Datenschutz und Datensicherheit im Netz

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

Verbraucherschutz-Konferenz 2010

Internet für alle - Senioren sicher online unterwegs

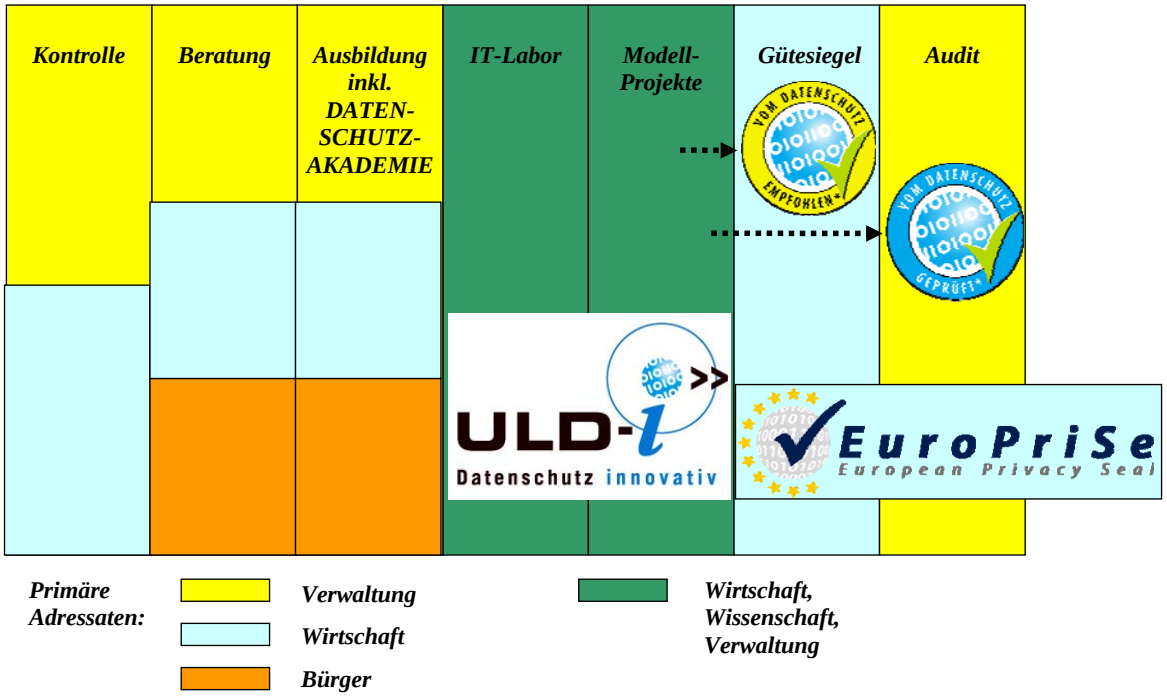
Kiel, 01.10.2010

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Internet
- Datenschutz
- Technische Angriffsmöglichkeiten
- Konkrete Anwendungen
- Staatliche Kontrolle
- Staatliche Hilfen
- Betroffenenrechte

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 (2009)

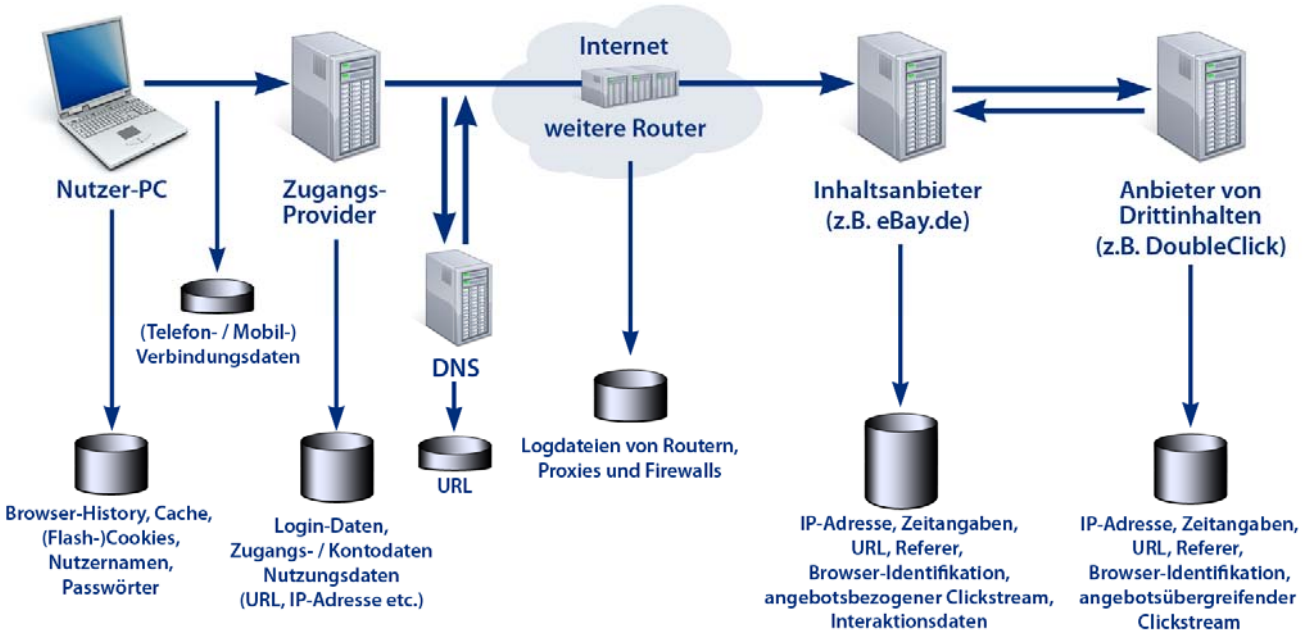
Datenschutzgesetze

- **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)

„Geschwätziger Browser“

U.a. Informationen (30 Felder) über Website, von der man kommt Betriebssystem- und Browserversion, Sprache

GET /datenspuren.html HTTP/1.1
Host: **http://www.datenspuren.de/**
Referer: **http://www.google.de/search?q=Datenspuren**
User-Agent: **Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.0.12) Firefox/3.0.12 (.NET CLR 3.5.30729)**
Accept: **text/html, text/plain, */***
Accept-Language: **de, en-us**

→**Logfile**
Hilfe: Umkonfiguration des Browsers

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)

Angriffe durch Malware

Viren, Trojaner, Würmer

- ➢ Zerstörung von Datenbeständen (evtl. zeitl. verzögert)
- ➢ Ausforschung von Informationen (PINs, Browser-History, Tastaturbefehle, gespeicherte Texte, Bilder, Dateien)
- 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)

Auswertung durch Diensteanbieter

Prinzip: kostenlose Angebote gegen Daten/Werbeschaltung

Oft: nicht erkennbare Weiterleitung auf andere Seiten

- 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

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

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)
- Vorratsdatenspeicherung wurde ausgesetzt
- Rechner-Beschlagnahme
- Auskunft durch Diensteanbieter (auch USA)
- Verdeckte Ermittlungen im Netz
- Online-Durchsuchung

Neuer Personalausweis

Ab 11/2010 obligatorisch, Karte mit geschütztem RFID-Chip

- Elektronische Identifikation (mit Besitz – Karte – und Wissen – PIN) gegenüber Behörden und Unternehmen
- Sichere und datensparsame Kommunikation mit Diensteanbietern (vorab Prüfung d. Datenerforderlichkeit, Entzug bei fehlender Zuverlässigkeit)
- Optional qualifizierte Signatur (sichert Unverfälschtheit von Dokumenten)
- Anonymer Merkmalsnachweis (Alter, Wohnort)
- Nutzung unter Pseudonym (z.B. Online-Dienste)

De-Mail

Ziel: Einfache sichere elektronische Erreichbarkeit mit Zugangsbestätigung

- sichere Absenderidentität (gegen Spam und Phishing)
- digitaler Zugangsnachweis (gem. ZPO, VwVfG)
- sichere Authentisierung (mit Token z.B. nPA od. mobileTAN; Passwort genügt bei Einschreiben nicht, 2 Merkmale)
- elektronisches Postfach

Funktionalitäten: Postfachdienst – Versanddienst, elektronisches Einschreiben – Dokumentensafe – Authentisierungsdienst – evtl. Zusatzdienste der Wettbewerber – Identitätsbestätigung gegenüber Dritten

Betroffenenrechte

- Auskunftsanspruch über eigene Daten
- Anspruch auf Sperrung und Berichtigung bei bestrittenen und falschen Daten
- Anspruch auf Löschung bei unzulässiger Speicherung (auch bzgl. anonymer Blogeinträge od. Forenbeiträge)
- Anspruch auf Schadenersatz (bei materiellen Schäden u. schwerwiegenden Persönlichkeitsbeeinträchtigungen)

Problem der Greifbarkeit bei anonymen Beeinträchtigungen und Hosting außerhalb des EWR

Fremde Hilfen

- Hilfen im Internet (www.datenschutz.de www.datenschutzzentrum.de www.surfer-haben-rechte.de)
- Beschwerden bei Verantwortlichen (siehe Impressum)
- Reputation Defending
- Strafanzeigen bei strafbaren Angriffen
- Verbraucherzentrale bei Verstößen gegen Verbraucherrecht, z.B. Abzocke, übermäßige Datenerhebung, benachteiligende Allgem. Geschäftsbedingungen
- Anrufung der örtlich für verantwortliche Stelle zuständigen Datenschutzaufsichtsbehörde

Datenschutz und Datensicherheit im Netz

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