Berichte und Thesen aus den Infobörsen

Sommerakademie 2015

„Vertrauenswürdige IT-Infrastruktur – ein (un?)erreichbares Datenschutziel“

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Sicher verschlüsseln mit GnuPG (Gnu Privacy Guard)

- Ausgehend vom Schutzbedarf für die personenbezogenen Daten ist Verschlüsselungstechnik einzusetzen (Anlage zu § 9 Satz 1 BDSG, Satz 3; § 6 Abs. 3 LDSG).
- Vertraulichkeit und Integrität von Informationen können mittels Verschlüsselung gewährleistet werden.
- GnuPG ist eine quelloffene Software, die für zahlreiche Betriebssysteme verwendbar ist.
- Mit GnuPG wird der OpenPGP-Standard implementiert.
- Es kommt eine starke Verschlüsselung zur Anwendung.
- Es gibt eine Vielzahl von Frontends und Plug-ins für Mail-Clients, die auf GnuPG aufsetzen.
- GnuPG ist kostenfrei nutzbar.
- Die Datenschutzaufsichtsbehörden in Deutschland nutzen GnuPG.

Vertrauensfrage: Warum mobile IT in Behörden und Unternehmen so problematisch ist

- Der Rechtsrahmen zur Nutzung mobiler IT ist unzureichend/veraltet.
- Klassische PCs stehen weitgehend unter der Kontrolle des Nutzers bzw. der Administration.
- Mobile IT verlagert die Kontrolle auf den Hersteller der Maschine.
- Wir diskutierten vier Vertrauensstufen:
  1. Anwendung wie ein Privatnutzer
  2. Managed Device/Bring your own device
  3. Container-Lösungen
  4. Verzicht auf Einsatz
- Empfehlungen zum Einsatz mobiler IT:
  1. Schutzniveauprüfung nach Standard-Datenschutzmodell
  2. Regelung in Betriebs- oder Dienstvereinbarung
  3. Gütesiegel
  4. Orientierungshilfen

Instrumente des BSI für vertrauenswürdige Infrastrukturen

- Vertrauenswürdigkeit basiert auf Transparenz, Unabhängigkeit und Objektivität
  - BSI stellt vertrauenswürdige IT bereit mittels
    - Zertifizierung
    - Kooperation mit Wirtschaft, Verwaltung, Justiz
- Standardisierung ist wesentliches Instrument für Herstellung von Vertrauenswürdigkeit
  - Einheitliche Vorgaben erhöhen allgemein IT-Sicherheit
  - Einhalten rechtlicher Anforderungen
  - Berücksichtigung der Markterfordernisse

Elektronische Gesundheitskarte (eGK) und Telematik-Infrastruktur (TI)

- Wenn eGK ab 2016 online geht, müssen diverse Probleme gelöst sein.
  - PIN-Problem: Patient müsste sich bis zu 8 PINs merken und beim Arztbesuch eingeben – nicht praktikabel!
  - Bestandsnetze: Bestehende Online-Anbindungen der Praxen müssen mit TI integriert werden.
  - Versichertenrechte: Datenzugriff erfordert PIN des Patienten und einen Heilberufeausweis – wie kann dann der Patient allein seine Rechte wahrnehmen? Kiosk?

- Fazit: Es gilt, offene Baustellen anzugehen, ohne dabei lebensfremde Forderungen zu stellen.

Datenschutz-Folgenabschätzung
Methode zur Vertrauensbildung

- Impact-Assessments: Risiko-Betrachtungen + Konzepte

- Unterschiede zwischen „Privacy-Impact-Assessment“ (PIA) und „Data-Protection-Impact-Assessment“ (DPIA)
- Orientierung an Privatheit bzw. Grundrechten
- DPIA: Organisation als „Angreifer“
- DPIA: Erhöhung des Schutzbedarfs, falls externe Mechanismen (z. B. Datenschutzrecht, Vollzug) versagen

- Grundzüge des Standard-Datenschutzmodells (SDM) als Operationalisierung datenschutzrechtlicher Anforderungen

- PIA + SDM = DPIA

Datenschutzrechtliche Anforderungen an schulische IT-Infrastrukturen

- Themenblöcke:
  - Schulverwaltung
  - Pädagogisches Netz
  - WLAN und Internetzugang
- Große Bandbreite an Anforderungen und Lösungen („von einzügiger Grundschule bis RBZ“)
- Nur zentrale Lösungen für alle genannten Punkte sind datenschutzrechtlich gesehen sinnvoll („einer für alle“, „einmal und dann gut“)

Das IT-Sicherheitsgesetz und die Praxis: Ziele und Wirkung

- Kritik am IT-Sicherheitsgesetz
  - Befugnis zur Speicherung von IP-Adressen für TK-Dienste wesentlich weiter als nötig
  - Für Telemedien fehlt dagegen eine Befugnis, obwohl auch hier Schutz gegen Angriffe dringend erforderlich ist
- Alternativvorschlag für die Praxis
  1. Intrusion Detection System
     - Auswahl zu speichernder Verkehrsdaten
  2. Analyse im Verdachtsfall
     - Pseudonyme Daten, auditierbares IT-Sicherheitsverfahren
  3. Ergebnis
     - Verfolgung relevanter Fälle, Löschung nicht relevanter Daten

Telekommunikations-Vorratsdatenspeicherung?!

- Diskussionspunkte zum Gesetzentwurf zur „Vorratsdatenspeicherung“
  - Bedarf für Vorratsdatenspeicherung
  - Folgerungen aus der EuGH-Entscheidung
  - Differenzierung bei der Speicherung
    - Personen
    - Anlässe
    - Datenarten
  - Berufsgeheimnisträger
  - Fristen -> Quick Freeze
  - „Überwachungs-Gesamtrechnung“

Tue Gutes und rede darüber – Zertifizierungen für mehr Vertrauen in IT?

- Aus unserer Erfahrung in den Zertifizierungsverfahren sind typische Probleme der IT-Sicherheit:
  - Mangelhafte (rechtliche und technische) Einbindung von Dienstleistern und Dritten,
  - Unzureichende Protokollierung,
  - Verzicht auf Verschlüsselung,
  - Unzureichende Mandantentrennung und
  - Nichtvorhandensein eines Datenschutzmanagementsystems.

- Audits, Gütesiegel und IT-Grundschutz-Zertifikate sind dazu geeignet, den eigenen Umgang mit Daten zu hinterfragen und verantwortungsbewusstes Handeln auch nach außen hin sichtbar zu machen.

Vertrauensinfrastrukturen: Gütesiegel für Sicherheit und Privatheit

- Internet-Dienste können von Nutzern nicht selber bewertet werden.

- Damit Online-Siegel Vertrauen aufbauen können, müssen klar Evaluierungsregeln her, sichere Übertragung u. a. durch Zertifikate gewährleistet und automatisierte Validierungen angeboten werden.