Android 10 erfordert fürs Geräte-management «Android Enterprise»

Spätestens mit Android 10 eröffnen sich neue Möglichkeiten zum Gerätemanagement, die sowohl die Sicherheit als auch die Benutzerfreundlichkeit erhöhen. Unternehmen, die ihre Geräteflotten nach wie vor gerätebasiert mit Device Admin managen, sollten deshalb jetzt unbedingt die Migration angehen.

Die Schweiz galt lange als Apple-Land, doch die Zeiten ändern sich. Der Anteil an Android-Geräten des Suchmaschinengiganten Google und diverser anderer Hersteller nimmt in den letzten Jahren auch hierzulande immer mehr zu und hat zu Ende des Jahres 2019 die 50-Prozent-Marke überschritten. Die Gründe liegen nicht zuletzt an der grösseren Gerätevielfalt der diversen Smartphone-Hersteller und damit verbunden den selbst im oberen Preissegment gegenüber iPhones deutlich niedrigen Preisen.

Wie früher, als durch den Druck der Mitarbeitenden mit dem iPhone die IT-Verantwortlichen gedrängt wurden, private Geräte für Unternehmenszwecke zu akzeptieren (Bring your own Device, BYOD), ist Android mittlerweile ein Muss bei der Geräteadministration. Dies bringt jedoch entsprechende Herausforderungen mit sich. Viele Firmen wickeln zwar bereits seit Jahren erfolgreich ihre Android-Geräteadministration mittels Device Admin ab, allerdings ist dies nur noch mit Geräten möglich, die mit Android 9 und früheren Versionen laufen. Ab Android 10 wird ohne Android Enterprise eine vollumfängliche, sichere Geräteadministration nicht mehr möglich sein. Unternehmen sollten deshalb möglichst zeitnah auf Android Enterprise wechseln. Das bedingt zwar einen gewissen Aufwand, bietet aber zusätzliche Möglichkeiten heute und in Zukunft. Die Migration muss geplant, Android Enterprise in der bestehenden EMM-Lösung (Enterprise Mobility Management) konfiguriert, getestet und auf neu zu registrierenden und/oder bereits registrierten Geräten ausgerollt werden.

Bild: elenabsl / AdobeStock.com

Einfacher, sicherer, mitarbeiterfreundlicher

Die Vorteile gegenüber dem bisherigen Gerätemanagement mit Device Admin sind umfassend: Dazu gehören nicht nur die verbesserte Sicherheit, sondern auch die besser abgestufte Kontrolle über die Funktionen der registrierten Geräte. So kann der Arbeitgeber auf BYOD-Geräten lediglich das «Work Profile» (Arbeitsprofil) und einige elementare Gerätefunktionen beeinflussen, während auf voll registrierten Geräten zusätzliche Funktionen wie der Kiosk-Modus zur Verfügung stehen. Darüber hinaus können beliebige Apps aus Managed Google Play innerhalb des Arbeitsprofils verwendet und vorkonfiguriert werden, was die Integration von Apps im Unternehmen vereinfacht.

Ein grosses Plus ist die Trennung von firmeneigenen und privaten Daten. Im Kontext von BYOD-Geräten bietet die Verfügbarkeit der zwei komplett unterschiedlichen Profile (Arbeit, Privates) die Möglichkeit, zu definieren, wann mit dem Gerät gearbeitet und wann keine geschäftlichen Informationen und Apps mehr verfügbar sein sollen. Dies ist ja bekanntlich bei iPhones nicht möglich, da bei Apple-Geräten dieses Konzept der auf Betriebssystemebene getrennten Profile nicht existiert und deswegen jede App nur einmalig auf dem Gerät installiert werden kann.

Fazit

Mit den Mechanismen von Android Enterprise können Organisationen nicht nur die Sicherheit erhöhen, sondern auch ihren Benutzern die Möglichkeit bieten, das Gerät zu verwenden, das sie bereits privat besitzen und die darauf verteilten Apps genau dann ein- und auszuschalten, wenn sie es möchten. In Zeiten der sozialen Medien, Kununu und Co. ist schliesslich eine hohe Mitarbeiterzufriedenheit ein nicht zu unterschätzender Faktor fürs Employer Branding und eine tiefe Fluktuationsrate.

DER AUTOR

Jonas Hofer
Mobile Security Engineer, Nomasis

Android ist mittlerweile ein Muss bei der Geräteadministration.

Den Artikel finden Sie auch online
www.netzwoche.ch