Bundesamt
für Sicherheit in der
Informationstechnik

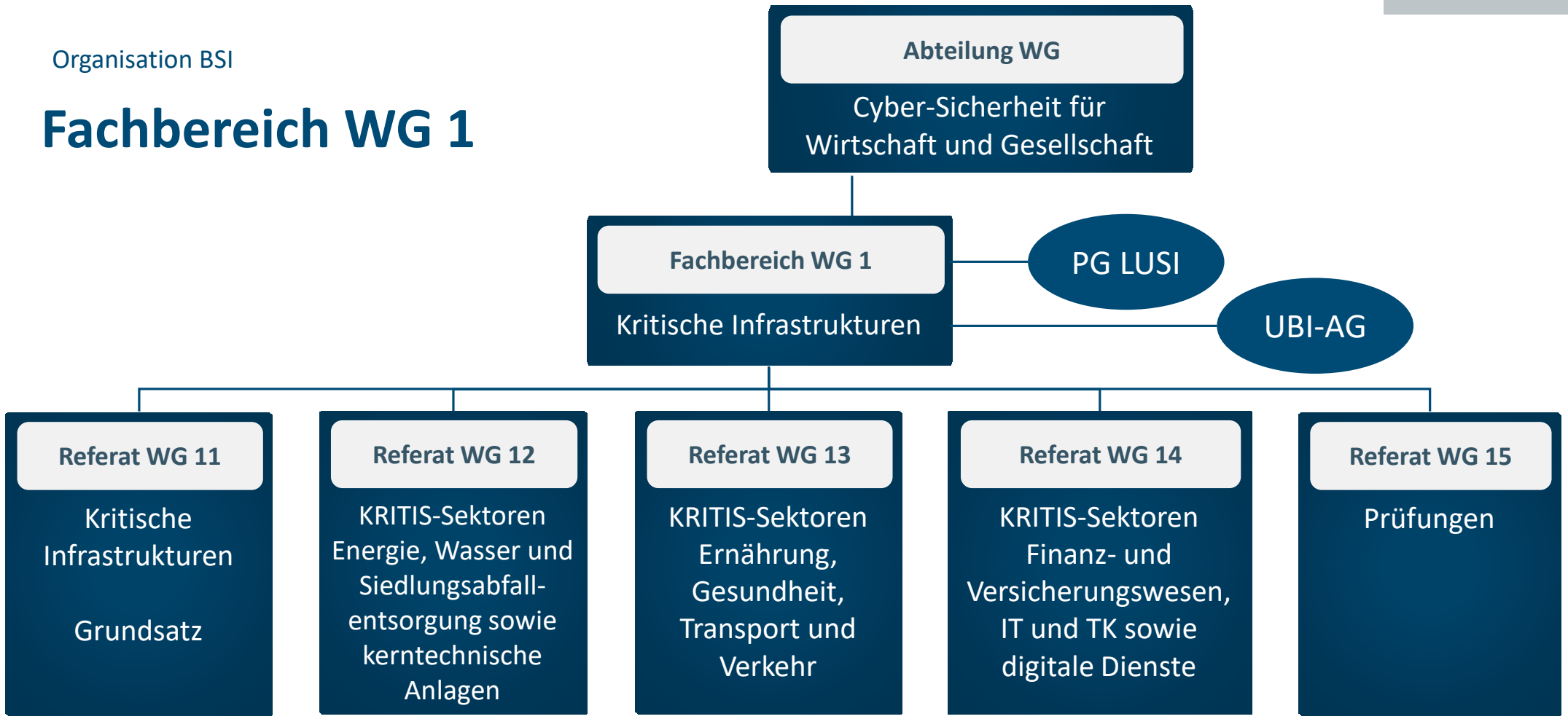
Deutschland
Digital•Sicher•BSI•

Zur Konkretisierung des Standes der Technik bei KRITIS – Ein Wechselspiel zwischen BSI und Betreibern

IT-Sicherheitsrechtstag 2022 des Bundesverband IT-Sicherheit e.V. (TeleTrusT)
21.09.2022, Berlin

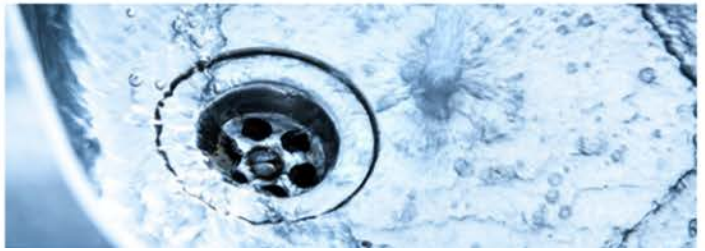
Dr. Timo Hauschild, BSI

Fachbereich WG 1



1. Einführung

Kritische Infrastrukturen

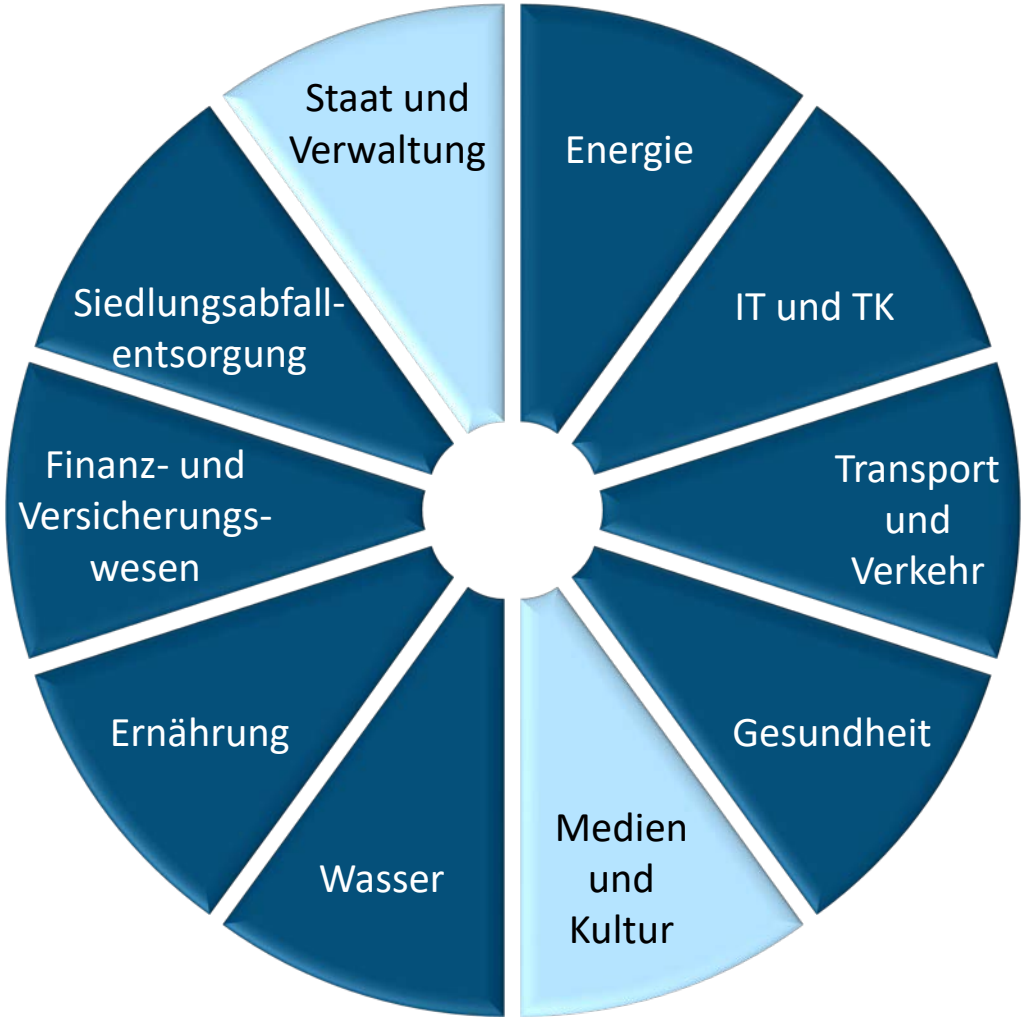

Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden



KRITIS-Sektoren

Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon aus folgenden Sektoren:

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Siedlungsabfallentsorgung



Beispiele

Kritische Dienstleistungen

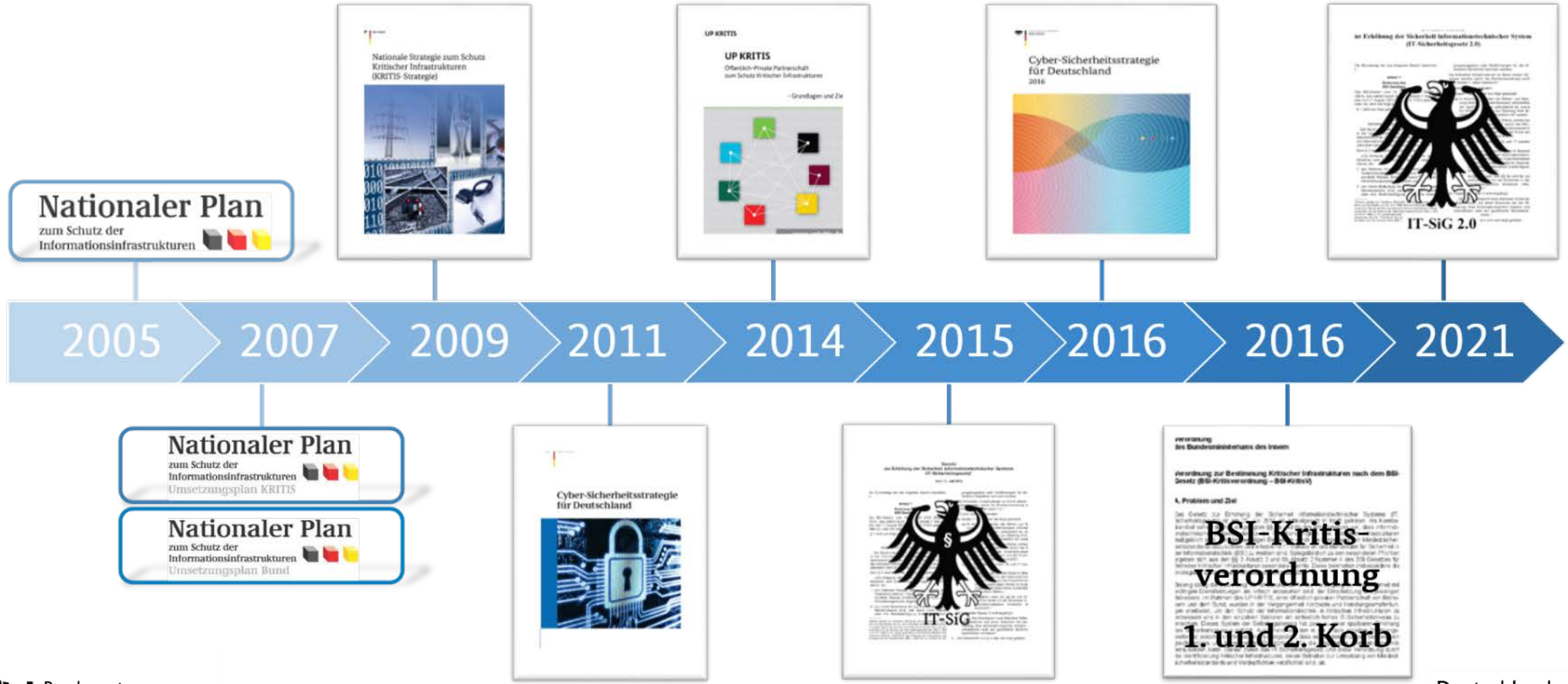
Schutz von KRITIS ist wesentlich für das Funktionieren der Gesellschaft

Zunehmende Digitalisierung führt zu geänderter Bedrohungslage

Stetige Weiterentwicklung der Schutzkonzepte ist erforderlich

2. Regulierung

Kritische Infrastrukturen



EU-Ebene

2008: EPSKI-Richtlinie

2016: NIS-Richtlinie

2022 (voraussichtlich): NIS2-Richtlinie, DORA-Verordnung

2023 (voraussichtlich): CER-Richtlinie

Rollen des BSI

Regulierung/Aufsicht & Kooperation/Unterstützung

Rechte und Pflichten von KRITIS-Betreibern und BSI durch IT-Sicherheitsgesetze eingeführt

Enge Kooperation des BSI mit der Wirtschaft, z. B. im UP KRITIS oder der Allianz für Cybersicherheit

UP KRITIS

Allianz für Cyber-Sicherheit

Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme

- Artikelgesetz, Änderung von
  - BSI-Gesetz
  - Energiewirtschaftsgesetz
  - Telemediengesetz
  - Telekommunikationsgesetz
- Adressaten:
  - KRITIS-Betreiber
  - Betreiber von Web-Angeboten
  - TK-Unternehmen
- BSI als Aufsichtsbehörde

Entwicklung der BSI-Kritisverordnung

Fassung der BSI-KritisV	Inkrafttreten
Versionen „0.5“ und „1.0“ (zwei „Körbe“) 7 KRITIS-Sektoren mit Schwellenwerten	**2016, 2017**
„Version 1.5“ BSI-KritisV mit nach wie vor 7 Sektoren, aber **angepassten Schwellenwerten** („Zweite Verordnung zur Änderung der BSI-Kritisverordnung“)	**01/2022**
„Version 2.0“ Neuer Sektor **Siedlungsabfallentsorgung**, erneut angepasste Schwellenwerte („Dritte Verordnung zur Änderung der BSI-Kritisverordnung“)	**in Ausarbeitung**

Auszüge aus dem § 8a BSIG

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, […], **angemessene organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. **Dabei soll der Stand der Technik eingehalten werden**. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

[…]

Auszüge aus dem § 8a BSIG

(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können **branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach den Absätzen 1** und 1a vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach den Absätzen 1 und 1a zu gewährleisten. […]

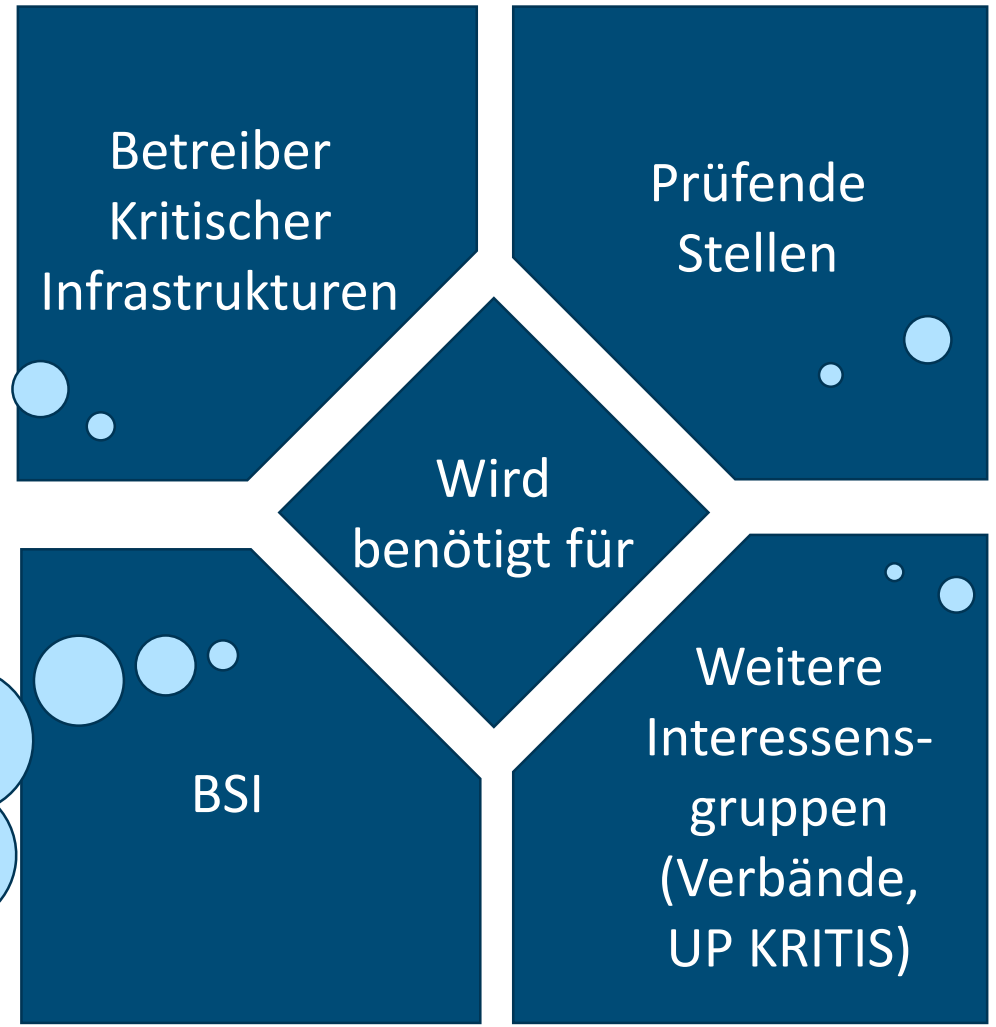
(3) Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend **alle zwei Jahre dem Bundesamt nachzuweisen**. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. […]

[…]

3. Stand der Technik und Konkretisierung

„Stand der Technik“ – Beteiligte

- Umsetzung der Anforderungen nach § 8a Absatz 1 BSIG
- Erbringen der Nachweise nach § 8a Absatz 3 BSIG



- Herleitung Prüfgrundlage
- Prüfdurchführung
- Prüfdokumentation

- Erstellung von Anforderungen an Prüfung und Nachweiserbringung
- Überprüfung der Erfüllung der gesetzlichen Anforde-rungen durch KRITIS-Betreiber

- u. a. Erstellung von B3S

„Stand der Technik“ – Vorgehen zur Konkretisierung

Grundlegende IT-Sicherheits-Anforderungen	• Geben das Niveau der Informationssicherheit vor. • Entsprechen anerkannten Standards der Informationssicherheit. • Sind generisch und für alle Betreiber identisch.
KRITIS Anforderungen	• Fokussieren die kritische Dienstleistung. • Legen grundlegende Rahmenbedingungen fest (bspw. Beschränkung der Behandlungsalternativen für Risiken). • Ergeben sich verbindlich aus der Gesetzgebung für alle Betreiber.
Spezielle technische Anforderungen	• Ergänzen die grundlegenden IT-Sicherheitsanforderungen um spezielle technische Anforderungen, wo diese nicht ausreichen (bspw. bei Operativer Technik (OT) wie Cloud, IoT, ICS, etc.). • Fokussieren auf Informationstechnik, die eine besondere Relevanz hat. • Können über mehrere Sektoren und Branchen hinweg gleich sein.
Spezielle organisatorische Anforderungen	• Berücksichtigen die konkreten Gegebenheiten der KRITIS und des Betreibers (KRITIS-Schutzziele, Bedrohungslage, Schutzbedarf, Risikobehandlung). • Sind individuell für Anlage und Betreiber festzustellen. • Berücksichtigen weitere geltende Regularien.

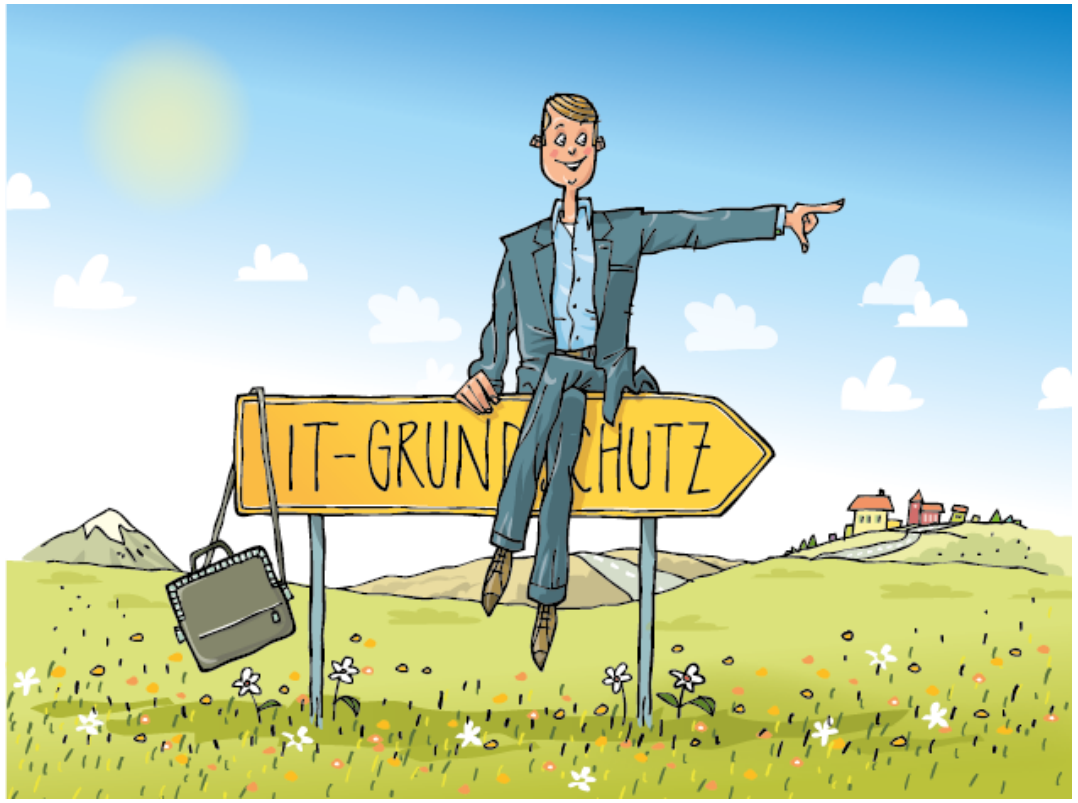
Grundlage
vergleichbare Anforderungen

Ergänzung
technikspezifisch

Ausgestaltung
anlagenspezifisch

Grundlegende IT-Sicherheitsanforderungen: Ansatzpunkt IT-Grundschutz (und BSI-Standards)

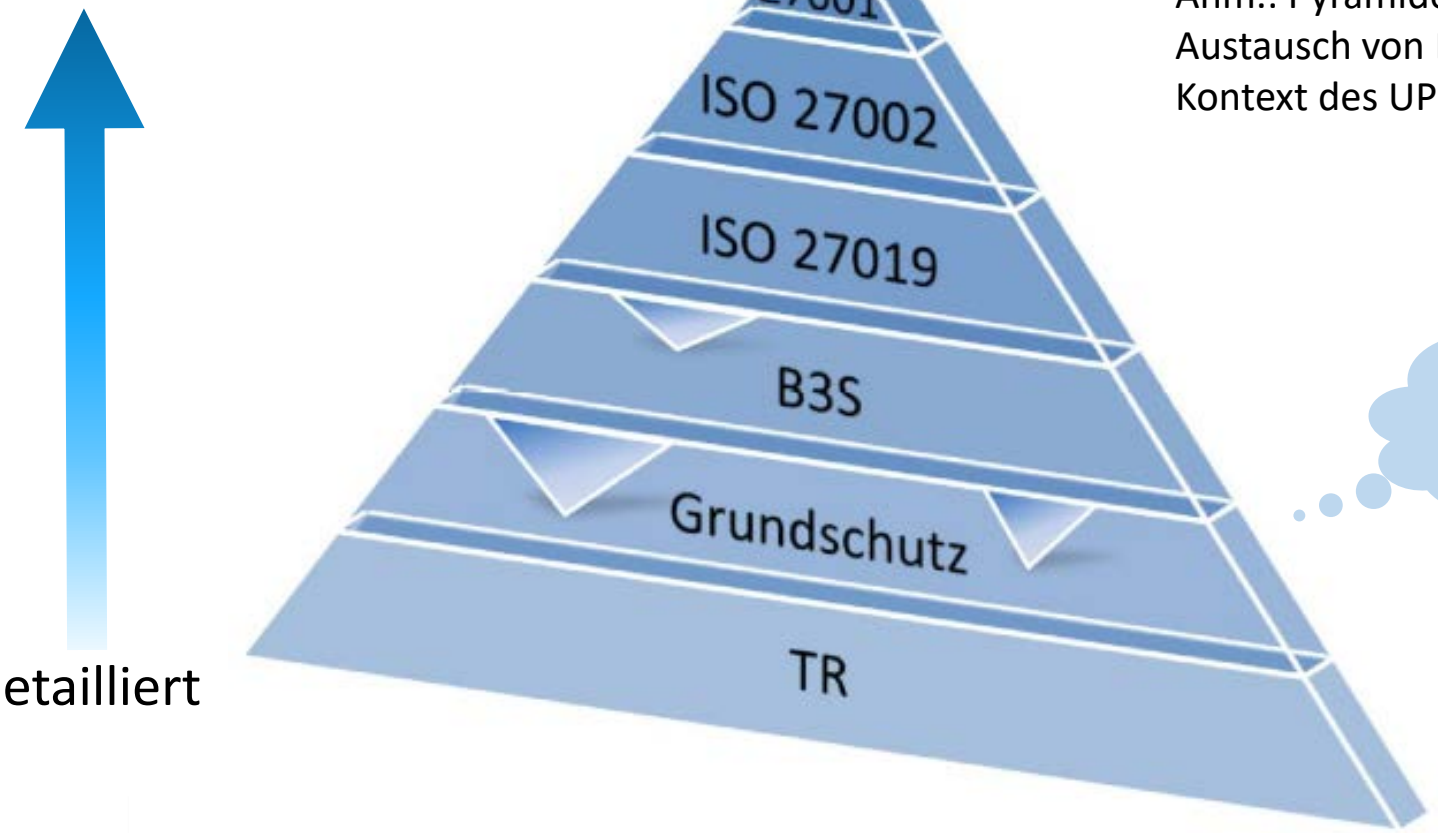
- IT-Grundschutz-Kompendium
- Standardisierte Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, IT-Systeme, etc.
- IT-GS-Bausteine bilden den Stand der Technik ab, basierend auf den Erkenntnissen zum Zeitpunkt der Veröffentlichung.
- Die dort formulierten Anforderungen beschreiben, was generell umzusetzen ist.



KRITIS-Anforderungen: Besonderheiten

Angemessener Abstraktionsgrad

abstrakt



detailliert

Anm.: Pyramide zeigt frühere Überlegungen im Austausch von BSI mit Betreibern und Prüfern im Kontext des UP KRITIS

IT-KRITIS-GS-Profile

„Stand der Technik“ – Umsetzung

Grundlegende IT-Sicherheits-Anforderungen	• Geben das Niveau der Informationssicherheit vor. • Entsprechen anerkannten Standards der Informationssicherheit. • Sind generisch und für alle Betreiber identisch.
KRITIS Anforderungen	• Fokussieren die kritische Dienstleistung. • Legen grundlegende Rahmenbedingungen fest (bspw. Beschränkung der Behandlungsalternativen für Risiken). • Ergeben sich verbindlich aus der Gesetzgebung für alle Betreiber.
Spezielle technische Anforderungen	• Ergänzen die grundlegenden IT-Sicherheitsanforderungen um spezielle technische Anforderungen, wo diese nicht ausreichen (bspw. bei Operativer Technik (OT) wie Cloud, IoT, ICS, etc.). • Fokussieren auf Informationstechnik, die eine besondere Relevanz hat. • Können über mehrere Sektoren und Branchen hinweg gleich sein.
Spezielle organisatorische Anforderungen	• Berücksichtigen die konkreten Gegebenheiten der KRITIS und des Betreibers (KRITIS-Schutzziele, Bedrohungslage, Schutzbedarf, Risikobehandlung). • Sind individuell für Anlage und Betreiber festzustellen. • Berücksichtigen weitere geltende Regularien.

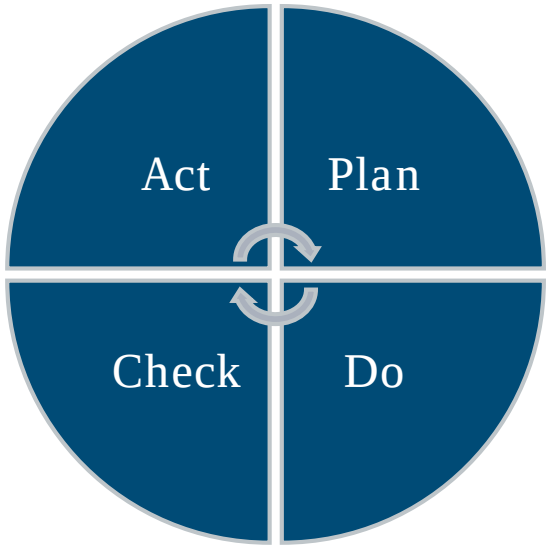
Grundlage
vergleichbare Anforderungen

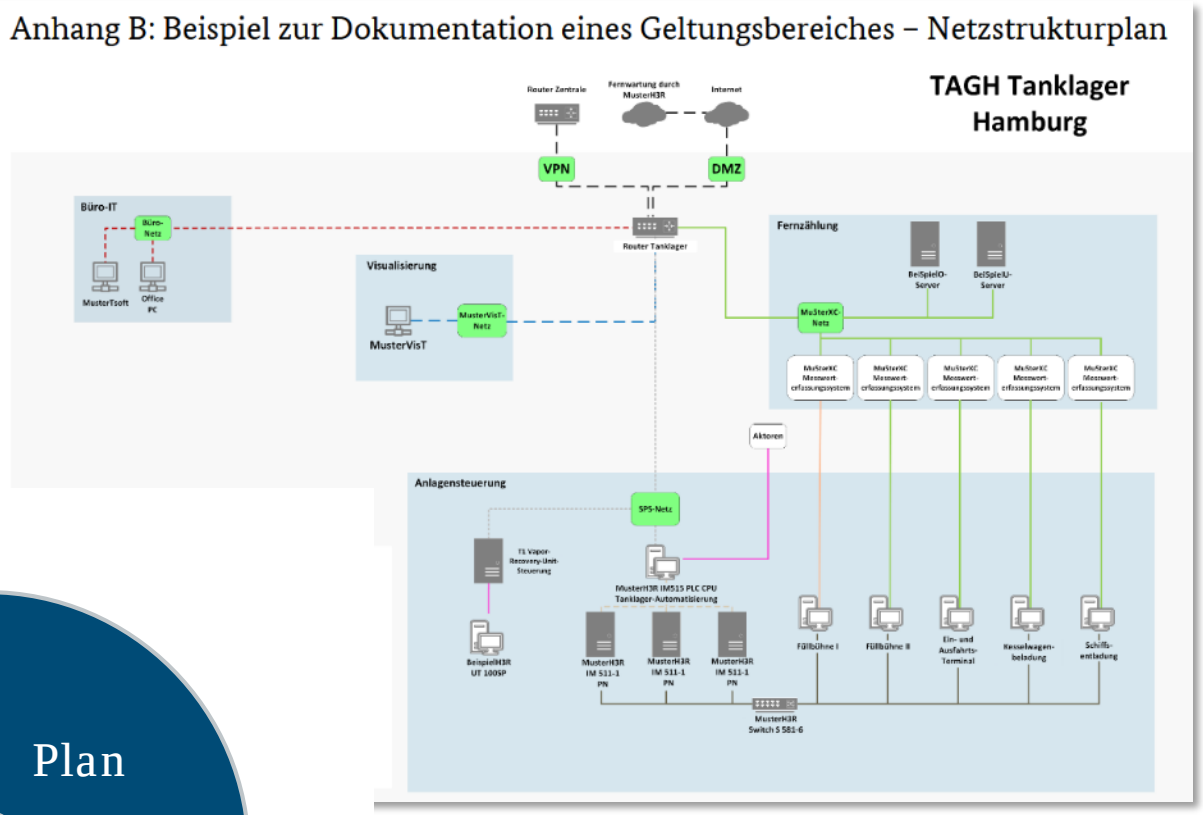
Ergänzung
technikspezifisch

Ausgestaltung
anlagenspezifisch

Umsetzung

- In Ausgestaltung und Umsetzung ist der einzelne Betreiber besonders gefordert
- ISMS ist Grundpfeiler der Informationssicherheit
- Klare Festlegung des Geltungsbereiches ist notwendig
- Besonderheiten der Anlage sind zu berücksichtigen
- IT-Sicherheit ist eine kontinuierliche Aufgabe





4. Austausch und Kooperation

UP KRITIS

Teilnehmer (800):

- Betreiber Kritischer Infrastrukturen
- Verbände
- Zuständige Behörden

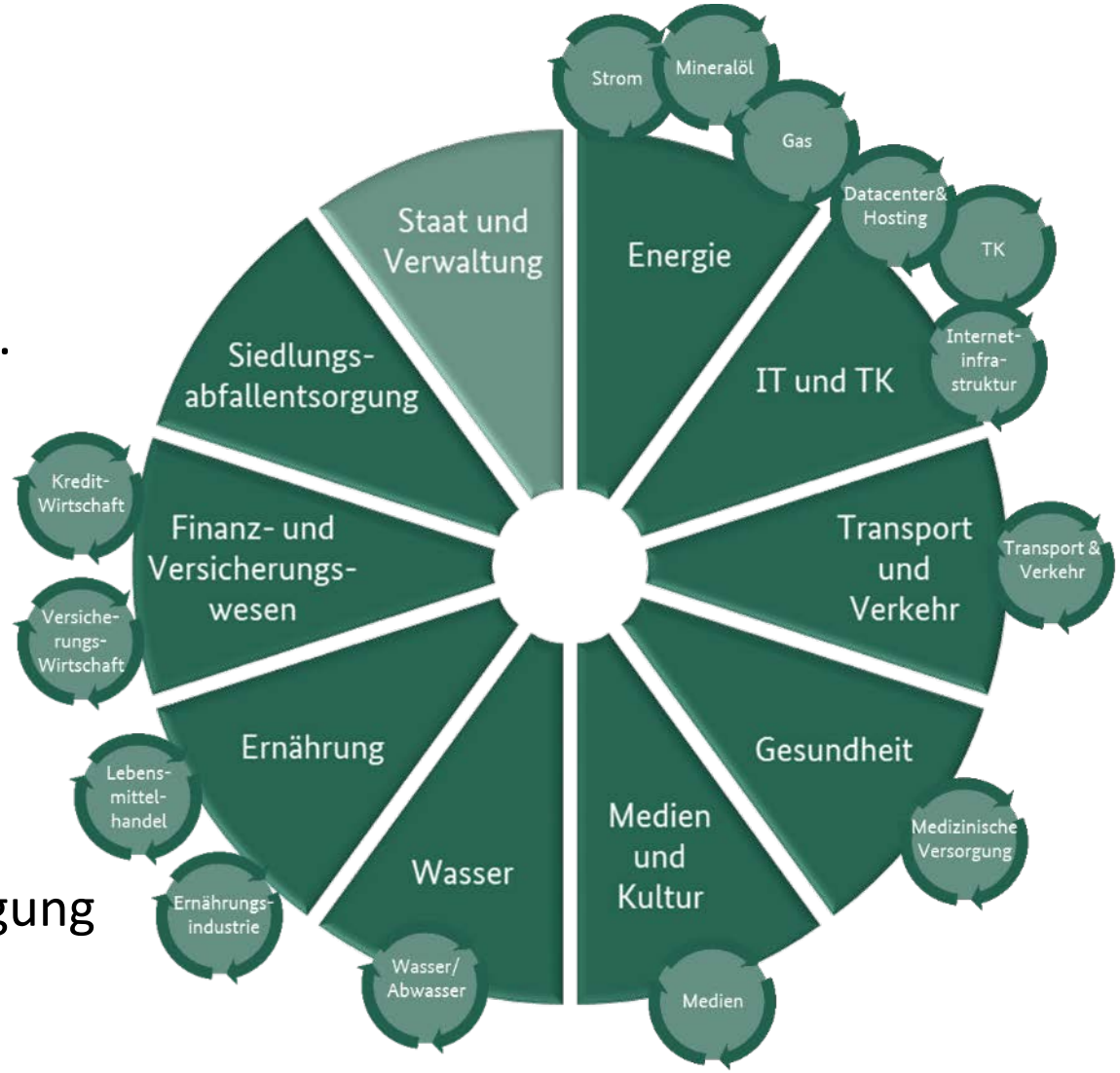
UP KRITIS

Produkte des UP KRITIS:

- Teilnahme an Branchen- und Themenarbeitskreisen
- Positionspapiere
- Arbeitshilfen (z. B. Security Level Agreement)
- Meldewesen und Diskussion von Vorfällen
- Krisenmanagementstrukturen
- Koordinierte Krisenreaktion und -bewältigung
- Teilnahme an Notfall- und Krisenübungen
- Gemeinsames Handeln gegenüber Dritten

Aktivitäten

- **Gemeinsames Handeln** gegenüber Dritten z. B. durch
  - Positionspapiere
  - Entwicklung von Arbeitshilfen „Security Level Agreement“
- **Branchenarbeitskreise (BAK) und Themenarbeitskreise (TAK)**
- **Meldewesen** und Diskussion von Vorfällen
- Etablieren von **Krisenmanagementstrukturen** koordinierte Krisenreaktion und Krisenbewältigung
- Teilnahme an Notfall- und Krisen**übungen**



Überblick

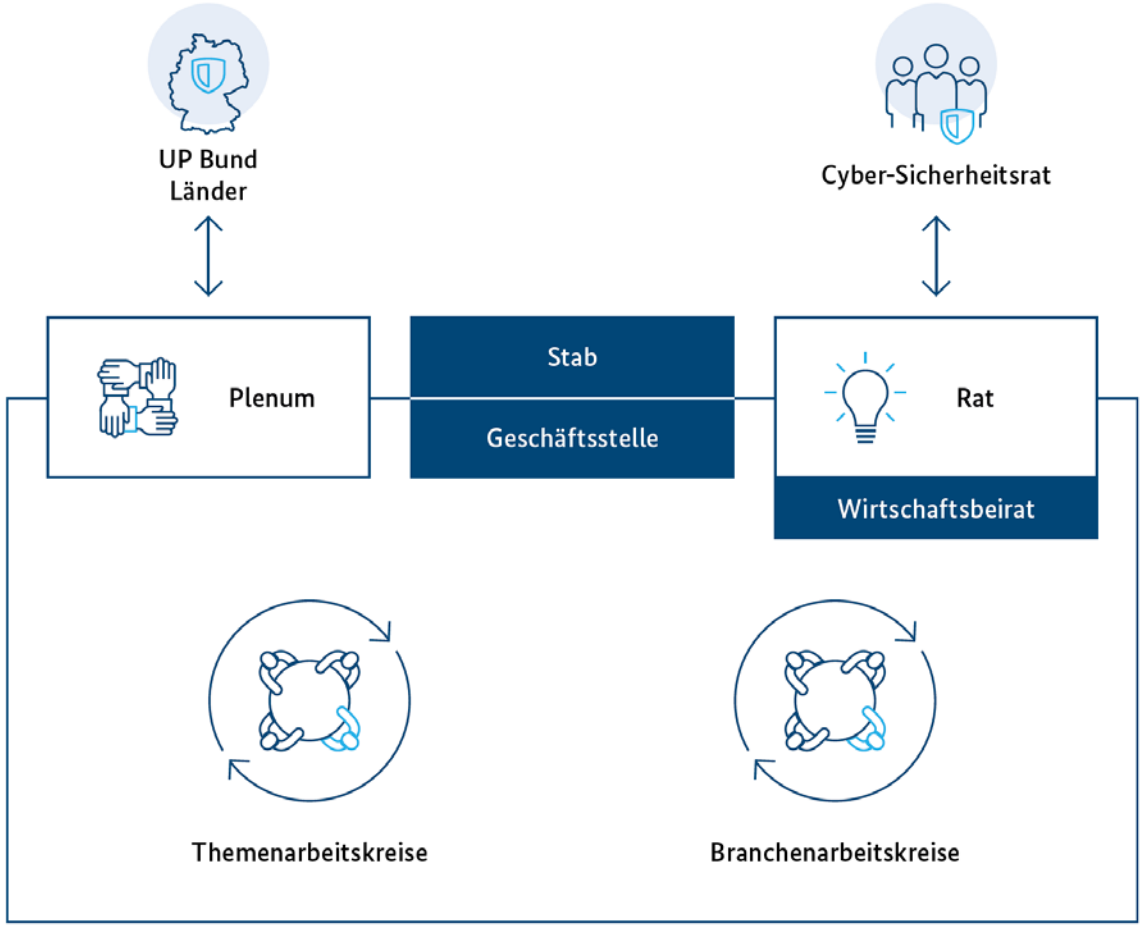
Öffentlich-private Kooperation zwischen

- Betreibern Kritischer Infrastrukturen,
- deren Verbänden und
- den zuständigen staatlichen Stellen.

Ziel: Aufrechterhaltung der Versorgung mit kritischen Infrastrukturdienstleistungen in Deutschland

Strategisch-konzeptionelle Mitarbeit

- Fachliche und politische Gremien
- Cybersicherheit ist ein Schwerpunkt der Arbeiten



Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Kontakt

Dr. Timo Hauschild
timo.hauschild@bsi.bund.de
Tel. +49 (0) 228 99 9582-5824

Bundesamt für Sicherheit in der Informationstechnik
Fachbereich WG 1
Godesberger Allee 185 -189
www.bsi.bund.de