Proaktiver Schutz industrieller Netzwerke

Alle Bilder © Moxa

systerra computer GmbH
www.systerra.de

In den letzten Jahren haben Vorfälle im Bereich der Cybersicherheit kritische Infrastrukturen vermehrt lahmgelegt und Unternehmen geschädigt. Bei einigen handelte es sich um gezielte Angriffe, wie z. B. Ransomware, bei anderen jedoch um ungezielte Vorfälle, wie z. B. die Kontaminierung durch Malware, welche sich Zugang zu einem nicht autorisierten Computer verschaffte und sich von dort auf das gesamte industrielle Steuerungsnetzwerk ausbreitete.

Die Umsetzung einer zonenbasierten industriellen Netzwerkarchitektur kann den Schaden verringern.

Proaktive Maßnahmen sind wichtig

Cybersicherheitsexperten schlagen inzwischen verstärkt zusätzliche, proaktive Maßnahmen zum Schutz industrieller Netzwerke vor. Zum Beispiel ein industrielles Intrusion-Prevention-System (IPS), das Eindringlinge wirksam abwehrt und die Auswirkungen auf industrielle Systeme reduzieren kann.

Was ist ein IPS?

Ein IPS ist eine Netzwerksicherheitslösung, die Bedrohungen durch ständige Überwachung der Netzwerke erkennt und blockiert, nach möglichen schädlichen Cyber-Vorfällen sucht und Informationen darüber protokolliert. Es verfügt über eine Deep Packet Inspection (DPI)-Technologie, die durch vollständige Überprüfung der Datenpakete die Transparenz der Netzwerksicherheit erhöht und letztlich dazu beiträgt, Risiken zu mindern und industrielle Netzwerke vor Sicherheitsbedrohungen zu schützen.

Industrielles IPS, maßgeschneidert für industrielle Netzwerke

Obwohl die IPS-Technologie in IT-Netzwerken seit einiger Zeit sehr gut funktioniert, ist es schwierig, ein IPS direkt in operativen Netzwerken einzusetzen. Hier stehen sich Leistung und Verfügbarkeit mit Datensicherheit gegenüber. Die

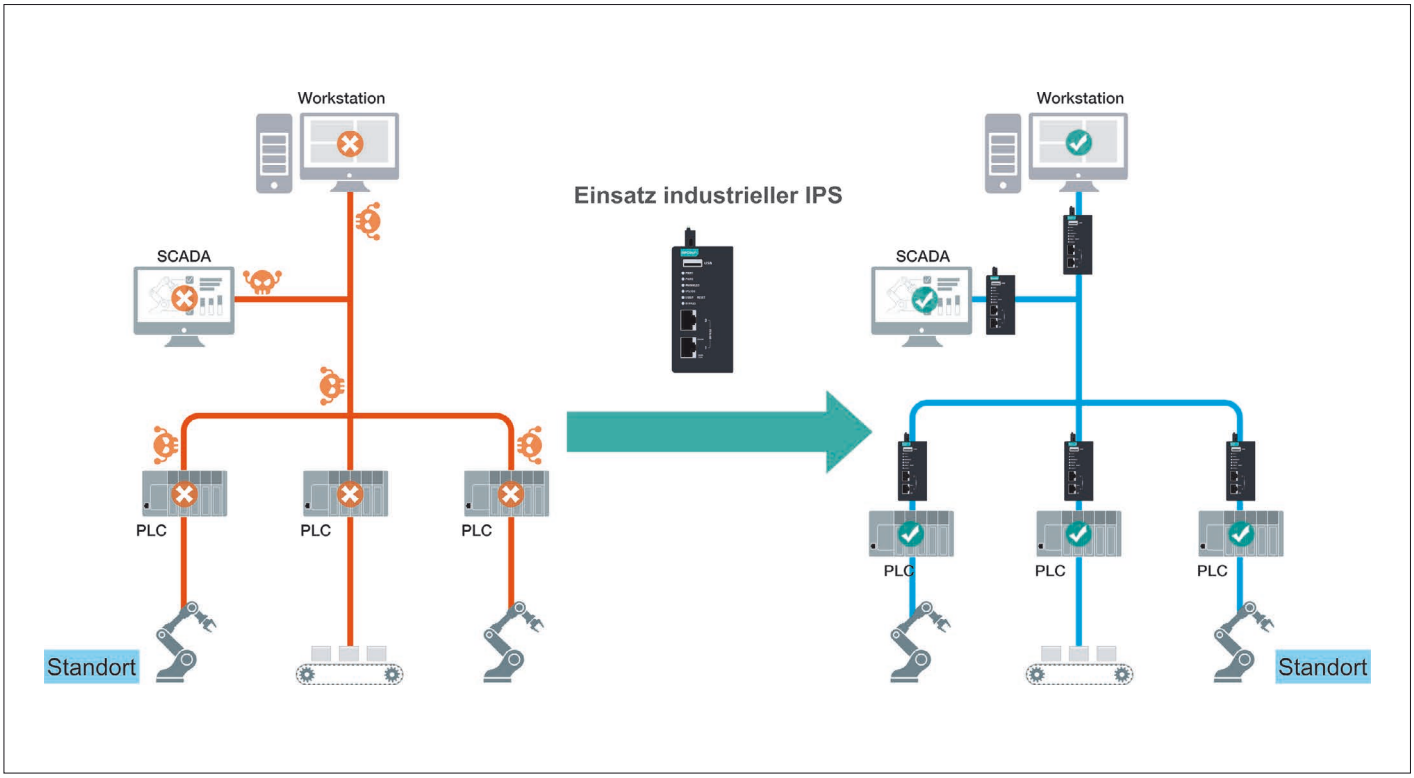

Bild 1: Industrielles IPS sichert den Datenverkehr in industriellen Netzwerken

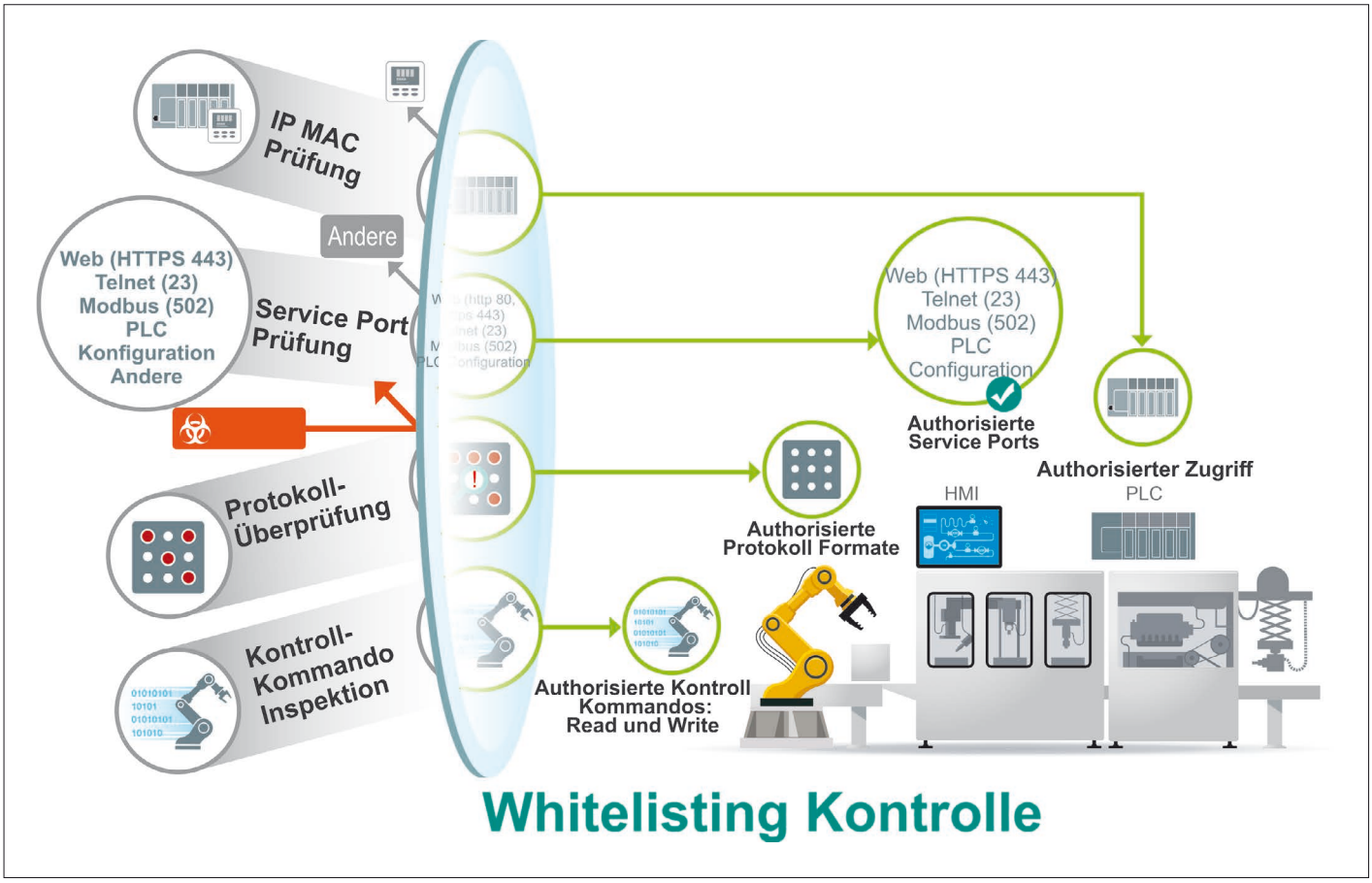

Bild 2: Whitelisting-Kontrolle erlaubt den Zugriff nur für auf einer Whitelist autorisierte Geräte, Dienste, Protokollformate und Steuerbefehle

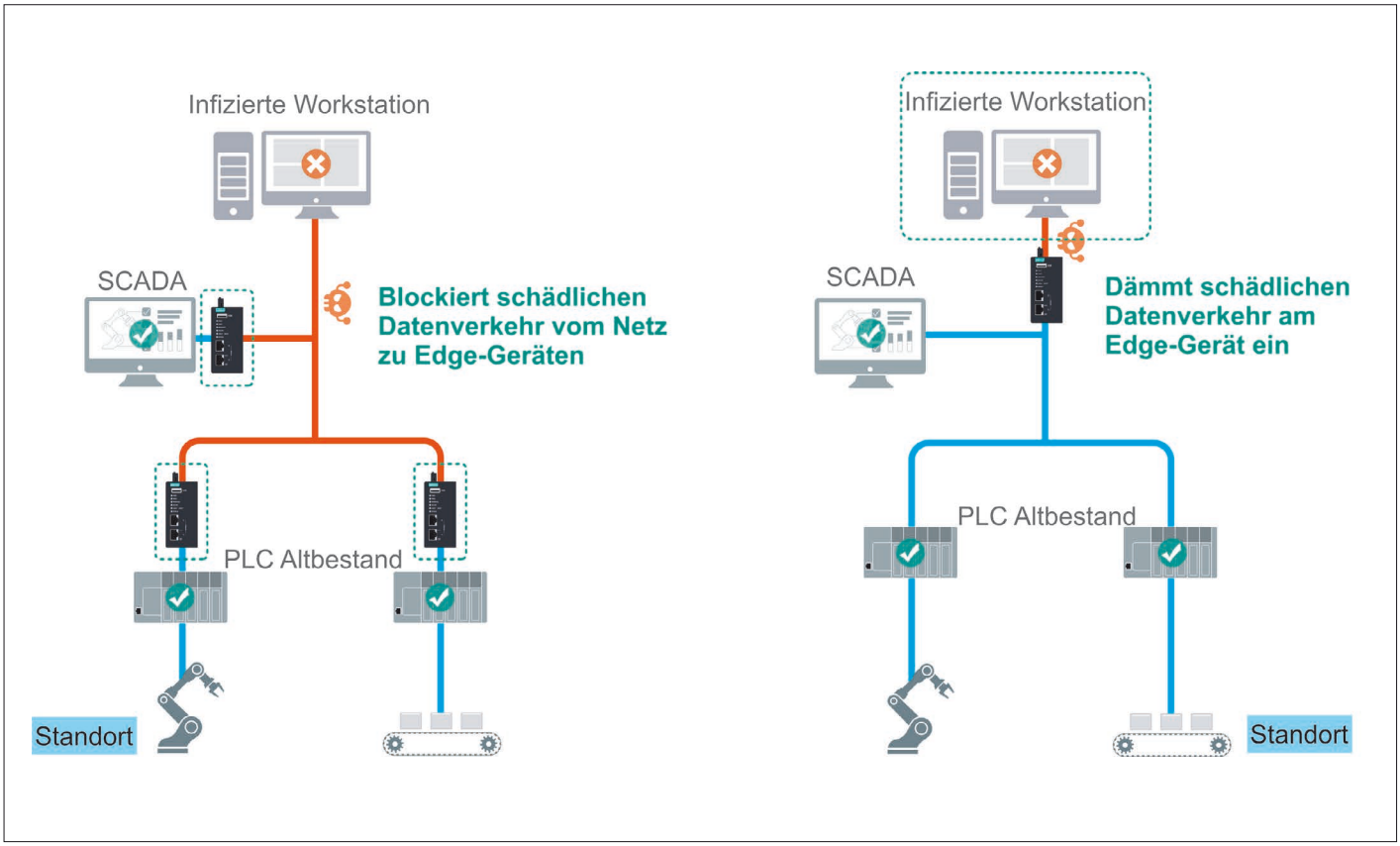

Bild 3: Ein Industrielles IPS kann den schädlichen Datenverkehr vom Netzwerk zu Edge-Geräten blockieren

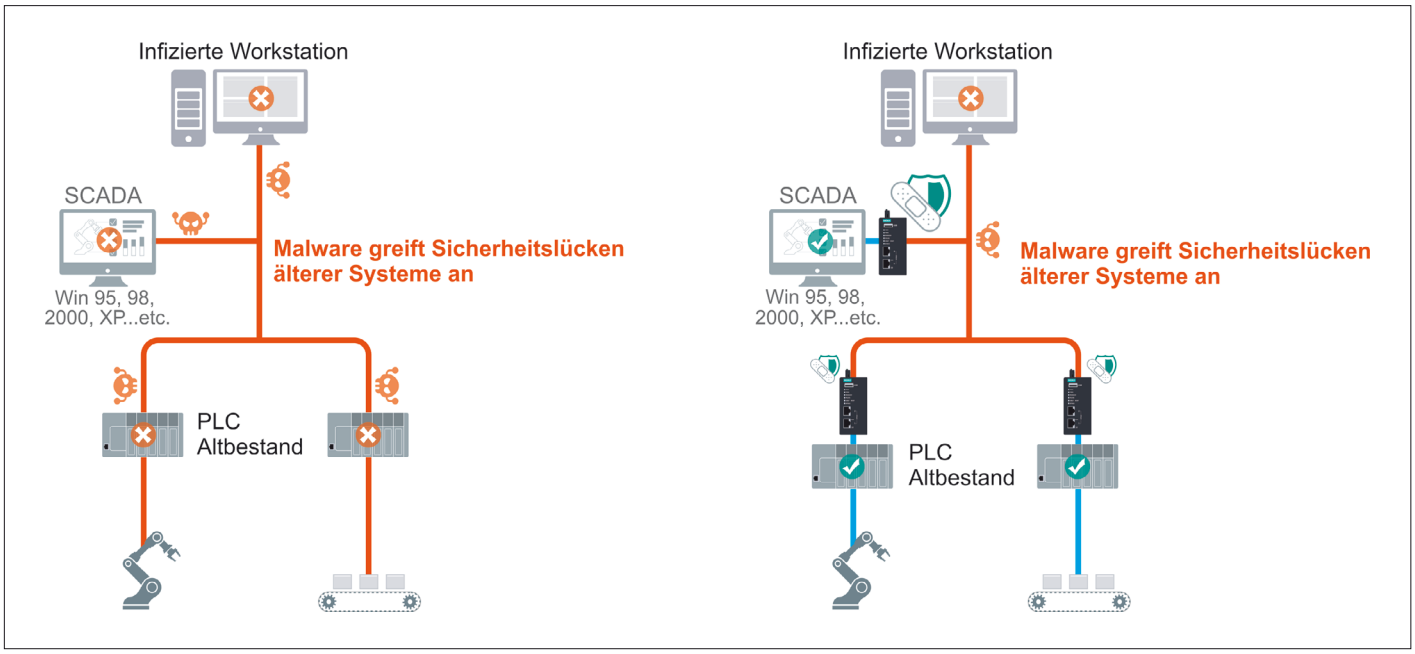

Bild 4: Virtuelles Patching behebt Schwachstellen von Altgeräten

Implementierung eines IPS in operativen Netzwerken ohne Berücksichtigung der täglichen Betriebsanforderungen könnte möglicherweise wichtige Steuerbefehle für die Produktion blockieren und damit den Betrieb stören.

Um die Anforderungen an die Cybersicherheit zu erfüllen, ist es unerlässlich, operativ bezogene DPI-Technologie zu nutzen. DPI kann mehrere Industrieprotokolle identifizieren und bestimmte Funktionen, wie z. B. Lese- oder Schreibzugriffe, zulassen oder sperren. Basierend auf dem identifizierten Protokoll kann ein industrielles IPS dann alle nicht autorisierten Protokolle oder Funktionen verhindern. So wird sichergestellt, dass der Datenverkehr in industriellen Netzwerken sicher und unschädlich ist (Bild 1).

Whitelisting-Kontrolle definiert eine granulare Zugriffsregelung

Bei der Whitelisting-Kontrolle (Bild 2) handelt es sich um einen Genehmigungs- und Freigabemechanismus. Der Zugriff wird nur von autorisierten Geräten, Diensten, Protokollformaten und Steuerbefehlen zugelassen, die auf der Whitelist aufgeführt werden. Der Mechanismus stellt sicher, dass alle Netzwerkaktivitäten in industriellen Netzwerken autorisiert sind. Netzwerkbetreiber können je nach betrieblichen Anforderungen differenzierte Zugriffskontrollen auf verschiedenen Ebenen definieren.

So können Netzwerkingenieure beispielsweise eine Whitelist von Geräten und Diensten oder IP-Ports definieren, die auf das gesamte oder einen Teil des gesamten Netzwerks zugreifen dürfen.

Darüber hinaus ist es möglich, ein genehmigtes Protokollformat zu definieren, um zu verhindern, dass nicht autorisierte Befehle durch das Netzwerk geleitet werden. Außerdem können Netzwerkingenieure sogar festlegen, welche Steuerbefehle das Netzwerk passieren dürfen, um menschliches Versagen im Zusammenhang mit dem Senden eines falschen Steuerbefehls zu reduzieren. Mit der Whitelisting-Kontrolle kann die Wahrscheinlichkeit eines DoS-Angriffs durch Trojaner erheblich reduziert werden.

Einsatzszenarien für ein industrielles IPS

1. Blockieren und Eindämmen von schädlichem Datenverkehr

Ein industrielles IPS schützt, indem es schädlichen Datenverkehr vom Netz zu den Edge-Geräten blockiert und ihn schon an den Edge-Geräten eindämmt. Es kann vor kritischen Anlagen wie SPS und HMI platziert werden, um die Netzwerksicherheit zu erhöhen, Netzverfügbarkeit zu gewährleisten und gleichzeitig kritische Anlagen vor Manipulation durch böswillige Akteure zu schützen.

Ist beispielsweise ein Arbeitsplatzrechner mit Malware infiziert, findet die Malware oft einen Weg, sich auf so viele Geräte und Netzwerke wie möglich zu verbreiten. Bis ein Netzwerkingenieur oder Netzwerkbetreiber sie bemerkt, hat sie vermutlich schon die meisten Geräte im Netzwerk befallen. Daher sind zwei proaktive Maßnahmen wichtig, um die Risiken zu mindern. Zum einen muss, wenn das Netzwerk verseucht ist, der schädliche Datenverkehr sofort blockiert werden, und zum anderen muss er auf ein überschaubares Maß beschränkt werden können (Bild 3).

2. Virtuelles Patching zur Verringerung der Anfälligkeit eines Systems für Cyber-Bedrohungen

Häufiges Patching reduziert die Gefährdung eines Systems durch Cyberbedrohungen erheblich. In industriellen Netzwerkumgebungen stellt dies jedoch nach wie vor eine große Herausforderung dar. Geräte in industriellen Kontrollsystemen sind nicht immer sofort für Updates verfügbar, wenn Sicherheitslücken entdeckt werden. So muss beispielsweise ein Produktionsbetrieb bis zum nächsten Wartungsplan eine gewisse Zeit lang in Betrieb bleiben.

Manchmal sind Aktualisierungen nicht möglich, weil einige Geräte in industriellen Steuerungssystemen ihren Lebenszyklus bereits hinter sich haben und die Hersteller keine Updates mehr bereitstellen. Die virtuelle Patching-Technologie kann bestehende Patch-Management-Prozesse ergänzen, indem sie Schwachstellen abschirmt. Virtuelles Patching fungiert als agentenloses Notfall-Sicherheitstool, das Netzwerkadministratoren und -Betreiber nutzen können, um Schwachstellen in betroffenen Geräten schnell zu beheben (Bild 4).

Resümee

Im Hinblick auf die Betriebseffizienz und Verfügbarkeit ist es unabdingbar, Cybersicherheit zu berücksichtigen. Der Gedanke, dass Netzwerke isoliert und sicher sind, wurde durch mehrere Cybersecurity-Zwischenfälle in Produktionsanlagen widerlegt.

Um die Netzwerksicherheit zu verbessern, können zwei verschiedene Wege beschritten werden. Zum einen kann man sicherstellen, dass die Industrienetzwerke über eine sichere Grundlage verfügen - eine sichere Netzwerkinfrastruktur, die den autorisierten Datenverkehr an die richtigen Stellen weiterleitet. Alternativ dazu kann man kritische Anlagen identifizieren und sie mit einem mehrschichtigen, proaktiven Schutz ausstatten, z. B. mit einem industriellen IPS und der Whitelisting-Kontrolle. ◄