Key Insight Brief

Fertigungsindustrie | 3 Strategien für den sicheren Fernzugriff

wallix

Fernwartung: Schlüssel zur Effizienzsteigerung in der Industrie

Die Fernwartung revolutioniert die Betriebseffizienz in der Industrie und ist in einer zunehmend digitalen und vernetzten Welt unverzichtbar. Ob bei der Diagnose, Überwachung oder Fehlerbehebung – die Nachfrage nach sicheren Fernzugriffslösungen steigt kontinuierlich. Gleichzeitig ist die Absicherung dieser Zugänge entscheidend, denn die Einführung von VPN-Gateways durch Hersteller und externe Dienstleister hat die Angriffsflächen industrieller Netzwerke erheblich vergrößert.

Der Balanceakt zwischen Effizienz und Sicherheit

Industrieunternehmen stehen vor der Herausforderung, Effizienz und Cybersicherheit in Einklang zu bringen. Fernzugriff ist zwar essenziell, bringt jedoch auch erhebliche Risiken mit sich, wenn keine ausreichenden Schutzmaßnahmen ergriffen werden. Unsicherheiten darüber, wo mit der Absicherung begonnen werden sollte, führen häufig dazu, dass Unternehmen zögern, entscheidende Schritte zu unternehmen. Ein klarer, strategisch fundierter Plan kann hier Abhilfe schaffen.

Ein strategischer Ansatz für eine sichere Fernwartung

Um den Herausforderungen der Fernzugriffssicherung erfolgreich zu begegnen, ist ein strukturierter und strategischer Ansatz erforderlich. Eine durchdachte Planung und die Umsetzung konkreter Maßnahmen sind der Schlüssel, um Sicherheit und Effizienz gleichermaßen zu gewährleisten.

Wir haben diese komplexe Aufgabe für Sie in drei zentrale Strategien unterteilt, die Ihnen den Einstieg erleichtern und Ihnen dabei helfen, die Fernwartung in Ihrem Unternehmen sicher und effizient zu gestalten.

Drei Strategien für sicheren Fernzugriff in industriellen Umgebungen

01 Implementierung von Zero-Trust-Security-Frameworks

Das Zero-Trust-Sicherheitsframework ist mittlerweile ein zentraler Bestandteil moderner IT-Sicherheitsstrategien. Obwohl das Konzept vielen vertraut sein dürfte, wird es in vielen Unternehmen noch nicht konsequent umgesetzt. Doch die Zeit zu zögern, ist vorbei: Zero-Trust ist heute unverzichtbar, um aktuellen Cyberbedrohungen effektiv zu begegnen.

Was unterscheidet Zero-Trust? Im Gegensatz zu herkömmlichen Sicherheitsmodellen, die Vertrauen innerhalb eines Netzwerks voraussetzen, überprüft Zero-Trust kontinuierlich alle Nutzer und Geräte, unabhängig von ihrem Standort oder Zugriffsweg. Nur authentifizierte und autorisierte Entitäten erhalten Zugang zu Ressourcen – ein entscheidender Schutzmechanismus gegen Angriffe.

Wie gelingt der Einstieg? Zu Beginn sollte eine vollständige Übersicht über alle Anlagen und Ressourcen erstellt werden, um Transparenz über die Infrastruktur zu schaffen. Gleichzeitig gilt es, grundlegende Sicherheitsschichten einzurichten, etwa durch Privileged Access Management (PAM). Diese Tools ermöglichen eine granulare Zugriffskontrolle und kontinuierliche Überwachung sensibler Bereiche.

Vorteile von Zero-Trust:

> Reduzierter unbefugter Zugriff durch umfassende Überprüfung.

> Erhöhte Transparenz bei Netzwerkaktivitäten.

> Verhinderung seitlicher Angriffe innerhalb des Netzwerks.

Mit Zero-Trust stärken Unternehmen ihre Sicherheitsarchitektur und schützen sich vor aktuellen Bedrohungen.

02 Zentralisierung und Vereinfachung

Nach der Segmentierung Ihres Netzwerks, einem entscheidenden Schritt zum Schutz Ihrer OT-Umgebungen, ist **die Einrichtung eines einzigen Zugangspunkts für den Zugriff auf Ihre OT-Systeme** unerlässlich. Dieser Ansatz vereinfacht Remote-Verbindungen über ein zentrales Tool und macht zahlreiche unkontrollierte VPN-Zugangspunkte überflüssig. Dies muss jedoch mit **benutzerfreundlichen** Tools geschehen, die perfekt auf bestehende OT-Prozesse abgestimmt sind, um eine nahtlose Sicherheit zu gewährleisten, ohne die Produktion zu stören.

Genau das bieten die Tools für das **Privileged Access Management (PAM)**, deren Hauptziele sind:

> **Isolierung Ihrer Produktionsumgebung** durch eine Protokollunterbrechung, die von einem zentralisierten PAM verwaltet wird.

> **Rückverfolgbarkeit aller Remote-Verbindungen**, unabhängig von ihrem Ursprung (Dienstleister, Hersteller, interne Teams, usw.).

> **Überwachung sämtlicher Aktivitäten**, die die authentifizierte Person auf den Zielsystemen unternimmt.

> **Beschränkung des Zugriffs auf bestimmte Bereiche oder Geräte**, um unbefugte Aktionen zu verhindern.

> **Delegierte Verwaltung von Benutzerkonten**, damit Produktionsteams gegebenenfalls Fremdpersonal in Echtzeit hinzufügen können.

03 Kontinuierliche Überwachung und Erkennung von Anomalien

Die kontinuierliche Überwachung von Fernzugriffen und die Erkennung von Anomalien gehören zu den essenziellen Maßnahmen, um die Sicherheit moderner IT- und OT-Infrastrukturen zu gewährleisten. Aber warum ist dies so entscheidend? Nun, durch den Einsatz zentralisierter, fortschrittlicher Cybersicherheitslösungen **können ungewöhnliche Aktivitäten oder Verstöße in Echtzeit erkannt werden**. Dies ermöglicht es, potenzielle Bedrohungen frühzeitig zu identifizieren und schnell Gegenmaßnahmen zu ergreifen, bevor erhebliche Schäden entstehen. Empfohlene Maßnahmen zur Absicherung:

> Integrieren Sie Systeme zur Verhaltensanalyse und Anomalieerkennung, die verdächtige Aktivitäten automatisch identifizieren.

> Richten Sie Echtzeitwarnungen für unbefugte Zugriffe oder Abweichungen ein, um sofort auf potenzielle Sicherheitsvorfälle reagieren zu können.

> Verknüpfen Sie diese Informationen mit einem zentralen SIEM-System (Security Information and Event Management), um Vorfälle effizient zu analysieren und die Zugriffsverwaltung gezielt zu optimieren.

Vorteile einer kontinuierlichen Überwachung:

> **Erfassung aller Aktivitäten**: Ereignisprotokolle bieten eine transparente Dokumentation, die für Analysen und Nachverfolgung genutzt werden kann.

> **Frühzeitige Bedrohungserkennung**: Durch die Kombination mit einem SIEM-System können Angriffe abgewehrt werden, bevor Schäden entstehen.

> **Verbesserung der Sicherheitsstrategie**: Die Analyse von Vorfällen liefert wertvolle Einblicke zur kontinuierlichen Optimierung der Sicherheitsmaßnahmen.

> **Compliance-Einhaltung**: Die Überwachung hilft Unternehmen, regulatorische Anforderungen wie NIS2, IEC 62443 und ISO 27001 zuverlässig zu erfüllen.

Anwenderbericht

Ein führendes deutsches Unternehmen aus der Fertigungsindustrie hat den Schutz seiner kritischen Server und Infrastruktur durch gezielte Investitionen in die Zugriffskontrolle erheblich verbessert. Ziel dieser Maßnahmen war es, den reibungslosen Betrieb sicherzustellen und die Ausfallsicherheit auch für die Zukunft zu steigern.

Welche konkreten Schritte das Unternehmen unternommen hat, um seine Cybersicherheitsstrategie zu optimieren, erfahren Sie auf den folgenden Seiten…

Wie ein führender Hersteller hochwertiger Arbeitskleidung seine kritischen Server und Infrastrukturkomponenten absichert

Engelbert Strauss, ein renommierter Hersteller hochwertiger Berufsbekleidung, betreibt eine umfangreiche IT-Infrastruktur mit 80 Servern, 1.200 Mitarbeitern und 10 Niederlassungen. Angesichts dieses Umfangs sah sich das Unternehmen mit mehreren zentralen Herausforderungen konfrontiert:

> **Stabile und sichere IT-Infrastruktur:** Sicherstellung einer zuverlässigen und geschützten Netzwerkumgebung.

> **Passwort- und Identitätsmanagement:** Aufbau eines robusten Systems zur Verwaltung von Passwörtern und Identitäten.

> **Benutzerfreundlichkeit:** Optimierung der Prozesse für eine nahtlose Nutzererfahrung.

> **Sicherheits- und Usability-Balance:** Hohe Sicherheitsstandards ohne Einbußen bei der Benutzerfreundlichkeit.

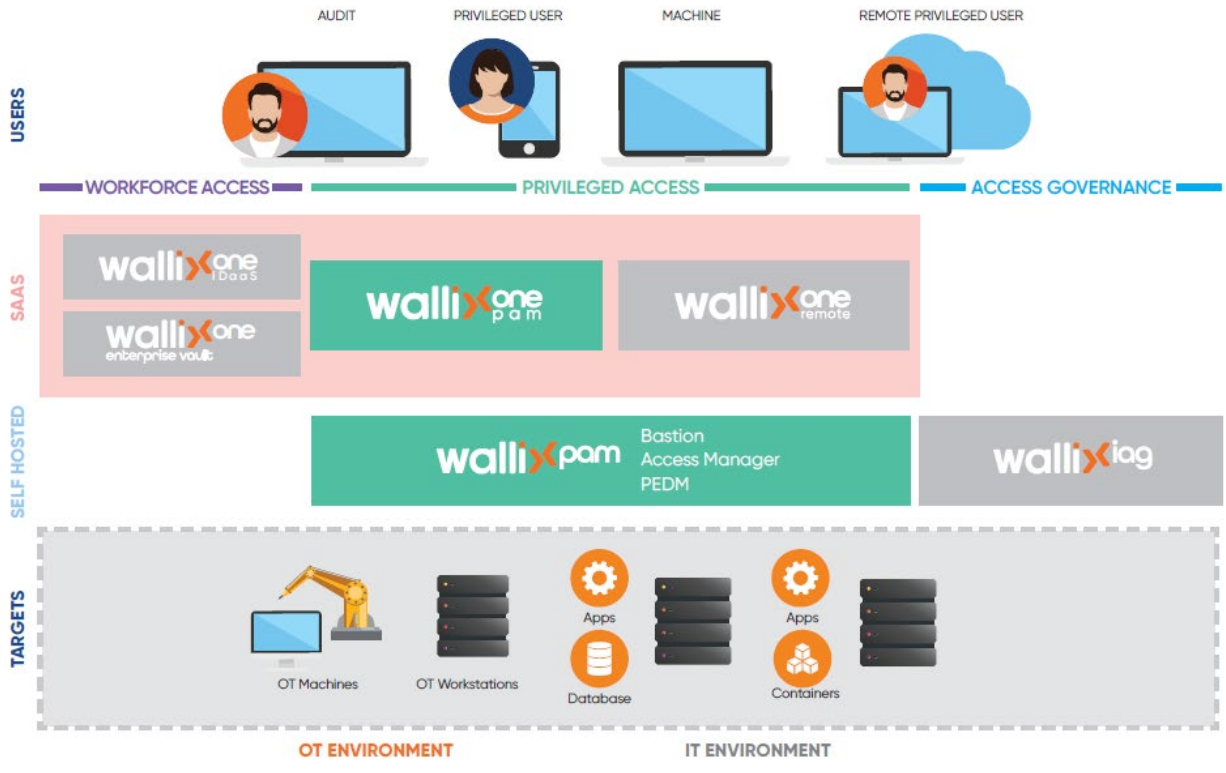
Um diesen Anforderungen gerecht zu werden, wurde eine umfassende Lösung implementiert, die den privilegierten Zugriff auf kritische Ressourcen zentralisiert und eine detaillierte Übersicht darüber bot, wer wann auf welche Systeme zugriff. Zudem wurde das Privileged Access Management (PAM)-System nahtlos in die bestehende Sicherheitsinfrastruktur integriert, einschließlich des Security Information and Event Management (SIEM)-Systems. Diese Integration ermöglichte eine klare Trennung zwischen primären und sekundären Sitzungsverbindungen sowie eine verbesserte Kontrolle autorisierter Zugriffe.

Die erzielten Vorteile waren vielfältig:

> Eine effizientere Nutzung der IT-Ressourcen,

> Eine verbesserte Überwachung und Kontrolle von Serverzugriffen,

> Die Reduzierung von Supportanfragen auf ein Minimum.



Zusammenfassung

ANDRÉ THEILIG

› Field Territory Account Manager

Hallo, mein Name ist **André Theilig**. Ich bin Field Territory Account Manager bei WALLIX in der DACH-Region. Dieses Dokument soll Ihnen aufzeigen, welche wichtige Bedeutung ein sicherer Fernzugriff im industriellen Umfeld hat. Sollten Sie noch Fragen rund um dieses Thema haben, kommen Sie bitte einfach auf mich zu.

atheilig@wallix.com

wallix

WALLIX ist ein weltweit tätiger Anbieter von Cybersicherheitssoftware. Das Unternehmen wurde 2003 gegründet und ist heute weltweit führend im Bereich Identitäts- und Zugangssicherheit. WALLIX wird regelmäßig von den renommiertesten Analystenfirmen ausgezeichnet und hat es sich zur Aufgabe gemacht, seinen Kunden einen einfachen und sicheren identifizierten Zugangsservice anzubieten, der ein sicheres Arbeiten in digitalen (IT) und industriellen (OT) Umgebungen ermöglicht.

- **Prinzregentenstraße 91, 81677 München, Deutschland**
- **+49 89 52 03 65 68**
- **sales-dach@wallix.com**