TeleTrusT
Pioneers in IT security.

TeleTrusT-Auditorium (it-sa 2016)

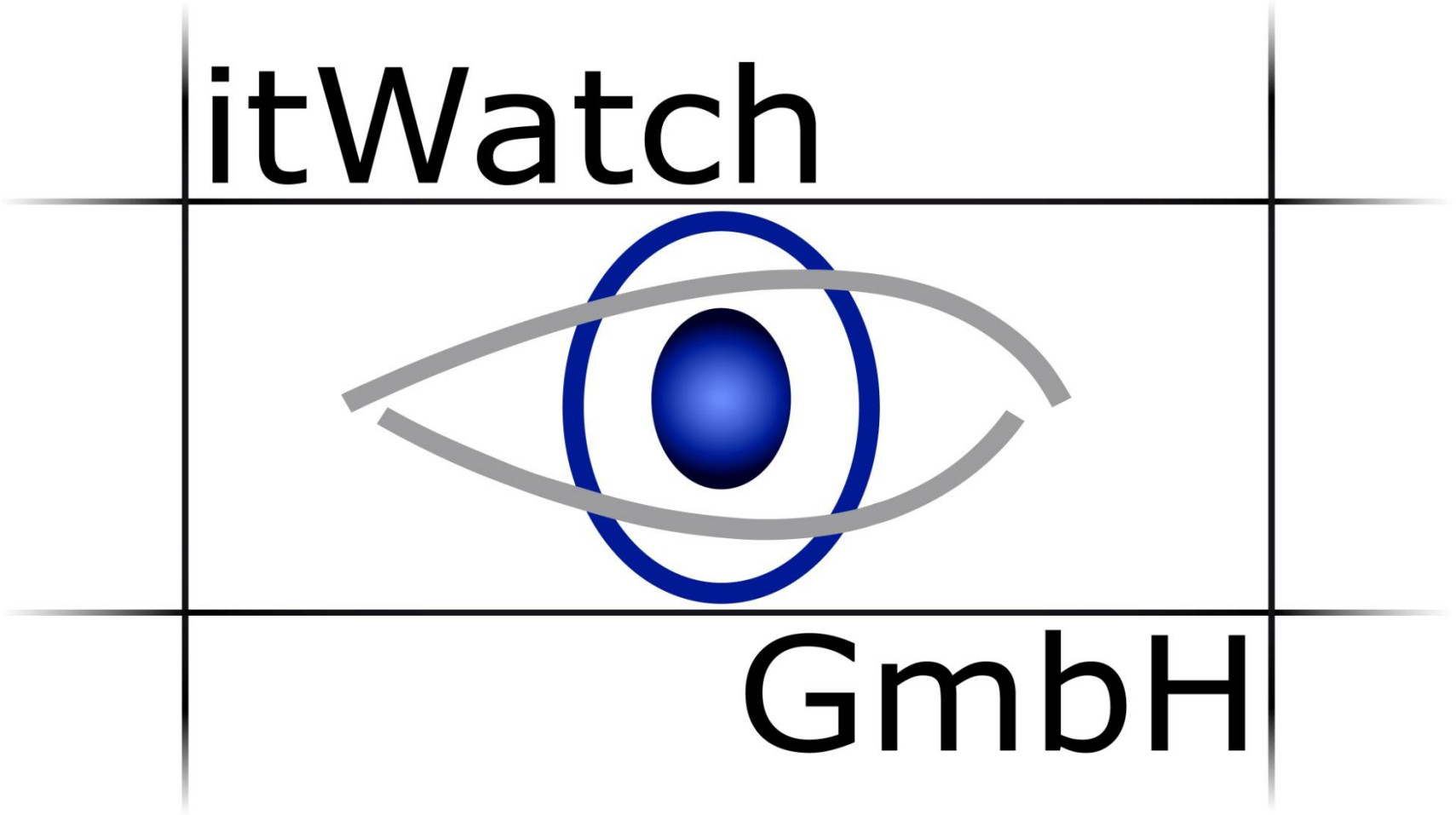
Nürnberg, 19.10.2016

Safety - Konvergenz Shop & Office-Floor - welche Rolle spielt die Verlässlichkeit / Sicherheit der IT?

Ramon Mörl, itWatch GmbH

itWatch GmbH

Ihre Sicherheit …
… unsere Mission



Kurzvorstellung Ramon Mörl

- 25 Jahre Erfahrung als Berater in der IT-Sicherheit
- Leitende Tätigkeiten in Projekten für Firmen wie HP, IBM, Siemens, ICL und Bull in Belgien, Deutschland, Frankreich, Italien, Österreich, Schweiz und USA
- Als unabhängiger Evaluator und Berater der Europäischen Union vor allem im Bereich der ECMA und ISO-Standards für die IT-Sicherheit tätig
- Seit 2002 **Geschäftsführer der itWatch GmbH**

itWatch GmbH

Safety - Konvergenz Shop & Office-Floor – welche Rolle spielt die Verlässlichkeit / Sicherheit der IT?

Bedrohungen in Industrie 4.0 Szenarien – was ist anders?

Wo stehen wir?

Strategien zur Verteidigung – Angriffs-robuste Architekturen – Betrachtung vollständiger Vertrauensketten

Kostensenkung durch Vernetzung

Vernetzung von Systemen schafft geringere Kosten, da:

- notwendige Services von überall erbracht werden können.
- man Reisezeiten und –kosten einsparen kann.
- eigene Ressourcen effizienter eingesetzt werden können.
- Funkprotokolle lästige Kabel abschaffen.

… aber sie öffnet Wege für neue Angriffe

Priorisierung der Themen

Allen ist klar, dass ein AKW nicht einfach mit seinen produktiven Elementen an das Internet angeschlossen werden sollte.

?

Wo liegt aber nun die Grenze zwischen einem AKW und einen privaten internetfähigen Kühlschrank?

FDP Parteitag

Priorisierung der Themen

Eine Priorisierung der Themen ist zwingend notwendig, um der Komplexität der IT-Security gerecht zu werden:

- Überlässt man die Antwort nur den klassischen markt-regulierenden Faktoren, werden aus Kostengründen Risiken für Leib und Leben im Risikomanagement nicht adäquat berücksichtigt und durch Haftungsübergänge und organisatorische Hinweise abgewälzt.

- Die neue Doktrin muss heißen, dass die Einsparungspotentiale durch Vernetzung, und den Einsatz von COTS (Commercial off the shelf) Produkten erst realisiert werden können, wenn die Safety in allen Eventualitäten dadurch nicht schlechter ist als vorher.

Herausforderung

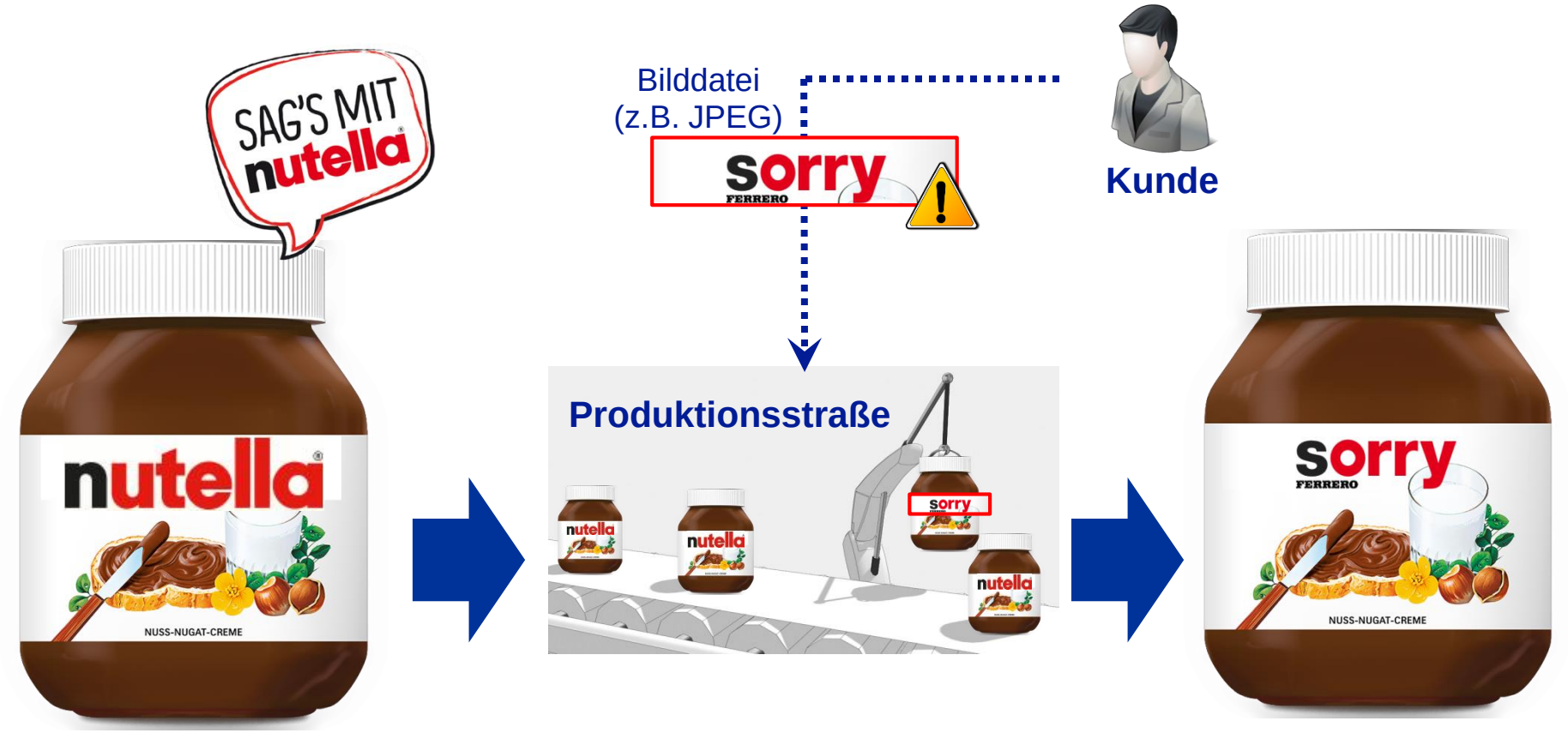
Dr. Peter Schaar (ehem. Bundesdatenschutzbeauftragter):

"Eine Anwendung kann nur so sicher sein, wie das Betriebssystem auf dem sie läuft."

Daraus resultiert:

Für eine IT-gestützte Handlungsweise mit Auswirkungen auf Leib und Leben von Menschen ist mehr zu tun als eine Anwendung nach aktuellen best practices möglichst Plattform- und Hardware-unabhängig zu entwickeln.

Problem Individualisierung 4.0



- Kunde möchte individualisiertes Produkt
- Kunde liefert die passende Bilddatei inklusive Schadcode zur Individualisierung (z.B. JPEG)
- Die Bilddatei wird in der Produktionsstraße direkt verarbeitet.

Schadcode in Bilddateien

Auf der Sicherheitskonferenz RSAConference 2015 in San Francisco stellte Marcus Murray eine einfache Methode vor, wie Angreifer in Bilddateien Schadcode versteckten und ganze Webserver übernehmen können.

- Murray versteckte bei seinem Versuch schadhaften Code als Kommentar innerhalb der EXIF-Informationen von Bilddateien (z.B. "jpg", "tiff"). Eine serverseitige automatische Bildvorschau führte den entsprechenden Schadcode dann aus, ohne dass ein Anwender starten muss.

- Unternehmen überprüfen zwar häufig die Endungen ankommender und ausgehender Dateien, weniger Häufig deren Authentizität, fast nie deren weitere Inhalte, die einfach abgetrennt werden können.

- Ausführbare Programme können jedoch z.B. wie durch Marcus Murray auf der RSA 2015 bewiesen **in Bilddateien (z.B. JPEG)** versteckt sein - und damit unbemerkt Schaden anrichten.

itWatch GmbH

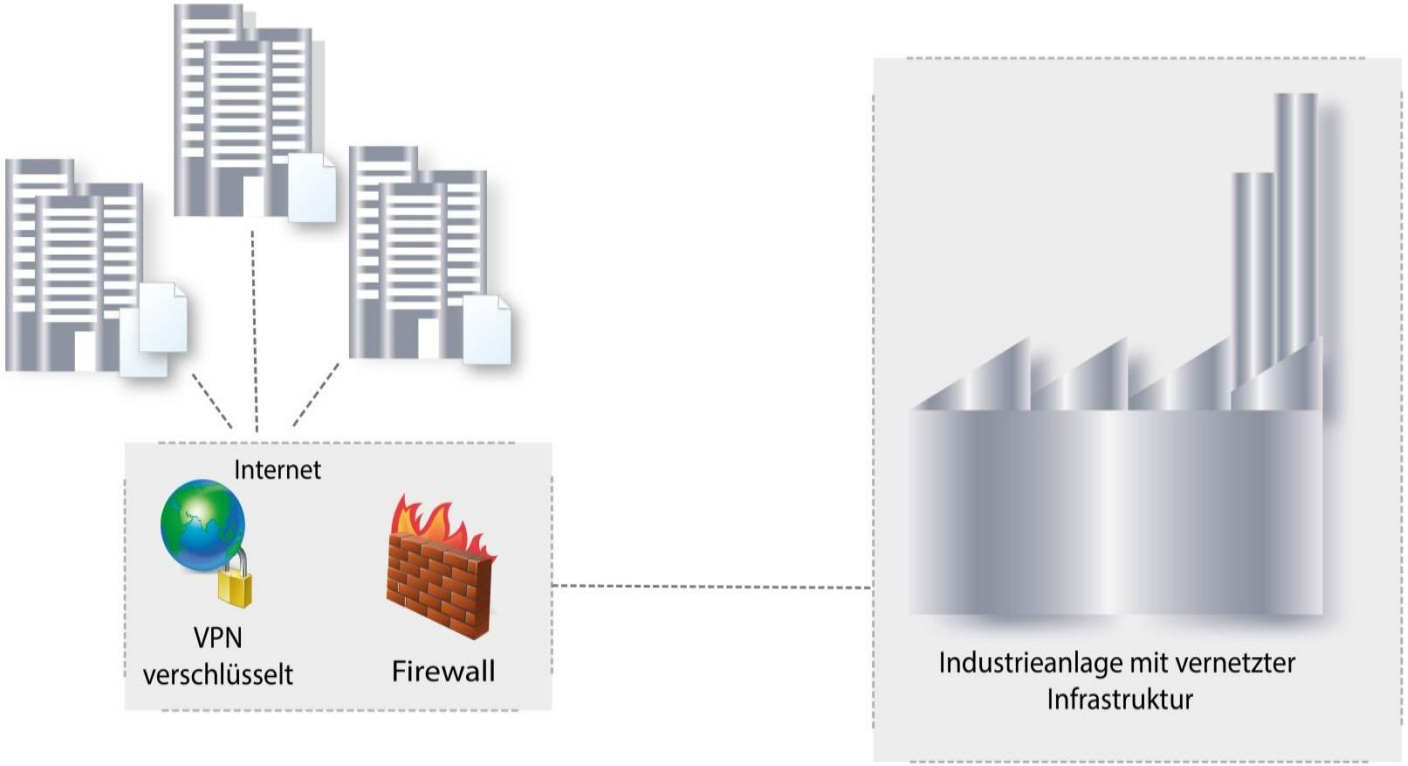
Safety - Konvergenz Shop & Office-Floor – welche Rolle spielt die Verlässlichkeit / Sicherheit der IT?

Bedrohungen in Industrie 4.0 Szenarien – was ist anders?

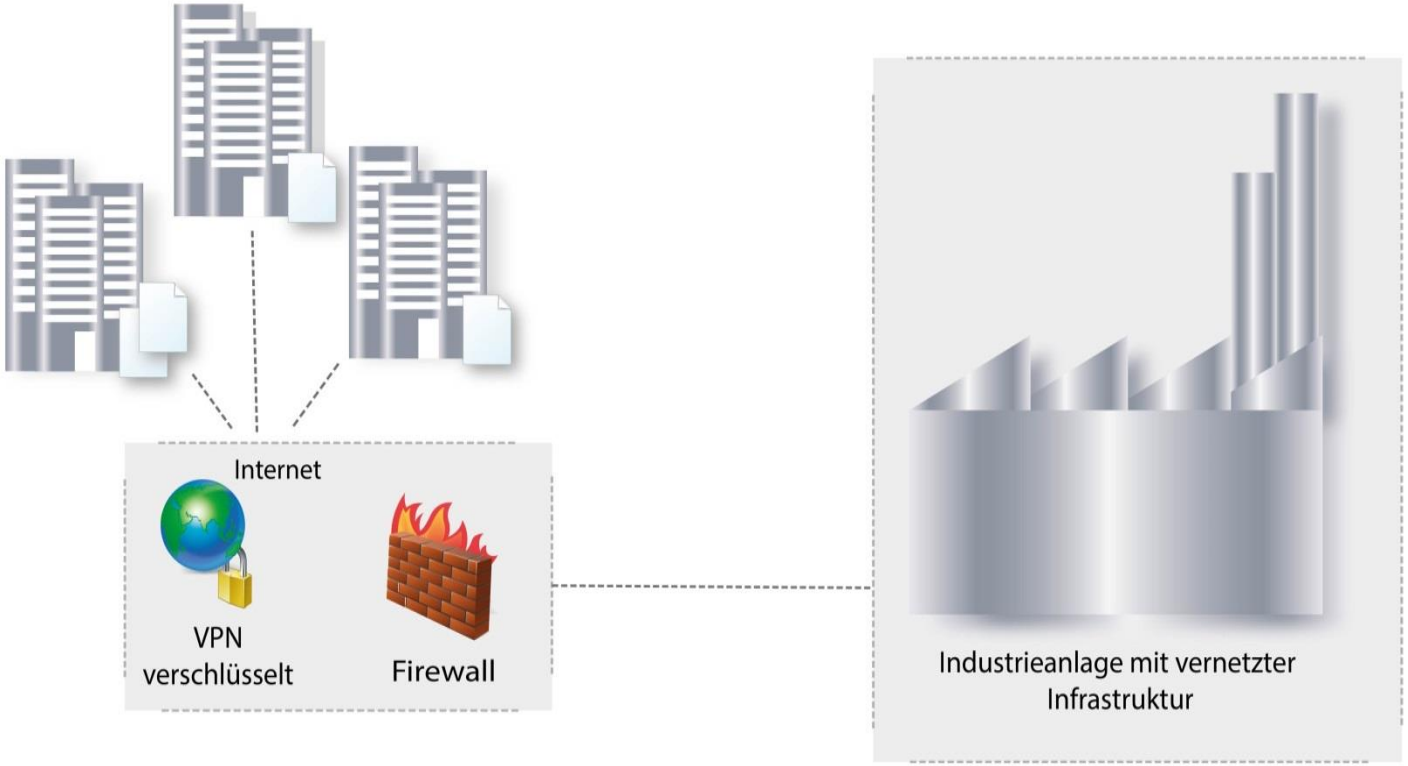
Wo stehen wir?

Strategien zur Verteidigung – Angriffs-robuste Architekturen – Betrachtung vollständiger Vertrauensketten

Ist- Stand Lösung – Bsp. Industrie



Ist- Stand Lösung



- Gibt es in der aktuellen Architektur eine Vertrauenskette?
- Ist diese lückenlos?
- Was tun wir gegen die Lücken?

itWatch GmbH

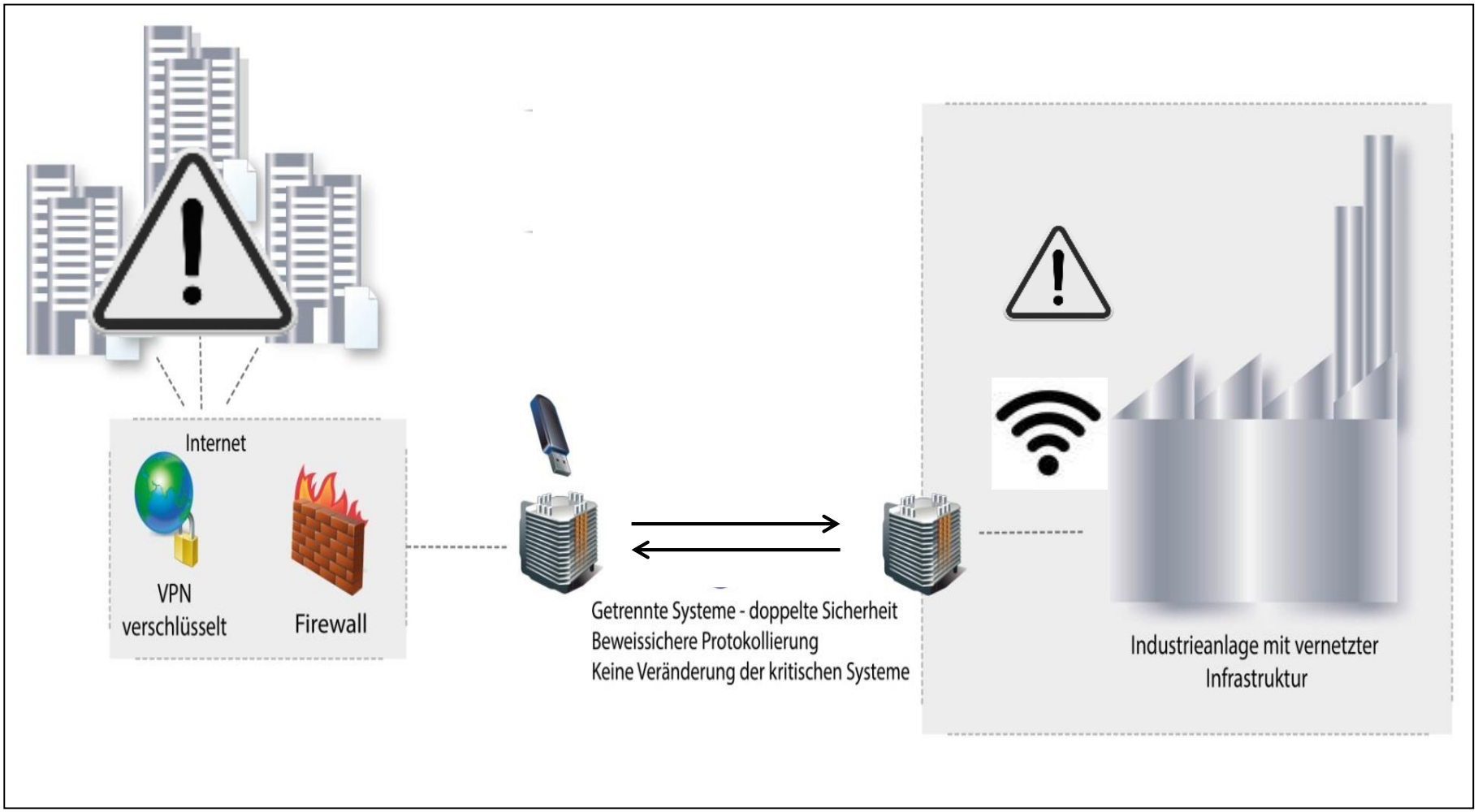
Safety - Konvergenz Shop & Office-Floor – welche Rolle spielt die Verlässlichkeit / Sicherheit der IT?

Bedrohungen in Industrie 4.0 Szenarien – was ist anders

Wo stehen wir?

Strategien zur Verteidigung – Angriffs-robuste Architekturen – Betrachtung vollständiger Vertrauensketten

Lösung



Lösung – zusätzlich zu den bekannten

- Gehärteter Client unter Kontrolle des Systembetreibers mit folgendem Ziel
  - Beweissicherung bereits am Point of Action
  - Schutz vor Infiltration durch unsichere Netze des Partners
  - Schutz vor MAC-Spoofing und vielen anderen Angriffen zur Übernahme von authentisierten Sessions
- Netztrennung durch Virtualisierung
- Einfügen einer virtuellen Schleuse vor sicherheitskritischen Netzteilen:
  - Inhaltlicher Kontrolle
  - Protokollierung
  - Vertraulichkeit
  - Integrität
- USB und physikalische Schnittstellen absichern
- Funksteuerung schützen gegen Jammer und dedizierte Angriffe

Lösung - beispielhaft

Fernzugriff (Remote Admin)

- gehärteter Client mit VPN, keine DMA, BadUSB … Angriffe
- mit geeigneter Schutz Policy und Monitoring
- wird als bootfähiges Device mit Sicherheitsmerkmalen zur Authentisierung an den Remote Admin verteilt.
- Viele Sicherheitsfeatures:
  - Handshake gegenseitig authentisiert
  - beim booten werden alle "überflüssigen" Devices geblockt, der VPN Tunnel im Systemmodus aufgebaut, ohne dass der Anwender sie verändern kann
  - Datenaustausch über protokollierte und inhaltskontrollierte Schleusenfunktion
- zulässig sind Datentransfers der definierten Fachanwendungsdaten in verschlüsselter Form auf definierte oder beliebige Memorysticks (content-abhängig)
- Zur Bearbeitung der Daten stehen definierte Geräte (Drucker, Scanner, Biometrie) zur Verfügung, nicht gelistete Geräte sind nicht erlaubt.

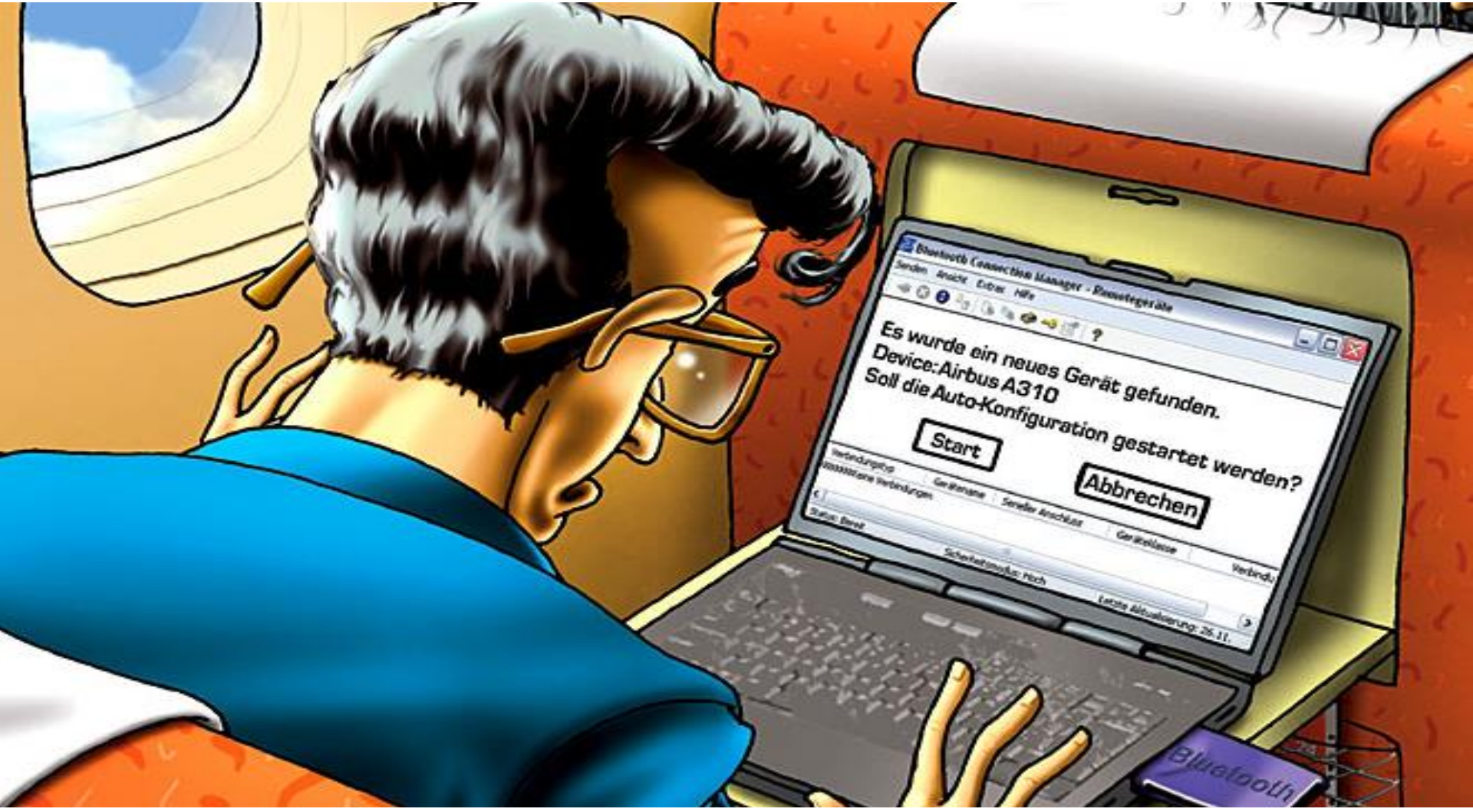
Lösung - beispielhaft

Technologie der virtuellen Schleuse:

- Transparenter Datentransfer nach Erfüllung folgender Anforderungen:
  - Inhaltlicher Kontrolle
  - Protokollierung
  - Verschlüsselter Transport
  - Integritätsschutz
- schützt Systeme vor:
  - Schadcode
  - Angriffen aus anderen Netzsegmenten (u.a. Internet)
- Wird für ICS zwischen System und Wartungsrechner gebracht
  - Schleusensystem selektiert Inhalte für die ICS

Besten Dank für Ihre Aufmerksamkeit

itWatch GmbH



Besuchen Sie uns: Halle 12, Stand 301