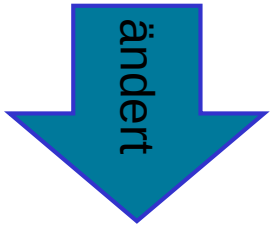
Die langen Schatten des IT-Sicherheitsgesetzes

Rüdiger Gruetz
Klinikum Braunschweig
Geschäftsbereich IT und Medizintechnik

IT-Sicherheitsgesetz



Art. 2.: Atomgesetz
Art. 3 : Energiewirtschaftsgesetz
Art. 4 : Telemediengesetz
Art. 5 : Telekommunikationsgesetz
Art. 6 : Bundesbesoldungsgesetz
Art. 7 : BKA-Gesetz

Art. 1 : BSI-Gesetz

BSI-KRITISV

Das ITSiG imTelekommunikationsgesetz

- Pflicht zu IT-Sicherheitsmaßnahmen nach dem „Stand der Technik“ zum Schutz personenbezogener Daten und vor unerlaubten Eingriffen in die Infrastruktur
  (§ 109 Absätze 1 und 2 TKG)
- Informationspflicht über Schadprogramme, ihre Erkennung und Beseitigung gegenüber den Nutzern
  (§ 109a Absatz 4 TKG)
- Meldepflicht bei erheblichen IT-Störungen gegenüber den Nutzern
  (§ 109a Absatz 5 TKG).

➢ Für Anbieter von Telekommunikationsdiensten

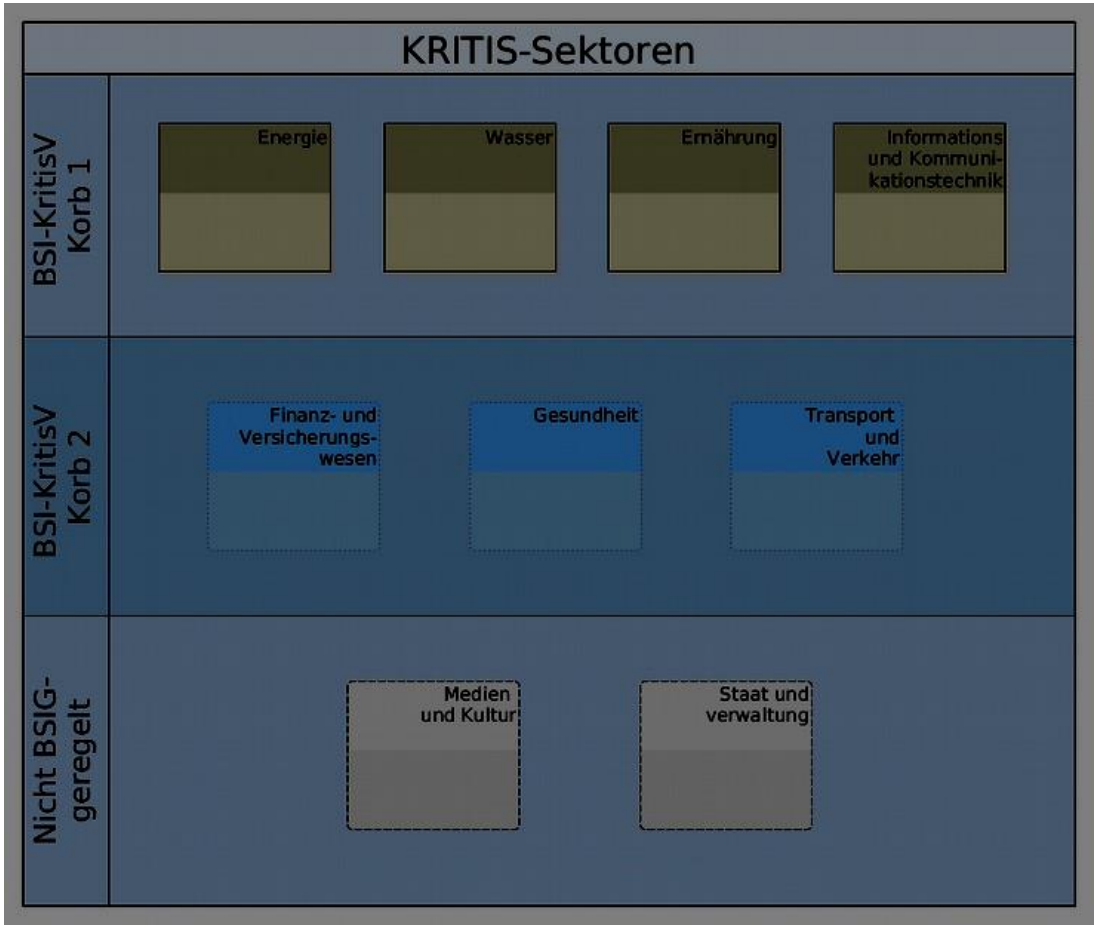
Das ITSiG im Telemediengesetz

- Pflicht zu IT-Sicherheitsmaßnahmen nach dem „Stand der Technik“ zum Schutz personenbezogener Daten und vor unerlaubten Eingriffen in die für die „Telemedienangebote genutzten technischen Einrichtungen“
  (§ 13 Absatz 7 TMG)

Weitere Pflichten bleiben unverändert !
(z.B.: Unterrichtung, Einwilligung, Impressum, …)

➢ *Für Anbieter von Webangeboten*

Anforderungen aus dem IT-Sicherheitsgesetz



Quelle: BSI

Wer fällt unter die BSI-KRITISV ?

Bisher z.B.

- Fernwärmenetz
  Angeschlossene Haushalte : 250 000

- Anlage zur Produktion von Lebensmitteln
  Menge der gewonnenen Lebensmittel :
  Speisen: 434 500 t/Jahr oder
  Getränke: 350 Millionen l/Jahr

(BSI-KRITISV v. 22.04.2016)

Wer fällt unter die BSI-KRITISV ?

Vorgesehene Erweiterung zum Mai 2017 (u.a.)

- Krankenhäuser
  vollstationäre Fälle pro Jahr: 30.000
  (inkl. der eigenen Labore)

- Labore
  Anzahl Aufträge/Jahr 1.500.000

Mit Veränderung der Risikobetrachtung !

- Fokus gem. BSI-Gesetz liegt auf der Versorgung der Bevölkerung
  nicht auf Unternehmensrisiken

Wesentliche Pflichten aus dem BSI-Gesetz

- § 8a (1)
  Angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse

- § 8a (2) Möglichkeit zu branchenspezifischen Sicherheitsstandards mit definiertem Stand der Technik für die Branche

- § 8a (3) Nachweispflicht mindestens alle zwei Jahre für die Erfüllung dieser Anforderungen

- § 8a (3) Übermittlung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel an das BSI

- § 8b (3,4) BSIG -> Meldepflicht für IT-Störungen

§ 14 Bußgeldvorschriften BSIG

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,

2. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 4
a) Nummer 1 oder b) Nummer 2 zuwiderhandelt,

3. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine Kontaktstelle nicht oder nicht rechtzeitig benennt oder

4. entgegen § 8b Absatz 4 Satz 1 Nummer 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 Buchstabe b mit einer Geldbuße bis zu hunderttausend Euro, in den übrigen Fällen des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

Und die Hersteller?

Bisher positives Echo des BVITG

§7(3)

Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts vor

Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen…

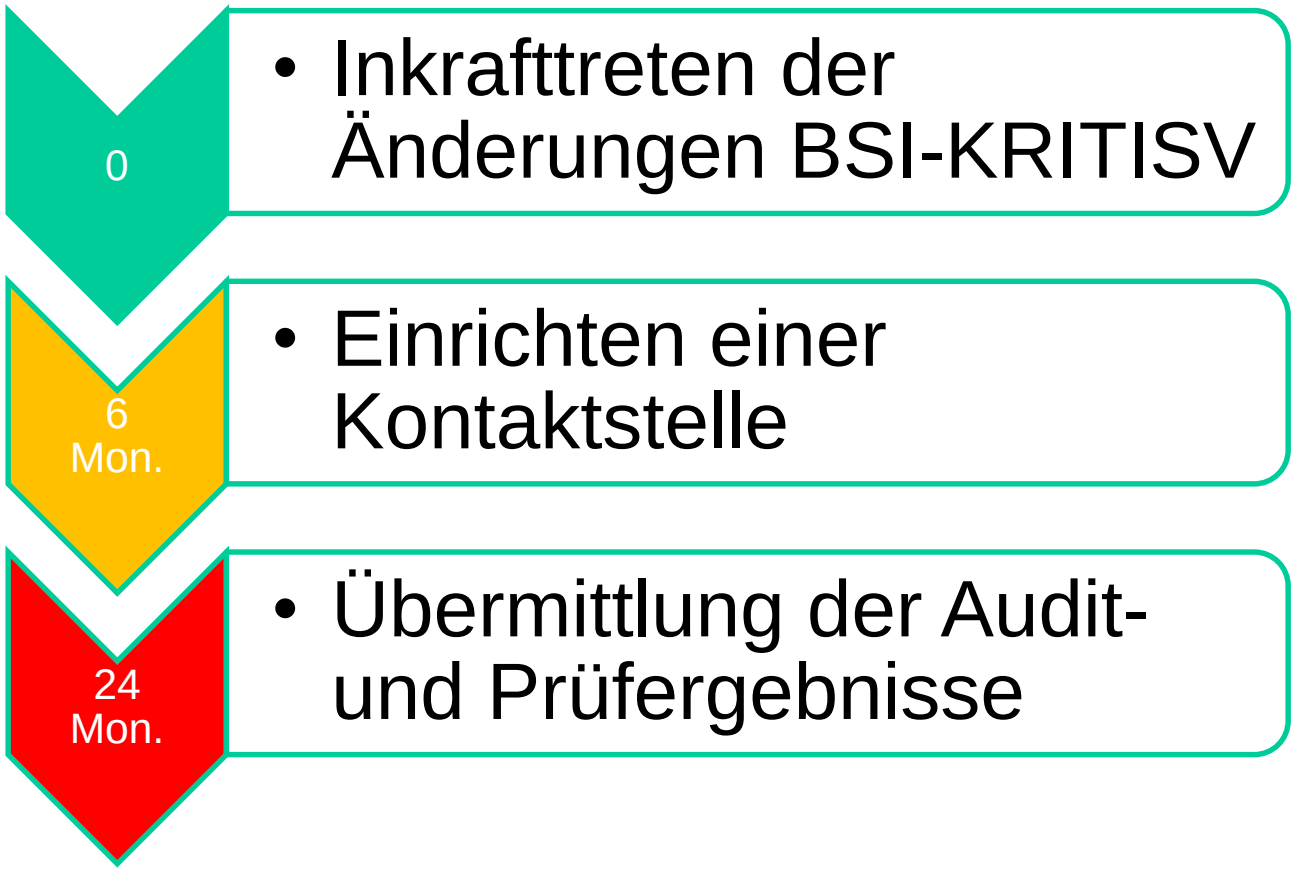
§7a (2)

Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.

§8b (6)

Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen..

Die Uhr läuft .....



Die Uhr läuft .....

6 Mon.

- Einrichten einer Kontaktstelle §8b(3)

Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind.
Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.

- Festlegung von Zuständigkeiten
- und Abläufen
- Definition der Störungskategorien
- Personalstellung
- …

Auch Kontakt- und Meldestelle für Datenschutzvorfälle, Ermittlungsbehörden, Versicherungen,
… ?

Beteiligung am BSI-Meldeverfahren auch freiwillig möglich =>Informationsgewinn

Die Uhr läuft .....

24 Mon.

- Übermittlung der Audit- und Prüfergebnisse §8a(3)

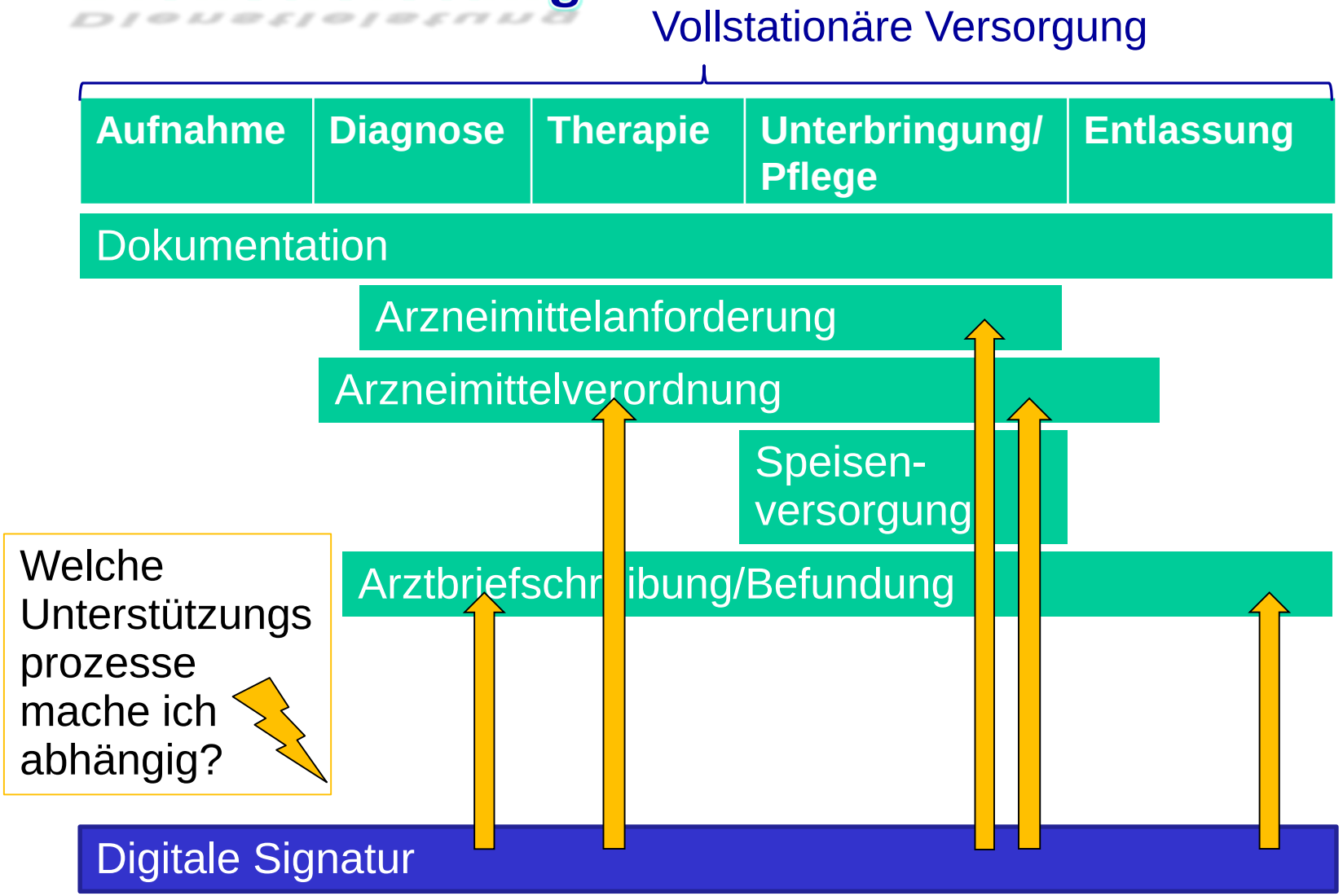
Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen.

- Identifizierung der Systeme, Komponenten, Prozesse
- Umsetzung der Sicherheitsmaßnahmen
- Herstellen der Auditierbarkeit
- Erstellen von Umsetzungsplänen
- Durchführung der Prüfung(en)
- ..

Und wenn der Hersteller nicht mitspielt?

-> §7 BSIG

Unterstützung der kritischen Dienstleistung



Einige weiterführende Quellen

Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/mindeststandards_node.html

https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/it_sig_node.html

Datenschutz:

http://www.datenschutz.de/

Umsetzungsplan Kritische Infrastrukturen

http://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/nationales_node.html

http://www.kritis.bund.de/SubSites/Kritis/DE/Aktuelles/aktuelles_node.html

Ihre Fragen ..