BSI-Regelwerk fürs Mobile Device Management

Vorgegeben

Volker Weber

Auch in Behörden und anderen öffentlichen Stellen halten Smartphones und Tablets Einzug. Das BSI widmet nun dem sicheren Einsatz und dem Management dieser Geräte einen eigenen Mindeststandard.

Ein neues Regelwerk des Bundesamts für Sicherheit in der Informationstechnik (BSI) widmet sich dem Mobile Device Management (MDM). Das BSI legt für die Stellen des Bundes allgemeine Mindeststandards fest, die Behörden der Länder und Kommunen heranziehen können, um eigene Standards anzupassen. Fürs MDM definiert er in 40 technischen und organisatorischen Regeln die Anforderungen, die ein solches System umsetzen können muss, lässt aber Spielraum bei deren Ausgestaltung.

Obwohl solche Mindeststandards nicht automatisch verpflichtend sind, bieten sie dennoch eine Checkliste, anhand derer man eigene Dienste und Anbieter prüfen kann. So erhalten Verantwortliche eine erste Orientierung in strittigen Fragen wie einem Jailbreak oder Rooting.

Kein MAM oder MCM

Der Mindeststandard beschäftigt sich ausschließlich mit dem eigentlichen Management und nicht mit den verwandten Themen, die kommerzielle Angebote ebenfalls abdecken. Hierunter fällt das Administrieren vertrauenswürdiger Applikationen (Mobile Application Management – MAM), das Verwalten von Inhalten (Mobile Content Management – MCM) oder das sichere Verbinden der Applikationen mit dem Backend. Insofern ist der Mindeststandard nicht geeignet, den passenden EMM-Dienst (Enterprise Mobility Management) auszuwählen, da die gängigen Anbieter die geforderten Eigenschaften mühelos erreichen. Zudem beschäftigt sich das Regelwerk explizit ausschließlich mit Smartphones, Phablets und Tablets mit Android, iOS oder BlackBerry. Andere mobile Geräte oder IoT-Clients finden keine Erwähnung.

Manche Regeln des BSI-Mindeststandards für MDM-Systeme sind ziemlich schlicht, zum Beispiel die Regel 30: „Das MDM muss von geschulten Administratoren bedient werden.“ Andere haben es dagegen in sich. So fordert Regel 35, dass MDMs und mobile Endgeräte, für die der Hersteller keine sicherheitsrelevanten Aktualisierungen mehr bereitstellt, außer Betrieb zu nehmen sind. Die Regel 4 besagt außerdem, dass Verantwortliche kompromittierte verwaltete mobile Endgeräte schnell erkennen und vom MDM sowie der Infrastruktur der Stelle des Bundes ausschließen müssen. Ferner bezeichnet das BSI dabei ein Jailbreak und Rooting als Kompromittierung. Die Regel 25 legt fest, dass alle mobilen Endgeräte im MDM zu verwalten sind und dass sie sich vor der Verteilung der Grundkonfiguration im Werkszustand befinden müssen.

Nimmt man allein die Regeln 4, 25 und 35 als Maßstab, müssen Administratoren viele Android-Geräte mangels Sicherheitsupdates ausmustern oder dürfen sie gar nicht erst in Betrieb nehmen. Individuelle Anpassungen durch Root-Rechte bleiben verboten. Die Forderung nach dem Werkszustand schiebt damit zugleich Custom ROMs oder Geräten, die Anwender bereits privat nutzen, den Riegel vor. BYOD-Szenarien, bei denen Container amtliche Daten schützen, scheinen ausgeschlossen zu sein. Eine private Nutzung thematisiert der Mindeststandard nicht.

Unbequeme oder unbeliebte Verordnungen kann der IT-Leiter einer Behörde in der Diskussion mit der Amtsleitung oder den Anwendern leichter durchsetzen. So fordert Regel 28, dass mobile Geräte mit Kennwörtern zu schützen sind und dass eine automatische Sperre nach spätestens zehn Minuten zu wirken hat. Dabei sieht der Standard keine Abweichung für mobile Geräte vor – die Kennwörter unterliegen den gleichen Anforderungen wie die PCs derselben Behörde.

In Regel 31 findet sich selbst eine salvatorische Klausel: Sollte das MDM eine Änderung der Konfiguration durch den Anwender nicht verhindern können, dann müssen Verantwortliche diese verpflichten, solche Änderungen zu unterlassen. Besser kann man nicht darstellen, dass ausschließlich ein verantwortungsvoller Umgang mit den Smartphones einen sicheren IT-Betrieb gewährleistet.

Fazit

Der BSI-Mindeststandard für das Mobile Device Management kommt spät und er ist dennoch nicht auf der Höhe der Zeit. Es geht längst um mehr als Sicherheitseinstellungen und einfache Konfigurationsprofile, nämlich darum, den Zugang zu dienstlichen Informationen über alle Geräte und Applikationen hinweg zu regeln. Dennoch ist er ein guter Anfang, er ist die Grundlagen für eine sichere Handhabung von Smartphones. (fo)

Volker Weber

ist Korrespondent der Heise Medien GmbH und arbeitet als Autor, Consultant und Systemarchitekt.

Alle Links: www.ix.de/ix1708078