Die Antwort Europas auf die US-amerikanische Missachtung des Datenschutzes

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

DiWiSH-Fachgruppe IT-Security
IHK Kiel
29. Oktober 2014

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Angriffe durch NSA & Co.
- Datenschutz in den USA?
- Europäischer Grundrechtsschutz
- Transatlantische Reibungspunkte
- Nationale Maßnahmen
- Selbstschutz
- Europäische Reaktionen

Überwachung durch Geheimdienste

Seit Anfang Juni 2013: Enthüllungen durch Edward Snowden

- National Security Agency (NSA - USA): Prism u. a.
- Government Communications Headquarters (GCHQ – GB): Tempora u. a.
- Direction Générale de la Securité Extérieure (DGSE – F)
- Bundesnachrichtendienst (BND – D): Strateg. TKÜ u. a.
- Weitere Five Eyes (Kanada, Australien, Neuseeland)
- Spionage aus China, Russland...

> Politische Spionage, Wirtschaftsspionage, allgem. Netzüberwachung

Legitimation: Terrorismusbekämpfung

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 (z. B. Adressbücher)
- 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)
- Verdeckte technische und personale Ermittlungen
- Sammeln und Auswerten „öffentlicher Quellen“ (im Netz)

sonstige Risiken und Hilfen

- Unternehmens-Wirtschaftsspionage
- Kriminelle Hacker – Abzocke, Sabotage
- Innentäter

- Spionageabwehr: Aufgabe der Ämter für Verfassungsschutz
- Informationssicherheit: Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Cyber-Strafverfolgung, Gefahrenabwehr: Bundeskriminal-amt, LKÄ, Europol, Staatsanwaltschaften
- Datenschutz: Aufsichtsbehörden, z. B. ULD (Kunden, Beschäftigte)

Bewusster Grundrechtsverzicht in USA

- Keine digitalen Grundrechte (schon gar nicht für Ausländer)
- US-Supreme Court: Reasonable Expectations of Privacy
- Vorrang der Sicherheitsbelange
- Keine (gesetzliche) Bindung von Privaten

1890 - Warren/Brandeis: „Right to Privacy“

1967 - Westin: „Privacy and Freedom“

Seitdem keine rechtsstaatliche Weiterentwicklung trotz verfassungsrechtlicher Grundlagen in Amendments

> Sicherung der globalen Sicherheitshegemonie

> Sicherung der globalen wirtschaftlichen Hegemonie

USA zwingt zur Datenherausgabe

US-Bundesgericht: Microsoft muss Ermittlern Daten aus Europa bereitstellen

Das Urteil von Ende Juli 2014 besagt, dass der Softwarekonzern Microsoft Ermittlern auch dann Daten herausgeben muss, wenn diese auf Servern innerhalb von Europa liegen. Microsoft will den US-Gerichtsentscheid anfechten.

- **Patriot Act**
- **FISA** (Foreign Intelligence Surveillance Act)
- **Weitere Rechtsgrundlagen**

Siehe Positionspapier des ULD 2011:

https://www.datenschutzzentrum.de/internationales/20111115-patriot-act.html

Problemlagen für deutsche Unternehmen

Nutzung

- US-amerikanischer Clouds (z. B. auch Microsoft Office 365, Amazon, Salesforce)
- US-amerikanischer sozialer Netzwerke (Facebook, Twitter, LinkedIn, Google+)
- US-amerikanischer Soft- und Hardware (iOS, Windows, Android)
- US-amerikanischer Internet-Anwendungen (Analytics, Likes, Google Docs ...)

Probleme mit südkoreanischen und chinesischen Anbietern sind bisher noch nicht vertieft untersucht

Europäischer Grundrechtsstandard I

Datenschutz:

- Seit 70er gesetzliche Regelungen
- 1980 OECD Datenschutz-Leitlinien zur Verhinderung von Handelshemmnissen
- 1981 Europarat Datenschutzkonvention
- 1983 deutsches BVerfG: Datenschutz erhält Grundrechtsstatus
- 1995 Europäische Datenschutz-Richtlinie
- 2008 deutsches BVerfG: Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme
- 2009 Art. 8 EUGR-Charta: Grundrecht auf Datenschutz

Europäischer Grundrechtsstandard II

- Digitale Meinungsfreiheit
- Kommunikationsfreiheit
- Informationsfreiheit (Zugang zu Verwaltungsinformationen, seit 2013 gem. EGMR auf Art. 10 EMRK mit Grundrechtsstatus)
- Digitale Versammlungsfreiheit
- Eigentumsrecht (Betriebs- und Geschäftsgeheimnisse)
- Petitionsrecht
- Digitale Komponente der analogen Freiheit (Religion, Familie, Beruf, Wohnung, Freizügigkeit ...)
- Gleichbehandlung (Diskriminierungsverbot wg. Geschlecht, Abstammung, Herkunft, Glauben ...)

Politische Kooperationsverträge

- Safe Harbor (2000)
- Passenger Name Records (PNR)
- Terrorist Finance Tracking Program (SWIFT, Analyse internationaler Banktransaktionen)
- Künftig Transatlantic Trade and Investment Partnership (TTIP – Freihandelsabkommen)?

Gegenstrategien

- No-Spy-Abkommen (gescheitert)
- Politische Aufarbeitung (NSA-Untersuchungsausschuss)
- UNO-Resolution 26.11.2013: Art. 12 Allgem. Erkl. der Menschenrechte, Art. 17 Int. Pakt für ziv. u. pol. Rechte: „Schutz der Privatheit im digitalen Zeitalter“ = Schutz vor „massenhafter Überwachung, Abhören und Sammeln persönlicher Daten“
- Schengen-Routing, Hochseekabel Europa-Brasilien
- Juristische Aufarbeitung d. NSA/GCHQ-Rechtsverletzungen (nationale strafrechtliche Verfolgung, Klagen vor EuGH, EGMR)
- Schnelle Verabschiedung der Europäischen Datenschutz-Grundverordnung (Marktortprinzip, europaweiter effektiver Rechtsschutz gegen US-Unternehmen)

Denkbare weitere Maßnahmen

- Diplomatische Sanktionen
- Schutz durch Aufenthalt für Edward Snowden
- Internationaler Schutz von Whistleblower
- Aktualisierung der eigenen Geheimdienstgesetze
- Kündigung der Kooperationsabkommen mit USA über Roadmaps (Safe Harbor, PNR, SWIFT ...)
- Aussetzung d. Verhandlungen zum Freihandelsabkommen

Schwarz-roter Koalitionsvertrag 2013

- Bündelung der IT-Netze in einer einheitliche Plattform
- Verstärke Standardisierungsarbeit
- Zertifizierung von Cloud-Infrastrukturen
- Ausbau Kryptografie
- Ende-zu-Ende-Verschlüsselung bei De-Mail
- Integration „Stiftung Datenschutz“ in „Stiftung Warentest“
- Privacy by Design, Privacy by Default
- EU-Datenschutzgrundverordnung
- Datenschutzabkommen mit den USA
- Neuverhandlung von Safe Harbor, SWIFT, PNR-Abkommen

Digitale Agenda August 2014

Inhalte u.a. Schaffung digitaler Infrastrukturen, Innovationsförderung, Vermittlung von Medienkompetenz und Wissenschaftsförderung

Kapitel VI Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft

- Förderung einfacher Sicherheitstechniken
- Weiterentwicklung und Angebot vertrauenswürdiger Hard- und Software
- Schaffung sicherer IT-Infrastrukturen (nPA, De-Mail, „Verschlüsselungsstandort Nr. 1 auf der Welt“
- Förderung von datenschutzfreundlichen Geschäftsmodellen
- Moderner Datenschutz in Europa und „führende Rolle bei der Entwicklung internationaler Datenschutzprinzipien“
- „einer der sichersten digitalen Standorte weltweit“
- IT-Sicherheitsgesetz

Unternehmensdilemma

- Schaden durch Cyber-Kriminelle contra Image-Schaden durch Veröffentlichung des Datenlecks
- Kostenfolgenabschätzung wichtiger als Compliance
- Vorrang sollte Kundenvertrauen durch Transparenz haben (Beispiele: Telekom)

Entwurf IT-Sicherheitsgesetz (08/2014)

- Meldepflicht bei Betreibern kritischer IT-Infrastrukturen und Telekommunikationsprovidern
- Informationssammlung und –auswertung durch das Bundesamt in der Informationstechnik (BSI)
- Erstellung von Lagebildern
- Zuverlässigkeitsüberprüfung von TK-Anlagenbetreibern
- Erhöhte Sicherheit der Bundesverwaltungs-IT
- Zuständigkeitskonzentration des Bundeskriminalamtes (BKA) für Cyberkriminalität
- Verpflichtung ausgewählter Stellen zu Maßnahmen des Risikomanagements

Technische Datenschutz-Ziele

Technisch-organisatorische Maßnahmen der Datensicherheit intern und im offenen Netz (§ 9)

- **Vertraulichkeit** (z.B. Verschlüsselung)
- **Integrität**, Authentizität (Backup, digitale Signatur)
- **Verfügbarkeit** (ausfallsichere Stromversorgung, Datenmanagement)
- **Intervenierbarkeit** (Löschen, Sperren, Beauskunften)
- **Unverknüpfbarkeit** (Abschottung)
- **Transparenz**,Revisionsfähigkeit (Protokollierung, Kontrolle der SysAdmin, Dokumentation, Anwenderhandbücher, Information bei Erhebung, Benachrichtigung bei Bearbeitung)

Datenschutzmanagement

verpflichtend

- Betrieblicher Datenschutzbeauftragter (§§ 4f, 4g: ab 9 Personen in ADV, sonst ab 20 Personen)
- Vorabkontrolle (§ 4d V)
- Verfahrensverzeichnis (§§ 4d, 4e)
- Verpflichtung auf das Datengeheimnis (§ 5)

zu empfehlen

- Datenschutzkonzept
- IT-Sicherheitskonzept
- Konzept bei IT-Einführungen (incl. Betriebsrat)
- Ausbildungskonzept
- Beschwerdemanagement (Betroffeneneingaben)
- Durchführung von Audits

Konkrete Beispiele

- Eigene soziale Kommunikation (kein Facebook od. Google+)
- Nutzen anonymer Suchmaschinen (z. B. Ixquick)
- Nutzung von Anonymisierungsdiensten (Tor, JonDos)
- Eigene IT oder Trusted Cloud (Schengen-Anbieter, Zertifizierung), Kontrolle Auftragsdatenverarbeiter
- Nutzung sichere Infrastrukturen (nPA, De-Mail)
- Internes Netz als VPN
- Externe Kommunikation mit Verschlüsselungsangebot (PGP, GnuPG)
- Klare Trennung beruflich-privat (z. B. bei BYOD)

Europäischer Gerichtshof (EuGH)

Urteil v. 08.04.2014 (TK-Vorratsdatenspeicherung)

- Vorratserhebung schränkt Freiheitsrechte stark ein und setzt hohe materielle und prozedurale Hindernisse voraus
- Keine Garantie, dass Datenverarbeitung nur in Europa

Urteil v. 13.05.2014 (Google Suche Spanien)

- Es gilt das Marktortprinzip > nationales Datenschutzrecht ist anwendbar (A. M. bisher OVG Schleswig-Holstein)
- US-Unternehmen haben datenschutzrechtliche Verantwortlichkeit
- Betroffene haben Abwehranspruch gegen US-Anbieter

Vorlagebeschluss Irish High Court v. 18.06.2014 (Facebook)

- Safe Harbor verstößt gegen Grundrechte?

Europäische Datenschutz-Grundverordnung I

Zeitplan

- Januar 2012 Vorschlag Kommission
- März 2014 Beschluss 1. Lesung Europaparlament
- Derzeit: Ratsstellungnahme
- Dann: Trilaterale Gespräche

Ziele

- Ausrichtung auf Online-Datenverarbeitung
- Harmonisierung – Vereinheitlichung
- Möglichst hohe Standards

Europäische Datenschutz-Grundverordnung II

- Marktortsprinzip
- Allgemeine Erlaubnistatbestände, Grundregeln
- Sonderschutzregelungen für Kinder und Jugendliche
- Transparenzregelungen
- Recht auf Vergessenwerden
- Recht auf Portabilität (Datenübertragbarkeit)
- Beschränkung von Tracken, Scoren und Profilen
- Privacy by Design und Privacy by Default
- Breach Notification, massive Sanktionen
- Klagemöglichkeit auch für Verbände
- Koordination der Datenschutzkontrolle

Generelle Schlussfolgerungen

- Deutsch-Europäisches Selbstbewusstsein statt US-Hörigkeit
- Kein Sparen bei IT-Sicherheit und Datenschutz
- „Security“ durch Transparenz, nicht „by Obscurity“
- Kommunikative besser als individuelle Lösungen

Die Antwort Europas auf die US-amerikanische Missachtung des Datenschutzes

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