Aktuelle Fragen zu Internetnutzung und Datenschutz

Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz Schleswig-Holstein

Rotary Club Schenefeld

18. Schenefelder Rübenschmaus

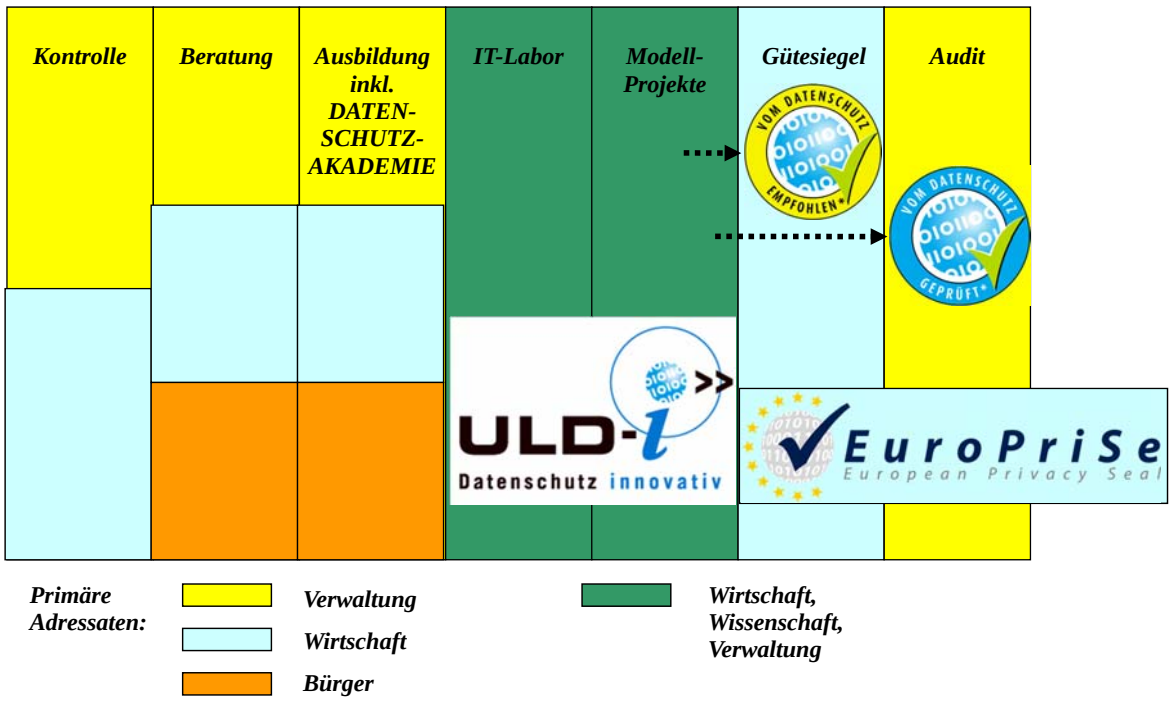
8. November 2011

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Internet
- Datenschutz
- Technische Angriffsmöglichkeiten
- Konkrete Anwendungen
- Staatliche Kontrolle
- Aktuelle Konflikte – u. a. um Facebook
- Lösungen

Unabhängiges Landeszentrum für Datenschutz



Eigenschaften des Netzes

- **Virtualität**
- **Globalität**
- **Universalität** (Konvergenz)
- **Intransparenz**

Netznutzen

Information und Kommunikation

- Verwaltung und Bereitstellung eigener Daten, Bilder, Texte
- E-Mail, Teilnahme an Foren, Austausch mit Behörden und Unternehmen, berufliches Engagement im Netz
- eCommerce, Webshops
- Wikipedia, Blogs
- Demokratischer Austausch, Online-Petitionen
- Soziale Netzwerke
- Informationsportale, Selbstdarstellungen, Veröffentlichungen zu Wissenschaft, Literatur, Kunst ..., örtl. Orientierungshilfen
- Newsportale (Schrift, Ton und Bild)
- Suchmaschinen
- Unterhaltung und Spiele

Netzrisiken

- Ausforschung, Ausspionieren der Privat- und Sozialsphäre
- Anprangerung, Diskreditierung, Rufmord
- Manipulation und Falschinformation
- Belästigung durch Werbung, Spam
- Identitätsdiebstahl
- Internetbetrug
- Abzocke
- Internetabhängigkeit, Netz als Droge (Sex, Glücksspiele, Soziale Netzwerke)

> Nutzen, aber mit Vorsicht

Grundlagen in der Verfassung

- Art. 10 GG Post- und Fernmeldegeheimnis
- Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG allg. Persönlichkeitsrecht

  Recht auf informationelle Selbstbestimmung

  BVerfG: Volkszählung – 1983: Bestimmen, wer was wann weiß

  Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

  BVerfG: Online-Durchsuchung – 2008: digitale Privatsphäre
- Sonstige (digitale) Grundrechte, z.B.
  Art. 13 GG Schutz der Wohnung vor Überwachung
  Art. 4 GG Schutz der Familie vor Fremdbestimmung
- Ebenso: Europäische Grundrechtecharta der EU (seit 2009)

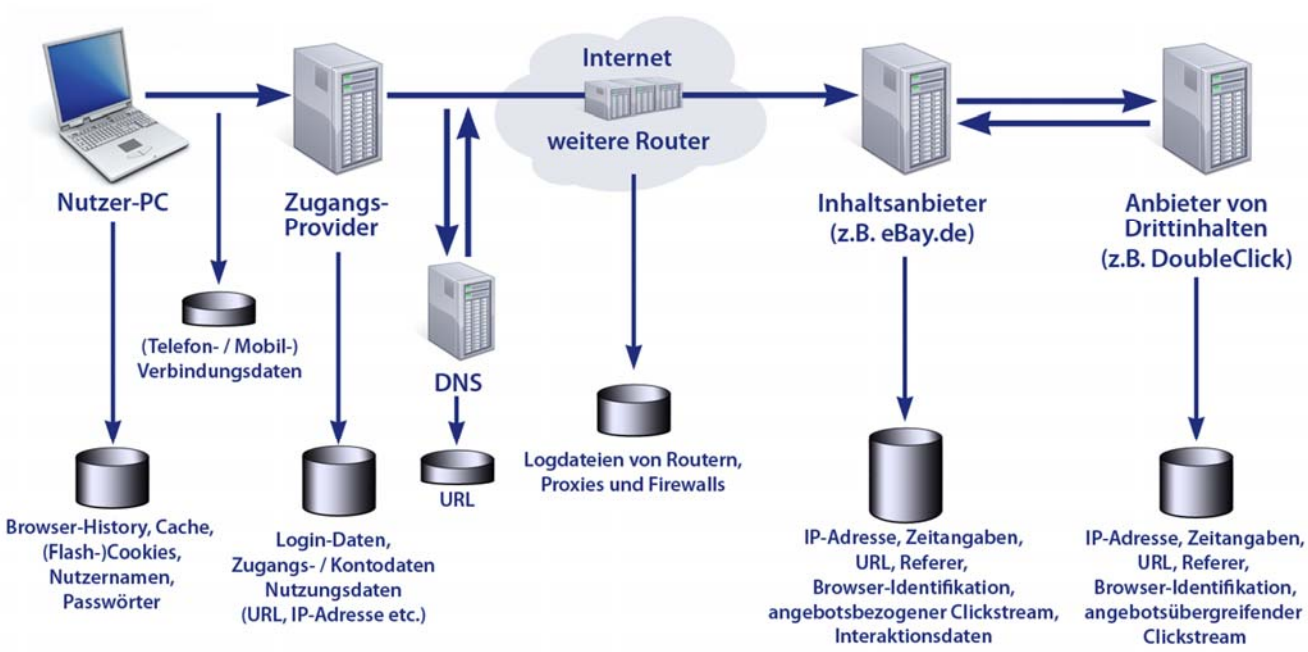
Datenschutzgesetze

- **Bundesdatenschutzgesetz** (BDSG) gilt für alle Inhalte im Internet
- **Telemediengesetz** (TMG) gilt für Nutzungsdaten bei Internetdiensten
- **Telekommunikationsgesetz** (TKG) gilt für Zugangsdienste
- Viele weitere Gesetze, z.B. zum **Verbraucherschutz**, AGB, Fernabsatz, BGB

7 Regeln des Datenschutzes

- Rechtmäßigkeit
- Einwilligung
- Zweckbindung
- Erforderlichkeit und Datensparsamkeit
- Transparenz und Betroffenenrechte
- Datensicherheit
- Kontrolle

Datenspuren bei Internetnutzung



Problem der Verkettung

Zuordnungsmerkmale

- Name, Pseudonyme
- Geburtsdatum, Sozialdaten, persönliche Merkmale
- E-Mail-Adresse, Telefonnummer
- Adresse, Georeferenz
- Ordnungsnummern (z.B. Kundennummer, Kontonummer)
- Cookies, JavaScripts
- Sonstige elektronische Identifikatoren (GUIs - global unique identifier)

Verkettung ermöglicht Erstellung von Persönlichkeitsprofilen (zeit-, raum- und rollenübergreifend)

Auswertung von IP-Adressen

- IP-Adressen ermöglichen (evtl. mit Hilfe des Zugangsdienstes) Identifizierung des Nutzerrechners und räumliche Zuordnung)
- Umsetzung der URL (Uniform Ressource Locator) in „Internet-Adressen“ durch Domain Name Server (DNS)
- Verfolgbarkeit grds. auf gesamter Strecke (evtl. über Ausland; Routing nicht kalkulierbar)
- Zuordnung durch Urheberindustrie zur Sanktionierung von illegalen Up- und Downloads
- IP-Adressen sind verschleier- und fälschbar (Anonymisierungsdienst – z.B. AN.ON)
- Künftig: unbegrenzte Zahl von Adressen über IPv6

Angriffe durch Malware

Viren, Trojaner, Würmer

- ➢ Zerstörung von Datenbeständen (evtl. zeitl. verzögert)
- ➢ Ausforschung von Informationen (PINs, Browser-History, Tastaturbefehle, gespeicherte Texte, Bilder, Dateien)
- ➢ Kapern des Rechners für Bot-Netz-Angriffe
- Kein Herunterladen verdächtiger Angebote
- Kein Öffnen unbekannter Mail-Anhänge
- Geheimhaltung von PINs, sichere Verwahrung von Token
- Einsatz von dauernd aktualisierten Virenscannern
- Einsatz von Firewall (Zulassung nur von definierten Abläufen)

Gefahr des Phishing

- Nachgemachte Seiten animieren zur Preisgabe von PINs, TANs und sensiblen Daten
- Nutzung der Geheimnisse zur Kontoplünderung

Vorkehrungen:

Nutzung Home Banking Computer Interface (HBCI) o. Ä.

achten auf Verschlüsselungszeichen bei https

kein Copy and Paste bei unbekannten Quellen

Vermeiden unbekannter Links

Auswertung durch Diensteanbieter

Prinzip: kostenlose Angebote gegen Daten/Werbeschaltung

Oft: nicht erkennbare Weiterleitung auf andere Seiten (z.B. Facebook-Gefällt-mir-Button)

- Surfverhalten (Tracking)
- Suchprofile (früher Aufbewahrung ohne Frist, jetzt Monate)
- Externe Nutzungsanalyse (Einsatz von Google Analytics mit Übermittlung ins Drittausland)
- Reaktion auf Angebote
- Eingabe in Datenmasken
- E-Mail-Kommunikation

Schutz: Cookie-Löschung, Opt-out, Browser-Konfiguration, Datensparsamkeit

Tracking durch Cookies

- Minidateien auf eigenem Rechner, die Wiedererkennen bei neuem Einloggen erlauben
- Erstellung von pseudonymen Profilen: Surfverhalten, Interessen
- Zuordnungsmöglichkeit bei personalisierten Diensten

> Google kennt jeden

Schutzmöglichkeiten

- Cookies nicht zulassen (evtl. Funktionsbeeinträchtigung)
- Cookies nachträglich löschen
- CookieCooker: Nutzer tauschen Cookies und verwischen so Profile

Web 2.0

- Nutzende erstellen, bearbeiten und verteilen Inhalte selbst
- Wikis, Blogs, Foto- und Videoportale, Soziale Netzwerke, Maps-Dienste
- Das Mitmach-Netz hinterlässt Mitmach-Spuren
- Datenlöschung schwierig bis unmöglich

Maßnahmen:

- Überprüfung der Datenschutzeinstellungen (z.B. Freischaltung von Freunden)
- Keine (kompromittierenden) Daten von Dritten – ohne deren Zustimmung
- Abschottung von Adressverzeichnissen

Kontrolle von Kommunikation

- Datenpakete und deren Inhalt an jedem Router abhörbar (z.B. Kontodaten, Passwörter, PINs)
- Lösung:

Verschlüsselung von E-Mails (z.B. PGP, GnuPG)

Kommunikation mit verschlüsselten Seiten (https, SSL-Verschlüsselung – Secure Socket Layer)

- Identifikation der Kommunikationspartner
- Lösung:

Identitätsmanagement, Nutzung von Pseudonymen

Nutzung von Anonymisierungsdiensten (z.B. AN.ON, TOR)

Smartphones

= Internet-Computer in der Hosentasche

Risiko verlorenes Gerät

- Hüten des Geräts wie Geldbeutel und Schlüsselbund
- Standard: PIN-Schutz
- Sperrung der SIM-Karte
- Verschlüsselung der Speicherungen
- Fernlöschen bzw. Fernsperren

Risiko Lokalisierung

- Ausschalten des Geräts, Ausschalten von GPS

Risiko Malware durch App-Download

- Nutzung nur von geprüften Apps, Information über App im Netz
- Dauernde Sicherheits-Updates
- Prozessmonitore zeigen laufende Anwendung

Nutzung von W-LANs

- Einloggen Dritter, evtl. mit krimineller Absicht bei ungenügender Absicherung

> Gefahr von Schadensersatzansprüchen wg. Urheberrechtsverstößen

> Gefahr von Strafverfolgungsmaßnahmen

- Verschlüsselung der Verbindung zwischen W-LAN-Router und Endgerät
- Gegenseitige Authentisierung von Router und Endgeräten

Staatliche Kontrollen

- Auswertung von Verkehrsdaten (wer, wann, wo, mit wem, was), z. B. auch Funkzellenabfrage
- Vorratsdatenspeicherung wurde ausgesetzt
- Rechner-Beschlagnahme
- Auskunft durch Diensteanbieter (auch USA)
- Verdeckte Ermittlungen im Netz
- Quellen-Telekommunikationsüberwachung
- Online-Durchsuchung

Aktuelle Konflikte

- 2008: Google Analytics und Google Street View
- 2011: Facebook Fanpages und „Gefällt mir“-Button

- Probleme:
- Anbieter in den USA oder im sonstigen Ausland (z. B. Irland)
- Allgemein zugängliche Daten
- Verantwortlich: Nutzer, Webseitenbetreiber, Internetkonzern
- Intransparenz der Datenverarbeitung und der Nutzungsbedingungen
- Fehlende Wahlmöglichkeiten (Opt-in, Opt-out)
- Datenschutzunfreundliche Grundeinstellungen (Social Community, Browser)

ULD-Vorgehen zu Facebook

- 19.08.2011 Veröffentlichung des Arbeitspapiers, Ankündigung des weiteren Vorgehens des ULD
- 07.09.2011 Besuch Facebooks im ULD und im Landtag SH, tags drauf: Treffen zwischen BMI Friedrich und Facebook
- 16.09.2011 Schriftliche ausführliche Reaktion von Facebook
- 28./29.09.2011 Konferenz der Datenschutzbeauftragten
- Gespräche mit DiWiSH und Staatskanzlei
- Anfang Oktober Aufforderung zur Stellungnahme an Fanpage-Betreiber mit Frist Ende des Monats
- 13. und 20.10. Weitere Gespräche mit Facebook
- 24.10.2011 Unterausschuss Neue Medien des Bundestags
- Anfang November erste Sanktionen

Lösungsvorschläge

- Gesetzliche nationale Regelungen (Änderungen des TMG und des BDSG)
- Europäische Regelungen
- Nationale Verhaltensregeln (Codes of Conduct) mit oder ohne Genehmigung durch Aufsichtsbehörden
- Europäische Verhaltensregeln
- Internationale Standards (ISO/IEC)

BITKOM-Kodex

- Positives
- Flexible und anwendungsnahe Regulierung und Umsetzung
- Verantwortung der Branche
- Fragwürdiges
- Weshalb keine Zertifizierung nach § 38a BDSG?
- Weshalb nur und gerade Panoramadienste
- Widerspruch sollte Anbieterübergreifend sein
- Weshalb Zurückbleiben hinter den Street-View-Anforderungen (Vorabwiderspruch, Rohdatenlöschung, Sicherheitskonzept)

Vorschlag „Rote Linien“ § 38b BDSG-E

- Regelt rechtlich Selbstverständliches:
- Verbot schwerer Eingriffe ins Persönlichkeitsrecht (StGB)
- Verbot von Persönlichkeitsprofilen (BVerfG seit 1969, Mikrozensus)

Regelt nicht die wichtigen Fragen:

- Wie halten wir es mit der Meinungs- und Informations-freiheit?
- Ist § 29 BDSG noch anwendbar oder nicht und inwieweit?
- Wie werden internationale Player im europäischen Markt erfasst?
- Wie werden Konflikte geklärt und gelöst?

ULD-Gesetzgebungsvorschläge

- § 1 V BDSG **Zuständigkeit** nach ökonomischen Kriterien
- § 3 IV Nr. 2a BDSG (neu) Begriff „**Veröffentlichen**“
- § 3 VII BDSG **Verantwortlichkeit** nach §§ 7-10 TMG (Kenntniserlangung nötig)
- § 3b BDSG (neu) **Privacy by Default**
- § 4a BDSG Elektronische Einwilligung gem. § 13 II TMG
- § 29a BDSG (neu) Veröffentlichung
- § 38 Ia BDSG (neu) **elektronisches Beschwerdemanagement**
- § 43 BDSG Bußgelder: Verweigerung von elektronischer Antwort und Benachrichtigung

Vorschläge Bundesrat (BT-Drs. 17/6765)

- Änderung des **Telemediengesetzes**

- Informationspflichten bei Datenerhebung (auch über Datenschutzaufsicht, Übermittlung ins Drittausland)
- Sicherstellung technischer Nutzerrechte (Änderung, Löschung, Abschottung, Zweckbegrenzung)
- Einwilligungserfordernis bei Cookies ohne Funktion für Dienst
- Nutzergenerierte Telemediendienste: Privacy by Default, Informationspflichten, Wahlmöglichkeiten, Suchmaschinen-Blocking, Jugendschutz
- Löschpflicht bei nutzergenerierten Inhalten

Aktuelle Fragen zu Internetnutzung und Datenschutz

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
(Independent Centre for Privacy Protection Schleswig-Holstein)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de