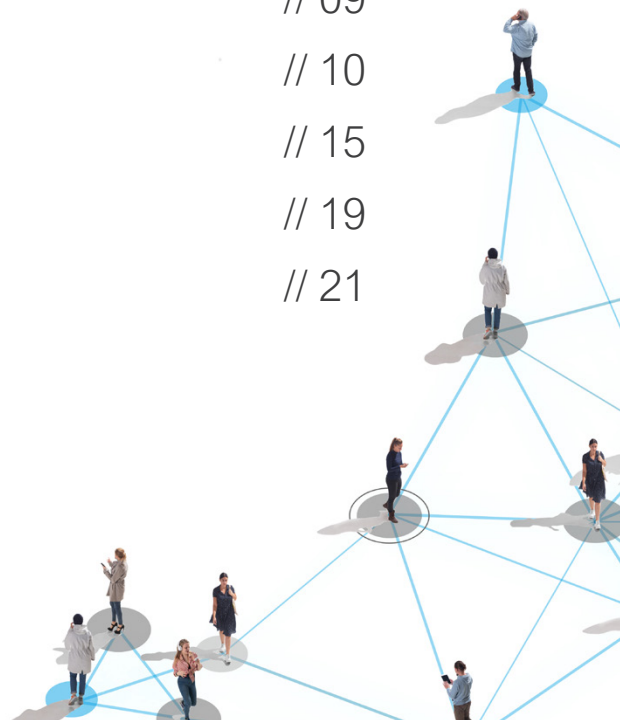
how to

WORAUF ES BEI BYOD UND COPE ANKOMMT – CHANCEN, HERAUSFORDERUNGEN & BEST PRACTICES

INHALT



BYOD & COPE

Die Chancen des New Normals mit einem modernen Gerätemanagement nutzen

Remote Work, überregionale Teams und flexible Arbeitszeiten: Die digitale Welt bietet für Unternehmen eine Vielzahl neuer Möglichkeiten. Dadurch verschwimmen auch die Grenzen zwischen Arbeit und Privatleben zunehmend. Mit Modellen, die den Einsatz mobiler Endgeräte sowohl für berufliche als auch für private Zwecke erlauben, erleichtern Unternehmen ihren Mitarbeitenden den Arbeitsalltag. Dies wirkt sich positiv auf ihre Zufriedenheit und Produktivität aus.

Jedoch steigen mit der Zahl mobiler Geräte wie Smartphones und Tablets auch die Risiken für Datenschutz und IT-Sicherheit. Um den Mitarbeitenden eine gleichermaßen sichere wie auch effektive Arbeitsumgebung zur Verfügung zu stellen, müssen Unternehmen das Gerätemanagement neu denken.

Zu den beliebtesten Modellen gehören BYOD und COPE. Wir erklären, um was es sich bei den beiden Modellen handelt, zeigen Vorteile, Herausforderungen und rechtliche Aspekte auf und beleuchten Best Practices, mithilfe derer die Implementierung einer modernen Geräteverwaltung zum Erfolg wird.

DEFINITION

DEFINITION

Was bedeutet BYOD und COPE überhaupt?

Bei „Bring your own Device” (BYOD) und „Corporate Owned, Personally Enabled” (COPE) handelt es sich um verschiedene Modelle für Unternehmen zur Geräteverwaltung. BYOD erlaubt es Mitarbeitenden, ihre privaten Geräte auch für berufliche Zwecke zu nutzen. Bei COPE werden die Geräte vom Unternehmen bereitgestellt, das den Mitarbeitenden erlaubt, diese auch privat zu nutzen. Bei beiden Modellen ist jedoch eine strikte Trennung zwischen privaten und geschäftlichen Daten erforderlich, um einen datenschutzkonformen Einsatz sicherzustellen.

VORTEILE UND HERAUSFORDERUNGEN

VORTEILE UND HERAUSFORDERUNGEN

Die beiden Modelle im Vergleich

Die Einführung von BYOD und COPE bedeutet mehr Flexibilität für die Mitarbeitenden. Sie haben die Möglichkeit, Geräte für ihre Arbeit zu nutzen, die zu ihren Vorlieben, ihrem Arbeitsstil und ihren Gewohnheiten passen und müssen nicht zwei Smartphones in ihrem Alltag jonglieren. Doch nicht nur für die Endnutzer birgt die berufliche und private Nutzung mobiler Geräte Vorteile. Mit einer flexiblen Nutzung von Smartphone & Co. können Unternehmen im War of Talents herausstechen und qualifizierte Mitarbeitende locken. Denn während in der Vergangenheit, die am häufigsten gestellte Frage in Vorstellungsgesprächen nach dem Firmenwagen war, haben heute das Arbeitsumfeld und die Arbeitsmittel einen weitaus höheren Stellenwert erlangt.

BYOD

Flexibel und einfach implementiert

Aufgrund der einfachen Implementierung hat sich BYOD bei vielen Unternehmen als der Weg des geringsten Widerstands für die Verwaltung mobiler Geräte durchgesetzt. Um die Kosten für die Anschaffung und Wartung der Geräte zu umgehen, überlassen Unternehmen den Erwerb dieser ihren Mitarbeitenden.

So sind die **VORTEILE** von BYOD ziemlich offensichtlich:

- **Hohe Anwenderzufriedenheit:** Die Mitarbeitenden können ihre Geräte selbst auswählen und haben in der Regel Kenntnisse über die Bedienung des Geräts.
- **Einfache Implementierung:** Der Gerätekauf sowie die Kosten für Netzbetreiber werden von den Mitarbeitenden getragen.
- **Gesteigerte Produktivität:** Mitarbeitende haben jederzeit Zugriff auf die geschäftlichen E-Mail-Konten und andere berufsbezogene Daten und Anwendungen.

BYOD ist jedoch nicht unproblematisch. In der Eile, ein modernes Gerätemanagement einzuführen, verzichten viele Unternehmen auf eine sorgfältige Evaluierung der Risiken und Fallstricke.

Denn BYOD birgt neben zahlreichen Vorteilen auch einige **Herausforderungen**:

- **Sicherheitsrisiken:** Wenig Kontrolle und erhöhte Anfälligkeit für Malware und Viren; Verloren gegangene oder gestohlene Geräte bergen die Gefahr eines unerwünschten Zugriffs auf sensible Unternehmensdaten.
- **Aufwendiger Support:** Die interne IT muss eine unbegrenzte Anzahl an Geräten und Betriebssystemen verwalten und sichern.
- **Versteckte Kosten:** Implementierung einer neuen Infrastruktur für die Geräteverwaltung, IT-Support und Anspruch auf Aufwendungsersatz bei Verlust oder Reparatur des Geräts können hohe Kosten mit sich bringen, die jedoch nur schwer kalkulierbar sind.
- **Haftung:** Bei Verlust des Geräts oder Datendiebstahl durch Sicherheitslücken, muss geprüft werden, inwieweit sich die Haftung auf den Arbeitnehmer oder den Arbeitsgeber erstreckt.

COPE

Hohe Datensicherheit und Kontrolle

Angesichts der eingeschränkten Kontrolle bei BYOD ist COPE eine praktikable Alternative, die Unternehmen die Möglichkeit gibt, unvorhergesehene Aufwände für mobile Geräte zu begrenzen und Sicherheitsrisiken zu minimieren.
Mit COPE liegt die Verantwortung für das Gerät beim Unternehmen selbst. In den meisten Fällen erstellt die IT-Abteilung eine Auswahl verfügbarer Geräte, aus der die Mitarbeitenden selbst wählen können. Diese werden dann gemäß den Sicherheitsrichtlinien des Unternehmens verwaltet.
Darüber hinaus nutzen viele Unternehmen Dienste für ein Mobile-Device-Management (MDM), um die Einhaltung von Vorschriften und die Überwachung der Gerätesicherheit im gesamten Unternehmen zu unterstützen, wobei alle Kosten für Geräte, Verwaltung, MDM-Dienste und Netzbetreiber vom Unternehmen übernommen werden.

COPE beseitigt also viele der Risiken, die mit BYOD verbunden sind, und bietet zusätzlich:

- **Gleichbehandlung der Mitarbeitenden:** Allen Mitarbeitenden steht die gleiche Auswahl an Geräten zur Verfügung.
- **Hohe Datensicherheit:** Unternehmen besitzen die Kontrolle über arbeitsrelevante Daten und können angemessene Vorkehrungen zu deren Schutz treffen.
- **Einfache Implementierung neuer Funktionen:** Ein modernes Gerätemanagement hilft dabei, die Geräte auf dem neusten Stand zu halten und erleichtert die Installation und Aktualisierung von Anwendungen.

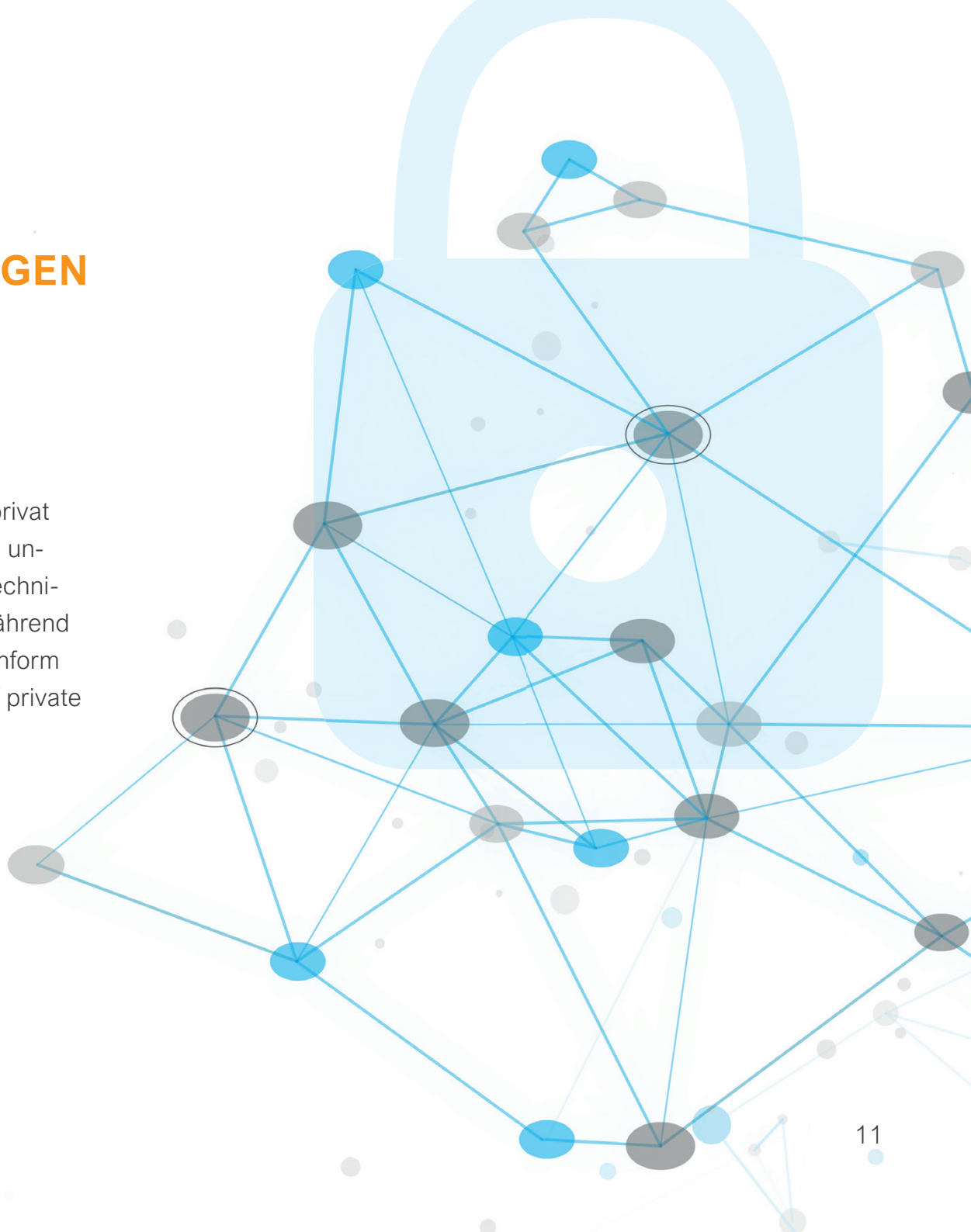
Durch die Kombination der Flexibilität von BYOD mit den Vorteilen von Unternehmenseigentum ist COPE eine Win-Win-Situation für Unternehmen und Mitarbeitende gleichermaßen.

RECHTLICHE GRUNDLAGEN

RECHTLICHE GRUNDLAGEN

Compliance & Datenschutz

Die Integration mobiler Geräte, die sowohl privat als auch geschäftlich genutzt werden, in die unternehmenseigene IT-Struktur wirft neben technischen auch einige rechtliche Fragen auf. Während geschäftliche Daten zentral und DSGVO-konform verwaltet werden müssen, ist der Zugriff auf private Daten für Unternehmen streng untersagt.



Schutz personenbezogener Daten

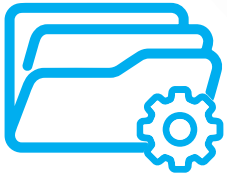
Die **DSGVO** stellt Unternehmen in die Pflicht, personenbezogene Daten von Kunden und Drittpersonen zu schützen. Sie sollten deshalb zu jeder Zeit Kontrolle über die geschäftlichen Daten, wie z.B. Dokumente und E-Mails, haben. Hierzu müssen sowohl technische als auch entsprechende organisatorische Maßnahmen getroffen werden, um die Erhebung, Verarbeitung und Nutzung der geschäftlichen Daten zu überwachen und die Anforderungen der Datenschutzgrundverordnung (DSGVO) zu gewährleisten. Private Daten müssen von der Kontrolle des Unternehmens jedoch ausgeschlossen bleiben.

Bei der Erstellung entsprechender **Regularien** sollte grundsätzlich berücksichtigt werden:

- **Welche Art** von Daten werden gespeichert?
- Wie werden die Daten **übertragen**?
- Wo bestehen **Risiken** für die IT-Sicherheit?
- Wie werden geschäftliche von privaten **Daten getrennt**?
- Wie wird mit **Support, Ausfall oder Verlust** des Geräts umgegangen?

Schutz des Geschäftsgeheimnisses

Cyberangriffe, Verlust des Geräts oder Diebstahl: Mobile Geräte bringen zahlreiche Gefahren mit sich. Aus diesem Grund müssen Unternehmen sicherstellen, dass Geschäftsheimnisse im Sinne von § 2 Nr. 1 Geschäftsgeheimnisgesetz nicht in die Hände von Unbefugten gelangen. Damit firmeneigenes Know-how geschützt werden kann, muss die IT-Abteilung entsprechende Sicherheitsmaßnahmen implementieren. Hierzu zählen unter anderen die **Verschlüsselung** von Daten bei der Übertragung von Dokumenten, Nachrichten, etc. sowie ein angemessener **Zugriffsschutz**.



Aufbewahrungspflichten

Eine weitere Rechtsgrundlage bezieht sich auf die steuerlich relevanten Aufbewahrungspflichten. Um die Grundsätze ordnungsgemäßer Buchführung und Dokumentation (GoBD) zu wahren, muss jegliche Kommunikation über die **geschäftlichen Kommunikationswege** abgewickelt werden. Damit wird verhindert, dass relevante Aufzeichnungen nicht zentral gespeichert und innerhalb der gesetzlichen Fristen aufbewahrt werden können.

Mitteilungspflichten

Um zu garantieren, dass bei Verlust oder Diebstahl eines geschäftlich genutzten Geräts zeitnah eine Fernlöschung sensibler Daten durchgeführt werden kann, lohnt es sich, den **Mitarbeitenden** eine **Mitteilungspflicht** aufzuerlegen. Dabei sollte auch sichergestellt sein, dass etwaige Meldepflichten des Unternehmens gemäß Art. 33 DSGVO erfüllt werden, sollte es zu einer Verletzung des Schutzes von personenbezogenen Daten kommen. Dies ist beispielsweise der Fall, wenn sich Dritte unbefugt Zugriff auf das Gerät verschaffen.

Haftung

Grundsätzlich ist der Arbeitgeber für die Umsetzung und Einhaltung der gesetzlichen Vorgaben verantwortlich. Besonders bei BYOD-Geräten ist dies jedoch mit einem hohen Risiko behaftet. Werden personenbezogene Daten auf privaten Endgeräten verarbeitet, können fehlende Updates oder das Umgehen von Sicherheitsmaßnahmen massive Gefahren nach sich ziehen. Deshalb empfiehlt es sich für Arbeitgebende ihre Mitarbeitenden in einer schriftlichen Vereinbarung auf ihre Pflichten und eine etwaige Arbeitnehmerhaftung hinzuweisen.

BEST PRACTICE: MDM, MAM & CONTAINER

Eine Vielzahl an Geräten, die sowohl privat als auch geschäftlich zum Einsatz kommen, erhöht neben der User Experience auch die Produktivität in Unternehmen. Allerdings bedeutet sie ein erhebliches Sicherheitsrisiko, wenn die Geräte nicht ordnungsgemäß verwaltet werden. Gehen mobile Endgeräte verloren, werden gestohlen oder gehackt, kann der Schutz sensibler Daten enorm kompromittiert werden. Auch bei der Installation unsicherer Anwendungen oder einem unregelmäßigen Updaten der Geräte, können Lücken in der IT-Sicherheit entstehen. Mithilfe von MDM-, MAM- und Container-Lösungen können diese Gefahren minimiert und eine sichere Verwaltung der Geräte gewährleistet werden.

Mobile Device Management

Je mehr mobile Geräte in Unternehmen zum Einsatz kommen, desto höher ist das Risiko, dass Sicherheitslücken entstehen oder Datenschutzrichtlinien nicht eingehalten werden. Um alle Geräte auf dem aktuellen Stand zu halten und sicher zu konfigurieren, helfen Mobile-Device-Management-Systeme (MDM). Bei MDM-Systemen handelt es sich um eine Software zur zentralen Verwaltung mobiler Endgeräte. Dabei wird die Konfiguration der Geräte regelmäßig mit der Zentrale abgeglichen, wodurch ein sicherer Betrieb gewährleistet wird. Wird eine Sicherheitslücke identifiziert oder eine nicht freigegebene Software installiert, kann der Administrator veranlassen, dass ein Gerät neu konfiguriert wird oder alle schützenswerten Daten von diesem entfernt werden. Hierfür können sogenannte Eskalationsregeln definiert werden, auf deren Grundlage die entsprechenden Maßnahmen ergriffen werden.

Mobile Application Management

Mit einem Mobile Application Management (MAM) haben Unternehmen die Möglichkeit, einzelne Apps auf geschäftlich genutzten Endgeräten bereitzustellen und zu verwalten, ohne direkten Zugriff auf das Gerät zu haben. Somit ist die Installation eines MAM-Systems sowohl auf privaten als auch betrieblichen Endgeräten möglich.
MAM-Systeme identifizieren risikobehaftete Apps und kritisches Datenverhalten und können so Sicherheitslücken und Datenschutzrisiken kalkulieren, ohne die Produktivität der Mitarbeitenden einzuschränken. Während im MDM die Sicherheitsanforderungen durch den Administrator in Form von gerätespezifischen Parametern definiert werden, kann das MAM Verstöße gegen Datenschutzbestimmungen, unkontrollierten Datenabfluss zu unternehmensfremden Servern und unzulässige Verbindungen sowie die unsichere Speicherung sensibler Daten auf App-Ebene steuern.
Diese Informationen werden dem MDM-System zur Verfügung gestellt, wodurch der Administrator die Möglichkeit hat, ein gezieltes App Risk Management durchzuführen. Im Anschluss können risikobehaftete Apps aus dem Unternehmensnetzwerk ausgeschlossen werden.

Containerisierung

Das reine Managen von Applikationen sorgt jedoch noch nicht für deren Sicherheit. Deshalb empfiehlt sich der Einsatz von Containerlösungen. Diese können schnell und kostengünstig im Unternehmen implementiert werden. Container haben den entscheidenden Vorteil, dass sie einzelne Anwendungen und Daten vollkommen von allen anderen Bereichen des Mobilgeräts isolieren. So können etwaige Schwachstellen am Gerät oder Fehler des Anwenders weitläufig eliminiert werden. Darüber hinaus werden ein unkontrollierter Datenabfluss oder die Manipulation der in den Apps gespeicherten Daten verhindert. Je nach Konfiguration der Containerlösung kann beispielsweise auch ein Copy&Paste der Daten verhindert werden, sodass diese nicht ohne weiteres aus der App kopiert und in einer anderen Anwendung gespeichert werden können.
Durch die Trennung von geschäftsrelevanten Inhalten und privaten Inhalten auf dem Gerät können diese gesichert und kontrolliert werden, ohne dass es zu Interaktionen oder Eingriffen in private Inhalte kommt.
Containerlösungen bringen jedoch auch Risiken mit sich. Viele sind der Ansicht, dass diese Lösungen in sich sicher sind. Dies ist jedoch nicht der Fall. Nur durch eine MDM- oder MAM-Lösung in Verbindung mit einer Containerisierung kann sichergestellt werden, dass wertvolle Daten geschützt werden, während die Privatsphäre des Anwenders gewahrt bleibt.

CHECKLISTE FÜR DIE IMPLEMENTIERUNG

CHECKLISTE FÜR DIE IMPLEMENTIERUNG

Modell für Gerätemanagement wählen
Zunächst muss geprüft werden, welches Modell für das Unternehmen geeignet ist. Hierzu sollten die Vor- und Nachteile sowie die Auswirkungen von eingeschränkter Kontrolle und Datenhoheit abgewogen werden.

Nutzungsrichtlinien definieren
Neben der strikten Trennung von privaten und beruflichen Daten, empfiehlt es sich für Unternehmen, klare Nutzungsrichtlinien zu etablieren, um Unklarheiten bei den Mitarbeitenden zu beseitigen und Risiken zu reduzieren.

Notfallplan erstellen
Ein IT-Notfallplan ist ein Handbuch, das wichtige Handlungsanweisungen und Maßnahmen beinhaltet, die im Eskalationsfall ergriffen werden.

MDM bzw. MAM implementieren
Mithilfe von MDM- und MDM-Systemen kann ein sicherer und datenschutzkonformer Einsatz des Geräts gewährleistet werden, ohne die private Nutzung einzuschränken.

Container auswählen
Containerapps ermöglichen im Zusammenspiel mit MDM- bzw. MAM-Systemen die Trennung geschäftlicher und privater Daten sowie die sichere und effiziente Verwaltung der Endgeräte, ohne die Usability für die Endnutzer einzuschränken.

Zugriffsschutz aktivieren
Um nicht autorisierte Zugriffe zu verhindern, sollten Sicherheitsvorkehrungen durch Passworteingabe bzw. Finger- oder Gesichtsscan eingerichtet werden.

Sensibilisierung der Mitarbeitenden
Die Mitarbeitenden sollten für die Gefahren, die die geschäftliche und private Nutzung mobiler Endgeräte birgt, sensibilisiert werden. In diesem Zug sollten sie beispielsweise darüber aufgeklärt werden, wie wichtig regelmäßige Updates sind und wie eine sinnvolle Passwortverwaltung umgesetzt werden kann.

Regelmäßige Updates einspielen
Die Geräte sollten regelmäßig auf die Aktualität ihrer Betriebssysteme hin geprüft werden. Mitarbeitende, die keine Updates durchgeführt haben, sollten daran erinnert werden, dies nachzuholen.

FAZIT

Welches Modell ist für mein Unternehmen am besten geeignet?

Wer viel Wert auf Datenschutz und geringe Sicherheitsrisiken legt, für den ist COPE wahrscheinlich die beste Lösung. Zwar scheint COPE mit höheren Kosten und Verwaltungsaufwänden verbunden zu sein, jedoch sind dies Investitionen, die sich für Unternehmen auszahlen und die Betriebssicherheit schützen. Auf der anderen Seite steht BYOD für einen Laissez-faire-Ansatz. Diese Freiheit hat jedoch ihren Preis, wie z.B. den Verlust des Überblicks über die Ausgaben für mobile Geräte, erhöhte Compliance- und Sicherheitsrisiken sowie eine eingeschränkte Kontrolle. Letztlich hängt die Entscheidung für BYOD oder COPE von der Bereitschaft ab, eine eigene interne Richtlinie für das Management mobiler Geräte zu implementieren und die laufenden Verwaltungsaufgaben zu übernehmen.

Mit MDM-Systemen stehen Unternehmen wertvolle Werkzeuge zur Verfügung, um geschäftliche und private Daten zu trennen und die Geräte auf dem neusten Stand zu halten.