Ungeahnt verzahnt? –

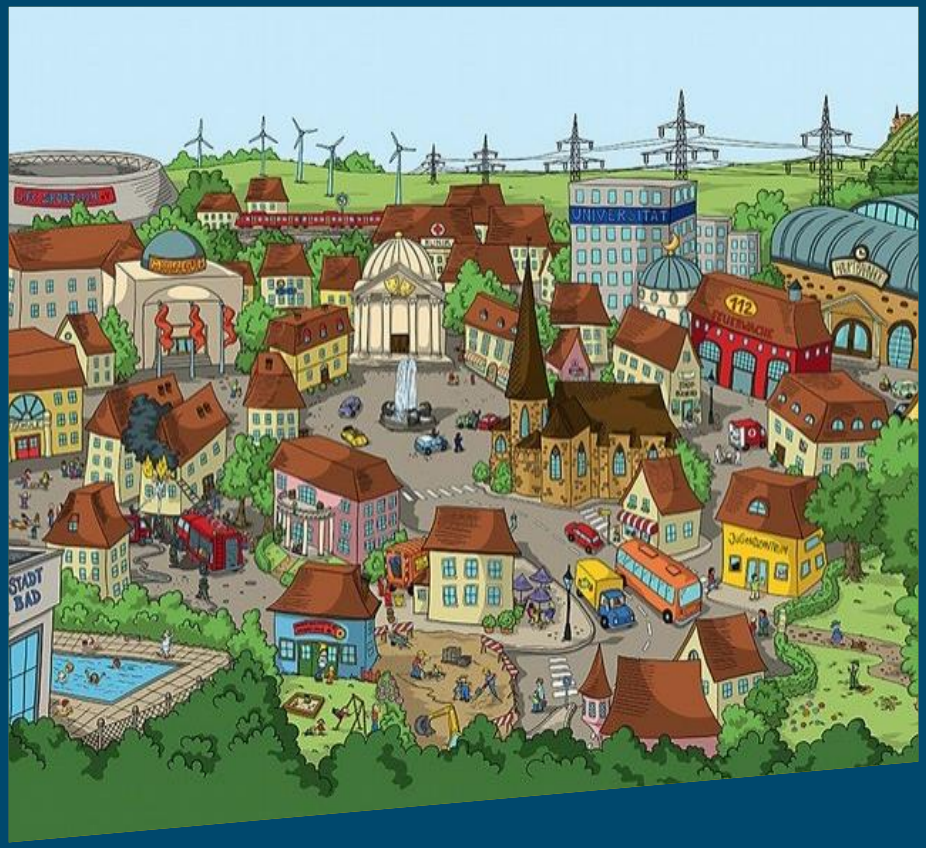
Kaskadeneffekte kritischer Infrastrukturen

Brunnenstraße 15-17
45128 Essen
Tel. 0201 – 879990
www.rst-beratung.de
E-Mail: essen@rst-beratung.de

Ungeahnt verzahnt? Kaskadeneffekte Kritischer Infrastrukturen

- Warum?
  - Wie abhängig sind wir?
    - Kann wirklich etwas passieren?
      - Regulatorik: notwendiges Übel oder gute Gegenmaßnahme?
        - Wirksamer Schutz!

Verletzlichkeitsparadoxon – eine Frage der Abhängigkeit?



Je mehr sich die Gesellschaft auf etwas verlässt, desto gravierender sind die Folgen eines Ausfalls.

Das hohe subjektive Sicherheitsempfinden unserer Gesellschaft birgt Gefahren.

- Wie resilient sind unsere kritischen Infrastrukturen?
- Wie resilient ist unsere Gesellschaft?

Kann wirklich etwas passieren?

Hackerangriff auf die Funke Mediengruppe in Essen

- Verlust des Zugangs zu Informationen (Verfügbarkeit)
  - Verschlüsselung von Daten
  - Lösegelderpressung
  - Betriebsunterbrechung und Notbetrieb über mehrere Tage
  - Hoher Imageschaden und Vertrauensverlust

Kann wirklich etwas passieren?

Hackerangriff auf die Kassen von Media Markt (2021)

Angriff auf die Universitätsklinik Düsseldorf (2020)

Angriff auf den UK National Health Service (2017)

Sicherheitslücke Microsoft Exchange (2021)

Angriffe auf Pipelines in den USA (2021)

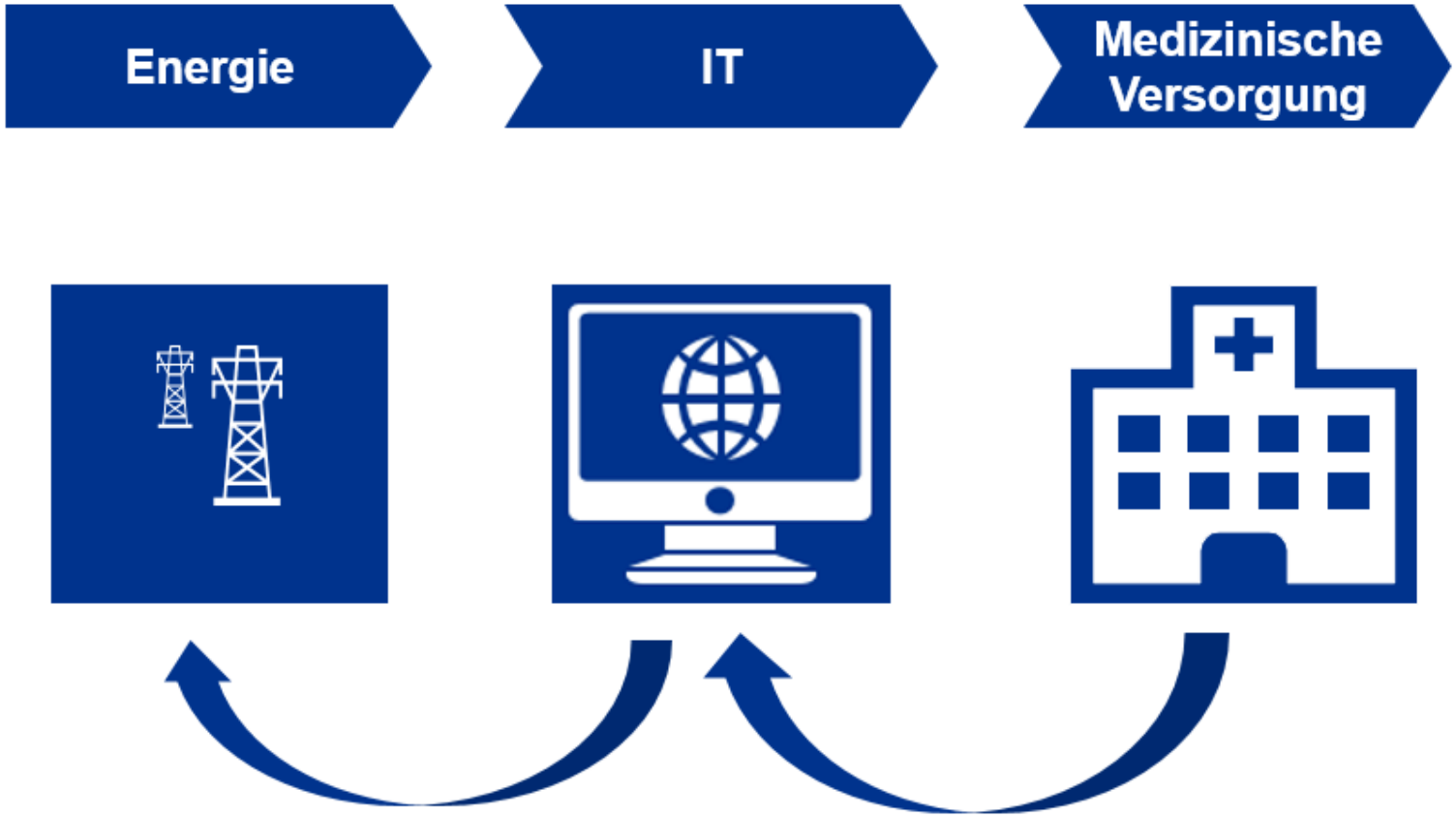
Log4j (13.12.2021)

Es trifft nicht nur die Großen – ein Beispiel aus dem Mittelstand

Hackerangriff auf ein mittelständisches Unternehmen

- Verlust des Zugangs zu Informationen (Verfügbarkeit)
  1. Verschlüsselung von Daten
  2. Lösegelderpressung
  3. 6 Werktage Betriebsunterbrechung
- Verlust von Kundendaten kann nicht ausgeschlossen werden
  1. Meldung einer Datenschutzverletzung an die Aufsichtsbehörde
  2. Regressforderungen von Kunden
  3. Vertrauensverlust bei Kunden
- Schaden (erste Schätzung ohne Folgeschäden durch Prozesse/ Kundenverlust)
  - ca. 62.000€ Lösegeld
  - ca. 20.000€ Beraterkosten
  - ca. 70.000€ Betriebsunterbrechung

Abhängigkeiten und Kaskadeneffekte



Regulatorik: Das IT-Sicherheitsgesetz

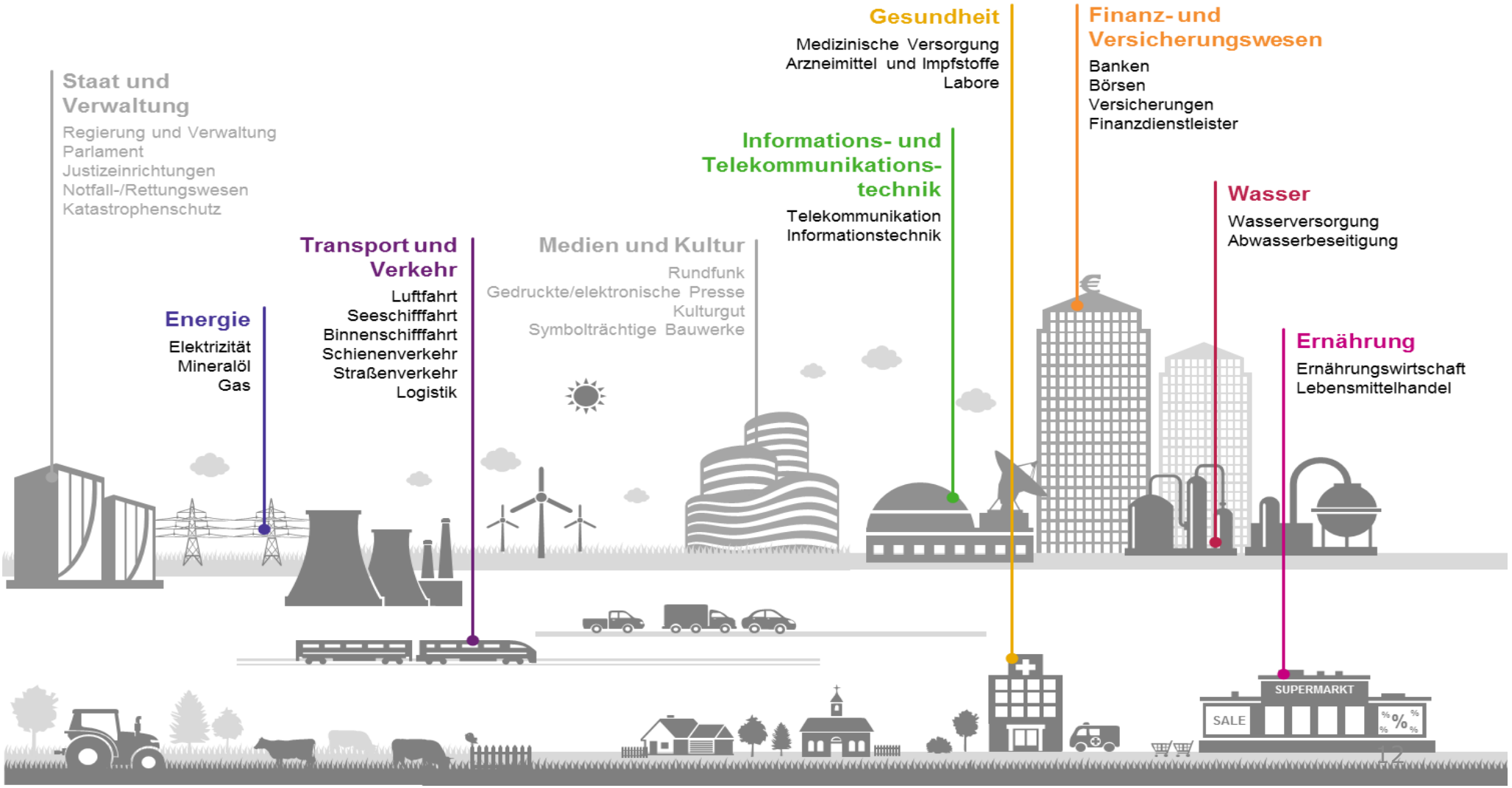
- Das IT-Sicherheitsgesetz legt Regelungen für die IT-Sicherheit für Betreiber Kritischer Infrastrukturen fest, um die Versorgungssicherheit der Bevölkerung sicherzustellen.
- Die Kritischen Infrastrukturen im Sinne des Gesetzes werden durch die Rechtsverordnung BSI Kritisverordnung (BSI-KritisV) näher bestimmt.
- Das IT-Sicherheitsgesetz ist die nationale Ausgestaltung des Europäischen Rechtsrahmens, der durch die EU-Verordnung 2016/1148 vorgegeben wurde (Directive on security of network and information systems (NIS Directive)).
- Für Betreiber Kritischer Infrastrukturen erfordert das IT-Sicherheitsgesetz – neben den zusätzlichen regulatorischen Anforderungen – auch Anpassungen der internen Prozesse der IT-Sicherheit.

Grundprinzip der Versorgungssicherheit

Gewährleistungsverantwortung

Betriebsverantwortung

Die Sektoren Kritischer Infrastrukturen gemäß §2 (10) BSI-Gesetz



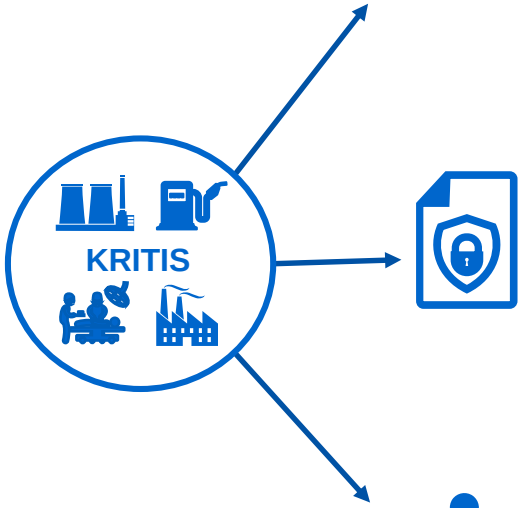
Wann bin ich betroffen: Beispiel Krankenhaus

Sektor		Gesundheit
Dienstleistung		Medizinische Versorgung
Prozessschritt		Therapie
Anlage		Krankenhaus
Schwellenwert	30.000	vollstationäre Fälle pro Jahr

Wann bin ich betroffen? Beispiel Lebensmittelproduktion

Sektor		Ernährung
Dienstleistung		Herstellung von Lebensmitteln
Prozessschritt		Produktion von Getränken
Anlage		Abfüllanlage/ Produktionsstätte
Schwellenwert	350.000.000	Liter Produktionsvolumen pro Jahr

Hauptanforderungen an Betreiber Kritischer Infrastrukturen



Meldung von Sicherheitsvorfällen (§8b (4) BSIG)

Erhebliche **Sicherheitsvorfälle** müssen zeitnah erkannt, analysiert und bewertet werden. Ferner ist eine Meldung an das BSI als zuständige Behörde notwendig, wobei alle Anforderungen des BSI an zu meldende Informationen berücksichtigt werden müssen.

Etablierung von Sicherheitsstandards (§8a (1) BSIG)

Es müssen allgemeine und branchenspezifische **Sicherheitsstandards** implementiert und gelebt werden. Dies betrifft sowohl organisatorische als auch technische Vorkehrungen und erfordert eine strukturierte, weitsichtige Lenkung aller Einzelmaßnahmen.

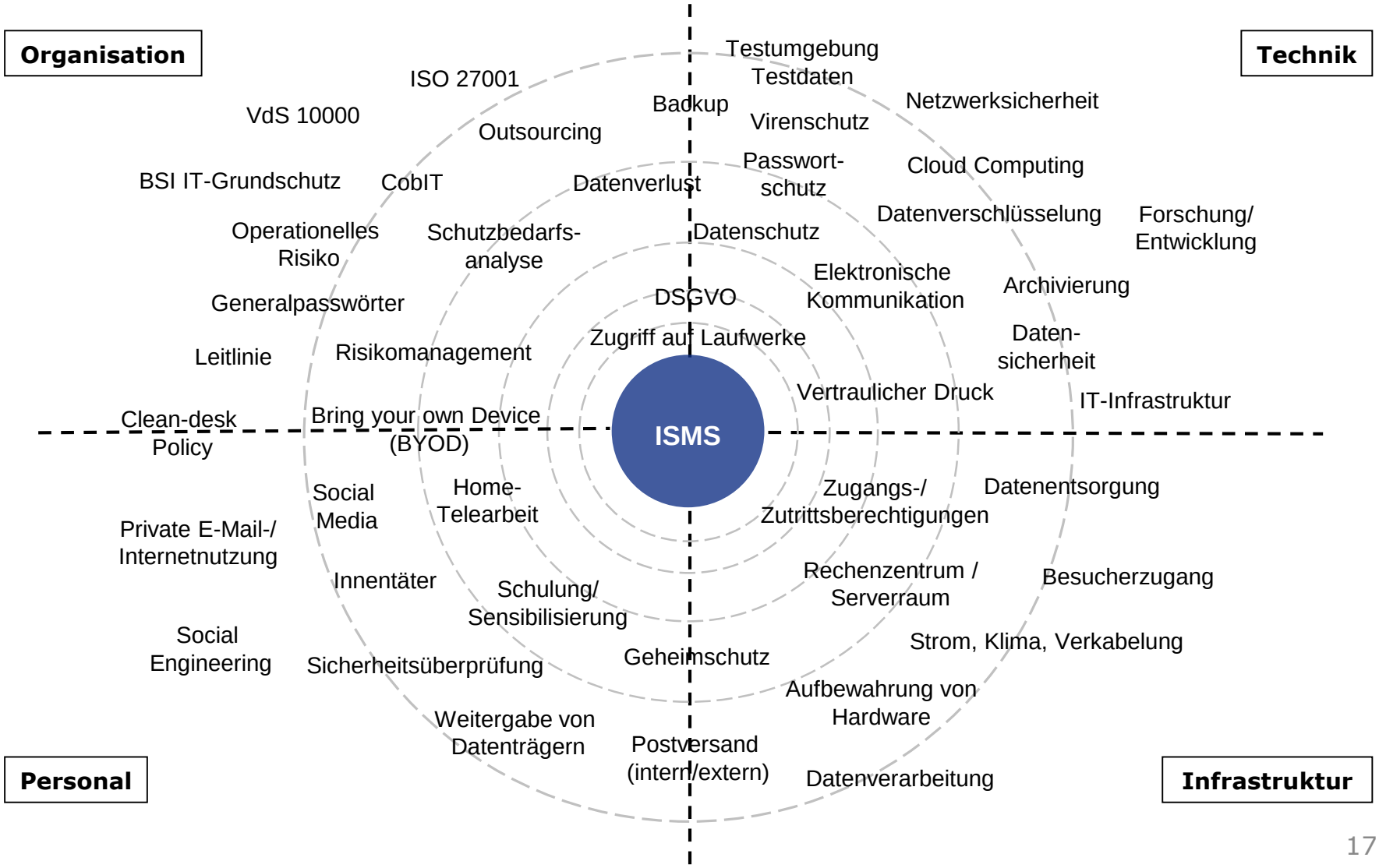
Nachweis der Umsetzung (§8a (3) BSIG)

In regelmäßigen Zeitabständen (alle 24 Monate) muss die **Erfüllung der Vorgaben** zu Sicherheitsstandards und Meldepflicht **nachgewiesen** werden. Hierfür müssen fortlaufend geeignete Nachweise gesammelt und durch Managementebenen ausgewertet werden.

Lösungsansätze und wirksamer Schutz

- Bestandsaufnahme und Gap-Analyse der kritischen Geschäftsprozesse und der organisatorischen und technischen Sicherheitsmaßnahmen.
- Aufbau und Betrieb eines Informationssicherheitsmanagementsystems anhand etablierter Sicherheitsstandards (z. B. ISO 27001 oder BSI IT-Grundschutz).
- Umsetzung der Anforderungen des IT-Sicherheitsgesetzes, falls Sie Betreiber einer kritischen Infrastruktur sind.
- Aufbau einer Notfallorganisation durch Erstellung von Notfallkonzepten und Durchführung von Notfallübungen.
- Umsetzung von begleitenden Maßnahmen, wie z.B. Schulungen für Ihr Personal.

Informationssicherheitsmanagementsysteme



Fazit

- Betreiber Kritischer Infrastrukturen haben eine hohe gesellschaftliche Verantwortung!
- Die Bedrohungen im Cyberraum nehmen stetig zu!
- Handeln Sie präventiv! Behalten Sie die Kontrolle über Ihre Informationswerte!

Ein guter Ansatz von Governance, Risk & Compliance dient dem Wohl der Gesellschaft und Ihres Unternehmens!

Wir bringen die Dinge auf den PUNKT.

RST

Dr. Marian Corbe

- Geschäftsführender Gesellschafter RST Informationssicherheit GmbH
- Telefon: 0201 87999 52
- Mobil: 0151 11775994
- E-Mail: mcorbe@rst-beratung.de

Tätigkeitsschwerpunkte u.a.:

- Implementierung, Reifegradfeststellung und Auditierung von Informationssicherheitsmanagementsystemen (ISMS)
- Beratung von Betreibern Kritischer Infrastrukturen zur Umsetzung der Anforderungen des IT-Sicherheitsgesetzes und zur Durchführung der Nachweisprüfungen gemäß §8a (3) BSI-Gesetz
- Informationssicherheitsschulungen und Sensibilisierungsmaßnahmen
- Erstellung von Notfallkonzepten, Aufbau von Notfallorganisationen, Durchführung von Krisenübungen und Krisenstabsarbeit