

Mobile Device Management

Smartphones sollen Arbeit erleichtern und kein Sicherheitsrisiko darstellen

Smartphones und Tablet-PC halten zunehmend Einzug in Finanzinstitute. Bisher bringen Mitarbeiter meist ihre privaten Geräte mit an den Arbeitsplatz und möchten sie von der IT-Abteilung in die Unternehmens-EDV einbinden lassen. Um unnötige Sicherheitsrisiken zu vermeiden, sollten Organisationen bereits heute nach Möglichkeiten suchen, diese mobilen Arbeitsmittel effektiv und sicher in ihre IT zu integrieren.

Aktuell drängen besonders Mitarbeiter aus dem Management und Vertrieb dazu, ihre mobilen Endgeräte auch geschäftlich in ihren Finanzinstituten einzusetzen. Die IT-Abteilung trifft diese Nachfrage nach mehr Mobilität bislang meist noch unvorbereitet. Nicht selten entwickeln sie dann eine „Kopf-in-den-Sand“-Taktik, um diesem eher unliebsamen Thema aus dem Weg zu gehen. Doch auf Dauer wird die IT nicht umhinkommen, Lösungen dafür anzubieten. Denn die Entwicklung, dass Mitarbeiter mehr und mehr ihre mobilen Endgeräte für ihre Arbeit nutzen möchten, ist nicht zu stoppen.

Statt dem Geräte-Wildwuchs freien Lauf zu lassen und am Ende den Überblick über Endgeräte und die eigenen Daten zu verlieren, müssen Institute sich für die richtige Integration mobiler Geräte wappnen. Zwar sind Verwaltung und Support für eine Vielzahl solcher Endgeräte komplex, zeitaufwendig und letztlich kostenintensiv. Ein fehlendes Management dieser Geräte bedeutet jedoch nicht nur für den Datenschutz und den Schutz des geistigen Eigentums der Institute ein hohes Risiko. Es stellt auch für die Betriebskosten wie Support und Anwenderunterstützung eine kritische Komponente dar.

Die Strategie festlegen

Die Auseinandersetzung mit den Themen Sicherheit und Datenschutz ist für die Verantwortlichen in Finanzinstituten Teil ihres Alltags. Nun müssen sie eine Strategie entwickeln, um sowohl private als auch vom Unternehmen zur Verfügung gestellte Endgeräte sicher in die betriebliche IT einzubinden. Vorher gilt es herauszufinden, welche Daten Mitarbeiter auf ihren Geräten nutzen können. Institute müssen daraufhin prüfen, welche Informationen unternehmenskritisch sind, diese klassifizieren und den jeweiligen Schutzbedarf ermitteln.

Ziel ist es dabei, mögliche Datenlecks zu erkennen und zu schließen, um den Verlust vertraulicher Daten zu verhindern. Dabei können technische Lösungen wie „Data Leakage Prevention“ helfen. Zudem empfiehlt es sich, die mobilen Endgeräte in die IT-Infrastruktur zu integrieren. Ein eigenes „Mobile Device Management“ (MDM) bildet dafür die Basis. Alternativ können Finanzinstitute einen MDM als Dienst bei einem erfahrenen IT-Serviceanbieter in Anspruch nehmen. Der Dienstleister sorgt dann für die technischen Grundlagen, um den Informationsschutz den Vorgaben eines Instituts entsprechend zu unterstützen. Beispiele dafür sind eine Remote-Löschung bei Verlust des Endgeräts oder die Durchsetzung eines Passworts für die Freischaltung.

Einbindung mobiler Endgeräte

Mithilfe eines Mobile Device Managements können Organisationen Smartphones und Tablet-PCs in die Gesamtstruktur ihrer IT integrieren. Hat ein Finanzinstitut die Nutzergruppe festgelegt, die mobile Endgeräte für ihre Arbeit einsetzen soll, ist der nächste Schritt die Erarbeitung eines individuellen Rechte-Managements mit entsprechenden Sicherheitsregelwerken. Auf dem Markt gibt es dafür bereits Lösungen, die beispielsweise den Zugriff auf Unternehmensdaten über mobile Endgeräte in Form einer App anbieten. Der Vorteil solcher Apps ist, dass sie auf unterschiedlichen Endgeräten mit verschiedenen Betriebssystemen wie Apple iOS, BlackBerry OS oder Android laufen können. Das erlaubt ein heterogenes Management der Geräte und bietet ein hohes Maß an Flexibilität für die Nutzer.

Ein Institut gibt den Anwendern entweder Zugang zu der entsprechenden App, um sie herunterzuladen oder ein Gerät, auf dem die App bereits vorinstalliert ist. Der



Quelle: apple.com

Die sichere Einbindung von Smartphones in die IT von Kreditinstituten erfordert solides Know-how.

Zugriff auf die geschäftlichen Daten erfolgt über einen individuellen Benutzernamen mit Authentifizierungscode. Auf diese Weise können die Mitarbeiter mit ihren mobilen Endgeräten über einen gesicherten Zugang auf geschäftliche Anwendungen zugreifen, um dann Daten zu bearbeiten.

Besser gut vorbereitet

Der Einsatz mobiler Endgeräte am Arbeitsplatz wird in den nächsten Jahren zunehmend voranschreiten. Er trägt künftig auch zum Image der Institute als attraktiver Arbeitgeber bei. Um den Überblick über Geräte und die Kosten im Griff zu behalten, aber auch um die Sicherheit der eigenen Daten nicht zu gefährden, sollten sich Geschäftsleitung und IT-Abteilung daher schon heute gezielt mit diesem Thema auseinandersetzen. ◀