Totale Ausspähung – wie können sich unsere Unternehmen schützen?

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

Wirtschaftsrat der CDU e.V.
LV Schleswig-Holstein
Neumünster
4. Dezember 2013

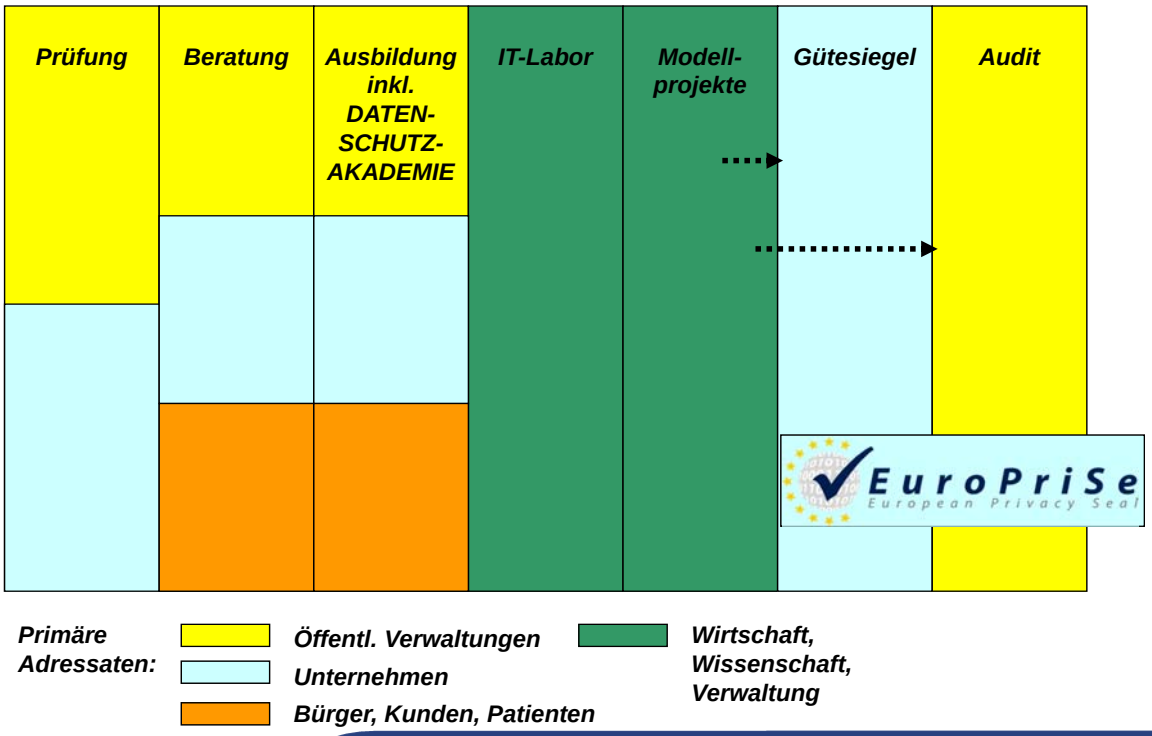
ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Themenschwerpunkte
- Angriffsarten und Risiken
- Staatliche Hilfen
- Koalitionsvertrag
- Technische Sicherungsmaßnahmen
- Datenschutzmanagement

Kurzvorstellung: Was macht das ULD?

Datenschutz und Informationsfreiheit



Themenschwerpunkte Unternehmensdatenschutz

- Banken und Finanzdienstleister (Inkasso, Scoring, SWIFT)
- Versicherungen
- Internet-Wirtschaft (E-Commerce, Spam, Pranger)
- Telemediendienste
- Arbeitnehmerdatenverarbeitung
- Wohnungswirtschaft
- Medizindatenverarbeitung
- Handel (E-Cash, Kundenbindung, Werbung)
- Auskunfteien
- Videoüberwachung

Weitere Sicherheitsthemen: Logistik, Forschung und Entwicklung, Produktion

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.
- Direction Générale de la Securité Extérieure (DGSE – F)
- Bundesnachrichtendienst (BND – D): Strateg. TKÜ u. a.
- Weitere Five Eyes (Canada, Australien, Neuseeland)
- Spionage aus China, Russland...

> Politische Spionage, Wirtschaftsspionage, allgem. Netzüberwachung

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)

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)

Unternehmensdilemma

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

Breach Notification

§ 43a BDSG: Bei unrechtmäßiger Kenntniserlangung von

- Sensiblen Daten
- Berufsgeheimnissen
- Strafverfolgungsdaten
- Bank- und Kreditkartendaten

Mitteilungspflicht an

- Betroffene (direkt, per Medien)
- Aufsichtsbehörde

Ähnliche Erwägung generell bei Cyberangriffen (Problem: Sicherheitsvorfälle sind Betriebsgeheimnisse

Vorschläge rot-schwarzer Koalitionsvertrag

- 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

Technische Sicherungsmaßnahmen

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

- **Vertraulichkeit** (z.B. Verschlüsselung)
- **Integrität**, Authentizität (Backup, digitale Signatur)
- **Verfügbarkeit** (ausfallsichere Stromversorgung, Datenmanagement)
- **Intervernierbarkeit** (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)

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

Totale Ausspähung – wie können sich unsere Unternehmen schützen?

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