Bring Your Own Device

Knackpunkt Privatgerät

Beim „Bring your own device", also beim Einsatz privater mobiler Geräte am Arbeitsplatz, lauern rechtliche Fallstricke – für das Unternehmen ebenso wie für Angestellte. Christian Solmecke

Eine zunehmende Zahl von Unternehmen erlaubt es ihren Mitarbeitern, private Mobilgeräte wie etwa Smartphones, Tablets oder Laptops auch während ihrer Arbeitszeit im Betrieb zu nutzen. Die Gründe für dieses als „Bring your own device" (BYOD) bekannt gewordene Phänomen sind vielfältig. Einige Unternehmer nennen Kostengründe, andere wollen es ihren Mitarbeitern ermöglichen, private und berufliche Aufgaben leichter zu verbinden, da sich dies positiv auf die Arbeitsleistung auswirke.

Doch der Einsatz privater Geräte im Unternehmen kommt in Deutschland mit ein paar rechtlichen Risiken im Schlepptau. Insbesondere aus der Perspektive von Datenschutz und Arbeitsrecht gibt es einiges, was Unternehmer beachten sollten, bevor sie ihren Mitarbeitern den Zugriff auf das interne Netz mit unternehmensfremden Geräten gestatten. Umgekehrt sollten sich auch die Mitarbeiter bereits im Vorfeld mit der rechtlichen Situation beschäftigen, sonst kommen unter Umständen ungeahnte Probleme auf sie zu.

Geschützte Daten

Beim Einsatz ihrer privat mitgebrachten elektronischen Geräte speichern und verarbeiten die Mitarbeiter automatisch auch sensible Daten des Unternehmens. Dazu zählen etwa Betriebsgeheimnisse und personenbezogene Daten von Mitarbeitern oder Kunden. Hier stellt sich die Frage, inwieweit Mitarbeiter beim Einsatz privater Geräte für einen Datenmissbrauch oder Datenverlust haften.

Die rechtliche Einordnung des Problems gilt unter Juristen als umstritten. Im Ergebnis sind sich jedoch alle einig: Der Arbeitgeber hat dafür zu sorgen, dass die Mitarbeiter die nötigen datenschutzrechtlichen Vorkehrungen einhalten. Dies ergibt sich zumindest aus § 9 des Bundesdatenschutzgesetzes (BDSG), der besagt: „Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes [...] zu gewährleisten."

Unternehmer müssen die oft sensiblen Daten vor dem Zugriff von außen schützen. Und sie müssen dafür sorgen, dass beim Schreiben von E-Mails und beim Speichern von Dokumenten geeignete Verschlüsselungsmethoden zum Einsatz kommen. Zudem sollten sie private und betriebliche Daten trennen.

Vor allem Letzteres entpuppt sich als wichtiger Punkt: Vermischen sich private E-Mails mit geschäftlicher Korrespondenz, ist es dem Arbeitgeber verboten, diese E-Mails ohne Erlaubnis des Arbeitnehmers zu lesen. Tut er es doch, verstößt er gegen das Fernmeldegeheimnis. Anders herum sollten weder die Kinder, noch die Lebenspartner der Mitarbeiter auf die geschäftlichen Daten zugreifen können.

Es ist Sache des Unternehmers, ein entsprechendes Verbot gegenüber den Beschäftigten auszusprechen und sie zum Einhalten der Verbote und Sicherheitsmaßnahmen anzuhalten. Möglicherweise ist zusätzlich eine Schulung im Umgang mit gängigen Sicherheitsmaßnahmen nötig. Zu den üblichen Maßnahmen gehört es etwa, immer einen aktuellen Virenschutz bereitzuhalten und keine unzertifizierte Software zu installieren.

Um den Datenschutz durchzusetzen, muss das Unternehmen auch die Möglichkeit haben, die Daten zu kontrollieren. Zu diesem Zweck sind Zugriffe auf die privaten Geräte der Mitarbeiter unvermeidbar. Der Unternehmer muss die Beschäftigten

allerdings über die Art und die Häufigkeit der Zugriffe in Kenntnis setzen – und diese müssen dem Eingriff zustimmen. Zudem darf die Kontrolle nicht in einem unverhältnismäßigen Maße erfolgen. Die Akteure müssen die Maßnahmen mit dem Persönlichkeitsrecht des Mitarbeiters abwägen und zudem das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme achten.

Nicht zuletzt ist der Arbeitnehmer nach einer Kündigung dazu verpflichtet, alle unternehmensbezogenen Daten von seinen mobilen Geräten zu löschen.

Wer haftet wofür?

Auch die arbeitsrechtlichen Probleme, die sich im Zusammenhang mit BYOD ergeben, sind nicht zu unterschätzen. Bereits im Vorfeld sollten sich die Mitarbeiter bewusst machen, welche Konsequenzen für ihr Arbeitsverhältnis entstehen, wenn sie fahrlässig die angeordneten Sicherheitsbestimmungen umgehen.

Bei einem Verlust oder einer Beschädigung des Geräts haftet in der Regel das Unternehmen. Genauso verhält es sich grundsätzlich auch bei Datenklau oder ähnlichen Vorfällen. Anders sieht die Sache aus, wenn der Arbeitnehmer die vereinbarten Sicherheitsvorkehrungen nicht getroffen und so den Datenverlust begünstigt hat.

In diesem Fall kommen die Grundsätze der gestuften Arbeitnehmerhaftung zur Geltung. Das heißt, der Mitarbeiter haftet nur bei leichter Fahrlässigkeit nicht für sein Handeln. Liegen hingegen vorsätzliches Handeln oder grobe Fahrlässigkeit vor, haftet der Arbeitnehmer allein.

Daher sollten Arbeitgeber und Mitarbeiter stets vertraglich miteinander regeln, in welchem Umfang Letztere das Gerät in der Firma nutzen dürfen und unter welchen Bedingungen. Dabei wäre auch zu klären, inwieweit die private Nutzung während der Arbeitszeit erfolgen darf.

Abbildung 2: Verhält er sich grob fahrlässig, kann ein Mitarbeiter vollständig für den Verlust von Daten haften, etwa bei einem Datendiebstahl.

Der Arbeitgeber darf Mitarbeiter natürlich nicht vertraglich dazu verpflichten, private Geräte während der Arbeitszeit zu nutzen. Umgekehrt kann sich aber das Recht, ein privates Gerät im betrieblichen Umfeld einzusetzen, aus betrieblicher Übung, also aus der Gewohnheit heraus, ergeben. Das ist gefährlich, denn meist handelt es sich um einen schleichenden Prozess, den die IT-Abteilung des Unternehmens nicht rechtzeitig erfasst, sodass keine Zeit bleibt, ausreichende Sicherheitsvorkehrungen für Datensicherheit und -schutz zu treffen.

Ist im Unternehmen ein Betriebsrat tätig, muss dieser zudem vor der Einführung von BYOD-Regeln seine Zustimmung geben. Unternehmen sollten darüber hinaus nicht vergessen, dass sich durch den Einsatz privater Geräte im Arbeitsalltag die üblichen Arbeitszeiten der Mitarbeiter verschieben könnten. Auch dafür sollte das Unternehmen Regelungen treffen und gegebenenfalls den Betriebsrat anhören.

Klärungsbedarf besteht häufig auch in der Frage, inwieweit sich die Unternehmen an den Anschaffungs- und Wartungskosten für die privaten Geräte beteiligen müssen. Gesetzlich ist geregelt, dass der Arbeitgeber seinen Mitarbeitern das notwendige Arbeitsmaterial zur Verfügung stellen muss.

Fazit

Ob BYOD im Unternehmen positive Effekte zeitigt, muss jeder Unternehmer nach Abwägung der Vor- und Nachteile für sich selbst entscheiden. Fest steht, dass er rechtliche und technische Vorkehrungen treffen sollte, bevor er den Mitarbeitern die Nutzung privater Geräte erlaubt. So wird die BYOD-Strategie nicht zum Fiasko. *(kki)*

Abbildung 1: Bevor Firmen private Geräte ins eigene Netzwerk lassen, sollten sie sich rechtlich absichern.

Der Autor

Die Kölner Kanzlei Wilde Beuger Solmecke hat sich auf die Beratung der IT- und Onlinebranche spezialisiert. Rechtsanwalt Christian Solmecke (40) hat in den vergangenen Jahren den Bereich IT-und E-Commerce stetig ausgebaut und betreut Medienschaffende und Web-2.0-Plattformen. Daneben ist er Geschäftsführer des Deutschen Instituts für Kommunikation und Recht im Internet (DIKRI) an der Cologne Business School [http://www.dikri.de].