Europäische Akademie für Informationsfreiheit und Datenschutz
Académie européenne pour la liberté d'information et la protection des données
European Academy for Freedom of Information and Data Protection
EAID

Cybersecurity: Möglichkeiten und Grenzen praxisgemäßer rechtlicher Regulierung

Dr. Dennis-Kenji Kipker

Freitag, 17. Februar 2017
6. DialogCamp, München

Europäische Akademie für Informationsfreiheit und Datenschutz
Académie européenne pour la liberté d'information et la protection des données
European Academy for Freedom of Information and Data Protection

EAID

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 die 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**

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

- Gesetzliche 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**
  - **EU NIS-RL (2016) + nationales Umsetzungsgesetz (2017)**

- § 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**

- §§ 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 **unbestimmte Rechtsbegriffe** oder **Generalklauseln**
  - Zweck: Implementierung außerhalb des Rechts stehender Sachverhalte in Gesetze → 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? 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

- 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 bzw. BSI-Grundschutz 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 Anpassungen (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**

- Fazit – Cybersecurity: Möglichkeiten und Grenzen praxisgemäßer rechtlicher Regulierung:
  - Cybersecurity stellt Gesetzgeber aufgrund der **interdisziplinär veranlagten** Regelungsmaterie 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**?

Europäische Akademie für Informationsfreiheit und Datenschutz
Académie européenne pour la liberté d'information et la protection des données
European Academy for Freedom of Information and Data Protection

EAID

Mehr zum technischen Datenschutz…

Workshop der EAID:
„Technologischer Datenschutz – Vorgaben der Datenschutzgrundverordnung“

2. März 2017, Europäische Akademie Berlin

13:00 - 18:00

Referenten u.a. Marit Hansen (ULD SH), Prof. Dr. Hannes Federrath (Univ. Hamburg), Prof. Dr. Kai Rannenberg (Goethe-Univ. F.a.M), Gabriel Schulz (stellv. LfDI Mecklenburg-Vorpommern), Roland Schwaiger (Deutsche Telekom)

Europäische Akademie für Informationsfreiheit und Datenschutz
Académie européenne pour la liberté d'information et la protection des données
European Academy for Freedom of Information and Data Protection

EAID

Dr. Dennis-Kenji Kipker
Europäische Akademie für
Informationsfreiheit und Datenschutz (EAID)
Bismarckallee 46/48
D-14193 Berlin-Grunewald
Mail: kipker@eaid-berlin.de