TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT-Workshop "Industrial Security" 2015

München, 11.06.2015

Separierung/Isolation

Steffen Heyde
secunet

Premium IT-Sicherheit Made in Germany von secunet

- führender Spezialist für innovative und anspruchsvolle IT-Sicherheit
- Erfahrung und Expertise aus über 5.000 namhaften, nationalen und internationalen Referenzprojekten über alle Branchen
- Vom BSI zertifizierter IT-Sicherheitsdienstleister
- Sicherheitspartner der Bundesrepublik Deutschland

Agenda

1. **Warum? Zusammenspiel der Anwendungen und Netze von unterschiedlichen Partnern mit ggf. unterschiedlichem Schutzbedarf**

2. Maßnahmen für eine sichere Separierung / Isolation

3. Grundprinzipien: Netzwerksegmentierung, Datendioden, sichere Ausführungsebenen und deren Zusammenwirken

4. Anwendungsfall "Digitale Fabrik"

Fabrik – gestern und morgen

- Reine SCADA-Systeme
- Wenige definierte Schnittstellen
- Keine / wenige Office-IT
- Wenig änderbare Funktionalität (Massenproduktion)
- Wenig Steuerungsfunktionalität
- Wenig Abhängigkeiten von Dritten

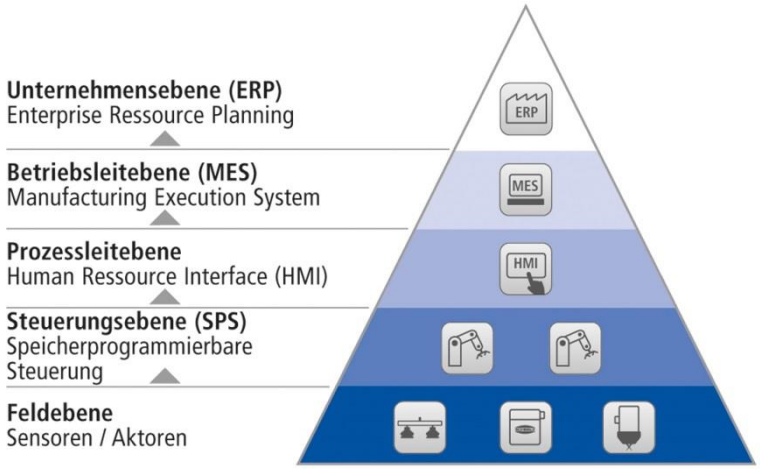
- Erweiterte Funktionalität
- Viele Schnittstellen
- IT-Systeme (DBMS, Applikationen, …)
- Zugriff von Office-IT auf Prozess-IT und umgekehrt
- Kommunikation zu externen Komponenten und Dritten
- Vielzahl an Protokollen

secunet

Warum Separierung / Isolation

Derzeit:

- Existierende Insellösungen (ggf. einzelner Hersteller)
- Separierung durch Nicht-Existenz von Schnittstellen
- Vereinzelt: Fernwartung, Fernsteuerung



Bei Industrie 4.0:

- Datenkommunikation von Marktplattformen über ERP bis zum Bussystem
- Einbindung von Zulieferer- und Logistik/Transport-Plattformen
- Schaffung neuer Separierung mit dedizierten Schnittstellen

Mit Vernetzung entstehen neue Bedrohungen

secunet

Unterschiedlicher Schutzbedarf - Beispiele

- Entwicklungsbereich
  - 1. Know-How sichern – Vertraulichkeit
- Produktionsbereich
  - 1. Safety und Verfügbarkeit sichern
  - 2. Daten vor Manipulationen sichern (Integrität, Authentizität)
  - 3. Vertraulichkeit von Programmen und Log-Daten der einzelnen Maschinen sichern
- Enterprise Ressource Planning bzw. auch Office-IT
  - 1. Daten vor unbefugten Zugriff sichern (Vertraulichkeit)
  - 2. Daten vor Manipulationen sichern

Unterschiedliche Schutzniveaus bzw. Sicherheitsklassen

secunet

Agenda

1. Warum? Zusammenspiel der Anwendungen und Netze von unterschiedlichen Partnern mit ggf. unterschiedlichem Schutzbedarf

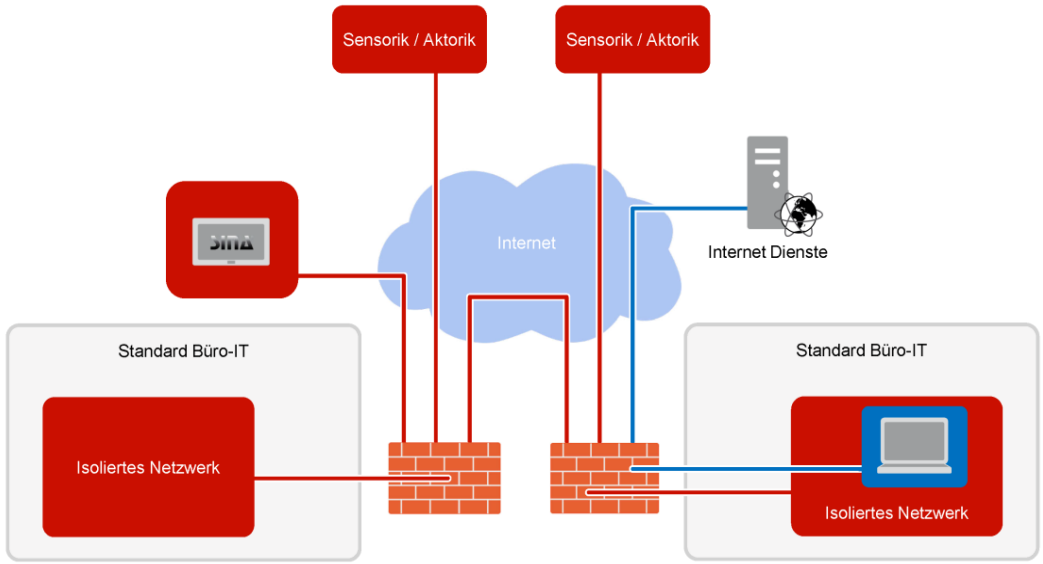
2. **Maßnahmen für eine sichere Separierung / Isolation**

3. Grundprinzipien: Netzwerksegmentierung, Datendioden, sichere Ausführungsebenen und deren Zusammenwirken

4. Anwendungsfall "Digitale Fabrik"

Security by Isolation / Separation

- ***Sichere*** …
  - Netzwerksegmentierung
  - Netzwerkübergänge für Datentransfer
  - Authentisierung der Devices und Nutzer
  - Authentifizierung
  - Autorisierung
  - Boot-Prozesse
  - Verschlüsselung von Daten und Kommunikation
  - Ausführungsebenen
  - Kapselung von Ausführungsebenen für unterschiedliche Sicherheitsniveaus
  - Umsetzung eines zentralen User-, Konfigurations- und Device Managements



mit Hilfe sicherer Virtualisierung im Netzwerk und auf dem Device

secunet

Agenda

1. Warum? Zusammenspiel der Anwendungen und Netze von unterschiedlichen Partnern mit ggf. unterschiedlichem Schutzbedarf

2. Maßnahmen für eine sichere Separierung / Isolation

3. **Grundprinzipien: Netzwerksegmentierung, Datendioden, sichere Ausführungsebenen und deren Zusammenwirken**

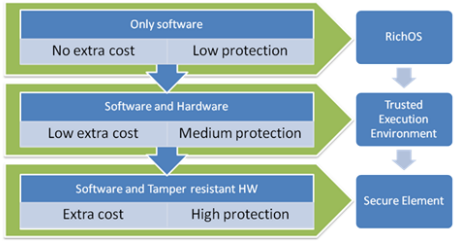
4. Anwendungsfall "Digitale Fabrik"

Grundprinzipien

- Netzwerksegmentierung
  - » Unterschiedliche Bereiche in unterschiedlichen Netzwerksegmenten z.B. Office-IT, Leitstand, …

- Datendioden
  - » Kommunikation ist nur in eine Kommunikationsrichtung möglich

- sichere Ausführungsebenen
  - » Sichere Ausführung von Applikationen und sichere Verarbeitung von Daten



- deren Zusammenwirken
  - » durch eine gesicherte Kommunikation
    - » zwischen der sicheren Ausführungsebene und einem Netzwerksegment (SINA VW und SINA-Box)
    - » zwischen Netzwerksegmenten mit gleichem Sicherheitsniveau (SINA-Box Layer 3/2)
    - » zwischen 2 Netzwerksegmenten mit unterschiedlichen Sicherheitsniveaus (z.B. SINA One Way)

secunet

Agenda

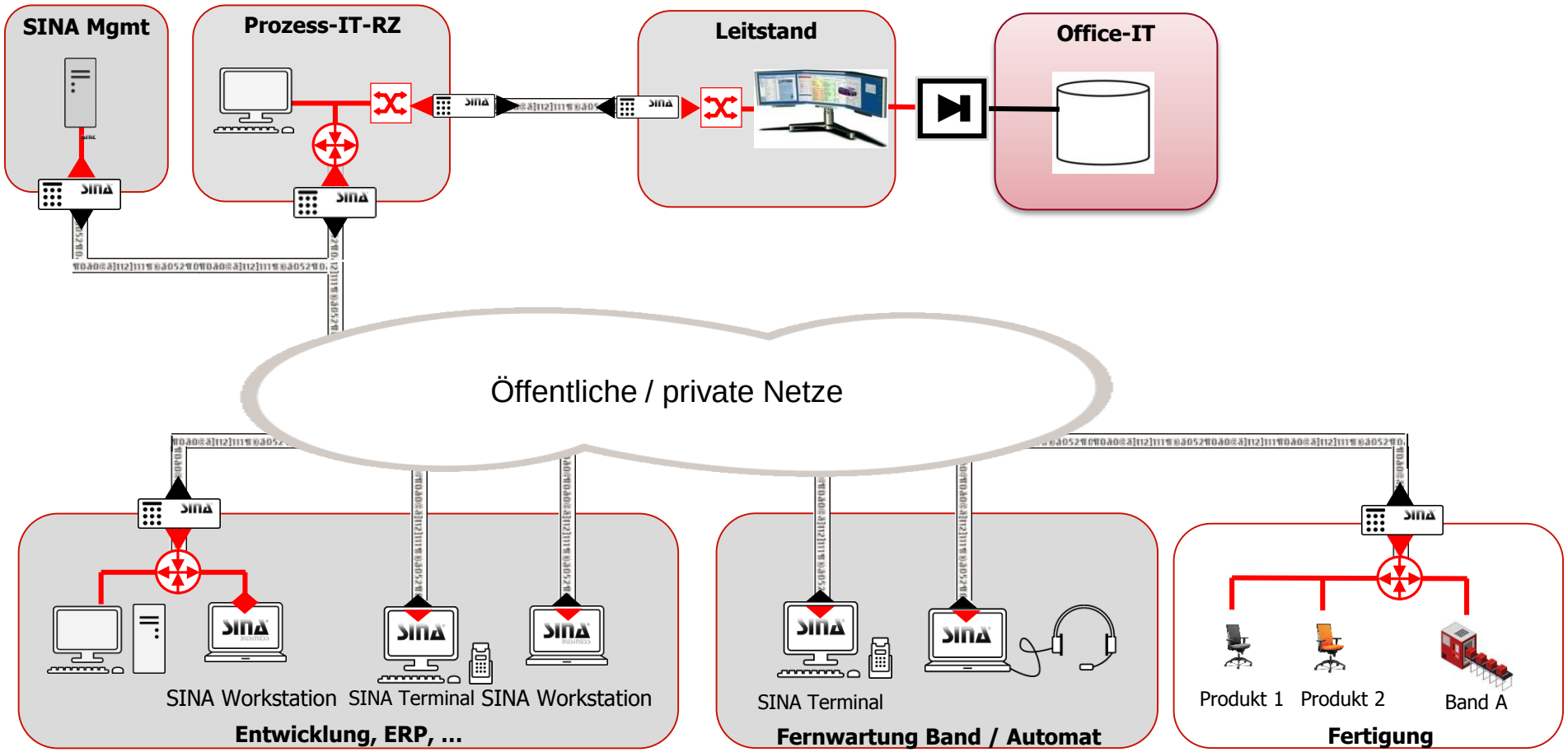
1. Warum? Zusammenspiel der Anwendungen und Netze von unterschiedlichen Partnern mit ggf. unterschiedlichem Schutzbedarf

2. Maßnahmen für eine sichere Separierung / Isolation

3. Grundprinzipien: Netzwerksegmentierung, Datendioden, sichere Ausführungsebenen und deren Zusammenwirken

4. **Anwendungsfall "Digitale Fabrik"**

Beispiel: Anwendungsfall Digitale Fabrik



secunet

secunet

secunet Security Networks AG

Steffen Heyde

Kronprinzenstraße 30
45128 Essen
Tel.: +49-201-5454-2025
Mobil: +49-160-4720676
steffen.heyde@secunet.com
www.secunet.com