Ulrich Emmert

Rechtliche Fallstricke bei Bring Your Own Device

Security Journal, GAI Net Consult, 06/2012

Der Siegeszug von Smartphone und Tablets macht auch vor den Toren der Unternehmen nicht mehr halt – Mitarbeiter wollen ihre gewohnten Geräte von zuhause auch dienstlich nutzen und mit dem Firmennetzwerk verbinden.

Technisch ist diesem Phänomen zumindest bei größeren Unternehmen durch den Einsatz einer Mobile Device Management Software beizukommen, wie sieht es aber rechtlich aus, insbesondere nach der Novelle des Telekommunikationsgesetzes, die zum Teil schon in Kraft getreten ist, zum Teil noch in Kraft treten wird?

Smartphones und Tablets sind nicht wie Blackberrys im Hinblick auf dienstliche Nutzung unter Berücksichtigung von IT-Sicherheit und einfache zentrale Verwaltung über einen Server wie den Blackberry Enterprise Server konzipiert worden, sondern im Hinblick auf besonders komfortable Bedienung und einfache Nutzung von Multimedia-Inhalten privater Nutzer.

Manchen IT-Sicherheitsverantwortlichen treibt daher der Wunsch vieler Mitarbeiter, Geräte mit z.B. IOS oder Android Betriebssystem mit dem Firmennetz zu verbinden, Sorgen- oder sogar Zornesfalten ins Gesicht.

Was von vielen Unternehmen angestrebt wird, wird von sicherheitsorientierten Unternehmen sogar als fristloser Kündigungsgrund gesehen.

Das Bundesarbeitsgericht hat jedoch im März 2011 (AZ 2 AZR 282/10) die Verwendung eines privaten Endgerätes ohne Genehmigung sowie die Verwendung unverschlüsselter Passwörter durch einen IT-Leiter nicht als fristlosen Kündigungsgrund gesehen, sondern eine vorherige Abmahnung verlangt.

1. Rechtliche Schwierigkeiten bei BYOD

BYOD wirft noch viel mehr Probleme auf als die bisherigen Schwierigkeiten mit der Behandlung privater Internet- und E-Mail-Nutzung, da die Möglichkeiten zur Einwirkung auf die Geräte bei privaten Geräten viel geringer sind als bei firmeneigenen Geräten.

a) Eigentum am Gerät
   Der Nutzer kann als Eigentümer des Gerätes erst einmal ohne vertragliche Vereinbarung nicht gezwungen werden, Einschränkungen bei der Nutzung

des Gerätes hinzunehmen. SO lange der Druck von Seiten der Mitarbeiter höher ist als das Interesse des Unternehmens, sowieso schon vorhandene private Geräte aus Kostengründen zu nutzen, kann das Unternehmen verlangen, dass die Mitarbeiter dann gewisse Regeln einhalten, wenn sie ihr Smartphone bzw. Tablet an das Unternehmensnetz anschließen wollen.

b) Unabhängig vom Gerät gibt es auch bei der Frage, wer den genutzten Mobilfunkvertrag abschließt, verschiedene Modelle:

aa. Das Unternehmen schließt für seine Mitarbeiter Mobilfunkverträge ab, die die Mitarbeiter auch privat nutzen dürfen.
bb. Der Mitarbeiter nutzt seinen privaten Mobilfunkvertrag auch dienstlich und bekommt dafür vom Unternehmen Ersatz für Grundgebühr und die Gebühren dienstlicher Nutzung.
cc. Es gibt 2 getrennte Nummern für private und dienstliche Nummern, wobei der dienstliche Vertrag vom Arbeitgeber und der private Vertrag zu Gruppenkonditionen vom Arbeitnehmer abgeschlossen wird.

Bei privaten Verträgen ist nur dann eine Kontrolle möglich, wenn zuvor auf die Rechte aus Datenschutz und Fernmeldegeheimnis verzichtet wurde. Daneben sind noch die Beschränkungen zur Speicherung von Mitarbeiterdaten im BDSG bzw. den Landesdatenschutzgesetzen zu beachten, soweit die privaten Daten nicht für das Arbeitsverhältnis notwendig sind.

c) Fernmeldegeheimnis
Bei dienstlich zur Verfügung gestellten Geräten kann die private Nutzung von Endgeräten insgesamt reglementiert werden. Sowohl die dienstliche Nutzung des Internets als auch das private Versenden von E-Mails kann einseitig vom Arbeitgeber verboten oder bestimmten Regeln unterworfen werden. Lediglich die Kontrolle solcher Einschränkungen oder Verbote ist dann mitbestimmungspflichtig, wenn es in dem Unternehmen oder der Behörde einen Betriebs- bzw. Personalrat gibt.
Gehört das Endgerät jedoch dem Nutzer selbst, können solche Regeln nicht für die private Nutzung außerhalb der Dienstzeit aufgestellt werden, da sonst keine sinnvolle private Nutzung mehr möglich ist. Zeitbasierte Regeln ausschließlich für die Dienstzeit sind im Zeitalter von flexiblen Arbeitszeiten relativ schwer zu überwachen.

Die Nutzung sozialer Netzwerke auf Smartphones kann nicht in private und dienstliche Nutzung getrennt werden, da soziale Netzwerke üblicherweise gemischt genutzt werden, ohne dass der Nutzer dazu wie bei der Nutzung von E-Mail dafür getrennte Accounts verwenden kann. Damit ist das Unterbinden privater Instant-Messenger und Social Network Kommunikation nur sehr schwer zu unterbinden.

Private Programme, die Verschlüsselung oder Tunneling unterstützen, ermöglichen private Kommunikation auch im Firmennetzwerk, die nur erschwert durch HTTPS-Gateways, bei Verwendung zweiseitig verschlüsselter Kommunikation sogar gar nicht durch das Unternehmen kontrolliert werden kann.

d) Rechtliche Anforderungen an Datenschutz und Datensicherheit

Telekommunikationsrechtlich ist der TK-Anbieter – in dem Fall der Kommunikation über das Unternehmensnetz also das Unternehmen – für die Datensicherheit verantwortlich. § 109 TKG verlangt, dass der TK-Diensteanbieter selbst für Datensicherheit und die Einhaltung des Fernmeldegeheimnisses zu sorgen hat.

Auch aus datenschutzrechtlicher Sicht erweist sich BYOD als problematisch. Auf der einen Seite gebietet der Datenschutz die Erfassung des Nutzers bei jeglicher Verarbeitung von Daten durch das Unternehmen aufgrund der Vorschriften zu technischen und organisatorischen Maßnahmen (vgl. § 9 BDSG mit Anhang bzw. entsprechende Vorschriften in den Landesdatenschutzgesetzen).

Auf der anderen Seite ist der Arbeitgeber nicht berechtigt, die bei der privaten Nutzung angefallenen personenbezogenen Daten auf dem Endgerät des Mitarbeiters umfassend zu kontrollieren. Dagegen sprechen die Regelungen des Datengeheimnisses ebenso wie § 32 BDSG zur beschränkten Nutzung von Mitarbeiterdaten. Auch das allgemeine Persönlichkeitsrecht des Mitarbeiters aus Artikel 2 Grundgesetz steht einer vollständigen Überwachung des privaten Endgerätes entgegen.

e) Verantwortlichkeit

Die Verantwortlichkeit für die Nutzung des Endgerätes hängt nicht am Eigentum des Gerätes, sondern an der Identität des Vertragspartners der SIM-Karte. Der Anschlussinhaber haftet zunächst einmal nach der Rechtsprechung als Störer, wenn er nicht plausibel machen kann, dass es einen Geschehensablauf gibt, der ausreichend wahrscheinlich ist und nicht zu einer Haftung für den Anschlussinhaber führt. Wenn der Mitarbeiter mit einem privaten Mobilfunkvertrag das Endgerät für dienstliche Zwecke nutzt, übernimmt er damit aber auch die Risiken der Nutzung.

f) Nutzung von VPN mit dem Smartphone bzw. Tablet

Sowohl IOS als auch Android Geräte können per VPN mit dem eigenen Firmennetz verbunden werden, bei IOS ist ein VPN sogar schon in der Grundversion ab IOS 3 eingebaut. Wenn private Apps nicht kontrolliert werden können, geht die Firma damit ein erhebliches Risiko ein, dass schädliche Inhalte in das Firmennetz gelangen oder parallele Verbindungen ins Internet und ins Firmennetz möglich sind, Daten also an der Firewall vorbei übertragen werden können. Aber auch auf dem Gerät selbst könnten firmeneigene Daten durch andere Applikationen ausgelesen und verarbeitet werden, die dann ggf. zu einem späteren Zeitpunkt an den Hersteller der App oder Dritte übertragen werden.

Das Unternehmen muss als „Herr der Daten“ selbst dafür sorgen, dass personenbezogene Daten geschützt werden und kann diese Entscheidung nicht Mitarbeitern auf ihren privaten Endgeräten überlassen, da diese die Auswahl ihrer Applikationen in erster Linie nach ihrer Freizeitgestaltung und nicht nach Gesichtspunkten des Datenschutzes oder der IT- und TK-Sicherheit auswählen.

Zudem ist bei einer gemischten privaten und geschäftlichen Nutzung auch das Verlustrisiko des Geräts während der Freizeit höher, das Unternehmen sollte also dafür sorgen, dass die dienstlichen Daten bei privater Nutzung nicht zugreifbar sind, was z.B. durch die Verwendung einer Mobile Device Management Software mit verschlüsselter Partition oder kompletter verschlüsselter Virtueller Maschine möglich wird.

Die Auswahl der Applikationen daher streng zu reglementieren und durch technische Maßnahmen oder rechtliche Verbote nur noch einen eng begrenzten Katalog an Apps auf den Endgeräten zuzulassen ist auch keine Lösung.

Der Reiz von Iphone, Ipad und Co. geht völlig verloren, wenn der Nutzer zu viele Einschränkungen bei der privaten Nutzung im Mutimediabereich hinnehmen muss. Gerade die Vielzahl der Apps und der freie Zugriff darauf sind für viele Nutzer ausschlaggebend für die Anschaffung eines doch relativ teuren Endgeräts. Sowohl die mangelnde Bereitschaft der Mitarbeiter, zwei mobile Endgeräte herumzutragen als auch die erheblichen Kosten für moderne Smartphones von 600 bis 800 Euro beim Samsung Galaxy S3 bzw. Iphone 4S zwingen die Firmen dennoch zu einer anderen Vorgehensweise.

2. Empfehlungen zu BYOD

Für Unternehmen, die private Endgeräte zulassen wollen, ist es daher sinnvoll, die Verwendbarkeit der privaten Apps für dienstliche Zwecke wirksam zu begrenzen. Dies ist durch ein Mobile Device Management System möglich, die in der Lage sind, auf dem gleichen Gerät sowohl eine private als auch eine dienstliche Umgebung mit jeweils unterschiedlichen Regeln einzurichten und einen Zugriff auf die jeweils andere Umgebung mittels einer „Sandbox“ zu begrenzen.

Dabei ist abhängig von der Größe des Unternehmens und dem Schadenspotential eines Datenverlusts aus den verschiedenen technischen Möglichkeiten von der einfachen Dual SIM über getrennte Speicherbereiche des Gerätes bis hin zu einer kompletten VIrtualisierung mittels Hypervisor zu wählen.

Dabei halte ich es auch für sinnvoll, die beiden Nutzungsteile an unterschiedliche Rufnummern zu binden, die jeweils nur aus dem jeweiligen Teil des Gerätes nutzbar sind. Dies hat gleich mehrere Vorteile auf einmal:

- -Die dienstlichen Daten können weitgehend einfacher protokolliert werden, da die privaten Daten getrennt protokolliert werden. Ein paar Dinge sind dennoch zu beachten: Es können private empfangene Mails auf dem Dienstaccount empfangen werden, die datenschutzkonform behandelt werden müssen.
- -Private Abrechnungen müssen nicht vom Arbeitgeber abgerechnet werden, sondern werden direkt vom Mobilfunkanbieter erstellt. Durch die Sandbox ist es wesentlich unwahrscheinlicher, dass privat genutzte Apps Sicherheitsprobleme bei der dienstlichen Nutzung des Gerätes verursachen.

Das „jailbreaken“ von IOS Geräten oder „rooten“ von Android Geräten öffnet zunächst einmal mehr Sicherheitslücken, da der Nutzer volle Administratorrechte auf dem Gerät bekommt und diese erhöhten Rechte auch bösartiger Software zu mehr Schadenspotential verhelfen kann. Zudem wird beim IOS Jailbreak ein OpenSSH Server auf dem Gerät installiert, der mit dem Standardpasswort „alpine“ Rootrechte von außen gewährt. Es ist für größere Unternehmen nicht möglich, die zusätzlichen Möglichkeiten durch ein „geöffnetes“ Gerät mit vertretbarem Aufwand hinreichend abzusichern. Verwendet der Mitarbeiter das Gerät geschäftlich, ist das Unternehmen als datenverarbeitende Stelle auch für dadurch verursachte fahrlässige Datenschutzverletzungen voll haftbar. Daher sollte für eine Verwendung von Geräten im Firmennetz zur Bedingung gemacht werden, dass das anzuschließende Gerät weder „gerootet“ noch „gejailbreakt“ ist.

Auch bei der Trennung der verschiedenen Nutzungsbereiche durch technische Maßnahmen ist es sinnvoll, klare rechtliche und organisatorische Regelungen zur

Abgrenzung von Nutzung und Kontrolle zu schaffen. Optimalerweise werden dabei auch Berater eingebunden, die sich sowohl technisch als auch datenschutzrechtlich schon intensiv mit dem Thema Mobile Device Management auseinandergesetzt haben. Da alle Infrastruktur- und Kontrollmaßnahmen, die Mitarbeiterdaten betreffen, zwingend mitbestimmungspflichtig sind, wenn ein Betriebs- oder Personalrat vorhanden ist, empfiehlt es sich zudem, frühzeitig die Arbeitnehmervertretung in die Planung eines Mobile Device Managements einzubinden.

Wer Sicherheitsmaßnahmen bewusst unterlässt, kann als Unternehmen aufgrund der auch vom Bundesgerichtshof bestätigten Störer-Rechtsprechung allein deshalb für Schäden in die Haftung genommen werden. Noch höher wird das Risiko durch den § 42a BDSG oder den seit Mitte geltenden § 109a TKG, bei denen eine Offenbarungspflicht bei Dateschutz- und Datensicherheitsschäden besteht. Bei § 42a BDSG kann dies so weit gehen, dass Zeitungsanzeigen über eigene Datenschutzverfehlungen zum Preis von über 20.000 Euro geschaltet werden müssen.

BYOD ist also kein reines Technikthema, sondern sollte durch ausreichende organisatorische Maßnahmen sowie die Einführung darauf abgestimmter Nutzungsrichtlinien im Unternehmen begleitet werden.

Ulrich Emmert

Partner der überörtlichen Sozietät esb Rechtsanwälte, Büro Stuttgart

Lehrbeauftragter für IT-, Urheber- und Wettbewerbsrecht an der Hochschule für Wirtschaft und Umwelt Nürtingen

Vorstand des Verbands Organisations- und Informationssysteme VOI e.V., Bonn

Schockenriedstr. 8A, 70565 Stuttgart

www.kanzlei.de, Mail ulrich.emmert@kanzlei.de