Geräte-Management

Standards für den sicheren Betrieb

[06.12.2017] Ein Mobile Device Management hilft Behörden dabei, mobile Endgeräte zentral zu verwalten und sicher zu betreiben. Für die Auswahl eines geeigneten Systems hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Mindeststandards definiert.

Smartphones und Tablets haben in der öffentlichen Verwaltung in den vergangenen Jahren vermehrt Einzug gehalten. Die Nutzung mobiler Endgeräte umfasst auch die Speicherung und Verarbeitung sensibler Informationen. Dabei können vielfältige Bedrohungen und Risiken entstehen, denen unter anderem mit technischen Hilfsmitteln begegnet werden muss.
Mithilfe von Systemen für das Mobile Device Management (MDM) können mobile Endgeräte in die IT-Infrastruktur einer Verwaltung integriert und zentral verwaltet werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für Stellen der Bundesverwaltung technische und organisatorische Mindeststandards definiert, die ein MDM-System zu erfüllen hat, wenn es in einer Stelle des Bundes eingesetzt werden soll – daran können sich auch die Kommunen orientieren.

Funktionale Anforderungen

Der Mindeststandard des BSI formuliert unter anderem funktionale Sicherheitsanforderungen an die Arbeitsweise der MDM-Lösung. So müssen etwa Nutzdaten des MDM innerhalb der IT-Infrastruktur des Betreibers verbleiben. Wird das MDM ganz oder teilweise von einem externen Cloud-Anbieter bezogen, sind zusätzlich die Anforderungen des BSI-Mindeststandards zur Nutzung externer Cloud-Dienste einzuhalten. Des Weiteren gilt: Werden mehrere Mandanten auf einem MDM verwaltet, so muss eine wirksame Trennung erfolgen.
Ein wichtiger Punkt zum Schutz des Mobile Device Management und der Konfiguration ist zudem, dass kompromittierte mobile Endgeräte zeitnah erkannt und vom MDM ausgeschlossen werden. Es muss also gewährleistet werden, dass Sicherheitsvorfälle dem Administrator in geeigneter Weise angezeigt werden. Des Weiteren muss das MDM über ein Rechte-Management verfügen, das sicherstellt, dass Benutzergruppen und Administratoren nur über solche Zugriffsrechte verfügen, die für die Aufgabenerfüllung notwendig sind (Minimalprinzip).
Im Rahmen der Applikationsverwaltung legt der Mindeststandard des BSI fest, dass eine zentrale Verteilung von Applikationen möglich sein muss. Werden Sicherheitsprobleme einer Applikation bekannt, so muss diese zeitnah von allen mobilen Endgeräten deinstalliert werden können. Dieser Vorgang muss durch das MDM erzwungen werden können. Im Rahmen des Mobile Device Management muss zudem der Lebenszyklus einschließlich der Konfigurationshistorie eines jeden in der Verwaltung eingesetzten mobilen Endgeräts ausreichend protokolliert und zentral abrufbar sein. Bei Bedarf muss der Administrator den aktuellen Status der verwalteten Endgeräte ermitteln können (Device Audit). Das umfasst insbesondere die Abfrage sicherheitstechnisch relevanter Konfigurationseinstellungen, installierter Zertifikate und Applikationen.

Sicher konfigurieren und betreiben

Hinsichtlich der sicheren Konfiguration mobiler Endgeräte in der öffentlichen Verwaltung hat das BSI unter anderem Vorgaben für die Konfigurationsprofile, die sichere Erstinstallation, zu Kennwörtern und

Gerätecodes, Zertifikaten sowie zur Verschlüsselung des Gerätespeichers erarbeitet.
Wichtige Punkte sind zudem die Fernlöschung (Remote Wipe) und Außerbetriebnahme sowie die automatische Sperre von Geräten (Remote Lock). So muss das MDM laut BSI sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät, einschließlich Zugangsdaten und Zertifikaten, auch aus der Ferne gelöscht werden können. Werden in dem mobilen Endgerät externe Speicher genutzt, ist zu prüfen, ob diese bei einem Remote Wipe ebenfalls gelöscht werden sollen und ob dies vom MDM unterstützt wird. Der Prozess zur Außerbetriebnahme des mobilen Endgeräts (Unenrollment) muss gewährleisten, dass darauf sowie auf den eingebundenen Speichermedien keine sensitiven Daten verbleiben – insbesondere dann, wenn das Unenrollment aus der Ferne durchgeführt wird. Die Einrichtung und wirksame Durchsetzung einer automatischen Sperre des mobilen Endgeräts nach Zeitvorgabe muss zentral konfigurierbar sein. Eine Gerätesperrung muss durch den Administrator auch aus der Ferne möglich sein (Remote Lock). Kann der Remote Lock auf dem mobilen Endgerät nicht ausgeführt werden, muss dies vom MDM angezeigt werden können.
Die Wirksamkeit von Sicherheitsmechanismen hängt auch vom jeweiligen Betrieb ab. Der Betreiber der mobilen Endgeräte hat daher nach Angaben des BSI einige technische und organisatorische Maßnahmen umzusetzen. So müssen etwa wirksame Mechanismen für das Backup aller Daten und Einstellungen des MDM existieren, sodass dieses im Bedarfsfall funktionsfähig wiederhergestellt werden kann. Fernzugriffe auf das MDM müssen auf einem kryptografisch abgesicherten Kanal erfolgen (vertraulich, integer, authentisch). Alle in einer Behörde eingesetzten mobilen Endgeräte sind in dem MDM zu verwalten und müssen sich vor Verteilung der Grundkonfiguration im Werkszustand befinden. Organisatorisch empfiehlt das BSI, geschulte Administratoren zur Bedienung eines Mobile Device Management einzusetzen und die Nutzer mobiler Endgeräte für Sinn und Zweck der festgelegten Sicherheitsmaßnahmen zu sensibilisieren. Wichtig auch: Konfigurationsprofile und Sicherheitseinstellungen sind regelmäßig zu überprüfen.

Auf Sicherheitsvorfälle vorbereitet sein

Aber selbst wenn alle notwendigen Schutzmaßnahmen ergriffen werden, lassen sich Sicherheitsvorfälle nicht immer verhindern. Für diesen Fall muss ein angemessener Prozess etabliert sein, der insbesondere folgende Szenarien abdeckt: Verlust eines mobilen Endgeräts, Verlust der Integrität des mobilen Endgeräts (etwa durch Jailbreak oder Rooting), kein Kontakt des mobilen Endgeräts zum MDM über einen längeren Zeitraum hinweg. Zudem müssen Arbeitsprozesse geplant, getestet und angemessen dokumentiert sein, um sicherheitsrelevante Patches und Updates unverzüglich einspielen zu können. MDM-Systeme und mobile Endgeräte, für die keine sicherheitsrelevanten Aktualisierungen mehr bereitgestellt werden, sind außer Betrieb zu nehmen.
Außerdem ist sicherzustellen, dass ausschließlich sicherheitsgeprüfte Applikationen bereitgestellt werden. Dabei helfen kann ein definierter Freigabeprozess mit geeigneten Bewertungskriterien. Die Nutzung von vorinstallierten Applikationen und Online-Diensten, insbesondere von externen cloudbasierten Diensten, muss bewertet und im Bedarfsfall systemseitig verhindert werden. Die Freischaltung von Schnittstellen und Funktionen ist zu regeln und auf das dienstlich notwendige Maß zu reduzieren.

Auch die Peripherie berücksichtigen

Die Einführung mobiler Endgeräte bringt für die Verantwortlichen zudem die Pflicht mit sich, datenschutzrechtliche, sicherheitstechnische und betriebliche Anforderungen für die Einbindung von Peripherie-Geräten zu definieren. So ist es oft alles andere als einfach, eine Strategie zum mobilen Drucken zu implementieren, da innerhalb der meisten Institutionen eine breite Palette von Hardware, Software und Serviceangeboten je nach Drucker und zugrunde liegender Druckerinfrastruktur berücksichtigt werden muss. Die Evaluierung, welche Lösung die Sicherheitsstrategie der Institution

hierbei am besten unterstützt, sollte ein fester Bestandteil der Planungs- und Konzeptionsphase sein. Ansonsten ist damit zu rechnen, dass die Nutzer mobiler Endgeräte sich Workarounds aufbauen, um die etablierten Sicherheitsmaßnahmen zu umgehen.
Da es eine Vielzahl von MDM-Produkten auf dem Markt gibt, empfiehlt das BSI, bei der Auswahl vor allem darauf zu achten, dass die Lösung die definierten Anforderungen einer Behörde unterstützt. Die Verantwortlichen sollten sicherstellen, dass nur solche MDM-Software genutzt oder beschafft wird, die alle technischen und organisatorischen Sicherheitsmaßnahmen umsetzen kann und alle freigegebenen mobilen Endgeräte unterstützt.

()

Weitere Informationen zum Mindeststandard des BSI
Dieser Beitrag ist in der Dezember-Ausgabe von Kommune21 im Schwerpunkt Geräte-Management erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Infrastruktur, Mobile Device Management, IT-Sicherheit, Datenschutz