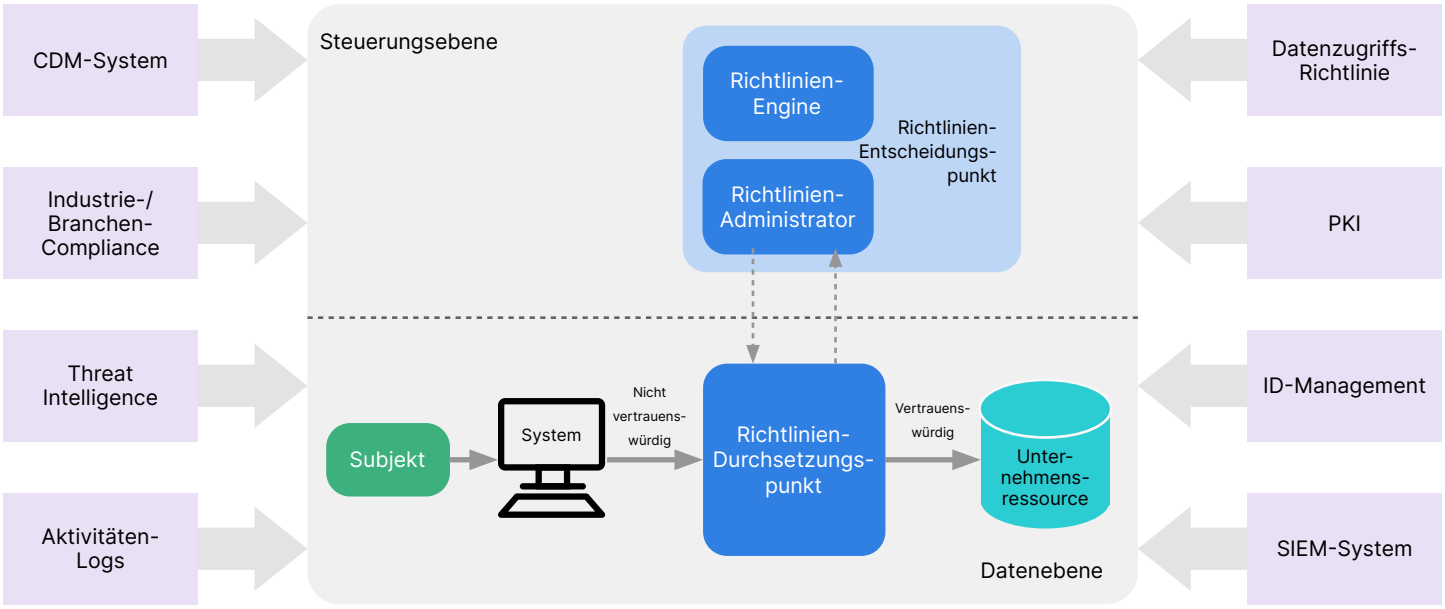
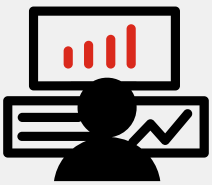


Abbildung 1: Logische Hauptelemente von Zero-Trust nach NIST SP 800-207[7]

Eine weitere große Herausforderung bei der Zero-Trust-Implementierung in vernetzten IT-OT-Umgebungen sind die unterschiedlichen Zuständigkeiten für beide Bereiche. Das ZTA-Konzept funktioniert in der Praxis nur dann richtig gut, wenn sich die Sicherheitsabläufe des IT- und OT-Managements mit unterschiedlichen Prioritäten konvergieren lassen. Getrennte Security Operations Center (SOC) für IT und OT sind wenig sinnvoll. Das erhöht nicht nur die Komplexität, sondern verursacht auch potenzielle Sicherheitsrisiken in beiden Umgebungen, was das Asset- und Richtlinienmanagement, die Aufnahme und Analyse von Daten aus IT- und OT-Systemen oder die Abwehr von Cyberangriffen angeht.

Die Anschaffung und Wartung von Zero-Trust-Lösungen setzt internes Know-how und operative Ressourcen für das Management der Protokollierung und Zugriffskontrollen voraus. Angesichts knapper Budgets und des Fachkräftemangels haben viele Unternehmen womöglich damit zu kämpfen, qualifizierte Security-Mitarbeiter für die Bereitstellung und Wartung der Zero-Trust-Lösungen zu finden oder zu halten. In solchen Fällen sollte unbedingt geprüft werden, ob der Anbieter der Lösung die Implementierung und den Support übernehmen kann.



Die Anzahl der OT-Security-Verantwortlichen, die das Sicherheitsprofil ihres Unternehmens als „sehr ausgereift" bezeichnen, ist von 21 % auf 13 % in diesem Jahr zurückgegangen – was vermuten lässt, dass OT-Experten das eigene Sicherheitsprofil realistischer einschätzen und über mehr effektive Tools zur Bewertung der vorhandenen Cybersecurity-Funktionen verfügen.[8]

Zukunftssicherheit beginnt jetzt

Da IT und OT immer schneller zusammenwachsen, sollten Security-Verantwortliche auf ein Zero-Trust-Modell umstellen, um ihre OT-Umgebungen vor Störungen durch interne oder externe Sicherheitsvorfälle zu schützen. Für die erfolgreiche Einführung von Zero-Trust für Betriebstechnologie haben sich grundlegende Schritte bewährt:

- **Belegschaft:** Sensibilisieren Sie die Benutzer für die Risiken der IT/OT-KKonvergenz, unterstützt von Informations- oder Schulungsangeboten dazu, wie Zero-Trust-Lösungen den Bedrohungsschutz des Unternehmens verbessern.
- **Prozess:** Die Zeiten des implizierten Vertrauens bei der OT-Sicherheit sind vorbei. Alle Sicherheitsrichtlinien und -protokolle sollten jetzt auf einer neuen Art von Vertrauen basieren, das kontextbezogen verifiziert und ständig neu überprüft wird. Unternehmen brauchen eine umfassende, kontinuierliche und konsequente Kontrolle darüber, wer und was sich im Netzwerk befindet (einschließlich Automatisierungsanbieter und Service Provider).
- **Technologie:** Bewerten Sie Zero-Trust-Lösungen für OT-Umgebungen – auch hinsichtlich der Folgen für Ihre gesamte Lieferkette. Ideal ist, wenn der Anbieter einer Zero-Trust-Sicherheitslösung starke Partnerschaften im gesamten Technologie-Ökosystem unterhält.

[1] „IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems". Carnegie Mellon University, 18. Juli 2022.

[2] Ebd.

[3] „Converge IT and OT to turbocharge business operations' scaling power". McKinsey & Company, 28. Juni 2022.

[4] „2023 State of Operational Technology and Cybersecurity Report". Fortinet, Mai 2023. (Deutsche Ausgabe erhältlich. Bitte fragen Sie Ihren Ansprechpartner bei Fortinet.)

[5] Ebd.

[6] „How to Create a Comprehensive Zero Trust Strategy". Fortinet, 15. Mai 2023.

[7] "SP 800-207: Zero Trust Architecture". NIST, August 2020.

[8] „2023 State of Operational Technology and Cybersecurity Report". Fortinet, Mai 2023. (Deutsche Ausgabe erhältlich. Bitte fragen Sie Ihren Ansprechpartner bei Fortinet.)

31. Oktober 2023

2177370-0-0-DE