BYOD 2.0 – Trennung von Privat- und Berufsleben

Thorsten Freitag, 2013-09-04

Die Vorteile, Mitarbeiter ihre eigenen Geräte am Arbeitsplatz nutzen zu lassen, sind offensichtlich und wurden bereits ausreichend dokumentiert. Gut 60% von uns tun dies bereits (Ovum, November 2012). Aber BYOD hat auch seine Nachteile, sowohl aus persönlicher Sicht als auch für die IT.

Abgesehen davon, dass das Gerät Eigentum des Mitarbeiters und nicht des Unternehmens ist und damit die Möglichkeiten zur Umsetzung von Sicherheitsrichtlinien und zum Schutz sensibler Geschäftsdaten eingeschränkt sind, wird meist übersehen, welche Auswirkungen dies auf unser Privatleben haben kann.

Ohne eine klare Trennlinie zu ziehen, werden persönliche und berufliche Dinge auf einem Gerät miteinander vermischt. Wenn es ein Problem mit dem Gerät gibt und alle Inhalte gelöscht werden müssen, gehen sämtliche Daten verloren.

Das mag aus Sicht des Unternehmens sinnvoll sein, möglicherweise verliert ein Mitarbeiter dabei jedoch alle seine Fotos, Videos, E-Mails, Kontaktdaten und SMS-Nachrichten aus den letzten Jahren.

Stellen Sie sich nur vor, Sie würden die Fotos aus dem letzten Urlaub oder die Bilder Ihrer Kinder verlieren. Wenn Sie die Daten auf Ihrem Mobilgerät nicht regelmäßig sichern (und viele von uns tun das nicht), ist diese Gefahr nur allzu real.

Und hierbei geht es nicht nur um die Sicherung der Daten, die sich auf dem Gerät befinden. Wenn Sie über Ihr eigenes Mobilgerät in ständigem Kontakt mit Ihrem Unternehmen stehen, weicht dies die Grenze zwischen Privat- und Berufsleben auf, bis sie schließlich ganz verschwindet.

Urlaube und Wochenenden bieten immer weniger Gelegenheit, sich von der Arbeit zu erholen und die Batterien wieder aufzuladen. Stattdessen werden Bürozeiten verlängert, indem auch zu Hause das Smartphone zur Hand genommen wird, um ein paar E-Mails zu beantworten oder den Rest zu erledigen, der am Freitagnachmittag liegengeblieben ist.

Die Idealvorstellung wäre natürlich eine Trennung zwischen dem privaten und beruflichen Kontext eines Mobilgeräts, egal ob es sich dabei um ein Smartphone, ein Tablet oder ein Laptop handelt. Dies bedeutet, dass das Gerät weiterhin umfassend verwaltet wird und die IT kontrolliert, welche Apps heruntergeladen werden und sogar bestimmte Gerätefunktionen einschränken kann, die der Produktivität nicht zuträglich sind.

Diese Trennung von Beruflichem und Privatem hat auch Auswirkung auf die Einstellung des Benutzers. Wenn Benutzer ihre Geräte für berufliche Zwecke nutzen, sind sie viel eher geneigt, als Vertreter des Unternehmens zu denken und zu handeln, etwa so, als ob sie an ihrem Schreibtisch säßen. Möglicherweise bleiben dem Unternehmen so peinliche Zwischenfälle erspart, beispielsweise anstößige Tweets, die aus Versehen veröffentlicht wurden und ein schlechtes Licht auf das Unternehmen werfen.

Diese Umgangsweise mit BYOD – **wir bei F5 nennen das BYOD 2.0** – bietet Unternehmen und Mitarbeitern genau das, was sie wollen: Die Freiheit, ein Gerät eigener Wahl für berufliche und private Zwecke zu nutzen, jedoch mit einer klaren Trennung der Benutzerrollen auf dem Gerät sowie mit der Gewissheit, dass Unternehmensdaten sicher sind und die IT ein gewisses Maß an Kontrolle behält.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com