TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT-Workshop "Industrial Security" 2015

München, 11.06.2015

ICS Security Kompendium
und industriespezifische Konzepte und Technologien zur Separierung / Isolation

Markus Bartsch
TÜViT

KRITIS (1)
„Kritische Infrastrukturen”

Bundesamt für Sicherheit in der Informationstechnik

Sektoren & Branchen

Transport / Verkehr
- Luftfahrt
- Seeschifffahrt
- Binnenschifffahrt
- Schienenverkehr
- Straßenverkehr
- Logistik

Energie
- Elektrizität
- Gas
- Mineralöl

Staat und Verwaltung
- Regierung / Verwaltung
- Parlament
- Justizeinrichtungen
- Notfall-, Rettungswesen Katastrophenschutz

IKT
- Telekommunikation
- Informationstechnik

Medien und Kultur
- Rundfunk (Fernsehen und Radio), gedruckte und elektronische Kulturgut
- symbolträchtige Bauwerke

Wasser
- Wasserversorgung
- Abwasserbeseitigung

Ernährung
- Ernährungswirtschaft
- Lebensmittelhandel

Gesundheit
- Medizinische Versorgung
- Arzneimittel / Impfstoffe
- Labore

Finanz-, Versicherungs-wesen
- Banken
- Börsen
- Versicherungen
- Finanzdienstleister

KRITIS (2)
Standards, Studien und Testmethoden

Sektoren & Branchen

Transport / Verkehr
ISO 270xx
IT-Grundschutz
Common Criteria
DO-178B SIW
ARINC
ICS Sec. Komp.

Energie
VGB S175
ISO 27019
IT-Grundschutz
IEC 62351 / **62443**
NISTIR 7628
Namur NA115
Common Criteria
ICS Sec. Komp.

Staat und Verwaltung
IT-Grundschutz
ISO 27001
Common Criteria
Techn. Richtlinien
…

IKT
ISO 270xx
ITSEC
Common Criteria (ISO 15408)
FIPS 140-2
Techn. Richtlinien

Medien und Kultur
?

Wasser
DWA M 145/151/207/253
IT-Grundschutz

Ernährung
?

Gesundheit
Common Criteria
Techn. Richtlinien

Finanz-, Versicherungs-wesen
DK
EMVCo
PCI
…

KRITIS (3)
deutsche Standards, Studien und Testmethoden

Sektoren & Branchen

Transport / Verkehr

ISO
IT-Gr
Common Crite
DO-178B SIW
ARINC
ICS Sec.

Staat und Verwaltung

IT-Grundschutz
ISO 27001
Common Criteria
Techn. Richtlinien
…

IKT

ISO 270xx
ITSEC
Common
(ISO 154
FIPS 140
Techn. R

Medien und Kultur

?

asser

A M 145/151/207/253
T-Grund

Ern

?

Gesundheit

Common Criteria
Techn. Richtlinien

Finanz-, Versicherungs-wesen

DK
EMVCo
PCI
…

ICS Security Kompendium
Zweck und Zielgruppe

- **Grundlagenwerk**
- **IT-Grundschutz-Bezug**
- Vorstellung von **Best Practices**
- **Audit-Methodik**
- **Ausblick**

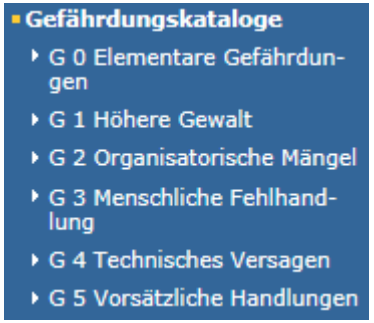
Bundesamt für Sicherheit in der Informationstechnik

Das ICS-Security-Kompendium bildet einen allgemeinen **Rahmen** für die verschiedenen Anwendungsbereiche industrieller Steuerungssysteme. Ein solches **Grundlagenwerk** kann natürlich nicht auf alle Spezifika der unterschiedlichen Industriesektoren detailliert eingehen. Daher ist das Kompendium als Aufforderung an die jeweiligen Verbände und Organisationen zu verstehen, auf dieser Grundlage **eigene, sektorenspezifische Ausprägungen oder Präzisierungen** des Kompendiums zu erstellen und dabei die jeweils geltenden Besonderheiten im Detail zu erläutern. Nur so ist es möglich, die industriespezifischen Grundlagen passgenau für bestimmte **Anwendungsbereiche** darzustellen.

Das Kompendium richtet sich primär an **Betreiber** und macht auf das Thema IT-Security aufmerksam. Die Implementierung von IT-Security in Form der erarbeiteten Best Practices führt zu einer Risikominderung in ICS.

Kapitel 3: Gefährdungen der IT Security
angelehnt an die IT-Grundschutz-Kataloge des BSI

1. **Organisatorische Gefährdungen**
   1. Unzureichende Regelungen zur IT-Security
   2. Unzureichende Dokumentation
   3. Unvollständige Absicherung der Fernwartungszugänge
   4. Einsatz von Standard-IT-Komponenten *(COTS)* mit bereits identifizierten Schwachstellen
   5. Fehlende Überwachung der unterstützenden Infrastruktur
   6. Abhängigkeiten des ICS-Netzes von IT-Netzen
2. **Menschliche Fehlhandlungen**
   1. Unzureichende Absicherung oder zu weitreichende Vernetzung
   2. Mangelhafte Konfigurationen von Komponenten
   3. Fehlende Backups
   4. Mobile Datenträger und Laptops
   5. Unzureichende Validierung von Eingaben und Ausgaben
3. **Vorsätzliche Handlungen**
   1. Kommunikation von Mess- und Steuerwerten *(Klartext)*
   2. Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen
   3. Systematische Schwachstellensuche über das Netzwerk *(Pentests)*
   4. Denial-of-Service-Angriffe (DoS)
   5. Man-in-the-Middle-Angriff
   6. Phishing
   7. Injection-Angriffe
   8. Cross-Site-Scripting *(XSS)*
   9. Drive-By-Downloads
   10. Schadsoftware auf EWS *(Engineering-Workstations)*
   11. Schadprogramme *(aus Office-IT)*
   12. Replay-Angriff
   13. Physischer Angriff zur Provokation administrativer Eingriffe



Top 10

1. Unberechtigte Nutzung von **Fernwartung**szugängen
2. Online-Angriff über **Unternehmens-IT**
3. Angriffe auf eingesetzte COTS-Produkte in der Prozess-IT
4. (D)**DoS**-Angriffe
5. Menschliches Fehlverhalten und **Sabotage**
6. Einschleusen von Schadcode über **Wechseldatenträger** und **externe Hardware**
7. Lesen und Schreiben von **Nachrichten** in der Prozess-IT
8. Unberechtigter **Zugriff** auf Ressourcen
9. Angriffe auf **Netzwerkkomponenten**
10. **Technisches** Fehlverhalten und höhere Gewalt

Kapitel 5: Best Practices für Betreiber (1)

1. Grundsätzliches Vorgehen im Engineering-Prozess
2. Einstieg

3. Security-spezifische **Prozesse / Richtlinien**
   1. Security Management
   2. Technische Dokumentation
   3. Durchgängiges Management aller ICS-Komponenten
   4. Notfallmanagement
   5. Personal
   6. Revision & Tests

4. *Auswahl verwendeter **Systeme/Komponenten** sowie **Dienstleister/Integratoren***
   1. Vertrauenswürdigkeit
   2. IT-Security-Merkmale von ICS-Komponenten
   3. Kompatibilität eingesetzter Technologien zu Standards
   4. Inbetriebnahme in sicherer Konfiguration
   5. Soft- und Hardware Support
   6. **Fernwartung durch Hersteller und Integrator**
   7. **Absicherung von Feldgeräten**

Kapitel 5: Best Practices für Betreiber (2)

5. Bauliche und **physische Absicherung**

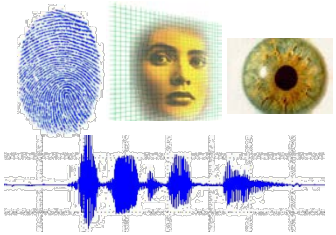
6. Technische **Maßnahmen**
   1. **Absicherung der Netze**
   2. **Absicherung von Diensten und Protokollen**
   3. Härtung der IT-Systeme
   4. Patchmanagement
   5. **Authentisierung**
   6. **Zugriffskontrolle**
   7. Schutz vor Schadprogrammen
   8. Mobile Datenträger
   9. Datensicherung
   10. Protokollierung und Auswertung

7. **Gegenüberstellung** mit vorhandenen Standards

Lösungsansätze
Security-by-Design → Basistechnologien

- (authentifizierbare) **Id**entitäten

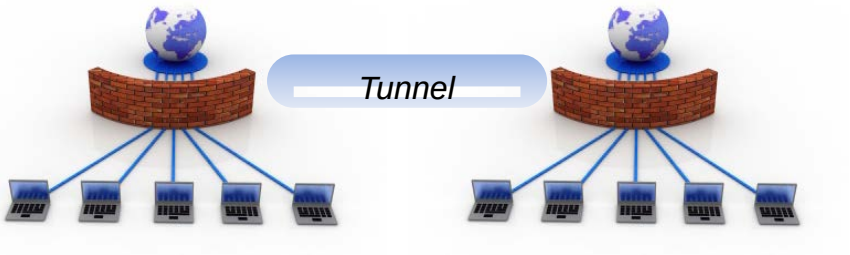
Personen



Geräte

→ M2M

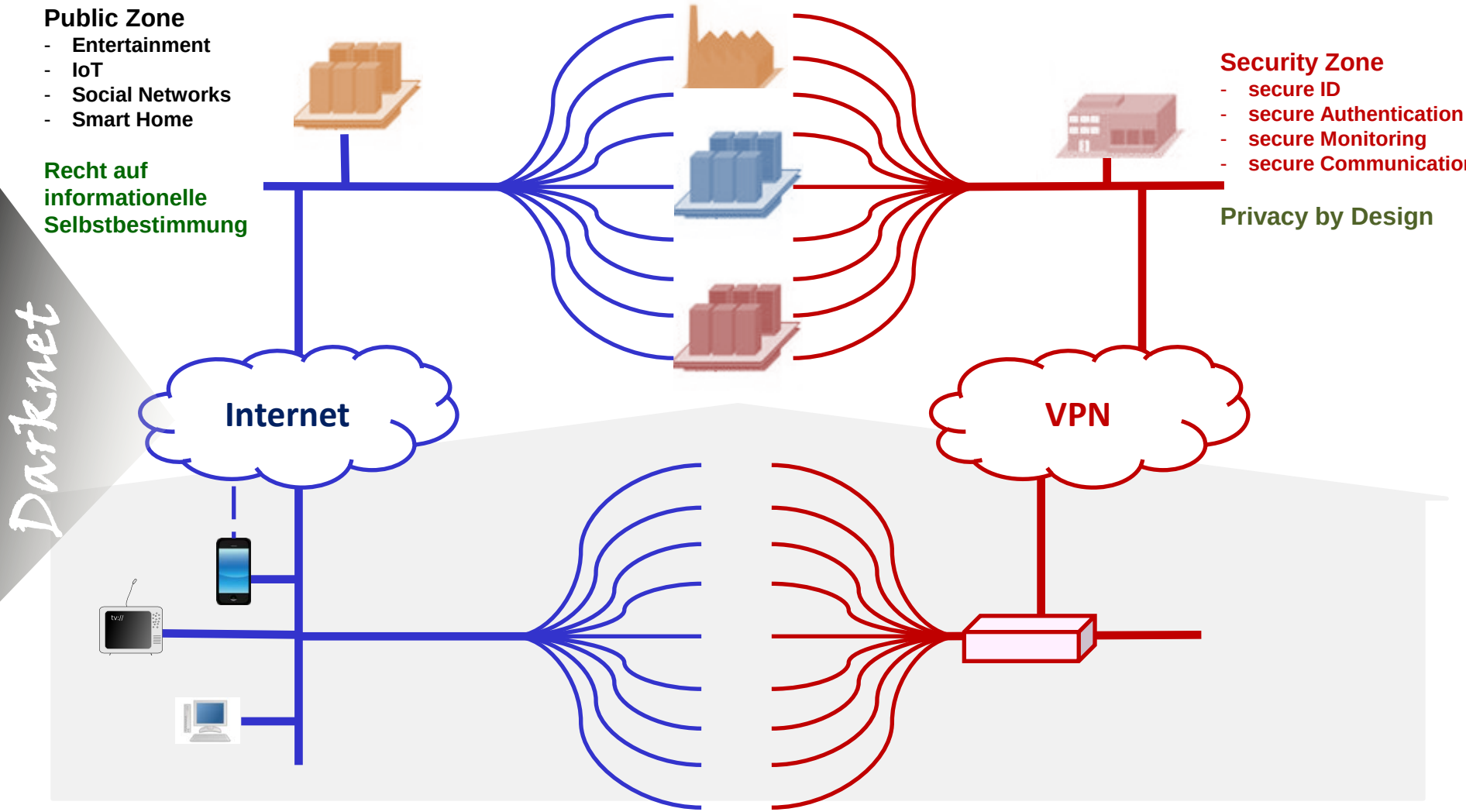
- **Separierung**



Security Zone (1)
generisch

Public Zone
- Entertainment
- IoT
- Social Networks
- Smart Home

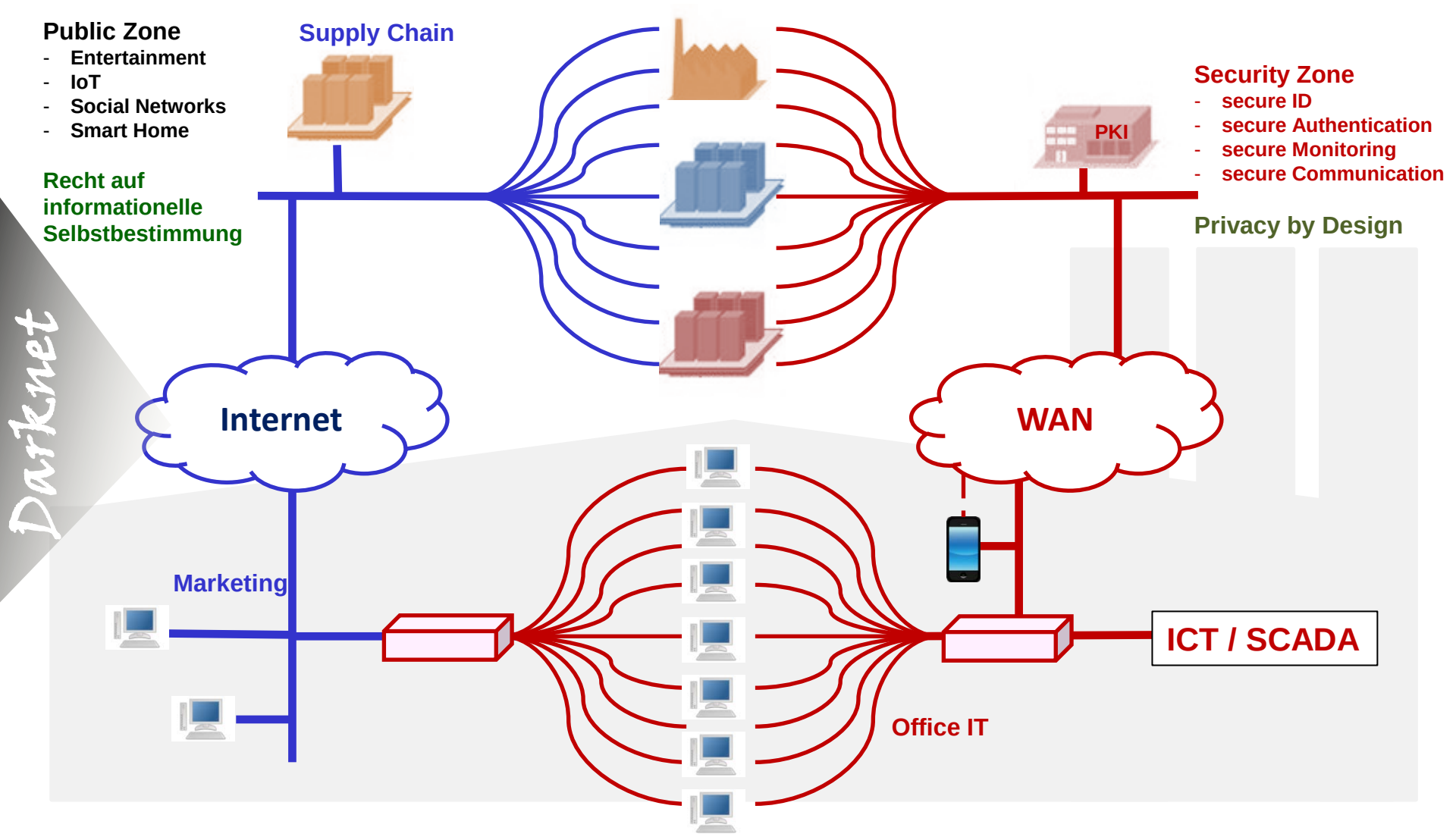
Recht auf informationelle Selbstbestimmung



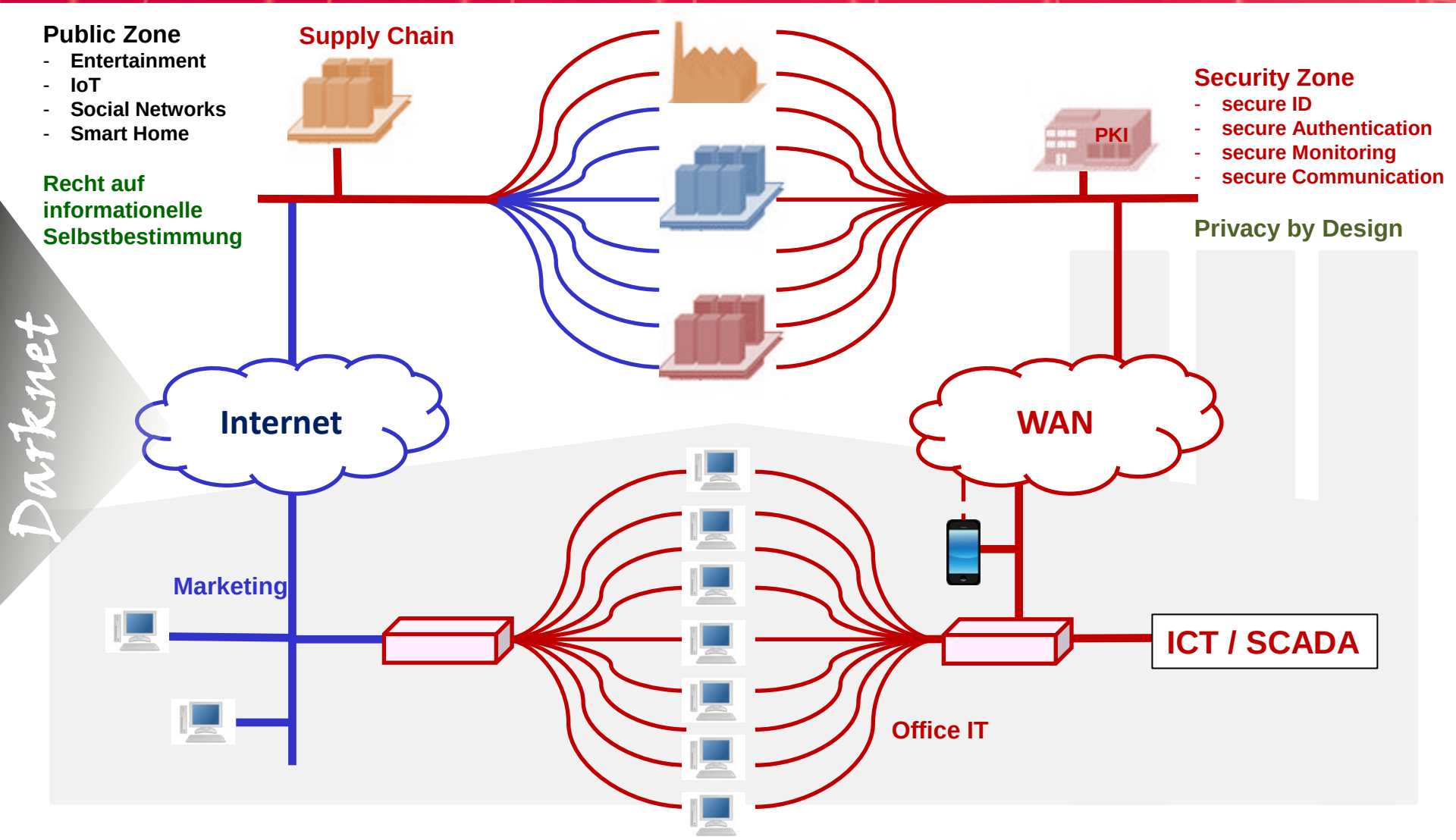
Security Zone
- secure ID
- secure Authentication
- secure Monitoring
- secure Communication

Privacy by Design

Security Zone (2a)
Industrie



Security Zone (2b)
Industrie



Vielen Dank!

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD

Markus Bartsch
IT Security

Langemarckstr. 20
45141 Essen
Germany

Phone: +49 201 8999 – 616
Fax: +49 201 8999 – 666
E-Mail: m.bartsch@tuvit.de
URL: www.tuvit.de

Quellen des BSI:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/inhalt_node.html
https://www.bsi.bund.de/DE/Themen/weitereThemen/ICS-Security/Empfehlungen/Empfehlungen_node.html