




U N I K A S S E L
V E R S I T Ä T

Das IT-Sicherheitsgesetz – Zielsetzungen und Sicherheitsmaßnahmen

Prof. Dr. Gerrit Hornung, LL.M.
Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht

Inhaltliches Rahmenprogramm
der provet-Mitgliederversammlung 2015
Kassel, 13. November 2015



Übersicht

Gerrit Hornung

Hintergründe

Überblick

Einzelfragen

- **Hintergründe**
- **Überblick zum IT-Sicherheitsgesetz**
- **Einzelfragen**

- Bedeutung der IT-Sicherheit in Kritischen Infrastrukturen (KRITIS)
- Regulierungsfrage: sinnvolles Maß an
 - Staatlichen Vorgaben
 - Selbstverantwortung und Selbstregulierung
- Besonderheiten:
 - Geringe intrinsische Anreize für kostenträchtige IT-Sicherheitsmaßnahmen
 - Hohe potentielle Auswirkungen von Vorfällen
 - Unterentwickelte Kommunikation über Probleme und Vorfälle
- Paralleles EU-Gesetzgebungsverfahren: Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS-RL)

- IT-Sicherheitsgesetz vom 17.7.2015
- Anwendungsbereich:
 - KRITIS
 - Alle (!) geschäftsmäßig erbrachte Telemedien
- Hauptsächliche Inhalte
 - Vorgaben für IT-Sicherheitsstandards – und Nachweis der Einhaltung
 - Meldepflichten für IT-Sicherheitsvorfälle

§ 2 BSIG: Begriffsbestimmungen

(10) 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 näher bestimmt.

Nicht erfasste Bereiche

Gerrit Hornung

Hintergründe

Überblick

Einzelfragen

- Öffentlicher Sektor
- Kleinstunternehmen (außer: Webseitenbetreiber)
- Kultur und Medien

- Pflicht:
 - angemessene
 - organisatorische und technische Vorkehrungen
 - zur Vermeidung von Störungen
 - der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit
 - der IT-Systeme, Komponenten oder Prozesse
- Branchenstandards können vorgeschlagen werden (außer im EnWG) – offene Probleme:
 - Keine Ersatzvornahme des BSI bei Untätigkeit der Branchen
 - Keine Regelung bei verschiedenen Vorschlägen für selbe Branche
 - Keine (explizite) Pflicht zur Pflege der Standards
- Nachweis: Sicherheitsaudits, Prüfungen oder Zertifizierungen (alle 2 Jahre) – Problem der Effektivität

- Meldepflichtig nach BSIG:
 - Erhebliche Störungen
 - der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit
 - von IT-Systemen, Komponenten und Prozessen
 - die
 - a) zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur führen können
 - b) oder schon geführt haben
- Umsetzung:
 - Namentliche Meldung, wenn Störung eingetreten ist
 - Pseudonyme Meldung (über Kontaktstelle), wenn nicht eingetreten
- Erhebliche terminologische und tlw. auch inhaltliche Abweichungen im TKG, EnWG, AtomG

- IT-Sicherheitsstandards
 - Ursprünglich: Bußgelder nur für Webseitenbetreiber (TMG)
 - Jetzt:
 - a) TMG + BSIG
 - b) Immer noch nicht: EnWG + TKG
- Meldepflichten:
 - Ursprünglich: Bußgelder nur für TK-Anbieter (TKG)
 - Jetzt:
 - a) TKG + BSIG
 - b) Immer noch nicht: AtomG + EnWG

- Starke Regulierung der Informationsflüsse *zum* BSI
- Fragmentarische Regulierung der Information *durch das* BSI
 - Information der KRITIS-Betreiber: OK (Ermessen – ggf. Reduktion auf Null)
 - Information Dritter:
 - a) Nur auf Antrag (Anlass für Antrag auf Information – ohne Information?)
 - b) Keine Abwägung mit legitimen Informationsinteressen
 - c) Keine Beteiligung des KRITIS-Betreibers, über den informiert wird
 - Information der Öffentlichkeit:
 - a) Explizit nur im TKG
 - b) Allgemeine Befugnis zu Warnungen nach BSIG – Reichweite offen

- Pflichten nach § 13 VII TMG – (weit) über KRITIS hinaus
- (Sehr) unbestimmte Regelung in § 100 I TKG beibehalten
- Befugnis des BS, IT-Produkte und -Systeme zu untersuchen – auch gegen den Willen und ohne Information der Hersteller
- Erweiterte Befugnis zur Erarbeitung von Mindeststandards für IT-Sicherheit des Bundes
- Haftungsfragen: nicht explizit adressiert – Auswirkungen?

Das IT-Sicherheitsgesetz – Zielsetzungen und Sicherheitsmaßnahmen

- *Hornung*, Neue Pflichten für Betreiber Kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes, NJW 2015, i.E.

Prof. Dr. Gerrit Hornung, LL.M.

gerrit.hornung@uni-kassel.de

<https://www.uni-kassel.de/go/gerrithornung>