IT-Sicherheitsgesetz

Was muss ich als Unternehmen in der Praxis beachten?

Heiko Schöning, LL.M.
Rechtsanwalt, Fachanwalt für IT-Recht
SDS Rechtsanwälte Sander Dahm Schöning Partnerschaft mbB

Ihr Referent

- Heiko Schöning, LL.M. (Informationsrecht)
  - Rechtsanwalt
  - Fachanwalt für IT-Recht
- Wesentliche Schwerpunkte in der Beratungspraxis
  - Vertragsrecht im Kontext der IT-und Medienbranche
  - Datenschutzrecht
  - Geschäftsführerhaftung / Insolvenzrecht

Agenda

- Teil 1: IT-Sicherheitsgesetz
  - Was ist das IT-Sicherheitsgesetz?
  - Was muss ich als Adressat beachten?
  - Welche Konsequenzen drohen?
- Teil 2: Ausblick auf die EU – NIS-Richtlinie
- Teil 3: Praxisbeispiel
  - Sicherheitsanforderungen für Telemediendienste - § 13 Abs. 7 TMG n.F.

Teil 1: IT-Sicherheitsgesetz

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.Juli 2015

Heiko Schöning, LL.M.
Rechtsanwalt, Fachanwalt für IT-Recht
SDS Rechtsanwälte Sander Dahm Schöning Partnerschaft mbB

RoadShow Cybercrime
Technologie-Zentrum Kleve

Einführung

- **IT-Sicherheitsgesetz**

  - Artikelgesetz
    - IT-Sicherheitsgesetz ändert bestehende Gesetze, z.B.:

      - Art. 1: BSI-Gesetz („Bundesamt für Sicherheit in der Informationstechnik“)
      - Art. 2: AtomG
      - Art. 3: EnWG
      - Art. 4: TMG
      - Art. 5: TKG

    - IT-Sicherheitsgesetz findet keine unmittelbare Anwendung, sondern verändert bestehende Gesetze

Einführung

- **Sinn und Zweck des IT-Sicherheitsgesetzes**

  - **Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland**
    - **Schutzziele sind:**
      - Vertraulichkeit
      - Integrität
      - Authentizität
      - Verfügbarkeit
  - **Verbesserung der IT-Sicherheit von Betreibern kritischen Infrastrukturen durch Mindeststandards**
  - **Einführung von Meldepflichten für erhebliche „IT-Vorfälle“**

Einführung

- **Vertraulichkeit:**
  - Lesen und **Bearbeiten von Daten nur durch autorisierte Anwender**, bei Zugriff und Übermittlung
- **Integrität:**
  - **keine unbemerkte** und nicht nachvollziehbare **Veränderung von Daten**, bei Zugriff und Übermittlung
- **Authentizität:**
  - **eindeutige Zuordnung** der Daten **zum Ersteller**/Bearbeiter
- **Verfügbarkeit:**
  - **Gewährleistung des Zugriffs** im gewünschten Zeitraum

Wer ist Adressat der Neuregelungen?

- **Betreiber „Kritischer Infrastrukturen“** (wer das ist, regelt eine VO)
  - Ausnahme: Kleinstunternehmen gem. § 8c BSI-G; Verweis auf 2003/361/EC
- **Atomkraftwerkbetreiber** („Genehmigungsinhaber nach dem AtomG“)
- **Betreiber von Energieversorgungsnetzen und Energieanlagen die als „Kritische Infrastruktur“ eingeordnet werden** (s.a. VO)
- **Betreiber öffentlicher Telekommunikationsnetze oder öffentlich zugänglicher Telekommunikationsdienste** (§ 3 Nr.16a, 17a TKG)
- **Telemediendienstanbieter** (sehr weiter Anwendungsbereich!)
  - *Diensteanbieter ist jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt* (§ 2 Nr. 1 TMG)

Kritische Infrastruktur (1)

- **§ 2 Abs. 10 BSI-G:**
  - Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

    - 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
    - 2. von **hoher Bedeutung** für das Funktionieren **des Gemeinwesens** sind, weil durch ihren **Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit** eintreten würden.

  - Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 (BSI-G) näher bestimmt.

Kritische Infrastruktur (2)

- **Meldepflichtige Betreiber: ca. 2.000 (Schätzung der BReg)**
- **Konkretisierung durch „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung)“**
- in den vier (von insgesamt sieben betroffenen) Sektoren **Energie, Wasser, Ernährung** und **IKT** werden **730** „KritiS“-Betreiber (nicht Anlagen!) von der VO erfasst (laut der VO)
  - ➢ Weitere Konkretisierung erfolgt, wenn die noch ausstehenden Sektoren **Transport und Verkehr, Gesundheit und Finanz- und Versicherungswesen** geregelt werden
- „*Auswirkungen aus Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten*“

Kritische Infrastruktur (3)

- **Umsetzungsfrist**: **2 Jahre** ab Inkrafttreten der Rechtsverordnung (03.05.2016)
  - („spätestens“) § 8a Abs. 1 S. 1 BSI-G → Mai 2018
- Nachweispflicht der Betreiber bezüglich der Umsetzung der vom Gesetz geforderten Maßnahmen „*mindestens alle **zwei Jahre***“ (§ 8a Abs. 3 S. 1 BSI-G)
  - Nachweis kann erbracht werden durch
    - Sicherheitsaudits
    - Prüfungen oder
    - Zertifizierungen
  - „*Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen* (…) *Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen*.“

Kritische Infrastruktur (4)

- Bei Zuwiderhandlungen drohen erhebliche Bußgelder, § 14 BSI-G

  - bis zu 50.000 EUR

  - bei Zuwiderhandlungen gegen Beseitigungsanordnungen des BSI (bezogen auf die Sicherheitsmängel) bis zu 100.000 EUR

Kritische Infrastruktur (5.1)

- **Kritis-Betreiber sind** (gemäß § 8a Abs. 1 BSI-G) **verpflichtet,**

  - angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse 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**.

Kritische Infrastruktur (5.2)

- „*Bei der Frage der Angemessenheit ist der bei dem Betreiber erforderliche Aufwand, insbesondere die von ihm aufzuwendenden Kosten, zu berücksichtigen*“ *(Begründung BT-Drs. 18/4096, S. 26)*

- Die Angemessenheit der Kosten müssen jeweils abgewogen werden, gegenüber dem jeweiligen Schaden, der bei einem Ausfall droht

- **Fazit**

  - Es herrscht derzeit Rechtsunsicherheit, welche Maßnahmen konkret umzusetzen sind, damit der unbestimmte Rechtsbegriff der **Angemessenheit** von den Normadressaten erfüllt werden kann

Kritische Infrastruktur (6.1)

- **Der „etablierte Dreiklang“ von**
  - **allgemeinen Regeln der Technik** (z.B. DIN-Normen)
  - **Stand der Technik**
  - **Stand von Wissenschaft und Technik**
- **Drei-Stufen-Theorie des Bundesverfassungsgerichts („Kalkar“)**

Kritische Infrastruktur (6.2)

- **„Stand der Technik“**
  - Laut Gesetzesbegründung „*der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen* (…) *gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lassen*“ (BT-Drucks. 18/4096, S. 26)
  - „in der Praxis eingesetzte fortschrittliche Verfahren“ (und somit besser als der Durchschnitt)
  - Durch das Wort „soll“ sind in begründeten Fällen Ausnahmen vom „*Stand der Technik*“ möglich, z.B. weil Sicherheitsupdates oftmals nicht sofort umsetzbar sind
- ISO 27001 wohl nicht ausreichend
- BSI-Grundschutz-Katalog?

Teil 2: Ausblick auf die EU – NIS-Richtlinie

Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, COM(2013) 48 final 2013/002 (COD)

Heiko Schöning, LL.M.
Rechtsanwalt, Fachanwalt für IT-Recht
SDS Rechtsanwälte Sander Dahm Schöning Partnerschaft mbB

RoadShow Cybercrime
Technologie-Zentrum Kleve

Anwendungsbereich der NIS-RL

- **Erfasst nicht nur den privaten, sondern auch den öffentlichen Sektor**
  - Bund und Länder werden entsprechende Regelungen erlassen müssen
- **Betreiber kritischer Infrastrukturen werden über Annex definiert**
- **Erfasst werden auch „Anbieter digitaler Dienste“ (Annex III)**
  - Cloud-Dienste
  - Online-Handelsplattformen (Waren und Güter)
  - Suchmaschinen
  - Art. 3 NIS-RL erwähnt ferner Domain-Name-Server und Registrare
  - **Ausnahme: Kleinstunternehmen** (2003/361/EC) bis 10 MA, max. 2 Mio. Umsatz
  - Nicht erfasst: Hersteller von Hard- und Software, Plattformbetreiber / soziale Netze

Befugnisse der Aufsichtsbehörden

- **Weitergehende Befugnisse** (im Vergleich zum BSI-G)
  - **Aufsichtsbehörde darf Sicherheitsaudit selbst durchführen**
    - **Kann hier einen „qualified auditor“ beauftragen**

Stand der Technik

- Es besteht zwar gem. Art. 16 NIL-RL eine Plicht, dass die Mitgliedstaaten die Verwendung von europäischen oder international akzeptierten Standards fördern, aber es gibt keinen Mechanismus, diese Standards EU-weit zu akzeptieren
- Es besteht die Gefahr, dass es länderspezifisch unterschiedliche „Stand der Technik“ („state of the art“) geben wird, ohne die Möglichkeit einer Harmonisierung

Teil 3: Praxisbeispiel

Sicherheitsanforderungen für Telemediendienste § 13 Abs. 7 TMG n.F.

Heiko Schöning, LL.M.
Rechtsanwalt, Fachanwalt für IT-Recht
SDS Rechtsanwälte Sander Dahm Schöning Partnerschaft mbB

RoadShow Cybercrime
Technologie-Zentrum Kleve

§ 13 Abs. 7 TMG (n.F.)

- 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.

Geschäftsmäßig i.S.v. § 13 Abs. 7 TMG

- Geschäftsmäßig ist ein Angebot dann, wenn es auf einer nachhaltigen Tätigkeit beruht, es sich also um eine planmäßige und dauerhafte Tätigkeit handelt.
- Bei einem entgeltlichen Dienst liegt dies regelmäßig vor, so z.B. bei werbefinanzierten Webseiten.
- Das nicht-kommerzielle Angebot von Telemedien durch Private und Idealvereine wird demgegenüber nicht erfasst.

- **Problem:** keine Harmonisierung mit § 5 TMG (wohl Redaktionsversehen)

Adressaten / Betroffene

- Neben Webseitenbetreiber gemäß der allgemeinen Definitionen der §§ 1, 2 TMG auch

  - Cloud Computing Anbieter
  - Telemedienanbieter auf Plattformen wie *Facebook* u.a.
  - Betreiber von Blogs

Die Definition der Telemedien

- § 1 Abs. 1 S. 1 TMG:
  „Dieses Gesetz gilt für

  alle elektronischen Informations- und Kommunikationsdienste,

  soweit sie **nicht**
  - TK-Dienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen,
  - TK-gestützte Dienste nach § 3 Nr. 25 des TKG oder
  - Rundfunk nach § 2 RStV

  sind (Telemedien).“

Die Definition der Telemedien

- Was fällt unter den Begriff der Telemedien i.S.v. § 1 Abs. 1 S. 1 TMG?

  alle

- elektronischen Informationsdienste

  und

- elektronischen Kommunikationsdienste

Sicherungsmaßnahmen des Diensteanbieters

- „Kritische Infrastruktur“ i.e.S. nicht erforderlich
- Sicherungsmaßnahmen nach dem „Stand der Technik“ erforderlich,
  - im Rahmen des technisch Möglichen und
  - wirtschaftlich Zumutbaren,
- um unerlaubte Zugriffe auf Telemedienangebote und die technischen Einrichtungen zu verhindern sowie
- den Schutz pbD zu gewährleisten und
- Störungen (auch von außen) zu verhindern.
  - z.B. durch https („SSL“) als anerkanntes Verschlüsselungsverfahren

Stand der Technik i.S.v. § 13 Abs. 7 TMG

- „Berücksichtigung“ des „Standes der Technik“ erlaubt – anders als das BSI-G – ein weitergehendes Abweichen von diesem, sofern dieser zuvor eruiert und bedacht wurde (Dokumentation!)
- Aber: Begrenzung auf „technische Möglichkeiten“ ist nicht subjektiv auf den einzelnen Anbieter bezogen, sondern auf den durchschnittlichen vergleichbaren Anbieter (umstr.)
  - ➢ Ziel: Gewährleistung eines allgemeinen Sicherheitsniveaus

- Kontrollfrage:
  - ➢ Kann etwas technisch unmöglich sein, wenn es „Stand der Technik“ ist?
    - o Objektive / subjektive Betrachtung

Was wollte der Gesetzgeber?

- **Betreiber von Telemedien sollen Software regelmäßig aktualisieren bzw. Patches einspielen**
- **Werbedienstleiter sollen vertraglich verpflichtet werden, z.B. um Drive-by-Downloads zu verhindern**
- **Kriterium: Herrschaft des Telemediendienstanbieters**
  - Nutzer bei *Facebook* kann keine Sicherungsmaßnahmen der von *Facebook* betriebenen Systeme vornehmen

Vielen Dank für Ihre Aufmerksamkeit

Fragen? Anmerkungen? … Diskussion!

Heiko Schöning, LL.M.
Rechtsanwalt und
Fachanwalt für IT-Recht

0203 / 39 20 89 00
schoening@sds.ruhr

Rechtsanwälte
SANDER DAHM SCHÖNING
Partnerschaft mbB

Harmoniestraße 2a, 47119 Duisburg
https://www.sds.ruhr