SIEMENS

Hintergrund-
information

Nürnberg, 11. April 2023

Industrial Cybersecurity

Siemens ist One-Stop-Shop für Cybersicherheitslösungen in der Industrie

- **Digitale Transformation und Cybersicherheit sind zwei Seiten einer Medaille**
- **Konvergenz von IT und OT erfordert höhere Cybersicherheitsanstrengungen**
- **Mehrstufiges Defense-in-Depth-Konzept als Goldstandard**

Die zunehmende Verbindung von Produktions- und Office-Netzwerken im Zuge der IT-OT-Integration und die Nutzung des Internets der Dinge bieten Industrieunternehmen viele Vorteile, z. B. durch digitalisierte Prozesse und die unternehmensübergreifende Zusammenarbeit in Ecosystems. Dadurch erhöht sich aber auch das Risiko von Cyberbedrohungen. Siemens ermöglicht mit Industrial Cybersecurity umfassenden Schutz von Systemen und Anlagen in der Operational Technology (OT) und im Internet der Dinge. Zu diesem Zweck setzt Siemens auf das mehrstufige Defense-in-Depth-Konzept – erweitert um Zero-Trust-Prinzipien. Denn: Cyberbedrohungen können aus Siemens-Sicht nur mit einem umfassenden Konzept wirksam begegnet werden, das auf allen relevanten Ebenen eines Industrieunternehmens greift.

"Ohne Cybersicherheit kann es keine digitale Transformation geben. Die Abwehr von Bedrohungen und Angriffen ist eine Grundvoraussetzung für das Digital Enterprise", sagt Michael Metzler, Vice President Horizontal Management Cybersecurity for Digital Industries bei Siemens. "Siemens ist bestens aufgestellt, um Systemintegratoren und Anlagenbetreiber als Komplettanbieter von industriellen Automatisierungs- und Kommunikationssystemen auf allen Ebenen zu unterstützen."

Die für Industrieunternehmen entscheidenden Sicherheitsstufen sind die Anlagensicherheit, die Netzwerksicherheit und die Systemintegrität von Automatisierungssystemen. Siemens bietet ein breites Spektrum an Netzwerk- und Automatisierungskomponenten mit integrierten Security-Funktionen und den

Siemens AG
Kommunikationen
Leitung: Lynette Jackson

Werner-von-Siemens-Straße 1
80333 München
Deutschland

dazugehörigen Security-Services für die Umsetzung mehrschichtiger Sicherheitskonzepte für die Industrie.

Das Defense-in-Depth-Konzept entspricht den Empfehlungen der IEC 62443, dem führenden Standard für Sicherheit in der industriellen Automatisierung. Dabei werden alle wesentlichen Faktoren berücksichtigt, darunter der physische Zugriffsschutz und organisatorische Maßnahmen wie Richtlinien und Prozesse sowie technische Maßnahmen zum Schutz von Netzwerken und Systemen vor unbefugtem Zugriff, Spionage und Manipulation.

Startpunkt Anlagensicherheit

Die Anlagensicherheit sorgt dafür, dass technische IT-Sicherheitsmaßnahmen nicht umgangen werden. Dafür werden physische Zugangsschutzinfrastrukturen und organisatorische Maßnahmen implementiert, beispielsweise: Schranken, Drehkreuze, Kameras und Kartenleser sowie ein Sicherheitsmanagementprozess. Der physische Zugangsschutz umfasst die Verhinderung von unbefugtem Zutritt, die Trennung von Produktionsbereichen und die Sicherung kritischer Automatisierungskomponenten. Die Stärke von IT-Sicherheitsmaßnahmen hängt vom Grad des physischen Zugriffsschutzes ab. Effektive Anlagensicherheit erfordert demnach eine Kombination aus organisatorischen und technischen Maßnahmen, einschließlich einer Risikoanalyse, um Sicherheitsziele und potenzielle Schwachstellen zu identifizieren. Siemens-Experten für industrielle Sicherheit helfen bei der Gestaltung sicherer Produktionsumgebungen, der Bewertung des Sicherheitsstatus und der Erstellung einer Sicherheits-Roadmap zur Einhaltung internationaler Sicherheitsstandards wie IEC 62443.

Absicherung von Produktionsnetzwerken

Netzwerksicherheit ist entscheidend für den Schutz vor Cyberangriffen. Mit zunehmender Vernetzung stoßen traditionelle Abwehrkonzepte aber an ihre Grenzen. Dies hat unter anderem zur Einführung des Zero-Trust-Sicherheitskonzepts führt, das sich auf die Verifizierung und Autorisierung kommunizierender Einheiten konzentriert. Da viele OT-Geräte jedoch nicht über die dafür notwendige Funktionalität verfügen, ist für eine umfassende Sicherheit eine Kombination aus Zero-Trust-Prinzipien, Firewalls und perimeterbasierten Netzwerken erforderlich.

Ein sicherer Zugriff auf OT-Netzwerke auf Basis von Zero-Trust-Prinzipien kann durch VPN-Lösungen wie Zscaler Private Access erreicht werden, die IT- und OT-Netzwerke zuverlässig und sicher verbinden. Siemens kooperiert zu diesem Zweck intensiv mit dem IT-Sicherheitsunternehmen Zscaler. Auf diese Weise können Schnittstellen zu anderen Netzwerken überwacht und durch Firewalls und demilitarisierte Zonen (DMZ) geschützt werden. Netzwerksegmentierungs- und Zellschutzkonzepte beinhalten die Trennung von Automatisierungszellen mit technischen Sicherheitsmechanismen, um Risiken zu minimieren, Zugriffsversuche zu kontrollieren und eine verschlüsselte Datenübertragung zu ermöglichen. Komponenten wie die Industrial Security Appliances SCALANCE S von Siemens lassen sich zur Umsetzung dieser Maßnahmen nutzen. Da Anlagen zunehmend direkt mit dem Internet oder über Mobilfunknetze für die Fernwartung und -überwachung verbunden sind, ist die Zugriffssicherung von entscheidender Bedeutung. Mithilfe von VPN-Mechanismen kann die Datenübertragung verschlüsselt und Kommunikationsknoten authentifiziert werden. Die Industrie-Router SCALANCE M und die Industrial Security Appliances SCALANCE S von Siemens bieten benutzerspezifische Firewall-Regeln, die einen temporären, benutzergebundenen Zugriff ermöglichen.

Darüber hinaus bietet die Siemens-Management-Plattform SINEMA Remote Connect einen sicheren und effizienten Fernzugriff auf weltweit verteilte Maschinen und Anlagen über VPN-Tunnel und eine zentrale Benutzerverwaltung. Das Netzwerk-Management-System SINEC NMS ermöglicht eine zentrale Überwachung und Konfiguration von Netzwerken sowie Sicherheit durch verschlüsselte Datenkommunikation und lokale Dokumentation. Zu den Netzwerksicherheitsdiensten im Siemens-Portfolio gehören Industrial Next Generation Firewalls und Industrial-DMZ-Infrastructure-Lösungen, die das Systemnetzwerk vor unbefugtem Zugriff schützen. Die verfügbare industrielle Anomalieerkennung, die auf der Threat Detection Software von Claroty basiert, hilft bei der frühzeitigen Erkennung von Netzwerkanomalien, indem der Echtzeit-Datenverkehr mit dem Basisniveau des normalen Betriebs verglichen wird.

Aufrechterhaltung der Systemintegrität

Die Systemintegrität ist die dritte Stufe eines ausgewogenen Sicherheitskonzepts, die sich auf den Schutz von Steuerungskomponenten, Automatisierungs-, SCADA- und HMI-Systemen konzentriert. Dieser mehrstufige Ansatz ist notwendig, um die

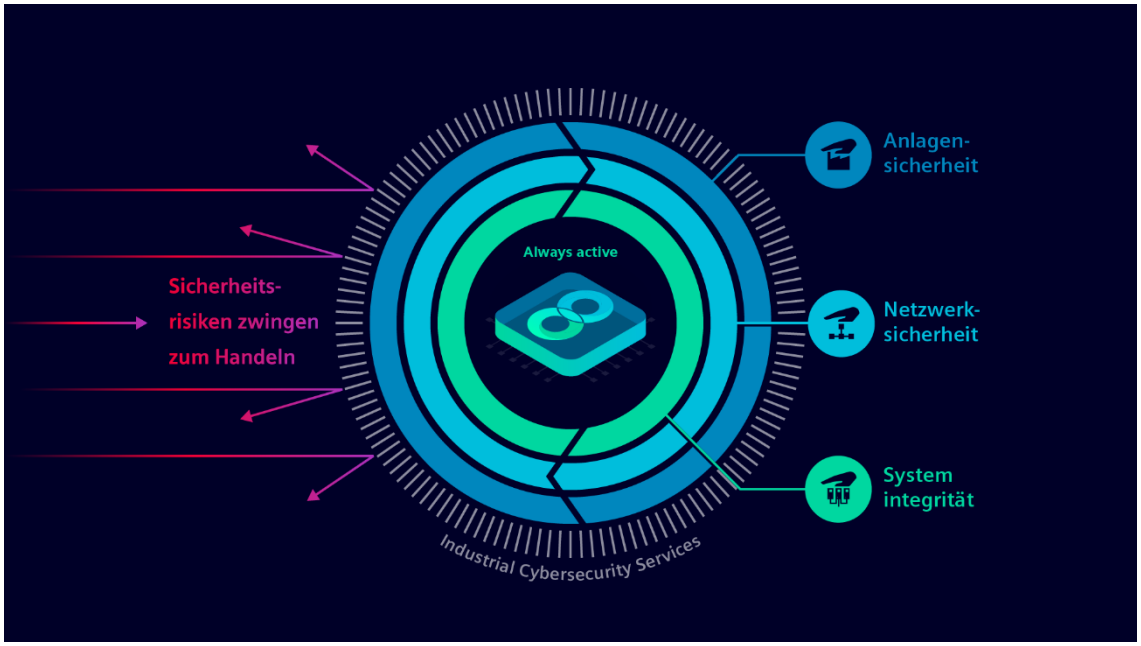
Verteidigung in der Tiefe aufrechtzuerhalten. Der Schutz auf Steuerungsebene wird durch Sicherheitsmechanismen erreicht, die in Standard-Automatisierungskomponenten integriert sind und je nach gewünschtem Schutzniveau der jeweiligen Maschine oder Anlage konfiguriert werden können.

Die Steuerungsfamilien SIMATIC S7-1200 und SIMATIC S7-1500 verfügen über integrierte Features zum Zugriffs- und Manipulationsschutz. Die sichere Kommunikation zwischen S7-Steuerungen und Engineering Stations bzw. HMI-Stationen wird durch TLS-basierte Verschlüsselung ermöglicht. Der TIA Portal Security Wizard unterstützt Anwender außerdem dabei, Sicherheitskonfigurationen für die Steuerungen einzurichten. Auch der Schutz des geistigen Eigentums ist von entscheidender Bedeutung – Siemens-Steuerungen bieten hierfür Know-how-Schutz und Kopierschutzfunktionen. Zudem sind eine Stateful Inspection Firewall und VPN in den Security-Kommunikationsprozessoren für S7-Steuerungen integriert und schaffen so sichere Schnittstellen zum gesamten Anlagennetzwerk.

Zum Schutz von PC-basierten Systemen im Werksnetzwerk werden Anti-Viren-Software, Whitelisting-Lösungen und integrierte Sicherheitsmechanismen in Windows-Betriebssystemen eingesetzt. Siemens unterstützt den Schutz von Industrie-PCs und PC-basierten Systemen durch die Prüfung der Softwarekompatibilität mit Virenscannern und Whitelisting-Software und stellt Richtlinien für die Systemhärtung bereit.

Ein sicheres Zutrittsmanagement für Maschinen und Anlagen ermöglicht der Access Control Reader SIMATIC RF1000, der das Maschinenbedienpersonal identifiziert und entsprechende Zutrittsrechte über RFID-Karten und benutzerspezifische Login-Daten zuweist. Auf diese Weise lassen sich Sicherheitsvorfälle transparent zurückverfolgen. Die Siemens-Systemintegritätsdienste basieren auf bewährten Technologien und Partnern. Siemens bietet Endpoint Protection über zwei Ansätze an: Antivirus, das Schadprogramme blockiert, und Application Whitelisting, bei dem nur vertrauenswürdige Anwendungen ausgeführt werden können. Darüber hinaus unterstützt Siemens seine Kunden mit Endpoint Detection and Response (EDR)-Lösungen von Drittanbietern. Die hauseigene Industrial Vulnerability Manager App hilft beim Management von Cyber-Risiken, indem sie Komponenten auf veröffentlichte Schwachstellen überwacht. Darüber hinaus eignet sich der Patch-Management-Service von Siemens für das Management von Schwachstellen und kritischen Updates

in Microsoft-Produkten mit getesteten und freigegebenen Patches für die Kompatibilität mit Steuerungssystemen wie SIMATIC PCS 7. Schließlich bieten Siemens-Service-Experten über den Managed Hardening Service Unterstützung für SIMATC-Controller an, um sicherzustellen, dass das volle Sicherheitspotenzial der eingesetzten Steuerungen ausgeschöpft wird.



Defense-in-Depth-Konzept für Industrial Cybersecurity

Weitere Informationen zu Siemens Industrial Cybersecurity finden Sie unter www.siemens.de/cybersecurity-industry

Pressemitteilung zur Zscaler-Partnerschaft:
https://press.siemens.com/global/de/pressemitteilung/siemens-und-zscaler-kooperieren-fuer-durchgaengige-sicherheitsloesungen-mit-zero

Kontakt für Journalistinnen und Journalisten
Christoph Krösmann
Telefon: +49 162 7436402
E-Mail: christoph.kroesmann@siemens.com

Folgen Sie uns in **Social Media**:
Twitter: www.twitter.com/siemens_press und www.twitter.com/SiemensIndustry
Blog: https://blog.siemens.com

Siemens Digital Industries (DI) ist ein Innovationsführer in der Automatisierung und Digitalisierung. In enger Zusammenarbeit mit Partnern und Kunden, treibt DI die digitale Transformation in der Prozess- und Fertigungsindustrie voran. Mit dem Digital-Enterprise-Portfolio bietet Siemens Unternehmen jeder Größe durchgängige Produkte, Lösungen und Services für die Integration und Digitalisierung der gesamten Wertschöpfungskette. Optimiert für die spezifischen Anforderungen der jeweiligen Branchen, ermöglicht das einmalige Portfolio Kunden, ihre Produktivität und Flexibilität zu erhöhen. DI erweitert sein Portfolio fortlaufend durch Innovationen und die Integration von Zukunftstechnologien. Siemens Digital Industries hat seinen Sitz in Nürnberg und beschäftigt weltweit rund 72.000 Mitarbeiter.

Die Siemens AG (Berlin und München) ist ein Technologieunternehmen mit Fokus auf die Felder Industrie, Infrastruktur, Mobilität und Gesundheit. Ressourceneffiziente Fabriken, widerstandsfähige Lieferketten, intelligente Gebäude und Stromnetze, emissionsarme und komfortable Züge und eine fortschrittliche Gesundheitsversorgung – das Unternehmen unterstützt seine Kunden mit Technologien, die ihnen konkreten Nutzen bieten. Durch die Kombination der realen und der digitalen Welten befähigt Siemens seine Kunden, ihre Industrien und Märkte zu transformieren und verbessert damit den Alltag für Milliarden von Menschen. Siemens ist mehrheitlicher Eigentümer des börsennotierten Unternehmens Siemens Healthineers – einem weltweit führenden Anbieter von Medizintechnik, der die Zukunft der Gesundheitsversorgung gestaltet. Darüber hinaus hält Siemens eine Minderheitsbeteiligung an der börsengelisteten Siemens Energy, einem der weltweit führenden Unternehmen in der Energieübertragung und -erzeugung.
Im Geschäftsjahr 2022, das am 30. September 2022 endete, erzielte der Siemens-Konzern einen Umsatz von 72,0 Milliarden Euro und einen Gewinn nach Steuern von 4,4 Milliarden Euro. Zum 30.09.2022 hatte das Unternehmen weltweit rund 311.000 Beschäftigte. Weitere Informationen finden Sie im Internet unter www.siemens.com.