Cybersecurity-Gegenmaßnahmen für den Aufbau einer sicheren Netzwerkinfrastruktur

Heutzutage verstehen immer mehr Unternehmen, dass die Digitalisierung notwendig ist, um zu überleben und zu florieren. Eine Deloitte-Studie zu Smart Factory aus dem Jahr 2019 ergab, dass 86 % der Hersteller der Meinung sind, dass ihre Smart-Factory-Initiativen in den nächsten fünf Jahren der wichtigste Faktor für ihre Wettbewerbsfähigkeit sein werden. Im Jahr 2020 wurden diese Initiativen aufgrund der globalen Pandemie beschleunigt. In einem kürzlich erschienenen Bericht des Weltwirtschaftsforums mit dem Titel „Building Resilience in Manufacturing and Supply Systems in the COVID-19 Context and Beyond" wird vorgeschlagen, dass die Hersteller neue Arbeitsmodelle einführen und anwenden, um die Widerstandsfähigkeit der Produktion zu erhöhen. Angesichts der aktuellen Krise reicht eine beschleunigte Digitalisierung allein jedoch nicht mehr aus. In diesem Artikel gehen wir der Frage nach, wie belastbare Industrienetzwerke aufgebaut und Cybersicherheitsmaßnahmen eingesetzt werden können, um einen kontinuierlichen industriellen Betrieb aufrechtzuerhalten.

Wege zur Cybersicherheit

Die Zahl der Cybersecurity-Vorfälle in industriellen Kontrollsystemen (ICS) nimmt immer weiter zu. Viele Unternehmen haben begonnen, ihre eigenen Cybersecurity-Strategien zu entwickeln und Anlagen zu schützen, die sie als kritisch für einen erfolgreichen Betrieb ansehen. Leider gibt es kein Patentrezept für die Beseitigung aller Schwachstellen im ICS. Die Cybersicherheit muss aus verschiedenen Perspektiven betrachtet werden. Der Weg zur Cybersicherheit beginnt oft mit einer Risikobewertung. Danach können die Unternehmen entsprechende Sicherheitsrichtlinien aufstellen. Um diese umzusetzen, lohnt es sich, eine Sicherheitsarchitektur zu schaffen, die zu einer sicheren Netzwerkinfrastruktur beiträgt. Beispielsweise lässt sich mit Hilfe von Zugriffskontrolllisten regeln, wer auf das Netz zugreifen darf.

Schließlich können Unternehmen Cybersecurity-Vorfälle proaktiv überwachen und darauf reagieren, indem sie industrielle Cybersecurity-Gegenmaßnahmen implementieren (Bild 1).

Cybersecurity muss holistisch sein

Wie im vorangegangenen Absatz erwähnt, umfasst jeder Weg zur industriellen Cybersicherheit verschiedene Phasen mit entsprechenden Gegenmaßnahmen. Da es keine Einzellösung gibt, die alle Aspekte abdecken kann, empfehlen wir, Cybersicherheit aus einer ganzheitlichen Perspektive zu betrachten. Herkömmliche Gegenmaßnahmen wie Firewalls verstärken den Perimeterschutz von Industrienetzwerken. Sie bieten einen wirksamen vertikalen Schutz, um zu verhindern, dass Personen, die keine Berechtigung haben, auf das Netzwerk zugreifen. Wenn es jedoch gelingt, diesen Schutz zu überwinden, oder Mitarbeiter versehentlich einen falschen Befehl innerhalb des Netzes absetzen, gibt es keine Maßnahmen zur Minderung der Risiken, die dadurch entstehen können.

Daher ist es wichtig, auch horizontalen Schutz wie virtuelles Patching und ein IDS (Intrusion Detection System) oder IPS (Intrusion-Prevention-System) einzusetzen. In den folgenden Abschnitten werden wir die herausragende Rolle des vertikalen und horizontalen Schutzes bei der Sicherung industrieller Netzwerke untersuchen (Bild 2).

Vertikaler Schutz

Aufbau einer sicheren Netzwerkinfrastruktur zur Umsetzung von Sicherheitsrichtlinien

Netzwerkmanagement

Industrielle Netzwerke sind oft über Jahre oder sogar Jahrzehnte hinweg gewachsen. Es kann daher ein schwieriger erster Schritt sein, sich einen Überblick über das Netzwerk und seine verschiedenen Komponenten und Architekturen zu verschaffen. Unserer Erfahrung nach liefert ein industrielles Netzwerkmanagement-Tool, das ein Netzwerk scannen und automatisch die Topologie erstellen kann, den Ingenieuren viele nützliche Informationen für die Entwicklung eines Aktionsplans.

Netzwerkschutz

Die Netzsegmentierung ist eine grundlegende Vorsichtsmaßnahme, mit der sichergestellt werden kann, dass ein bestimmter Datenverkehr nur innerhalb festgelegter Bereiche fließen kann. Es gibt verschiedene

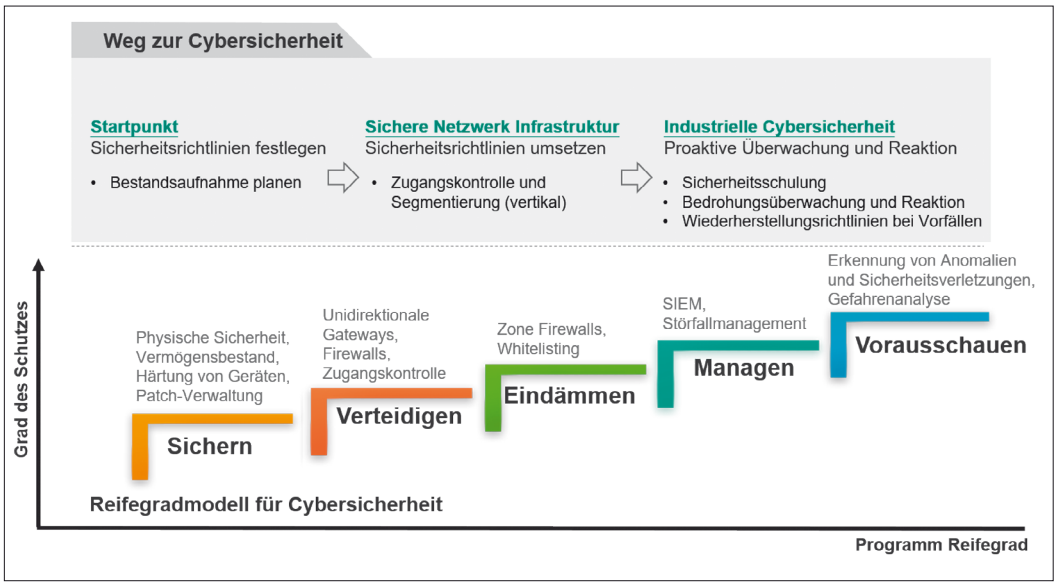

Bild 1: Weg zur Cybersicherheit
© ARC Advisory Group, https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model

systerra computer GmbH
www.systerra.de

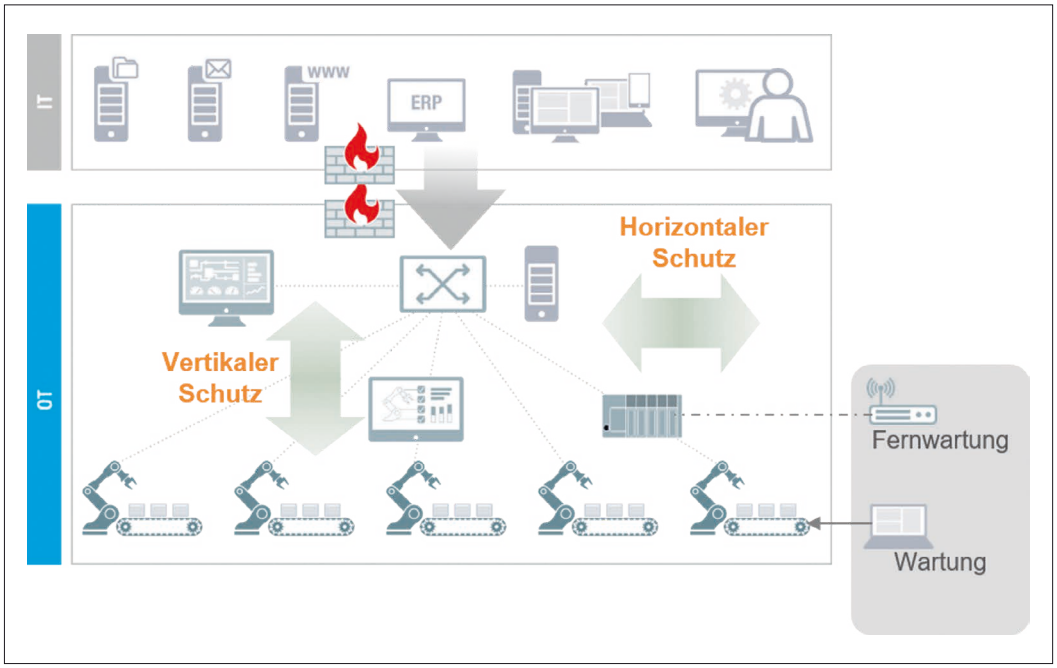

Bild 2: Für ganzheitliche Gegenmaßnahmen zur Cybersicherheit sollte sowohl der horizontale als auch der vertikale Verkehr berücksichtigt werden.

Methoden, um eine Netzwerksegmentierung zu erreichen. So können z. B. Stateful Firewalls dazu beitragen, eine erste Verteidigungslinie zu schaffen, ohne dass die Netzwerktopologie geändert werden muss. Das ist insbesondere für Bereiche vorteilhaft, die unterbrechungsfrei arbeiten müssen.

Die Einrichtung virtueller LANs (VLANs) innerhalb eines größeren Netzwerks kann ebenfalls zur Segmentierung von Netzwerken beitragen. Eine weitere Faustregel ist die Implementierung von Authentifizierung über 802.1x (AAA/Radius TACACS) und Zugriffskontrolle über eine ACL (Access Control List).

Nicht zuletzt sind Fernsteuerung, -überwachung und -wartung im täglichen Betrieb immer häufiger anzutreffen. Die Sicherstellung eines geschützten Fernzugriffs verringert die Wahrscheinlichkeit von Sicherheitsverletzungen und muss unbedingt mitbedacht werden.

Gerätesicherheit

Anfangs bestehen die beiden größten Herausforderungen in der Entwicklung und Umsetzung praktischer und angemessener Sicherheitsrichtlinien für die Authentifizierung und Netzwerksegmentierung. Normen wie IEC 62443 können bei der Festlegung von Richtlinien, die für industrielle Netzwerke sinnvoll sind, sehr hilfreich sein.

Horizontaler Schutz

Cybersicherheit zur proaktiven Überwachung und Reaktion einsetzen. Wenn Unternehmen mit der Implementierung von Cybersicherheitsmaßnahmen in ihren industriellen Netzwerken beginnen, ist der erste Schritt zum Schutz des vertikal verlaufenden Netzwerkverkehrs häufig ein Abwehrmechanismus wie die Netzwerksegmentierung. Ist dies ausreichend?

Die Antwort lautet leider: Nein. Auch wenn der vertikal gebundene Datenverkehr gut verwaltet und geschützt ist, haben Mitarbeiter, Lieferanten und Auftragnehmer immer noch direkten Zugang zu den Netzwerken. Ohne Schutzmaßnahmen können sie unbeabsichtigt traditionelle Abwehrmechanismen wie Firewalls umgehen und möglicherweise Viren oder Malware in die Industrienetze einschleusen.

Aus diesem Grund sind horizontale Schutzmaßnahmen wie virtuelles Patching und Intrusion Prevention von entscheidender Bedeutung für den Schutz kritischer Anlagen wie SPS und HMI.

Industrielles IPS schützt kritische Anlagen

Da PLCs und HMIs für die Steuerung von Produktionsprozessen konzipiert sind, könnte eine Beeinträchtigung der Kommunikation zwischen PLCs und dem Kontrollzentrum oder eine Fehlfunktion der HMIs zu Schäden an Anlagen oder sogar an Personen führen. Daher muss verhindert werden, dass unbefugte Protokolle und Funktionen über PLCs und HMIs laufen. Ein industrielles IPS (Intrusion Prevention System) verfügt über eine OT-zentrierte Deep Packet Inspection-Technologie, die mehrere industrielle Protokolle identifizieren und bestimmte Funktionen wie Lese-/Schreibzugriffe zulassen oder blockieren kann. Auf diese Weise kann man sicherstellen, dass der Datenverkehr in industriellen Netzwerken vertrauenswürdig und nicht bösartig ist.

Virtuelles Patching schützt ungepatchte Geräte

Es ist eine bekannte Regel, Geräte immer auf dem neuesten Stand zu halten, um Cyberbedrohungen vorzubeugen. In Industrienetzen ist es jedoch manchmal ungünstig, den Betrieb für die Durchführung von Aktualisierungen zu unterbrechen. Außerdem kann es vorkommen, dass für manche kritischen Anlagen keine Updates verfügbar sind. So laufen beispielsweise einige HMIs unter Windows XP, das keine Updates mehr unterstützt. Unter solchen Umständen spielen virtuelle Patches eine wichtige Rolle, um kritische Anlagen vor den neuesten Bedrohungen der Cybersicherheit zu schützen.

Sicherheitsmanagement bietet klare Sichtbarkeit

Wenn ein Netzwerk in Betrieb ist, kann es eine ziemliche Herausforderung sein, das Netzwerk zu warten und schnell anzupassen. Sicherheitsmanagement-Software ist daher sehr hilfreich für die Verwaltung von Geräten und Sicherheitsrichtlinien sowie für die Durchführung virtueller Patches.

Da es keine Einzellösung für die Cybersicherheit gibt, müssen Unternehmen ihren aktuellen Status prüfen und die richtige Kombination von Lösungen auswählen. Man sollte versuchen, beide Perspektiven - sichere Netzwerkinfrastruktur und industrielle Cybersicherheit - zu berücksichtigen, um einen vertikalen und horizontalen Schutz aufzubauen (Bild 3). ◄

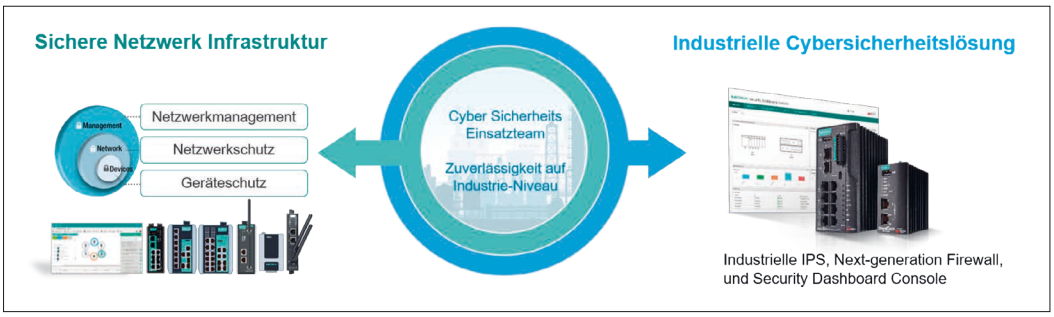

Bild 3: Sichere Netzwerk-Infrastruktur