

TeleTrust-interner Workshop

Essen, 29./30.06.2017

Herausforderungen der Digitalisierung für die IT-Sicherheit

Bernd Kowalski

Bundesamt für Sicherheit in der Informationstechnik

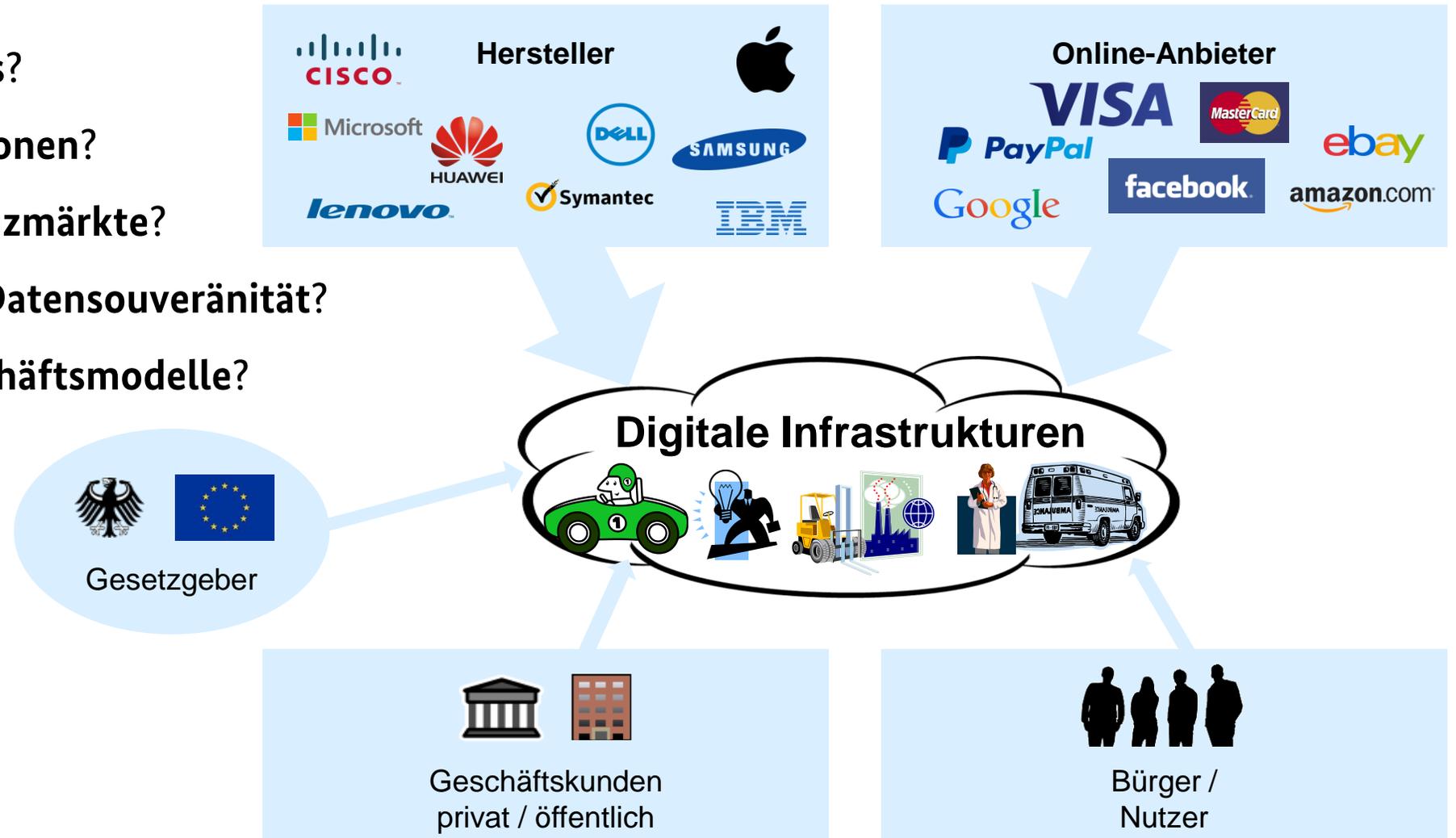
Abteilungspräsident der Abteilung D

Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung

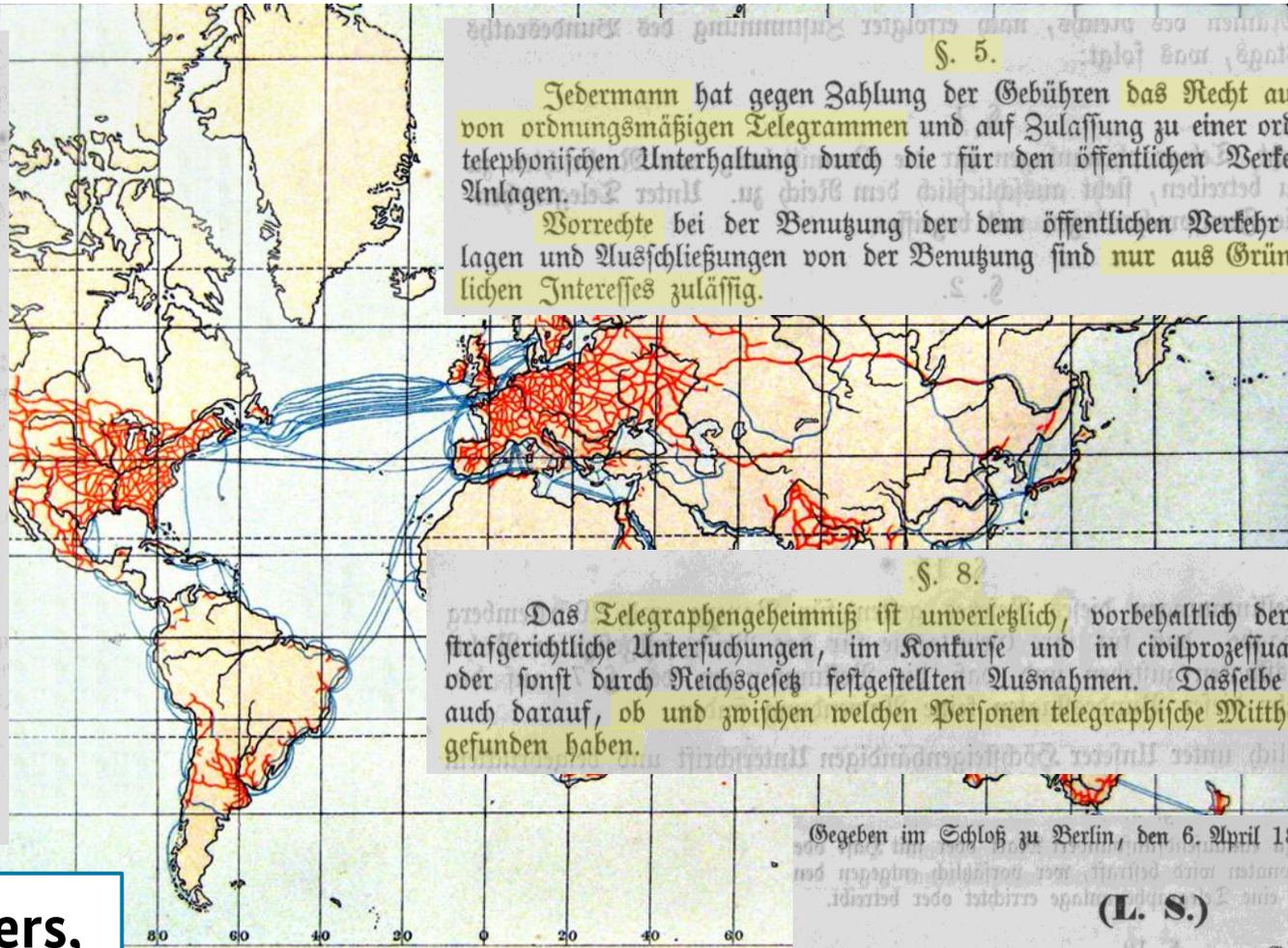
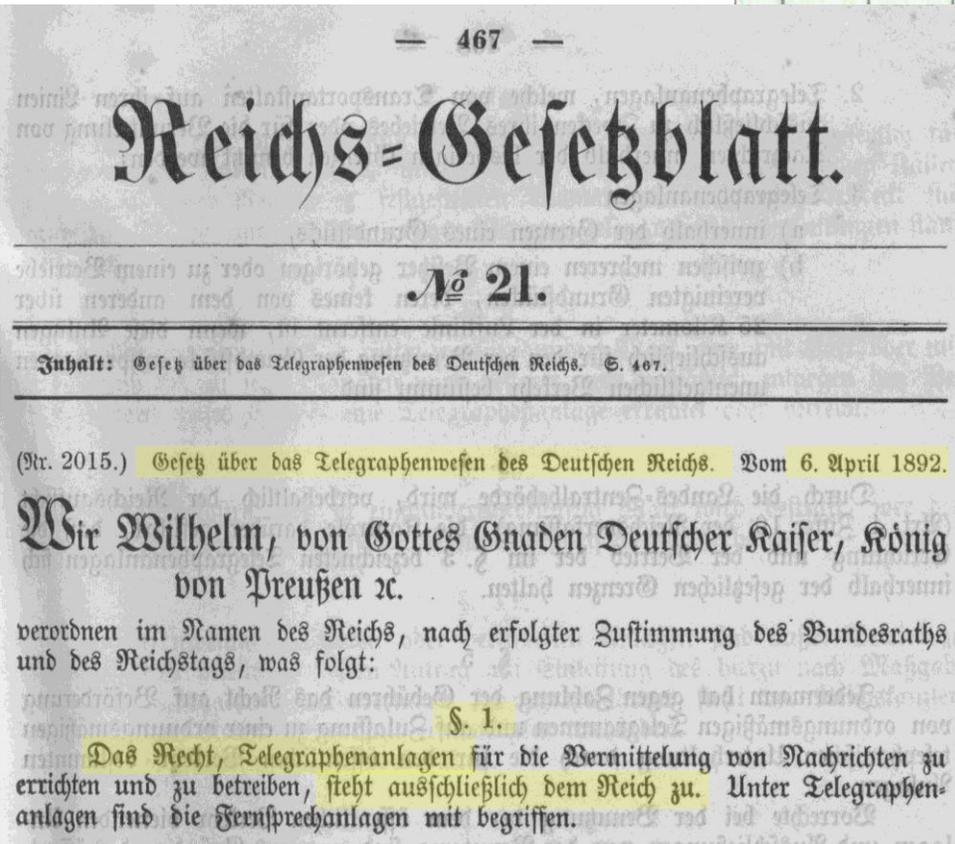
Digitalisierung gestalten!

... aber:

- Wer setzt die **Standards**?
- Wer treibt die **Innovationen**?
- Wer schafft die **Referenzmärkte**?
- Wer gewährleistet die **Datensouveränität**?
- Wer bestimmt die **Geschäftsmodelle**?



Vor 125 Jahren: Telegraphengesetz – „1. Digitalisierungsgesetz“



**Was ist heute anders,
was vergleichbar?**

Eisenbahnen- und Telegraphendichte der Erde.

Eisenbahnen Telegraphen

Gestaltungsrahmen des BSI in der Digitalisierungspolitik

Auf Basis des
BSIG

Gesetzgebung
Rechtlicher Rahmen
und Steuerungsanreize



**IT-Sicherheitsanforderungen
an
IT-Sicherheitsprodukte,
Infrastrukturen und Dienste**

Zertifizierung
Sichtbare IT-Sicherheit und
Datenschutz schaffen
Vertrauen in der Digitalisierung

Standardisierung
Eingebaute Sicherheit
(*security by design*),
bedarfsorientiert und
mit Unterstützung
der Wirtschaft



Digitalisierungspolitik

Auftrag der **Digitalen Agenda**

Digitalisierung, Automation, Vernetzung in allen Lebensbereichen:

- Smart Grid, Smart Metering (KRITIS)
- Smart Home, Smart Services
- Industrie 4.0 / Fernwartung
- eMobility / Car-to-Car / Car-to-X
- eHealth / eGovernment
- Cloud Computing
- eID / ePayment
- eCommerce
- Big Data



Verfügbarkeit, Vertrauenswürdigkeit, Transparenz

Europäischer Rahmen der Digitalisierungspolitik

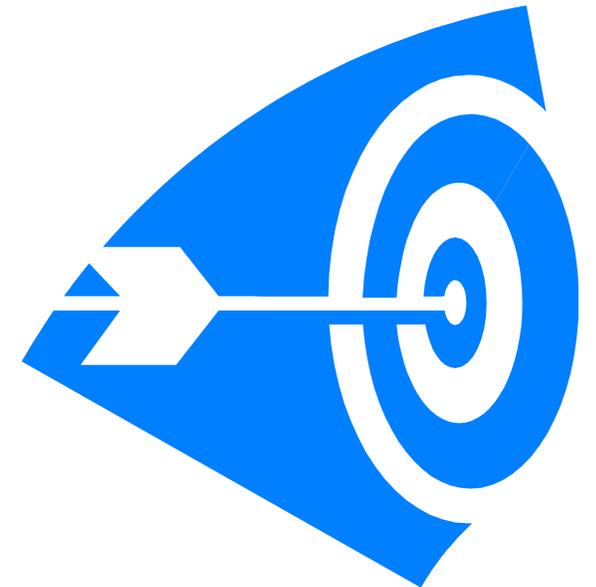
- **EU-KOM** Strategie für einen **Digitalen Binnenmarkt** COM(2015) 192
 - Europäische **Grundwerte**: Freiheitsrechte der Bürger
 - Sichere **eID und Vertrauensdienste** in allen Digitalisierungsbereichen
 - **Europäischer Rechtsrahmen**: eIDAS-VO, PSD2, DSGVO
- **ECIL** (European Cybersecurity Industry Leaders) Recommendations an Oettinger (Lille, 25. Jan. 2016)
 - Europäische **Zertifizierungs- und Standardisierungspolitik**
 - **Rechtsrahmen** in allen Digitalisierungsbereichen
 - „**security by design**“ und „**pre-market approval**“



Ziele

im Rahmen der Digitalisierungspolitik

- **Innovative Technologieentwicklung** mitgestalten
- Nutzung der **Digitalisierungsprojekte** für Industriekooperationen
- Stärkung der **Digitalen Souveränität**:
 - **Rechte des Bürgers** als Gewährleistungspflicht des Staates
 - Gestaltung und Durchsetzung **technischer Standards**
 - Erhaltung der **Regulierungshoheit** für IT-Sicherheit/Krypto



Handlungsbedarf im Rahmen der Digitalisierungspolitik

- Sicherheitstechnologien bereits in der Innovationsphase mitgestalten – **security by design**
- **Standardisierungs- und Zertifizierungspolitik** für alle Digitalisierungsbereiche
- **Referenzmärkte** schaffen:
 - **Investitionsanreize** setzen
 - **Technische Standards** entwickeln
 - **Europäische und/oder nationale Rechtsrahmen** setzen



Produktzertifizierungen im BSI

Technische Richtlinien und Schutzprofile

Gesetzliche Vorgaben
(z.B. EnWG, EEG)



**Technische
Prüfvorschrift**
(BSI TR / PP)

**Die Zertifizierung weist
nach, dass ein Produkt die
in den Rechtsvorschriften
geforderten technischen
Eigenschaften (TR, PP)
erfüllt.**

Konformitätsprüfung
private qualifizierte
Prüfstelle

Zertifizierung
BSI



Produktzertifizierung im BSI ... auf Nachfrage durch **Hersteller**



**Lesegeräte für
Chipkarten**



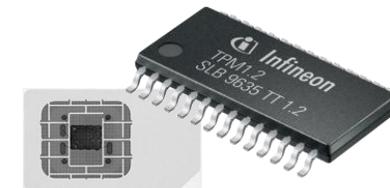
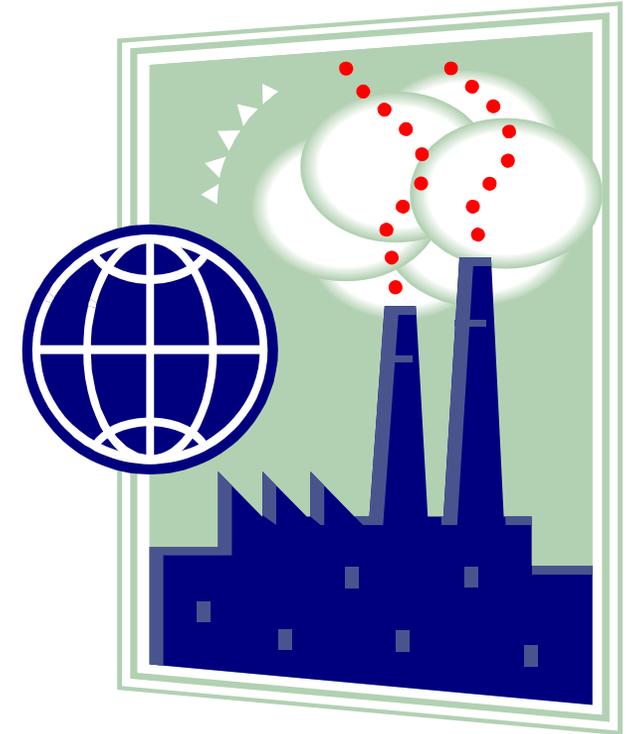
Speichernetzwerke
(z.B. Dell EqualLogic PS Series **Storage Array**)



Alle kommerziell relevanten
Datenbank- und Applikationssysteme
(z.B. Oracle, IBM, Microsoft, SAP, Red Hat)
und Server-Betriebssysteme
(z.B. z/OS, SUSE, Red Hat, AIX)



Hochresistente Firewalls
(z.B. genugate der genua mbH)



Sicherheitselemente
(z.B. Trusted Platform Module)

Produktzertifizierung im BSI

... auf Veranlassung durch Gesetzgeber / EU-Kommission



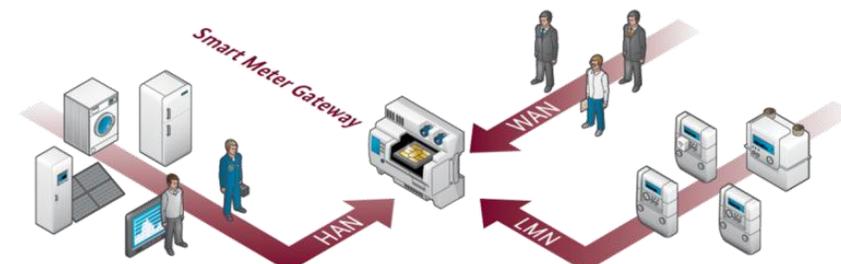
Gesundheitswesen
Elektronische Gesundheitskarte
Heilberufsausweis
Stationärer Kartenleser
Mobiler Kartenleser
Konnektor



Digitaler Tachograph (EUVO)

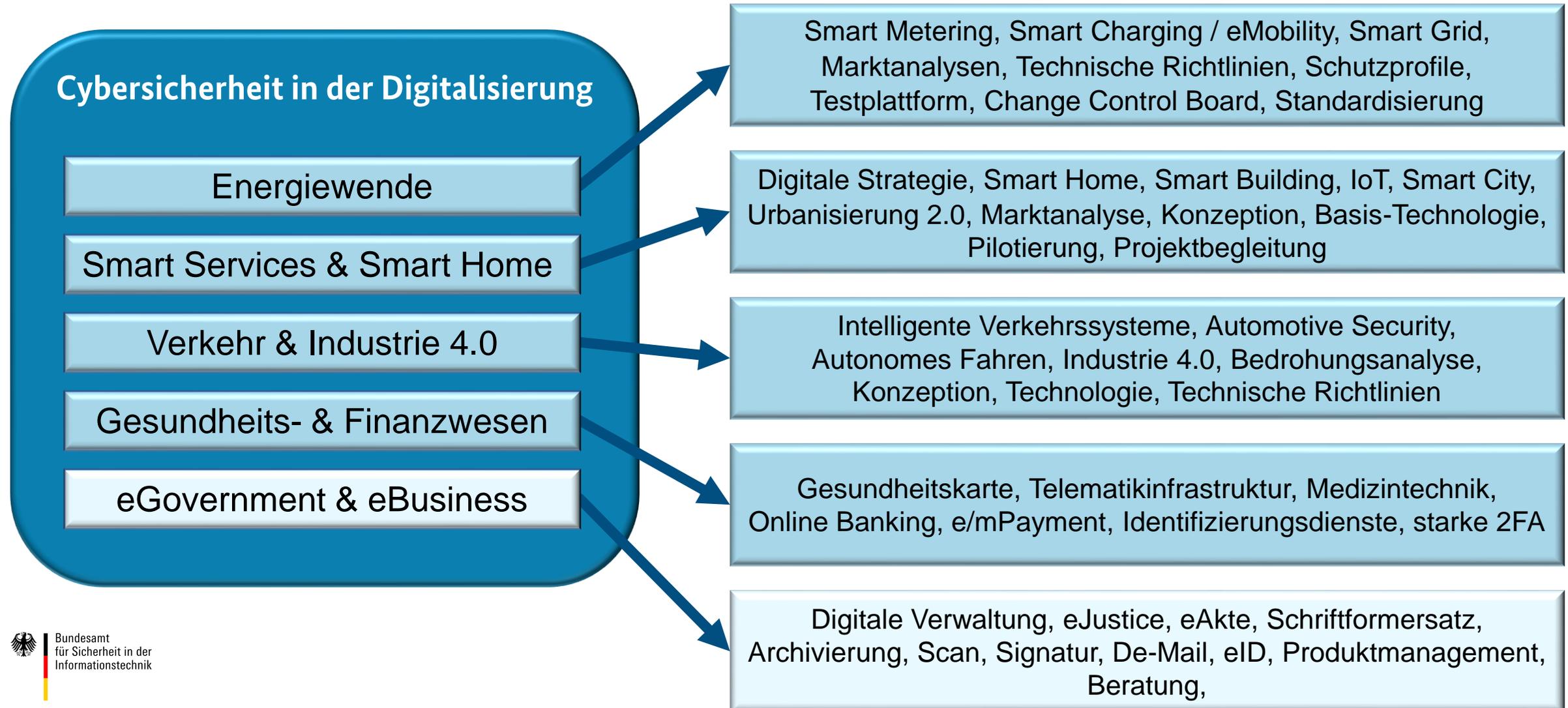


Elektronische Identitätsdokumente (ePass, nPA, eAT)



Smart Grid
(Sicherheitsmodul, Smart Meter Gateway)

Handlungsfelder, Vorhaben & Schwerpunkte im Rahmen der Digitalisierungspolitik



Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Bernd Kowalski

Abteilungspräsident

Abteilung D - Cyber-Sicherheit in der Digitalisierung, Zertifizierung und Standardisierung

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189

53175 Bonn

E-Mail: bernd.kowalski@bsi.bund.de

Telefon: +49 228 99 9582-5700

Fax: +49 228 99 10 9582-5700

Internet: www.bsi.bund.de



Backup

Neue Produktzertifizierung BSI

Basis-Zertifizierung, Ausgangslage

Basis-Zertifizierung, Pilotprojekt

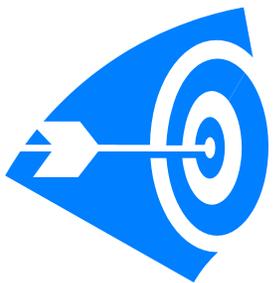
Neue Produktzertifizierung im BSI

Basis-Zertifizierung: Die Ausgangslage

Aktueller Stand

- **Unzureichende IT-Sicherheit** von COTS-/ Consumer-Produkten
 - IT-Sicherheitsniveau nicht ausgewiesen
 - wenige Consumerprodukte IT-sicherheitszertifiziert
- **Markteintrittsbarriere:** Herstellerdokumentation, Reifegrad der Entwicklungsprozesse

Idee: Basis-Zertifizierung mit geringen Dokumentationsanforderungen (Blackbox-Tests)



Zielgruppe

- Einsteiger in Zertifizierung, Start-Up geeignet
- Produkte mit schnellen Lebenszyklen: Router, Handys, SmartHome-Produkte, Apps , ...
- Industrie 4.0 (industrielle Steuerungsanlagen, IoT), Produkte für KRITIS-Betreiber
- Betreiber und Nutzer von COTS-Komponenten (Orientierungshilfe bei Einkauf)

Neue Produktzertifizierung im BSI

Basis-Zertifizierung: Pilotprojekt

Vorgehen

- Fundierte **Schwachstellenanalyse und Penetrationstests durch qualifizierte Stelle**
- Notwendiger **Umfang wird vorab festgelegt** (nach Produkt und Herstellerzulieferung ~ 25 PT)
- **Linearer Prozess:** kaum Nachforderungen, **fix planbar, Ergebnisse direkt verwertbar** (Pass oder Fail)



Unterschied zur CC

- **Vereinfachte Sicherheitsvorgaben** (ST, 10-15 Seiten)
- **Evaluierungsfokus auf Pentesting / Hacking**, keine Betrachtung des Lebenszyklus
- **Durchführung ohne Herstellerunterstützung** (Gegenstand Pilotprojekt)
- **Blackbox-Tests**
- **Keine weiteren Zusatzdokumente** (nur Ergebnisbericht, 80-100 Seiten)

Umsetzung im Pilotprojekt: Basis-IT-Sicherheits-Zertifizierung

- Einbindung aller Beteiligten (Abteilungen im BSI, internationale Partner, Hersteller)

Digitalisierungsprojekte des BSI

Energiewende

eHealth-Gesetz, Telematik-Infrastruktur

Intelligente Verkehrssysteme, autonomes Fahren

Digitalisierungsprojekte

Energiewende

- **Regulierung:**
 - Verabschiedung EnWG/MsbG in 6/2016
 - Rollout ab 1/2017, Testbetrieb läuft
- **Aufgabe BSI**
 - Technische Standards, Zertifizierung
 - Beratung Gesetzgeber
- **Hohe Relevanz für deutsche Industrie**
 - RWE, EnBW, EON u.a. als Messstellenbetreiber
 - NXP, TSI, Utimaco, mtg als IT-Sicherheitsindustrie
- **Perspektive: BSI-Smart Meter Gateway als Steuerelement**
 - für dezentrale Lasten, Erzeuger, Speicher
 - für zunächst Strom, später Gas, Wasser und Smart Home Anwendungen
- **Ausstattung BSI:**
 - 20,5 Mio € (2014 – 2019) durch BMWi
 - 30 Stellen ab 2017



Digitalisierungsprojekte

eHealth-Gesetz, Telematik-Infrastruktur

- **Elektronische Gesundheitskarte (eHealth-Gesetz in Q4/2015)**
- **Telematik-Infrastruktur (TI)**
 - Versichertenkarte (eGK Gen1, Gen2) 80 Mio.
 - Heilberufeausweis (HBA), Terminals je 0,3 Mio.
 - Netz-/Anwendungskonnektoren 0,3 Mio.
 - Erprobungs-Rollout ab 6/2016
- **AufgabeBSI:**
 - Technische Standards, Zertifizierung
 - Beratung Gesetzgeber
- **Beteiligte:** BMG, Gematik, Gesellschafter (GDV, KBV, KZBV, BÄK, DKG)
- **Perspektive:** Online Roll-Out Stufe 2, elektr. Fallakte, Notfalldaten-Management, mobile Geräte



Digitalisierungsprojekte

Intelligente Verkehrssysteme, autonomes Fahren

- **Erarbeitung technischer Vorgaben im Bereich intelligenter Verkehrssysteme (ID/Auth.)**
 - Car-to-Car, Car-to-X, AVF
 - C-ITS (Cooperative Intelligent Transport System)
Pilot-PKI, ISO 27000 SiKo, PP für Road Works Warning etc.
- **Aufgabe BSI:**
 - Technische Standards, Zertifizierung
 - Beratung Gesetzgeber
 - Leitung UAG Sicherheit der „Datenrunde“ im BMVI
- **Perspektive:**
 - Gremienarbeit EU, international

