SIEMENS

Fachartikel

Industrielle Kommunikation

IT-Sicherheit von Automatisierungssystemen

Abgestufter Schutz bis in die Anlagenstruktur

IT Security in der Automatisierung ist für unseren Industriestandort eminent wichtig, weil die benötigten Automatisierungs- und Prozessleitsysteme in nahezu allen Industriebereichen eingesetzt werden: von der Energieerzeugung und -verteilung über die Wasserversorgung bis hin zur Produktion, Verkehrsleittechnik und zum Gebäudemanagement. Um zudem Menschen und Anlagen zu schützen, sind anlagenspezifische Maßnahmen erforderlich. Hilfe bietet ein abgestuftes Schutz-Angebot, das tief in die spezielle Anlagenstruktur reicht.

Insbesondere aufgrund der zunehmenden Vernetzung von Ethernet-Verbindungen bis in die Feldebene hinein gewinnen in der Industrie auch die damit verbundenen Sicherheitsfragen an Bedeutung. Denn offene Kommunikation und zunehmende Vernetzung von Produktionssystemen bergen nicht nur enorme Chancen, sondern ebenso große Risiken deren jeweiliges Schadenspotenzial für diese vernetzten Systeme ermittelt werden muss.

Die Zeit von abgeschotteten Automatisierungssystemen, basierend auf proprietären Protokollen und ohne Möglichkeiten, von außen zugreifen zu können, ist nicht mehr gegeben. Eine Anbindung von Automatisierungssystemen an das Internet oder an vorhandene Office-Netzwerke ist heutzutage Standard, wobei allerdings sehr unterschiedliche Anforderungen an die Automatisierungsnetzwerke exitieren:

Unterschiedliche Anforderungen an Automatisierungsnetzwerke

Im aktuellen „ICS Security Kompendium" des Bundesamts für Sicherheit in der Informationstechnik (BSI) werden die verschiedenen Anforderungen an klassische IT-Netze und Automatisierungsnetze aufgezeigt. Es soll als Grundlagenwerk für das Betreiben von Industrieanlagen bzgl. der Absicherung von Produktion und Prozessanlagen dienen und adressiert alle Energie- und Wasserversorger, Anbieter für Verkehrsleittechnik oder auch Unternehmen der Gebäudemanagement-Branche.

Ein wesentlicher Unterschied ist die Bewertung der Risiken der verschiedenen Systeme. Während bei einem Angriff auf die IT-Infrastruktur „nur" die Datenintegrität und im schlimmsten Fall der Verlust von Geschäftsdaten im Vordergrund stehen, kann ein Hackerangriff auf die Prozesse und Automatisierungswelt zu einer Gefährdung von Menschen führen und die Zerstörung von Produktionskapazitäten bis hin zu unkontrollierbaren Schäden auf die Umwelt zur Folge haben.

Beim Thema Netz-Sicherheit gibt es gravierende Unterschiede:

Kategorie	Klassische Unternehmens-IT	Automatisierung
Performance	• keine garantierten Abarbeitungszeiten • hohe Latenz u. U. akzeptabel	• garantierte Abarbeitungszeiten • Latenz ist zum Teil hart begrenzt
Verfügbarkeit	• Reboot produktiver Systeme nicht ungewöhnlich • Kurzfristig anberaumte Wartungsvorgänge (z. B. Patch) • Wartungsausfälle verursachen geringe Kosten	• Reboot im produktivem Umfeld nicht akzeptabel • Wartungszyklen nur mit langem Vorlauf • Wartungsausfälle verursachen hohe Kosten
Beurteilung von Risiken	• Vertraulichkeit und Integrität von Daten stehen im Vordergrund • Wesentliche Risiken betreffen die nachhaltige Störung von Geschäftsprozessen	• Schutz von Mensch und Umwelt stehen im Vordergrund • Wesentliche Risiken betreffen den unzureichenden Schutz von Menschen und die Zerstörung von Produktionskapazitäten. Auswirkungen auf die Umwelt sind möglich
Systemressourcen / Dediziertheit	• Systeme verfügen über freie Ressourcen, die beispielsweise die Installation von IT-Security-Tools auf dem System erlauben	• Installation von fremden Softwarekomponenten auf den Systemen nicht oder erst nach Freigabe vorgesehen, z. B. Virenschutzprogramme, Programme für Videoanbindung
Lebenszeit der Komponenten	• wenige Jahre	• bis zu 20 oder 25 Jahre

(Quelle: BSI ICS-Security-Kompendium 2013)

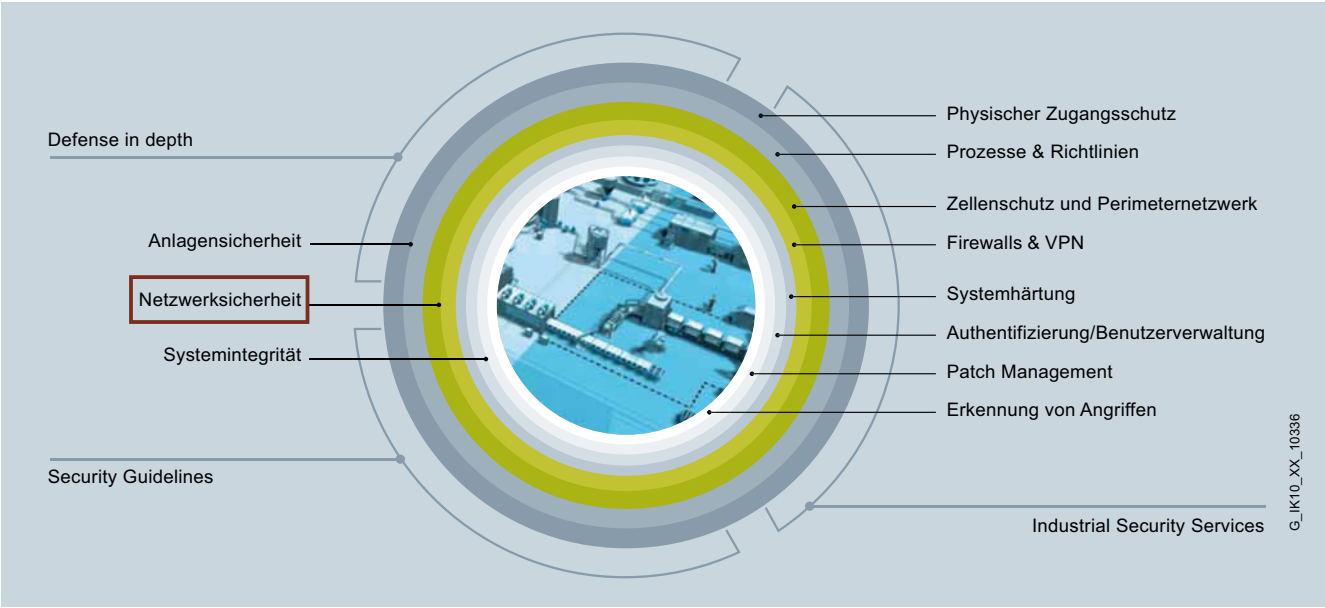

Bild 1: Siemens Industrial Security Strategy: Defense-in-Depth

Um eine Industrieanlage unter dem Aspekt der Sicherheit umfassend vor Angriffen zu schützen, müssen entsprechend gestaffelte und aufeinander abgestimmte Maßnahmen getroffen werden.

Dabei reicht es nicht aus, nur einen einfachen System-Zugangsschutz per Passwort zu implementieren, da Angriffe von außen auf mehreren Ebenen erfolgen können. Für einen umfassenden Schutz industrieller Anlagen hat die Siemens AG beispielsweise ein „Defense-in-Depth"-Konzept entwickelt, das in Bild 1 dargestellt ist.

Rundumschutz, der auch in die Tiefe geht

Mit Defense in Depth bietet Siemens für industrielle Anwender ein vielschichtiges Konzept, das Industrie-Anlagen sowohl insgesamt gegen Angriffe von außen als auch innerhalb in mehreren Ebenen schützt. Das Konzept basiert auf den Komponenten Anlagensicherheit, Netzwerksicherheit sowie Systemintegrität nach den Empfehlungen der ISA 99 / IEC 62443 – dem führenden Standard für Security in der industriellen Automatisierung. Während der klassische Anlagenschutz physische Zugriffe abwehrt, bewahren Netzwerkschutz und Schutz der Systemintegrität vor Cyber-Übergriffen und nicht autorisiertem Zugriff nicht zugelassener Bediener oder betriebsfremder Personen. Der Vorteil ist, dass ein Angreifer erst mehrere Sicherheitsmechanismen überwinden muss und die Sicherheitsanforderungen der einzelnen Schichten anlagenspezifisch berücksichtigt werden können.

Erfolgsfaktor: Netzwerksicherheit

Netzwerksicherheit bedeutet Schutz von Automatisierungsnetzen vor unbefugten (externen wie internen) Zugriffen. Dies beinhaltet die Kontrolle aller Schnittstellen wie z. B. zwischen Büro- und Anlagennetzwerk oder die Kontrolle der Fernwartungszugänge zum Internet und kann mittels Firewalls und gegebenenfalls Aufbau einer DMZ (demilitarisierte Zone = sicherheitstechnisch abgeschirmte Zone) erfolgen. Die DMZ dient zur Bereitstellung von Daten für andere Netze, ohne direkten Zugang zum Automatisierungsnetz zu gewähren. Die sicherheitstechnische Segmentierung des Anlagennetzwerks in einzelne geschützte Automatisierungszellen, dient der Risikominimierung und Erhöhung der Sicherheit. Die Aufteilung der Zellen und Zuordnung der Geräte erfolgt nach den anlagenspezifischen Kommunikations- und Schutzbedürfnissen. Die Datenübertragung zwischen den Zellen wird mittels ausschließlicher Verbindung über VPN (Virtual Private Network) hergestellt und zusätzlich verschlüsselt und so vor Datenspionage und Manipulation geschützt. Die Kommunikationsteilnehmer werden sicher authentifiziert. Mit den erwähnten „Security Integrated"-Komponenten des Anbieters Siemens (wie beispielsweise den SCALANCE S Security Modules oder Security CPs für SIMATIC-Steuerungen) kann ein Zellenschutzkonzept aufwandsarm realisiert und die Kommunikation gesichert werden.

Komponenten für die Netzwerksicherheit

Bei der Realisierung solcher Schutzkonzepte haben sich zwei Sicherheitsmittel bewährt: die Firewall und der VPN-Tunnel.

Die Firewall wird eingesetzt, um den Datenverkehr inhaltlich zu schützen. Dabei können durch Filterung verdächtige/unzulässige Pakete verworfen und ggf. Netzzugänge Paket-abhängig gesperrt bzw. wieder gewährt werden. Zur Sicherung der physikalischen Kommunikation wird am häufigsten das Tunnelling-Verfahren eingesetzt (Bild 2).

Die Firewall und VPN-Funktionen werden von den „Security Integrated"-Produkten (rotes Schloss-Symbol) unterstützt und bieten somit dem Anwender Schutz bis in jede Automatisierungszelle.

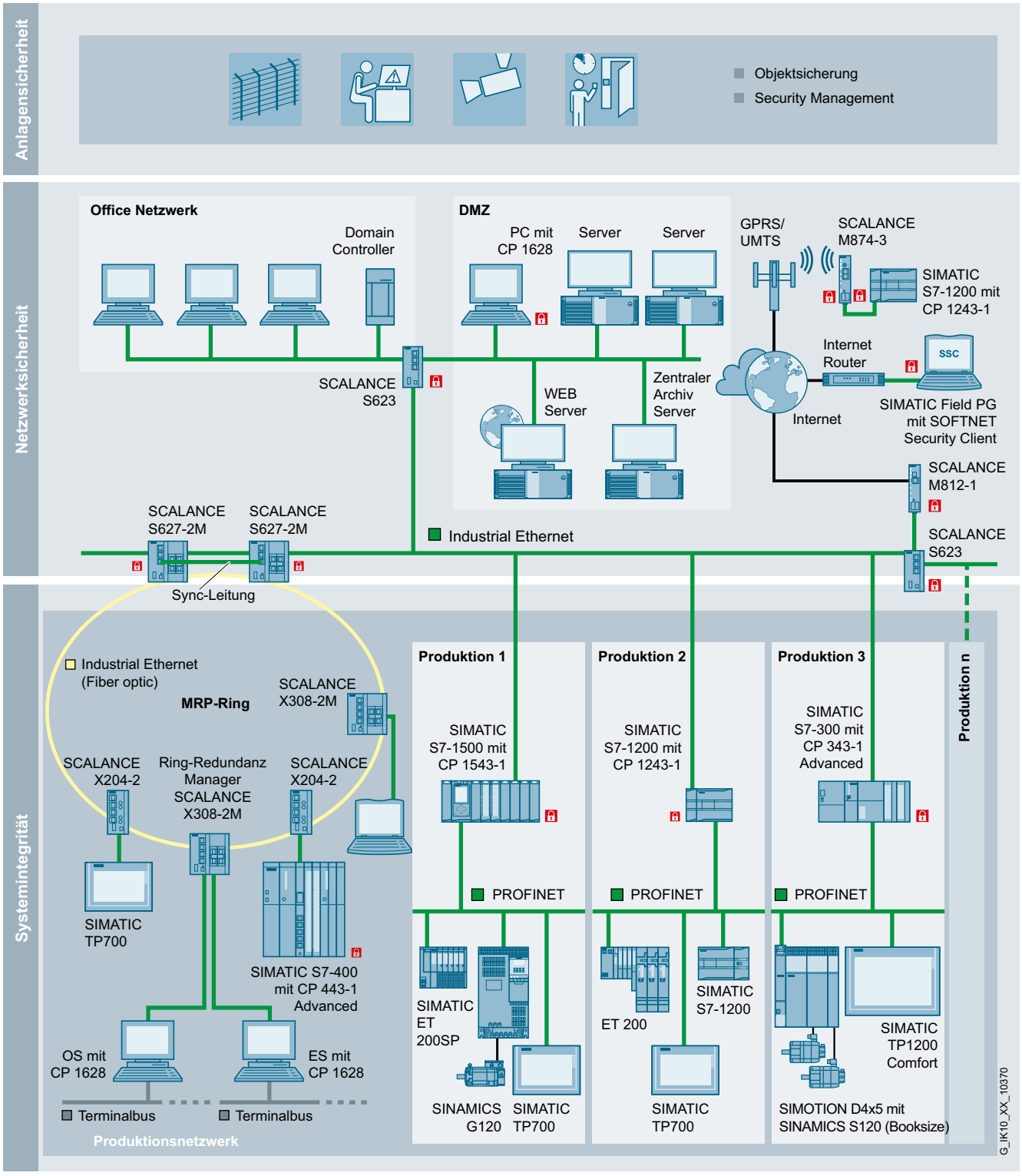

Bild 2: Sichere Kommunikation, Netzzugangsschutz und Netzsegmentierung mit Security-Integrated-Produkten (Siemens-Anlagenbild)

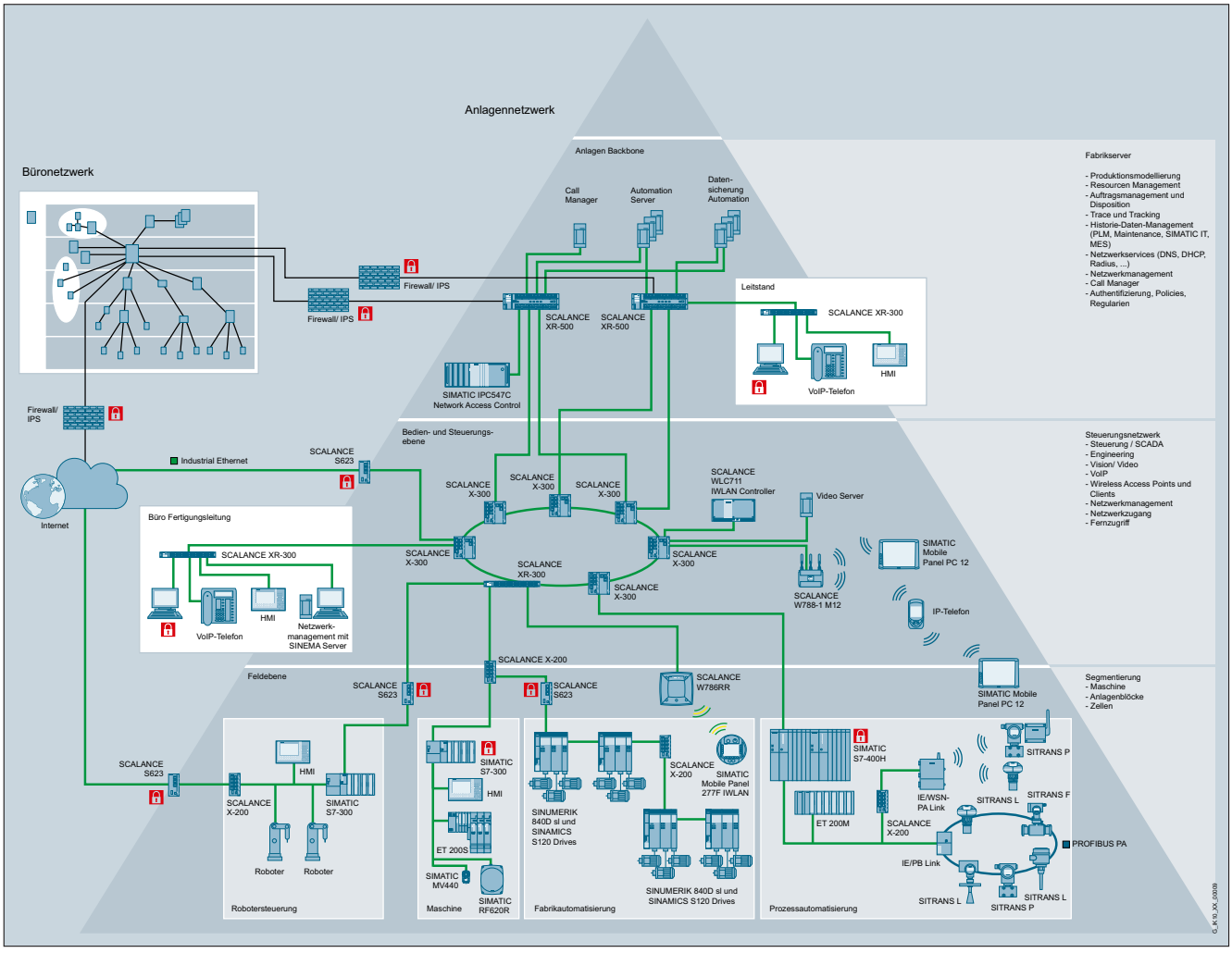

Bild 3: Sichere industrielle Kommunikation, aufgebaut mit SIMATIC NET-Komponenten (Siemens-Anlagenbild)

Auswahl an verschiedenen Security-Produkten für anwendungsspezifische Anlagensicherheit

Um möglichst allen Anlagenbetreibern einen aufwandsarmen Aufbau sicherer Netze zu ermöglichen, bietet Siemens ein breites Spektrum an „Security Integrated"-Produkten an. Dabei wird unterschieden zwischen „Stand Alone"-Baugruppen wie DSL-Modems//Routern oder Mobilfunk-Routern und den Kommunikationsprozessoren, welche die Security-Funktionalität direkt in die Controller-Welt integrieren (Bild 3).

Gekennzeichnet werden diese Produkte mit dem typischen roten Vorhängeschloss. Die Security-Integrated-Produkte sind für den rauen industriellen Einsatz ausgelegt und bieten einen bewährten Schutz für Produktionsanlagen.

Zusätzlich zum Security-Produktangebot unterstützt Siemens die Anwender bei der Umsetzung des „Defense in Depth"-Konzepts durch Plant Security Services. Das Service-Angebot umfasst die in Bild 4 dargestellten Elemente.

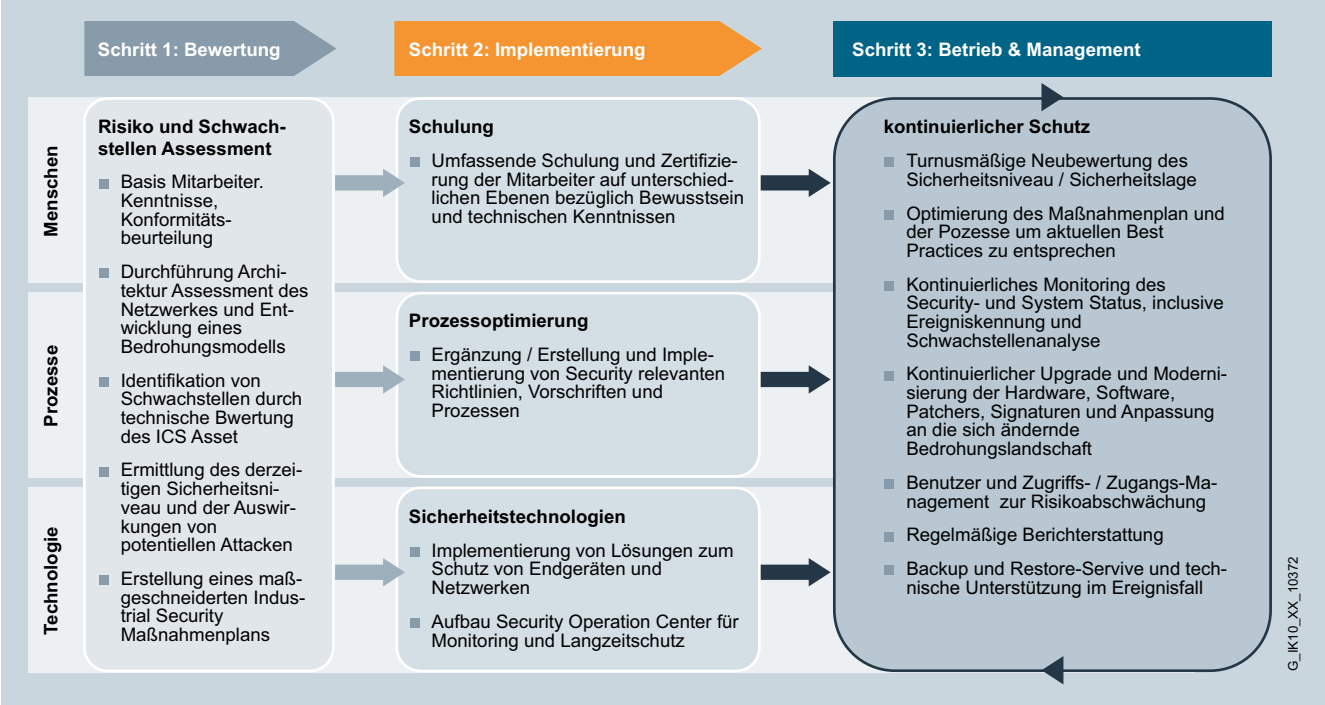

Bild 4: Schritte zur sicheren Kommunikation in industriellen Anlagen

Security ist ein kontinuierlicher Prozess

Industrial Security ist aber nicht nur ein rein technisches Thema, sondern muss bereits im Bewusstsein aller Ebenen des Managements und der Mitarbeiter verankert sein. Security ist dabei ein kontinuierlicher Prozess, der „zu jeder Zeit" berücksichtigt werden muss. Man muss dabei beachten, dass die Anforderungen der klassischen „Office-IT" sich von denen der „Automatisierungs-IT" unterscheiden und es deshalb darauf ankommt, auf bewährte Security-Produkte für die Automatisierungswelt zu setzen. Im Idealfall integrieren die Komponenten-Hersteller die benötigten/notwendigen Sicherheitsfunktionen direkt als Standard in ihr Automatisierungsproduktspektrum.

Auszug aus dem Security Integrated Portfolio der Siemens AG:

- Mobilfunk-Router SCALANCE M874/M875 und DSL-Router SCALANCE M812
- Security-Module SCALANCE S
- Die Software 'Softnet Security Client'
- Kommunikationsbaugruppen CP1628, CP 343-1 Advanced, CP 443-1 Advanced und (neu) CP1543-1 für die High-End-Steuerung SIMATIC S7-1500

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Änderungen vorbehalten
PDF
Technischer Fachartikel
FAV-634-2014
DR.PN.PA15.XXXX.95.11
Produced in Germany

www.siemens.de/industrialsecurity