Fachartikel

Sicherer und bedarfsgerechter Fernzugriff: Zero Trust stärkt Zellenschutz

Homeoffice, Fernzugriff, Cybersicherheit: Was IT-seitig in vielen Unternehmen bereits Alltag ist, weckt in OT-Kreisen Begehrlichkeiten. Auch im industriellen Produktions- und Entwicklungsumfeld sollen und können diverse Jobs von extern erledigt, bestimmte Abläufe vorbereitet, initiiert und überwacht werden. Genauso dynamisch und sicher? Siemens und Zscaler Inc. haben diese Aufgabe gemeinsam angepackt und verbinden bewährten perimeterbasierten Zellenschutz mit flexiblen Zero Trust-Prinzipien.

Es war ohnehin nur eine Frage der Zeit, bis das in der Büro-/IT-Welt weit verbreitete mobile Arbeiten – aus dem Homeoffice oder Büro, aus der Ferne allgemein – auch von der OT (Operational Technology), der industriellen Automatisierungs- und Netzwerktechnik, eingefordert werden würde. Zumal beide Welten mehr und mehr ineinandergreifen und die IT schon unternehmensintern abgesicherten Durchgriff auf die OT realisieren muss. Die Pandemie hat den Wunsch vieler Prozess- und Anlagenbetreiber nach flexibleren und sicheren Zugriffsmöglichkeiten von außen, über die klassische Fernwartung hinaus, weiter verstärkt. So haben sich Siemens, führender Anbieter industrieller Netzwerktechnik, und Zscaler Inc., führender Anbieter einer cloudbasierten Sicherheitsplattform, zusammengetan, um die relevanten Aufgaben zu lösen.

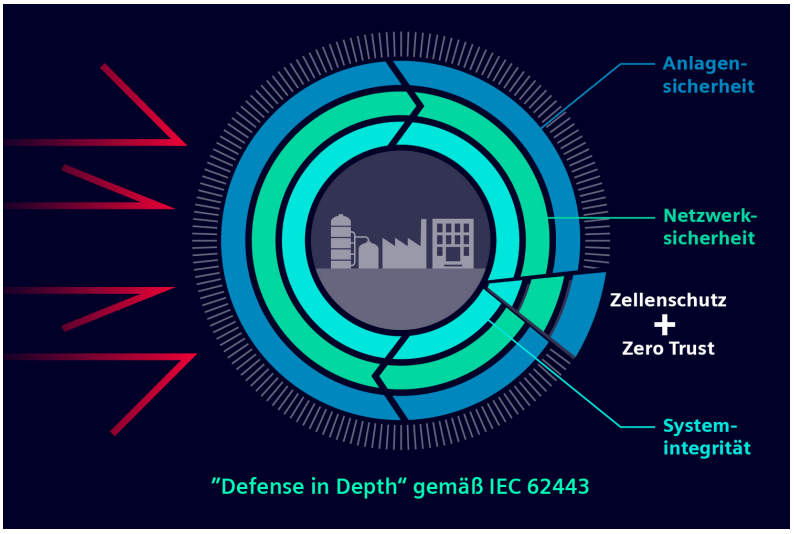
SIEMENS

siemens.de/zero-trust

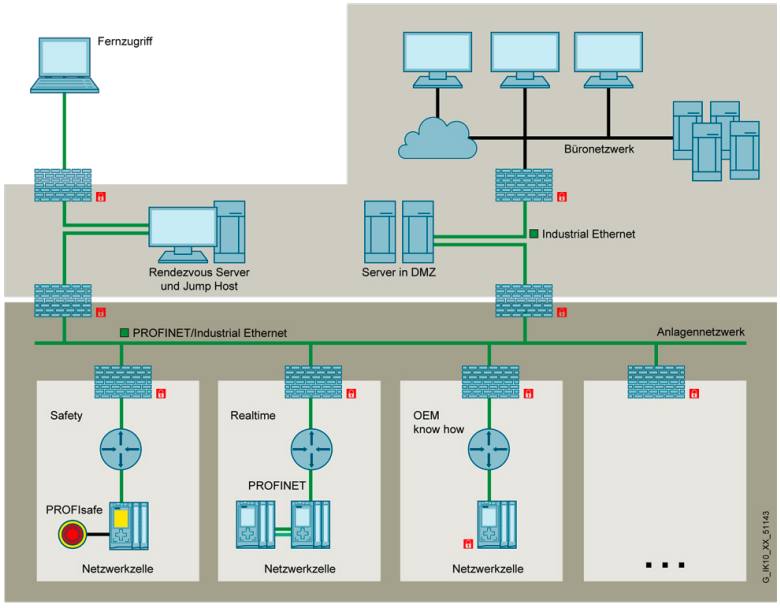
OT ist nicht IT – Netzwerk nicht gleich Netzwerk

Heterogene, oft über Jahre gewachsene industrielle Kommunikationsnetzwerke stellen in mehrfacher Hinsicht ganz andere Anforderungen als reine IT-Lösungen. So müssen Daten in der Produktion vielfach deterministisch in Echtzeit kommuniziert werden. Zudem sind oft gleichzeitig Safety-Funktionen zu realisieren sowie höchste Verfügbarkeit und auch Know-how-Schutz zu gewährleisten. Hinzu kommt, dass ältere Komponenten mitunter gänzlich offen und unverschlüsselt kommunizieren. Um Cyberangriffe dennoch abwehren zu können, wurden auf die Industrie abgestimmte Schutzkonzepte entwickelt, wie das Defense in Depth Konzept, die tiefengestaffelte Verteidigung nach IEC 62443. Die Netzwerksicherheit fußt dabei auf einer individuellen Risikobewertung und segmentierten Netzwerken mit separat über eigene Firewalls geschützten Produktionszellen. Die Kommunikation aus/mit dem Büronetzwerk oder dem Internet läuft in einem solchen perimeterbasierten Netzwerk über eine sogenannte demilitarisierte Zone (DMZ) oder spezielle Rendezvous Server und Jump Hosts.

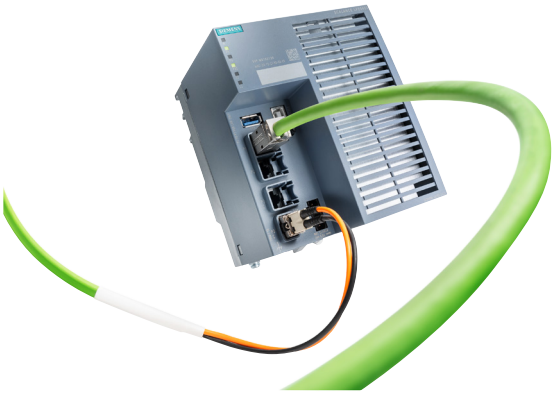
In Büronetzwerken, mit unzähligen, meist neueren Devices und ständigen Veränderungen, hat sich dagegen häufig ein Schutzkonzept etabliert, bei dem keinem Teilnehmer per se vertraut wird („never trust, always verify“). Dieser „Zero Trust“ genannte Ansatz setzt voraus, dass alle Netzwerkteilnehmer – Benutzer wie Geräte – immer erst ihre Identität und Integrität nachweisen, bevor die Kommunikation mit der gewünschten Zielressource aufgebaut wird. Viele bestehende Automatisierungskomponenten und Netzwerkinfrastrukturen sind damit überfordert. Weshalb sich das flexiblere, einfacher handhabbare – weil zentral und unternehmensweit verwaltete – Zero Trust-Konzept nicht ohne Anpassungen in vollem Umfang auf industrielle Netzwerke übertragen oder ausweiten lässt.



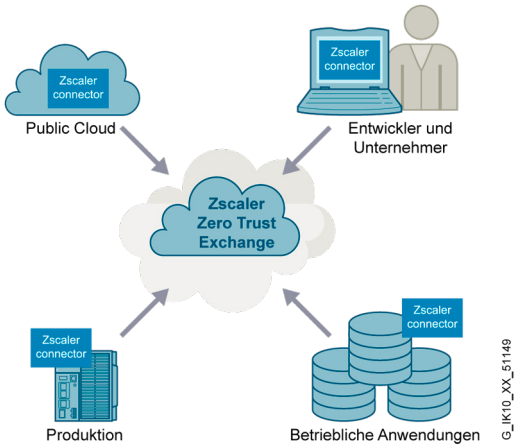
Zero Trust und Zellenschutz als feste Bestandteile des "Defense in Depth”-Konzeptes, welches sowohl technische als auch organisatorische Maßnahmen ergreift, um Produktionsanlagen vor Cyberangriffen zu schützen.



Klassischer perimeterbasierter Ansatz mit Fernzugriff über Rendezvous Server und Jump Host auf segmentiertes OT-Netzwerk mit separaten, über eigene Firewalls abgesicherten, „vertrauenswürdigen“ Zellen



SCALANCE LPE ist eine kleine und robuste lokale Verarbeitungsplattform mit einer performanten CPU. Sie ist flexibel einsetzbar, z. B. für Edge-Anwendungen, mit denen sich die Anlageneffizienz deutlich steigern lässt.



Zscaler Zero Trust Exchange ermöglicht es einem Administrator zentralisiert in der Zscaler Cloud-Plattform benutzerspezifische Regelsätze zu definieren, die den anwendungsspezifischen Zugriff auf entsprechende Zielressourcen kontrollieren.

Intelligent kombiniert zu konvergenten Lösungen

Um die Integration von OT und IT dennoch voranzutreiben, haben Siemens und Zscaler ihre Kompetenzen für einen durchgängigen Zero Trust-Sicherheitsansatz für OT/IT gebündelt. Als performante Hardware im rauen Produktionsumfeld, direkt an oder auch in den Fertigungszellen, dient die lokale Verarbeitungsplattform SCALANCE LPE (Local Processing Engine) von Siemens. Deren eigentliche Kernaufgabe ist das Sammeln von Daten und deren Vorverarbeitung nahe am Prozess. Dazu wird das Gerät einfach via Ethernet in ein vorhandenes, per Firewall abgesichertes Zellennetzwerk eingebunden.

Mit ihrem offenen Betriebssystem auf Linux-Basis und einer leistungsstarken CPU ist die lokale Verarbeitungsplattform prädestiniert für den sicheren, zuverlässigen Betrieb zusätzlicher Applikationen. In diesem Fall durch den App Connector des cloudbasierten Remote Access-Service Zscaler Private Access (ZPA), der als Docker-Container schnell und einfach installiert werden kann. Über den Zscaler App Connector kann jede SCALANCE LPE initial in der Zero Trust Exchange-Cloud Plattform aufgenommen und konfiguriert werden. Anschließend fungiert sie als Zero Trust-Gateway für ihre Zelle, die in sich als vertrauenswürdig betrachtet wird. Die Zero Trust Exchange-Plattform überwacht sämtliche für den Zugriff notwendige Regelsätze und stellt die Schnittstellen für diverse Identity Provider bereit. Sie gewährt nur eindeutig identifizierten und autorisierten Teilnehmern Zugriff auf die für diese freigegebenen Ressourcen.

So können unternehmensweit administrierte Anwender flexibel, bedarfsgerecht und sicher auch aus der Ferne auf lokale Produktions- oder Entwicklungssysteme zugreifen, ohne diese einem erhöhten Bedrohungspotenzial auszusetzen. Bedingt durch spezifische Berechtigungskonzepte lassen sich die speziellen Anforderungen von Echtzeit- oder Safety-Anwendungen beziehungsweise der Verfügbarkeit und des Know-how-Schutzes gewährleisten. Ohne die Architektur des industriellen Netzwerks grundlegend ändern zu müssen.

Das zentrale Management in der Zero Trust Exchange-Plattform und ausschließlich ausgehende Verbindungen reduzieren bestehende Firewall-Regeln und damit auch die Kosten für Administration und Überwachung. Mit anderen Worten: Obwohl zusätzliche Verbindungen für das Zusammenspiel von OT und IT eingerichtet werden, können Firewall-Regelsätze restriktiver konfiguriert werden.

Weitere Informationen

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts. Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter **www.siemens.de/industrialsecurity**

Siemens AG
Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Deutschland

PDF
Fachartikel
DI PA-2122-2
PDF 1121 4 De
Produced in Germany

In-house-Tests überzeugend – Roll-out gestartet

Dieser Zusammenarbeit vorausgegangen war ein großflächiger Test mit mehreren hunderttausend Zscaler-Teilnehmern im IT-Netzwerk von Siemens. Auf der gleichen Basis wurden zudem verschiedene Projekte im Bereich Entwicklung und Qualitätssicherung in eigenen Produktionsnetzwerken erfolgreich umgesetzt.

Jetzt gilt es, weitere geeignete Anwendungen im Produktions- und Entwicklungsumfeld zu definieren und konkrete Lösungen dafür umzusetzen. Im Fokus stehen dabei zunächst Unternehmen, die IT-seitig bereits auf die Zscaler-Plattform und in der Produktion auf Netzwerktechnik von Siemens setzen. Diese können den neuen Ansatz ohne großen Aufwand und grundlegende Veränderungen an der Netzwerkinfrastruktur implementieren und von den Vorteilen profitieren.

Sie realisieren damit konvergente Unternehmensnetzwerke mit einheitlichen IT-/OT-Sicherheitsrichtlinien für Ihr Büro- und Produktionsnetzwerk. Und damit letztendlich höhere Cybersicherheit, Flexibilität und Effizienz beim mobilen Arbeiten in Produktion und Entwicklung.

Bestehende Lösungen weiter nutzbar

Die speziellen Rahmenbedingungen industrieller Kommunikation sprechen dafür, Zscaler und Zero Trust-Prinzipien als Add-on zu bisherigen Konzepten zu implementieren, um flexibler und dynamischer agieren zu können. Das "Defense in Depth"-Konzept bleibt somit weiterhin bestehen und wird im Bereich Netzwerksicherheit zusätzlich um Zero Trust-Funktionalitäten erweitert. Auch werden klassische VPN-basierte Fernzugriffe sowie die dazugehörige Managementplattform ebenso in Zukunft Bestand haben und weiterentwickelt. Je nach Branche, Anwendungsfall oder Unternehmensrichtlinie bieten beide Konzepte entsprechende Vorteile. Langfristig gesehen werden durchgängige Zero Trust-Konzepte nicht nur Betriebskosten senken, sondern auch zu einer höheren Cybersicherheit im Produktionsumfeld beitragen.