Spannungsfeld:
System- und Datenschutz

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

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

Inhalt des Vortrags

- Abgrenzung Fernmeldegeheimnis / Datenschutzrecht.
- Systematik des Datenschutzrechts:
  - TKG,
  - TMG,
  - BDSG.
- Personenbezug von IP-Adressen.
- Exkurs: Spamtraps und Honeypots.
- Exkurs: Vorratsdatenspeicherung.

Struktur Datenschutzecht

- Person <-> Datum
- Bsp auth.log:
  „Sep 17 13:07:09 alan sshd[...]: (pam_unix) session opened for user koch2“
- koch2 (Person) hat sich am 17.9. um 13:07 auf dem Rechner alan über ssh angemeldet (Datum).

Struktur Fernmeldegeheimnis

- Information, die dem Fernmeldegeheimnis unterliegt.
- KEIN Personenbezug erforderlich (aber nicht schädlich)!
- Bsp (Mailinhalt):
  „... ist das Wetter in Bonn herrlich ...“
- Fernmeldegehemnisrelevanz, obwohl unklar ist, wer mit wem über das Wetter in Bonn kommuniziert.

Quellen des Datenschutzrechts

- Grundgesetz (GG): Recht auf informationelle Selbstbestimmung:
  - BVerfG, Urt. v. 15.12.1983 – Az. 1 BvR 209/83 u.a.
  - Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.
- Bundesdatenschutzgesetz (BDSG).
- Sektorspezifisches Recht:
  - Telekommunikationsgesetz (TKG),
  - Telemediengesetz (TMG).

Personenbezug

- § 3 Abs. 1 BDSG:
  „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“
- Für die Bestimmbarkeit ist auf die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle abzustellen.
  - Personenbezug mit verhältnismäßigem Aufwand herstellbar?

IP-Adressen

- Speichernde Stelle:
  - ISP,
  - Diensteanbieter
- Statische IP-Adressen:
  - Personenbezug nahezu einhellig anerkannt.
  - Warum eigentlich?
- Dynamische IP-Adressen:
  - Personenbezug ist in Wissenschaft und Rechtsprechung heftig umstritten.
  - Spielstand in der Rechtsprechung derzeit 1:1.

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

AG Berlin, Urt. v. 23.11.2006

- Beklagte: Bundesrepublik Deutschland, vertreten durch das Bundesministerium der Justiz.
- Hintergrund: Das BMJ hat im WWW-Log IP-Adressen protokolliert.

Das Urteil im Einzelnen

- IP-Adressen haben immer Personenbezug.
- Gilt auch für dynamische IP-Adressen.
- Bei IP-Adressen ist der Betroffene jedenfalls bestimmbar (praktische Erfahrung ...).
- Hilfsüberlegung: Ohne Personenbezug könnten Daten etwa an Zugangsanbieter weitergegeben werden, die die Zuordnung Nutzer-IP ohne Probleme herstellen könnten.
- Datenschutzrecht soll gerade auch vor Missbrauchskonstellationen schützen.

AG München, Urt. v. 30.9.2008

- Das Gericht stellt in einem obiter dictum fest, dass IP-Adressen *keine* personenbezogenen Daten sind.
  - Allerdings keine Auseinandersetzung mit dem Problemkreis.
- Obergerichtliche Klärung steht nach wie vor aus.

Zwischenstand

- IP-Adressen sollten als personenbezogene Daten behandelt werden.
- Die Speicherung und Nutzung bedarf einer ausdrücklichen gesetzlichen Erlaubnis – oder der Betroffene willigt in die Verarbeitung ausdrücklich ein.

Subsidiarität des BDSG

- § 1 Abs. 3 BDSG.
- TKG und TMG enthalten Regeln für den Umgang mit personenbezogenen Daten.
- BDSG wird im Bereich von Log-Daten weitgehend verdrängt.

Auf Log-Daten anwendbares Recht

- Abgrenzung Telemedien- / Telekommunikationsrecht:
  - § 1 Abs. 1 TMG: TM-Dienste sind elektronische Informations- und Kommunikationsdienste, soweit sie nicht TK-Dienste sind.
  - § 3 Nr. 24 TKG: TK-Dienste sind Dienste, die ganz oder teilweise in der Übertragung von Signalen bestehen.
- Faustformel:
  - TCP, IP (und niedriger): TKG.
  - Anwendungsschicht: TMG.
  - Ausnahmen: E-Mail, VoIP: TKG...

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

TKG-Datenschutzrecht

- Ermächtigung für Eingriffe:
  - § 109 TKG? (-)
    - Schutz von Daten, nicht Eingriff!
  - § 100 Abs. 2 TKG? (-)
    - Zugriff auf Kommunikationsinhalte.
    - Nicht auf IP-Kommunikation übertragbar.
  - § 100 Abs. 3 TKG?
    - Bekämpfung rechtswidriger Inanspruchnahmen.
    - Wohl keine allgemeine Ermächtigung. (-)
  - § 100 Abs. 1 TKG?
    - Schutz von TK-Anlagen. (+)

§ 100 Abs. 1 TKG

- Erkennen, Eingrenzen oder Beseitigen
- von Störungen oder Fehlern
- an TK-Anlagen,
  - also keine Endgeräte!
- Bestands- und Verkehrsdaten.
  - Keine Inhaltsdaten!
- D.h.:
  - Viren- und Spamfilter (?),
  - IDS (-).

Lösung: Einwilligung!

- Problem: Es ist praktisch nur die Einwilligung der eigenen Angestellten, nicht aber deren Kommunikationspartner einholbar.
- Fernmeldegeheimnis ist auf 3-Personen-Verhältnis zugeschnitten.
- Fernmeldegeheimnis gilt nicht zwischen den Kommunikationspartnern.
- Jeder kann (grundsätzlich ...) in die eigene Überwachung einwilligen ...
  - ... und damit indirekt in die seines Kommunikationspartners ...

TM-Datenschutz

- § 12 TMG
  - Personenbezogene Daten dürfen nur erhoben und verwendet werden, soweit das TMG oder eine andere TM-Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat.
- § 15 TMG
  - Personenbezogene Daten dürfen nur erhoben und verwendet werden, um die Inanspruchnahme zu ermöglichen und abzurechnen.

TM-Datenschutz

- § 15 Abs. 8 TMG
  - Bei „zu dokumentierende[n] tatsächliche[n] Anhaltspunkte[n]“ einer unentgeltlichen Nutzung dürfen personenbezogene Daten über das Ende des Nutzungsvorgangs gespeichert werden.
- Eine hierüber hinausgehende Regelung wie § 100 TKG fehlt im TMG!
  - TMG sieht also keine Datenverarbeitung aus Gründen der Systemsicherheit vor.
  - Wurde bereits zu Zeiten des TDG kritisiert.
  - Novelle ist kürzlich erst gescheitert ...

BDSG

- Was bleibt?
  - Dienste, die weder TK noch TM sind!
  - Dienste, die überhaupt nicht angeboten werden: Portscanns!
  - Intern genutzte Dienste (z.B. ssh, Intranet).
- Nutzung:
  - § 28 Abs. 1 Nr. 2 BDSG: Interessenabwägung.

Interessenabwägung

Datenverarbeitung ist zulässig,

Speichernde Stelle:

„soweit es zur Wahrung ***berechtigter Interessen*** der verantwortlichen Stelle ***erforderlich*** ist ...“

Betroffener:

„... und kein Grund zu der Annahme besteht, dass das ***schutz-würdige Interesse*** des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung ***überwiegt*** ...“

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

Exkurs: Honeypots und Spamtraps

- Erheben von Daten?
  - Daten werden „freiwillig“ geliefert.
- TMG?
  - Honeypot, der einen TMD simuliert ist TMD?
  - Drittbezug erforderlich?
- BDSG:
  - § 28 Abs. 1 Nr. 2: Interessenabwägung.

Exkurs: Vorratsdatenspeicherung

- § 113a TKG.
- E-Mail-Anbieter müssen speichern:
  - Absender und Empfänger (Postfach und IP),
  - Zugriffe auf Postfach,
  - Zeitpunkt.
- Internetzugangs-Anbieter müssen speichern:
  - IP-Adresse,
  - Kennung des Teilnehmers,
  - Beginn und Ende.

Vorratsdatenspeicherung

- Vorratsdaten unterliegen einer strengen Zweckbindung.
- Keine Nutzung für eigene Zwecke!
- Ggf. doppelte Log-Dateien!
- ... Verfassungsbeschwerden laufen noch ...

Fazit...

- TK-Bereich: Systemschutz möglich.
- TM-Bereich: Keine Logs für Systemschutz...
- Einwilligung!
- Indirekte Detektion: ungenutzte Ports, Honeypots, Spamtraps.

- ... hoffen auf den neuen Gesetzgeber ...

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

WWW: http://www.irnik.de

IRNIK

Institut für das Recht der Netzwirtschaften,
Informations- und Kommunikationstechnologie