BAKER & MCKENZIE

Data Loss Prevention

Rechtliche Herausforderungen beim Kampf gegen Datenabfluss

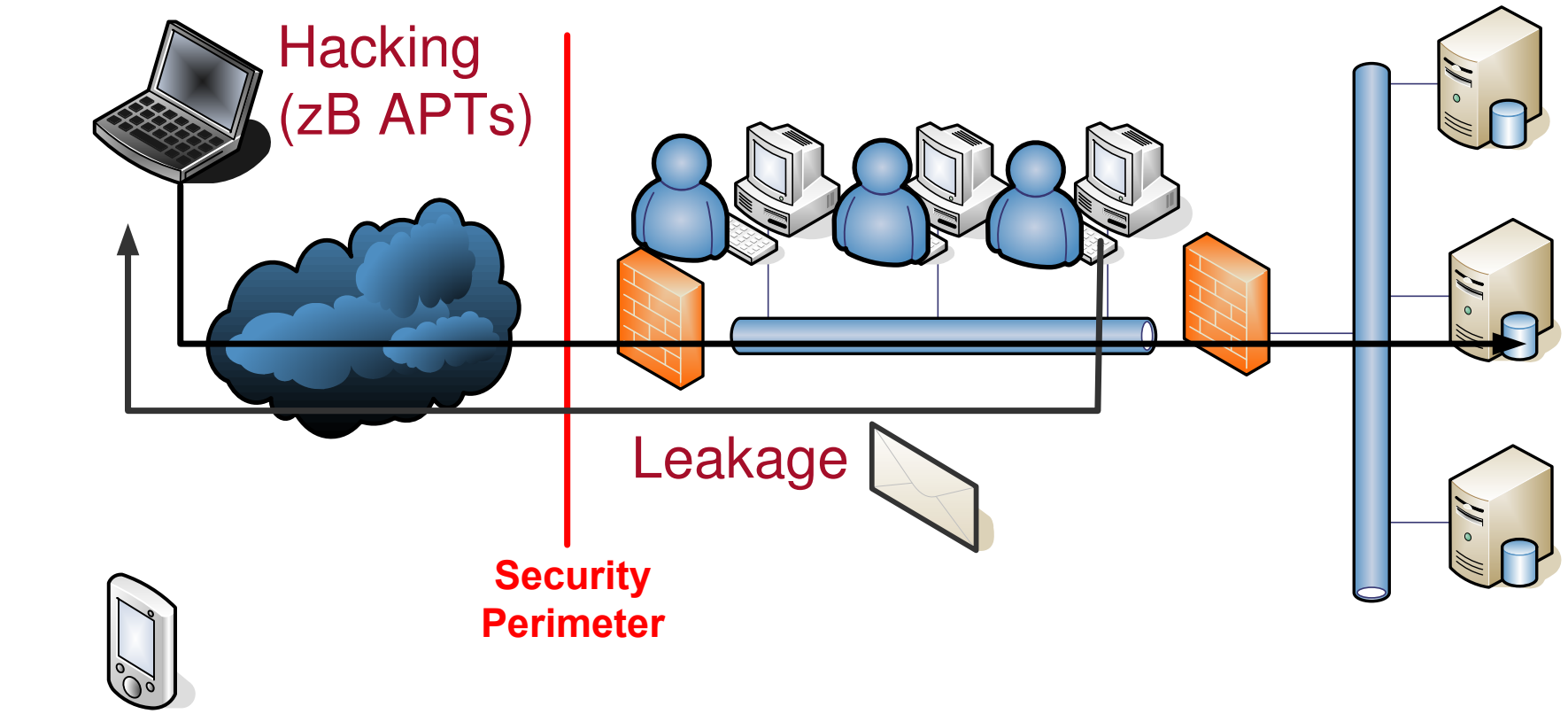
Dr. Lukas Feiler, SSCP

Baker & McKenzie • Diwok Hermann Petsche Rechtsanwälte

TOPICS

1. Gesetzliche Pflichten zur Implementierung von Sicherheitsmaßnahmen
2. Haftung für Data Loss
3. Data Loss Detection durch Traffic Monitoring
4. Mobile Device Security & BYOD

Data Loss – Neue Herausforderungen



Gesetzliche Pflichten zur Implementierung von Sicherheitsmaßnahmen

- Verpflichtende Maßnahmen nach dem Datenschutzgesetz
  - Risiko-angemessene Maßnahmen
  - Jedenfalls (§ 14 Abs 2 DSG):
    - Zugriffsberechtigungen auf Daten & Datenträger (vgl ISO 27002, § 11.6.1)
    - Physische Zutrittsberechtigungen (vgl ISO 27002, § 9.1.2)
    - Protokollierung von Zugriffen/Änderungen (ISO 27002, § 10.10)

Gesetzliche Pflichten zur Implementierung von Sicherheitsmaßnahmen #2

- Verpflichtendes Internes Kontroll-Systems (IKS)
  - U.S. Sarbanes-Oxley Act (SOX) §§ 302, 404
  - EU: Richtlinie 2006/46/EG (sog. „EuroSOX“)
  - Österreich: § 22 GmbHG / § 82 AktG
  - IKS muss angemessen sein, um zu gewährleisten
    - Compliance
    - Ordnungsgemäße & verlässliche Rechnungslegung
    - Schutz des Gesellschaftsvermögens
      → einschließlich Digital Assets

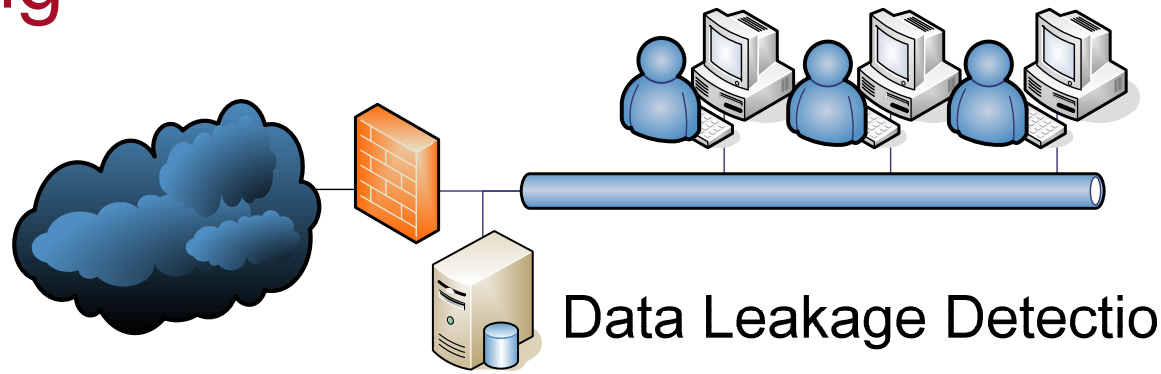
Haftung der Geschäftsleitung für Data Loss

- Haftung des Geschäftsführers/Vorstandes gegenüber der Gesellschaft
  - Geschäftsleitung haftet für Einhaltung der Sorgfalt eines ordentlichen Geschäftsmannes (§ 25 GmbHG / § 84 AktG)
- Strafrechtliche Verantwortlichkeit der Geschäftsleitung oder des gewerberechtlichen Geschäftsführers
  - Verwaltungsstrafe bis EUR 10.000, wenn personenbezogene Daten nicht angemessen geschützt (§ 52 DSG)

Haftung des Unternehmens für Data Loss

- Unternehmen haftet für Data Loss:
  - Solidarische Haftung für Verwaltungsstrafen nach DSG
  - Vertragliche Haftung gegenüber Kunden / Geschäftspartnern
  - Gesetzliche Haftung gegenüber Betroffenen bei Datenschutzverletzung (§ 33 DSG)

Data Leakage Detection durch Traffic Monitoring



- Arbeitsrechtliche Voraussetzungen (Menschenwürde ist berührt)
  - Zustimmung des Betriebsrats erforderlich, sofern einer vorhanden (§ 96 ArbVG)
  - Wenn kein Betriebsrat: Individualvereinbarungen mit jedem Arbeitnehmer (§ 10 AVRAG)

Mobile Device Security & Bring Your Own Device (BYOD)

- BYOD verringert Sicherheitsniveau erheblich:
  - Authentifizierung der Nutzer am Endgerät?
  - Patch Management?
  - Datenverschlüsselung?
- Sicherheitsniveau häufig nicht angemessen (§ 14 DSG / § 25 GmbHG / § 84 AktG)
  - Kompensatorische Maßnahmen nötig
  - z.B. Remote Wiping und/oder Usage Monitoring

BYOD: Remote Wiping

- Szenario: Dienstnehmer verlegt (verliert?) sein Gerät mit
  - Privaten Daten (Urlaubsfotos etc.)
  - Geschäftsgeheimnissen/Kundendaten
- Darf der Arbeitgeber ohne Zustimmung des Dienstnehmers ein Remote Wiping vornehmen?
  - Problem: Datenbeschädigung (§ 126a StGB)

    Wer einen anderen dadurch schädigt, dass er Daten, über die er nicht oder nicht allein verfügen darf, löscht

    Strafdrohung: 6 Monate bzw für Unternehmen bis zu ca. 15% des Jahresumsatzes

BYOD: Remote Wiping #2

- Zustimmung des Dienstnehmers erforderlich
- Sollte vorab von allen Dienstnehmern schriftlich eingeholt werden
- Inhalt der Vereinbarung
  - Informationspflicht des Dienstnehmers an den Dienstgeber, wenn Endgerät verlegt/verloren
  - Voraussetzungen des Remote Wiping sind genau zu definieren

BYOD: Usage Monitoring

- Frühzeitige Missbrauchserkennung durch Usage Monitoring, z.B.:
  - GPS Tracking
  - Traffic Monitoring
  - Überwachung der Verwendung lokaler Apps

→ Menschenwürde ist idR berührt:

  - Zustimmung des Betriebsrats erforderlich, sofern einer vorhanden (§ 96 ArbVG)
  - Wenn kein Betriebsrat: Individualvereinbarungen mit jedem Arbeitnehmer (§ 10 AVRAG)

BYOD: Legal Incident Response nach Verlust eines Endgeräts

- Pflichten zur Data Breach Notification
  - *Die Pflicht, betroffene Personen von der Kompromittierung ihrer personenbezogenen Daten zu informieren.*
  - Zweck:
    - Betroffene sollen reaktive Maßnahmen ergreifen können
    - Markt-Transparenz hinsichtlich Daten-Sicherheit
  - Rechtsquellen in Österreich:
    - DSG & Vertragsrecht

BYOD: Gesetzliche Breach Notification nach Verlust eines Endgeräts

- § 24 Abs 2a DSG: Notifikations-Pflicht, wenn:
  - Unternehmen bekannt wird, dass personenbezogene Daten „systematisch und schwerwiegend“ unrechtmäßig verwendet wurden und
  - den Betroffenen Schaden droht
- Problem: Wann besteht Kenntnis?
- Rechtsfolge der Verletzung:
  - Verwaltungsstrafe: bis zu EUR 10.000 (§ 52 Abs 2 DSG 2000)
  - Haftung für Vermögensschäden nach allgem. Zivilrecht

BYOD: Vertragliche Breach Notification nach Verlust eines Endgeräts

- Wenn Breach Notification in einem Vertrag nicht geregelt ist, gilt:
  - Notifikation einer Sicherheitsverletzung hat zu erfolgen, wenn dem Vertragspartner aus dieser ein Schaden droht (sog. nebenvertragliche Schutzpflicht) → nicht nur, wenn Datenmissbrauch „bekannt“
  - Betroffene sind unverzüglich zu informieren
- Rechtsfolge der Verletzung:
  - Vertragliche Haftung für Vermögensschäden

BAKER & MCKENZIE

Danke für Ihre Aufmerksamkeit!

Kontaktadresse

Dr. Lukas Feiler, SSCP

Baker & McKenzie • Diwok Hermann Petsche Rechtsanwälte

Schubertring 25, 1010 Wien

Tel.: +43 (0) 1 24 250

Fax: +43 (0) 1 24 250 600

E-Mail: lukas.feiler@bakermckenzie.com