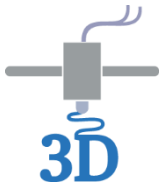
# Entwurf zum IT-Sicherheitsgesetz & Bird & Bird

Sebastian Hinzen, LL.M.
Bird & Bird LLP

6. IT LawCamp 2015




LawCamp

# Agenda

Einleitung

Wesentliche neue Regelungen im

- BSI-Gesetz
- TMG
- TKG

Fazit & Ausblick

# Einleitung (1) – Ziel und Mittel des Gesetzes

- Ziel: IT-Sicherheit in Deutschland verbessern
- Adressaten: Betreiber Kritischer Infrastrukturen
- Mittel:
  - Verpflichtende IT-Sicherheitsanforderungen
  - Meldepflicht bei Sicherheitsvorfällen
  - Information/Warnung durch BSI
- Verfahrensstand

# Einleitung (2) Europäischer Kontext

Netz- und Informationssicherheitsrichtlinie (NIS)

- Inhaltlich große Überschneidungen
  - Verpflichtende IT-Sicherheitsanforderungen
  - Meldepflicht bei Sicherheitsvorfällen
- aber auch einige Unterschiede
  - Anwendungsbereich
    - (P) Dienste der Informationsgesellschaft
  - Überprüfung der Sicherheitsvorkehrungen und Meldepflicht

# Einleitung (3) – Europäischer Kontext

Netz- und Informationssicherheitsrichtlinie (NIS)

- Nur Mindestharmonisierung, d.h.
  - Europäischer "Flickenteppich" wahrscheinlich
  - (P) Wettbewerbsnachteile für deutsche Unternehmen wegen strengerer Vorgaben nach dem IT-Sicherheitsgesetz
- Ggfs. Doppelter Umsetzungsbedarf
- Verfahrensstand: Verabschiedung für 07/2015 geplant; Umsetzung binnen 18 Monaten

# Überblick zu neuen Regelungen im BSI-G

1. § 2 X iVm. § 10 I: Definition "Kritische Infrastrukturen" mit VO-Ermächtigung
2. § 8a: IT-Sicherheitsanforderungen an Betreiber von KI
3. § 8b IV: Meldepflicht für Sicherheitsvorfälle
4. § 7a: Untersuchung von IT-Produkten

# Neue Regelungen im BSI-G - § 2 X: Definition "Kritische Infrastrukturen" mit VO-Ermächtigung

*"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 [Qualität] für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe [Quantität] oder Gefährdungen für die öffentliche Sicherheit eintreten würden.*

*Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt."*

# Neue Regelungen im BSI-G – § 8a: Sicherheitsanforderungen an Betreiber von KI

- Technische und organisatorische Vorkehrungen zur Vermeidung von Störungen/Ausfällen
- Angemessenheit (+), wenn (finanzieller) Aufwand nicht außer Verhältnis zu Ausfall/Beeinträchtigung steht
- "Stand der Technik" zu berücksichtigen
- Zertifizierung "branchenspezifischer Sicherheitsstandards" durch BSI
- Umsetzungsfrist: 2 Jahre nach Erlass der RVO; danach im Abstand von 2 Jahren nachzuweisen

# Neue Regelungen im BSI-G – § 8b IV: Meldepflicht für Sicherheitsvorfälle

- Zu melden sind: "[…] *erhebliche Störungen* […], *die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit* […] *führen können oder bereits geführt haben*"
- (P) Unbestimmtheit ("Störung/Beeinträchtigung")
- (P) auch potentielle Störungen
  - Regelbeispiele?
- Anonyme Meldung möglich, solange es nicht tatsächlich zu Ausfall/Beeinträchtigung kam

# Neue Regelungen im BSI-G – § 7a: Untersuchung von IT-Produkten

- Befugnis, IT-Produkte/Systeme zu Beratungs- und Warnungszwecken zu untersuchen
- Auf dem Markt bereitgestellte sowie zur Bereitstellung vorgesehene Produkte
- Untersuchung kann durch Dritte erfolgen (sofern keine entgegenstehenden Interessen der Hersteller)
  - (P) Geheimnisschutz
- Zweckbindung bzgl. der Erkenntnisse
- Stellungnahmemöglichkeit für Hersteller

# Neue Regelungen im TMG - § 13 VII: Sicherheits-anforderungen für Telemediendiensteanbieter

- Adressat: Diensteanbieter, die geschäftsmäßig Telemedien anbieten (weites Verständnis)
- Technische und organisatorische Vorkehrungen, um sicherzustellen, dass
  - Kein unerlaubter Zugriff
  - Schutz personenbezogener Daten
  - Schutz gegen äußere Angriffe
- Regelbeispiel: Verschlüsselungsverfahren
- Stand der Technik, aber nur soweit technisch möglich und wirtschaftlich zumutbar

# Neue Regelungen im TKG - § 109 II TKG: Verschärfung der technischen Schutzmaßnahmen

- Berücksichtigung des Stands der Technik: nunmehr auch bei technischen und organisatorischen Maßnahmen zur IT-Sicherheit (§ 109 II)
  - Änderungen des Sicherheitskatalogs nach § 109 VI TKG?
- Überprüfung Umsetzung des Sicherheitskonzepts durch BNetzA:
  - Bislang nur Befugnis und keine Pflicht
  - Nunmehr Pflicht zur regelmäßigen Überprüfung (ca. alle 2 Jahre)

# Neue Regelungen im TKG - § 109 V TKG: Erweiterung der Meldepflicht

- Ausweitung der Meldepflicht auf Beeinträchtigungen, die zu beträchtlichen Sicherheitsverletzungen führen können
  - Ziel: Früherkennung
  - (P) Bestimmtheit
- Adressat: weiterhin BNetzA, die an das BSI weiterleitet
- Keine Möglichkeit der anonymen Meldung

# Neue Regelungen im TKG - § 109a IV TKG: Informationspflicht gegenüber Nutzern

- Informationspflicht gegenüber Nutzern, sofern Störungen vom Nutzersystem ausgehen
- Inhalt:
  - Hinweis auf angemessene, wirksame und zugängliche Mittel, mit denen Störungen erkannt und beseitigt werden können
- nur soweit bekannt
  - Keine Untersuchungspflicht
  - Keine Ermächtigung zur Datenerhebung

# Zusammenfassung

- Sicherheitsanforderungen
  - Neu: für KI-Betreiber, Telemediendiesteanbieter
  - Ausweitung für TK-Anbieter
- Meldepflichten
  - Neu: für KI-Betreiber
  - Ausweitung für TK-Anbieter
- BSI kann IT-Produkte untersuchen und warnen
- TK Betreiber haben Nutzer über Störungen, die von ihren Systemen ausgehen, informieren

# Fazit & Ausblick

- Umfangreicher Umsetzungsbedarf für KI-Betreiber, Telemediendienstebetreiber und TK-Anbieter
- Hoher Beratungsbedarf wegen unbestimmter Rechtsbegriffe
- Gesetzgebungsverfahren verfolgen
- Europäischen Kontext beachten (NIS-RiLi)

# Vielen Dank & Bird & Bird

Sebastian Hinzen LL.M.
Bird & Bird LLP
Carl-Theodor-Straße 6
40213 Düsseldorf
sebastian.hinzen@twobirds.com