Cybersicherheit: Neue Herausforderungen, neue Bedürfnisse

Kritische Infrastrukturen sind ebenso wie andere Anlagen in der OT-Branche (Betriebstechnologie) anfällig für Malware und andere IT-Sicherheitsrisiken. Wie der Stuxnet-Wurm, der auf die SCADA- und SPS-Systeme eines großen Atomprogramms im Nahen Osten abzielte, zeigt, ist keine Anlage vor Angriffen oder Ausfällen durch Cyberbedrohungen gefeit.

Wenn kritische Infrastrukturen betroffen sind, steht sogar noch mehr auf dem Spiel, bis hin zur nationalen Sicherheit. Aus diesem Grund muss die Netzwerksicherheit im OT-Bereich und die betriebliche Sicherheit heute immer einen Schritt voraus sein, um kritische Infrastrukturen vor neuen und sich ständig weiterentwickelnden Bedrohungen zu schützen.

In den letzten Jahren hat nicht nur die Zahl der Malware-Angriffe und anderer Sicherheitsvorfälle zugenommen, sondern die Cyberbedrohungen betreffen auch immer mehr verschiedene Industriesektoren, darunter wichtige Infrastrukturen wie die Energie-, Wasser- und Gesundheitsindustrie. Eine weitere besorgniserregende Beobachtung ist, dass die gleichen Arten von Cyberangriffen in verschiedenen Branchen eingesetzt werden. Daher müssen die heutigen OT-Cybersicherheitslösungen vielseitig sein und den Sicherheitsanforderungen verschiedener Branchen gerecht werden.

Warum die ideale OT-Cybersicherheitsplattform flexibel sein muss

Da die branchenspezifischen OT-Bereiche komplexe und stark angepasste Konfigurationen an verschiedenen Kontrollpunkten und Geräten erfordern, ist die Sicherheit anfällig für menschliches Versagen, was zu Schwachstellen führen kann die leicht übersehen werden. Um diese Verwundbarkeit zu beheben, ermöglicht eine zentrale Netzwerkmanagement-Plattform eine einfachere Bereitstellung und Flexibilität bei der Übertragung von Befugnissen. Bestimmten Zonen oder Funktionen können unterschiedliche Verwaltungsberechtigungen zugewiesen werden, wodurch mögliche menschliche Fehler reduziert werden. Die zentrale Kontrollplattform bietet auch einen besseren Zugang zu Daten über den Netzwerkverkehr für Analysen.

IPS-Cybersicherheitsplattform

Warum ist eine IPS-Cybersicherheitsplattform ein integraler Bestandteil einer ganzheitlichen OT-Netzwerkverteidigungslösung? OT-Experten sind sich einig, dass die Anwendung von Sicherheits-Patches wichtig ist. Viele ältere Software und Geräte unterstützen jedoch keine neuen Patches, was bei OT-Anwendungen schnell zu einer Gefahr für die Cybersicherheit werden kann. In der Tat ist es nicht einfach, Geräte im industriellen Bereich zu aktualisieren. Diese Schwachstellen können mit industriellen Intrusion Prevention Systemen (IPS) behoben werden (Bild 1).

Virtuelles Patching

IPS sind in der Lage, virtuelles Patching durchzuführen, um anfällige Anlagen zu schützen, und überwachen die Netzwerkumgebung, schützen OT-Geräte und liefern Sicherheits-Patches rechtzeitig, ohne den Betrieb zu unterbrechen (Bild 2).

Proaktiv handeln

IPS kann proaktiv verdächtige Aktivitäten und bekannte Angriffsmuster im Netzwerkverkehr erkennen (Bild 3). Sobald eine böswillige Aktivität erkannt wird, verwirft das IPS das Paket und blockiert den Datenverkehr von der IP-Adresse des Angreifers, während der legitime Datenverkehr weiterhin durchgelassen wird. Die Erkennung in Echtzeit stoppt externe Angriffe, bevor sie anfällige Systeme wie SCADA-Systeme oder SPS erreichen können. Eine IPS-Cybersicherheitsplattform wurde speziell für die besonderen Anforderungen von OT-Systemen entwickelt und bietet robuste und zuverlässige Funktionen, die die Fehlersuche und die Bedenken bei der Bereitstellung und Aufrechterhaltung eines ganzheitlichen Schutzes gegen Cyberbedrohungen beseitigen. ◄

übersetzt von
Marianne Ruskowski
systerra computer Systeme
www.systerra.de

Moxa Inc.
www.moxa-europe.com

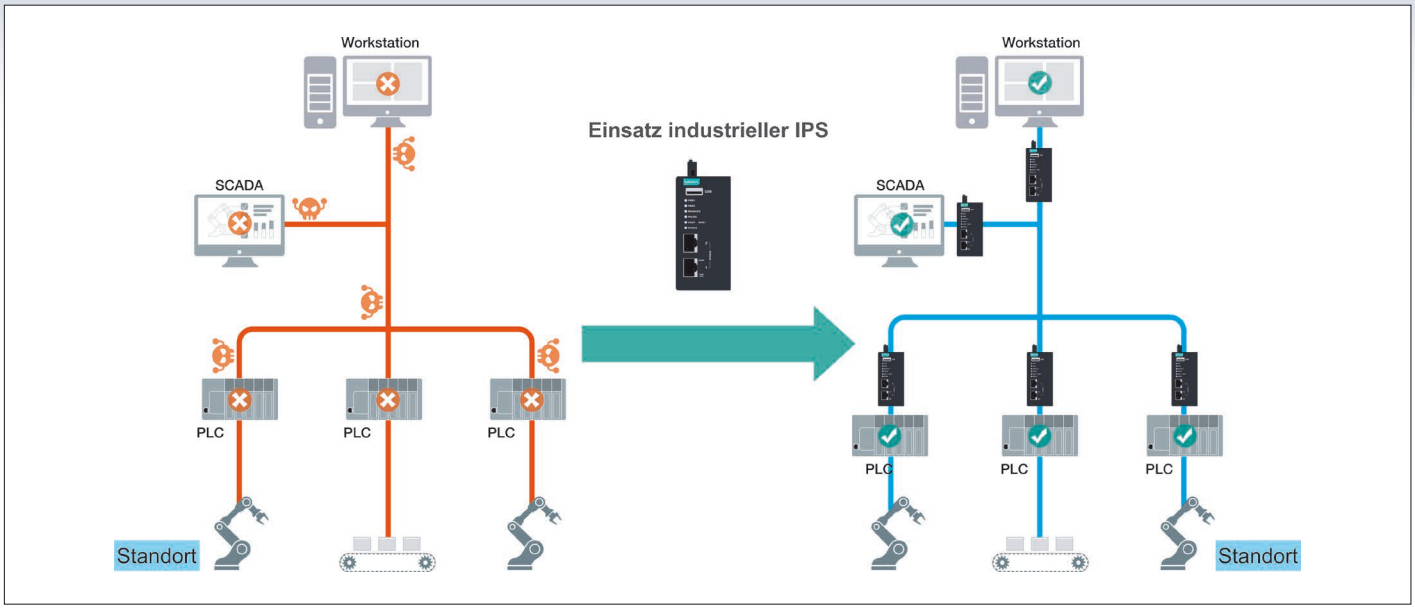

Bild 1: Industrielles IPS sichert den Datenverkehr in industriellen Netzwerken

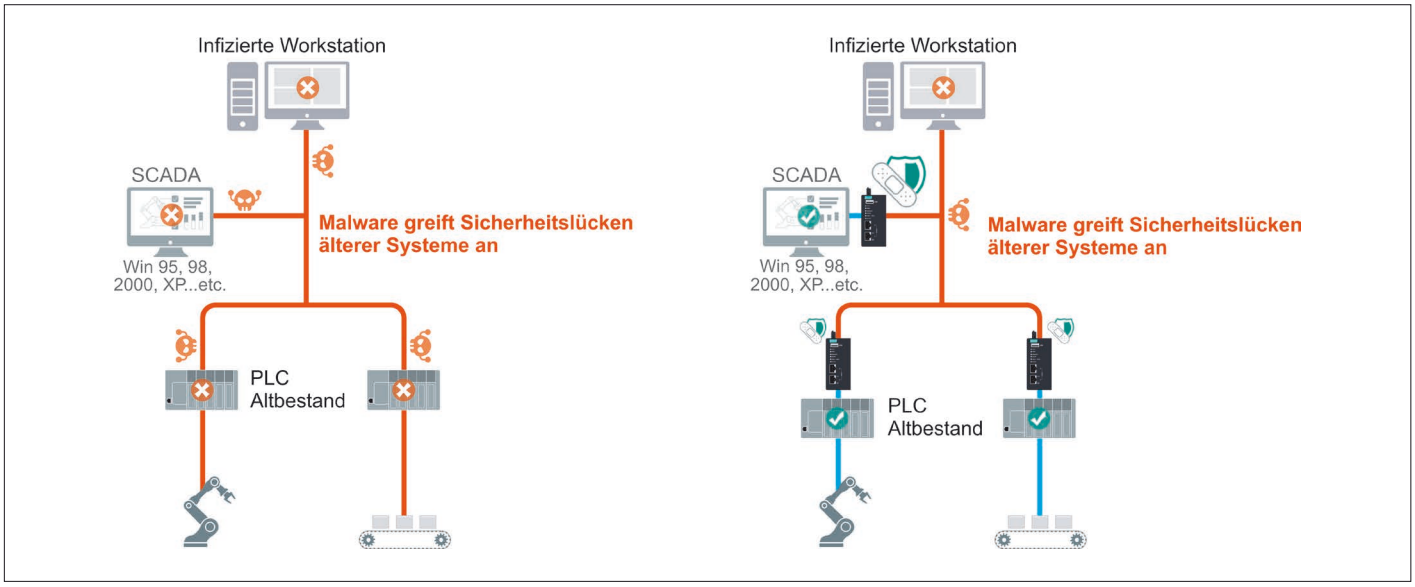

Bild 2: Virtuelles Patching über IPS verhindert die Ausbreitung von Malware. Links: Zustand ohne IPS

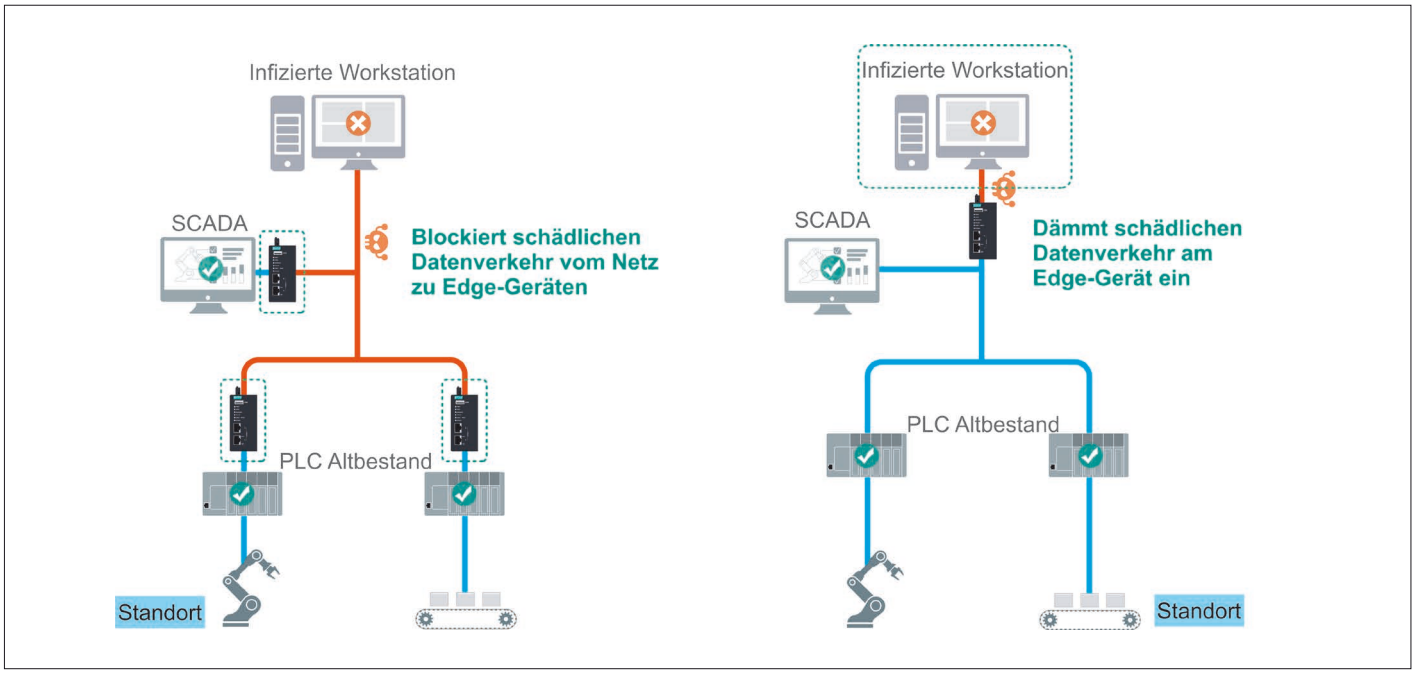

Bild 3: Ein Industrielles IPS blockiert den schädlichen Datenverkehr vom Netzwerk zu Edge-Geräten © Text und Bilder liegt bei Moxa Inc.