

PRODUKTION

» SICHERHEIT IN PRODUKTIONSNETZWERKEN

In modernen Produktionsanlagen ist der Shopfloor häufig direkt mit einem ERP-System verbunden, um etwa die Produktionsplanung zu optimieren. Die Schnittstellen zu den verschiedenen Maschinen und Systemen beinhalten oft unbekannte Angriffsvektoren. Die Angriffe durch Stuxnet und dessen Nachfolger Duqu haben diese Verwundbarkeit offengelegt.

» INDUSTRIE 4.0 UND LEGACY MACHINES

Die digitale Transformation, bekannt als Industrie 4.0, ermöglicht Echtzeitüberwachung von Maschinendaten zur Optimierung von Fertigungsprozessen und Produktionsplanung. Allerdings befinden sich durch lange Lebenszyklen plötzlich Produktionsmaschinen im Netzwerk, die ursprünglich nicht dafür konzipiert waren. Dadurch ergeben sich potenzielle Einfallstore für Angreifer, die durch Spionage, Sabotage oder Ransomware-Angriffe schwerwiegende finanzielle und betriebliche Schäden verursachen können.

» WEITERE HERAUSFORDERUNGEN

- » Komplexe Systemlandschaft: Fördertechnik, Produktionsmaschinen, Roboter und SPS können oft nicht mit herkömmlichen Sicherheitsmaßnahmen geschützt werden.
- » Externe Wartung: Wartungsarbeiten durch externe Dienstleister, die Zugang zum IT-Netzwerk benötigen, erhöhen das Risiko von Sicherheitsvorfällen.
- » Regulatorische Anforderungen: Neue EU-Verordnungen wie die EU-Maschinenverordnung, die NIS2-Richtlinie oder der Cyber Resilience Act (CRA) erfordern verstärkte Sicherheitsmaßnahmen in Produktionsnetzwerken.
- » Standards & Zertifizierungen: Unternehmen sind zudem gefordert, Zertifizierungen wie ISO 27001, BSI-Grundschutz sowie COBIT/ITIL und branchenspezifische Standards wie TISAX zu erfüllen.

» EIN DURCHGÄNGIGES SICHERHEITSKONZEPT

ARP-GUARD ist eine umfassende IT-Sicherheitslösung, die alle Netzwerkgeräte eindeutig identifiziert und kontinuierlich überwacht. Fremdgeräte werden isoliert, um unbefugten Zugriff zu verhindern, und durch integriertes VLAN-Management wird das Netzwerk in logische Subnetze unterteilt, die durch präzise Richtlinien geschützt werden. Die frei skalierbare Systemarchitektur ermöglicht eine standortübergreifende Netzwerksicherheit ohne Infrastrukturänderungen mit umfassenden Funktionen für das Sicherheits- und Netzwerkmanagement.

Ungewollte Datenabflüsse und Produktionsunterbrechungen werden unterbunden, indem nur autorisierte Geräte mit rollenbasierten Zugriffsrechten zugelassen werden. So können beispielsweise Gastzugänge für Wartungstechniker nur für ausgewählte Maschinen eingerichtet werden, während die integrierte Firewall andere Zugriffe blockiert.

ARP-GUARD liefert Echtzeit-Netzwerkdaten, unterstützt das Asset-Management mit grafischen Netzwerktopologien und erleichtert die Einhaltung zahlreicher Zertifizierungen, insbesondere für kritische Infrastrukturen.

KUNDENSTIMMEN

KURTZ HOLDING GMBH & CO. BETEILIGUNGS KG - KREUZWERTHEIM

„Wenn Industriespione Zugriff auf die Daten unserer Entwicklung bekämen, wäre das für uns existenzbedrohend“, erläutert Tom Eiermann, Team Leader IT-Administration, Corporate Information and Organisation (CIO) in der Kurtz Holding.

„Daher haben wir uns entschieden, unser Netz gezielt gegen alle Arten unautorisierter Zugriffe zu schützen - proaktiv, bevor das Kind sprichwörtlich in den Brunnen fällt.“