Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

Haftungsfalle Rechenzentrum?

IT-Sicherheit zwischen Rechtssetzung und Rechtsanwendung

ZKI-Frühjahrstagung – 8.März 2016

a | i3
Arbeitsgruppe **Identitätsschutz im Internet**

ZKI
Zentren für Kommunikation und Informationsverarbeitung e.V.

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

Das Institut für Rechtsinformatik

- Aktuelle Veröffentlichung: Rechtshandbuch Cloud Computing
- Aktuelle Projekte (Auszug)
  - VERTRAG: „Vertrauenswürdiger Austausch Geistigen Eigentums in der Industrie“ (gefördert vom BMBF)
  - Verifi-eID: Rechtssichere Verifikation elektronischer Identitäten in „betreibersicheren“ Cloud-Systemen (gefördert vom BMBF)
  - elektronische Personalakte (mit Staatskanzlei des Saarlandes)
  - „Sicheres Arbeiten im Web 2.0“: Fokus kollaboratives Arbeiten
- Forschungspartner
  - EDV-Gerichtstag
  - SAP (IT-Law in Research and Practice)
  - Horst-Görtz-Institut für IT-Sicherheit
  - Arbeitsgruppe Identitätsschutz im Internet (a-i3)

a | i3

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

a-i3/BSI Symposium 2016

Bundesamt für Sicherheit in der Informationstechnik

a | i3
Arbeitsgruppe Identitätsschutz im Internet

Medienpartner des a-i3/BSI-Symposiums 2016

itrb IT-Rechts-berater

CR Computer und Recht

www.a-i3.org

a | i3

Agenda

I. **Überblick**

II. Mechanismen zur Regulierung von IT-Sicherheit

III. IT-Sicherheit durch zivilrechtliche Haftung

IV. Lösungsansätze

V. Fazit

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

I. Überblick

- Handlungsziel: IT-Sicherheit

  „IT-Sicherheit umfasst Vertraulichkeit, Verfügbarkeit, Authentizität und Integrität informationsverarbeitender Systeme.“

- Mechanismen zur Verhaltensbeeinflussung

Markt	Moral	*nicht-staatliches Handeln*
Information	**Gesetz**	*staatliches Handeln*
normunabhängig	*normgeleitet*	

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

Agenda

I. Überblick

II. Mechanismen zur Regulierung von IT-Sicherheit

III. IT-Sicherheit durch zivilrechtliche Haftung

IV. Lösungsansätze

V. Fazit

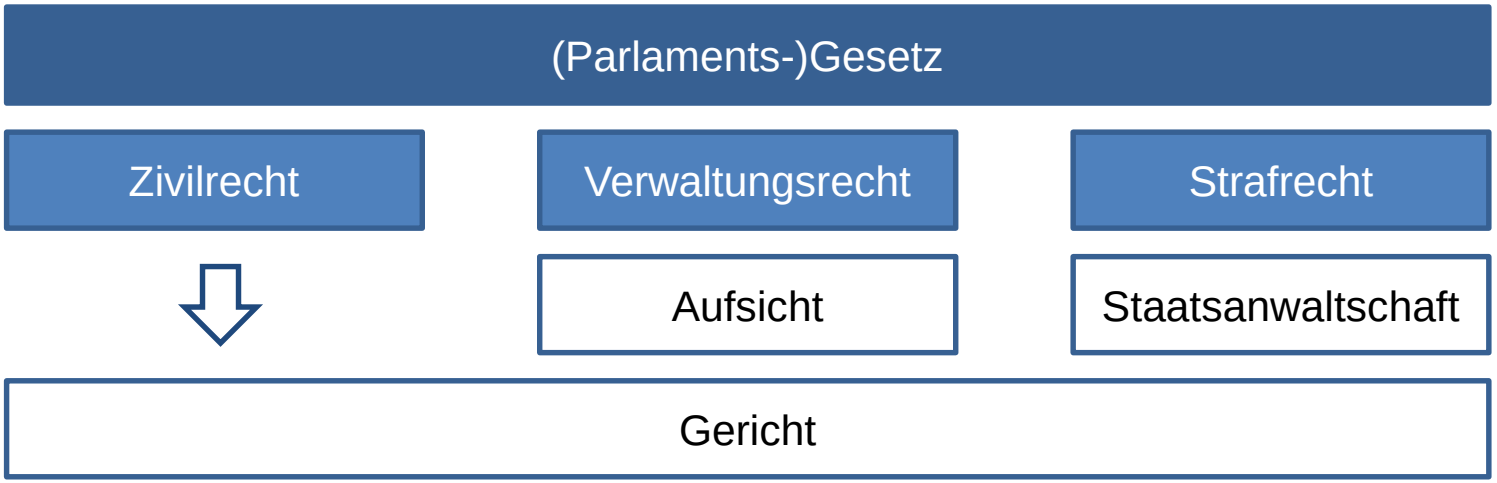
Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

II. Mechanismen zur Regulierung von IT-Sicherheit

1. Handlungsanreize im Recht

- Subventionen
- Sanktionen



Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

II. Mechanismen zur Regulierung von IT-Sicherheit

2. Spezifische Anforderungen im Bereich IT-Sicherheit

- IT-Sicherheit erfordert flexible Regelungen
  - IT-Sicherheit ist schnelllebig
  - Gesetzgebung ist (zu) zeitintensiv
  - Entwicklung durch Rechtsprechung ist (zu) zeitintensiv

- Alternativen zum Parlamentsgesetz
  - Rechtsverordnungen
  - Verwaltungsvorschriften
  - Technische Standards
  - Zertifizierung

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

II. Mechanismen zur Regulierung von IT-Sicherheit

3. Spezifische Regelungen im Bereich IT-Sicherheit

- IT-Sicherheitsgesetz
  - §§ 8a, 8b BSI-G

    (1) Betreiber Kritischer Infrastrukturen sind verpflichtet, […] ***angemessene organisatorische und technische Vorkehrungen*** *zur Vermeidung von Störungen der* ***Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit*** *ihrer informations-technischen Systeme, Komponenten oder Prozesse zu treffen […]*
    (2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können ***branchenspezifische Sicherheitsstandards*** *zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten.*
    (3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch ***Sicherheitsaudits, Prüfungen oder Zertifizierungen*** *erfolgen.*
  - kritische Infrastrukturen: auch Rechenzentren (ab 50 MW)
  - Rechtsfolge bei Verstoß: Bußgeld bis 100.000 €

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

II. Mechanismen zur Regulierung von IT-Sicherheit

3. Spezifische Regelungen im Bereich IT-Sicherheit

- IT-Sicherheitsgesetz
  - § 13 Abs. 7 TMG

    *Diensteanbieter haben, soweit dies **technisch möglich und wirtschaftlich zumutbar** ist, […] 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.*
  - Rechtsfolgen bei Verstoß:
    - Bußgeld bis 50.000 €
    - umstritten: Haftung auf Schadensersatz

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

II. Mechanismen zur Regulierung von IT-Sicherheit

3. Spezifische Regelungen im Bereich IT-Sicherheit

- Datenschutzrecht
  - § 9 BDSG (zukünftig auch: Art. 30 DSGVO)

    Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die ***technischen und organisatorischen Maßnahmen*** *zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. (§ 9 BDSG)*
  - Möglichkeit des Datenschutzaudits (§ 9a BDSG)
  - Rechtsfolgen bei Verstoß
    - Eingriffsbefugnis der Aufsichtsbehörde
    - umstritten: Schadensersatzanspruch

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

II. Mechanismen zur Regulierung von IT-Sicherheit

3. Spezifische Regelungen im Bereich IT-Sicherheit

- zahlreiche Vorschriften, die an „Stand der Technik“ anknüpfen
  - Anlage zu § 9 BDSG; § 3 VI BImSchG; § 21e III EnWG
  - § 1 II Nr. 5 ProdHaftG

- Auswertung
  - keine strafrechtlichen Vorschriften
  - häufig: verwaltungsrechtliche Vorschriften
  - selten: zivilrechtliche Vorschriften

- **Frage: Kann Zivilrecht Anreize für IT-Sicherheit setzen?**

Agenda

I. Überblick

II. Mechanismen zur Regulierung von IT-Sicherheit

III. IT-Sicherheit durch zivilrechtliche Haftung

IV. Lösungsansätze

V. Fazit

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

III. IT-Sicherheit durch zivilrechtliche Haftung

1. Haftungsszenarien

- Rechtsverletzungen durch Nutzer (z.B. WLAN)
- Ausspähen unzureichend gesicherter persönlicher Daten
- Datenverlust durch unzureichende Sicherungsmaßnahmen
- Identitätsdiebstahl durch Missbrauch von Benutzerkonten
- Servermissbrauch zur Versendung von Spam-Mails

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

III. IT-Sicherheit durch zivilrechtliche Haftung

2. Grundlagen zivilrechtlicher Haftung

- Haftung auf Schadensersatz
  - Ziel: Kompensation für erlittene Nachteile
  - Verschuldenshaftung
    - Haftung für Verletzung vertraglicher Pflichten
    - Haftung für Verletzung absoluter Rechte (≠ Vermögen)
      insbesondere: Verkehrssicherungspflichten
    - Haftung für Schutzgesetzverletzung
    - Fahrlässigkeit

      „…wer die im Verkehr erforderliche Sorgfalt außer Acht lässt…“
    - Kausalzusammenhang
  - Haftung für besondere Gefahr (Gefährdungshaftung)
    z.B. Halterhaftung für Kfz, Herstellerhaftung für Produkte

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

III. IT-Sicherheit durch zivilrechtliche Haftung

2. Grundlagen zivilrechtlicher Haftung

- Haftung auf Unterlassen
  - Ziel: Verhinderung künftiger Rechtsverletzungen
  - Grundlage: Vertrag, Verkehrssicherungspflicht, Spezialgesetz
  - Voraussetzung: Drohen zurechenbarer Rechtsverletzung
    - Drohen: Eintritt bei ungehindertem Geschehensablauf
      ggf. Beweiserleichterung bei **Wiederholungsgefahr**
    - Rechtsverletzung: absolute Rechte, auch: Schutzgesetz
    - Zurechenbarkeit: ~ Fahrlässigkeit
  - typischerweise verbunden mit Erstattung von Abmahnkosten

III. IT-Sicherheit durch zivilrechtliche Haftung

3. Persönliche Haftung

- Rückgriffsmöglichkeiten abhängig von der Art der Beschäftigung

- Arbeitsrechtliche Grundsätze (beschränkte Arbeitnehmerhaftung)
  - Regress beim Arbeitsgeber bei leichter Fahrlässigkeit
  - gilt auch für Angestellte im öffentlichen Dienst

- Beamtenrechtliche Grundsätze (Art. 34 S. 2 GG)
  - Rückgriff nur bei Vorsatz und grober Fahrlässigkeit
  - Art. 34 S. 2 GG gilt für Beamte im statusrechtlichen Sinne

- Haftung des Datenschutzbeauftragten – Sonderfall?

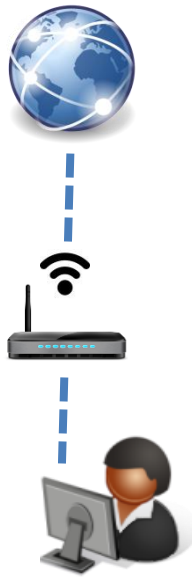
Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

III. IT-Sicherheit durch zivilrechtliche Haftung

4. Szenario: Rechtsverletzung über (Funk-)Netzwerk

- Szenario: Urheberrechtsverletzungen
- Schadensersatzanspruch (§ 97 I, II UrhG)
  - BGH (bisher): keine eigenhändige Tatbegehung
  - Beweisrechtliche Lösung: Vermutung täterschaftlicher Verantwortlichkeit, Entkräftung durch Anschlussinhaber
  - Problem: Haftungsmaßstab / Beweislast unklar



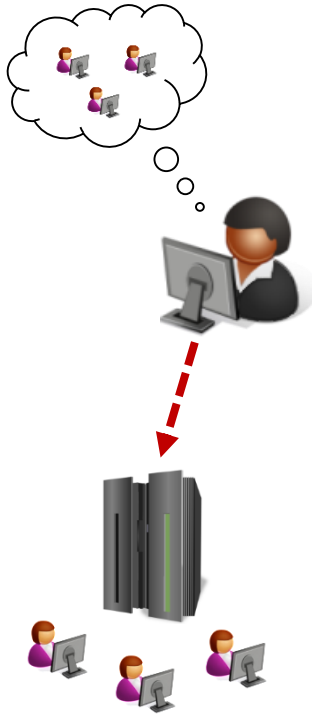
- Unterlassungsanspruch
  - Störerhaftung (§ 1004 I BGB, § 97 UrhG)
  - Zurechenbarkeit: Sicherungspflichtverletzung
    TMG-E: angemessene Sicherungsmaßnahmen + Nutzererklärung
  - Problem: Regelung künftig nur für Funknetzbetreiber

Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

III. IT-Sicherheit durch zivilrechtliche Haftung

5. Szenario: Ausspähen personenbezogener Daten



- Schadensersatzanspruch
  - § 7 BDSG, § 823 II BGB i.V.m. § 9 BDSG
  - Problem: Kenntniserlangung des Betroffenen
  - Problem: Beweislastverteilung
  - Problem: Bezifferung des Schadens

- Unterlassungsanspruch
  - §§ 1004 I 2, 823 II BGB i.V.m. § 9 BDSG (Art. 30 DSGVO)
  - weiteres Problem: Wiederholungsgefahr

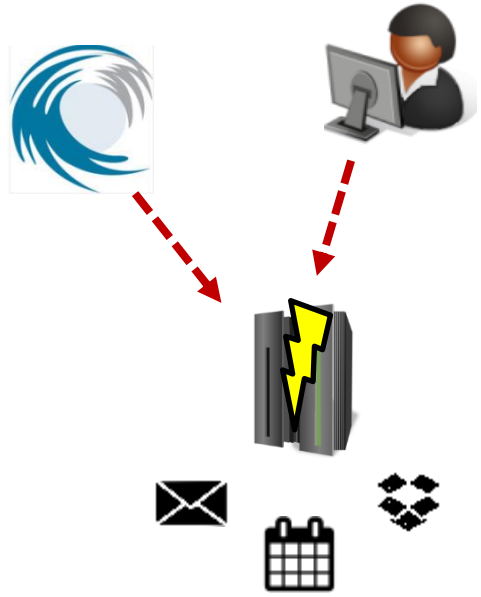
Andreas Sesing
Institut für Rechtsinformatik
Wissenschaftlicher Mitarbeiter

UNIVERSITÄT DES SAARLANDES

III. IT-Sicherheit durch zivilrechtliche Haftung

6. Szenario: Systembeeinträchtigung von außen

- Szenario: Verletzung von Datenintegrität / Datenverfügbarkeit
- Schadensersatzanspruch
  - Vertrag, § 823 I BGB
  - Problem: Daten als Eigentum
  - Problem: Beweislastverteilung
  - § 7 BDSG, § 823 II BGB i.V.m. § 13 VII TMG
  - Problem: Beweislastverteilung
  - Problem: Bezifferung des Schadens



- Unterlassungsanspruch
  - §§ 1004 I 2, 823 II BGB i.V.m. § 13 VII TMG
  - weiteres Problem: Wiederholungsgefahr

Agenda

I. Überblick

II. Mechanismen zur Regulierung von IT-Sicherheit

III. IT-Sicherheit durch zivilrechtliche Haftung

IV. Lösungsansätze

V. Fazit

IV. Lösungsansätze

- Voraussetzungen für wirksame Verhaltensanreize
  - Erkennbarkeit der Haftungsmaßstäbe für Adressaten
  - ausreichende Information der Betroffenen
  - angemessene und klare Beweislastverteilung

- Schutz von Daten
  - Schadensersatzpauschalen im Datenschutzrecht
  - Integritätsschutz von Daten über Personenbezug hinaus

- Grundlagen der Haftung
  - Schadenskollektivierung / Anspruchsbündelung
  - Gefährdungshaftung für Schäden durch Software

Agenda

I. Überblick

II. Mechanismen zur Regulierung von IT-Sicherheit

III. IT-Sicherheit durch zivilrechtliche Haftung

IV. Lösungsansätze

V. Fazit

V. Fazit

- Vorteile zivilrechtlicher Lösung
  - Fahrlässigkeit / Pflichtverletzung → flexibler Haftungsmaßstab
  - schlankere Verwaltung → Minimierung staatlicher Ausgaben

- IT-Sicherheit setzt erkennbaren Haftungsmaßstab voraus

- Lösungsansätze
  - stark kontextabhängig
  - Recht als Instrument zur Verhaltensbeeinflussung
  - interdisziplinärer Austausch für Rahmensetzung unerlässlich

Fragen?

Andreas Sesing
wiss. Mitarbeiter

andreas.sesing@uni-saarland.de