Nach Snowden: Bedrohungen und Schutz für unsere Daten

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

Lions Club Lübecker Bucht

Timmendorfer Strand

6. November 2013

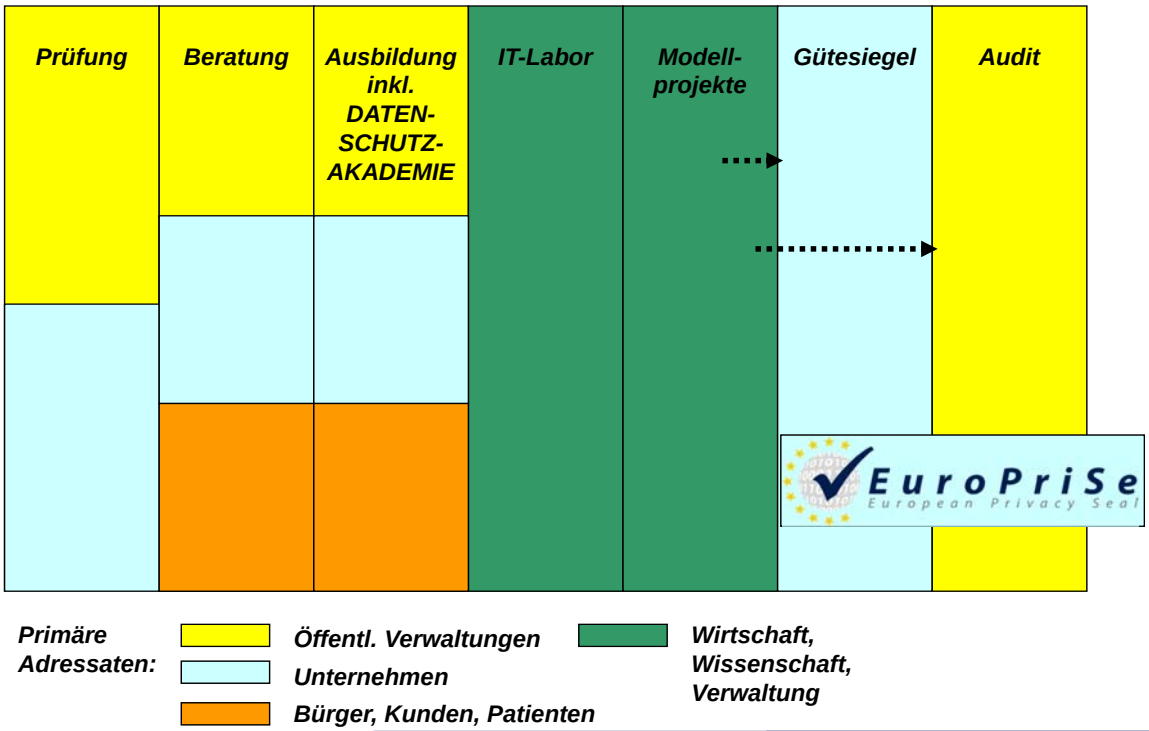
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Datenspuren
- Geheimdienstüberwachung
- Rechtsgrundlagen
- Angriffsarten
- Staatlicher Schutz
- Hilfen im Netz
- Selbstschutz

Kurzvorstellung: Was macht das ULD?

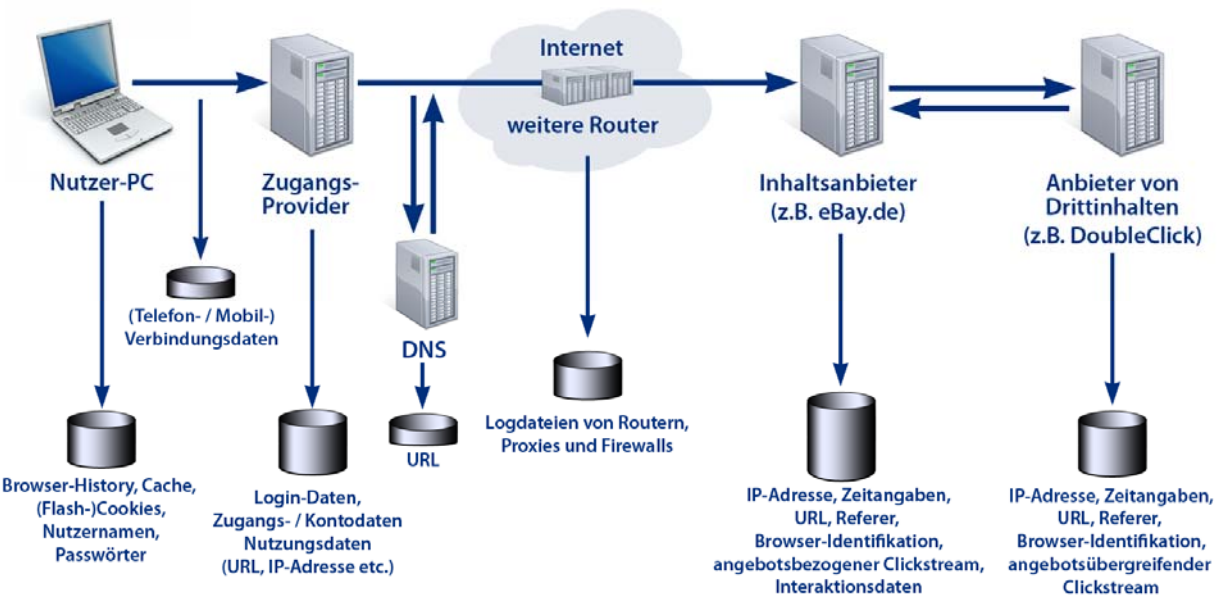
Datenschutz und Informationsfreiheit



Bedrohungen für unsere Daten

- als BürgerIn > Verwaltung (Meldebehörde, Kfz-Zulassungsstelle, Finanzamt, Polizei...), künftig verstärkt eGovernment
- als ArbeitnehmerIn > Arbeitgeber, künftig verstärkt Inanspruchnahme von Cloud-Services
- als VerbraucherIn > Handel, Werbefirmen, Adressenhändler, künftig verstärkt Online-Handel (eCommerce)
- als Einzelperson > Vermieter, Auskunfteien, Vertragspartner (Kundendaten, Videoüberwachung ...)
- als TK-NutzerIn > Netzanbieter (verstärkt Internet)
- als TelemediennutzerIn > von Google, Facebook bis zur eigenen Webseite

Datenspuren im Internet



Gefahrenherde im Internet

Präsenz über Smartphone, Tablet, WLAN, PC, Firmennetz

- Eigene Unachtsamkeit
- Datenlecks von Internetanbieter
- Wirtschaftsspione
- Kriminelle Hacker (Identitätsklau, Kontoplünderung)
- Online-Werbeanbieter (Persönlichkeitsprofile)
- Staatliche Überwachung (z. B. Sicherheitsbehörden, Finanzbehörden)
- Portalanbieter (Apple, Google, Facebook, Amazone, Microsoft)

seit Snowden im Fokus: Geheimdienste

Überwachung durch Geheimdienste

- Anfang Juni 2013: Enthüllungen durch Edward Snowden
  Politische und wirtschaftl. Spionage, Vollüberwachung der Bevölkerung zw. Terrorismusbekämpfung
- National Security Agency (NSA - USA): Prism u. a.
- Government Communications Headquarters (GCHQ – GB): Tempora u. a.
- Bundesnachrichtendienst (BND – D): Strateg. TKÜ u. a.
- Bundesamt für Verfassungsschutz (BfV): Projekt 6 u. a.

> TK-Verkehrsdaten, Zugriff auf Internet (Cloud, soziale Netzwerke), Zugriff auf Internetknoten und -kabel, klassisches Hacking, Entschlüsselung

NSA – National Security Agency

- US-Geheimdienst, seit 1952, zuständig für Auslandsaufklärung im IT-Bereich
- Präsenz in weltweit vielen Staaten, auch Deutschland (Bad Aibling, Darmstadt/Griesheim, Wiesbaden)
- Seit 1960 Einsatz von Spionagesatelliten
- 1990er: Kooperation mit „Five Eyes“ (USA, UK, Ca, Au, Nz), u. a. globales Abhörprogramm Echelon
- Sitz: Fort Mead/Maryland, geplantes RZ: Bluffdale/Utah
- Ca. 40.000 Mitarbeitende, Budget: ca. 10 Mrd US-$/2013
- Ziele: Politik, Wirtschaft, Terrorismus, Bevölkerung
- Juni 2013: Snowden: Spionage und Überwachung, Prism u.a.

Government Communications Headquarters (GCHQ)

- Vorläufer: Communication Electronics Security Group (Enigma-Entschlüsselung im 2. Weltkrieg)
- Sitz: Cheltenham/UK, Gebäudekosten 450 Mio. Euro, Etat (gem. mit MI5 u. MI6): ca. 2 Mrd. Euro/Jahr
- Enge Kooperation und Austausch mit NSA, Horchstationen in anderen Ländern
- Ziele: Beobachtung von Politik, Wirtschaft, Terrorismus, Bevölkerung
- Methoden: jede Form der digitalen Überwachung, u. a. Überseekabel, Netzwerkbeobachung (BelgaCom)

Bundesnachrichtendienst (BND)

- Deutscher Auslandsgeheimdienst (neben BfV, MAD, LäfV)
- Entstand aus „Organisation Gehlen“ (Abteilung Fremde Heere Ost)
- Sitz: Pullach bei München, künftig Berlin, mit Nebenstellen und ca. 100 Auslandsresidenturen
- Ausgaben 2012: 504 Mio. Euro
- Anlassabhängige Ermittlungen („Vorgänge von außen- und sicherheitspolitischer Bedeutung“)
- Strategische Fernmeldeüberwachung (früher Telefonie, heute v. a. Internet), max. 20%, faktisch 1%

Rechtsgrundlagen NSA / GCHQ

USA

- Foreign Intelligence Surveillance Act 1978 – Geheim-gerichtliche (Massen-) Genehmigungen durch FISCourt
- Patriot Act (2001) – Erlaubt Überwachung bei einem für die Sicherheit „erheblichen Zweck“
- 2012/2013 Klagen vor US-Supreme Court erfolglos, weil individuelle Betroffenheit nicht nachgewiesen

United Kingdom

- Regulation of Investigatory Powers Act 2000, ermächtigt 792 Behörden v. Polizei, Militär, Zoll, Gesundheit, Schule, Justiz, Geheimdienste, Sonstige u. 474 Lokalregierungen

Geheimhaltungspflicht aller Beteiligten

Deutsche Rechtsgrundlagen

- § 100a StPO (Strafprozessordnung), Polizeirecht

Mat.rechtl. Anforderungen, Verdacht, Ultima Ratio.
Richtervorbehalt, Benachrichtigungspflicht, Löschung

- BVerfSchG (ebenso Länder), MAD-G, BND-G
- G-10-Gesetz (Telekommunikationsüberwachung)

Parlamentarisches Kontrollgremium, G-10-Kommission

Schutz des Kernbereichs privater Lebensgestaltung

Rechtsschutzmöglichkeit, Verhältnismäßigkeitsprüfung

Europäische Grundrechte-Charta

Art. 7:

Jeder Mensch hat das Recht auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seiner Kommunikation.

Art. 8:

(1) Jeder Mensch hat das Recht auf Schutz der ihn betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Angriffsarten

- Abgreifen von Internetdienstleistern, z. B. Soziale Netzwerke od. Clouds (in den USA, zwangsweise od. freiwillig)
- Verdeckter Zugang zu einem Netzbetreiber (GCHQ-BelgaCom)
- Brechen von Kryptografie
- Verdeckter Zugang zu Internetdiensten (über Backdoors) zur Beschaffung von Meta- und Inhaltsdaten (Adressdaten)
- Abhören von Internetkabeln oder von Internetknoten
- Beschaffung von (evtl. zulässig erlangten Daten von) „befreundeten“ Diensten (z. B. strategische BND-TKÜ)
- Kapern von Rechnern und Rechnernetzen (unterschiedliche Methoden, z. B. Online-Durchsuchung)

Staatlicher Schutz

- Strafrechtliche Regelungen und Ermittlungen
- Datenschutzregelungen und Datenschutzaufsicht
- Hoheitliche Cybersecurity-Strategien (BSI)
- Bereitstellung einer sicheren Infrastruktur (nPA, De-Mail)
- Hilfen zum Selbstschutz (BSI, Surfer haben Rechte)

Hilfen im Netz

- Deutsche/Europäische Webangebote (eCommerce, Soziale Netzwerke)
- Deutsche/Europäische E-Mail-Dienste
- Deutsche/Europäische Speicherdienste (EuroCloud)
- Nutzung von (vertrauenswürdigen) zertifizierten Produkten
- Anonymisierungsdienste (TOR, anonym-surfen.de)
- Blocking-Werkzeuge (Add-Blocker, DoNotTrack)
- Mail-Verschlüsselungstools
- Transparenz-Tools (Ghostery, Collusion, PrivacyBucket)

Selbstschutz I

- Analog statt digital, Datenvermeidung u. - sparsamkeit
- Löschen von Cookies
- Regelmäßige „Reinigung“ des Rechners
- Datenschutzeinstellungen von Browsern, Sozialen Netzwerken, Apps ...
- Vorsicht bei Apps (Lokalisierung, Metadaten)
- Nutzen verschiedener sicherer Passwörter
- Nutzung sicherer Webseiten (insbes. eCommerce: https)
- Offline gehen, Speicherung auf Wechselplatte/USB
- Nutzen von Festplattenverschlüsselung
- Selbstsuche im Netz, Dashboards u. Ä.

Selbstschutz II

- Authentisierung neuer Personalausweis, Nutzung De-Mail
- Nutzung verschiedener Browser, E-Mail-Konten, Einwegadressen, Pseudonyme (ID-Management)
- Nutzen datenschutzfreundlicher Angebote (z. B. anonyme Suchmaschinen ixquick, duckduckgo, blekko, startpage)
- Verschlüsselte Cloud-Dienste
- Meiden US-amerikanischer Dienstleister, Meiden von „Gefällt mir“ u. Ä.
- Anonyme Webseitenanalysen (Piwik statt G. Analytics)
- Notfalls Geltendmachen der gesetzlichen Betroffenenrechte
- Notfalls Anrufung der Aufsichtsbehörde
- Notfalls Reputation Management

Perspektiven

- Europäische Datenschutz-Grundverordnung, Kündigung von Safe Harbor u. A.
- Europäisierung der Internetangebote
- Weiterentwicklung des Selbstschutzangebots, Datenschutz und Datensicherheit als Wettbewerbsfaktor

Einfach mal wieder Offline gehen

Nach Snowden: Bedrohungen und Schutz für unsere Daten

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