Rechtliche Regulierung von Cybersecurity

OPEN CAMPUS 2017, Universität Bremen

17.06.2017

Dr. Dennis-Kenji Kipker
IGMR
Universität Bremen

Gefördert vom
FKZ: 16KIS0213
bis 16KIS0216

Bundesministerium für Bildung und Forschung

Universität der Bundeswehr München

FAU Friedrich-Alexander Universität Erlangen-Nürnberg

DKE VDE DIN

Universität Bremen

„**WannaCry**“, 12.05.2017:

„Dabei ist wichtig, dass bei IT-Störungen zwingend die Ereignisse an das **Bundesamt für Sicherheit in der Informationstechnik** gemeldet werden, um daraus Schlüsse zu ziehen und im Zweifel Gegenmaßnahmen zu entwickeln. Dazu müssen im **IT-Sicherheitsgesetz** die Vorkehrungen getroffen werden.“

- Alexander Dobrindt, Bundesminister für Verkehr und digitale Infrastruktur, 15.05.2017

Corporate Governance
&
(IT-Security) Compliance

- Was ist Compliance?
  - “Compliance” übersetzt:
    - Einhaltung
    - Übereinstimmung
    - Regelbefolgung
  - Compliance somit nichts anderes als die Einhaltung und Befolgung von Vorgaben
  - **Offener Begriff ohne starre Definition**

Was ist Corporate Governance?

- "Corporate Governance" übersetzt: Grundsätze der Unternehmensführung
- Hintergrund: Unternehmensleitung hat Verantwortung für Gesellschaft, Anteilseigner, Mitarbeiter und Kunden
- Umfasst inhaltlich u.a.:
  - Risikobewertung
  - Transparenz
  - Funktionsfähige Unternehmensstrukturen
  - Wert- und Nachhaltigkeit unternehmerischer Entscheidungen
  - Angemessene Interessenvertretung der verschiedenen Akteure eines Unternehmens
  - **Somit: Festlegung von Aufgaben, Zielen und Kontrolle der Unternehmensführung**

- # Wie ist Corporate Governance zu realisieren?
  - Maßnahmen:
    - Befolgung von anerkannten Standards und (branchenspezifischen) Regelwerken
    - Entwicklung und Befolgung von eigenen Unternehmensleitlinien
    - **Einhaltung von gesetzlichen Vorschriften**
    - Implementierung von Leitungs- und Kontrollstrukturen zur Umsetzung und Überprüfung der Maßnahmen
  - **Compliance ist somit ein Bestandteil von Corporate Governance**

Warum Compliance und Corporate Governance?

- Vorrangig: **Vorteile für das Unternehmen** in wirtschaftlicher Hinsicht durch transparente, nachhaltige und kontrollierte Unternehmensführung
- Aber auch **Abwendung möglicher Nachteile**, die durch Nichteinhaltung von Vorschriften & Best Practices entstünden:
  - Straf- und Ordnungswidrigkeitenrecht (z.B. § 404 AktG; § 44 BDSG; § 43 BDSG)
  - Gewerbeaufsichtsrechtliche Maßnahmen wegen Unzuverlässigkeit, z.B. Entziehung der Gewerbeerlaubnis
  - Ansprüche auf Unterlassung, Schadensersatz und Schmerzensgeld (zivilrechtliche Haftung)
  - Versicherungsbezogene Folgen (Leistungsfreiheit oder -minderung des Versicherers, erhöhte Versicherungsprämien z.B. bei Cyber-Versicherungen)
  - Informationspflicht ggü. der Öffentlichkeit bei Datenlecks gem. § 42a BDSG
  - Reputationsverlust, mittelbare wirtschaftlich benachteiligende Konsequenzen

Was ist IT-(Security-) Compliance?

- Einhaltung derjenigen Vorgaben, die sich speziell mit **IT-Sicherheit**, im weitesten Sinne auch **Datenschutz**, befassen
- **Unterschiedlichste Erkenntnisquellen** für IT-(Security)Compliance:
  - Allgemeine gesetzliche Vorschriften (z.B. BSIG, BDSG)
  - Branchenspezifische gesetzliche Vorschriften (z.B. für Banken, Versicherungen, Industrie, IuK, Logistik, öffentliche Verwaltung)
  - Normen und Standards
  - Unternehmensinterne Vorgaben, vertragliche Bestimmungen und Selbstverpflichtungen (Geheimhaltungsverpflichtung, Vertraulichkeitsvereinbarung)
  - "Soft Law" (z.B. Deutscher Corporate Governance-Kodex – DCGK, § 161 AktG)
- Daraus folgt auch: **Keine kodifizierte Regelung** der IT-Sicherheit
- **Herausforderung** für IT-(Security)Compliance

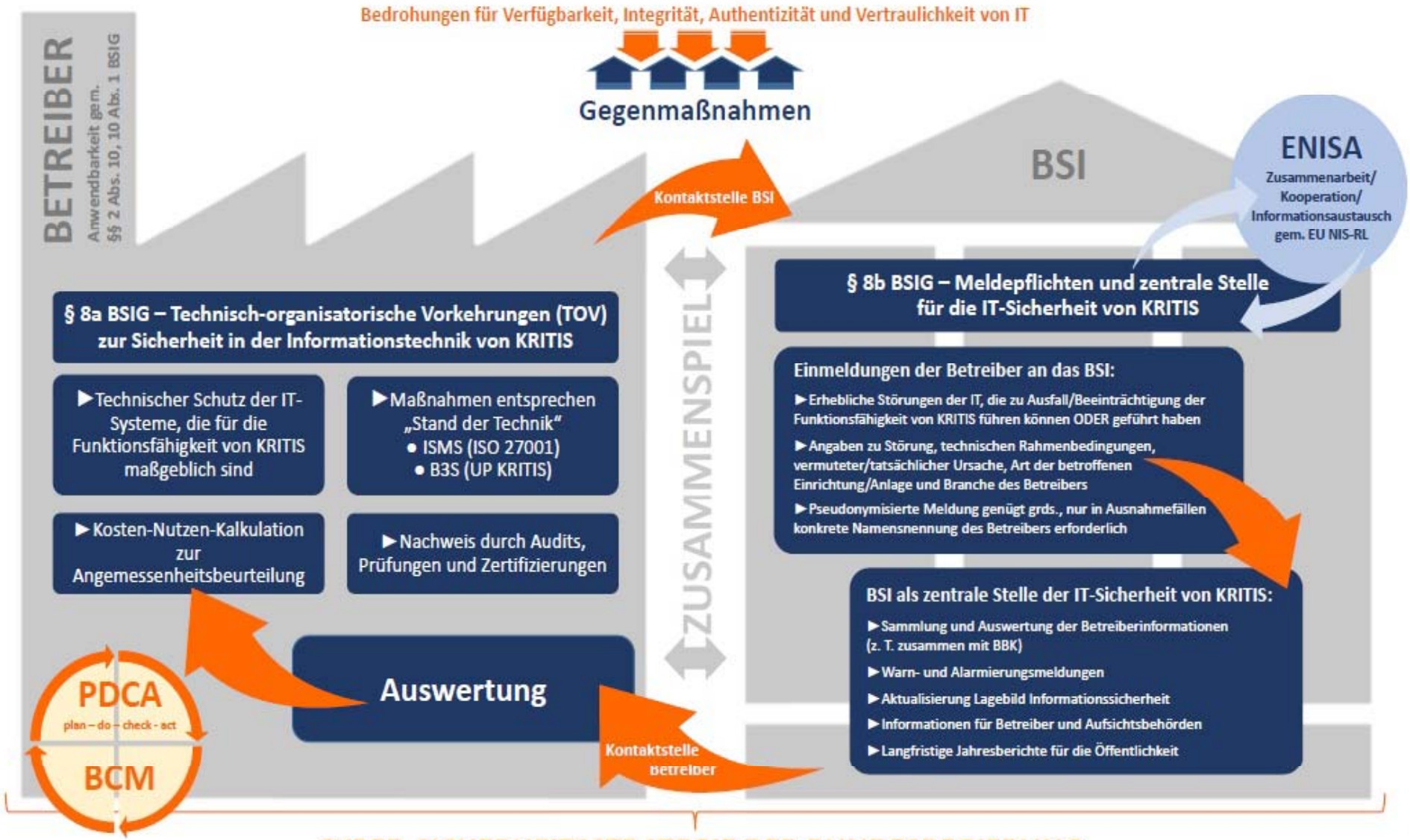
Corporate Governance & (IT-Security) Compliance

- Neue Nationale Cyber-Sicherheitsstrategie von November 2016:
  - Handlungsfeld 1 – Sicheres und selbstbestimmtes Handeln in einer digitalisierten Welt
  - Handlungsfeld 2 – Gemeinsamer Auftrag von Staat und Wirtschaft:
    - **Kritische Infrastrukturen sichern**
    - **Unternehmen in Deutschland schützen**
  - Handlungsfeld 3 – Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur:
    - **Nationales Cyber-Abwehrzentrum** weiterentwickeln
    - Fähigkeit zur **Analyse und Reaktion vor Ort** stärken
    - **Strafverfolgung im Cyber-Raum** intensivieren
    - **Cyber-Spionage** und **Cyber-Sabotage** effektiv bekämpfen
    - **Frühwarnsystem gegen Cyber-Angriffe** aus dem Ausland
    - Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (**ZITiS**)
    - **CERT-Strukturen in Deutschland** stärken
    - **Bundesverwaltung sichern**
  - Handlungsfeld 4 – Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

- Deutsche Erkenntnisquellen für die IT-(Security) Compliance – Beispiele "von A bis Z":
  - AktG, § 91
  - AtG, §§ 7 ff., 44b
  - BDSG, §§ 9, 9a, 11, 42a
  - BSIG, §§ 3, 4, 7, 7a, 8a ff.
  - EnWG, §§ 11 ff., 21e, 49
  - GmbHG, § 43
  - KWG, § 25a
  - TKG, §§ 109, 109a
  - TMG, § 13
  - VAG, § 64a
  - WpHG, § 33
  - …
  - **IT-SiG (2015) → Artikelgesetz! → Änderungsgesetz ändert nur Reihe von Fachgesetzen**

Dr. Dennis-Kenji Kipker
IGMR
Universität Bremen

INFORMATIONSFLÜSSE UND SCHUTZPROZESSE IN DER IT-SICHERHEIT KRITISCHER INFRASTRUKTUREN



CYBER-SICHERHEITSSTRATEGIE DER BUNDESREGIERUNG

(BSIG ergänzt durch Spezialregelungen wie § 109 TKG, § 11 EnWG, § 44b AtG; Öffnungsklausel in § 8c Abs. 2 Nr. 5, Abs. 3 Nr. 5 BSIG, z. B. für Telematik im Gesundheitswesen)

- Europäische Erkenntnisquellen für die IT-(Security) Compliance – Beispiele “von alt nach neu”:
  - RL 2002/58/EG über elektronische **Kommunikationsnetze** (E-Privacy-RL) und 2009/136/EG (Cookie-RL)
  - RL 2006/32/EG zu **Energieeffizienz** und **Energiedienstleistungen**
  - RL 2008/114/EG über die **Ermittlung und Ausweisung europäischer kritischer Infrastrukturen** und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern
  - RL 2009/72/EG zum **Elektrizitätsbinnenmarkt**
  - RL 2013/40/EU über **Angriffe auf Informationssysteme**
  - RL 2014/53/EU über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von **Funkanlagen** auf dem Markt (RED)
  - VO (EU) Nr. 910/2014 über **elektronische Identifizierung und Vertrauensdienste** für elektronische Transaktionen im Binnenmarkt (eIDAS VO)
  - **VO (EU) 2016/679** zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, **Art. 5 Abs. 1 lit. f und Art. 32 (EU DS-GVO, anzuwenden ab 25.05.2018)**
  - **EU NIS-RL (2016) + nationales Umsetzungsgesetz (2017)**

NIS-RL – Rechtspolitische Erwägungen:

- NIS als zentraler Faktor für ein **funktionierendes Gemeinwesen und für die Wirtschaft** der EU, **Kernelement der europäischen Cyber-Sicherheitsstrategie von 2013**
- Tragweite, Häufigkeit und Auswirkungen von Sicherheitsvorfällen nehmen zu
- **EU-weit koordinierte Cyber-Sicherheitsstrategie** setzt hinsichtlich aller Mitgliedstaaten ein Mindestniveau voraus
- **Bestehende Fähigkeiten nicht ausreichend**, um ein hohes Niveau von NIS in der EU zu gewährleisten
- **Uneinheitliches Schutzniveau der Mitgliedstaaten**
- Fehlende gemeinsame Anforderungen für Betreiber von „wesentlichen Diensten“
- **NIS-RL konzipiert als „umfassender Ansatz** […], der gemeinsame Mindestanforderungen für Kapazitätsaufbau und -planung, Informationsaustausch, Zusammenarbeit sowie gemeinsame Sicherheitsanforderungen für **Betreiber wesentlicher Dienste** und **Anbieter digitaler Dienste** beinhaltet“

- NIS-RL – Zentrale Regelungsgegenstände:
  - Festlegung **nationale Strategie für NIS**
  - Einrichtung einer **Kooperationsgruppe** zur strategischen Zusammenarbeit und für **interstaatlichen Informationsaustausch**
  - Einrichtung eines **CSIRTs-Netzwerks** (Computer Security Incident Response Teams Network) zur Förderung der **operativen interstaatlichen Zusammenarbeit** im Bereich IT-Security
  - Festlegung von **Sicherheitsanforderungen** und **Meldepflichten** für die Betreiber **wesentlicher Dienste** und für Anbieter **digitaler Dienste**
  - Benennung von nationalen **IT-Sicherheitsbehörden**, zentralen Anlaufstellen und CSIRTs

NIS-RL – Rechtsnatur:

- EU-Richtlinie (RL) ≠ EU-Verordnung (VO)
- Art. 288 AEUV (Vertrag über die Arbeitsweise der EU):
  - „Die VO hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat." → Kein nationales Umsetzungsgesetz zur Wirksamkeit notwendig (z.B. EU DS-GVO)
  - „Die RL ist für jeden Mitgliedstaat […] hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel." → Nationales Umsetzungsgesetz zur Wirksamkeit notwendig
- Deutschland: **Nationales Umsetzungsgesetz** ändert Einzelgesetze ab („Gesetz zur Umsetzung der EU RL 2016/1148"), **Bundestagsbeschluss am 27.04.2017** erfolgt
- **Mindestharmonisierung:** Deutschland kann auch ein höheres IT-Sicherheitsniveau schaffen, als es die EU NIS-RL vorgibt

Nationales Umsetzungsgesetz – wesentliche Eckpunkte I:

- Wenig Überraschendes: Alle Gesetzesänderungen von BSIG, AtG und EnWG liegen **im erwartbaren Rahmen**
- Die Maßgaben für betroffene **Betreiber** von Kritischen Infrastrukturen erfahren **keine wesentlichen Anpassungen**
- Wesentlichste Änderungen:
  - Neue **Vorgaben an die Gesellschaft für Telematik** durch Änderung des SGB V
  - Neuer § 5a BSIG: **Unterstützungsleistungen des BSI** zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit von IT-Systemen in herausgehobenen Fällen durch Mobile Incident Response Teams (**MIRT**)
  - Änderung § 8c BSIG: Bestimmung neuer **IT-Security-Anforderungen** für die **Anbieter von digitalen Diensten** (Online-Marktplatz, Online-Suchmaschine, Cloud-Computing-Dienst)

Nat. Umsetzungsgesetz – wesentliche Eckpunkte II:

- Bisherige gesetzgeberische Vorarbeit im Bereich der IT-Security in Deutschland zahlt sich aus:
  - IT-SiG hat in erheblichen Teilen **Einfluss auf die Konzeptionierung der EU NIS-RL** genommen
  - **Deutschland zurzeit europäischer Vorreiter** in Sachen gesetzlicher IT-Security-Regulierung
  - Für betroffene Betreiber ebenfalls **kein „doppelter Implementierungsaufwand“** in technischer Hinsicht zu erwarten
- Nicht unerheblicher Umsetzungsaufwand aber für die beteiligten Behörden:
  - **Faktisch ungleiches IT-Sicherheitsniveau in Europa** ist auszugleichen
  - Aufbau und Verstetigung des **transnationalen Informationsaustauschs** im Bereich der IT-Sicherheit
  - (Politische) Stärkung des notwendigen **Vertrauens in die zwischenstaatliche Zusammenarbeit**
  - → Abstimmungsbedarf zwischen Gesetzgebung und Verwaltung, Wissenschaft und Anwendungspraxis
- **Fünf Jahre nach Inkrafttreten: Evaluierung** des Umsetzungsgesetzes gemäß dem Arbeitsprogramm der Bundesregierung zur besseren Rechtsetzung

- § 11 EnWG – Betrieb von Energieversorgungsnetzen:

  (1) Betreiber von Energieversorgungsnetzen sind verpflichtet, ein **sicheres, zuverlässiges und leistungsfähiges Energieversorgungsnetz** diskriminierungsfrei zu betreiben, zu warten und bedarfsgerecht zu optimieren, zu verstärken und auszubauen, soweit es wirtschaftlich zumutbar ist. […]

  (1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen **angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme**, die für einen sicheren Netzbetrieb notwendig sind. […]

  (1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 8 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben innerhalb einer von der Regulierungsbehörde festzulegenden Frist **einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind**. […]

- § 25a KWG – Besondere organisatorische Pflichten:

  (1) Ein Institut muss über eine **ordnungsgemäße Geschäftsorganisation** verfügen, die die Einhaltung der vom Institut zu beachtenden **gesetzlichen Bestimmungen** und der betriebswirtschaftlichen Notwendigkeiten gewährleistet. […] Eine ordnungsgemäße Geschäftsorganisation muss insbesondere ein angemessenes und wirksames **Risikomanagement** umfassen, auf dessen Basis ein Institut die Risikotragfähigkeit laufend sicherzustellen hat; das Risikomanagement umfasst insbesondere […] 5.die Festlegung eines **angemessenen Notfallkonzepts, insbesondere für IT-Systeme**

Corporate Governance & (IT-Security) Compliance

- §§ 109, 109a TKG – Technische Schutzmaßnahmen und Daten- und Informationssicherheit:

  (1) Jeder Diensteanbieter hat **erforderliche technische Vorkehrungen** und sonstige Maßnahmen zu treffen

  1. zum Schutz des Fernmeldegeheimnisses und
  2. gegen die Verletzung des Schutzes personenbezogener Daten.

  Dabei ist der **Stand der Technik** zu berücksichtigen.

  (2) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen **angemessene technische Vorkehrungen und sonstige Maßnahmen** zu treffen

  1. zum **Schutz gegen Störungen**, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch soweit sie durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und
  2. zur **Beherrschung der Risiken für die Sicherheit** von Telekommunikationsnetzen und -diensten.

  Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme **gegen unerlaubte Zugriffe zu sichern** und Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten. Bei Maßnahmen nach Satz 2 ist der **Stand der Technik** zu berücksichtigen.

- § 13 TMG – Pflichten des Diensteanbieters:

  (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**.

- § 8a BSIG – Sicherheit in der Informationstechnik Kritischer Infrastrukturen:

  (1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 **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.

- § 9 BDSG – Technische und organisatorische Maßnahmen:

  Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben **die technischen und organisatorischen Maßnahmen zu treffen**, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz **genannten Anforderungen**, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

- § 43 GmbHG – Haftung der Geschäftsführer:

  (1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft **die Sorgfalt eines ordentlichen Geschäftsmannes** anzuwenden.

  (2) Geschäftsführer, welche ihre **Obliegenheiten verletzen, haften** der Gesellschaft solidarisch für den entstandenen Schaden.

- §§ 91 Abs. 2, 93 Abs. 1 AktG – Organisation, Sorgfaltspflicht und Verantwortlichkeit der Vorstandsmitglieder:
  - Der Vorstand hat geeignete Maßnahmen zu treffen, damit „**den Fortbestand der Gesellschaft gefährdende Entwicklungen**“ frühzeitig erkannt werden
  - Die Vorstandsmitglieder haben bei ihrer Geschäftsführung „**die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters**“ anzuwenden

- IT-(Security)Compliance als interdisziplinäres Themenfeld:
  - **IT-Security-Bezug** bei gesetzlichen Vorschriften **nicht immer klar erkennbar** bzw. Erwartungshorizont **nicht hinreichend konkretisiert**
  - Allgemeine gesellschaftsrechtliche Beobachtungs- und Sorgfaltspflichten beziehen sich aber auch auf die Gewährleistung der IT-Security
  - Zugang über sog. "**unbestimmte Rechtsbegriffe**" oder "**Generalklauseln**"
  - Zweck: Implementierung außerhalb des Rechts stehender Sachverhalte in Gesetze → das Recht als "Einfallstor" für technische Vorgaben → **Flexibilität, Anpassungsfähigkeit und Technikoffenheit**
  - Jedoch: **Teils erhebliche Schwierigkeiten in der Anwendungspraxis, vor allem für KMUs**
    - Bei Bezugnahme auf außerhalb des Rechts liegende Sachverhalte
    - Bei noch nicht abschließender Konkretisierung unbestimmter Rechtsbegriffe, z.B. für neue Gesetze, vgl. "Stand der Technik" gem. IT-SiG (2015)
  - **Ausfüllung der unbestimmten Rechtsbegriffe kann v.a. durch technische Normen & Standards erfolgen**

Unbestimmte Rechtsbegriffe
&
Technische Normen und Standards

- Rechtswirkungen von Normen und Standards:
  - Grundsätzlich: **Keine**!
  - Warum? → Siehe Finanzierung: Technische Normen werden von einer Vereinigung privaten Rechts, **nicht aber in einem verfassungsrechtlich geregelten Gesetzgebungsverfahren** durch das staatliche Parlament geschaffen
  - **Ausnahmen**, die zum Bestehen einer Bindungswirkung führen können:
    - Aufnahme in privatrechtliche **Verträge**
    - Benennung in **gesetzlichen Vorschriften**

- Wie können Normen & Standards gesetzestechnisch einbezogen werden?
  - **Verweisung**
  - **Inkorporation**

- Die normkonkretisierende gleitende Verweisung:
  - Führt zur gesetzlichen Verwendung **unbestimmter Rechtsbegriffe**
  - **Drei wesentliche Kategorien** von unbestimmten Rechtsbegriffen in der gesetzgeberischen Verwendung:
    - Allgemein anerkannte Regeln der Technik
    - Stand der Technik
    - Stand von Wissenschaft und Technik
  - Konkretisiert durch **BMJV: Handbuch der Rechtsförmlichkeit**

- **Allgemein anerkannte Regeln der Technik**:
  - Schriftlich fixierte oder mündlich überlieferte technische **Festlegungen**
  - Für Verfahren, Einrichtungen und Betriebsweisen, die nach **herrschender Auffassung von Fachleuten**, Anwendern, Verbrauchern und der öffentlichen Hand die **Eignung besitzen**,
  - das **gesetzlich vorgegebene Ziel** zu erreichen und
  - die sich in der Praxis **allgemein bewährt** haben bzw. deren Bewährung in naher Zeit bevorsteht

- **Stand der Technik**:
  - Entwicklungsstand **fortschrittlicher Verfahren**, Einrichtungen und Betriebsweisen,
  - der nach **herrschender Auffassung** führender Fachleute das Erreichen des gesetzlich vorgegebenen **Ziels gesichert** erscheinen lässt, wenn sich
  - die entsprechenden Verfahren bereits in der Praxis **bewährt haben** oder zumindest aber im Betrieb mit Erfolg **erprobt wurden**

- **Stand von Wissenschaft und Technik**:
  - Entwicklungsstand **fortschrittlichster Verfahren**
  - Nach Auffassung **führender Fachleute** aus Wissenschaft und Technik
  - Auf der Grundlage **neuester wissenschaftlich vertretbarer Erkenntnisse** im Hinblick auf das gesetzgeberische Ziel für erforderlich gehalten
  - **Zielerreichung** erscheint gesichert

Unbestimmte Rechtsbegriffe und deren Konkretisierung

- Drei-Stufen-Theorie (BVerfG, Beschluss vom 08.08.1978, 2 BvL 8/77):
  - Ermöglicht bessere **Abgrenzung** zwischen vorgenannten drei unbestimmten Rechtsbegriffen
  - Je weiter eine bestimmte technische Vorgehensweise oder Methode in der Praxis etabliert und allgemein anerkannt ist, umso eher wird von einer **allgemein anerkannten Regel der Technik** auszugehen sein
    - Folglich immer dann einschlägig, wenn eine Maßnahme der **Mehrheitsauffassung** aller Praktiker entspricht
  - Gegensatz dazu: **Stand von Wissenschaft und Technik**
    - Vornehmlich solche Methoden, die nur dem aktuellsten technischen Erkenntnisstand entsprechen und sich folglich in der Praxis **noch nicht durchgesetzt** haben.
  - **Stand der Technik** als Mittelmaß
    - Solche Vorkehrungen, die zwar noch **nicht unbedingt bei jedem Fachmann** oder Anwender angelangt sein müssen, aber zugleich auch nicht so neu sind, dass sie die Grenze des wissenschaftlich bzw. technisch Realisierbaren bedeuten

- Beispiel: Konkretisierung des **Standes der Technik** durch das ISMS:
  - Information Security Management System (**ISMS**) nach ISO/IEC 27001 setzt voraus, dass laufend neue Bedrohungslagen erfasst und wirksame und aktuelle Gegenmaßnahmen implementiert werden (vgl. BT-Drs. 18/4096, S. 27)
  - Dies umfasst auch technisch neue Situationen, die teils im Anwenderkreis angelangt sind (**Stand der Technik**)
  - Durch **laufende und aktuelle Anpassung (PDCA + BCM)** technischer Systeme wird dafür Sorge getragen, dass deren Stand nicht auf das Niveau der „allgemein anerkannten Regel der Technik“ zurückfällt
  - **Somit wichtig**: Zuordnung einer getroffenen TOV/TOM zu einer Stufe kann sich im Laufe der Zeit ändern, sodass diese ggf. nicht mehr dem gesetzlich geforderten Stand entspricht!
  - Besonders wichtig für Normen & Standards: Da diese nur den technischen Stand zu einem bestimmten Zeitpunkt abbilden, ist deren **regelmäßige Überprüfung + Dokumentation notwendig**

Technik und Recht – Konflikt oder Kooperation?

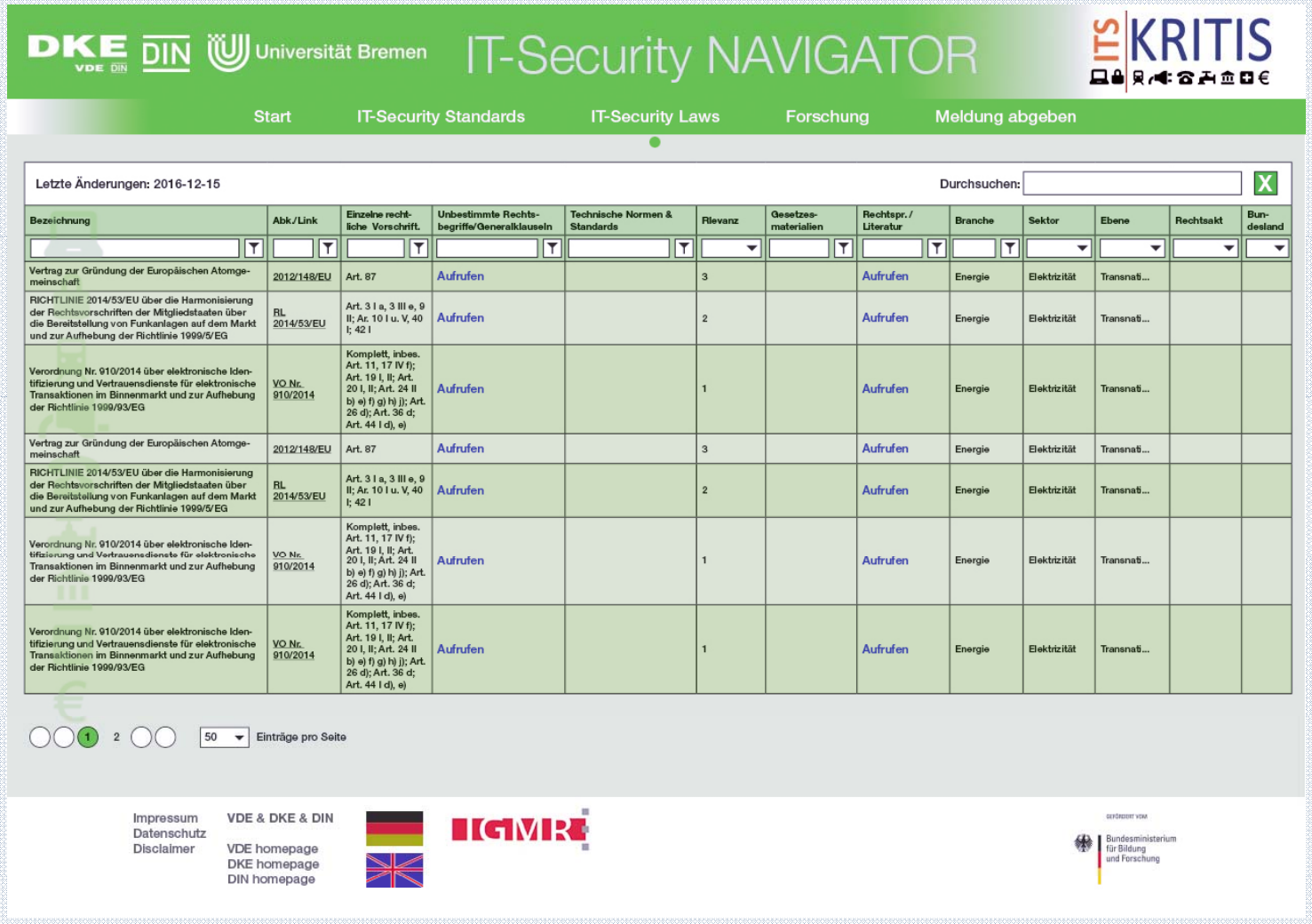
- Deutschland und die EU stellen insb. **seit 2015 einen umfassenden Regulierungsrahmen für Cybersicherheit** auf, basierend auf den jeweiligen politischen Strategien
- **Transnationale Cybersecurity-Kooperation** steht im Vordergrund, genauso der Ausbau von **Präventions- wie Reaktionsmöglichkeiten**
- Cybersecurity stellt den Gesetzgeber aufgrund der **interdisziplinär veranlagten** Regelungsmaterie zugleich vor **Herausforderungen**
- Rechtliche **Regulierungsgrenzen** zeigen sich anhand **laufend aktualisierter technischer Sachverhalte**
- Pragmatischer Lösungsansatz: Konkretisierung und flexible Anpassung des Rechts durch **unbestimmte Rechtsbegriffe bzw. durch Generalklauseln**
- Problem aber: **Flexibilität führt zu Unbestimmtheit**, genutzte Regulierungsmöglichkeit damit gleichsam Grenze zur Praxistauglichkeit
- Vor allem **problematisch für KMUs** ohne eigenen juristischen/technischen Sachverstand
- Tatsächlich aber **(noch zu lösender) Zielkonflikt** oder bloße Folge eines für sich genommen denknotwendigen wie **alternativlosen Regelungskonzepts**?

IT-Security NAVIGATOR

Ab Juni 2017

Quelle: D. Kipker/A. Harner/S. Müller VDE/DKE/IGMR 2017

IT-Security NAVIGATOR



DKE VDE DIN DIN Universität Bremen IT-Security NAVIGATOR ITS KRITIS

Start | IT-Security Standards | IT-Security Laws | Forschung | Meldung abgeben

Letzte Änderungen: 2016-12-15 Durchsuchen:

Bezeichnung	Abk./Link	Einzelne rechtliche Vorschrift.	Unbestimmte Rechtsbegriffe/Generalklauseln	Technische Normen & Standards	Rlevanz	Gesetzesmaterialien	Rechtspr./Literatur	Branche	Sektor	Ebene	Rechtsakt	Bundesland
Vertrag zur Gründung der Europäischen Atomgemeinschaft	2012/148/EU	Art. 87	Aufrufen		3		Aufrufen	Energie	Elektrizität	Transnati...		
RICHTLINIE 2014/53/EU über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG	RL 2014/53/EU	Art. 3 I a, 3 III e, 9 II; Ar. 10 I u. V, 40 I; 42 I	Aufrufen		2		Aufrufen	Energie	Elektrizität	Transnati...		
Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG	VO Nr. 910/2014	Komplett, inbes. Art. 11, 17 IV f); Art. 19 I, II; Art. 20 I, II; Art. 24 II b) e) f) g) h) j); Art. 26 d); Art. 36 d; Art. 44 I d), e)	Aufrufen		1		Aufrufen	Energie	Elektrizität	Transnati...		
Vertrag zur Gründung der Europäischen Atomgemeinschaft	2012/148/EU	Art. 87	Aufrufen		3		Aufrufen	Energie	Elektrizität	Transnati...		
RICHTLINIE 2014/53/EU über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG	RL 2014/53/EU	Art. 3 I a, 3 III e, 9 II; Ar. 10 I u. V, 40 I; 42 I	Aufrufen		2		Aufrufen	Energie	Elektrizität	Transnati...		
Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG	VO Nr. 910/2014	Komplett, inbes. Art. 11, 17 IV f); Art. 19 I, II; Art. 20 I, II; Art. 24 II b) e) f) g) h) j); Art. 26 d); Art. 36 d; Art. 44 I d), e)	Aufrufen		1		Aufrufen	Energie	Elektrizität	Transnati...		
Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG	VO Nr. 910/2014	Komplett, inbes. Art. 11, 17 IV f); Art. 19 I, II; Art. 20 I, II; Art. 24 II b) e) f) g) h) j); Art. 26 d); Art. 36 d; Art. 44 I d), e)	Aufrufen		1		Aufrufen	Energie	Elektrizität	Transnati...		

1 2 50 Einträge pro Seite

Impressum Datenschutz Disclaimer VDE & DKE & DIN VDE homepage DKE homepage DIN homepage IGMR Bundesministerium für Bildung und Forschung

Quelle: D. Kipker/A. Harner/S. Müller VDE/DKE/IGMR 2017

Dr. Dennis-Kenji Kipker
Wissenschaftlicher Geschäftsführer
Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)
Universität Bremen
Universitätsallee GW1
28359 Bremen
Tel.: 0421 218 66049
Mail: kipker@uni-bremen.de

Besuchen Sie unsere Website: www.itskritis.de
Folgen Sie uns auf Twitter: @itskritis

der Bundeswehr Universität München
FAU Friedrich-Alexander Universität Erlangen-Nürnberg
DKE VDE DIN
Universität Bremen