

Remote Support mit Mobile Device Management

Beim Betrieb mobiler Geräte in Unternehmen können technische Probleme auftreten. Um diesen zu begegnen, bietet ein MDM den Remote Support. In diesem E-Book erfahren Sie, wie Sie diesen zum Troubleshooting einsetzen können und User Errors per MDM verhindern.

User Errors mit MDM verhindern

Bei der Nutzung von Smartphones und Tablets kann es immer zu sogenannten User Errors (Nutzerfehlern) kommen. Mit einem MDM kann man diese oftmals verhindern und somit nicht nur die Arbeit erleichtern, sondern auch die Lebensdauer der Geräte erhöhen. Dafür werden im MDM verschiedene Richtlinien vergeben, die als Bedienvorgabe für die Geräte fungieren. Auf den folgenden Seiten gehen wir auf verschiedene Fehler ein und wie diese mit dem MDM behandelt werden können.



Technik- und Bedienfehler

Apps immer offen lassen

Laufen Apps immer im Hintergrund, kann dies die Performance des Gerätes verschlechtern.

Updates ignorieren

Sicherheits- oder Systemupdates werden oft verschoben oder ignoriert, was zu Sicherheitslücken oder Instabilitäten führen kann.

Kein Backup wichtiger Unternehmensdaten

Sollte das Gerät gestohlen oder unbenutzbar werden, sind ohne ein Backup in der Unternehmenscloud wichtige Daten weg.

Übermäßiger Speicherverbrauch

Zu viele Fotos, Videos, Apps oder große Datenmengen können den Speicher füllen und das Gerät verlangsamen.

Fehler in der App-Nutzung

Berechtigungen unüberlegt zustimmen

Werden Apps durch die Nutzer selbst heruntergeladen, werden oftmals Berechtigungen ohne weitere Überlegung erteilt. Dabei benötigen nicht alle Apps Berechtigungen für Kamera, Kontakte, Mikrofon usw.

Unbewusste In-App-Käufe

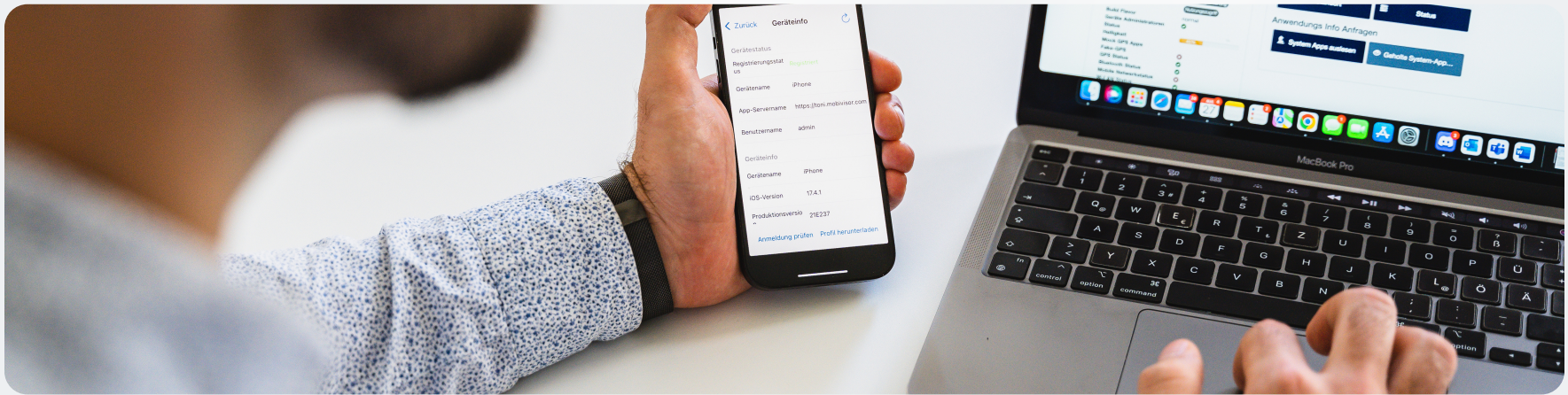
Nicht immer ist direkt ersichtlich, dass eine In-App-Funktion extra dazu gekauft werden muss. So können schnell erhöhte Kosten entstehen.

Wenig Bewusstsein für Datenschutz

Oftmals ist den Nutzer*innen mobiler Geräte nicht bewusst, wo ihre Daten überall erfasst und gesammelt werden. Gerade bei geschäftlichen Daten ist hier Vorsicht geboten.

Wie hilft Ihnen der MDM Remote Support beim Troubleshooting?

Ein MDM verfügt in der Regel über ein Remote Support Feature. Mit diesem kann der IT-Admin sich nach seiner Einwilligung auf den Bildschirm des Users schalten. So wird es möglich, bei Mitarbeitenden, die nicht vor Ort sind, eine erste Fehleranalyse durchzuführen. Zusätzlich ist es oftmals möglich, dass der Admin auch die Steuerung des mobilen Gerätes übernimmt. Außerdem kann man unter Remote Support auch die Möglichkeit verstehen, Befehle zu senden und Aktionen auf dem Gerät per MDM zu triggern.



Nutzerfehler mit Remote Support lösen

Apps immer offen lassen

Admins können im MDM den Stromverbrauch der Apps tracken. Als erste Lösung kann der Swipe-Kill aller im Hintergrund laufenden Apps remote durchgeführt werden.

Updates immer ignorieren

Im MDM kann die Version des installierten Betriebssystems eingesehen werden. Ist diese nicht aktuell, kann sie durch das MDM geupdated werden.

Kein Backup wichtiger Unternehmensdaten

Muss das Gerät zurückgesetzt werden, kann der Admin sich zuvor auf das Gerät schalten und für den User das Backup der Daten anstoßen, sofern dieser nicht weiß, wie das geht. Im Anschluss kann das Gerät per MDM auf Werkseinstellungen zurückgesetzt werden.

Nutzerfehler mit Remote Support lösen

Übermäßiger Speicherverbrauch

Im MDM kann eingesehen werden, wie viel Speicher auf dem Gerät belegt wird.

Falls ein Mitarbeitender diesen völlig ausnutzt und dadurch sich das Gerät verlangsamt oder heiß läuft, kann der Admin checken, ob es an zu vielen Fotos oder Videos liegt und diese ggf. löschen lassen.

Apps installieren sich nicht

In der MobiVisor MDM App kann vom Admin nachgeschaut werden, ob der User eingeloggt ist und eine Verbindung zum MDM hat.

Berechtigungen unüberlegt zustimmen

Per MDM lassen sich die Berechtigungen von Apps erteilen oder entziehen. Dies kann auf sehr granularer Ebene erfolgen, die weit über die Einstellungen auf dem Gerät selbst hinausgeht.

Nutzerfehler mit Remote Support lösen

Unbewusste In-App-Käufe

Über Richtlinien des MDMs lassen sich In-App-Käufe kategorisch verbieten (iOS). Alternativ wird der App Store bzw. der Play Store so konfiguriert, dass nur durch das MDM zugelassene Apps (ohne In-App Kaufoption) installiert werden können.

Wenig Bewusstsein für Datenschutz

Auf Geräten zur rein geschäftlichen Nutzung kann verboten werden, dass ein privater E-Mail-Account hinzugefügt wird, um zu verhindern, dass über diesen geschäftliche Daten in die falschen Hände gelangen. Durch einen strengen Spamfilter bei Unternehmens-Mails sinkt zudem die Wahrscheinlichkeit für Spam-Mails und Phishing.

Über die Autoren

Die IOTIQ GmbH ist ein internationales IT-Unternehmen mit Sitz in Leipzig. Seit 2017 bieten wir maßgeschneiderte Softwarelösungen, insbesondere für KMU an.

Unser Ziel: Die Digitalisierung in Deutschland vorantreiben – mit der besten Software für Ihr Smartphone. Unternehmen jeder Größe sollen von den Vorteilen der Digitalisierung profitieren können: von maßgeschneiderter App-Entwicklung bis zur Hardware-Beratung und -Beschaffung. Wir sind der Überzeugung, dass mobile Geräte der Schlüssel zum digitalen Vorankommen sind.

Die Autorin dieses Artikels ist Customer Care & Marketing Managerin bei der IOTIQ GmbH und zertifizierte Android-Expertin.



**Android
Enterprise**

Silver partner