SMARTPHONE & CO.

Wenn Grenzen zwischen Beruf und Privatleben verschwimmen

VON THOMAS BIERE
Thomas Biere ist Mitarbeiter beim Bundesamt für Sicherheit in der Informationstechnik und Dozent im Masterstudiengang Sozialinformatik an der Katholischen Universität Eichstätt-Ingolstadt. Dieser Artikel stellt seine persönliche Meinung zum Thema dar, nicht die des Bundesamtes.
E-Mail thomas.biere@bsi.bund.de

Der Einsatz privater »mobiler Endgeräte« sollte in einer Organisation oder einem Unternehmen gut bedacht werden. In einem schlüssigen Gesamtkonzept müssen alle Fragen um Handy und Smartphone beantwortet werden, vom Datenschutz bis zum Steuerrecht.

Keine Frage: Mobilgeräte wie Notebooks, Netbooks, Tablet-PCs und Smartphones sind schick und immer schnell zur Hand. Wer sie privat nutzt, möchte ihren Komfort auch im Beruf nicht missen: hier eine schnelle Mail, dort ein Schnappschuss vom Flipchart oder eine kurze Web-Recherche. Da liegt es nahe, das private Gerät auch im beruflichen Alltag zu nutzen – zumal, wenn der sozialwirtschaftliche Arbeitgeber mit der Ausstattung zögert.

In den USA sind Trends dieser Art schon länger zu beobachten, dort werden sie unter dem Begriff »Bring Your Own Device« (BYOD) verhandelt. Höhere Mitarbeiterzufriedenheit und Mitarbeitermotivation sowie gesteigerte Effizienz werden als Vorteile angeführt. Da die Mitarbeiter ihre Endgeräte selber beschaffen und sich der Arbeitgeber allenfalls mit einem Zuschuss beteiligt, sinken auch die Beschaffungskosten. Doch hat BYOD nicht nur Vorteile. Vielmehr ist eine Reihe von Fragen zu berücksichtigen, die vor einem Einsatz einer Lösung geklärt werden sollten.

Sicherlich kein gangbarer Weg ist es, den Mitarbeitern einfach nur zu erlauben, private Endgeräte am Arbeitsplatz einzusetzen. Vielmehr muss die Einführung von BOYD in ein Konzept eingebunden werden, das damit einhergehende Probleme vermeiden hilft.

Zunächst muss überlegt werden, wie private Endgeräte in die Informationstechnik des Unternehmens sicher eingebunden werden können. Fragen der Datensicherheit und des technischen Datenschutzes stehen bei diesen Überlegungen im Vordergrund. Der Arbeitgeber hat die privaten Endgeräte naturgemäß nicht unter vollständiger Kontrolle. Jedes dieser Geräte kann mit Schadsoftware infiziert sein, was dazu führen kann, dass Angreifer über ein solches Endgerät Zugriff auf sensible Daten bekommen.

»Unabdingbar ist die strikte Trennung von Unternehmensdaten und privaten Daten«

Daher muss jedes private Endgerät im Unternehmensnetz zunächst als »feindlich« angesehen werden. Als Folge ist die Netzarchitektur entsprechend anzupassen. Dabei wird ein besonderes Augenmerk auf die Firewall-Architektur zu legen sein.

Neben der Netztrennung müssen die Zugriffsberechtigungen angepasst werden. Auch ist zu überlegen, ob sensible Unternehmensdaten direkt auf dem Endgerät bearbeitet werden sollen, was zusätzliche Risiken birgt, oder ob von der Möglichkeit der Virtualisierung und von Terminalservern Gebrauch gemacht werden soll.

Bei den Endgeräten selbst ist zu bedenken, dass diese hinreichend gegen Schadsoftware geschützt werden müssen. Zudem muss – abhängig vom Einsatzszenario – über Verschlüsselung nachgedacht werden. Unabdingbar ist die strikte Trennung von Unternehmensdaten und privaten Daten. Auch dies muss im Konzept verankert werden.

Weiterhin ist zu bedenken, dass für das private Endgerät hinreichender Support geleistet werden muss. Dies stellt die Supportabteilung vor zusätzliche Herausforderungen, da durch den Einsatz von privaten Endgeräten eine größere Heterogenität der Systemlandschaft entsteht (zusätzliche Betriebssysteme, gegebenenfalls in verschiedenen Versionen, unterschiedliche Hardware etc.).

Zu lösen ist ferner eine Reihe von juristischen Problemen. Das fängt beispielsweise mit der Frage an, wie sich der Arbeitgeber an der Beschaffung der Endgeräte beteiligt. Dies kann in der Form eines Zuschusses, aber auch als Darlehen erfolgen. Damit verknüpft ist die Frage, wie im Falle des Verlustes oder der Beschädigung verfahren werden soll und welche Regeln beim Ausscheiden des Mitarbeiters aus dem Unternehmen gelten.

Schließlich müssen Zugriffsrechte des Arbeitgebers unter Berücksichtigung des Arbeitnehmerdatenschutzes festgelegt werden. Hierzu müssen die Arbeitsverträge entsprechend ausgestaltet werden. Möglicherweise kann der Abschluss einer Betriebsvereinbarung ein gangbarer Weg sein.

Auch steuerrechtliche Fragen gilt es zu berücksichtigen. So muss beispielsweise geklärt werden, inwieweit Software, die dem Arbeitnehmer auf diesem Wege zur Verfügung gestellt wird und die er privat nutzen kann, als geldwerter Vorteil zu versteuern ist. Dabei ist zu prüfen, ob bestehende Softwarelizenzen die Überlassung an den Arbeitnehmer überhaupt zulassen.

Als Fazit lässt sich festhalten, dass BYOD auf der einen Seite Vorteile für Unternehmen bietet, dass auf der anderen Seite aber auch eine Reihe von Problemen und Risiken zu berücksichtigen sind. Die Empfehlung kann nur lauten, Vorteile und Risiken von BOYD sorgfältig abzuwägen und insbesondere Sicherheitsaspekte bei den Überlegungen nicht außen vor zu lassen. ■