Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrusT, bevh und BISG

Berlin, 29.11.2016

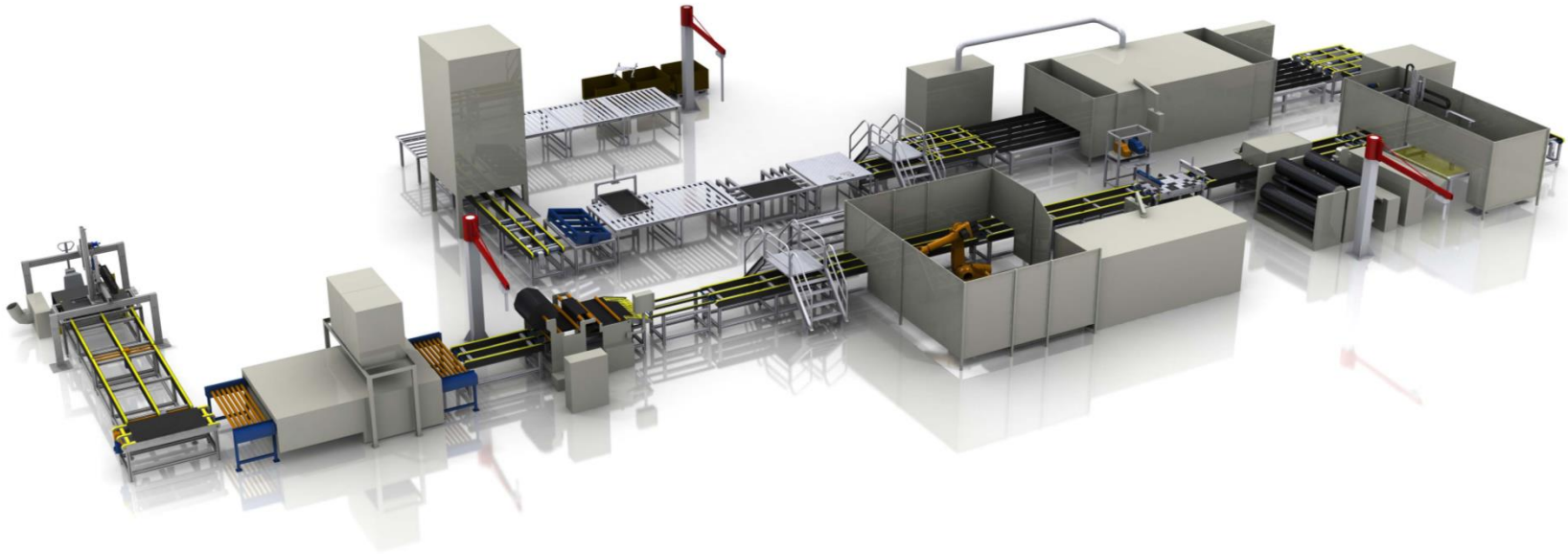
Auswirkungen des ITSiG auf industrielle Sicherheit - technische Anforderungen und Umsetzungen

Thorsten Vogel

PHOENIX CONTACT Cyber Security AG

Anforderungen der Betreiber an IT-Sicherheit

- Gefährdungspotentiale für Mensch und Umwelt
- Anlagenverfügbarkeit 24*7
- Hohe Anforderungen an Produktqualität
- Zuverlässige integrierte Produktion mit globalen Lieferketten
- Robustheit der physikalischen Prozesse



Mögliche Schadensfolgen

- Verlust der Verfügbarkeit des ICS
- Betriebsunterbrechungen und Anlagen-/Produktionsstillstände
- Datenabfluss / Verlust von Know-how (Intellectual Property)
- Herbeiführen von physischen Schäden an Anlagen
- Auslösen von Safety-Prozeduren oder Beeinträchtigung von Safety-Systemen
- Personen-, Umwelt- und Imageschäden
- Minderung der Qualität der Erzeugnisse und hohe Ausschussquoten
- Schadensersatzforderungen von Kunden

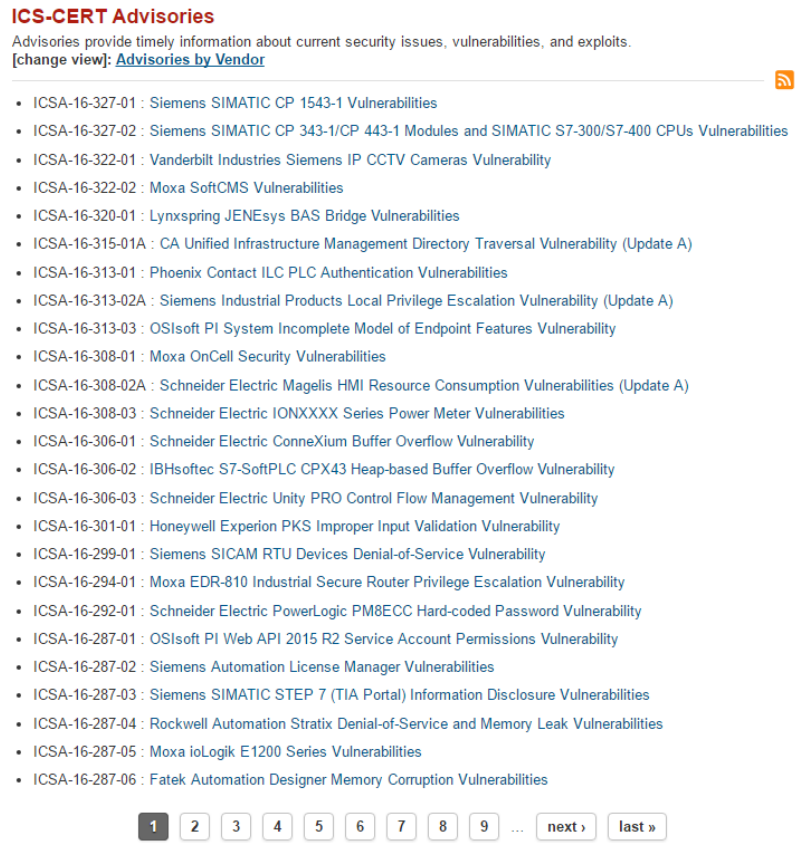
ICS-Cert

The Industrial Control Systems Cyber Emergency Response Team

https://ics-cert.us-cert.gov/advisories

https://ics-cert.us-cert.gov/alerts

- Mehr als 700 Hinweise auf Sicherheitslücken in ICS Automatisierungskomponenten
- 101 Sicherheitslücken in Siemens Komponenten



ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.
[change view]: Advisories by Vendor

- ICSA-16-327-01 : Siemens SIMATIC CP 1543-1 Vulnerabilities
- ICSA-16-327-02 : Siemens SIMATIC CP 343-1/CP 443-1 Modules and SIMATIC S7-300/S7-400 CPUs Vulnerabilities
- ICSA-16-322-01 : Vanderbilt Industries Siemens IP CCTV Cameras Vulnerability
- ICSA-16-322-02 : Moxa SoftCMS Vulnerabilities
- ICSA-16-320-01 : Lynxspring JENEsys BAS Bridge Vulnerabilities
- ICSA-16-315-01A : CA Unified Infrastructure Management Directory Traversal Vulnerability (Update A)
- ICSA-16-313-01 : Phoenix Contact ILC PLC Authentication Vulnerabilities
- ICSA-16-313-02A : Siemens Industrial Products Local Privilege Escalation Vulnerability (Update A)
- ICSA-16-313-03 : OSIsoft PI System Incomplete Model of Endpoint Features Vulnerability
- ICSA-16-308-01 : Moxa OnCell Security Vulnerabilities
- ICSA-16-308-02A : Schneider Electric Magelis HMI Resource Consumption Vulnerabilities (Update A)
- ICSA-16-308-03 : Schneider Electric IONXXXX Series Power Meter Vulnerabilities
- ICSA-16-306-01 : Schneider Electric ConneXium Buffer Overflow Vulnerability
- ICSA-16-306-02 : IBHsoftec S7-SoftPLC CPX43 Heap-based Buffer Overflow Vulnerability
- ICSA-16-306-03 : Schneider Electric Unity PRO Control Flow Management Vulnerability
- ICSA-16-301-01 : Honeywell Experion PKS Improper Input Validation Vulnerability
- ICSA-16-299-01 : Siemens SICAM RTU Devices Denial-of-Service Vulnerability
- ICSA-16-294-01 : Moxa EDR-810 Industrial Secure Router Privilege Escalation Vulnerability
- ICSA-16-292-01 : Schneider Electric PowerLogic PM8ECC Hard-coded Password Vulnerability
- ICSA-16-287-01 : OSIsoft PI Web API 2015 R2 Service Account Permissions Vulnerability
- ICSA-16-287-02 : Siemens Automation License Manager Vulnerabilities
- ICSA-16-287-03 : Siemens SIMATIC STEP 7 (TIA Portal) Information Disclosure Vulnerabilities
- ICSA-16-287-04 : Rockwell Automation Stratix Denial-of-Service and Memory Leak Vulnerabilities
- ICSA-16-287-05 : Moxa ioLogik E1200 Series Vulnerabilities
- ICSA-16-287-06 : Fatek Automation Designer Memory Corruption Vulnerabilities

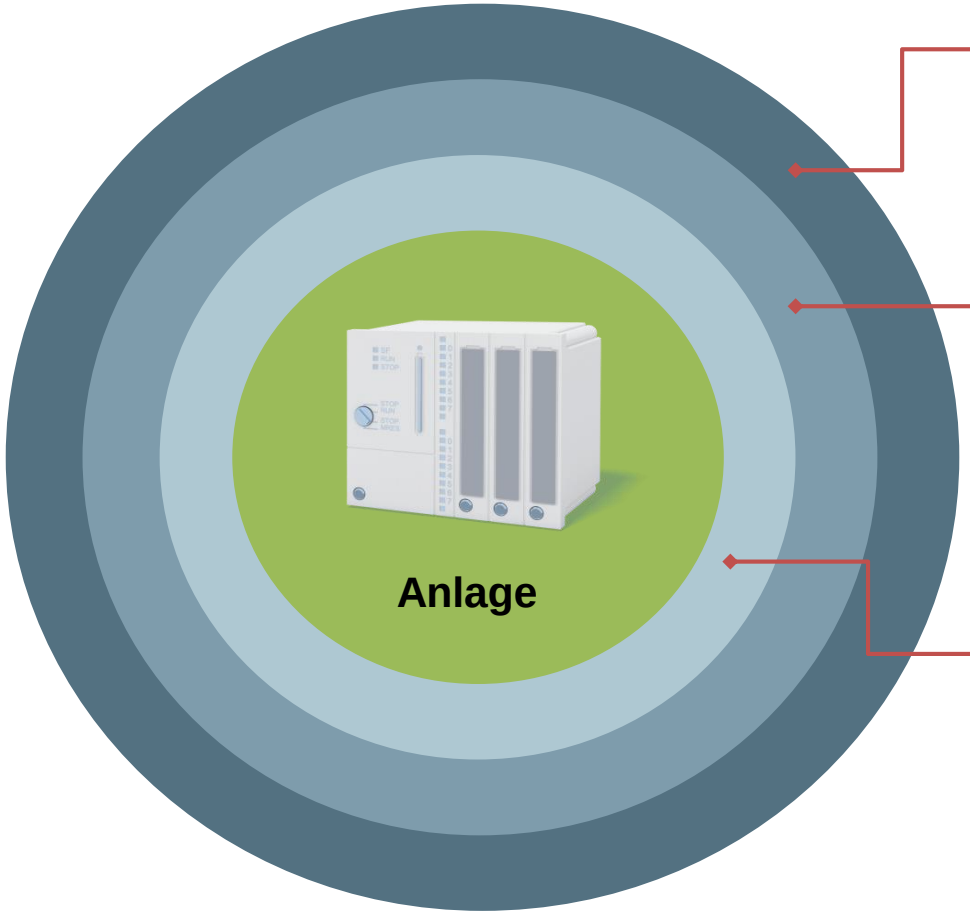
1 2 3 4 5 6 7 8 9 ... next › last »

TOP Bedrohungen (BSI)

Nr. (Nr. alt)	2016: Top 10	2014: Top 10
1 (3)	Social Engineering und Phishing	Unberechtigte Nutzung von Fernwartungszugängen
2 (2)	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3 (1)	Infektion mit Schadsoftware über Internet und Intranet	Social Engineering
4 (5)	Einbruch über Fernwartungszugänge	Menschliches Fehlverhalten und Sabotage
5 (4)	Menschliches Fehlverhalten und Sabotage	Einbruch über Fernwartungszugänge
6 (6)	Internet-verbundene Steuerungskomponenten	Internet-verbundene Steuerungskomponenten
7 (7)	Technisches Fehlverhalten und höhere Gewalt	Technisches Fehlverhalten und höhere Gewalt
8 (9)	Kompromittierung von Extranet und Cloud-Komponenten	Kompromittierung von Smartphones im Produktionsumfeld
9 (10)	(D)DoS Angriffe	Kompromittierung von Extranet und Cloud-Komponenten
10 (8)	Kompromittierung von Smartphones im Produktionsumfeld	(D)DoS Angriffe

Quelle: BSI

Defence-in-Depth



Anlagensicherheit

- Zutrittssperre für unbefugte Personen
- Verhinderung des physischen Zugangs zu kritischen Automatisierungskomponenten

Netzwerksicherheit

- Kontrollierte Schnittstellen zwischen Office- und Anlagennetzwerk, z. B. über Firewalls
- Gesicherte Kommunikation, z. B. über VPN
- Weitere Segmentierung des Anlagennetzwerks

Systemintegrität

- Software
- Wartungs- und Update-Vorgänge: Benutzerauthentifizierung Anlagen- oder Maschinenbediener

Beispiel IEC 62443

3-2 Zones & Conduits

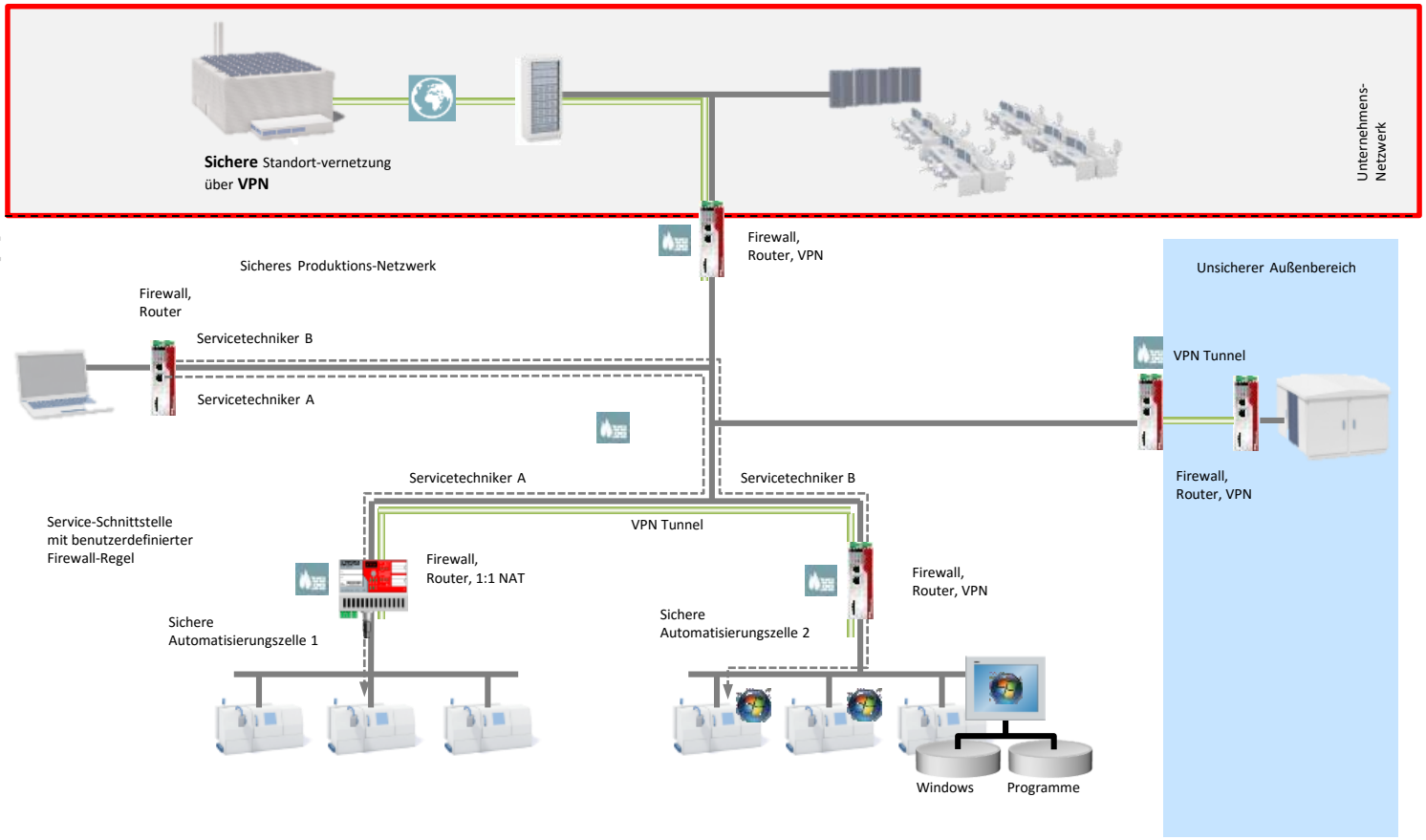
- Prinzip der Zonierung implementiert die physikalische und/oder logische Trennung auf der Netzwerkebene
- Härtung des Systems gegenüber Angriffen
- Zonen müssen miteinander verbunden sein, damit Kommunikation stattfinden kann
- Kommunikationskanal (Conduit) muss kontrolliert und abgesichert sein

3-3 Security Level

- Einführung von Security Level (SL) zur Durchführung von Risikoanalysen und Abschätzung der Häufigkeit bzw. Eintrittswahrscheinlichkeit von Bedrohungen

Industrial Security

- **Anlagensicherheit**
- Netzwerksicherheit
- Systemintegrität



Anlagensicherheit

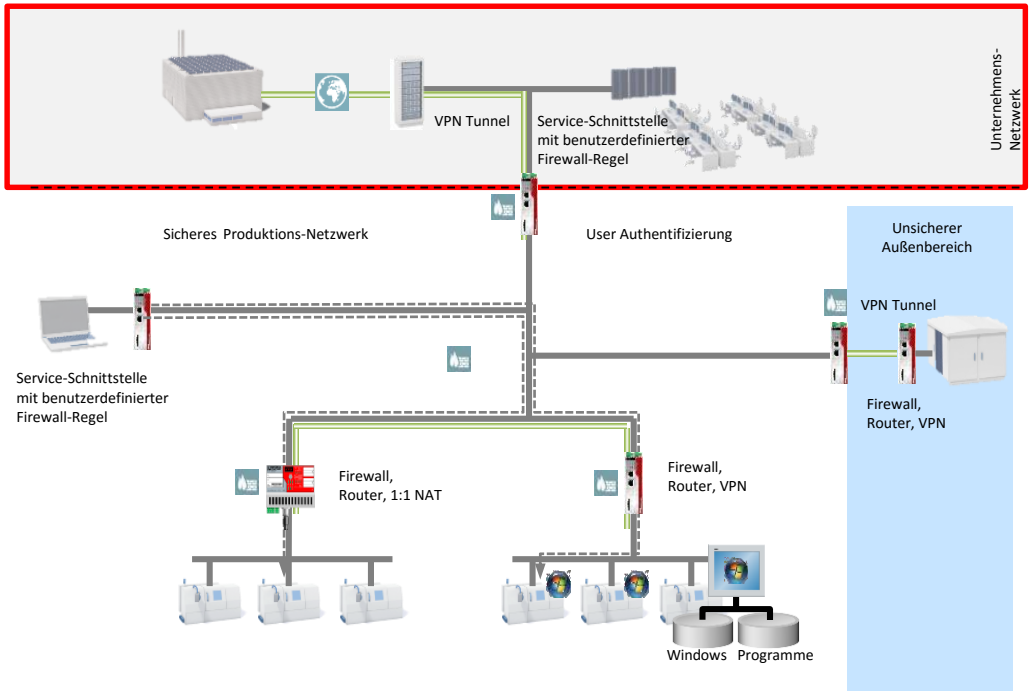
Physikalischer Schutz von kritischen Infrastrukturen

- Zugriffsschutz zu Anlagen durch Ausweis und Kontrolle an Toren und Schleusen
- Einsatz durch Wachpersonal
- Physischer Zugriffsschutz zu kritischen Infrastrukturen wie Serverräume und Leitwarten
- Überwachung mit Video-Kameras und Bewegungssensoren
- Security Elemente für RJ45-Netzwerk-Anschlüsse zum Schutz nicht belegter Ports gegen unberechtigten Zugriff

Anlagensicherheit

Zugriffssperre für unbefugte Personen

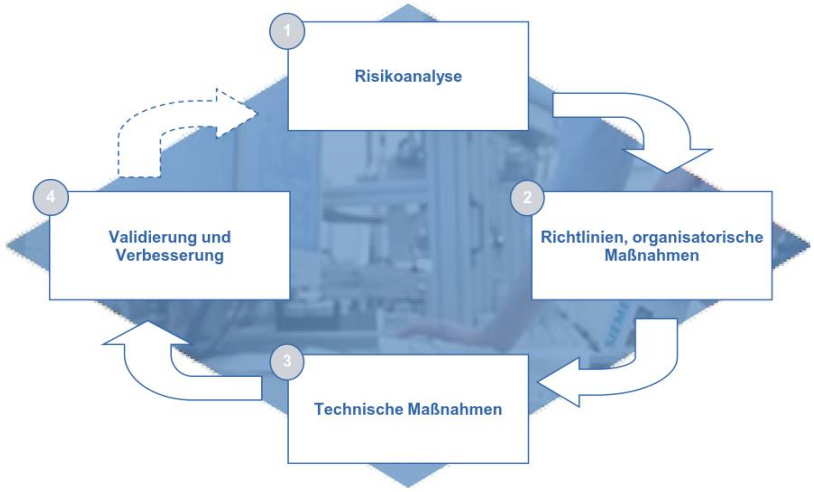
- Deaktivierung von nicht belegten Ports
- Zugriffssperre durch User Authentifizierung 802.1x
- Reglementierung der Zugriffe über Benutzer-Firewall
- Einschränkung des Netzwerk-Zugriffs z.B. über MAC-Adressfilter



Anlagensicherheit

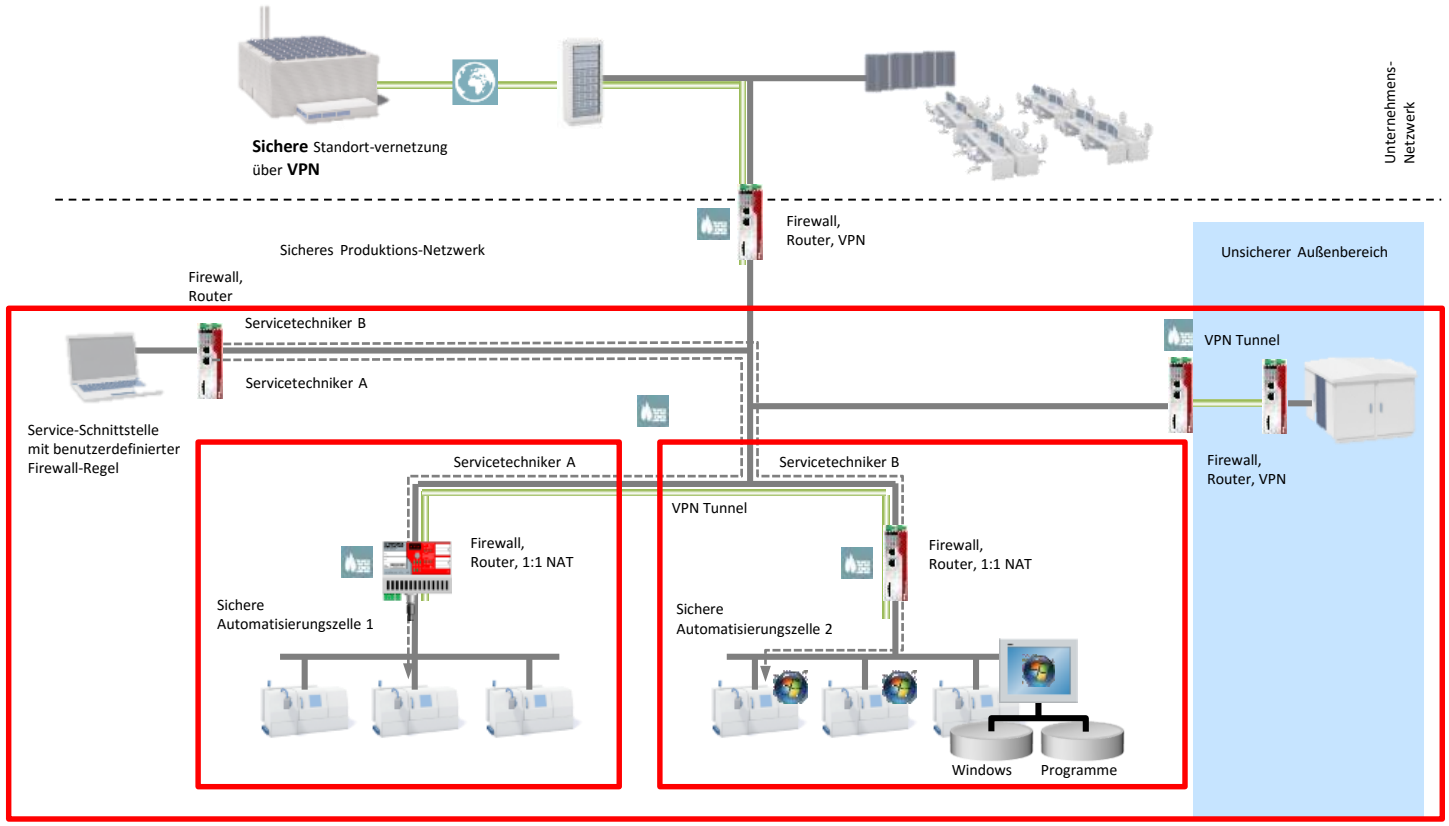
Security Management Prozess

- Ernennung eines IT-Sicherheitsbeauftragten in der Produktion
- Festlegung von Richtlinien
- Risikoanalyse mit Definition und Umsetzung von Security-Maßnahmen
- Etablieren strikter organisatorischer Security-Vorgaben und technischen Kontrollen
- Sensibilisierung und Schulung der Mitarbeiter durch Security-Awarenesstraining (TOP1 BSI)
- Regelmäßige/ereignisabhängige Wiederholung der Risikoanalyse



Industrial Security

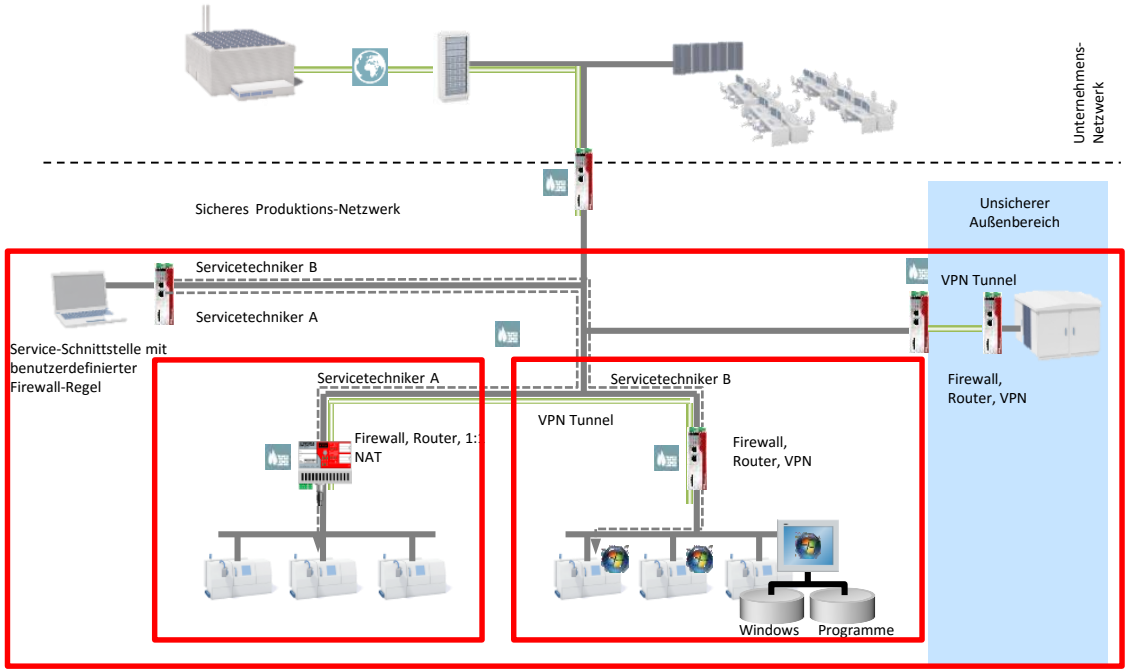
- Anlagensicherheit
- **Netzwerksicherheit**
- Systemintegrität



Netzwerksicherheit

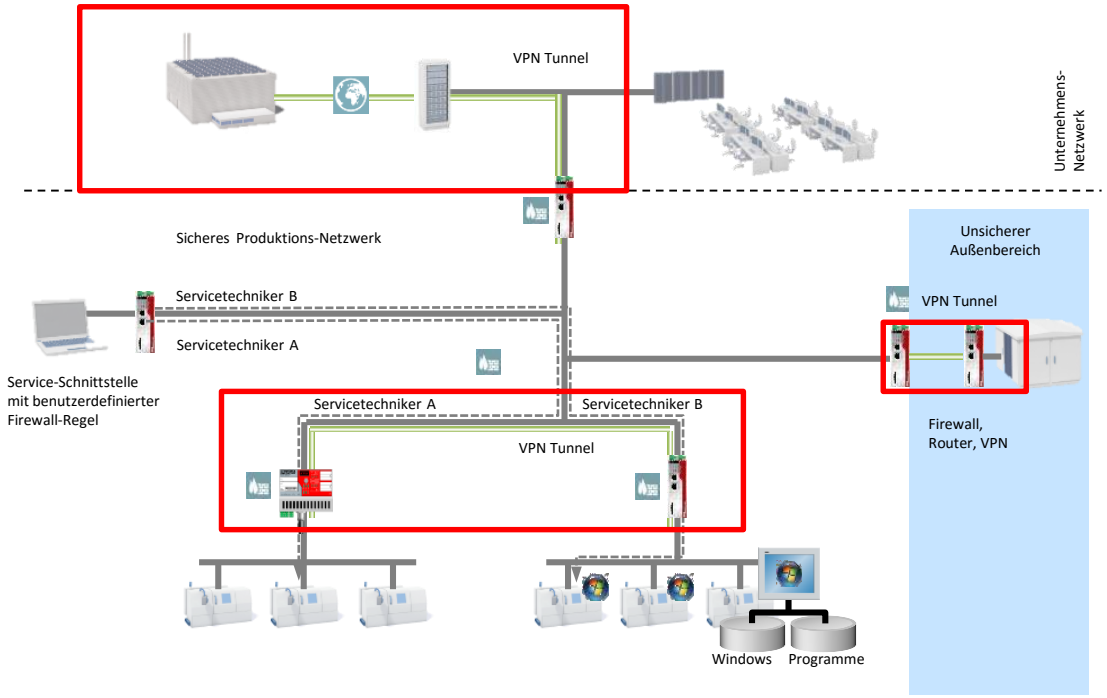
Einsatz von Firewalls

- Reglementierung der Kommunikationsbeziehungen über FW Regeln
- User Authentifizierungen über Benutzerfirewall
- Reduzierung der Netzlast durch Router-Funktionalität und QoS
- Segmentierung des Anlagen-Netzwerks



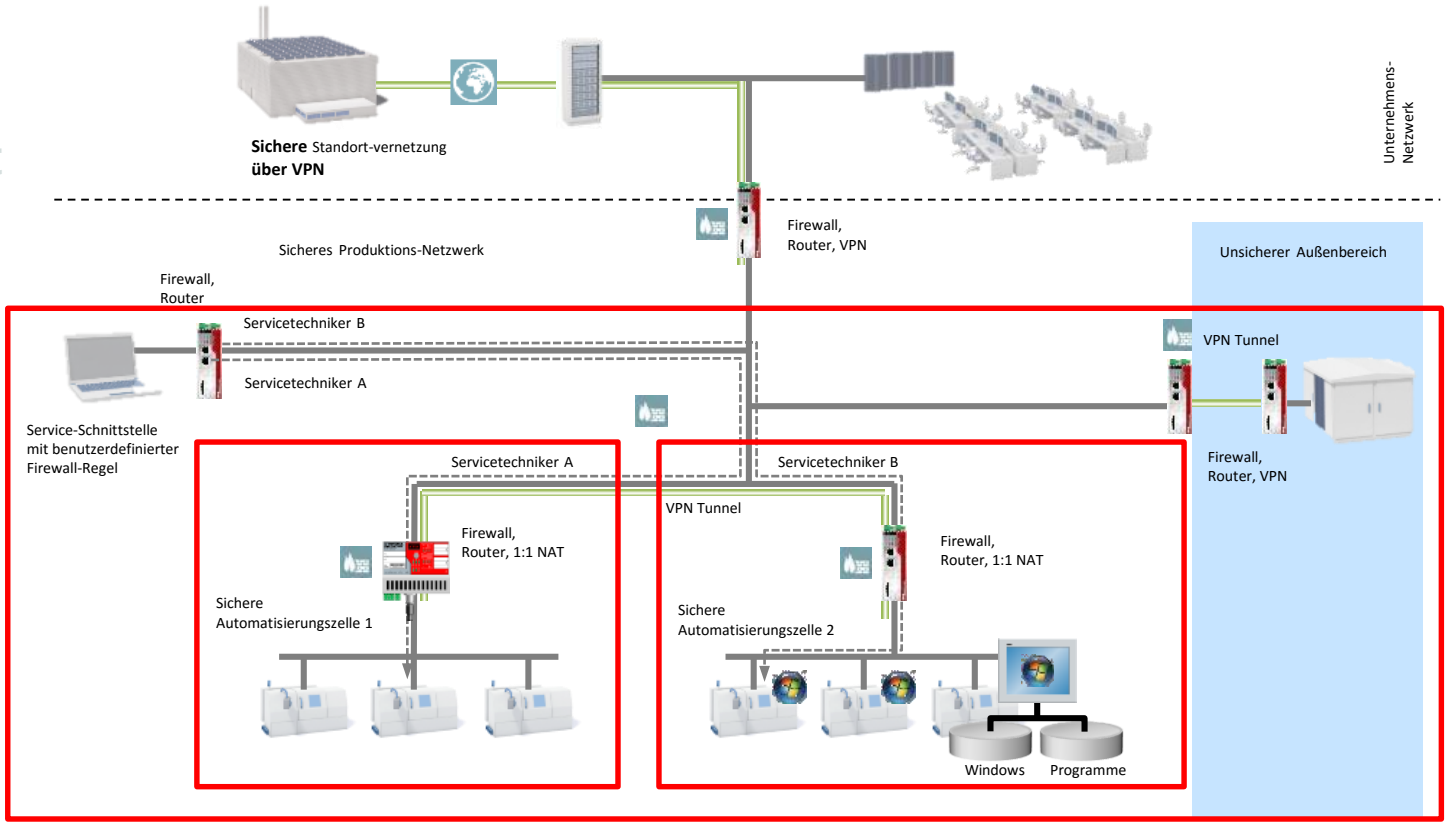
Einsatz von VPN

- Sichere und verschlüsselte Anlagenkommunikation über VPN
- Sichere und verschlüsselte Fernwartung über VPN
- Aktivierung der VPN Tunnel bedarfsorientiert
- Authentifizierung und Verschlüsselung durch Zertifikate



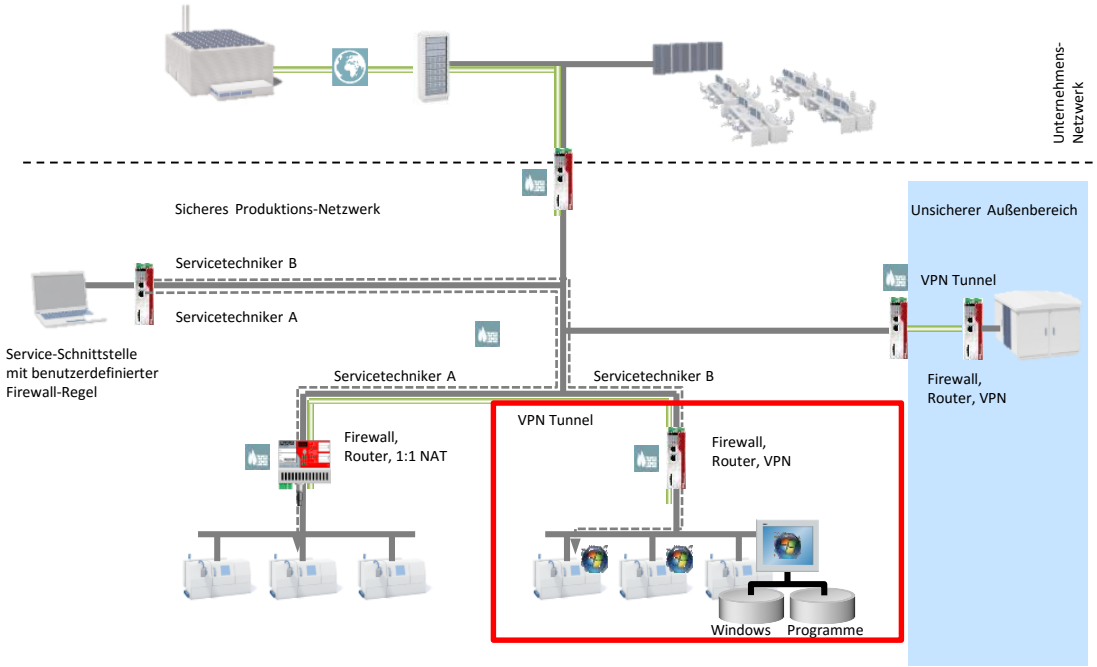
Systemintegrität

- Anlagensicherheit
- Netzwerksicherheit
- **Systemintegrität**



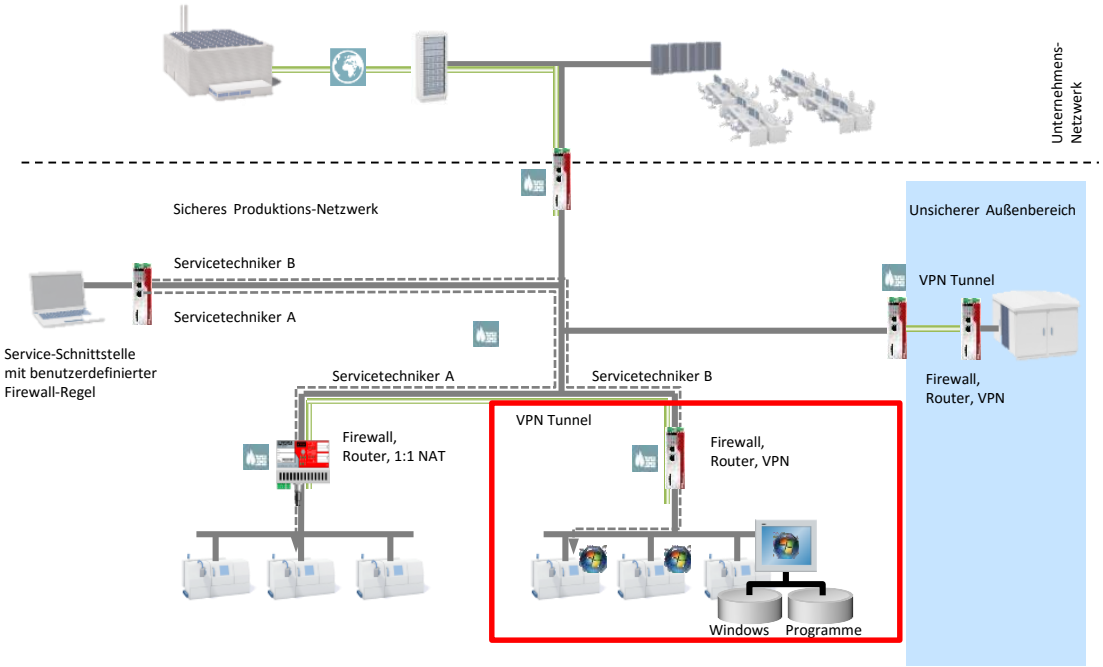
Zugriffsschutz auf das Netzwerk

- Port-Security über MAC- oder IP-Zugriffstabellen
- Port Security mit RADIUS-Authentication
- Firewall-Regelsätze



Zugriffsschutz auf die Netzwerkkomponenten

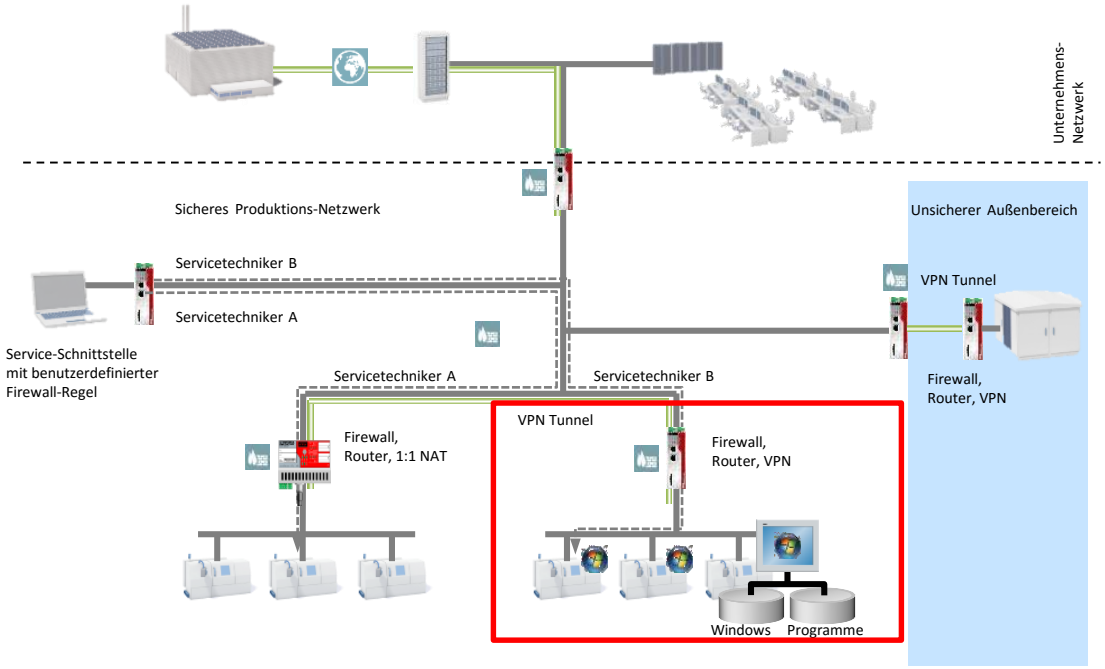
- Sicherer Zugriff auf WEB-Server über https
- Sicherer Dateitransfer über FTPS
- Abhörsichere Übertragung von Netzwerkanalyse-Informationen über SNMPv3
- Abgestufte Benutzerrechte durch unterschiedliche Passwörter
- Verschlüsselte Datenübertragung über VPN



Systemintegrität

Manipulationsschutz

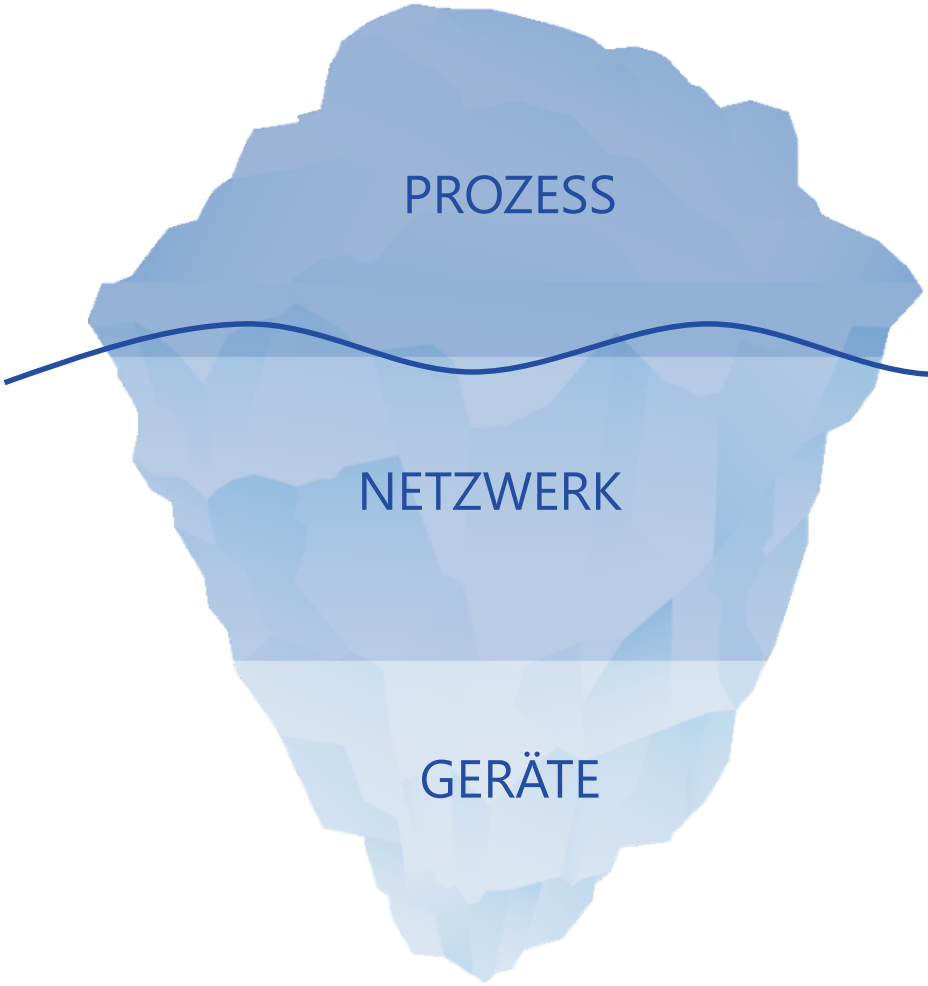
- Regelmäßiges Ausführen von Windows-Patches auf PC-basierten Steuerungen
- Schutz gegen unberechtigtes Öffnen der Applikationsprogramme
- Schutz vor unberechtigtem Ändern, Kopieren und Duplizieren der Projektierung
- Überwachung der Kommunikation



Trügerische Sicherheit

- Alle "Türen und Wege" von und nach außerhalb sind verschlossen oder werden überwacht
- Dauerhaftes Monitoring der Sicherheit bzw. Kommunikation muss gegeben sein
- Mögliche Bedrohungen von innen oder auch Fehlkonfigurationen werden nicht "bekämpft"

Das Problem



DCS/SCADA

Fehlende Sicht

Mögliche "Cyber-Angriffe”

Sicherheit | Vernetzung | Betrieb

Stuxnet
Havex
Ukraine-Blackout

Unerlaubte Zugriffe und Datenflüsse

Nutzung unsicherer Protokolle

Falsche Messergebnisse

Instabile Prozesse

Korrupte Daten / Nicht eingehaltene Protokoll-Spezifikation

Manipulation und Zugang von Außen

Misskonfiguration von Firewall und Netzkomponenten

Verbindungs-probleme zw. Geräten

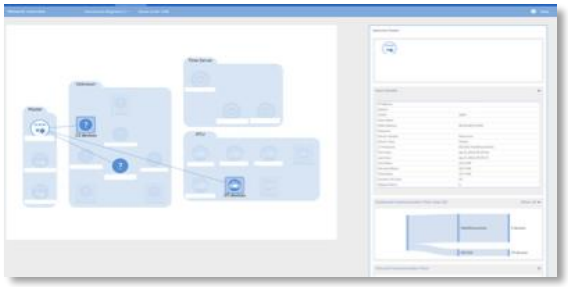
Störungen und Softwarebugs

Anomalien/ Stillstand der Schaltanlagen

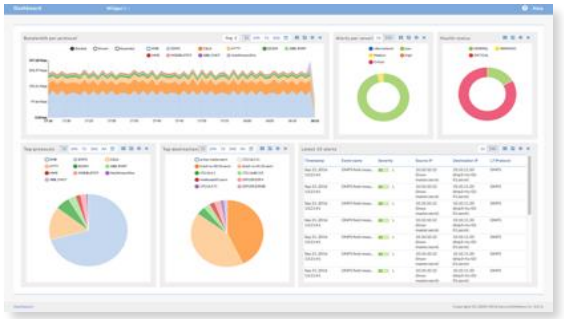
Unkontrollierte Regelschalter-bedienung

Notwendige Funktionalitäten

Asset Inventarisierung & Netzwerkübersicht
Automatische Inventarisierung der Netzwerk-geräte und deren Kommunikationsflüsse

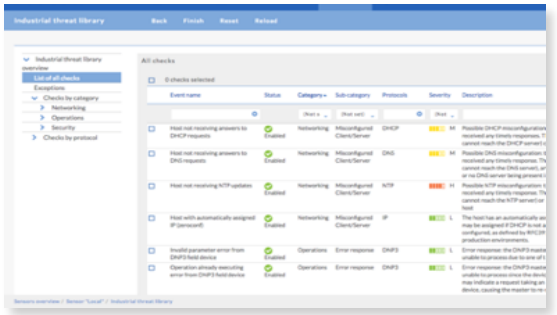


Visuelle Datenanalyse
Konfigurierbares Dashboard für Echtzeit- & forensische Netzwerkanalyse

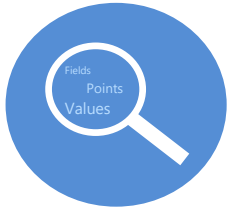


"Built-in" Module
Portscans, man-in-the-middle Attacken
und inkompatible/fehlerhafte Protokollnachrichten

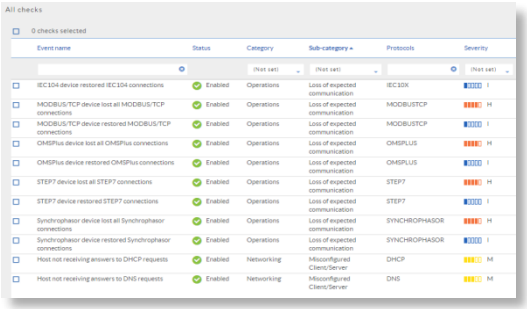
Kommunikationsmuster
Automatische Erkennung von erlaubten Kommunikationen zwischen Geräten, Protokollen und deren Funktionsweisen



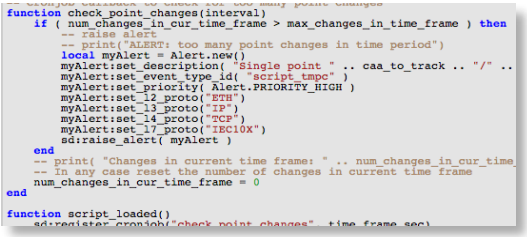
Notwendige Funktionalitäten



Deep Protocol Behavior Inspection von Industrieprotokollen, Automatisches Whitelisting von autorisierten Prozessen, Parametern und Werten



Industrial Threat Library
Out-of-the-Box Erkennung von Netzwerk- und Sicherheitsprobleme und Bedrohungen



Scripting engine
Benutzerdefinierte Erstellung von netzwerk-, prozess- oder anderer sicherheitsrelevanter Überprüfungen

Beispiele

- Entdeckung von unerlaubten Zugriffsversuchen aus dem TSO-Bereich (Übertragungsnetzbetreiber), um DSO-Prozesse (Verteilnetzbetreiber) zu verändern
- Fehler in NTP-Konfigurationen und Management der Server: Einige Systeme bekommen keine NTP-Aktualisierungen
- Identifizierung von alten / schwachen Protokollen (Telnet, FTP, SNMPv1, ...)
- Entdeckung von nicht zugewiesenen oder mehrfach vergebenen IP-Adressen, Beeinträchtigung der Verfügbarkeit der Hosts
- Erkennung, dass nachts zwei Programmierstationen eine vollständige Sicherung ihrer SPS-Programme und ihres Speichers ausführen

Notwendige Schnittstellen

- Interoperabilität zu ISMS, SIEM, …
- Um Verbreitung von Angriffen einzudämmen und Betreiber rechtzeitig vor Sicherheits- oder auch Konfigurationsproblemen zu warnen bzw. sie zu informieren

Fazit

- Security ist nicht statisch, es ist ein dauerhaft dynamischer Prozess
- Ressourcen und Budget müssen bereitgestellt werden
- Es gibt keinen "Königsweg", Standards (z.B. IEC 62443) dienen als Hilfestellung
- Jetzt handeln!

Informationstag "Umsetzung des IT-Sicherheitsgesetzes in der Unternehmenspraxis"

Gemeinsame Veranstaltung von TeleTrusT, bevh und BISG

Berlin, 29.11.2016

Vielen Dank.

Thorsten Vogel

PHOENIX CONTACT Cyber Security AG