Veranstaltung

Trustday: 11. Stuttgarter Informationssicherheitstag

16. Juli 2013 IHK Region Stuttgart

Vortrag

Rechtliche Aspekte – Nutzung von mobilen Endgeräten (BYOD)

Referent

Markus Schließ
Rechtsanwalt
Fachanwalt für Arbeitsrecht
Fachanwalt für IT- Recht
Lehrbeauftragter (DHBW) für Arbeitsrecht
Lehrbeauftragter (FH) für IT-Recht

20 Jahre Rechtsberatung und Schulungen

für Unternehmen an der Schnittstelle Mensch – Maschine

Anwaltskanzlei
RÜDISÜHLI BRENNER RENZ

Überblick

1. Einführung
2. Rechtliche Rahmenbedingungen
3. Handlungsempfehlungen und Tipps
4. Zusammenfassung

1. Einführung

BYOD (bring your own device)
= Nutzung mitarbeitereigener Endgeräte zu betrieblichen Zwecken

Vorteile:

Kostenreduktion – keine Anschaffung durch den Arbeitgeber
Produktivitätssteigerung – höherer Spaßfaktor
„Selbstadministration“ (?)
Versierte Handhabung durch den Nutzer (?)

Nachteile:

Heterogene technische Level
Unterschiedliches Nutzungsverhalten (etwa: Kinder „nutzen mit“)
Hoher Aufwand in der IT-Administration
u.U. kein Zugriff auf unternehmensbezogene Daten
Vermischung mit personenbezogenen Daten
(daher Nutzungskontrolle problematisch…)
Lizenzrechtliche Probleme
(Jailbreak/Rooting – Mitarbeiter ist Lizenznehmer!)

1. Einführung

Nutzung firmeneigener Endgeräte

Vorteile:

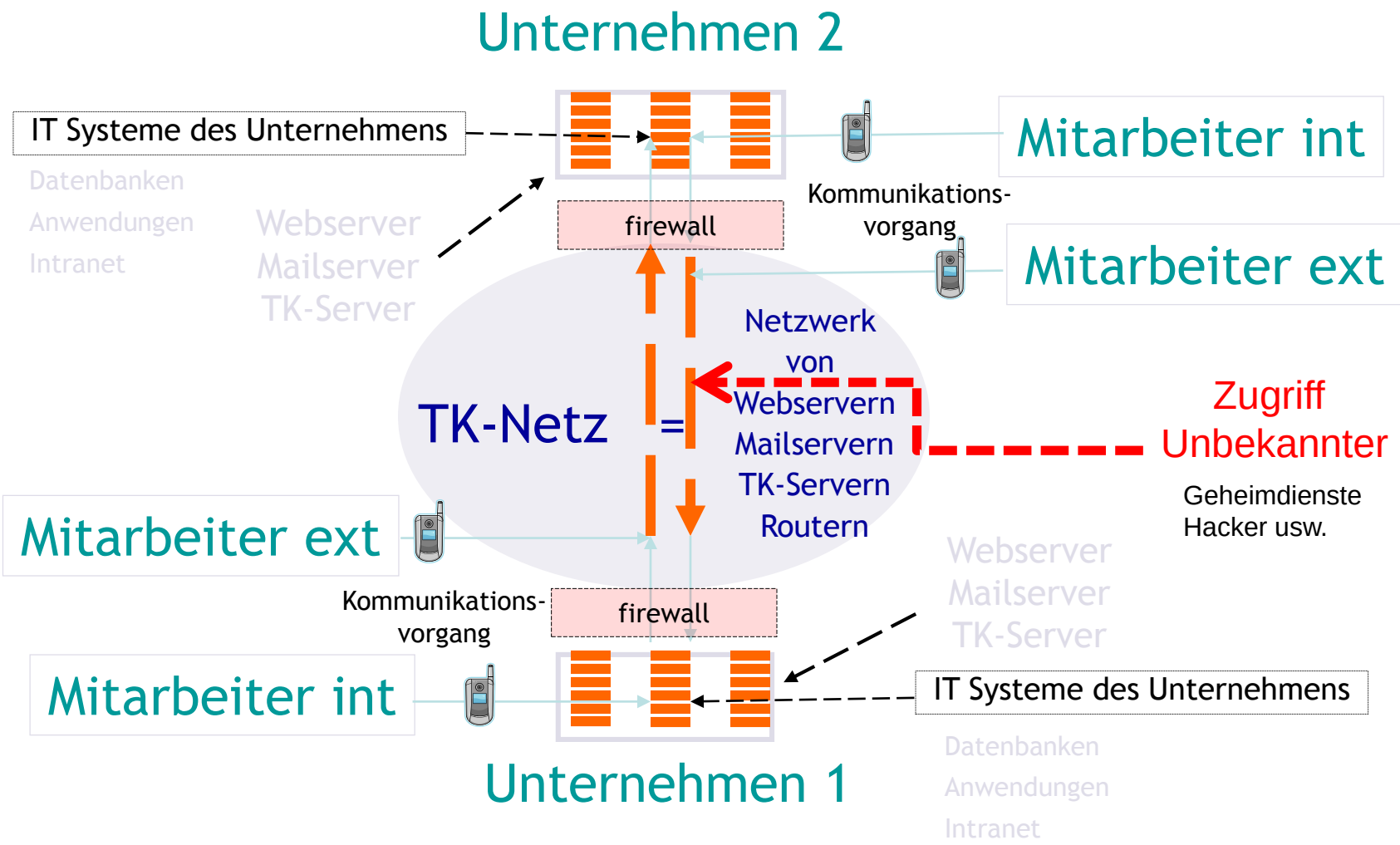
Homogener technischer Level auf allen Nutzungsebenen
Besserer Schutz gegen jede Art Spionage
Einheitliche Nutzung (natürlich erst nach Schulung)
Nutzungskontrolle grundsätzlich möglich (Firmeneigentum!)
Vereinfachung der Administration (release-Management)
Keine Lizenzprobleme (Unternehmen ist Lizenznehmer)

Nachteile:

Geringerer Spaßfaktor (keine Spiele, Kontrolle…)
Ggf. Regelung der privaten Nutzung erforderlich (Datenschutz!)

Mobile Endgeräte im Unternehmen

Datenübertragung in TK-Netzen



2. Rechtliche Rahmenbedingungen

Arbeits-/IT-Recht:	im BGB und im TeleKommunikationsGesetz (TKG) im TeleMedienGesetz (TMG) im BundesDatenSchutzGesetz (etwa: § 9 BDSG) im BetriebsverfassungsGesetz (BetrVG) in tausenden von Gerichtsentscheidungen
aber:	in den geltenden Gesetzen ist nur wenig geregelt
also Chancen:	es können Spielräume genutzt werden – noch!!
	die Betriebsparteien (Arbeitgeber und Betriebsrat) können im Rahmen des § 87 Absatz Nr. 6 BetrVG viel selbst regeln
	der Arbeitgeber *kann* die (berufliche) Nutzung der Endgeräte regeln – er sollte es aber auch tun!

2. Rechtliche Rahmenbedingungen

Gesetzesentwurf zum Arbeitnehmerdatenschutz (§ 32 BDSG neu)
…. nun nicht mehr in dieser Legislaturperiode

Endlose Diskussionen im Vorfeld – wer (Arbeitgeberverbände oder Gewerkschaften) setzt „seine“ Interessen besser durch?

Zweck des Gesetzes:

nicht:
Regelung der Internetnutzung durch den Arbeitnehmer

sondern:
was darf der Arbeitgeber mit den (personenbezogenen!) Daten des Arbeitnehmers machen (Kontrollen usw.)...

…also: Gesetzeslage immer noch lückenhaft = selbst regeln!

3. Handlungsempfehlungen und Tipps

Grundsatz: Jedes Unternehmen hat seine eigene Kultur und seine eigenen Spielregeln!

Wenn es einen Betriebsrat gibt:

Betriebsvereinbarung (BV) im Rahmen des § 87 Absatz 1 Nr. 6 BetrVG zu
- Einführung und Nutzung von IT-Systemen
- IT-Compliance und Datenschutz
- private/berufliche Nutzung von Internet
- private/berufliche Nutzung von Kommunikationsmitteln (Telefon E-Mail)

Wenn es keinen Betriebsrat gibt:

Arbeitgeber regelt die vorgenannten Punkte
- im Wege des Weisungsrechts
- bzw. vertraglich

3. Handlungsempfehlungen und Tipps

Was unbedingt bei BYOD geregelt werden muss:

- Strikte Trennung privater und geschäftlicher Daten
- Untersagung der Nutzung durch Unbefugte (Kinder!) oder
- Technische Sicherstellung von Störungsfreiheit bei unsachgemäßer Nutzung
- Sicherstellung, dass Gerät wirklich in Eigentum und Besitz des Mitarbeiters steht (und nicht: geleast, vom Ehepartner ausgeliehen etc.)
- ggf. Nutzung unterschiedlicher Accounts (twincard)
- Verpflichtung zur regelmäßigen selbstständigen Installation von Antivirensoftware
- Zugriffseinschränkung auf Unternehmensdaten
- Unterbinden von Screenshots-Funktionen
- Keine Nutzung von Cloud-basierten Diensten (Sprachanwendungen Dokumentenaustausch, Terminkalenderfunktionen)
- Zugriff auf Firmen-Intranet nur über eigene Browser (Verschlüsselung!)
- usw. …

3. Handlungsempfehlungen und Tipps

Was unbedingt bei der Nutzung
aller mobiler Endgeräte beachtet werden muss:

- Mitarbeiter schulen
- Aktueller technischer Stand aller Endgeräte
- Zugriff auf betriebsbezogene Daten regeln
- Vorgaben zum Verhalten des Mitarbeiters im Schadensfall/Eskalation/Verlust
- Regelung zu Sperrung und Löschung
- Meldepflicht des Mitarbeiters im Störungsfall
- Protokollierung der Datenverarbeitung
- Keine Sicherung privater Daten durch das Unternehmen und
  von Unternehmensdaten durch den Mitarbeiter
- Vorgaben zum Backup privater Daten

Wo kann man weitere Informationen finden?

http://www.bitkom.org/files/documents/20130404_LF_BYOD_2013_v2.pdf
= Leitfaden zum BYOD

3. Handlungsempfehlungen und Tipps

Stichwort: Industriespionage

Internet ist grenzüberschreitendes Medium (alle Rechtssysteme aller Staaten sind betroffen und – jeder Staat regelt unterschiedlich)

Kein verbindlicher Rechtsrahmen auf internationaler Ebene (UN etc.)

Datenausspähung ist nach deutschem Recht verboten § 202 a StGB

Zugriff auf Täter (erst recht Staaten) sehr schwierig (nur diplomatischer Weg bzw. bilaterale Abkommen

Fazit:

- Keinerlei Erwartungshaltung an Staat oder Institutionen
- Höchstmöglicher Selbstschutz (Guidelines, Schulungen)
- IT-Compliance und Knowhow-Schutz ernst nehmen

4. Zusammenfassung

Nutzung von betriebs- oder mitarbeitereigenen Ressourcen

- wird weiter zunehmen
- wird immer risikoreicher
- muss also unbedingt geregelt werden!

Ansatzpunkte:

- Guidelines (und weitere Dokumente)
  Nutzung von internen/externen Datenbanken, Handys, Laptops, E-Mail, social networks
- Schulungen
  Learning by doing
- „konstruktive“ Kontrollen
  natürlich nur hinsichtlich der betrieblichen Nutzung…
- Kooperation mit Betriebsrat, Datenschutzbeauftragtem und IT-Administratoren

Vielen Dank!

Kontakt zum Referent:

Markus Schließ

Rechtsanwalt
Fachanwalt für Arbeitsrecht
Fachanwalt für IT-Recht
Lehrbeauftragter für Arbeitsrecht (DHBW)
Lehrbeauftragter (FH) für IT-Recht

anwalt@schliess.de
0 171 - 720 12 31

20 Jahre Rechtsberatung und Schulungen für Unternehmen an der Schnittstelle Mensch – Maschine

Anwaltskanzlei
RÜDISÜHLI BRENNER RENZ