TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT "IT-Sicherheitsrechtstag 2022"

Berlin, 21.09.2022

Gesetzesvielfalt: Wie wappnet sich der Gesetzgeber gegen Cyber-Kriminelle?

Rechtsanwalt und Fachanwalt für IT-Recht

Fritz-Ulli Pieper, LL.M., Taylor Wessing

Inhalt

1 Aktuelle Gefährdungslage

Aktuelle Gefährdungslage

- In seinem Bericht für 2021 bezeichnet das BSI die IT-Sicherheitslage in Deutschland als „angespannt bis kritisch“
- Beispiel: „Sicherheitstacho“ der DTAG
  - Anzeige der weltweiten Cyberangriffe auf die „Honeypot“-Infrastruktur der DTAG sowie ihrer Partner
  - Zirka 30.000 Angriffe pro Minute

Quelle: https://www.sicherheitstacho.eu/start/main

2 Europäische Regulierung

Europäische Regulierung

Richtlinie (EU) 2016/1148 (NIS-RL)

Ziel: Stärkung der Cybersicherheit auf europäischer Ebene

Maßstäbe für Sicherheitsmaßnahmen und Meldepflichten

Adressaten: Betreiber wesentlicher Dienste und Anbieter digitaler Dienste

Bevorstehende Reform durch NIS 2.0

Umfangreichere Maßnahmen, Vorgaben zum Meldeinhalt

Erweiterung des Adressatenkreises

Einrichtung eines Europäischen Netzwerks für massive Cybersicherheitsvorfälle bestehend aus den zuständigen nationalen Behörden (EU-CyCLONe)

Während unter der NIS 1 Richtlinie die Mitgliedsstaaten die Kriterien zur Bestimmung der Anbieter wesentlicher Dienste vorgeben, stellt NIS 2.0 zukünftig eigenständig Schwellenwerte auf

Cyber Resilience Act

Verordnung über Cybersicherheitsanforderungen für Produkte mit digitalen Elementen

Vorschriften für das Inverkehrbringen von Produkten mit digitalen Elementen zur Gewährleistung der Cybersicherheit solcher Produkte

Grundlegende Anforderungen an die Gestaltung, Entwicklung und Herstellung von Produkten mit digitalen Elementen

Grundlegende Anforderungen an die Verfahren zur Behandlung von Schwachstellen für Hersteller, während des gesamten Lebenszyklus

Europäische Regulierung

Verordnung 2016/679 (Datenschutz-Grundverordnung, DSGVO)

- DSGVO enthält verschiedene Regelungen, die sich nicht nur mit dem Datenschutz, sondern auch mit der Datensicherheit beschäftigen, u.a.:
  - Art. 5 Abs. 1 lit. f DSGVO: Grundsatz der Integrität und Vertraulichkeit
  - Art. 32 DSGVO: Technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos
  - Art. 33 DSGVO: Meldepflicht bei Verletzung des Schutzes personenbezogener Daten

Europäische Regulierung

Verordnung (EU) 2019/881 (Rechtsakt zur Cybersicherheit)

- Stärkung der europäischen Cyber-Sicherheitsagentur ENISA, permanentes Mandat
- Einführung eines einheitlichen Zertifizierungsrahmens für IKT-Produkte, -Dienstleistungen und -Prozesse
  - Insbesondere Festlegung europäischer Schemata für die Cybersicherheitszertifizierung
  - Bei Zertifizierung wird zwischen verschiedenen Sicherheitslevel unterschieden

Zusätzlich: ePrivacy-Richtlinie, Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberattacken und Richtlinie (EU) 2013/40 über Angriffe auf Informationssysteme, eIDAS-Verordnung

3 Nationale Vorgaben

Nationale Vorgaben

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Bereichsspezische Regelungen - IT-Sicherheitsgesetz

- **IT-SiG 1.0 vom 12.06.2015:** Erster übergreifender Rechtsrahmen für die Gewährleistung von Cybersicherheit in Deutschland.
- **IT-SiG 2.0:** Trat am 28.05.2021 nach Verkündung in Kraft. Der Gesetzgebungsprozess hat sich über mehrere Jahre erstreckt.

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

- Ziele: Ganzheitliche Ausweitung der IT-Sicherheit für Gesellschaft, Wirtschaft und Staat.
  - Vermeidung von Ausfällen und Beeinträchtigungen im Bereich der Kritischen Infrastrukturen
  - Verbesserung der IT-Sicherheit bei Unternehmen und in der Bundesverwaltung
  - Besserer Schutz der Bürgerinnen und Bürger im Netz
- Adressaten: Betreiber kritischer Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse, KRITIS-Hersteller, Anbieter digitaler Dienste

Die IT-SiG 1.0 und 2.0 (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) sind sog. Artikel-gesetze, d.h. Änderung mehrerer Gesetze, neben BSIG u.a.:

- Telekommunikations-gesetz
- Energiewirtschaftsgesetz
- Atomgesetz
- Sozialgesetzbuch

Nationale Vorgaben

Bereichspezifische Regelungen

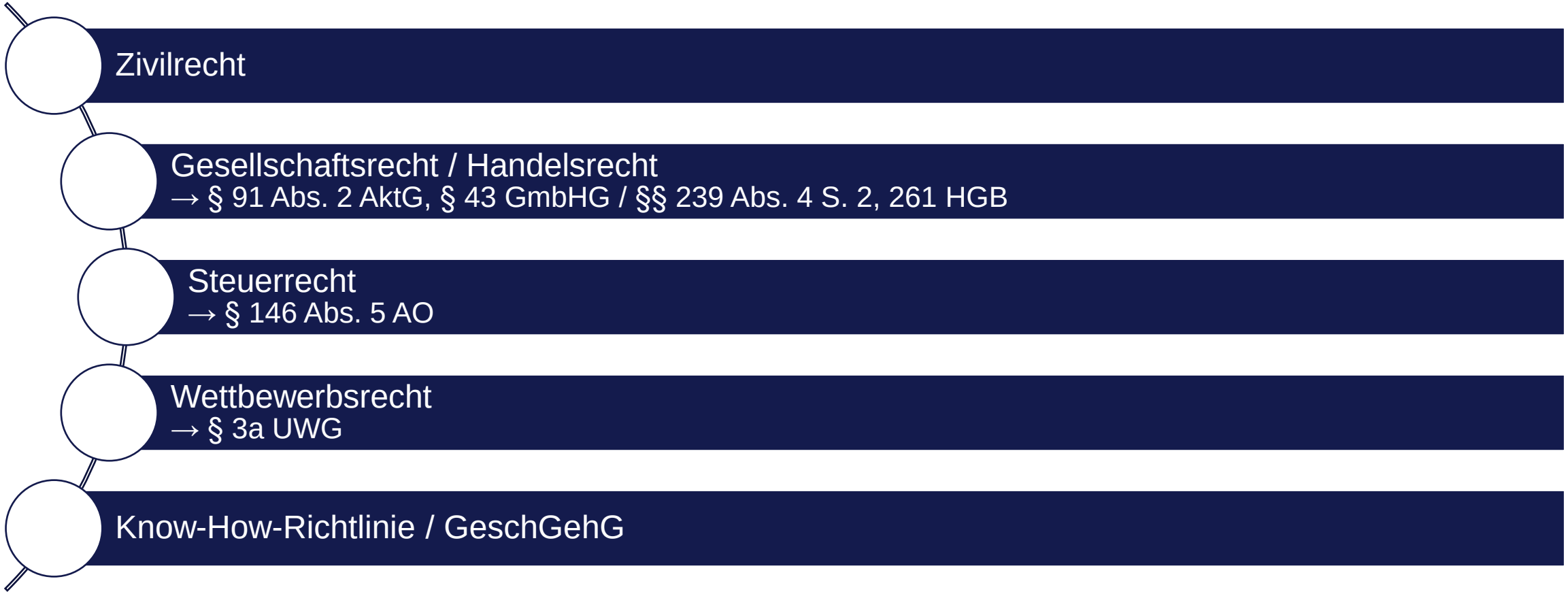
Neben den Artikelgesetzen finden sich bereichspezifische Regelungen in vielen verschiedenen Gesetzen wieder, u.a.:

§ 75c SGB V	§§ 165 – 169 TKG	§ 19 Abs. 4 TTDSG	§§ 475b, 475c BGB „Aktualisierungspflicht“	§ 25a Abs. 1 S. 3 Nr. 5 KWG
▪ Ab 1. Januar 2022: Krankenhäuser sind unabhängig eines Schwellenwerts verpflichtet angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen zu treffen.	▪ § 165 TKG: Den Betreibern öffentlicher TK Netze und den Erbringern öffentlich zugänglicher TK Diensten obliegen technische und organisatorische Schutzmaßnahmen. ▪ § 168 TKG: Mitteilungspflicht bei Sicherheitsvorfällen mit beträchtlichen Auswirkungen auf den Netzbetrieb und die Erbringung der Dienste.	▪ Anbieter von Telemedien müssen durch technische und organisatorische Vorkehrungen sicherstellen, dass 1. kein unerlaubter Zugriff auf die für das Telemedienangebot genutzten Einrichtungen möglich ist und 2. diese gegen Störungen gesichert sind.	▪ Umsetzung der Warenkaufrichtlinie und Digitale-Inhalte-Richtlinie. ▪ Im Rahmen von bestimmten Verbraucherverträgen obliegen dem Unternehmer Aktualisierungspflichten, welche wohl auch IT-Sicherheitsupdates einschließen.	▪ Allgemeine Pflicht zur Herstellung und Aufrechterhaltung einer angemessenen IT-Sicherheitsstruktur im Banken- und Finanzsektor. ▪ Konkretisiert von der BaFin in den Mindestanforderungen an das Risikomanagement (MaRisk) von Oktober 2017.

Nationale Vorgaben

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Allgemeine rechtliche Rahmenbedingungen



4 Diskussion und Ausblick

Diskussion und Ausblick

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Vergleich mit anderen Rechtsgebieten des Compliance Bereichs

Kartellrecht

- Art. 101 und 102 AEUV und Fusionskontrollverordnung
  - Anwendungsvorrang
- GWB als einheitliche nationale Rechtsgrundlage
  - Sonderregelungen für einige Branchen

➡ Einheitliche Vorgaben

(Wirtschafts-)Strafrecht

- „Repressive Facette“ von Compliance
- Straftatbestände befinden sich neben dem StGB **verstreut** in vielen verschiedenen Gesetzestexten z.B.:
  - GmbHG, AktG, UrhG, MarkenG, PatG, AO

➡ Ähnliche Diversifizierung wie im IT-Sicherheitsrecht, aber immer „Branchenbezug“ und Bezug zum Allgemeinen Teil des Strafrechts!

Datenschutz

- Hauptsächlich: DSGVO
  - Anwendungsvorrang
- BDSG und Landesdatenschutzgesetze als einheitliche nationale Rechtsgrundlagen
- Bereichsspezifische nationale Vorschriften

➡ Einheitliche (supranationale) Vorgaben

Diskussion und Ausblick

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Status Quo IT-Sicherheitsrecht

Mangelnde Systematisierung im Compliance Bereich eher untypisch

- Grundlegende Rechtsvorschriften im Sinne eines Allgemeinen Teils weder auf europäischer, noch auf nationaler Ebene
- Vielzahl an branchenspezifischen Vorgaben
  - Im Herbst 2017 gab es 63 Gesetze und Verordnungen des Bundes und weitere Rechtsvorschriften der Länder, die dem BSI eine mitwirkende, beratende oder sonstige Rolle zuweisen
  - Vergleich mit Kartellrecht zeigt, dass auch in einem einheitlichen Gesetz branchenspezifische Regelungen möglich sind

Vorteile

- Individualisierung der Anforderungen an IT-Sicherheit abhängig von Branche, Größe der Normadressaten

Nachteile

- IT-Sicherheitsrecht ist unübersichtlich und komplex
  - Erfordert hohe Sensibilität des Anwenders
- Vielzahl an unterschiedlichen Begrifflichkeiten erschweren Anwendung
- Unterschiedliche Schutzgüter bewirken divergierende Verfahrensweisen zur Risikoabschätzung
- Nationaler Alleingang kann zu einer wirtschaftlichen Belastung betroffener Unternehmen führen

Diskussion und Ausblick

1

Wird die IT-Sicherheit insgesamt vom Gesetzgeber zu nachlässig reglementiert?

2

Benötigen wir auf europäischer Ebene eine stärkere Regulierung durch Verordnungen anstatt durch Richtlinien? Oder koordinierteres Vorgehen?

3

Sollte es (national) eine stärkere Systematisierung in Form eines Allgemeinen Teils zum IT-Sicherheitsrecht geben?

Vielen Dank für Ihre Aufmerksamkeit!

Ihr Ansprechpartner

Fritz-Ulli Pieper, LL.M., berät als Fachanwalt für IT-Recht nationale und internationale Mandanten im IT-, Telekommunikations- und Datenschutzrecht. Er verfügt über besondere Erfahrung zu Rechtsfragen der Digitalisierung und Künstlicher Intelligenz.

Seine Aufgabenschwerpunkte umfassen die Gestaltung von IT-Verträgen sowie AGB und die Begleitung von komplexen Datenschutzprojekten sowie die Beratung von Telekommunikationsanbietern oder deren Vertragspartnern bei Infrastrukturprojekten und Produkteinführungen. Zudem berät er die öffentliche Hand bei großvolumigen IT- und Infrastrukturvorhaben, insbesondere das Bundesministerium des Innern, für Bau und Heimat sowie dessen nachgelagerten Bereiche.

Fritz-Ulli Pieper hält regelmäßig Vorträge und ist Autor zahlreicher Fachpublikationen sowie leitender Redakteur eines großen Internetportals zum „Recht der Informationsgesellschaft“.

Sprachen

- Deutsch, Englisch

Top Anwalt für IT-Recht, WirtschaftsWoche Ranking 2021 und 2022

Führender Anwalt im Datenschutzrecht, Deutsches Institut für Rechtsabteilungen und Unternehmensjuristen (diruj) – Kanzleimonitor 2019/2020, 2020/2021 und 2021/2022

Hervorgehoben als Kernanwalt für Datenschutz, Legal 500 Germany 2022

Hervorgehoben als Kernanwalt für Informationstechnologie & Digitalisierung, Legal 500 Germany 2021

Fritz-Ulli Pieper

Salary Partner
Düsseldorf

+49 211 8387-189
f.pieper@taylorwessing.com

Beratungsschwerpunkte

- Informationstechnologie/ Telekommunikation
- Litigation & Dispute Resolution