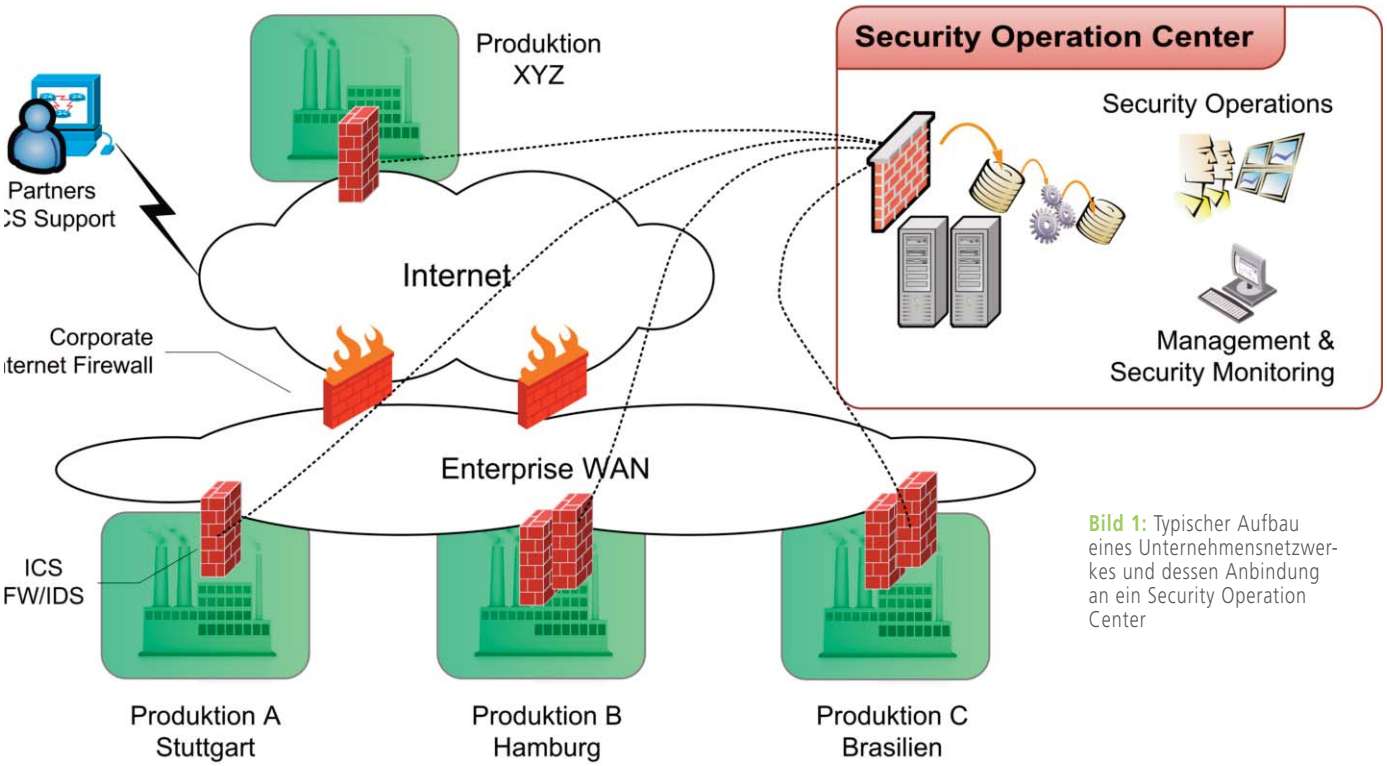

Bild: Verizon Deutschland GmbH

Bild 1: Typischer Aufbau eines Unternehmensnetzwerkes und dessen Anbindung an ein Security Operation Center

Mehr Sicherheit für die Industrie

Praxisbericht: Industrielle Sicherheit aus der Sicht eines Managed-Security-Service-Providers

Die zunehmende Konvergenz von Informationstechnologie und Automatisierungstechnik bzw. Prozesstechnik resultiert in einer veränderten Bedrohungslage, wodurch der Schutz von Produktionsanlangen und kritischen Infrastrukturen vor Cyber-Angriffen an Bedeutung gewinnt. Diese Entwicklung nimmt auch auf traditionelle Security-Service-Provider Einfluss.

Industrielle Anlagen besitzen eine Laufzeit von mehreren Jahrzehnten und wurden in der Vergangenheit, abgesehen von Betriebs- und Ausfallsicherheit, ohne Betrachtung weiterer Sicherheitsaspekte entwickelt. Die nachgelagerte Integration von Patch-Management, Zugriffs- und Berechtigungsmanagement oder Anti-Viren-Schutz stellt die Anlagenbetreiber vor eine oftmals nicht überwindbare Hürde. Darüber hinaus entstehen durch die globale Vernetzung von IT- und ICS-Umgebungen (Industrial Control Systems) neue Angriffsvektoren. Zur Reduzierung der Bedrohungslage empfiehlt Verizon ein abgewogenes Vorgehen unter Einbeziehung von Machbarkeitsaspekten, Zielsicherheitsniveau und einer messbaren Reduktion von Geschäftsrisiken. Bestehende Prozesssteuerungssysteme bleiben abhängig vom geforderten Sicherheitsniveau in vielen Fällen unverändert. Dagegen erfolgt eine systematische Analyse von Kommunikationsverbindungen, Netzwerksegmentierung und Echtzeitüberwachung des Sicherheitszustands basierend auf Best Practices und Industriestandards aus IT und ICS. Erfahrungsgemäß führen folgende Maßnahmen zu einem enormen Sicherheitszuwachs bei einem verhältnismäßig geringen Änderungsbedarf in bestehenden ICS-Umgebungen:

- Definition von Sicherheitszonen und Segmentierung von Netzwerken durch Sicherheitskomponenten
- Prozessabhängige Definition von Richtlinien und Whitelists für Kommunikationsverbindungen
- Absicherung und Echtzeitüberwachung der Segmentierung, Kommunikationsverbindungen und Remote- bzw. Wartungszugriffe (Betriebs- und Ausfallsicherheit, Authentifizierung, Verschlüsselung, Integrität)
- Erkennen von Richtlinienverstößen, Anomalien und Schadsoftware an Perimetern und zwischen den Zonen
- Definition von Verantwortlichkeiten und Etablierung eines Incident Response Prozesses

Bild 2 zeigt ein Segmentierungsbeispiel und die Anbindung eines Security Operation Centers (SOC) zur sicherheitstechnischen Überwachung interner und externer Kommunikationsverbindungen. Die Realisierung der Segmentierung erfolgt mit redundanten Firewalls und logischen Netzwerken (VLAN, Virtual Local Area Network). Logische Netzwerke trennen physikalische Netze in Teilnetze und ermöglichen eine kosteneffiziente Produktionsnetzsegmentierung. Kommunikationsverbindungen zwischen den Teilnetzen werden durch Firewalls limitiert und überwacht. Dieses Konzept ermöglicht beispielsweise von Viren befallene Komponenten oder Segmente zu isolieren und eine weitere Ausbreitung zu unterbinden. Die Absicherung von Fernwartungszugängen und externer Maschinenkommunikation erfolgt typischerweise mit VPN (Virtual Private Network), wodurch eine starke Authentifizierung und Verschlüsselung ermöglicht wird – auch wenn die ICS-Komponenten zunächst keine VPN-Funktionalität unterstützen. Externer Zugriff wird ausschließlich auf vorher definierte Komponenten und Segmente erlaubt. In Umgebungen mit hohen Sicherheitsanforderungen werden externe Verbindungen über eine sogenannte Jump Zone in der ICS-DMZ (Demilitarized Zone) geleitet. Die Kommunikation und der Datenaustausch zwischen ICS-Produktionssegmenten und dem Büronetz geschehen nur über eine dedizierte Information Zone. Dies ermöglicht eine granulare Kontrolle und Überwachung von Zugriffen und Maschinenkommunikation (siehe IEC62443, Zones, Conduits and Security Assurance Level).

Weitere Maßnahmen erhöhen die Sicherheit

Auf Basis der Segmentierung und Absicherung externer Verbindungen kann durch die Integration zusätzlicher Sicherheitstechnologien das Sicherheitsniveau weiter erhöht werden. Nachfolgende Technologievorschläge befinden sich nicht auf den ICS-Komponenten, sondern werden abhängig von Verfügbarkeitsanforderungen im aktiven oder passiven Modus integriert:

- Intrusion Detection Systems (IDS) zur Erkennung von Angriffen und Anomalien
- Anti-Viren-Schutz (AV) zur Erkennung von Schadsoftware
- Applikationssicherheit (AS) und URL-Filter zur Absicherung von Kommunikationsverbindungen auf Anwendungsebene

Der Betrieb und das Überwachen der Sicherheitstechnologien erfolgen im SOC. Zu den typischen Dienstleistungen eines SOC gehören Gerätemanagement, proaktive Analyse, Erkennen von Angriffen bzw. Zwischenfällen (Incidents) und Berichterstattung. Das SOC von Verizon arbeitet nach dem Drei-Schichten-Modell (Bild 3):

- Schicht 1: Produktionsstätten (Produktion A, B, C) beinhalten die zu betreibenden und überwachenden Firewalls, VPN-Gateways und weitere Sicherheitskomponenten (IDS, AV, AS, URL etc.).
- Schicht 2: Log-Daten werden über eine verschlüsselte Verbindung an das Security Management Center (SMC) übertragen, korreliert und analysiert.
- Schicht 3: Im SOC werden Angriffe und Incidents erkannt, überprüft und analysiert und bei Gefahr eskaliert. Aus Redundanzgründen betreibt Verizon drei SOC in verschiedenen Regionen (Deutschland, Australien, Nordamerika) im Schichtbetrieb (24h*7).

Personal und Wissen als Herausforderung

Die Umsetzung der beschriebenen Maßnahmen stellt in Hinblick auf Machbarkeit eine weniger große Hürde

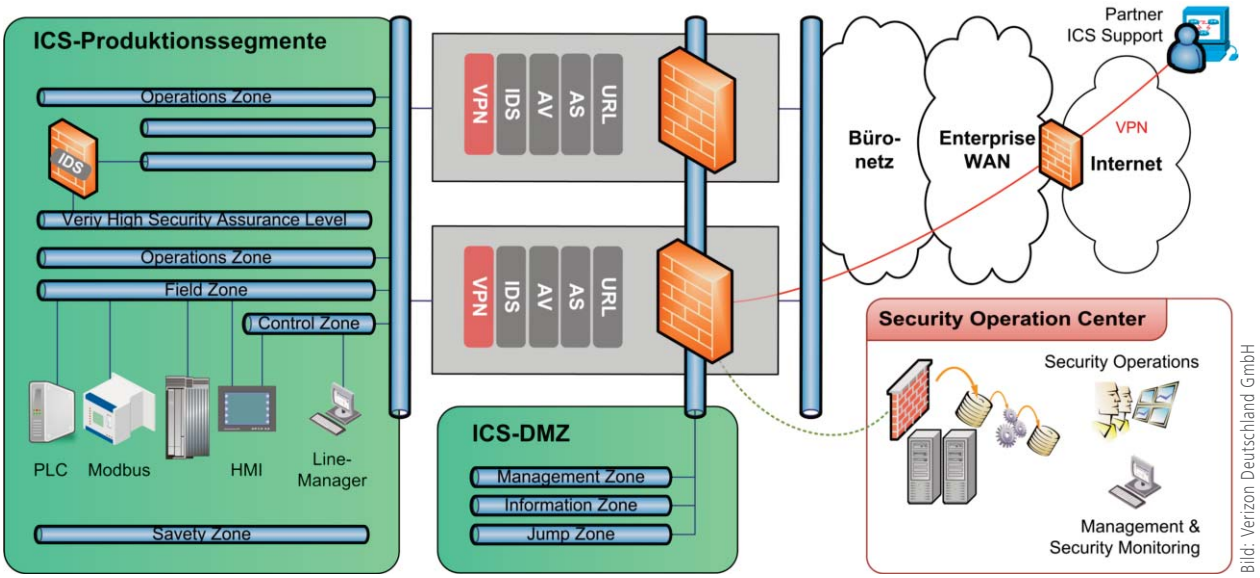

Bild 2: Segmentierung und Security Operation Center

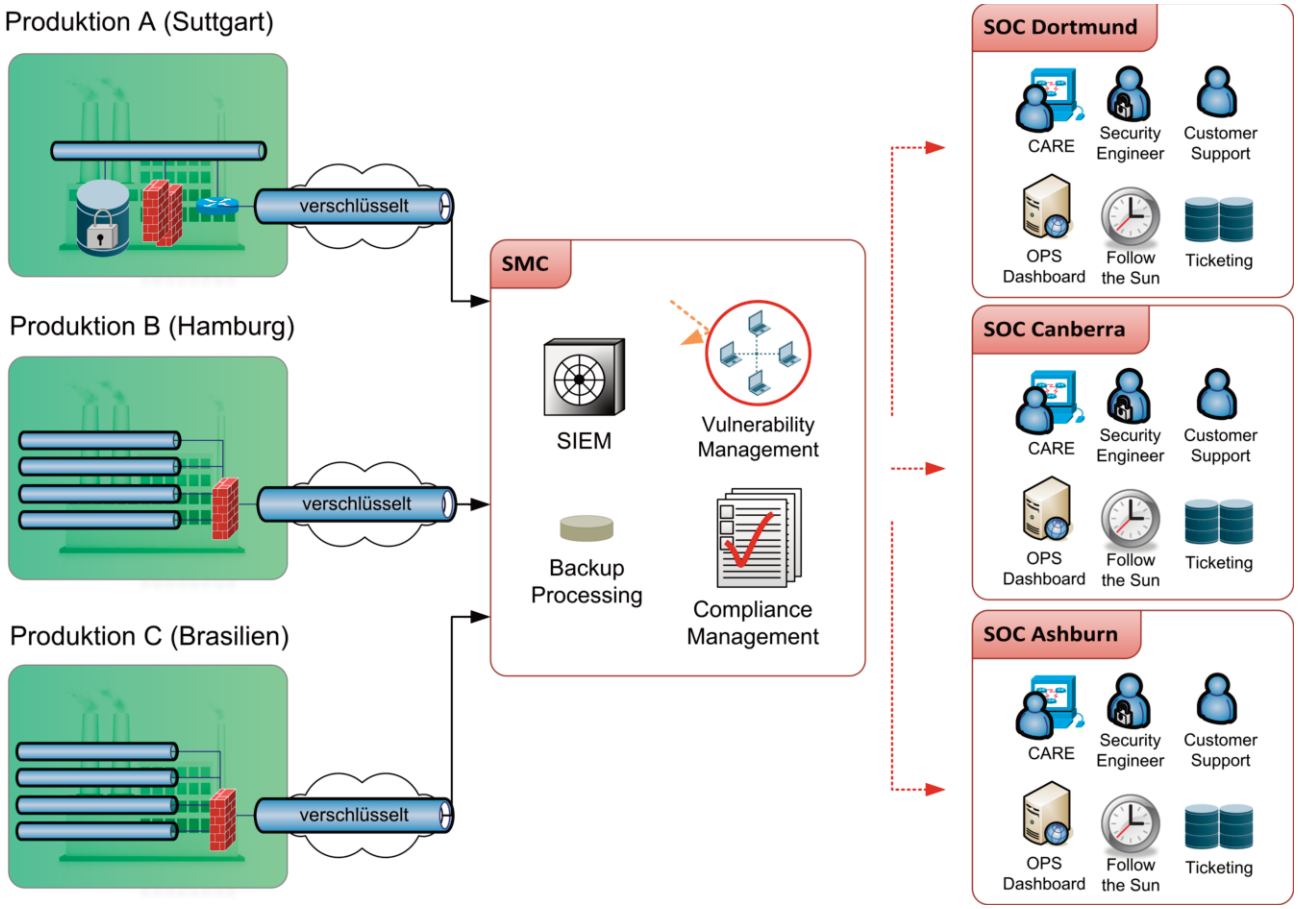

Bild: Verizon Deutschland GmbH

Bild 3: Aufbau eines MSSP – Betrieb und Überwachen der Infrastruktur

dar. Die Herausforderung für Unternehmen besteht jedoch darin, geeignetes Personal und Wissen aufzubauen. Diese Lücke schließt ein Managed Security Service Provider (MSSP) hinsichtlich Analyse, Design, Integration, Betrieb und sicherheitstechnischer Überwachung. Bei der Auswahl eines MSSPs sollte neben dem kontinuierlichen Betrieb eines SOC und der Verfügbarkeit an allen Unternehmensstandorten vor allem auf die Fähigkeiten der Erkennung von ICS-spezifischen Bedrohungen geachtet werden. Zur Priorisierung von Incidents wären Möglichkeiten zur Verknüpfung der Eintrittswahrscheinlichkeit mit der Schadenshöhe und zur Ableitung eines potenziell resultierenden Geschäftsrisikos ein weiteres wichtiges Auswahlkriterium.

Reduzierung des Sicherheitsrisikos

Die in diesem Praxisbericht aufgeführten Sicherheitsaspekte sind keineswegs vollständig. Die Wichtigkeit organisatorischer Maßnahmen zur Anlagensicherheit, wie z.B. physischer Zugangsschutz oder der Umgang mit externen Speichermedien bei Mitarbeitern und Partnern, muss an dieser Stelle nicht erläutert werden. Mittelfristig wird auch im Bereich industrieller Sicherheit ein Defense-in-Depth-Vorgehen Anwendung finden und auf allen Ebenen zusätzliche Maßnahmen wie Patch-Management, Anti-Viren-Schutz etc. berücksichtigt werden. Unter Einbezug der Machbarkeit ermöglicht der in diesem Bericht vorgestellte Ansatz zur Netzwerksegmentierung und sicherheitstechnischen Überwachung eine deutliche Reduzierung des Sicherheitsrisikos für derzeit im Betrieb befindliche Anlagen. Diesen Ansatz kann bei Personal- und Wissensmangel ein MSSP mit Expertenwissen und kontinuierlicher Sicherheitsüberwachung unterstützen. ■

www.verizonenterprise.com/de

Autor: Wolfgang Kiener, Security Solutions Architect, Verizon Deutschland GmbH, München