Trend “Bring Your Own Device” – Fluch oder Segen?

Das Vordringen privater Mobilgeräte verändert Unternehmen

Immer mehr Mitarbeiter nutzen ihre privaten Mobilgeräte, wie Smart Phones oder Tablet-PCs an ihrem Arbeitsplatz – und zwar sowohl für private als auch für geschäftliche Zwecke. Einschlägige Medien werten diesen Trend, genannt „Bring Your Own Device“ (BYOD), bereits als bedeutend und meinen, dass Bewerber heute ihre Entscheidung für ein Unternehmen auch davon abhängig machen, ob sie eigene Geräte mitbringen dürfen. CIOs jedoch runzeln die Stirn und argumentieren vor allem mit datenschutzrechtlichen Bedenken.

Von Ekkehart Gerlach und Frank Bitzer

Private Handys, die am Arbeitsplatz benutzt werden, sind heute keine Seltenheit mehr. Was aber passiert, wenn private Mobilgeräte auch für dienstliche Aufgaben im Unternehmen genutzt werden? Spätestens wenn diese Geräte mit der unternehmens-eigenen Technik gekoppelt und Daten ausgetauscht werden sollen, stellt sich Arbeitgebern die Frage, wie damit umzugehen ist.

Ein zentrales Problem ist der häufig ungenügende Schutz privater Geräte. Werden sie auch in der Firma eingesetzt, könnte Malware auf Unternehmensnetze übertragen werden, Apps könnten Daten ausspähen, beispielsweise auf Mail-Accounts oder – wie kürzlich bekannt wurde – durch das Auslesen von Adressbüchern. Ein weiteres Argument: Innovative mobile Geräte werden häufiger gestohlen als Desktops der vorletzten Generation, so dass betriebliche Daten vermehrt auf diesem Weg in die Hände Dritter gelangen. Noch nicht ausdiskutiert ist schließlich, wie sich die zunehmende Nutzung des Cloud Computing auswirkt, wo Daten vielfach hin und her synchronisiert werden

Datenschutz bei BYOD

Doch nicht nur die IT-Sicherheit muss beachtet werden, sondern auch das Urheberrecht und der Datenschutz. Kostenfreie Apps und „Open Source“-Software dürfen privat meist frei verwendet werden – die Nutzung im Unternehmen hingegen könnte gegen Lizenzrechte verstoßen. Darüber hinaus wird die schon heute problematische Frage, ob geschäftliche Daten und Mail-Accounts auch privat genutzt werden dürfen, weiter

verschärft. Diskutiert werden muss auch, wie Unternehmen bei einem Verlust oder Defekt der privaten Geräte bezüglich Software, Hardware sowie der darinf enthaltenen Daten vorgehen sollten.

Auswirkungen auf die Produktivität

Ungeklärt ist bislang auch, in wieweit der Einsatz privater Geräte die Produktivität der Mitarbeiter erhöht oder bremst. Optimisten gehen davon aus, dass Arbeitnehmer durch die Nutzung neuerer Geräte motivierter sind, Pessimisten fürchten hingegen, dass sie eher abgelenkt werden und verweisen auf erste Untersuchungen hierzu. Für die IT-Administration ist das Bild klarer: Je identischer die Hard- und Software, desto mehr standardisierte Wartung ist möglich. Mit anderen Worten: Die Vielfalt mitgebrachter innovativer Geräte könnte bei der IT-Administration eher zum Stau und Inkompatibilitätsproblemen führen.

Nicht zuletzt muss auch der „soziale Neid“ zwischen den Mitarbeitern mit eigenen schicken Geräten und jenen mit „alten Firmen-Handys“ berücksichtigt werden.

Genauso heterogen wie die Probleme von BYOD sind auch die Lösungsvorschläge. Sie reichen derzeit von einem generellen Verbot privater Geräte bei der Arbeit bis zu deren weitgehender Freigabe. Ein Kompromiss sieht eine Zulassung privater Geräte mit Einbettung in eine ganzheitliche IT-Compliance-Strategie vor. Einige Unternehmen, die diesen Ansatz bereits praktizieren, sichern sich beispielsweise das Recht, bei möglichen Konflikten, Support-Fragen, akuten Verdachtsmomenten oder sogar regelmäßig die privaten Geräte ihrer Mitarbeiter kontrollieren zu dürfen.

Einen etwas anderen Weg geht der Lösungsansatz „Choose Your Own Device“ (CYOD): Hierbei bieten Unternehmen ihren Mitarbeitern ausgewählte innovative Geräte für die geschäftliche und private Nutzung an. Vorteil: Durch die begrenzte Anzahl unterschiedlicher Hardware kann zumindest das Standardisierungsproblem bei der IT-Administration besser gelöst werden. Da damit aber beileibe nicht alle offenen Fragen beantwortet sind, wird wohl erst die Entwicklung der nächsten Jahre zeigen, welcher Ansatz in Zukunft bevorzugt wird. Deutlich wird aber schon heute: Unternehmen brauchen bei diesem Thema klar kommunizierte Regeln, damit alle Beteiligten wissen, was praktikabel und erlaubt ist.