Rechtliche Probleme von Warnungen vor Sicherheitslücken in IT-Produkten durch Behörden

Dr. Alexander Koch
Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

IRNIK
Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Relevante Konstellationen

- Eine Behörde leitet Warnhinweise des Herstellers weiter.
- Eine Behörde warnt die Öffentlichkeit aufgrund eigener Ermittlungen.
- Eine Behörde warnt ausgewählte Unternehmen (z.B. Betreiber kritischer Infrastrukturen).

Mögliche tatsächliche Probleme

- Die Warnung führt zu Umsatzeinbußen bei dem Unternehmen, vor dessen Produkt gewarnt wurde.
- Unternehmen, die nicht gewarnt wurden, fühlen sich benachteiligt.
- Ein Warnhinweis ist falsch und führt zu Schäden.

Rechtliche Probleme

- Grundrechtseingriff durch Warnung.
- Ungleichbehandlung durch Warnung.
- Welche Behörde darf warnen?
  - Problem der Aufgabenzuweisung und Befugnis.
- Staatshaftungsrecht.

Warnung an Nichtjuristen

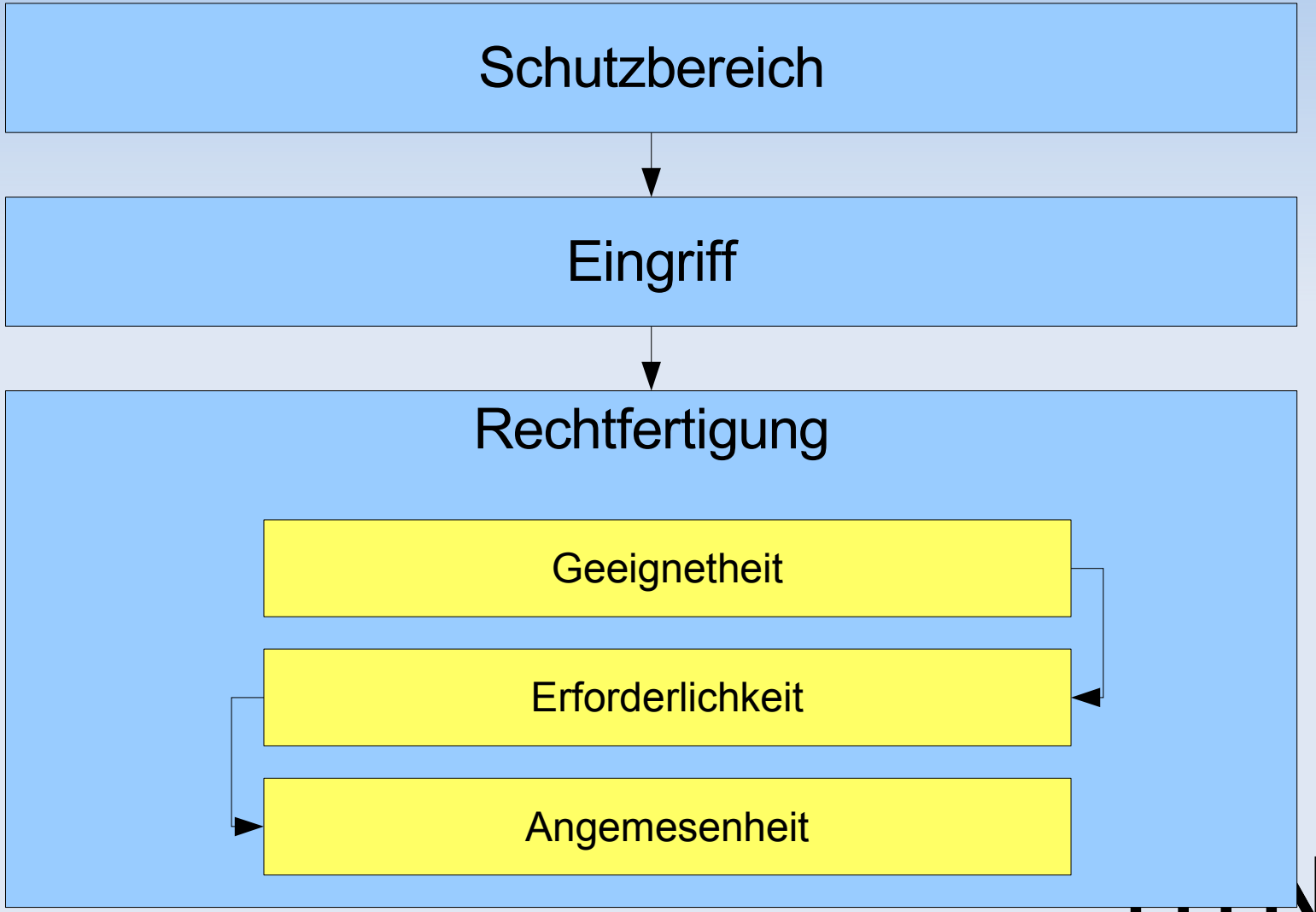
- Es gibt keine juristischen Wahrheiten.
  - „Zwei Juristen, drei Meinungen.“
- Gerichte entscheiden anders als man denkt.
  - „Auf hoher See und vor Gericht ist man in Gottes Hand allein.“
- Juristen legen sich nicht fest.
  - Standardantwort: „Es kommt darauf an.“

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Grundrechtsdogmatik
Eingriff in Freiheitsrecht

- Problemkreis: Produktwarnung.
- Bundesverfassungsgericht thematisiert Eingriff in Berufsfreiheit (Art. 12 GG).
- Warnung vor IT-Produkten ist somit letztlich am Verfassungsrecht zu messen.

Verfassungsrechtliche Rechtfertigung einer Warnung



Schutzbereich Art. 12 Abs. 1 GG

- Wahl und Ausübung eines Berufes.
- Beruf: Jede auf Dauer angelegte und in ideeller oder materieller Hinsicht der Schaffung und Erhaltung einer Lebensgrundlage dienende Tätigkeit.
- Auf das Grundrecht können sich auch Unternehmen berufen.

Schutzbereich

- BVerfG:
  - „Das Grundrecht schützt aber nicht vor der Verbreitung zutreffender und sachlich gehaltener Informationen am Markt ...“
- Literatur
  - Schutzbereich umfasst auch Freiheit vor staatlichen Warnungen.
  - BVerfG vermischt Fragen des Schutzbereichs mit Fragen des Eingriff bzw. der Rechtfertigung.

Eingriff

- Klassischer Eingriffsbegriff
  - Finalität, Unmittelbarkeit, Rechtsförmlichkeit und Verbindlichkeit.
- Moderner Eingriffsbegriff
  - Jedes dem Staat zurechenbare Handeln, das dem Einzelnen ein Verhalten, das in den Schutzbereich eines Grundrechts fällt, ganz oder teilweise unmöglich macht.

Eingriff?

Weiterleitung von Warnungen des Herstellers.

Kein Eingriff ☺

Weiterleitung / Verlinkung von Meldungen einschlägiger Mailinglisten (z.B. bugtraq).

Problem 😐

Verbreitung von selbst erstellten Warnungen.

BVerfG ☺ ./. Literatur ☹

Finanzielle Unterstützung von Sicherheitsforen.

Eingriff ☹

IRNIK

Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Geeignetheit / Erforderlichkeit

- Geeignetheit
  - Kann der Eingriff grundsätzlich ein legitimes Ziel erreichen?
    - Z.B. Warnung zum Schutz vor volkswirtschaftlichen Schäden.
- Erforderlichkeit
  - Gibt es mildere gleich wirksame Mittel?
    - Z.B. Hinweise zum Schließen der Lücke, statt Rat, Programm nicht zu nutzen.

Verhältnismäßigkeit eines Eingriffs in die Berufsausübung

- Grundsätzlich:
  - Jegliche vernünftigen Erwägungen des Gemeinwohls.
- Aber:
  - Auch Eingriffe in die Berufsausübungsfreiheit können massive Folgen – bis hin zur faktischen Unmöglichkeit der Berufsausübung – haben.
  - Deshalb immer Verhältnismäßigkeitsprüfung.

BVerfG zu Produktwarnungen

Staatliche Warnungen müssen immer:

- sachlich, d.h. neutral und objektiv,
- umfassend,
- unter Hinweis auf Unsicherheiten

erfolgen.

Das heißt:

- keine parteiergreifenden oder einseitigen Warnungen.

Probleme (ohne Gewähr ...)

- Warnungen vor einem Hersteller
  - KW-Betriebssysteme sind grundsätzlich unsicher.
    - Nicht objektiv ☹
  - In Hochsicherheitsumgebungen sollten nur nach XY zertifizierte Produkte eingesetzt werden, welche momentan nicht von XY angeboten werden.
    - Objektiv ☺

Probleme (ohne Gewähr ...)

- Warnung vor bestimmten Produkten
  - Der ITE ist grundsätzlich unsicher.
    - Nicht objektiv ☹
  - Vergleiche zwischen dem ITE und MZ zeigen, dass der MZ für unerfahrene Benutzer geeigneter ist.
    - Objektiv ☺

Probleme (ohne Gewähr ...)

- Warnung vor einzelnen Lücken
  - Der ITE sollte nicht genutzt werden, bis die XY-Lücke behoben ist.
    - Problem: Mildere Warnung möglich? 😐
  - Im ITE sollte ActivY deaktiviert werden, bis der Hersteller einen Patch bereitstellt.
    - Verhältnismäßig ☺
  - Der ITE ist anfällig für einen Pufferüberlauf, ein Patch steht unter ... zur Verfügung.
    - Verhältnismäßig ☺
  - Der ITE ist anfällig für einen Pufferüberlauf (der Patch wird verschwiegen).
    - „Mildere“ Warnung möglich! ☹

IRNIK

Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Der Gleichbehandlungsgrundsatz

Verfassungsrechtlich: Art. 3 Abs. 1 GG

(1) Alle Menschen sind vor dem Gesetz gleich.

...

Einfachgesetzlich: § 3 InformationsweiterverwendungsG

(1) Jede Person ist bei der Entscheidung über die Weiterverwendung vorhandener Informationen öffentlicher Stellen, die diese zur Weiterverwendung zur Verfügung gestellt haben, gleich zu behandeln. ...

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Der Gleichbehandlungsgrundsatz

- Gleiches darf nicht willkürlich ungleich,
- Ungleiches darf nicht willkürlich gleich behandelt werden.
- Ungleichbehandlung ist nur beim Vorliegen eines sachlichen Grundes zulässig.
  - Zulässiges Differenzierungsziel.
  - Zulässiges Differenzierungskriterium.
  - Verhältnismäßigkeit.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Differenzierungsziel u. -kriterium

- Zulässiges Differenzierungsziel
  - Schutz kritischer Infrastrukturen.
    - Zulässig ☺
  - Wettbewerbsvorteil für einen ehemaligen Monopolisten.
    - Unzulässig ☹
- Zulässiges Differenzierungskriterium
  - Betreiber kritischer Infrastrukturen.
    - Zulässig ☺
  - Großunternehmen.

    Unzulässig ☹

IRNIK

Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

„Verhältnismäßigkeit“

- Geeignetheit
  - „Ist die ausschließliche Warnung von Betreibern kritischer Infrastrukturen geeignet?“
- Erforderlichkeit
  - „Gibt es eine mildere Alternative zur Diskriminierung?“
    - Sicherheitsüberprüfung aller Interessenten?
- Angemessenheit
  - „Sind Gefahren, die durch eine allgemeine Veröffentlichung drohen, wirklich so groß, dass eine Ungleichbehandlung erfolgen muss?“

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Exkurs: „Gebühren“

§ 4 Abs. 3 IWG

Werden in einer Vereinbarung **Entgelte** für die Weiterverwendung verlangt, **dürfen** die Gesamteinnahmen aus der Bereitstellung von Informationen und der Gestattung ihrer Weiterverwendung **die Kosten** ihrer Erfassung, Erstellung, Reproduktion und Verbreitung zuzüglich einer angemessenen Gewinnspanne **nicht übersteigen.** Die Entgelte sollen für den entsprechenden Abrechnungszeitraum kostenorientiert sein und unter Beachtung der für die betreffenden öffentlichen Stellen geltenden Buchführungsgrundsätze berechnet werden.

Wer darf warnen?

- Warum ist das ein Problem?
  - Grundrechtseingriffe bedürfen einer gesetzlichen Grundlage.
  - Die Verwaltung darf nur handeln, wenn sie vom Gesetzgeber hierzu einen Auftrag erhält.
- Aufgabe und Befugnis
  - Aus einer Aufgabenzuweisung folgt noch nicht die Befugnis, in Grundrechte einzugreifen.

Sachfremdes Beispiel Bundespolizeigesetz

Aufgabe

§ 4 Luftsicherheit

Der Bundespolizei obliegt der **Schutz vor Angriffen** auf die Sicherheit des Luftverkehrs ...

Befugnis

§ 22 Befragung und Auskunftspflicht

(1) Die Bundespolizei kann eine Person **befragen** ... Zum Zwecke der Befragung kann die Person **angehalten** werden. Auf Verlangen hat die Person mitgeführte Ausweispapiere zur Prüfung **auszuhändigen**.

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

Aufgaben des BSI nach dem BSI-Gesetz

BSIG § 3 **Aufgaben** des Bundesamtes

(1) Das Bundesamt hat zur Förderung der Sicherheit in der Informationstechnik folgende Aufgaben:

1. **Untersuchung von Sicherheitsrisiken** bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik, **soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist,**

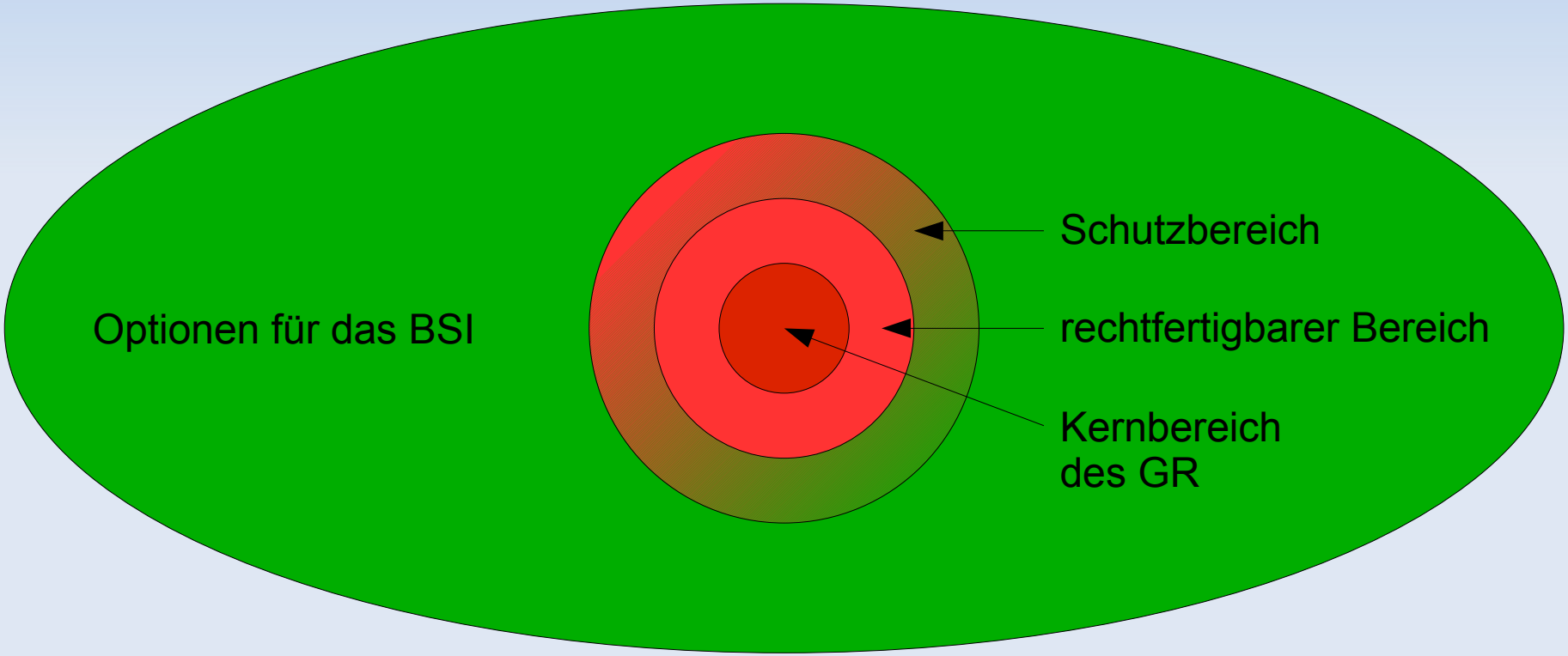
...

7. **Beratung der** Hersteller, Vertreiber und **Anwender in Fragen der Sicherheit in der Informationstechnik** unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen.

Befugnisse des BSI

- Im BSIG sind keine Befugnisse geregelt.
  - (D.h. § 4 BSIG könnte als Befugnisnorm zur Erteilung von Sicherheitszertifikaten gesehen werden – diese sind vorliegend aber irrelevant.)
- Das BSI ist also eine Behörde mit Aufgaben, aber ohne Befugnisse.

Optionen für das BSI im grundrechtlichen Bereich



IRNIK
Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie

Warnung durch Regierung

- BVerfG:
  - Zu den *Aufgaben* der Regierung zählt die Verbreitung von Informationen.
  - ... „staatliche Teilhabe an öffentlicher Kommunikation“, schnelle Reaktion in Krisen, Orientierung für die Bürger.
  - Schluss von der Aufgabe auf die Befugnis?

→ Minister darf in seinem Aufgabenbereich warnen.

Staatshaftungsansprüche

- Konstellationen
  - Schaden des Herstellers durch unrichtige Warnung.
  - Schaden von Anwendern durch Befolgung einer unrichtigen Warnung.
- Anspruchsgrundlage
  - § 839 BGB i.V.m. Art. 34 GG.

StaatshaftungsR

§ 839 BGB

(1) Verletzt ein Beamter vorsätzlich oder fahrlässig die ihm einem Dritten gegenüber obliegende Amtspflicht, so hat er dem Dritten den daraus entstehenden Schaden zu ersetzen. Fällt dem Beamten nur Fahrlässigkeit zur Last, so kann er nur dann in Anspruch genommen werden, wenn der Verletzte nicht auf andere Weise Ersatz zu erlangen vermag.

Art. 34 GG

Verletzt jemand in Ausübung eines ihm anvertrauten öffentlichen Amtes die ihm einem Dritten gegenüber obliegende Amtspflicht, so trifft die Verantwortlichkeit grundsätzlich den Staat oder die Körperschaft, in deren Dienst er steht. ...

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

StaatshafungsR

- Ausübung eines öffentlichen Amtes
  - Beamte
  - sonstige „Beamte im haftungsrechtlichen Sinne“, also auch Angestellte, Beliehene, Verwaltungshelfer.
- Handeln im öffentlich-rechtlichen Bereich
  - Verlautbarung der Behörde.
    - Öffentlich-rechtlich ☹
  - Private Äußerungen außerhalb des Dienstes.
    - Nicht öffentlich-rechtlich ☺

IRNIK
Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie

StaatshaftungsR

- Verletzung einer Amtspflicht.
  - Sorgfältige Prüfung von Warnungen vor Veröffentlichung.
  - Abwägung der widerstreitenden Interessen.
- Drittrichtung der Amtspflicht.
- Vermögensschaden.
- Kausalität.

StaatshaftungsR

- Verschulden
  - Vorsatz und Fahrlässigkeit.
    - ☹ Empfehlung wird nicht sorgfältig getestet.
    - 😐 Meldung wird ungeprüft weitergeleitet.
    - ☺ Problem tritt nur in ganz außergewöhnlichen Konstellationen auf.
  - Maßstab ist „pflichtgetreuer Durchschnittsbeamter“.
    - ☹ Mitarbeiter ist neu und unerfahren.
    - ☺ Problem wäre auch für andere Sicherheitsexperten nicht vorhersehbar gewesen.

Vielen Dank für die Aufmerksamkeit!

Für weitere Informationen:

IRNIK
Dr. Alexander Koch
Postfach 15 01 61
53040 Bonn
Tel.: 02 28 / 8 50 86 63
Fax: 02 28 / 8 50 86 62
ak@irnik.de
http://www.irnik.de

IRNIK

Institut für das Recht der Netzwirtschaften, Informations- und Kommunikationstechnologie