

# Keine Angst vor verschwundenen Firmenhandys

Mit diesen **21 Tipps** sorgen Unternehmen für bestmögliche Datensicherheit bei Geräteverlust



Laut einer im Juli 2021 veröffentlichten Umfrage des Branchenverbandes Bitkom ist vier von zehn Personen schon mal das Handy abhandengekommen. 15 Prozent wurde das Gerät mindestens einmal gestohlen, 27 Prozent haben es bereits mindestens einmal verloren.

Was bei verlorenen Privathandys unangenehm ist, kann bei Firmenhandys schnell zu einem gravierenden Sicherheitsproblem werden.

Jede.r Unbefugte, dem.der das Gerät in die Hände fällt, kann unter bestimmten Voraussetzungen auf Firmendaten zugreifen. Dies gilt es unbedingt zu verhindern.

## Die Basis für den Schutz der Daten: Ein Mobile-Device-Management-System

Eine der essenziellen Voraussetzungen, um Datenverlust abzuwenden, also der **allerwichtigste Tipp**, ist der Einsatz eines Mobile Device Management Systems (MDM). **Nur mit einem MDM können zentral Richtlinien im Sinne der bestmöglichen Datensicherheit definiert und durchgesetzt werden, die dann im Einzelnen für einen Schutz Ihrer Daten sorgen.**

## **1. Passwort-Anforderungen definieren und durchsetzen**

Die IT-Abteilung kann im Administrationsportal definieren, welche Anforderungen das Passwort zum Entsperren des Smartphones oder Tablets erfüllen muss. Erfüllt der/die Mitarbeiter in diese Anforderungen nicht, kann er/sie das Gerät nicht in Betrieb nehmen. Ein sicheres Passwort besteht aus mindestens acht Zeichen und verwendet Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen. [Tipps zum Erstellen sicherer Passwörter finden Sie beim Bundesamt für Sicherheit in der Informationstechnologie \(BSI\).](#)

## **2. Bildschirmsperre auf mobilen Geräten aktivieren**

Ist das Gerät verloren, sollte man zunächst versuchen, es zu orten und wiederzubeschaffen. Sollte dies nicht möglich sein, kann man im Administrationsportal das Gerät auswählen und den Bildschirm sperren. Sinnvoll ist es, den Sperrbildschirm mit Kontaktdaten Ihres Unternehmens anzuzeigen, damit sich ehrliche Finder:innen bei Ihnen melden können.

## **3. Arbeitsbereich auf Android-Geräten sperren**

Im Verlustfall kann im Administrationsportal der gesamte Arbeitsbereich auf dem Android-Gerät zunächst gesperrt werden.

## **4. Mobile Geräte komplett zurücksetzen bzw. Arbeitsbereich entfernen**

Ist das Firmengerät ohne private Nutzungserlaubnis nicht wiederauffindbar und ganz sicher verloren gegangen, kann es im Administrationsportal auf Werkeinstellungen zurückgesetzt werden. Bei privaten Geräten ist dies selbstverständlich nicht möglich. Bei BYOD-Geräten, also privaten Geräten, die auch beruflich genutzt werden, kann dediziert der berufliche Bereich auf dem Gerät gelöscht werden.

## **5. Verbieten Sie die Anzeige von Benachrichtigungsinhalten auf dem Sperrbildschirm**

Über Benachrichtigungen auf dem Sperrbildschirm können Dritte Informationen über den Besitzer des Smartphones entnehmen (Beispiel: Eingehende Mails, Chat-Nachrichten). Derartige Notifikationen sollten daher verboten sein.

## **6. Passcode des mobilen Gerätes zurücksetzen**

Es kann sinnvoll sein, den Passcode eines Gerätes über das Administrationsportal zurückzusetzen, so dass das Gerät für Außenstehende nutzlos ist.

## **7. Verlustmodus für mobile Geräte aktivieren**

Mit *Verlustmodus aktivieren* können in der Konsole Geräte lokalisiert werden, auch wenn die Ortungsdienste am Gerät selbst ausgeschaltet sind. Das Gerät muss dafür lediglich eingeschaltet sein. Auch dies funktioniert nicht bei privaten Geräten.

## **8. Zwei-Faktor-Authentifizierung**

Nutzen Sie zur Absicherung zusätzlich auch die Zwei-Faktor-Authentifizierung Ihres eingerichteten Google- oder Apple-Kontos auf dem Gerät.

## **9. Nutzen Sie Apple Device Enrollment AED (früher DEP) und Zero Touch**

Wenn Sie AED und Zero Touch nutzen, stellen Sie sicher, dass die Geräte nur geschäftlich mit Ihrem MDM genutzt werden können und für Dritte auch nach einem Werksreset unbrauchbar sind.

## **10. Regelmäßige Sicherheits- und Betriebssystem-Updates durchführen**

Wenn möglich, erzwingen Sie die automatische Aktualisierung des Betriebssystems, um auch regelmäßige Sicherheitsupdates für das Gerät zu erhalten.

## **11. Aktivieren Sie in den Systemeinstellungen die Funktion „Mein Gerät finden“**

Sowohl bei Apple- als auch bei Android-Geräten kann man einen Dienst zum Auffinden des Gerätes aktivieren. Hier ist eine [Anleitung zum Suchen des iPhones](#) und hier eine [Anleitung, was zu tun ist, um das Android-Gerät orten zu können](#).

## **12. Automatische Bildschirmsperrezeit definieren/aktivieren**

Aktivieren Sie eine automatische Bildschirmsperre. So kann man beispielsweise einstellen, dass das Smartphone gesperrt wird, wenn es eine bestimmte Zeit lang nicht verwendet wurde. Wählen Sie diese Zeitspanne aber nicht zu niedrig, sonst behindert sie bei der Arbeit.

## **13. Maximale Anzahl fehlgeschlagener Anmeldungen festlegen**

Stellen Sie ein, nach wie vielen fehlgeschlagenen Versuchen das Gerät gesperrt und damit für Unbefugte unbrauchbar wird.

## **14. Aktivieren Sie Factory Reset Protection (FRP) (Android) und Activation Lock (Apple)**

Selbst wenn es einem Dritten möglich ist, das Gerät auf Werkseinstellungen zurückzusetzen, kann ein mit FRP geschütztes Gerät im Anschluss nicht mit einem privaten Google Account eingerichtet werden. Hier hilft auch die Nutzung von Android Zero Touch und DEP für Apple Geräte. Analog dazu kommt bei Apple der Activation Lock zum Einsatz. Der funktioniert analog und wird durch das Aktivieren von „Mein Gerät finden“ automatisch aktiviert.

## Weitere Tipps zur Sicherung Ihrer Geräte und Daten

### 15. Von Google empfohlene Android-Geräte einsetzen

Falls Sie sich für Android-Smartphones oder -Tablets entscheiden, sollten Sie unbedingt Geräte wählen, die auf der [Liste der für den Firmeneinsatz empfohlenen Geräte](#) stehen. Diese sind von Google geprüft und mit einem MDM-System gut und sicher zu verwalten.

### 16. Aufklärung der Mitarbeiter.innen

Machen Sie den Mitarbeiter.innen klar, dass bei einem Enterprise Remote Wipe die persönlichen Daten nicht gelöscht werden. So können Sie sicher sein, dass Ihnen ein Geräteverlust schneller gemeldet wird.

### 17. Führen Sie ggf. ein BYOD-Programm ein

Bei einem Bring-your-own-Device-Programm nutzen Mitarbeiter.innen ihre eigenen privaten Geräte beruflich und erhalten zum Ausgleich eine Beteiligung an den Gerätekosten oder Gebühren. Ein Vorteil in Sachen Sicherheit: Bei privaten Handys bemerken Mitarbeiter.innen den Verlust schneller und melden Ihnen diesen ohne Zeitverzögerung.

### 18. Geeignete Versicherung abschließen

Schließen Sie unbedingt eine geeignete Versicherung für Ihre Geräte ab.

### 19. Nutzung von Cloud-Diensten/Cloud-Speicher

Nutzen Ihre Mitarbeiter.innen Cloud-Dienste, sind die in der Cloud liegenden Daten auch im Falle des Geräteverlusts gesichert.

### 20. Betriebsvereinbarung mit Mitarbeiter.innen abschließen

Wenn Kolleg.innen mit Firmengeräten ausgestattet werden, sollten sie unbedingt eine Vereinbarung unterschreiben, in der der sicherheitsrelevante Umgang mit den Geräten geklärt ist. Solch ein Dokument sichert nicht nur das Unternehmen ab, sondern schärft zudem die Sensibilität der Mitarbeiter.innen für Sicherheitsthemen. So muss den Mitarbeiter.innen beispielsweise klar sein, dass sie einen Geräteverlust unverzüglich melden müssen. Wenn Sie einen Vertrag zum Thema BYOD abschließen möchten, können Sie gern unsere [kostenlose BYOD-Mustervereinbarung herunterladen](#).

## 21. Schützende Accessoires verwenden

Um das Gerät gegen Schäden zu schützen, sollten Sie Panzerfolien und passende Handyhüllen verwenden. Wenn Sie bei Cortado Firmengeräte kaufen oder mieten, machen wir Ihnen auch Vorschläge für geeignetes Zubehör.

Sie haben weitere Fragen zur Sicherung oder auch Verwaltung Ihrer Firmengeräte? Dann freuen wir uns über eine E-Mail an [sales@cortado.com](mailto:sales@cortado.com).

Sie wollen Cortado MDM kostenlos und unverbindlich testen? Dann nutzen Sie gern unseren [Demo-Link](#)

Sie möchten die Beschaffung und Einrichtung Ihrer Firmen-Handys und -Tablets in kompetente Hände legen? Dann machen wir Ihnen gern ein [Angebot](#).

