Mobile Anwendungen (Bring Your Own Device)

RA Dr. Jan K. Köcher

Syndikus, Datenschutzbeauftragter, Datenschutzauditor (TÜV)

Zu unterscheiden...

- **Bring Your Own Device (BYOD)**
  - Arbeitsmittel im Eigentum des Mitarbeiters
  - Dienst-/Privatnutzung
- **Choose Your Own Device (CYOD)**
  - Arbeitsmittel im Eigentum des Arbeitgebers
  - Dienst-/Privatnutzung
- **Wildwuchs (WIWU)**

BYOD

- **Nutzung privater Geräte zu dienstlichen Zwecken**
  - Am Arbeitsplatz
  - Zu Hause

- **Nicht: Nutzung privater Geräte zu privaten Zwecken am Arbeitsplatz**

Ursache von Problemen...

§ 903 BGB Befugnisse des Eigentümers

„Der Eigentümer einer Sache kann, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache beliebig verfahren und andere von jeder Einwirkung ausschließen.“

Der Eigentümer...

- Profitiert vom Nutzen der Sache
  - → BYOD: Auch der Arbeitgeber soll profitieren!
- Trägt die Lasten (Kosten) der Sache und Folgekosten bei ihrer Nutzung
  - → BYOD: Beteiligung des Arbeitgebers? (AG)
- Haftet ggf. für Schäden, die durch die Sache verursacht werden
  - → BYOD: Wer haftet wann? (Haftpflicht)
- Trägt das Risiko von Beschädigung, Verlust, Zerstörung und Diebstahl
  - → BYOD: Wer trägt das Risiko? (AG)

Steuern

Aufwendungen Arbeitgeber: Betriebsausgaben

- Aspekt private Nutzungsmöglichkeit, geldwerter Vorteil

Aufwendungen Arbeitnehmer: Werbungskosten

- Doppelcharakter der Aufwendungen

Möglichkeit der Pauschalierung?

- Bei CYOD explizit Lohnsteuerbefreiung nach § 3 Nr. 45 EStG

Software

Herausforderungen:

- Dienstliche Software auf einem Privatgerät
- Nutzung privater Software zu dienstlichen Zwecken

Maßnahmen:

- → Bestandsaufnahme
- → Beschränkung, welche private Software dienstlich genutzt werden darf
- → Lizenzen ermitteln und juristisch bewerten
- → Ggf. Erweiterung von Lizenzvereinbarungen

Dezentrale Administration / Wartung / Gerätevielfalt

- Erhöhte Anfälligkeit in Bezug auf Schadsoftware bzw. Einschleusung von Schadsoftware durch infizierte mobile Devices
- **Lösungen:**
  - → Zentrale Wartung durch den Arbeitgeber
  - → Eingrenzung der Geräte- und Softwareauswahl
  - → Softwareupdates beim Arbeitgeber oder virtueller Desktop für die dienstliche Verwendung

IT-Sicherheit

- **Gleichzeitige Installation potentiell gefährlicher privater Anwendungen**
  - ➔ Verbot bestimmter Anwendungen
  - ➔ Effektive Trennung in privaten und dienstlichen Bereich
- **Jailbreaks**
  - ➔ Verbot!
- **Es gilt somit:**
  - Einbeziehung in das Sicherheitskonzept
  - Vertragliche Regelungen und Verwehrung des Zugangs bei Verstößen

Datenschutz

- **Unternehmensdaten: Schutz wie bei interner Datenverarbeitung**
- **Grundlegende Maßnahmen:**
  - Ausschluss von Personengruppen von der Teilnahme
  - Eingrenzung nach Anwendungen und ggf. Trennung über Netzbereiche
  - Nach Möglichkeit Trennung dienstliche und private Daten mit technischen Mitteln
  - Möglichst keine (wenig) Datenspeicherung, Verschlüsselte Speicherung obligatorisch

Datenschutz

- Verhinderung der Nutzung durch Unbefugte
  - Ehepartner, Kinder, sonstige Weitergabe
  - Fremdeigentum, Leasinggeber
  - Wartung und Reparatur
  - → Vertragliche Regelung

- Gewährleistung der Datenlöschung
  - Löschpflicht
  - Ausscheiden des Mitarbeiters
  - Diebstahl des Geräts
  - Weiterverkauf / Weitergabe
  - → Vertragliche Regelung, Fernlöschung

Datenschutz

- Zugriffskontrolle
  - Zertifikatbasierte Authentifizierung
- Weitergabekontrolle
  - Verbot der dienstlichen Nutzung von Cloud-Diensten
  - Unterbindung von Screenshot-Funktionen
  - Verschlüsselte Übermittlung (ggf. über VPN)
- Verfügbarkeit
  - Verbot von Backups in der Cloud

Datenschutz

- **Mitarbeiterdatenschutz (privat/dienstlich)**
  - Remote-Zugriff
  - Ortungsmöglichkeiten
  - Nutzungs- / Zugriffsprotokollierung

- **Maßnahmen:**
  - ➔ Trennung Privatbereich / dienstlicher Bereich
  - ➔ Regelung von Kontrollmöglichkeiten möglichst in einer Betriebsvereinbarung

Zusammenfassend:

- **Erforderliche Vertragliche Regelungen zu:**
  - Teilnahmebedingungen
  - Software/Kosten/Haftung/Steuern
  - Pflichten Datensicherheit und Datenschutz
  - Home-Office
  - Kontrollrechte
- **Wer ist zu beteiligen:**
  - Hochschulleitung und IT-Leitung
  - Datenschutz- und IT-Sicherheitsbeauftragter
  - Personal- bzw. Betriebsrat

Vielen Dank
für Ihre Aufmerksamkeit!

RA Dr. Jan K. Köcher, DFN-CERT
koecher@dfn-cert.de