Berichte und Thesen aus den Infobörsen

Sommerakademie 2014

„Supergrundrecht Sicherheit“
contra
digitale Menschenrechte

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Datenschutz im Vergleich: USA – Europa

Zentrale Frage: Wie sieht eine transatlantische Reformagenda zum Schutz digitaler Grundrechte aus?

1. Schritt: Nationalstaatliche Reformen
- Rechtliche Grundlagen für nachrichtendienstliche Überwachung
- Interpretation und Auslegung des Rechtsrahmens
- Kontrolle der Nachrichtendienste

2. Schritt: Entwicklung internationaler Standards
- Rechtsschutz von Ausländern
- Standards für den Zugriff auf Daten von Internetdienstleistern im transnationalen Raum
- Regeln für internationale Kooperation zwischen Nachrichtendiensten

Der NSA-Untersuchungsausschuss

- **Untersuchungsauftrag**
  - Massenüberwachung durch Five Eyes
  - Ringtauschthese/Beteiligung deutscher Dienste
  - IT-technische Schutzmaßnahmen
- **Rechtliche Möglichkeiten eines Untersuchungsausschusses**
  - Antrag eines Viertels der Mitglieder des Bundestags
  - Erhebung von Beweisen
  - Verwaltungsbehörden sind zur Amtshilfe verpflichtet.
- **Kontrolle der Geheimdienste**
  - regierungsintern
  - Kontrolle durch Gerichte
  - Parlamentarische Gremien
- **Ausblick**

Zusammenspiel von Datenschutz und Informationssicherheit

- Zusammenstellung der zahlreichen rechtlichen Festlegungen zur Implementierung von technischen Datenschutzmaßnahmen (z. B. BDSG, EU-DSRL, EU-DSGVO-E, PAuswG, De-Mail-G)
- Darstellung (klassischer) IT-Sicherheitsmaßnahmen für die Umsetzung von technischen Datenschutzmaßnahmen (Kryptographie, PKI, Mehrfaktor-Authentisierung, Security-by-Design)
- Beispiele für Zusammenarbeit mit der BfDI/den LfDs:
  - ePA, De-Mail
  - elektronische Bildübermittlung (Pass) mit De-Mail
  - Sichere elektronische Identitäten: eID-Strategie
    - Definition von Vertrauensniveaus nach BSI TR-03107
    - Elektronischer Schriftformersatz jenseits der QES
    - Zusammenarbeit bei Bürgerkonten

Datenerhebung durch polizeiliche Ermittlungsbehörden bei Internet-Diensteanbietern

- Nutzungsdaten besitzen hohen Informationsgehalt über Interessen und Nutzungsgewohnheiten. Sie erlauben die Erstellung von (partiellen) Persönlichkeitsprofilen.
- Nutzungsdaten unterliegen wegen der Sensibilität dem Fernmeldegeheimnis und damit einem besonderen rechtlichen Schutz.
- Das Telemediengesetz enthält nur eine Übermittlungsberechtigung für Diensteanbieter – Befugnisse für Anordnungen richten sich nach den Empfängern.
- Zum Zweck der Strafverfolgung fehlt, anders als bei Geheimdiensten oder im Hinblick auf TK-Daten, eine bereichsspezifische Anordnungsnorm.

Private – riskante IT-Dienstleister bei Behörden

- Gesetzgeberische Initiative zur Auftrags-DV nötig
  - Auftragsdatenverarbeitung ist Chance und Risiko für den Datenschutz
  - Auftraggeber muss Kontrolle und Sicherheit auch beim Auftragnehmer umfassend gewährleisten können – gerade bei Wahl von Anbieter in Drittstaaten
- EU-Gesetzgeber gefordert bei Auftragnehmern Drittstaaten
  - Verhinderung staatlicher Zugriffe
  - Transatlantische Handelsabkommen gefährden Datenschutz und Bürgerrechte

Spionage-Abwehr und Wirtschaftsschutz in Schleswig-Holstein

- Auch kleine und mittlere Unternehmen aus Schleswig-Holstein sind Ziel von Wirtschaftsspionage
- Verfassungsschutz ist zuständig und hilft auch vertraulich mit Beratungsangeboten, Prävention und nach Vorfällen
- Mithilfe durch Meldung von Vorfällen nötig, um mehr über Täter und deren Vorgehen zu erfahren und dadurch für alle bessere Prävention zu gewährleisten
- Maßnahmen gegen Spionage können auch wertvolle Argumentationshilfe für betriebliche DSB sein

Verschlüsselung heute

- Nachrichtendienste haben Zugriff auf Daten aller anderen Organisationen
- Sie können sich dem Zugriff der Judikative und Legislative entziehen
- Hersteller zentraler IT-Komponenten integrieren letztlich nicht prüfbar beliebige Funktionen in Hardware und Software
- Social-Web-Betreiber, Banken und Versicherungen lassen sich durch Einwilligungen „gedeckt“ beliebigen Zugriff auf personenbezogene Daten einräumen
- Verschlüsselung bedeutet, die Kenntnisnahme von Daten gemäß dem erforderlichen Sicherheitsniveau zu erschweren
- Neue Nutzungsmodelle (Mehrgeräte-Nutzung etc.) erschweren durchgängige Verschlüsselung

Sicherheit und Datenschutz in mobilen Endgeräten

- Mobile Endgeräte sind besonders lohnende Datenquellen
- Kein mobiles Betriebssystem wird aktuellen Datenschutzvorgaben gerecht
- iOS, Android und Windows Phone 8 bieten unterschiedliche Stärken und Schwächen
- Alternative Systeme mit Privatsphäre-Fokus sind im Entstehen
- Wearables bringen ganz neue und potenzieren bestehende Herausforderungen
- Europa ist derzeit kein Gestalter im Bereich Datenschutz und mobile Endgeräte

Big Data bei der Polizei

- Potentielle Anwendungsfelder: strategische und operative Auswertungen
- Keine Rechtsgrundlage im geltenden Recht für personenbezogene polizeiliche Auswertungen unstrukturierter Massendaten
- Grenzen für den Gesetzgeber:
  - Grundsatz der Zweckbindung als Kernelement informationeller Selbstbestimmung
  - Relevanzschwelle für die Einbeziehung von personenbezogenen Daten in Auswertungen
  - Schutz der Betroffenen vor Anwendung statistischer Werte auf Einzelne als Grundlage für staatliche Eingriffe

Bürgerrechtsschutz durch Whistleblowing – nicht nur bei Snowden

- Bedeutung von und Risiken für Whistleblower
  - Transparenz, Korruptionsbekämpfung, öffentliche Debatte u.a.
  - Bedrohung v. Leib/Leben, Freiheit, Kündigung, gesellschaftliche Exklusion u.a.
- Unzureichende gesetzliche Regelungen in Deutschland
- Anforderungen an ein nationales deutsches Gesetz zur Förderung und zum Schutz von Whistleblowern: Regelung v. sachlich./persönlich. Anwendungsbereich, Beweislastverteilung, Schutzvorschriften, externes Whistleblowing
- Anforderungen an den Einzelnen und an die Gesellschaft gegenüber Whistleblowing im öffentlichen Interesse (Akzeptanz in der Gesellschaft, Überwindung der vorhandenen negativen Assoziationen)