Wie man Fertigungsbetriebe mit zukunftssicheren Netzwerklösungen vor Cyberbedrohungen schützt

Im Jahr 2022 verzeichnete das verarbeitende Gewerbe die höchste Zahl von Cyberangriffen unter den großen Branchen weltweit. Der Hauptgrund für dieses Phänomen ist die Auflösung der Trennung zwischen industriellen Kontrollsystemen (ICS) und dem Internet, auch bekannt als Konvergenz von Operativer Technologie (OT) und Informationstechnologie (IT), die die Betriebsmittel-Infrastruktur neuen Cyberbedrohungen aussetzt. Die moderne Fertigung kann sich jedoch nicht von der Außenwelt abschotten, wenn sie wettbewerbsfähig bleiben will.

Dieser Artikel befasset sich mit den größten Herausforderungen bei zwei intelligenten Fertigungsanwendungen, nämlich

(1) der Vernetzung neuer Geräte in großem Maßstab für die Anlagenüberwachung in Echtzeit und

(2) der Integration mehrerer Netzwerke für optimale Betriebsabläufe.

Neue Bedrohung für intelligente Fertigungssysteme

Der Siegeszug der intelligenten Fertigung oder Industrie 4.0 hat zu einer wachsenden Zahl von Cyberbedrohungen im Industriesektor als unbeabsichtigte Folge der OT/IT-Konvergenz geführt. Die Verschmelzung von OT- und IT-Infrastruktur führt zwar zu besserer Effizienz und höherer Wertschöpfung, setzt aber auch traditionell isolierte OT-Systeme allen Arten von Cyberangriffen aus. Die Kombination aus einer sich ständig erweiternden Bedrohungslandschaft und der extrem geringen Toleranz von Fertigungsunternehmen gegenüber Ausfallzeiten macht sie zu einem bevorzugten Ziel für Cyberangriffe. Wie bereits erwähnt, war das verarbeitende Gewerbe im Jahr 2022 von allen Branchen am stärksten von Cyberangriffen betroffen.

Ein genauerer Blick auf die Arten von industriellen Anwendungen, die ins Visier genommen wurden, zeigt einige gemeinsame Herausforderungen, aber auch einige offensichtliche Bereiche mit Verbesserungspotenzial. Werfen wir einen Blick auf zwei praktische Beispiele für industrielle Anwendungen, wie sie von Cyberbedrohungen betroffen sein können und wie man ihre Anfälligkeit für Cybersicherheitsrisiken verringern kann.

Vernetzung neuer Geräte

Anwendung 1: Vernetzung neuer Geräte für die Anlagenüberwachung in Echtzeit

Anwendungen, die eine Echtzeit-Überwachung und -Steuerung für groß angelegte industrielle Netzwerke ermöglichen, sind zunehmend anfällig für Cyber-Bedrohungen. Diese Anwendungen erfordern in der Regel den Einsatz vieler vernetzter Geräte in großem Umfang, um große Datenmengen aus dem Feld zu sammeln, zu senden und im Steuerungszentrum zu analysieren. Folgende Punkte sind im Zusammenhang mit der Cybersicherheit zu beachten:

- Hunderte von speicherprogrammierbaren Steuerungen (SPS) und Sensoren müssen miteinander verbunden werden, um Daten über den Zustand der Produktionsanlagen zu sammeln und den Energieverbrauch zu optimieren. Jedes dieser Geräte ist ein neuer Knotenpunkt, der potenziell Opfer von Cybersicherheitsangriffen wie z. B. unbefugtem Zugriff oder Malware-Angriffen werden kann.

- Die Schwachstellen werden noch verstärkt, wenn diese Netze expandieren und eine große Anzahl von Edge-Geräten in der Distributionsebene zusammengeführt werden. Wenn das Netz nicht ordnungsgemäß untergliedert ist, ist das gesamte Netz anfällig, wenn nur ein einziger Knoten kompromittiert wird.

Defense-in-Depth-Ansatz

Für diese Anwendungen sollten die Betreiber einen Defense-in-Depth-Ansatz in Betracht ziehen.

Text und Bilder von Moxa Inc.
www.moxa.com
übersetzt von
Marianne Ruskowski
systerra computer Systeme
www.systerra.de

Dazu gehören

- die Verwendung sicherer Geräte
- der Aufbau untergliederter, robuster Netzwerk- Sicherheitsebenen (Segmentierung)
- die Echtzeit-Überwachung des Netzwerkstatus

um die Sicherheit und Verfügbarkeit des Netzwerks zu gewährleisten.

Die Auswahl von sicherheitsoptimierten Geräten, die internationale Sicherheitszertifizierungen bestanden haben oder über Sicherheitsfunktionen verfügen, die auf international anerkannten Standards wie IEC 62443 und NERC CIP basieren, kann beim Hinzufügen neuer Netzwerkknoten solide Bausteine liefern.

Segmentierung und Prävention

von Bedrohungen bieten eine weitere Sicherheitsebene zum Schutz vor Angriffen und verhindern, dass sich unerwünschte Eindringlinge und Bedrohungen auf andere Netzwerkknoten ausbreiten. Nicht zuletzt können Sie durch die ständige Überwachung des Sicherheitsstatus Ihrer Netzwerkknoten alle Probleme und Anomalien erkennen und darauf reagieren.

Integration mehrerer Netzwerke

Anwendung 2: Integration mehrerer Netzwerke für optimale Betriebsabläufe

Eine weitere Anwendung in der Fertigung, die für Bedrohungen der Cybersicherheit anfällig ist, ist die Integration von Industrieanlagen in Netzwerke zur Optimierung der Betriebsabläufe.

Bislang bauten Industrieingenieure eine geschlossene Netzwerkumgebung auf und verwendeten ähnliche Schemata, um den Maschinen IP-Adressen zuzuweisen.

Die Möglichkeit der Fernsteuerung und -verwaltung von Industriemaschinen erfordert jedoch den Anschluss industrieller Netzwerke an das Internet. Wenn diese traditionell isolierten Maschinen an ein zentrales Managementsystem angeschlossen werden müssen, kann die Verwendung desselben Musters zur Generierung von IP-Adressen für alle Maschinen zu IP-Konflikten führen und Ausfallzeiten im Netzwerk verursachen. Für alle Geräte muss dann die IP-Adresse neu konfiguriert werden, eine zeitaufwändige Aufgabe, die leicht zu Sicherheitslücken führen kann. Außerdem sind sie, wenn sie über ein internetfähiges öffentliches Netz verbunden sind, allen Arten von neuen Cyberbedrohungen ausgesetzt. Insbesondere vorhersehbare IP-Adressen werden schnell zum Ziel von Cyberangriffen.

NAT-Technologie

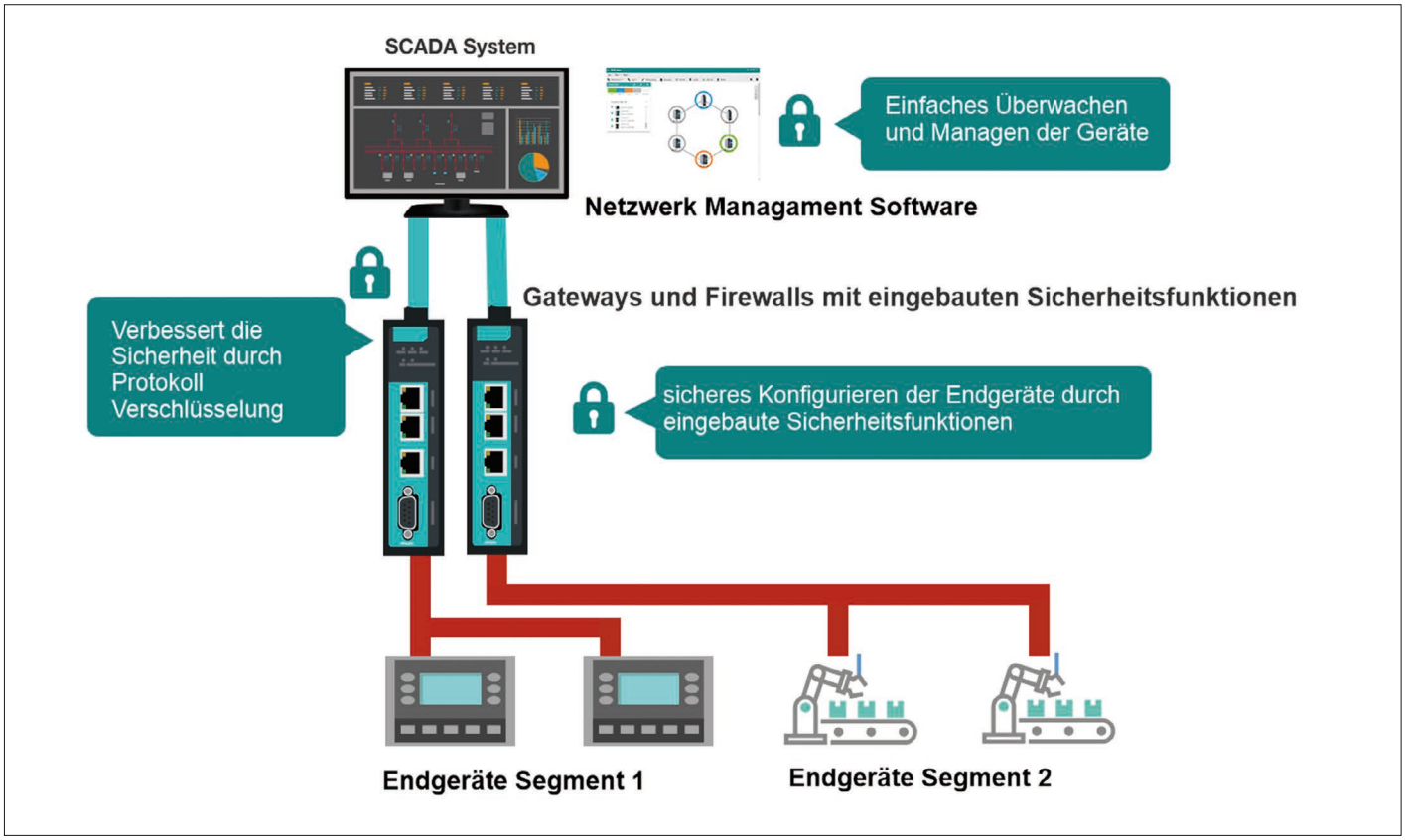
Eine vereinfachte Verwaltung und verbesserte Sicherheit können diese Schwachstellen weitgehend beseitigen. So könnten Systemintegratoren beispielsweise die Vorteile der NAT-Technologie (Network Address Translation) nutzen, um IP-Adressen vor unbefugten Zugriffen zu schützen und die Geräteintegration zu vereinfachen.

Neuere Hardware-Lösungen bieten auch eingebettete intelligente Mechanismen zur Abwehr von Bedrohungen, die automatisch Daten blockieren, die von nicht autorisierten IP-Adressen stammen. Zusammengenommen bieten diese Tools eine weitere robuste Schutzschicht für Maschinennetzwerke.

Netzwerksicherheit weiterentwickeln

Überwinden Sie die Hürden der OT-Vernetzung und schaffen Sie den Übergang zu einer intelligenten digitalen Zukunft. Mit der Konvergenz Ihrer OT- und IT-Netzwerke auf dem Weg zur Digitalisierung muss sich die Netzwerksicherheit weiterentwickeln, um neuen Cyber-Bedrohungen zu begegnen. Die regelmäßige Überwachung der Netzwerkinfrastruktur und die Aktualisierung der Schutzmechanismen sind wichtige Bestandteile einer dynamischen Sicherheitsstrategie, um angeschlossene Systeme zu schützen und kostspielige Ausfallzeiten zu reduzieren.

Anwender sehen sich oft der Herausforderung gegenüber, ihre Systeme gleichzeitig intelligent und sicher zu halten, die leicht überfordern kann. Um sich gegen Cyber-Bedrohungen zu schützen, müssen Systemintegratoren und Anwender in der Industrie ihre Fertigungsnetzwerke mit integrierten industriellen Netzwerklösungen zukunftssicher machen und einen auf OT-Ingenieure zugeschnittenen Defense-in-Depth-Ansatz anwenden. ◄



Beispiel eines gesicherten Industrie-Netzwerks