Das Benutzen mobiler Geräte von Mitarbeiterinnen und Mitarbeitern des Bundesministeriums für Inneres soll mit einem „Mobile Device Management“ geregelt werden.

Schutz von Unternehmensdaten

Das Innenministerium führt ein „Mobile Device Management“ für mobile Geräte ein. Damit sollen Daten bei einem Angriff durch Schadsoftware sowie bei Diebstahl oder Verlust geschützt werden.

Smartphones und Tablets werden auf Grund ihrer Vielseitigkeit auch beruflich viel verwendet. In Unternehmen kommen sie als effiziente Werkzeuge für Mitarbeiterinnen und Mitarbeiter mit für die Firmen maßgeschneiderten Apps zum Einsatz. Im öffentlichen Bereich werden sie vor allem für den mobilen Zugriff auf E-Mails und Termine genutzt. Das birgt auch Risiken, denn mobile Geräte werden zunehmend von Schadsoftware bedroht. Betroffen sind in erster Linie Firmen und öffentliche Einrichtungen, bei denen es um den Diebstahl von Betriebsgeheimnissen geht. Privatpersonen könnten mit persönlichen Daten, die vom Smartphone gestohlen wurden, erpresst werden. Ein Angriff durch Schadsoftware ist jedoch nur eine Facette der Risiken der mobilen Geräte. Weitere Risiken sind der Verlust und Diebstahl des Geräts.

Schutzmaßnahmen. Für ein Unternehmen sowie Institutionen im öffentlichen Bereich stellt sich daher zunehmend die Frage, wie Unternehmensdaten auf den mobilen Geräten wirksam geschützt werden können. Prinzipiell muss der Benutzer eines mobilen Geräts selbst Maßnahmen zum Schutz setzen. Die Sperre des Bildschirms ist ein erster Schritt, um Unbefugten den Zugriff auf das Gerät zu erschweren. Ein weiterer Schritt kann die sorgfältige Auswahl jener Apps sein, die auf dem Gerät installiert werden. Allerdings sind die Methoden für Angriffe auf ein Smartphone oder Tablet bereits sehr ausgereift und können vom Benutzer oft nicht erkannt werden. Um diesen und anderen Problemen entgegenzutreten, wurden technische Lösungen entwickelt, die den Anwender bei der Absicherung des mobilen Geräts unterstützen. Solche Sicherheitslösungen werden unter dem Titel *Mobile Device Management (MDM)* zusammengefasst. Ihre Kernfunktion besteht darin, die Einhaltung von Sicherheitsstandards sowie die zentrale Absicherung mobiler Geräte im Organisationsumfeld zu garantieren. Mit einem MDM wird zusätzlich der Nutzer im Hinblick auf Sicherheitsrisiken entlastet und es werden Gefahren im Zusammenhang mit Datenverlust reduziert.

Ein *Mobile Device Management* gliedert sich technisch in zwei Elemente, einen zentralen Server und mit ihm verbundene, direkt auf den mobilen Geräten installierte Clients. Über den zentralen MDM-Server werden die sicherheitsrelevanten Vorgaben eingestellt, wobei eine Unterscheidung nach Benutzergruppen erfolgen kann.

Die MDM-Clients erhalten automatisiert die passende Konfiguration vom Server übermittelt. Es muss also nicht jedes Gerät einzeln und manuell vom jeweiligen Benutzer selbst eingestellt werden. Bei neuen Gefahren kann zentral rasch eine Anpassung der Sicherheitseinstellung aller Geräte vorgenommen werden. Zur Unterstützung der Benutzer kann z. B. die Passwortmindestlänge, das Maximalalter oder die Mindestkomplexität des Passworts zentral festgelegt werden. Ebenso können unterstützend Konfigurationen wie WLAN-Einstellungen zentral erstellt und verteilt werden.

Zusätzlich sorgt der MDM-Client am mobilen Gerät dafür, dass die Unternehmensdaten verschlüsselt und vom restlichen System getrennt gespeichert werden können. Diese Art der Kapselung von sensiblen Daten in einem sogenannten „Container“ verhindert, dass am Smartphone (vor-)installierte Apps auf Unternehmensdaten zugreifen können. Das Gerät wird damit in zwei Zonen aufgeteilt, eine „offene“ private, in der auch allgemeine Apps installiert werden können, und eine „abgesicherte“ berufliche Zone, in der ausschließlich vom Unternehmen vorgegebene Anwendungen laufen dürfen. Der Zugriff auf den Container wird durch ein von der Gerätesperre getrenntes, zusätzliches Passwort und eine automatische Sperre bei Inaktivität gesichert.

Allein in der abgesicherten Zone ist der Zugriff auf die beruflichen E-Mails, Termine und Kontakte über eigens vom Container zur Verfügung gestellte Apps möglich. Die standardmäßige E-Mail- oder Kalender-App des

Fotos: Ophlia/Fotolia, Vizafoto/Fotolia

Der Zugriff auf berufliche Apps ist in einer abgesicherten Zone möglich.

mobilen Geräts liegt außerhalb des Containers und kann nicht mehr für die Unternehmenskommunikation verwendet werden. Dafür sind in der abgesicherten Zone zusätzliche Möglichkeiten für einen erweiterten Zugriff auf Unternehmensdaten, wie beispielsweise Dateiablagen, vorgesehen.

Der Verlust oder Diebstahl eines mobilen Geräts wird durch ein MDM noch weiter entschärft, indem die dienstlichen Daten auf Smartphones bzw. Tablets durch Fernzugriff von zentraler Stelle aus gelöscht werden können. Dadurch wird das mobile Gerät zwar nicht unbrauchbar, aber die Unternehmensdaten sind nicht mehr am Gerät gespeichert.

Im BMI wurden die Anforderungen von organisatorischer und technischer Seite für ein *Mobile Device Management* definiert und darauf aufbauend wurde ein Pflichtenheft erstellt. Dieses bildete die Grundlage für die europaweite öffentliche Ausschreibung unter Federführung der Vergabeabteilung des Ressorts. Acht Anbieter beteiligten sich an der Ausschreibung. Nach der formalen und technischen Prüfung erfolgte im Dezember 2014 der Zuschlag. Mittlerweile wird die technische Lösung umgesetzt. Ein wesentlicher Arbeitsschritt ist derzeit die Definition der nötigen Sicherheitseinstellungen in Form von Profilen und die Anpassung interner Prozesse durch die Integration des MDM.

Die Ausrollung des MDM auf jene mobilen Geräte des BMI, die über eine Datensynchronisation verfügen, wird nach einer Testphase ab Ende März 2015 nach und nach vorgenommen. Es soll den Mitarbeiterinnen und Mitarbeitern mehr Sicherheit im Umgang mit ihren mobilen Geräten bringen, bei gleichzeitiger Erleichterung für die zentrale Konfiguration und Verwaltung der Geräte. *Michael Mörz*

FOTO: BERNHARD ELBE