NIS2 - frühzeitig die richtigen Entscheidungen auch für die OT treffen

Referent: Stefan Menge
ACHT:WERK

Kundenworkshop
"NIS2-Regelung der EU: Herausforderungen der Cybersicherheit meistern"
26.11.2024

IRMA®
INDUSTRIE RISIKO MANAGEMENT AUTOMATISIERUNG

Was heißt überhaupt „OT (Operational Technology)"?

Kommerzielle & Büro IT

- Personal- und Kundendaten
- Abrechnung, Einkauf,
- Finanzbuchhaltung
- Berichtswesen
- …
- Cloud Services
- „Future Workplace"
- Digitalisierung

Der Produktionsbetrieb - OT

- Gesamtheit der Hardware und Software, die zur **Steuerung und Überwachung von physischen Prozessen** in industriellen Umgebungen zur Fertigung, Fabrikation, Herstellung, Bearbeitung oder Verarbeitung von Wirtschafts- oder Gebrauchsgüter

Angreifbarkeit von Kernprozessen in der Wertschöpfung

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop Schlagzeilen | Wetter | TV-Programm | mehr ▼

Login | Registrierung

SPIEGEL ONLINE NETZWELT

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto | Stil

Nachrichten > Netzwelt > Web > Hacker > Erpressung durch Cyberattacken: Angriffsziel Industrieanlage

Erpressung durch Hacker: Cyberattacke in der Keksfabrik

Von Uli Ries

Als die Konstrukteure einer kanadischen Keksfabrik gefragt wurden, welche Folgen sie sich durch Cyberangriffe auf die Anlage vorstellen könnten, antworteten sie: "versalzenen Keksteig". Mehr als der Verlust einer Tagesproduktion sei durch eine bösartige Manipulation nicht zu erwarten, dachten die Ingenieure. Leider falsch.

Tatsächlich stand die Fabrik komplett still, nachdem Unbekannte in deren Netzwerk eingedrungen waren. Die von den Angreifern zur Analyse des Netzes verwendete Software brachte die Steuerungscomputer der Fabrik aus dem Tritt.

Die empfindlichen SPS-Systeme (**S**peicher**p**rogrammierbare **S**teuerung) reagierten mit Chaos: Die Produktion brach zusammen, vorproduzierter Teig trocknete in den Transportrohren ein. Die Verstopfungen waren so hartnäckig, dass die Rohre schließlich herausgeschnitten werden mussten.

Quelle:
Spiegel Online, 17.08.2015

Mythen zur eigenen Informationssicherheit in der OT

Wir sind nicht mit dem Internet verbunden.

Unsere Systeme sind durch eine Firewall geschützt.

Hacker verstehen Automatisierung und Steuerungen nicht.

Unsere Firma ist kein Ziel.

Unser Sicherheitssystem / Team der IT- Abteilung beschützt uns.

NIS2 – SicherheitsLücken flächendeckend füllen

 Bearbeitungsstand: 22.07.2024 16:45

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

ITSiG 1.0
ISMS
Risikolage
Security & Risikomanagement

ITSiG 2.0
Protokollierung
Detection
Reaktion

EU-NIS2
» NISUmsuCG
EU Cybersicherheit
Haftung, Verantwortung
Resilienz

2015 — 2021 — 2023

Sicherheit in der Informationstechnik von Einrichtungen (§ 28)
Wer ist betroffen?

NIS2-Sektor aus Anlage 1

- Energie
- Transport und Verkehr
- Finanzen und Versicherungen
- Gesundheit
- Wasser
- Informationstechnik + Telekomunikation
- Weltraum

NIS2-Sektor aus Anlage 2

- Transport und Verkehr (Post und Kurier)
- Abfallbewirtschaftung
- Chemie
- Lebensmittel
- Verarbeitendes Gewerbe / Herstellung
- Anbieter digitaler Dienste
- Forschung

Besonders wichtige Einrichtung
wenn
>= 250 Mitarbeitende
oder
> 50 Mio Umsatz und > 43 Mio Bilanz

Wichtige Einrichtung
wenn
>= 50 Mitarbeitende
oder
> 10 Mio Umsatz und > 10 Mio Bilanz

Pflicht zum Einsatz von Systemen zur Angriffserkennung für KRITIS

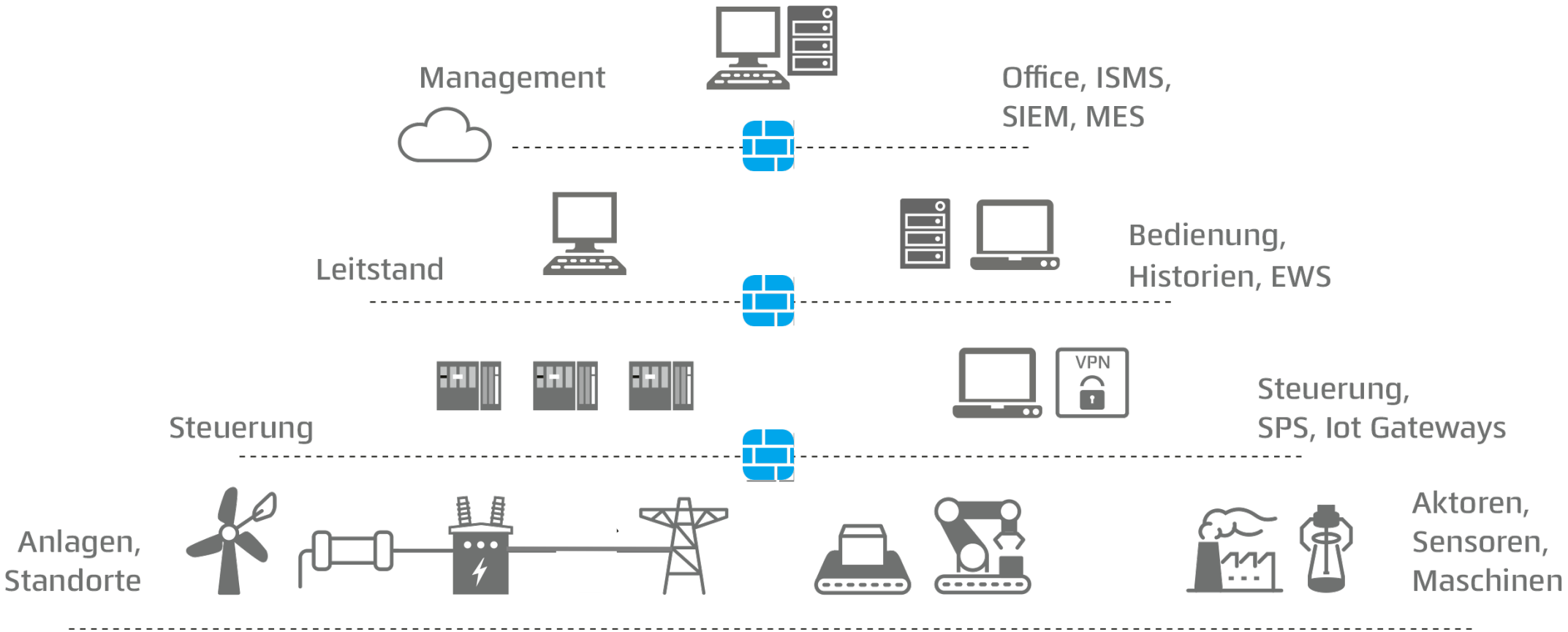
IRMA
SO EINFACH. SO SICHER!

IT-Sicherheitsgesetz 2.0 / NIS2UmsuCG-2_Entwurf (§ 31 BSIG - E)

„(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.“

Orientierungshilfe Systeme zur Angriffserkennung

Angestrebter Stand der Technik in Bezug auf Netzsegmentierung



Vertraulichkeit
vor unbefugter Preisgabe geschützt

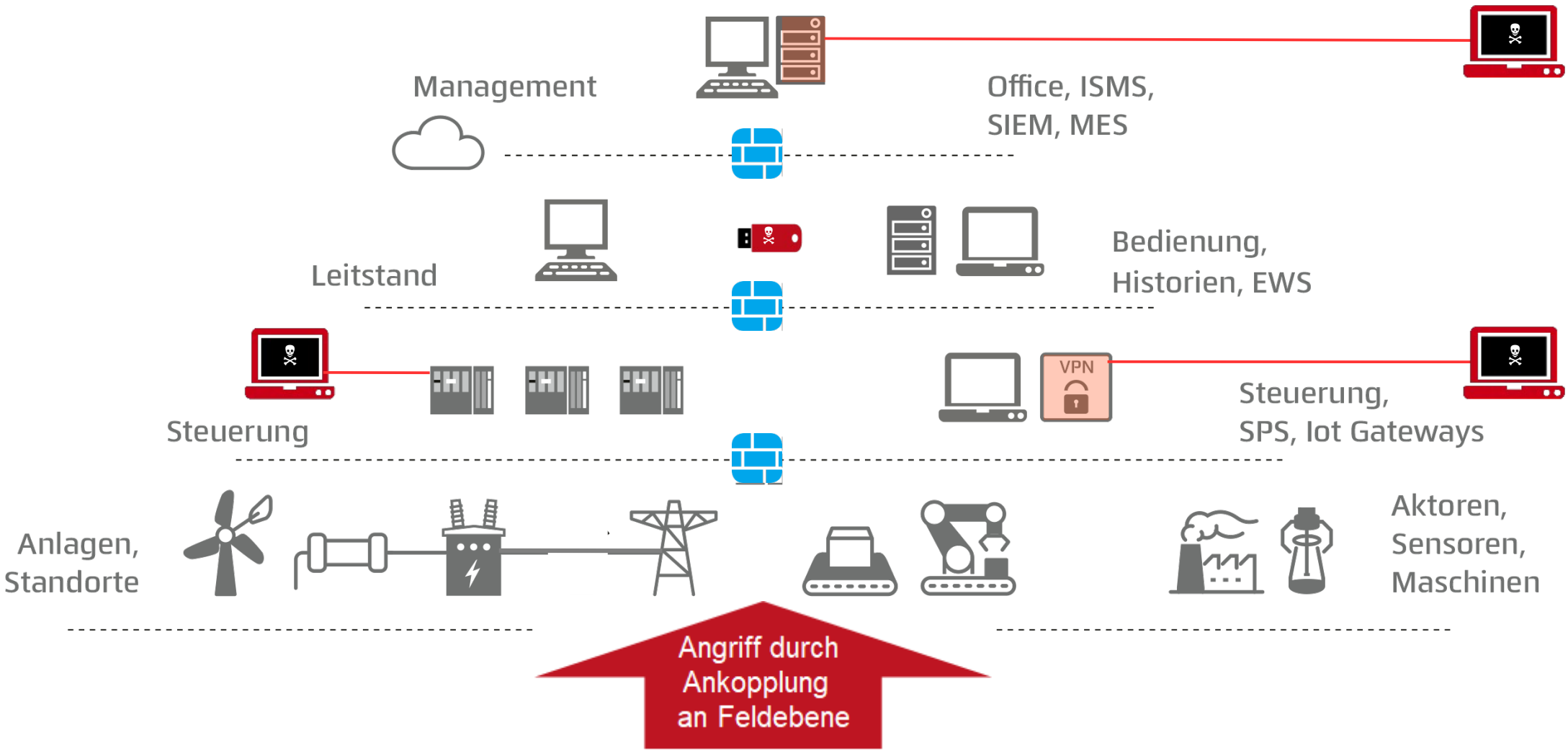
Integrität
vollständig und unverfälscht

Verfügbarkeit
stets wie vorgesehen nutzbar

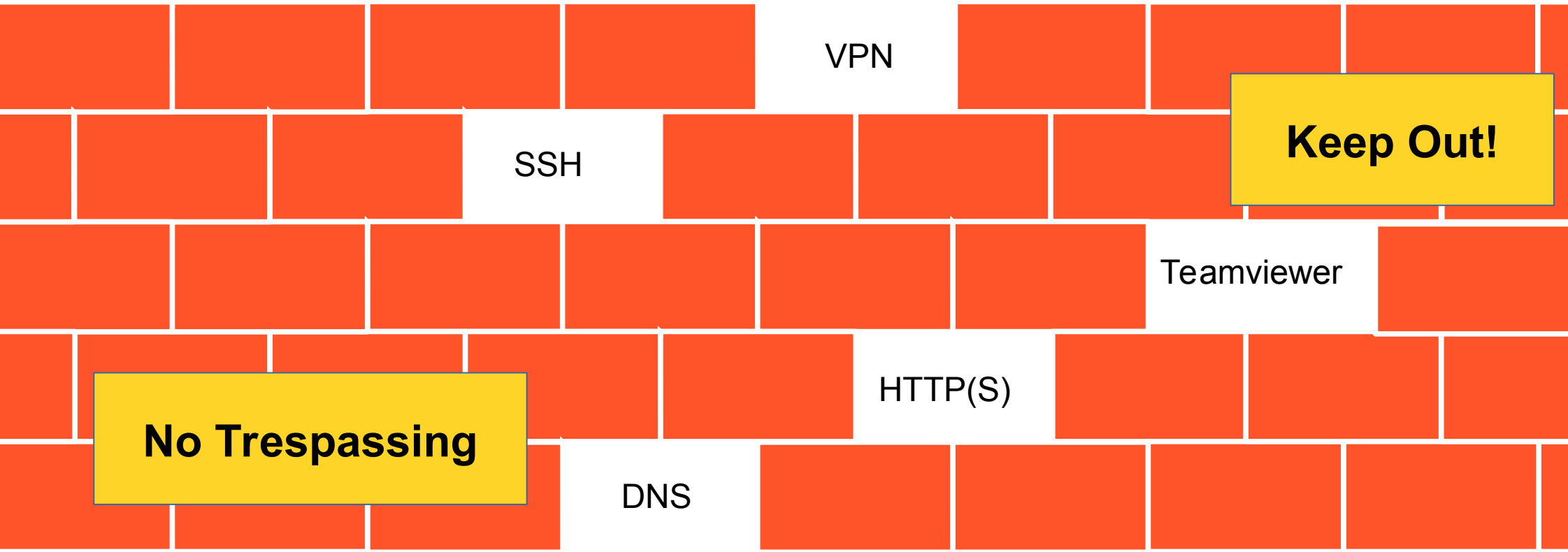
Geräte im Produtionsnetz

- Alte Hard- & Software ohne Patches
- Verschlüsselung ist selten (oder schlecht)
- Software und Protokolle oft proprietär
- Geräte empfindlich ggü. Störungen
- Schwachstellen werden oft nicht behoben
- Gewollte Funktionen können Prozess stören

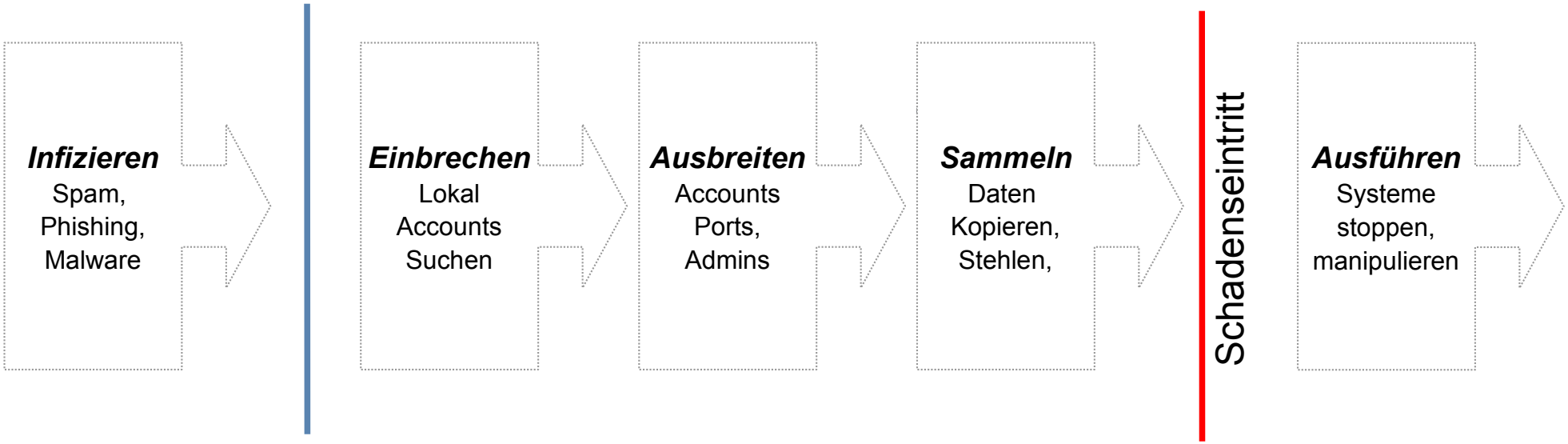
Stand der Technik nach IEC 62443 in Bezug auf Netzsegmentierung



Firewalls sind löchrig...



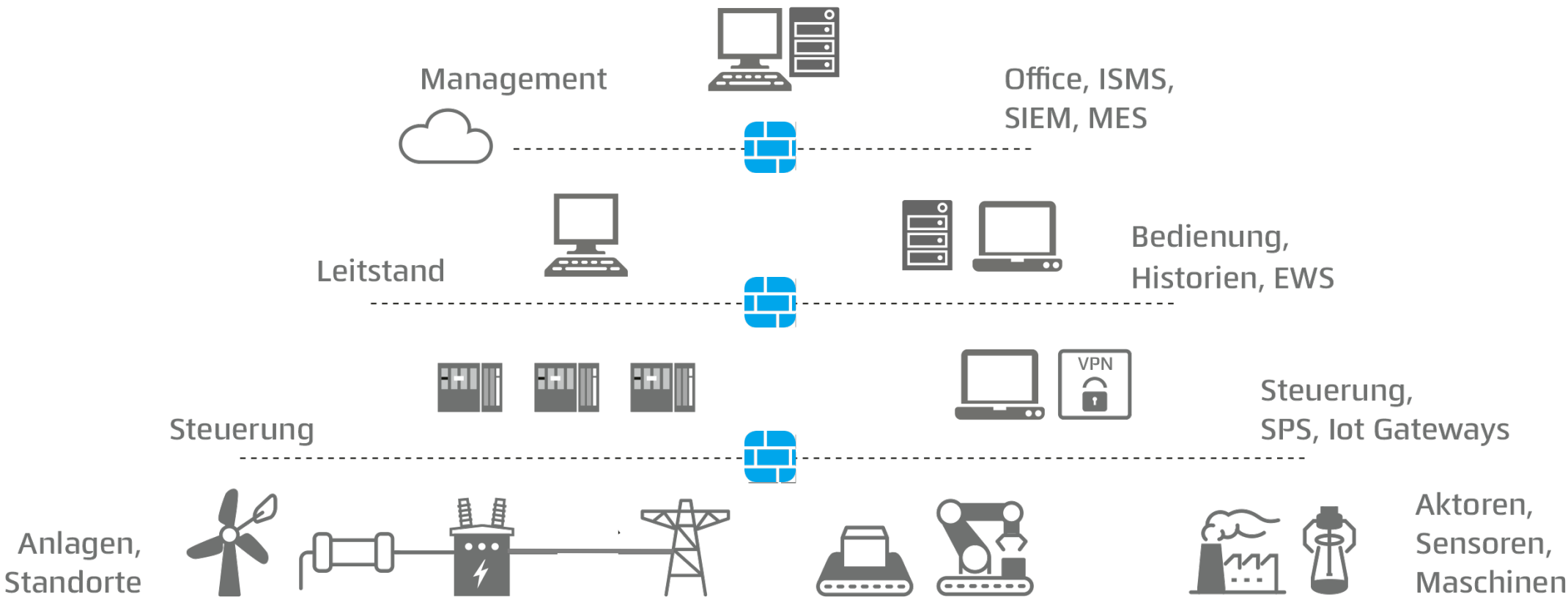
Von Anomalie- zur Angriffserkennung



NIS2 – § 30 BSIG-E: Risikomanagement-Maßnahmen (Auszug)

- **Stand der Technik**
- Konzepte für **Risikoanalyse** und die Sicherheit von Informationssystemen
- Strategien zur Bewältigung von **Sicherheitsvorfällen**
- **Business Continuity** durch Backup-Management und Notfallpläne
- Sicherheit der **Lieferkette** inkl. sicherheitsbez. Aspekte der Beziehungen zwischen einzelnen Einrichtungen
- Umsetzung grundlegender Maßnahmen der **Cyberhygiene**
- Anwendung von Multifaktor-Authentifizierung

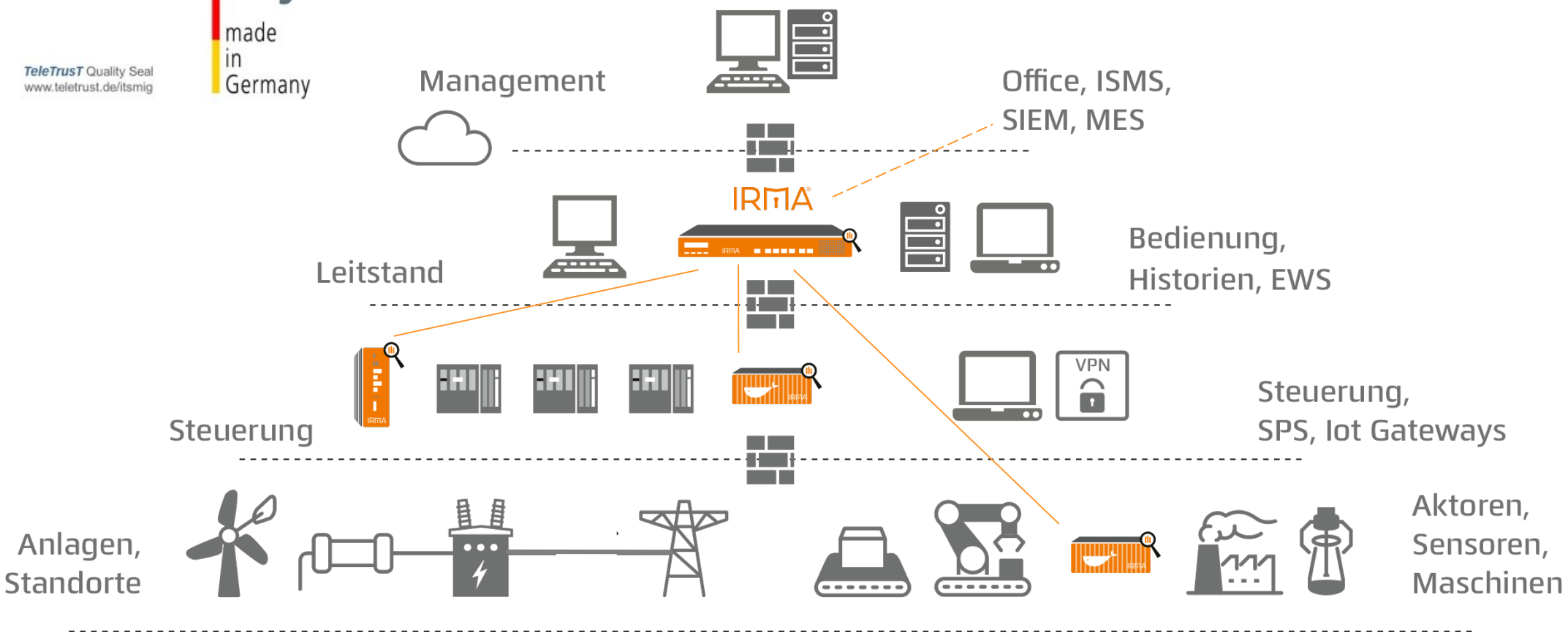
Stand der Technik nach IEC 62443 in Bezug auf Anomalieerkennung



Stand der Technik nach IEC 62443 in Bezug auf Anomalieerkennung

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig



BSI-Empfehlung CS-134 (zum Stand der Technik)

Kategorie: Außergewöhnliche bzw. ungewöhnliche Aktivitäten im (ICS)-Netzwerk

Basisanforderungen:

- Identifikation neuer Geräte im ICS-Netz
- Identifikation der Kommunikation zwischen zwei Geräten, zwischen denen bisher keine Kommunikation stattgefunden hat
- Identifikation der Kommunikation zwischen zwei Geräten über einen TCP/UDP-Port, der bisher nicht verwendet worden ist
- Identifikation neuer Protokolle oder der Veränderung von Protokollen zwischen einzelnen Komponenten
- Identifikation von Verbindungen in unsichere Netzwerke, z.B. Internet
- Identifikation unsicherer Kommunikationseigenschaften, z.B. fehlende Verschlüsselung

Überwachung & Kontrolle in Echtzeit

IRMA® ist ein Produkt mit

- einfachster Installation
- passivem Scannen der Teilnehmer (nach **Stand der Technik**)
- kontinuierlicher Überwachung Ihrer Anlagen (**Cyberhygiene**)
- Lieferung von Informationen zu Cyberangriffen und Unregelmäßigkeiten (**Bewältigung von Sicherheitsvorfällen**)
- Ermöglichung von Analyse (**Risikomanagement**) und intelligenter Alarmierung
- Historisierung der Netzwerkinformationen (**Bewältigung von Sicherheitsvorfällen**)
- Validierung jeder Verbindung / jedes Teilnehmers (**Cyberhygiene**)
- Reporting über den Zustand der gesamten Anlage (**Cyberhygiene**)
- Analyse der Verbindungen (u.a. in der **Lieferkette**)

ACHT:WERK

Dipl.-Ing. Stefan Menge · Geschäftsführer

Achtwerk GmbH & Co KG
Am Mohrenshof 11a
D-28277 Bremen

T +49 171 55 80 135
stefan.menge@acht-werk.de
www.acht-werk.de

Vielen Dank!

Nehmen Sie Kontakt mit uns auf unter:
T +49 (0) 421 – 878 478 80
www.irma-security.de