Kommunikationstechnik für Profis

funkschau

Ausgabe 19/2012 12. Oktober 2012 € 4,90 sfr 8,90

funkschau.de

Raus aus der Wolke

Was es beim Anbieterwechsel zu beachten gibt
So viel Standardisierung braucht die Cloud

ab Seite 10

IP-Centrex

Präsenzmanagement auf dem Prüfstand

Seite 20

BYOD

Rechtliche Herausforderungen

ab Seite 28

Bild: funkschau / Quelle: fotolia

Bring-Your-Own-Device: Rechtliche Herausforderungen

Unternehmen, die sich dem Trend zur „Consumerization" der IT und „Bring Your Own Device" stellen, müssen einige rechtliche Rahmenbedingungen beachten, um den BYOD-Ansatz erfolgreich und sicher zu implementieren. Neben den rechtlichen Herausforderungen und Regelungsmöglichkeiten gilt es wichtige Schritte zur Entwicklung einer individuellen BYOD-Strategie zu beachten.

Abends nochmal kurz die Mails „checken" oder sich einloggen, um dem Kollegen die Produktpräsentation weiterzuleiten – wer kennt das nicht? Smartphones und Tablet-PCs sind aus dem Geschäftsalltag nicht mehr wegzudenken. Mit den gleichermaßen praktischen wie populären mobilen Geräten greifen Nutzer von überall auf das Firmennetzwerk und Unternehmensdaten zu. Immer häufiger geschieht dies mit einem privaten Endgerät – mit oder ohne Wissen des Arbeitgebers.

BYOD – des Pudels Kern

Im engeren Sinne lässt sich BYOD definieren als die Nutzung privater mobiler Endgeräte als Arbeitsmittel in einer Firmenumgebung. Hinsichtlich rechtlicher Fragen spielt jedoch auch der umgekehrte Fall eine Rolle: wenn ein Mitarbeiter ein Firmengerät auch für private Zwecke nutzt. Sich mit dem Thema BYOD zu beschäftigen bedeutet daher, sich grundsätzlich mit der gemischt-privat-geschäftlichen Nutzung mobiler Endgeräte im Unternehmen auseinanderzusetzen. BYOD ist mittlerweile in vielen Unternehmen Praxis. Die Augen vor der ohnehin oft bereits gelebten Realität zu verschließen, hilft dabei ebenso wenig, wie ein generelles Verbot. Im Gegenteil: Wer hier zu rigoros reglementiert, riskiert im Endeffekt nur weitere Sicherheitslecks, da Geräte dann erfahrungsgemäß an der IT vorbei ins Unternehmen geschmuggelt werden. Firmen sollten daher proaktiv reagieren und frühzeitig eine individuelle BYOD-Strategie entwickeln.

Juristische Fallstricke

Haftungsfragen, Eigentumsverhältnisse, Support-Zuständigkeiten – BYOD hält einige juristische Fallstricke bereit.

Ein paar Beispielszenarien:

a) Der neue Mitarbeiter findet es umständlich, privat und dienstlich mit zwei Mobiltelefonen zu hantieren. Statt des Firmen-Blackberrys nutzt er immer häufiger sein privates I-Phone, um geschäftliche Mails abzurufen. Wer konfiguriert das I-Phone und kümmert sich um notwendige Sicherheits-Einstellungen und Updates?

b) Ein Mitarbeiter lädt sich zum Privatvergnügen eine Spiele-App aufs Firmengerät und schleust damit einen Trojaner ins Firmennetzwerk – wer haftet für den Systemausfall?

c) Ein Vertriebsmitarbeiter bahnt regelmäßig geschäftliche Kontakte über Social-Media-Plattformen an und nutzt dazu das Firmenhandy. Gilt das Surfen auf Facebook, Xing & Co in diesem Fall als private Nutzung? Wer leistet Support bei Gerätedefekten?

d) Ein Mitarbeiter nutzt mit Duldung des Arbeitgebers sein privates Gerät auch beruflich und hat Mails, Kontakte etc. darauf abgespeichert. Das Gerät ist weder passwortgeschützt noch verschlüsselt. Wer haftet im Diebstahlsfall? Darf der Arbeitgeber das Gerät – samt privaten Daten – ohne Weiteres aus der Ferne löschen?

Grundsätzliche Rechtslage BYOD

Ist BYOD eigentlich rechtlich zulässig? Wie stellt sich die grundlegende Rechtslage dar? Fakt ist: Diese ist bei BYOD mehrschichtig. Grundsätzlich ist das Einbringen von privaten Geräten in das Firmennetzwerk ohne Kenntnis und Zustimmung des Arbeitgebers nicht erlaubt. Leistet ein Arbeitnehmer diesem Grundsatz nicht Folge, stehen dem Arbeitgeber verschiedene Möglichkeiten zur Verfügung, so zum Beispiel:

- arbeitsrechtliche Mittel der Ermahnung und Abmahnung beziehungsweise je nach Grad der Gefährdung und/oder Schwere des Einzelfalls auch eine außerordentliche Kündigung des Arbeitsverhältnisses
- Schadensersatz – je nach Lage des Einzelfalls muss der Arbeitnehmer für den entstandenen Schaden aufkommen.
- Strafrechtliche Konsequenzen, zum Beispiel gemäß §17 UWG im Fall des Verrats von Geschäfts- und Betriebsgeheimnissen, der auch im Versuch bereits strafbar ist.

Im konkreten Beispiel bedeutet dies: Speichert ein Mitarbeiter ohne Kenntnis und Zustimmung des Arbeitgebers Daten auf seinem privaten Smartphone, um am Wochenende weiter arbeiten zu können, kann dies bereits strafrechtlich relevant sein oder werden – insbesondere dann, wenn es sich um streng vertrauliche Unterlagen handelt. Im Diebstahls- oder Verlustfall ist das Haftungsrisiko für den Arbeitnehmer jedoch kaum zu greifen. Hinzu kommt, dass der Schutz privater Geräte oftmals unzureichend ist und die Geräte aus der Ferne ohne entsprechende Mobile-Device-Management-Lösung nicht zu sperren beziehungsweise zu löschen sind.

Im umgekehrten Fall kann es sich um ein strafrechtlich relevantes Verhalten handeln, wenn der Arbeitgeber unberechtigterweise Informationen auf den BYOD-Privatgeräten der Mitarbeiter einsieht (§202a StGB).

Geduldeter „Wildwuchs“?

Ganz anders und weit komplexer wird es, wenn BYOD geduldet beziehungsweise explizit gestattet oder gar gewünscht ist. Im Duldungsfall ist einem Teamleiter, der IT oder der Geschäftsführung die BYOD-Praxis im Unternehmen zwar bekannt – es fehlen jedoch konkrete Aussagen und Regelungen. Die Duldung ist die mit Abstand komplizierteste Situation.

Was passiert zum Beispiel, wenn ein Nutzer sich durch den privaten Download einer App Schadsoftware einfängt und geschäftskritische Informationen kompromittiert? Die Rechtslage in einem solchen Fall ist nicht immer eindeutig, die Grenzen auch in den Ursächlichkeiten schwer zu greifen und im Einzelfall nicht vorherzusehen. Je länger der Zustand eines solch stillschweigend geduldeten „Wildwuchses“ andauert, desto schwieriger ist es, einen Rechtsrahmen für die Nutzung mobiler Geräte durchzusetzen – ganz zu schweigen von der technischen Herausforderung, unterschiedliche Endgerätetypen und -Betriebssysteme zu integrieren. Vor allem aber ist der Schaden dann meist bereits entstanden: Möglicherweise sind vertrauliche Daten in falsche Hände geraten. Dann helfen mögliche Haftungsansprüche auch nur noch, um den Schaden zu mildern.

BYOD explizit gestattet

Gestattet ein Unternehmen BYOD explizit oder fördert es diese Praxis sogar ausdrücklich, dann ist die Nutzung eigener Geräte beziehungsweise die private Nutzung von Geschäftsgeräten zwar erlaubt – aber nicht ohne Folgen.

Wichtig dabei sind klare Spielregeln. Die Durchsetzung solcher Regelungen sind ab einer Anzahl von zirka 50 mobilen Endgeräten jedoch meist nur noch mit einer einheitlichen technischen Mobile-Device-Management-Plattform möglich.

Haftung im Diebstahls- oder Schadensfall

Wird ein mobiles Gerät beschädigt oder geht es verloren, stellt sich die Frage, wer für den Schaden aufzukommen hat. Eine Haftung ist im Wesentlichen abhängig von zwei Dingen: Wurde das Gerät ursprünglich mit Wissen und Wollen des Arbeitgebers eingebracht? Und: Wann, wo und was ist genau geschehen? Geschah der Schaden im Büro während der Arbeitszeit, auf einer Geschäftsreise oder während des Feierabends, also in einer rein privaten Situation? Mit Verschulden oder aus Nachlässigkeit des Mitarbeiters?

Da im Bereich mobiler Endgeräte die Grenzen zwischen privater und geschäftlicher Nutzung häufig verschwimmen, ist es allerdings oft sehr schwierig, die konkreten Rahmenbedingungen und eine eindeutige Einordnung der Situation vorzunehmen. Eine Haftung bleibt daher stets eine Frage des Einzelfalls. Die Daumenregel lautet: Je „eher“ ein Gerät mit ausdrücklicher Zustimmung beziehungsweise auf Wunsch des Arbeitgebers in das Unternehmen eingebracht wird, desto wahrscheinlicher ist eine Haftung seitens des Arbeitgebers.

Oft unbeachtet bleibt daneben das Haftungsrisiko des Arbeitgebers gegenüber Dritten – insbesondere Kunden und Lieferanten. Was passiert, wenn ein Mitarbeiter mit Duldung des Arbeitgebers vertrauliche Daten auf sein ungeschütztes, privates Gerät speichert, dieses verliert und die Daten bekannt werden? Oft sind in laufenden Geschäftsbeziehungen erhöhte Sicherheits- und Geheimhaltungsmaßnahmen vereinbart, die empfindliche Vertragsstrafen zur Folge haben oder den Fortbestand der Geschäftsbeziehung gefährden können. Hier sind die Haftungsrisiken

Strategien zum Umgang mit BYOD

- BYOD-Spektrum vorab definieren und auf firmeneigene Gerätetypen/Betriebssysteme abstimmen, um Administrationsaufwand einzudämmen.
- Klare Regelungen von Zuständigkeiten (Anschaffung/Bezuschussung?, Konfiguration, Eigentumsverhältnisse, Support etc.).
- Einheitliche Mindeststandards für die Sicherheit (zum Beispiel Passwortschutz, Verschlüsselung etc.).
- IT-, HR- und Rechtsabteilungen sollten gemeinsam Richtlinien pro Nutzergruppe entwickeln/Regeln für die Nutzung von Unternehmensdaten definieren.
- Erweiterte Datenschutzbestimmung: Alle Nutzer müssen zustimmen – wer nicht zustimmt, darf sein Gerät nicht einbringen.
- Konsequenzen für „eingeschmuggelte“ Geräte festlegen und kommunizieren.

Speziell beim Einsatz einer Mobile-Device-Management-Lösung

- Wahrung der Datenschutzrechte der Mitarbeiter (Aufzeichnung, Nutzerverhalten etc. möglich), Zugriff auf Gerätedaten muss explizit schriftlich genehmigt werden.
- Fernlöschung Ja/ Nein – Wer darf den Löschbefehl geben? Wie wird die Identifikation des Anrufers sichergestellt?
- Applikationen: Kontrolle des Softwarestandes, auch bei privaten Apps (nur das „ob“ der Installation – nicht deren Inhalte und Nutzung).
- Den Betriebsrat und alle Betroffenen einbeziehen, durch eine aktive Informationspolitik Transparenz schaffen.

Quelle: MPC Mobilservice

funkschau *Expertenkommentar*

Bild: Profi Engineering Systems

Markus Hock,
Consultant für Sicherheitslösungen bei Profi Engineering Systems

Policies sind ein Muss

Bei der Nutzung von Smartphones und anderen mobilen Endgeräten im Geschäftsumfeld müssen in jedem Fall Policies erstellt werden, wie mit den Endgeräten im Unternehmen umgegangen werden soll. Diese Richtlinien müssen in Kooperation zwischen IT-Abteilung und verantwortlichem Management entwickelt werden, da vor der technischen Umsetzung zunächst Verhaltens- und Nutzungsregeln festgehalten werden müssen.

Um eine möglichst umfangreiche Kontrolle über die Einhaltung der Richtlinien zu gewährleisten, sind zentrale Managementsysteme (MDM, Mobile-Device-Management) unabdingbar. Der Kern eines MDMs besteht aus einem Inventar der Endgeräte sowie aus verschiedenen Richtlinien die darauf angewendet werden können. Des Weiteren lässt sich der aktuelle Status der Geräte abfragen. Über die Umsetzung der von den Betriebssystem-Herstellern gebotenen Schnittstellen hinaus unterscheiden sich die MDM-Hersteller dabei insbesondere durch Zusatzfunktionen, durch die die Administration der mobilen Endgeräte im Alltag erleichtert und die Sicherheit erhöht wird. *(DK)*

nahezu unüberschaubar und können schnell geschäftskritisch werden.

Softwarelizenzen und Multimediadateien

Ein weiterer wichtiger Aspekt ist die lizenzrechtliche Betrachtung von Applikationen und anderer Software sowie von Multimediadateien auf den Privatgeräten. Für den privaten Gebrauch sind Apps oft kostenfrei. Werden diese dann aber auch im geschäftlichen Kontext genutzt, handelt man sich schnell eine Verletzung des Lizenzvertrages mit oft dramatischen Folgen auch für den Arbeitgeber ein. Daher ist es immens wichtig, sehr genau zu beobachten, welche Applikationen eingesetzt werden und wie sich die Lizenzsituation im Einzelfall darstellt. Der Arbeitgeber wird im Idealfall seine Mitarbeiter nicht nur für diese Problematik sensibilisieren, sondern hier auch gegebenenfalls eine Prüfung der Rechtslage vornehmen.

Ähnlich stellt sich die Situation bei Musik- oder anderen Multimediadateien dar: Sobald diese Daten auch betrieblich genutzt werden wird es kritisch – dies kann bereits bei der Verwendung eines Musiktitels als Klingelton beginnen. Auch hier gilt es, die Mitarbeiter aktiv zu informieren und eine entsprechende Regelung zu finden.

Rechtliche Regelungsmöglichkeiten

Um Konflikten von vorneherein vorzubeugen, empfiehlt es sich, bereits bei der Anschaffung und vor der Einbindung von Geräten klar festzulegen, wer welche Leistung oder welchen Service leisten und bezahlen soll, wer in welchem Maße für den Support der Geräte in Bezug auf Hard- und Software zuständig ist oder wie die Wartung und Reparatur einzelner Geräte gehandhabt werden soll: Für welche Teile des Endgerätes, inklusive der Software, ist der jeweilige Mitarbeiter verantwortlich? Auch über eine mögliche Bezuschussung zum Erwerb von Hardware sollten sich Unternehmen im Vorfeld Gedanken machen. In diesem Zusammenhang sollten Eigentumsverhältnisse und Verantwortlichkeiten eindeutig festgelegt werden. Grundsätzlich empfiehlt sich – schon alleine aus Beweissicherungsgründen – entsprechende Regelungen stets schriftlich zu fixieren und diese unbedingt auch mit Organen der Arbeitnehmermitbestimmung, meist dem Betriebsrat, frühzeitig abzustimmen.

Regeln schriftlich fixieren – aber wie?

Das Privateigentum an eingebrachten Endgeräten unterliegt nur bedingt bis gar nicht der Dispositionsbefugnis des Arbeitgebers – deshalb eignet sich im BYOD-Fall eine arbeitsrechtliche Lösung im Rahmen des Direktionsrechts nicht. Auch eine arbeitsvertragliche Lösung ist nicht unbedingt BYOD-tauglich: Arbeitsverträge unterliegen der AGB-Kontrolle, daher sind hier nur zweifellos wirksame Klauseln brauchbar, Unwägbarkeiten gehen zu Lasten des Arbeitgebers. Darüber hinaus taugt die arbeitsvertragliche Lösung am ehesten für Neueinstellungen, eine spätere Änderung bestehender Verträge ist schwierig. Vor allem aber ist es sehr schwer, solche Vereinbarungen an die ständig neuen technischen Entwicklungen anzupassen. Bleibt noch die Betriebsvereinbarung, dort wo sie rechtlich möglich ist: Prinzipiell ein gangbarer Weg, allerdings wirken sich Änderungen auf alle Arbeitsverhältnisse aus und sind daher eher für die Regelung grundsätzlicher Fragen geeignet. Im BYOD-Fall sind die Anforderungen an die verschiedenen Nutzergruppen sehr individuell. Auch die Frage nach der Aktualität und des mit dem Abschluss und der Änderung verbundenden Prozesses stellen eine Unwägbarkeit dar.

Einzel-/Zusatzvereinbarung als Mittel der Wahl

Das Mittel der Wahl ist daher eine gesonderte Vereinbarung auf Organisationsebene. Der Vorteil: Eine solche Regelung – zum Beispiel zu den allgemeinen IT- und Datenschutzbestimmungen – kann auch als Einzelvereinbarung geschlossen werden, wenn ein einzelner Mitarbeiter aus betriebsorganisatorischen Gründen einer entsprechenden Sonderlösung bedarf. Die Regelung kann flexibel auf die jeweiligen Bedürfnisse eingehen und auf den Ebenen Abteilung, Bereich und sonstigen Organisationen laufend aktualisiert werden.

Eine optimale Lösung ist sicherlich die Regelung vorab als Zusatz zum Arbeitsvertrag. Ist dies nicht (mehr) möglich, bietet sich eine Betriebsvereinbarung oder Individualvereinbarung an. In allen Fällen jedoch ist eine laufende Kontrolle nötig.

Fazit: BYOD – Ja, aber nur mit klaren Spielregeln

Findet ein Unternehmen ein grundsätzliches „Ja" zu BYOD, sind eindeutige Regelungen für alle Mitarbeiter und Fälle das A und O (siehe Infokasten). Bei der Formulierung einzelner Richtlinien muss die IT-Abteilung Fingerspitzengefühl beweisen, um alle Parteien mit ins Boot zu holen und entsprechenden Rückhalt für die BYOD-Politik zu erhalten. Der Kompromiss zwischen Sicherheit und Produktivität bleibt dabei sicherlich ein schwieriger Balanceakt. *(DK)*

Robert Himmelsbach,
ist Rechtsanwalt und verantwortet bei MPC Mobilservice den Bereich Mobile-Device-Management