UNIKASSEL
VERSITÄT

Die Bedeutung des IT-Sicherheitsgesetzes für den Straßenverkehr

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

3. Würzburger Tagung zum Technikrecht: „Auf dem Weg zum autonomen Fahrzeug“
Würzburg, 12. Dezember 2015

Übersicht

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- Hintergründe
- Überblick zum IT-Sicherheitsgesetz
- Einzelfragen im Bereich Transport und Verkehr
- Insbesondere: Haftungsrechtliche Probleme
- Ausblick

Hintergründe

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- 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)
  - Grds. Einigung im Trilog in dieser Woche

Das IT-Sicherheitsgesetz

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- IT-Sicherheitsgesetz vom 17.7.2015

- Anwendungsbereich:
  - KRITIS
  - Alle (!) geschäftsmäßig erbrachte Telemedien
  - Nicht erfasst:
    a) Öffentlicher Sektor – Bundestag
    b) Kleinstunternehmen (außer: Webseitenbetreiber)
    c) Kultur und Medien – TV5Monde

- Hauptsächliche Inhalte
  - Vorgaben für IT-Sicherheitsstandards – und Nachweis der Einhaltung
  - Meldepflichten für IT-Sicherheitsvorfälle

Anwendungsbereich

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

§ 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.

Anwendung auf „Transport und Verkehr“

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

Bundesamt
für Sicherheit in der
Informationstechnik

KRITIS-Sektorstudie

Transport und Verkehr

Öffentliche Version – Revisionsstand 5. Februar 2015

Anwendung auf „Transport und Verkehr“

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- Bedeutung:
  - Hohe (und zunehmende) Bedeutung der IT-Sicherheit für vernetztes / autonomes Fahren – unabhängig von KRITIS
  - Besondere Rolle von KRITIS in der Verkehrstelematik
- Anwendung aus § 2 Abs. 10 BSIG de facto nicht ableitbar – VO entscheidend
  - Planung: Regulierung in 2 „Körben“ – Transport und Verkehr im 2. Korb (Ende 2016)
- Mutmaßliche Richtung:
  - Einzelne Fahrzeuge / Komponenten: keine KRITIS
  - Geonavigationssysteme (Galileo,…): (+)
  - Verkehrstelematik-Infrastruktur (Verkehrsleitsysteme, Ampelsysteme,…): (+) – je nach Bedeutung
  - Einzelne Hersteller?
    a) Grds. (-), aber (+), wenn Verkehrsleitinfrastrukturen betreiben
    b) Also: ggf. auch herstellerbezogene Infrastrukturen

Anwendung auf das vernetzte Automobil

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- Einzelnes Automobil ≠ KRITIS – **aber**: Vielzahl geschäftsmäßig angebotener Telemedien im vernetzten Automobil
  - Viele heutige Navigationsdienste
  - Mutmaßlich: viele Steuerungsdienste des autonomen Fahrens
  - Entertainment-Bereich

- Folge: § 13 VII 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**.

IT-Sicherheitsstandards

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- 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

Meldepflichten

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- 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)

Sanktionen

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- IT-Sicherheitsstandards
  - Ursprünglich: Bußgelder nur für Webseitenbetreiber (TMG)
  - Jetzt:
    a) TMG + BSIG (also für Transport und Verkehr)
    b) Immer noch nicht: EnWG + TKG

- Meldepflichten:
  - Ursprünglich: Bußgelder nur für TK-Anbieter (TKG)
  - Jetzt:
    a) TKG + BSIG (also für Transport und Verkehr)
    b) Immer noch nicht: AtomG + EnWG

Informationsflüsse

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- 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

Weitere Fragen

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

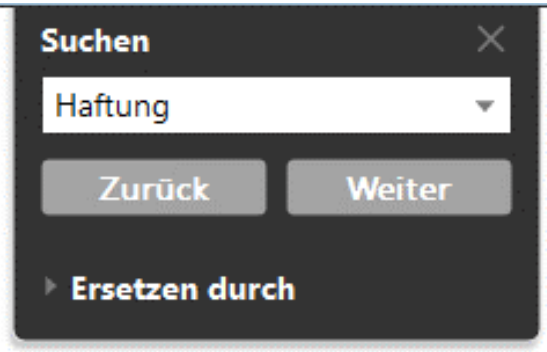
- ((Sehr) unbestimmte Regelung in § 100 I TKG beibehalten)
- (Erweiterte Befugnis zur Erarbeitung von Mindeststandards für IT-Sicherheit des Bundes)
- Befugnis des BSI, IT-Produkte und -Systeme zu untersuchen
  - Inhalt:
    a) Auch gegen den Willen der Hersteller
    b) Ohne Information der Hersteller
    c) Information erforderlich, wenn Veröffentlichung – aber kein Veto der Hersteller
  - Befugnis erfasst auch autonome Fahrzeuge + Komponenten der Verkehrstelematik

Ausgangspunkt

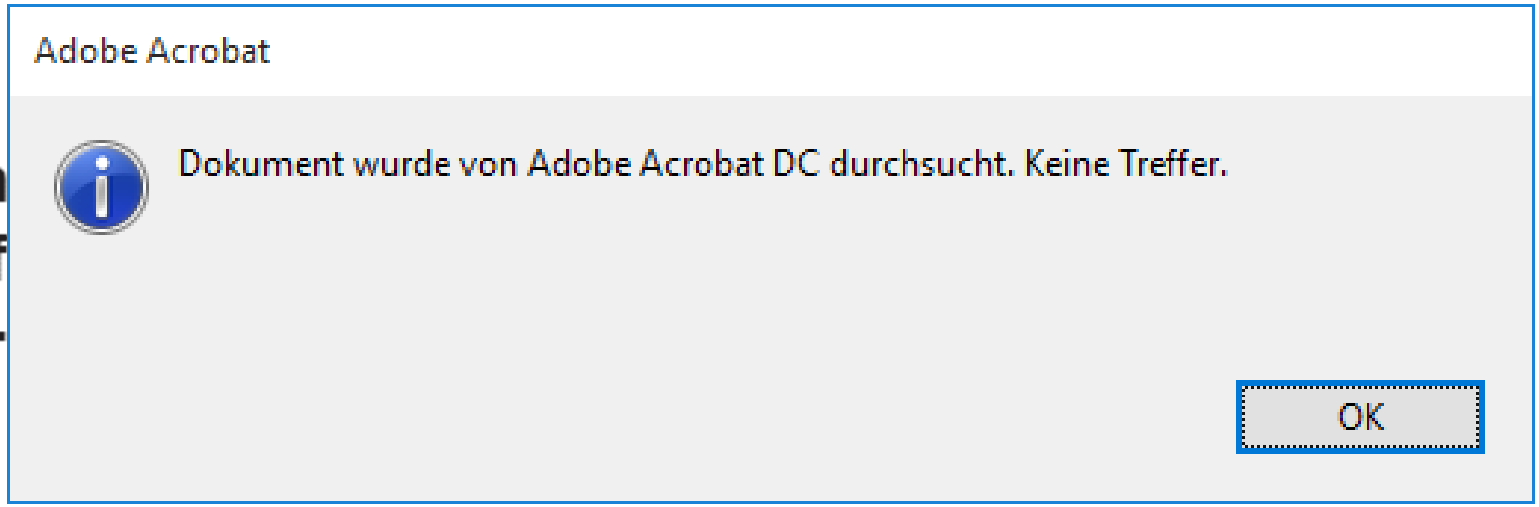
Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

Gesetzentwurf

der Bundesregierung



En
inf
(IT



Auswirkungen für allgemeine Haftungsfragen

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- Gesetz regelt spezifische Verhaltenspflichten der Anbieter im Bereich der IT-Sicherheit – Auswirkungen?
- Allgemeine Fahrlässigkeitsmaßstäbe – z.B. Begründung von Verkehrspflichten (für § 823 I BGB, i.V.m. „Stand der Technik“ + besonderer Bedeutung der KRITIS)?
- Meldepflichten als Schutzgesetze für andere KRITIS-Betreiber (für § 823 II BGB)?
  - Jedenfalls (wohl) nicht nach künftiger NIS-RL
- Vertragliche Haftung
  - Auswirkungen auf die AGB-Kontrolle – keine Haftungsfreistellung für Abweichungen von Branchenstandards?
  - Haftung von Zulieferern bei Lieferung von Komponenten, die Branchenstandards nicht einhalten?

Spezifische Ansatzpunkte (I)

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- § 13 VII 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**.

- Haftung
  - i.V.m. §§ 7, 8 BDSG?
  - i.V.m. § 823 II BGB?

Spezifische Ansatzpunkte (II)

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- Haftung der TK-Anbieter für autonome Automobile:
  - § 109a IV TKG n.F.: Werden dem Diensteanbieter nach Absatz 1 **Störungen bekannt**, die von Datenverarbeitungssystemen der Nutzer ausgehen, so **hat er die Nutzer**, soweit ihm diese bereits bekannt sind, unverzüglich darüber **zu benachrichtigen**. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche **technische Mittel hinzuweisen**, mit denen sie diese Störungen erkennen und beseitigen können.
  - §§ 44, 44a TKG: Haftung für Verstöße „gegen dieses Gesetz“
- Amtshaftung des BSI?
  - Zumindest für Informationspflichten nach § 8b II Nr. 4 BSIG: gut vertretbar
- Haftung der Verbraucher?
  - Im Einzelfall diskutabel: Ignorierung einer Benachrichtigung nach § 109a IV TKG
  - Allgemeine Verkehrspflichten? Änderung durch IT-SichG?

Ausblick

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

- Erfordernis technischer Gestaltung: in verschiedenen Dimensionen
  - KRITIS – auf Infrastrukturebene
  - Komponenten, die nicht für Gesellschaft, aber für den Einzelnen kritisch sind
- Als Instrument des Grundrechtsschutzes
  - „privacy by design“: Recht auf informationelle Selbstbestimmung
  - „IT-security by design“: Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Hintergründe
Überblick
Einzelfragen
Haftungsrecht
Ausblick

Die Bedeutung des IT-Sicherheitsgesetzes für den Straßenverkehr

- *Hornung*, Neue Pflichten für Betreiber Kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes, NJW 2015, 3334.
- *Hornung*, Verfügungsrechte an fahrzeugbezogenen Daten. Das vernetzte Automobil zwischen innovativer Wertschöpfung und Persönlichkeitsschutz, DuD 2015, 359-366.
- *Hornung/Goeble,* „Data Ownership“ im vernetzten Automobil. Die rechtliche Analyse des wirtschaftlichen Werts von Automobildaten und ihr Beitrag zum besseren Verständnis der Informationsordnung, CR 2015, 265-273.

Prof. Dr. Gerrit Hornung, LL.M.
gerrit.hornung@uni-kassel.de
https://www.uni-kassel.de/fb07/hornung