03. September 2012

Safety first – auch bei Tablets

Von **Katrin Quack** (COMPUTERWOCHE-Redakteurin)

Als weltweit operierender Sicherheitsdienstleister stellt Securitas hohe Anforderungen an die eigene IT-Security. Wie verträgt sich das mit dem Einsatz von iPads?

Antonio Valls Ruiz,
IT-Leiter Securitas GmbH

Geschäftsführung und Vertrieb der Securitas-Division Mobile Dienste nutzen seit etwa zwei Jahren iPads. Diese ergänzen die Notebooks - vor allem, um die Angebotserstellung zu beschleunigen; sie sind leichter und schneller, und ermöglichen elegantere Präsentationsformen. Zunächst kommen 100 Tablets zum Einsatz, langfristig sind 300 geplant.

Der erste Impuls zur Nutzung kam von der Geschäftsführung. Natürlich sind wir immer offen für Neuerungen, aber Sicherheit steht bei uns an erster Stelle, auch bei mobilen Geräten. Dazu gehörte die Einführung eines Mobile-Device-Managements (MDM) von MobileIron, bei der uns das IT-Beratungshaus EBF unterstützte.

Das MDM verfügt über eine "Jailbreak Detection": Es kann über Ortungsdienste selbständig feststellen, ob ein Gerät geknackt wurde, und sperrt dann die Verbindungen in das Securitas-Netz. Zudem können die Administratoren unerwünschte Apps definieren. Wird eine solche App auf einem iPad installiert, bleibt das Gerät blockiert, bis die App gelöscht wurde.

Nicht zuletzt besteht für alle mobilen Geräte die Pflicht, mindestens sechsstellige alphanumerische Codes zu nutzen, um das Gerät zu entsperren. Zusätzliche Sicherheit gibt der "EBF-Connector" für den sicheren Lesezugriff auf Dokumente, die auf einem dedizierten Server im Netzwerk abgelegt sind. Dabei werden keine Kopien auf den mobilen Geräten gespeichert, alle unternehmenskritischen Daten verbleiben in einer sicheren Umgebung im Netz.

ByoD nicht praktikabel

Mein IT-Kollege Stefan Schenke und ich sehen uns ständig nach IT-Innovationen für die Kolleginnen und Kollegen um. Bring your own Device ist für uns aber keine praktikable Möglichkeit. Ich glaube nicht, dass sich das in Deutschland durchsetzt. Wenn das Management mit seinen privaten Geräten kommt und sie ins Firmennetz integrieren möchte, muss ich da manchmal viel Überzeugungskraft aufwenden. Oberste Priorität hat aber immer die Datensicherheit - egal, wer Wünsche anmeldet.

Als Nächstes wird Securitas eine User Policy erstellen, die aus den bisherigen Erfahrungen resultiert. Sie wird intern publiziert und verteilt. Und bei Sicherheitsverstößen wird künftig automatisch jede Verbindung ins Netzwerk gesperrt.

Quelle: COMPUTERWOCHE, Ausgabe 36/12
Autor: Karin Quack