TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT-Workshop "Industrial Security" 2015

München, 11.06.2015

# Industrial Security

## Rechtliche Aspekte

RA Matthias Hartmann
HK2

HK2
Rechtsanwälte


- Rechtsanwalt
- Fachanwalt für IT-Recht
- Lehrbeauftragter der Europa-Universität Viadrina

# Überblick

- Haftung des Managements

Vertragsgestaltung / Beschaffung

Exkurs: Stand des ITSiG

# Haftung des Managements
# Grundlagen (Bsp. AktienG)

Verantwortlichkeit im Unternehmen für Industrial Security

1. Die Geschäftsleitung ist verantwortlich für die Organisation des Unternehmens
   - § 76 Abs. 1 AktG: Der Vorstand hat unter eigener Verantwortung die Gesellschaft zu leiten.

2. Bei Verletzung der Pflicht ist die Geschäftsleitung dem Unternehmen zum Ersatz der daraus resultierenden Schäden verpflichtet
   - § 93 Abs. 2 (1) AktG: Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast.

# Haftung des Managements

3. Den Aufsichtsrat einer AG treffen eigene Prüfungs- und Überwachungspflichten

4. Verletzt der Vorstand einer AG seine Pflicht, muss der Aufsichtsrat Schadensersatz gegen den Vorstand durchsetzen

5. Schadensersatzansprüche des Unternehmens gegen das Management können spätestens vom Insolvenzverwalter geltend gemacht oder von Gläubigern gepfändet werden.

# Haftung des Managements
# Maßstab: Gesetzliche Grundlagen

HK2 Rechtsanwälte

Welcher Aufwand ist erforderlich?

1. Ordentlicher Geschäftsleiter
   - § 93 Abs. 1 (1) AktG (entspr. § 43 Abs.1 GmbHG): Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden
2. Risikomanagement
   - § 91 Abs. 2 AktG: Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.
3. Geschäftsbericht
   - Lagebericht muss zukünftige Entwicklungen und Fortbestand beurteilen, § 321 Abs. 1 HGB.
   - ➢ Gegenstand der Abschlussprüfung

# Haftung des Managements
# Maßstab: Rechtsprechung

1. Der Geschäftsleiter kann sich weder auf mangelnden Sachverstand berufen noch entlastet ihn eigene Unkenntnis
   - BGH 20.9.2011, II ZR 234/09:

   Haftung von Vorstand und Aufsichtsrat für unzulässige Kapitalerhöhungsmaßnahme

2. Schadensprävention und Risikokontrolle gehören zur Organisationspflicht der Geschäftsleitung
   - LG München 10.12.2013, 5 HKO 1387/10 (n. rkr.: 7 U 113/14):

   Seiner Organisationspflicht genügt ein Vorstandsmitglied bei entsprechender Gefährdungslage nur dann, wenn er eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation einrichtet. Entscheidend für den Umfang im Einzelnen sind dabei Art, Größe und Organisation des Unternehmens, die zu beachtenden Vorschriften, die geografische Präsenz wie auch Verdachtsfälle aus der Vergangenheit.

# Haftung des Managements: ordentlicher und gewissenhafter Geschäftsleiter

HK2 Rechtsanwälte

1. Standards sollten eingehalten werden
   - Gesetze
   - Stand der Technik
   - Normung
2. Grenzen des erlaubten Risikos:
   - Rechtsverletzungen (Legalitätspflicht, Bsp.: Datenschutz, IT-SicherheitsG, Festlegungen in Satzung)
   - Rechtsgüter Dritter
   - Risiken außerhalb der eigentlichen Geschäftstätigkeit
   - Keine Plausibilitätskontrolle zu Stellungnahmen Dritter
   - Vernunft (Risikosenkung ohne gesonderte Ressourcen möglich)
   - Unkenntnis
   - Gesamtverantwortung (auch bei Unzuständigkeit)

# Haftung des Managements
# Mindestanforderungen

1. Risiken aus dem Bereich Industrial Security müssen beobachtet werden

2. Risiken sind zu bewerten:
   - Wahrscheinlichkeit
   - Auswirkung auf Fortbestand des Unternehmens
   - Verhinderungsaufwand

3. Vernünftige Maßnahmen sind zu veranlassen, andernfalls ist eine Entscheidung des Unternehmens herbeizuführen

# Mindestanforderungen an Organisation

# Überblick

Haftung des Managements

- Vertragsgestaltung / Beschaffung

Exkurs: Stand des ITSiG

# Industrial Security vertraglich vereinbaren

HK2 Rechtsanwälte

## Vertragliche Ansprüche und Industrial Security

- Erfüllung
  - Bestimmung von Leistungspflichten
  - Einhaltung von Normen, Stand der Technik, Standards
  - ➢ sollten ausdrücklich vereinbart werden (allgemein angewandter Stand der Technik –> Neuester Stand von Wissenschaft und Technik)

- Schadensersatz wg Pflichtverletzung
  - Kardinalpflicht (Bsp.: Firewall wird zu spät eingerichtet bei Firmennetz, kein Schutz gegen DoS bei Hosting einer Website)
  - Nebenpflichten, auch vorvertraglich (Bsp. Geschäftsgeheimnisse des Kunden werden in ungesicherter Produktion ausgespäht)

# Vertragliche Regelungen zur Industrial Security

HK2 Rechtsanwälte

1. Problem
   - Sicherheitsrisiko Leistungen von Drittunternehmen
   - ➢ Lieferanten, Dienstleister, Berater
   - ➢ Outsourcing von Sicherheit

2. Sicherungsklauseln
   - Geheimhaltung
   - Verpflichtung auf Standards
   - Transparenz (Information, Offenlegung)
   - Mittel (auch Kosten) zur Kontrolle: Zugang, Zugriff, Audit, Dokumentation
   - Anpassung während der Laufzeit an geänderte Lage
   - Absicherung der Pflichten durch
     - Vertragsstrafen
     - Schadenspauschalen, Liquidated Damages

# Vertragliche Regelungen zur Industrial Security

HK2 Rechtsanwälte

## Vertragsstrafen / -pauschalen als Sicherungsmittel

- geeignet um schwer überprüfbare Vertragsverletzungen abzuschrecken oder um nicht beweisbare Schäden auszugleichen
- Problematisch in AGB, sollten also individuell ausgehandelt werden
- Achtung: Strafen unwirksam in vielen Rechtsordnungen (Bspw. § 2-718 UCC)

# Vertragliche Regelungen zur Industrial Security

HK2 Rechtsanwälte

Beispiel Anti Spy Klausel

- Y sichert zu, dass keine Schnittstellen oder sonstigen Zugangs- oder Zugriffsmöglichkeiten für Dritte (einschließlich Behörden) in den vertragsgegenständlichen Produkten bestehen - außer den in der Dokumentation beschriebenen - und verpflichtet sich für den Fall, dass solche vorhanden sind zu einer Zahlung von 5.000 EUR für jedes einzelne an X im Rahmen dieses Vertrags gelieferte Gerät bis zu einem Maximalbetrag von 150.000 EUR pro Vertragsjahr. X ist in diesem Fall außerdem zur Kündigung des Vertrags berechtigt.

# Vertragliche Regelungen zur Industrial Security

Beispiel Hack Test

- X kann jederzeit und wiederholt die Sicherheit der Anlage selbst oder durch Dritte prüfen lassen. Y ist hierbei im Rahmen des Angemessenen auf eigene Kosten zur Mitwirkung verpflichtet. Sofern sich dabei eine Schwachstelle ergibt, die (i) nach dem Y zugänglichen Stand von Wissenschaft und Technik hätte verhindert werden können (ii) ein tatsächliches Risiko mit einem mehr als unerheblichen Schadenspotential eröffnet und (iii) X hierüber nicht vor Beginn der Prüfung schriftlich von Y informiert worden ist, verpflichtet sich Y in jedem einzelnen Fall (i) die Kosten der Überprüfung zu erstatten und – außer Y hat die Schwachstelle nicht zu vertreten - (ii) eine Vertragsstrafe in Höhe von 15.000 EUR an X zu bezahlen.

# Überblick

Haftung des Managements

Vertragsgestaltung / Beschaffung

- Exkurs: Stand des ITSiG

# BT DS 18/4096: Entwurfsbegründung

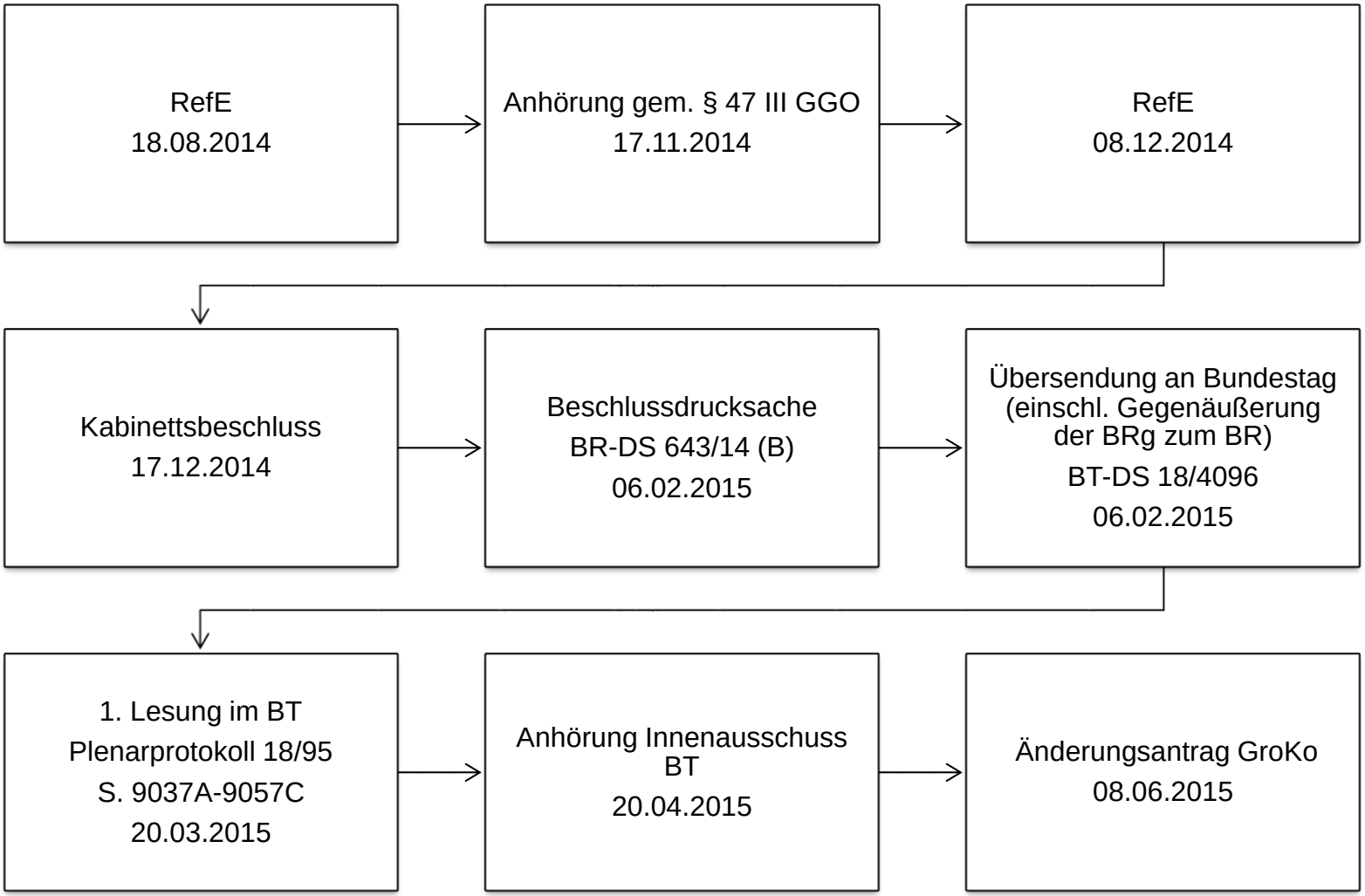
Problem

- „Die IT-Sicherheitslage in Deutschland ist weiterhin angespannt.“
- „Das (...) BSI erhält und analysiert (...) kontinuierlich eine Vielzahl von Informationen zu aktuellen Bedrohungssituation im Cyberraum. Die Angriffe erfolgen zunehmend zielgerichtet und sind technologisch immer ausgereifter und komplexer.“
- „... IT-Sicherheitsniveau bei Kritischen Infrastrukturen ist derzeit sehr unterschiedlich“

# ITSiG-E

- Parlamentarischer Verfahrensstand
- Aufbau + Inhalt
- Kritik + Alternativen
- Voraussetzungen und Folgen

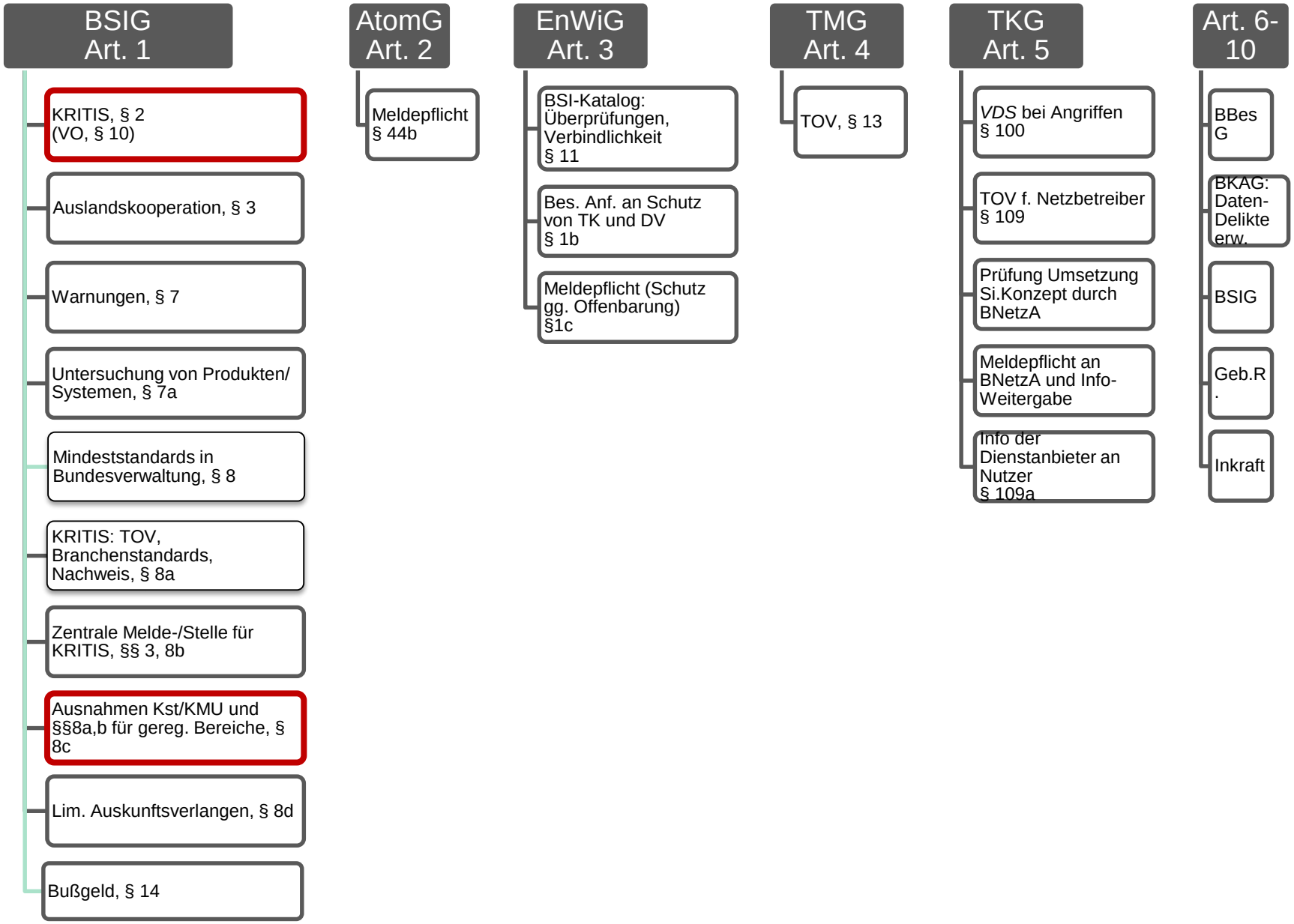
# Verfahrensstand



Wann kommt die NIS Richtlinie auf EU-Ebene!?

Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union

- Voraussichtlich in 2015,
- dann 18 Monate zur Umsetzung


BSIG Art. 1
KRITIS, § 2 (VO, § 10)
Auslandskooperation, § 3
Warnungen, § 7
Untersuchung von Produkten/ Systemen, § 7a
Mindeststandards in Bundesverwaltung, § 8
KRITIS: TOV, Branchenstandards, Nachweis, § 8a
Zentrale Melde-/Stelle für KRITIS, §§ 3, 8b
Ausnahmen Kst/KMU und §§8a,b für gereg. Bereiche, § 8c
Lim. Auskunftsverlangen, § 8d
Bußgeld, § 14
AtomG Art. 2
Meldepflicht § 44b
EnWiG Art. 3
BSI-Katalog: Überprüfungen, Verbindlichkeit § 11
Bes. Anf. an Schutz von TK und DV § 1b
Meldepflicht (Schutz gg. Offenbarung) §1c
TMG Art. 4
TOV, § 13
TKG Art. 5
*VDS* bei Angriffen § 100
TOV f. Netzbetreiber § 109
Prüfung Umsetzung Si.Konzept durch BNetzA
Meldepflicht an BNetzA und Info-Weitergabe
Info der Dienstanbieter an Nutzer § 109a
Art. 6-10
BBesG
BKAG: Daten-Delikte erw.
BSIG
Geb.R.
Inkraft

# KRITIS - § 2 Abs. 10 BSiG-E

Was sind KRITische InfraStrukturen?

- Sektorenzugehörigkeit
  - Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, *Wasser, Ernährung*, Finanz- und *Versicherungswesen*

- Fehlerfolgenerheblichkeit
  - Hohe Bedeutung für Funktionieren des Gemeinwesens, weil durch Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden

- Näheres soll in einer Rechtsverordnung bestimmt werden, § 10

➢ Versorgung mit was? Social Media, Versicherungen?

➢ Hersteller nicht adressiert sondern nur Betreiber

# Größenausnahmen - § 8c BSiG-E

§§ 8a, b gelten nicht für Kleinstunternehmen

Empfehlung 2003/361/EG:

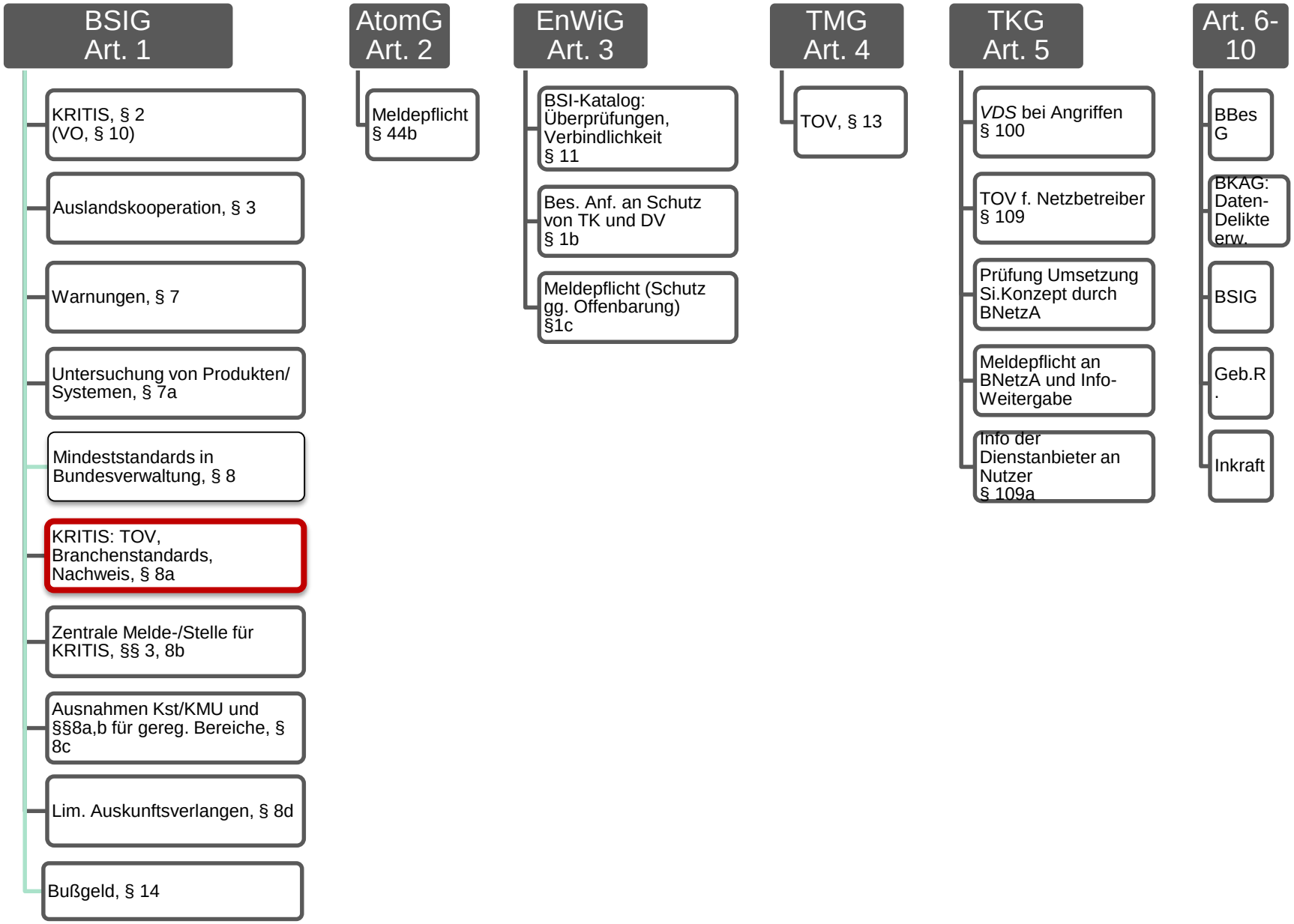
- Ein **mittleres Unternehmen:** weniger als 250 Mitarbeiter und Umsatz nicht größer 50 Mio. Euro oder Jahresbilanz nicht größer 43 Mio. Eur
- Ein **kleines Unternehmen:** weniger als 50 Mitarbeiter und Umsatz oder Jahresbilanz nicht größer 10 Mio. Eur
- Ein **Kleinstunternehmen:** weniger als 10 Mitarbeiter und Umsatz oder Jahresbilanz nicht größer 2 Mio. Eur

# Bereichsausnahmen - § 8c BSiG-E

Einschränkungen der §§ 8a und 8b wenn Sonderregelungen existieren:

- TK-Netz oder TK-Dienste
- Energie (Netz, Anlagen)
- AtomG
- Alle anderen Betreiber, **soweit** sie bereits § 8a oder 8b Abs. 3-5 vergleichbaren Anforderungen unterliegen

  - Telematikinfrastruktur im Gesundheitswesen
  - Neuer 13 Abs. 7 TMG?
  - BDSG wohl nicht gemeint …


BSIG Art. 1
KRITIS, § 2 (VO, § 10)
Auslandskooperation, § 3
Warnungen, § 7
Untersuchung von Produkten/ Systemen, § 7a
Mindeststandards in Bundesverwaltung, § 8
KRITIS: TOV, Branchenstandards, Nachweis, § 8a
Zentrale Melde-/Stelle für KRITIS, §§ 3, 8b
Ausnahmen Kst/KMU und §§8a,b für gereg. Bereiche, § 8c
Lim. Auskunftsverlangen, § 8d
Bußgeld, § 14
AtomG Art. 2
Meldepflicht § 44b
EnWiG Art. 3
BSI-Katalog: Überprüfungen, Verbindlichkeit § 11
Bes. Anf. an Schutz von TK und DV § 1b
Meldepflicht (Schutz gg. Offenbarung) §1c
TMG Art. 4
TOV, § 13
TKG Art. 5
VDS bei Angriffen § 100
TOV f. Netzbetreiber § 109
Prüfung Umsetzung Si.Konzept durch BNetzA
Meldepflicht an BNetzA und Info-Weitergabe
Info der Dienstanbieter an Nutzer § 109a
Art. 6-10
BBesG
BKAG: Daten-Delikte erw.
BSIG
Geb.R.
Inkraft

# TOV - § 8a ITSiG-E

(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.

(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können **branchenspezifische Sicherheitsstandards** zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen (…) .

(3) Die Betreiber Kritischer Infrastrukturen haben mindestens **alle zwei Jahre** die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise **nachzuweisen**. (…). Das Bundesamt kann bei Sicherheitsmängeln verlangen:
1. Auditergebnisse
2. die Beseitigung der Sicherheitsmängel

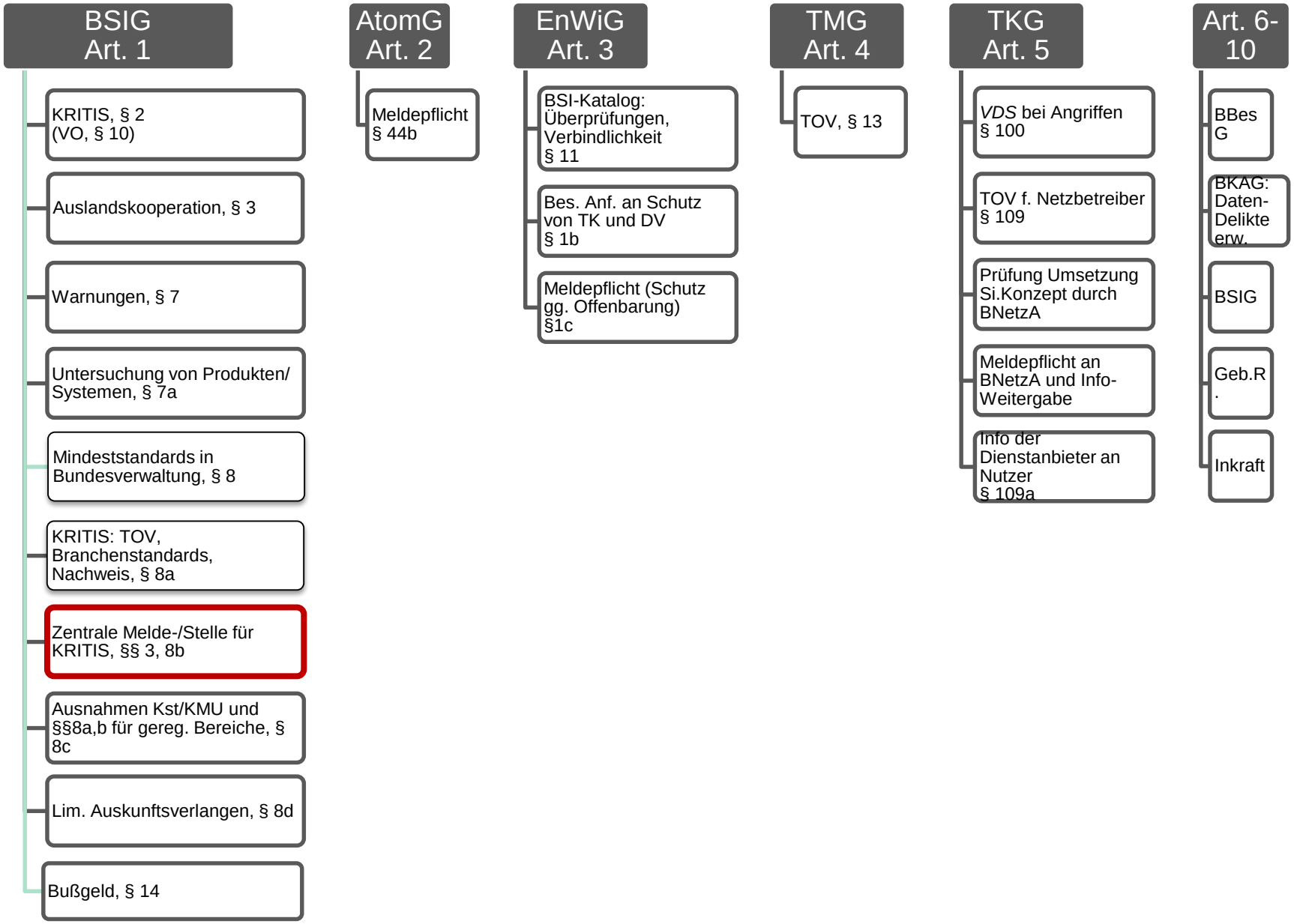
(4) BSI kann Anforderungen an Audits vorgeben

# KRITIS: TOV, Branchenstandards, Nachweis

- Technische und organisatorische Vorkehrungen (TOV)
  - Kein Mindestmaß an IT-Sicherheit
  - Keine Bewertungskriterien/ -maßstäbe
  - Stand der Technik ist nur zu „berücksichtigen“ nicht Maßstab
  - Branchenverbände werden nur Minimum vorschlagen
  - Verhältnis zum technischen Datenschutz unklar

- Nachweiserbringung:
  - Audits, Zertifikate
  - BSI kann diese anfordern bei Sicherheitsmängeln

- Bußgeld: Verletzung der TOV, Anordnungen bei Mängeln


BSIG Art. 1
KRITIS, § 2 (VO, § 10)
Auslandskooperation, § 3
Warnungen, § 7
Untersuchung von Produkten/ Systemen, § 7a
Mindeststandards in Bundesverwaltung, § 8
KRITIS: TOV, Branchenstandards, Nachweis, § 8a
Zentrale Melde-/Stelle für KRITIS, §§ 3, 8b
Ausnahmen Kst/KMU und §§8a,b für gereg. Bereiche, § 8c
Lim. Auskunftsverlangen, § 8d
Bußgeld, § 14
AtomG Art. 2
Meldepflicht § 44b
EnWiG Art. 3
BSI-Katalog: Überprüfungen, Verbindlichkeit § 11
Bes. Anf. an Schutz von TK und DV § 1b
Meldepflicht (Schutz gg. Offenbarung) §1c
TMG Art. 4
TOV, § 13
TKG Art. 5
VDS bei Angriffen § 100
TOV f. Netzbetreiber § 109
Prüfung Umsetzung Si.Konzept durch BNetzA
Meldepflicht an BNetzA und Info-Weitergabe
Info der Dienstanbieter an Nutzer § 109a
Art. 6-10
BBesG
BKAG: Daten-Delikte erw.
BSIG
Geb.R.
Inkraft

# BSI - § 8b ITSiG-E

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu **sammeln und auszuwerten**, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,
2. deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu **analysieren**,
3. das **Lagebild** bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren und
4. **unverzüglich**
   a) die Betreiber Kritischer Infrastrukturen über sie betreffende Informationen nach den Nummern 1 bis 3,
   b) die zuständigen Aufsichtsbehörden und die sonst zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3 sowie
   c) die zuständigen Aufsichtsbehörden der Länder oder die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3

**zu unterrichten**.

# Meldepflicht - § 8b ITSiG-E

(4) Betreiber Kritischer Infrastrukturen haben **erhebliche Störungen** der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

1. **führen können** oder
2. **geführt haben**,

über die Kontaktstelle unverzüglich an das Bundesamt **zu melden**. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten.

# Kritik § 8b ITSiG-E

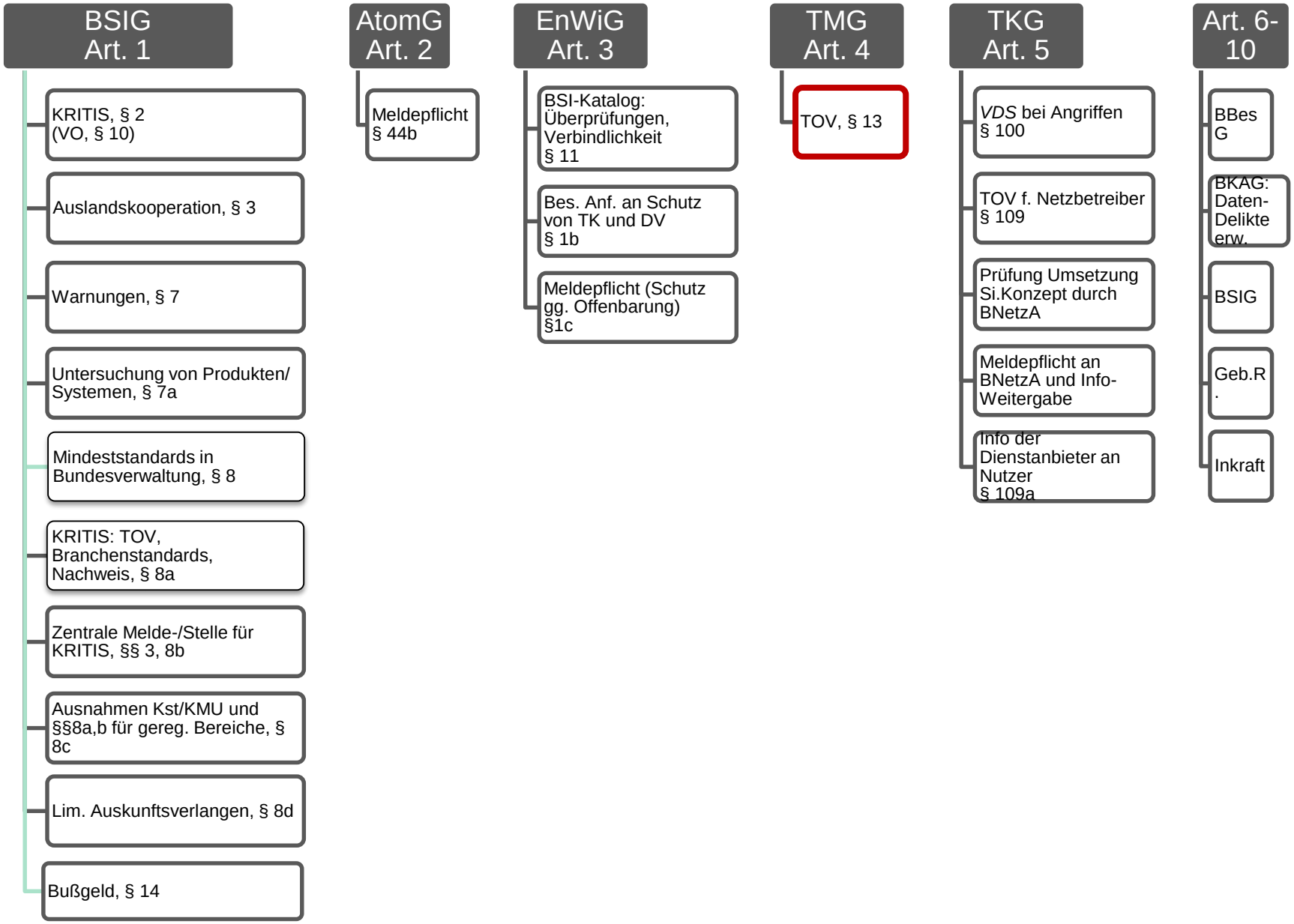
- Umgang mit Erkenntnissen
  - Warnungen, § 4 ITSiG-E
  - Untersuchungsergebnisse, § 7a ITSiG-E
- ➢ Keine Weitergabepflicht
- ➢ Unabhängigkeit des BSI?
- ➢ Unbestimmte Rechtsbegriffe
- Bußgeld: unterlassene / unrichtige Meldungen

# Anordnung an Hersteller § 8b ITSiG-E

Neu (08.06.2015):

(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. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8c Absatz 3 entsprechend.

- Unbestimmte Rechtsgrundlage zu allen möglichen Mitwirkungsmaßnahmen:
  - Offenlegung Code
  - Zugang zu verschlüsselten Informationen
  - „unmögliche“ Anordnungen
  - Wer trägt die Kosten?


BSIG Art. 1
KRITIS, § 2 (VO, § 10)
Auslandskooperation, § 3
Warnungen, § 7
Untersuchung von Produkten/ Systemen, § 7a
Mindeststandards in Bundesverwaltung, § 8
KRITIS: TOV, Branchenstandards, Nachweis, § 8a
Zentrale Melde-/Stelle für KRITIS, §§ 3, 8b
Ausnahmen Kst/KMU und §§8a,b für gereg. Bereiche, § 8c
Lim. Auskunftsverlangen, § 8d
Bußgeld, § 14
AtomG Art. 2
Meldepflicht § 44b
EnWiG Art. 3
BSI-Katalog: Überprüfungen, Verbindlichkeit § 11
Bes. Anf. an Schutz von TK und DV § 1b
Meldepflicht (Schutz gg. Offenbarung) §1c
TMG Art. 4
TOV, § 13
TKG Art. 5
*VDS* bei Angriffen § 100
TOV f. Netzbetreiber § 109
Prüfung Umsetzung Si.Konzept durch BNetzA
Meldepflicht an BNetzA und Info-Weitergabe
Info der Dienstanbieter an Nutzer § 109a
Art. 6-10
BBesG
BKAG: Daten-Delikte erw.
BSIG
Geb.R.
Inkraft

# § 13 TMG-E

(7) Diensteanbieter haben, soweit dies **technisch möglich** und **wirtschaftlich zumutbar** ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch **technische und organisatorische Vorkehrungen** sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
2. diese
   a) gegen Verletzungen des Schutzes personenbezogener Daten und
   b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gesichert sind. Vorkehrungen nach Satz 1 **müssen den Stand der Technik berücksichtigen**. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

# TMG

- TOV ohne Brancheneinbeziehung
- „geschäftsmäßig“ = auch Werbefinanziert
- Keine Umsetzungsfrist
- Keine Kleinstunternehmerausnahme, § 8c I BSIG-E
- Keine Regelung entsprechend § 100 TKG
  - „Kleine Vorratsdatenspeicherung“ zu Sicherheitszwecken wieder gelöscht
- § 16 TMG-E: Verstöße bußgeldbewehrt (bis 50 TEur) bei Zuwiderhandlung der Sicherstellung von
  - § 13 Abs. 7 S. 1 Nr. 1: unerlaubter Zugriff auf techn. Einrichtungen
  - § 13 Abs. 7 S. 1 Nr. 2 lit. a: Schutz der personenbezogenen Daten

HK2
Rechtsanwälte

# Vielen Dank