Bundesamt
für Sicherheit in der
Informationstechnik

Gesetzliche Anforderungen an Betreiber Kritischer Infrastrukturen

Dr. Stefanie Fischer-Dieskau
Bundesamt für Sicherheit in der Informationstechnik
Referatsleiterin WG 13
Fachtagung Eisenbahnrecht und Technik, 08.04.2019, Frankfurt am Main

Inhalt

1. Digitalisierung und Automatisierung
2. Gefährdungslage
3. Regulatorische Maßnahmen
4. Die Rolle des BSI
5. Fazit

1. Digitalisierung und Automatisierung

   Was ist los an der Cyber-Front?

Anwendungen der Digitalisierung

>> Vernetze Lieferketten

Industrie 4.0 / Smart Factory

>> Vernetztes Arbeitsumfeld

>> Smart Factory

>> intelligente Verkehrsführung

Vernetzte Stadt

>> Interagierende Infrastruktur

>> Smart City

>> selbstfahrende Autos

Vernetzte Autos

>> Interaktion mit Infrastruktur

>> Smart Car

>> Intelligente Infrastruktur

Digitale Stellwerke

>> Glasfaser statt Kupfer

>> Digitale Schiene

>> automatisierte Versorgung

Intelligente Stromnetze

>> Vernetztes Arbeitsumfeld

>> Smart Meter

>> Echtzeitortung

Digitale Leit- und Sicherungstechnik

>> Kapazitätserhöhung

>> ETCS

Technologien für die Digitalisierung

>> Kryptowährungen
Blockchain
>> Direkte Koordinierung von Geräten
>> Distributed Ledger

>> Synergieeffekte
Cloud Computing
>> Zentralisierung der Daten
>> Permanenter Zugriff

>> potenzierte Rechenleistung
Quantencomputer
>> Quantenkryptografie
>> Post-Quantum

>> Vernetzung im Cyberraum
Internet der Dinge
>> Komplexität durch Integration
>> Allgegenwärtigkeit

>> wissensbasierte Systeme
KI – Künstliche Intelligenz
>> Neue Problemlösungsmöglichkeiten
>> Digital Twin

>> Datengenerierung und Kontrolle
Big Data
>> vorausschauende Wartung
>> Automatisierte Steuerung

>> Neue Datengewinnung
Sensorik & Aktorik
>> Leuchtende Bahnsteigkante

>> Hohe Downloadgeschwindigkeit
G5 Mobilfunkstandard
>> Verbesserte Servicequalität

Cyber-Sicherheit in der Digitalisierung und Automatisierung

Vernetzung

Komplexität

Allgegen-wärtigkeit

Digitalisierung bedeutet…

…mehr Möglichkeiten,

auf die Deutschland nicht verzichten kann und soll

…mehr Gefahren,

auf die Deutschland vorbereitet sein muss

Cyber-Sicherheit **…unverzichtbare Voraussetzung für das Gelingen der Digitalisierung**

Bundesamt für Sicherheit in der Informationstechnik

2. Gefährdungslage

   oder: die nächste Attacke wird kommen...

Wie bedroht ist Deutschlands Cyber-Raum?

Organisierte Kriminalität macht mehr Gewinne mit **CyberCrime** als mit Drogen

Gezielte Cyber-Spionage

(Advances Persistent Threats) wird im Schnitt nach **243 Tagen** entdeckt

Bitkom-Studie: Wirtschaftsspionage kostet Unternehmen **55 Mrd. EUR** im Jahr

2017 wurden **über 600.000.000 Schadprogramme** gesichtet

über 1.000 Sicherheitslücken in den zehn meist genutzten Softwareprodukten

Quelle: BSI

IT-Sicherheitsvorfälle

WannaCry

- Schadprogramm, verschlüsselt Dateien bis zur Zahlung
- Entschlüsselung wird bei Zahlung von Lösegeld versprochen (BSI rät von Zahlung ab)
- Viele Organisationen betroffen
- Mai 2017

Quelle: heise.de

WannaCry: Was wir bisher über die Ransomware-Attacke wissen UPDATE

13.05.2017 16:20 Uhr – Volker Briegleb vorlesen

Nicht nur die Deutsche Bahn ist von WannaCry betroffen... (Bild: Martin Wiesner)

Es begann am Freitagabend mit Schreckensmeldungen aus Großbritannien: Computer des nationalen Gesundheitssystem waren von einer Ransomware infiziert. Inzwischen hat sich WannaCry weltweit verbreitet.

Seit Freitagabend breitet sich die Ransomware WannaCry (WanaDecrypt0r 2.0) im weltweiten Internet aus. Es handelt sich um einen Kryptotrojaner, der Daten auf den betroffenen Computern verschlüsselt. Am 19. Mai soll der Nutzer den Code für die Entschlüsselung erhalten, ansonsten sei die Löschung veranlasst. Die Zahlungen sollten in Bitcoin abgewickelt werden. Bislang zahlten 126 Opfer insgesamt etwa 30.000 Euro. Weltweit sollen zur Stunde über 220.000 Systeme betroffen sein. Anders als Locky & Co springt der Schädling von einem infizierten Rechner auf andere, übers Netz erreichbare Windows-Systeme über. In Deutschland hat das Bundeskriminalamt BKA Ermittlungen aufgenommen.

WannaCry traf nicht nur hier...

… sondern auch hier …

Quelle: Pixabay

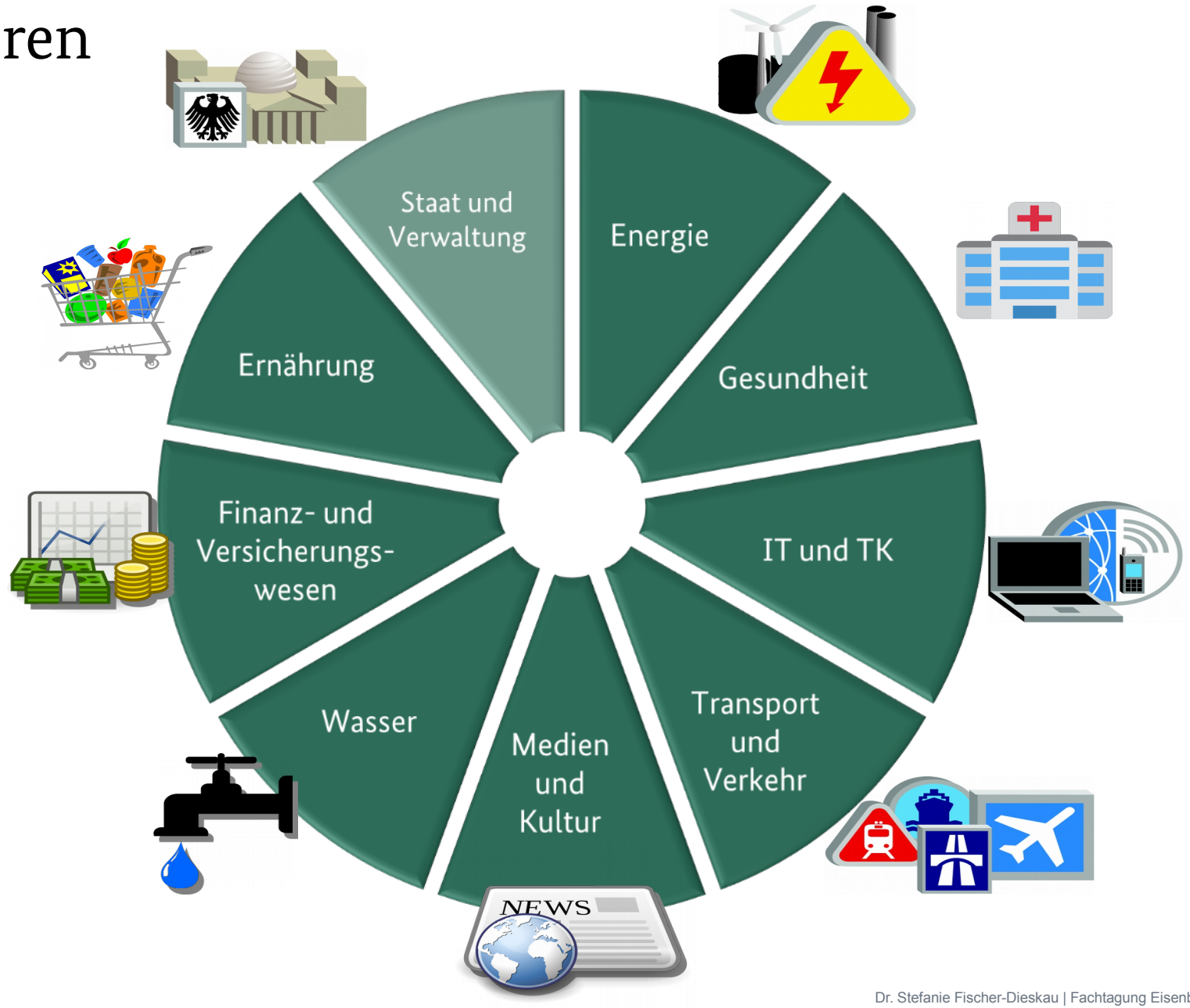
… und hier

Quelle: Twitter/uwepleban

3. Regulatorische Maßnahmen

Gesetzliche Anforderungen an KRITIS-Betreiber nach BSIG

KRITIS-Sektoren



Kritische Anlagen gemäß BSI-KritisV im Schienenverkehr

Anlagenbezeichnung	Bemessungskriterium	Schwellenwert
Personenbahnhof	Bahnhofskategorie	Jeweils höchste Kategorie
Güterbahnhof	Anzahl ausgehender Züge/Jahr	23.000
Zugbildungsbahnhof	Anzahl gebildete Züge/Jahr	23.000
Schienennetz und Stellwerke der Eisenbahn	Schienennetz nach TEN-V	Kernnetz
Verkehrssteuerungs- und Leitsystem der Eisenbahn	Leitsystem des Schienennetzes nach TEN-V	Kernnetz
Leitzentrale der Eisenbahn	disponierte Transportleistung in Zugkilometer/Jahr disponierte Transportleistung in Tonnenkilometer/Jahr	8.200.000 730.000.000

Bunde
für Sic
Inform

Neue gesetzliche Pflichten nach BSIG im Überblick

Prävention

Maßnahmen nach Stand der Technik

Betreiber muss angemessene **Maßnahmen** treffen nach

- **Stand der Technik**
- Branchenspezifischen Sicherheitsstandards (**B3S**)

§ 8a (1)
§ 8a (2)
§ 8a (4)

Wirksamkeit der Maßnahmen

- **Auditierungspflicht** (alle 2 Jahre)
- **Nachweis** gegenüber BSI
- Bei Sicherheitsmängeln → ggf. Einbindung der Aufsichtsbehörde

§ 8a (3)

Reaktion

Warnungen Meldungen Lagebilder

- BSI: Erstellung/Verteilung von **Warnungen & Lagebildern**
- KRITIS-Betreiber: **Meldepflicht** von (erheblichen) Störungen
- KRITIS-Betreiber: hat Informationsrecht

§ 8b (1)
§ 8b (2)
§ 8b (4)

Verordnung (BSI-KritisV)

- **Identifikation** der KRITIS-Betreiber

Bundesamt für Sicherheit in der Informationstechnik

4. Die Rolle des BSI

Partner oder Aufsichtsbehörde?

Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft

Bundesamt
für Sicherheit in der
Informationstechnik

Die Rolle des BSI

Mit dem IT-SiG kamen Aufsichtsfunktionen hinzu...
- Nachweise / Sicherheitsmängel / Meldepflicht
- Branchenspezifische Sicherheitsstandards

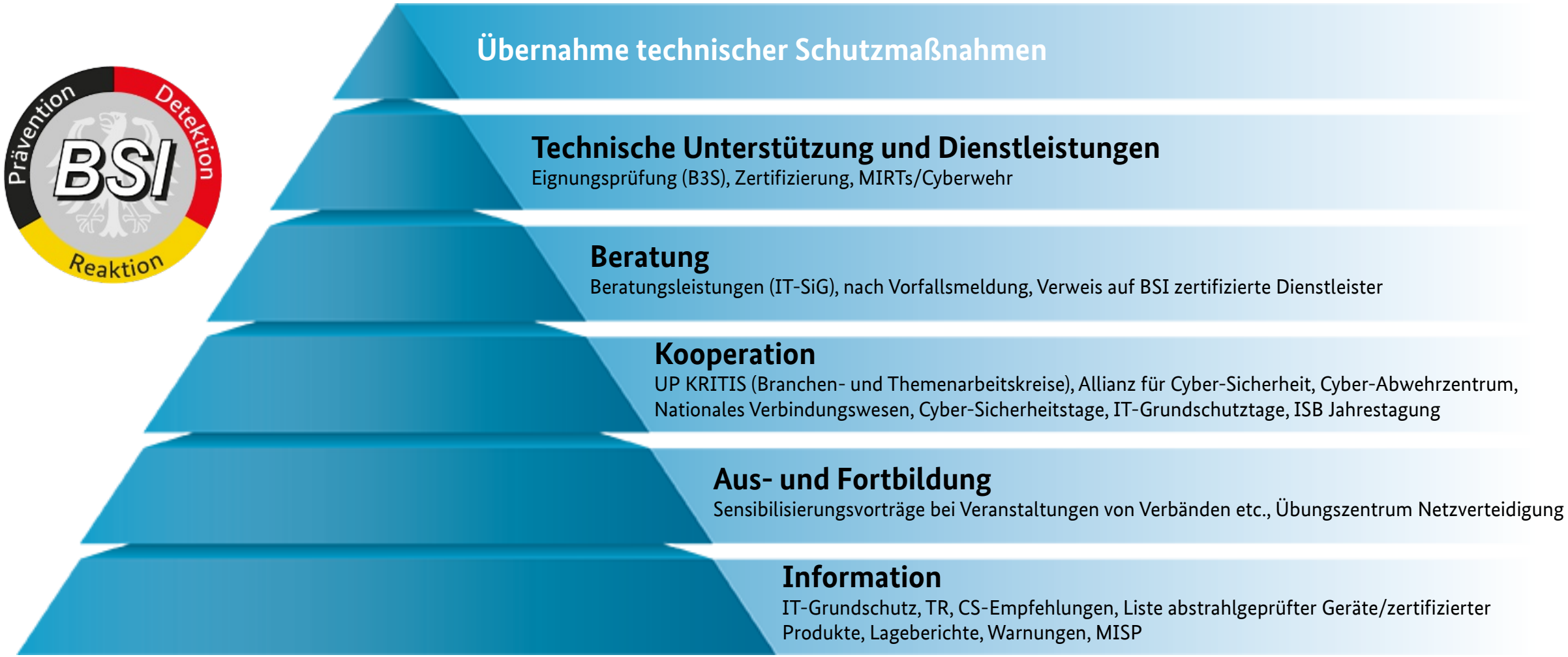
Das BSI sieht sich aber nicht als klassische Aufsichtsbehörde, sondern verfolgt weiterhin einen kooperativen Ansatz

Verbesserung der Cybersicherheit als gemeinsames Ziel von Staat und Wirtschaft

Vertrauen ist notwendige Voraussetzung für das (freiwillige) Teilen von Informationen

Mitwirkung der Betreiber ist notwendig!

BSI-Angebote für KRITIS



5. Fazit

Fazit

- Die Cyber-Sicherheitslage ist dynamisch und beständig angespannt.

- IT-Sicherheitsgesetz ist in Kraft:

  - beinhaltet neue Pflichten für BSI und Betreiber

  - Ziel: Win-win-Situation

- Das BSI bietet Betreibern Kritischer Infrastrukturen Hilfe in vielen Formen, Farben und Variationen.

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt
Dr. Stefanie Fischer-Dieskau
Referatsleiterin WG 13

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn

Referat-wg13@bsi.bund.de
Tel. +49 (0) 228 9582 5021
Fax +49 (0) 228 10 9582 5021
www.bsi.bund.de
www.bsi-fuer-buerger.de