IT-Sicherheitsrecht

Nationale und internationale Rahmenbedingungen

Dr. Dennis-Kenji Kipker

Aktuelle nationale Gesetzesänderungen durch das IT-Sicherheitsgesetz (IT-SiG)

IT-Sicherheit – nationale Rechtsvorgaben

- IT-Sicherheit wird **nicht kodifiziert** geregelt
- Zahlreiche **Einzelvorschriften**
- Abhängig vom jeweiligen **Geschäfts- bzw. Infrastrukturbereich**
- Beispiele „von A bis Z“:
  - AktG, § 91
  - AtG, §§ 7 ff., 44b
  - BDSG, §§ 9, 9a, 42a
  - BSIG, §§ 3, 4, 7, 7a, 8a ff.
  - EnWG, §§ 11 ff., 21e, 49
  - KWG, § 25a
  - TKG, §§ 109, 109a
  - TMG, § 13
  - IT-SiG, §§ … ???

IT-Sicherheit – nationale Rechtsvorgaben

- Zur Rechtsnatur des IT-SiG:
  - Artikelgesetz
  - **Kein Kodifikationscharakter!**
  - Ändert nur verschiedene Einzelgesetze, u.a.:
    - Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)
    - Atomgesetz (AtG)
    - Energiewirtschaftsgesetz (EnWG)
    - Telemediengesetz (TMG)
    - Telekommunikationsgesetz (TKG)
    - Bundeskriminalamtgesetz (BKAG)
  - **Betrifft in erheblichem Maße auch, aber nicht nur kritische Infrastrukturen**
  - IT-SiG in Kraft getreten am 25.07.2015
  - Bestandteil von Cybersicherheitsstrategie der BReg
  - Problem: Verteilung der IT-Sicherheitsvorschriften über zahlreiche Einzelgesetze führt zu Unübersichtlichkeit für den Anwender

IT-Sicherheit – nationale Rechtsvorgaben

- § 7 BSIG – Warnungen:
  - **Nicht neu:** Warnung durch das BSI vor Sicherheitslücken in Produkten oder Diensten und vor Schadprogrammen sowie Empfehlung zum Einsatz bestimmter Sicherheitsprodukte
  - **Erweiterung:** Warnung bei Datenverlust oder bei unerlaubtem Zugriff

  - **Auch neu + zugleich Problem:** Einbeziehung Dritter, „wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist“
  - Entwurfsbegründung: „Informationsintermediäre“
  - **Keine nähere Definition der Ausgestaltung einer Einbeziehung Dritter**
  - Speziell bei Verarbeitung personenbezogener Daten besteht erhöhtes Risiko für Persönlichkeit des Einzelnen
  - **Umgang mit Herstellergeheimnissen? Welche Aufgabe haben die Dritten?**
  - Daher flankierende Verfahrensregelungen oder aber Verweis auf BDSG nötig

IT-Sicherheit – nationale Rechtsvorgaben

- § 7a BSIG – Untersuchung der Sicherheit in der Informationstechnik:
  - **Neue Vorschrift** schafft Befugnis des BSI, Produkte und Systeme zu untersuchen, die auf dem Markt bereit gestellt werden/werden sollen
    - „Untersuchung“ umfasst u.a. auch Reverse Engineering (siehe BT-Drs. 18/4096, S. 25)
  - Bei Erforderlichkeit dürfen **Erkenntnisse weitergegeben und veröffentlicht werden**
  - Zuvor aber angemessene Frist für den Hersteller zu eigener Stellungnahme
  - **Problem:** Keine genauen gesetzlichen Anforderungen an Untersuchungsprozess
  - Auch hier dürfen wieder **Dritte einbezogen werden**, unklar aber ebenso wieder:
    - Mit welchen Aufgaben dürfen diese vom BSI betraut werden?
    - Sicherheitslücken sollten eigentlich möglichst vertraulich behandelt werden!
      - Beschränkungsregelung wie in § 7 BSIG fehlt
    - Rechtsverhältnis zu Dritten muss in jedem Falle weiter konkretisiert werden, z.B. durch Auftragsdatenverarbeitung, vgl. § 11 BDSG
      - Schutzwürdige Herstellerinteressen sind zu berücksichtigen
      - Beauftragte Dritte müssen zu Vertraulichkeit verpflichtet werden
      - Keine Beauftragung von direkten Konkurrenten als Dritten möglich

IT-SiG und Kritische Infrastrukturen

§§ 8a bis 8d BSIG als zentrale Neuerungen

IT-Sicherheit – nationale Rechtsvorgaben

- **Legaldefinition von Kritischen Infrastrukturen** in § 2 Abs. 10 BSIG, kumulative Kriterien:
  - 1. **Sektorale Zugehörigkeit** zu Energie, Informationstechnik, TK, Transport, Verkehr, Gesundheit, Wasser, Ernährung, Finanz- + Versicherungswesen
  - 2. Sog. **Fehlerfolgenerheblichkeit**: Hohe Bedeutung für das Funktionieren des Gemeinwesens, weil durch Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öff. Sicherheit einträten

IT-Sicherheit – nationale Rechtsvorgaben

- Konkretisierung der Kritischen Infrastrukturen erfolgt gem. § 10 BSIG durch RVO des BMI (sog. KritisVO)
  - Bestimmung, welche Einrichtungen, Anlagen oder Teile davon als KRITIS gelten
  - **Kriterium: Bedeutung als kritisch anzusehende Dienstleistung (Qualität) + Versorgungsgrad (Quantität)**
  - Anhörung von Wissenschaft, Betreibern und Wirtschaftsverbänden inkl. Einvernehmen verschiedener BM
  - § 10 Abs. 1 S. 2 BSIG: „Der […] als bedeutend anzusehende Versorgungsgrad ist anhand von **branchenspezifischen Schwellenwerten** für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen.“

IT-Sicherheit – nationale Rechtsvorgaben

- Zeitplanung KritisVO
  - Korb 1:
    - Energie, IKT, Ernährung, Wasser
    - Fertigstellung für Ende 2015 geplant
    - Inkrafttreten wohl im 1. Quartal 2016
  - Korb 2:
    - Finanzen, Gesundheit, Transport, Verkehr
    - Fertigstellung für Ende 2016 geplant
    - Inkrafttreten geschätzt 1. Quartal 2017

IT-Sicherheit – nationale Rechtsvorgaben

- § 8a BSIG – Sicherheit in der Informationstechnik Kritischer Infrastrukturen:
  - Regelt **„angemessene“ TOV**, die grds. spätestens zwei Jahre nach Inkrafttreten der RVO gem. § 10 BSIG von den Betreibern zu treffen sind
  - Maßnahmen müssen der Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit derjenigen **IT-Systeme** dienen, die **für die Funktionsfähigkeit von kritischen Infrastrukturen maßgeblich** sind
  - Maßnahmen **sollen den Stand der Technik einhalten**
    - Internationale, europäische + nationale Normen und Standards (z.B. ISMS, ISO/IEC 27001)
    - Betreiber und Branchenverbände können in Abstimmung mit BSI spezifische Standards zur Gewährleistung der IT-Sicherheitsanforderungen vorschlagen

      → UP KRITIS
  - **TOV sind angemessen, „wenn** der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht“ → Konkretisierungsbedürftig, in erster Linie Kostenrelevanz Kriterium!
  - TOV sind alle 2 Jahre nachzuweisen durch **Audits, Prüfungen, Zertifizierungen**

  Zu konkretisieren: Wer soll diese Nachweise durchführen? → Siehe auch: § 8a Abs. 4 BSIG

IT-Sicherheit – nationale Rechtsvorgaben

- § 8b BSIG – Zentrale Stelle für IT-Sicherheit der Kritischen Infrastruktur:
  - **BSI als zentrale Meldestelle für kritische Infrastrukturen** in Angelegenheiten der Sicherheit in der Informationstechnik
  - Verschiedene entsprechende Aufgaben:
    - Informationssammlung und -auswertung: Sicherheitslücken, Schadprogramme, erfolgte oder versuchte Angriffe, Vorgehensweise von Angreifern
    - Auswirkungen von Angriffen auf die Verfügbarkeit von krit. Infrastrukturen analysieren
    - Aktualisierung Lagebild Informationssicherheit kritische Infrastrukturen
    - Unterrichtung der Betreiber über Gefahren
    - Unterrichtung weiterer zuständiger (Aufsichts)behörden
  - **Betreiberpflicht zur Einrichtung einer Kontaktstelle** zur Krisenprävention und -bewältigung grds. innerhalb von 6 Monaten nach RVO gem. § 10 BSIG
  - Zusätzlich zu eigener Kontaktstelle **Benennung einer gemeinsamen, übergeordneten Anspruchstelle möglich**, soweit Zugehörigkeit zu gleicher Domäne → Dann Austausch im Regelfall hierüber

IT-Sicherheit – nationale Rechtsvorgaben

- § 8b BSIG – Meldepflicht:
  - **Wann ist zu melden?** Erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit von KRITIS
    - 1. führen können oder
    - 2. geführt haben
  - **Was ist zu melden?** Angaben zur Störung, den technischen Rahmenbedingungen, der vermuteten oder tatsächlichen Ursache, der Art der betroffenen Einrichtung oder Anlage und zur Branche des Betreibers

IT-Sicherheit – nationale Rechtsvorgaben

- **Benennung des konkreten Betreibers?** Nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der krit. Infrastruktur geführt hat, andernfalls pseudonymisierte Meldung
- **Was passiert mit den gemeldeten Daten?** BSI ist zentrale Meldestelle, das bedeutet…
  - Sammlung und Auswertung (z.T. zusammen mit BBK)
  - Aktualisierung Lagebild Informationssicherheit
  - Information für Betreiber und (Aufsichts)behörden
- **Wer muss nicht melden?** § 8c BSIG – Anwendungsbereich: Keine Anwendung auf Kleinstunternehmen (Mitarbeiter < 10; Jahresbilanz nicht größer als 2 Mio. €)
- **Bereichsausnahmen bei Sonderregelungen**, dazu sogleich…

IT-Sicherheit – nationale Rechtsvorgaben

- **Sonderregelungen – Meldepflichten nach anderen Gesetzen, § 8c BSIG:**
  - Betreiber von TK-Netzen oder TK-Diensten
    → § 109 TKG
  - Betreiber von Energieversorgungsnetzen oder -anlagen
    → § 11 EnWG
  - Genehmigungsinhaber gem. Atomgesetz
    → § 44b ATG
  - Sonstige Betreiber von kritischen Infrastrukturen, die dem BSIG vergleichbare Anforderungen erfüllen müssen
    → Insb.: Telematikinfrastruktur im Gesundheitswesen (vgl. aktuell eHealth-Gesetzentwurf der BReg vom 22.06.2015)
  - Es gilt somit: **BSIG als allgemeine Vorgabe, falls keine Spezialgesetze für den jeweiligen Infrastrukturbereich greifen** → Dieses Prinzip ist im Recht universell gültig (lex specialis)
  - Bereichsausnahmen des § 8c BSIG gelten auch für § 8a BSIG

IT-Sicherheit – nationale Rechtsvorgaben

- **Exkurs zu den Sonderregelungen - § 11 EnWG:**
  - Gegenüber BSIG vorrangige Vorschrift für Betreiber von
    - 1. Energieversorgungsnetzen
    - 2. Energieanlagen
  - 1. Energieversorgungsnetzbetreiber:
    - Verpflichtung zum Betrieb eines sicheren, zuverlässigen und leistungsfähigen Netzes (Abs. 1)
    - Sicherer Netzbetrieb umfasst auch angemessenen Schutz gegen Bedrohungen für TK- + EDV-Systeme, die für Netzbetrieb notwendig sind (Abs. 1a, modifiziert durch IT-SiG)
      - Angemessener Schutz gegeben, soweit **Sicherheitskatalog der BNetzA** eingehalten und vom Betreiber dokumentiert
      - EnWG selbst enthält keine Umsetzungsfrist, aber der Sicherheitskatalog:
        - Abschluss Zertifizierung der Maßnahmen ist bis 31.01.2018 der BNetzA mitzuteilen
        - **Ansprechpartner zur IT-Sicherheit ist bis zum 30.11.2015 mitzuteilen an: IT-Sicherheitskatalog@bnetza.de**
    - Soweit Betreiber der RVO nach § 10 Abs. 1 BSIG unterfallen, besteht eine eigene Meldepflicht gem. EnWG, vergleichbar mit BSIG (Abs. 1c, neu durch IT-SiG)

IT-Sicherheit – nationale Rechtsvorgaben

- 2. Energieanlagenbetreiber:
  - Soweit Betreiber der RVO nach § 10 Abs. 1 BSIG unterfallen + an ein Energieversorgungsnetz angeschlossen sind, haben sie einen angemessenen Schutz gegen Bedrohungen für TK- und EDV-Systeme zu gewährleisten, die für sicheren Anlagenbetrieb notwendig sind
  - Umsetzungsfrist: 2 Jahre nach Inkrafttreten der RVO (Abs. 1b, neu durch IT-SiG)
  - Hierzu soll ebenso ein Katalog von Sicherheitsanforderungen durch BNetzA und BSI erstellt werden
  - Angemessener Schutz gegeben, soweit **Sicherheitskatalog der BNetzA gem. § 11 Abs. 1b EnWG** eingehalten und vom Betreiber dokumentiert
  - Soweit Betreiber der RVO nach § 10 Abs. 1 BSIG unterfallen, besteht eine eigene Meldepflicht gem. EnWG, vergleichbar mit BSIG (Abs. 1c, neu durch IT-SiG)

IT-Sicherheit – nationale Rechtsvorgaben

- IT-Sicherheitskatalog der BNetzA gem. § 11 Abs. 1a EnWG – wesentliche regulatorische Vorgaben:
  - **Erschienen:** August 2015
  - **Ziel:** Gewährleistung eines sicheren Netzbetriebs (IT-Schutzziele)
  - **Maßnahmen:**
    - Kernforderung ist Einrichtung eines ISMS nach DIN ISO/IEC 27001 + Zertifizierung der Maßnahmen durch unabhängige Drittstelle in Kooperation mit der DAkkS → Mindeststandard für IT-Sicherheit
    - Benennung Unternehmens-Ansprechpartner IT-Sicherheit an BNetzA
    - Sicherstellung der Teilnahme des Betreibers am UP KRITIS
    - Geltungsbereich umfasst alle Komponenten für sicheren Netzbetrieb
    - Einführung des PDCA-Modells: Plan-Do-Check-Act → Definition von IT-Sicherheit als fortlaufendem Prozess
    - Detaillierte Vorgaben zur Implementierung des ISMS für konkreten Betreibertypus inkl. Verweisen auf ISO/IEC 2700X

IT-Sicherheit – nationale Rechtsvorgaben

- Ausbau der Befugnisse des Bundeskriminalamts gem. § 4 BKAG:
  - Bisher: Ermittlungszuständigkeit nur bei Computersabotage (§ 303b StGB) insb. bei lebenswichtigen Einrichtungen
  - **Neu:** Ausdehnung auf alle Arten von Computerdelikten sowie bei Angriffen auf Behörden oder Einrichtungen des Bundes

- IT-SiG – auch Verpflichtungen für den Bund neu gefasst (siehe BT-Drs. 18/5121):
  - Angriff auf die IT des BT 5/2015 als Auslöser für Erweiterung
  - BSI erarbeitet verbindliche Mindeststandards für IT des Bundes
  - Mindeststandards können als VwV durch BMI erlassen werden
  - Pflicht der Bundesbehörden, BSI Zugang zu behördeninternen IT-Sicherheitsdaten zu gewähren

IT-SiG – wie geht es weiter?

- Wichtige Umsetzungsfristen:
  - § 8a BSIG: Regelt TOV, die spätestens zwei Jahre nach Inkrafttreten der RVO gem. § 10 BSIG von den Betreibern zu treffen sind
  - § 8b BSIG: Betreiberpflicht zur Einrichtung einer Kontaktstelle zur Krisenprävention und -bewältigung innerhalb von 6 Monaten nach RVO gem. § 10 BSIG
  - Keine Fristen für: TK-Betreiber (§ 109 TKG); Atomkraftwerksbetreiber (§ 44b AtG) → Sofortige Umsetzung von TOV bzw. Meldepflichten nach § 109 TKG/§ 44b AtG
  - Sonderrolle Energieversorger und -anlagenbetreiber, § 11 EnWG
- Bußgeldvorschriften:
  - § 14 BSIG (sanktioniert u.a. Missachtung der Meldepflicht, *Maximum* 100.000 €)
  - § 149 Nr. 21a. TKG (*Maximum* 50.000 €)
  - § 16 TMG (*Maximum* 50.000 €)
- Kosten für Betreiber:
  - Können im Einzelnen nicht im Vorfeld quantifiziert werden, insb. auch nicht für notwendige Zertifizierungen und Audits
  - RVO nach § 10 BSIG soll weitere Hinweise liefern
  - Zahl der meldepflichtigen KRITIS-Betreiber soll deutschlandweit bei ca. 2.000 liegen
  - Schätzung BReg: 7 Meldungen pro Betreiber pro Jahr
  - Geschätzte Kosten pro Meldung: 660 € (11 Stunden Zeitaufwand, Stundensatz von 60 €)
  - Nationaler Normenkontrollrat: „Bezifferbarer Mehraufwand für die Wirtschaft = 9 Mio. €“
- Art. 10 IT-SiG: Evaluierung der neuen Vorschriften zu KRITIS vier Jahre nach Inkrafttreten der RVO gem. § 10 BSIG

Insb.: Richtlinie der EU über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS-RL)

IT-Sicherheit – internationale Rechtsvorgaben

- Auch hier wieder: IT-Sicherheit wird **nicht kodifiziert** geregelt
- Zahlreiche **Einzelvorschriften**, **unterschiedliche Verbindlichkeit**
- Abhängig vom jeweiligen **Geschäfts- bzw. Infrastrukturbereich**
- Verschiedene Beispiele:
  - 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)
  - RL 2009/136/EG über elektronische Kommunikationsnetze (E-Privacy-RL)
  - Teils Überschneidungen mit Datenschutzrecht bei personenbezogenen Daten, vgl. nur Art. 30 **EU-DS-GVO-E**
  - NIS-RL???

IT-Sicherheit – internationale Rechtsvorgaben

- NIS-RL – Zeitplan:
  - **07.02.2013:** Vorschlag der Europäischen Kommission für eine NIS-RL
  - …
  - **29.06.2015:** Vierte Trilog-Sitzung zwischen Kommission, Rat und EP, Einvernehmen über die Hauptprinzipien für die NIS-RL
  - Zügige Umsetzung des politischen Konsens in konkrete Rechtsvorschriften geplant, um endgültige Einigung herbeizuführen (u.a. 142 Änderungswünsche des RL-Vorschlags)
  - Fortgesetzte Verhandlungen im 2. Halbjahr 2015 unter luxemburgischem Vorsitz der Ratspräsidentschaft
  - Bereits mehrere Verhandlungsrunden, die fortgesetzt werden
  - **Inkrafttreten für Anfang 2016 möglich**
  - **Umsetzungsfrist nationales Recht: 18 Monate danach** (Art. 21)

IT-Sicherheit – internationale Rechtsvorgaben

- NIS-RL – Rechtsnatur:
  - Zentraler Bestandteil der **Cyber-Sicherheitsstrategie der EU**
  - 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, <u>überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel</u>.“ → Nationales Umsetzungsgesetz zur Wirksamkeit notwendig.
  - Deutschland: **Nationales Umsetzungsgesetz wohl das IT-SiG**, wird daher ggf. nach NIS-RL-Erlass novelliert
  - Mindestharmonisierung: Deutschland kann auch ein höheres IT-Sicherheitsniveau schaffen, als es die NIS-RL vorgibt

IT-Sicherheit – internationale Rechtsvorgaben

- NIS-RL – rechtspolitische Erwägungen:
  - **Zielsetzung:** Gewährleistung einer hohen NIS. „Hierbei geht es um die Erhöhung der Sicherheit des Internets und der privaten Netze und Informationssysteme, die für das Funktionieren unserer Gesellschaften und Volkswirtschaften unverzichtbar sind.“
  - **Mittel:** „NIS soll erreicht werden, indem die Mitgliedstaaten verpflichtet werden, ihre Abwehrbereitschaft zu erhöhen und ihre Zusammenarbeit untereinander zu verbessern, und indem die Betreiber kritischer Infrastrukturen und die öffentlichen Verwaltungen verpflichtet werden, geeignete Schritte zur Beherrschung von Sicherheitsrisiken zu unternehmen und den zuständigen nationalen Behörden gravierende Sicherheitsvorfälle zu melden.“

IT-Sicherheit – internationale Rechtsvorgaben

- NIS-RL – wesentliche regulatorische Aspekte im Überblick:
  - Gegenüber IT-SiG **eingeschränkte Definition von KRITIS**
  - Jeder Mitgliedstaat der EU soll **nationale NIS-Strategie** und **Kooperationsplan** ausarbeiten
  - Bestimmung einer für NIS zuständigen nationalen Behörde (**BSI**)
  - Verpflichtung zur Einrichtung eines nationalen CERTs (**BSI als CERT-Bund**)
  - Aufbau **Kooperationsnetz** zwischen EU-Kommission und nationalen IT-Behörden; Unterstützung durch **ENISA**
  - Einrichtung eines sicheren Systems für den **Informationsaustausch**; EU-weit koordinierte Reaktion von Sicherheitsrisiken
  - **Meldepflicht** für Private wie auch für öff. Verwaltung für Sicherheitsvorfälle, die „erhebliche Auswirkungen auf die Sicherheit der […]bereitgestellten Kerndienste haben“
  - Verpflichtung zu **Sicherheitsüberprüfungen**
  - **Sanktionsmöglichkeiten**

IT-Sicherheit – internationale Rechtsvorgaben

- Zentrale Dokumente des bisherigen Gesetzgebungsverfahrens zur NIS-RL:
  - EU-Kommissionsvorschlag, 07.02.2013
  - Schlussfolgerungen des Rates zur Cyber-Sicherheitsstrategie der EU, 22.07.2013
  - Änderungsanträge des LIBE-Ausschusses, 07.01.2014
  - Position des EP im Plenum, 13.03.2014
  - Sachstandsbericht, 22.05.2014
  - Position des Rates der Europäischen Union, 05.03.2015
  - Pressemitteilung Verhandlungsdurchbruch, 29.06.2015

Haben Sie vielen Dank für Ihre Aufmerksamkeit

Dr. Dennis-Kenji Kipker, IGMR an der Universität Bremen
Tel.: 0421 218-66049 | Mail: kipker@uni-bremen.de