Handbuch zur Umsetzung von BYOD-Richtlinien

Drei einfache Schritte zur legalen Verwaltung und Sicherung von privaten Mitarbeitergeräten in der IT-Umgebung eines Unternehmens

Absolute® Software

Wir möchten Sie nicht mit einer typischen Abhandlung darüber langweilen, dass Mitarbeiter in Zukunft immer mehr private Geräte in Unternehmensnetzwerken einsetzen werden. Wenn Sie dieses Dokument lesen, wissen Sie, dass BYOD (Bring Your Own Device – private Geräte am Arbeitsplatz) keine Zukunftsvision mehr ist, sondern bereits Realität.

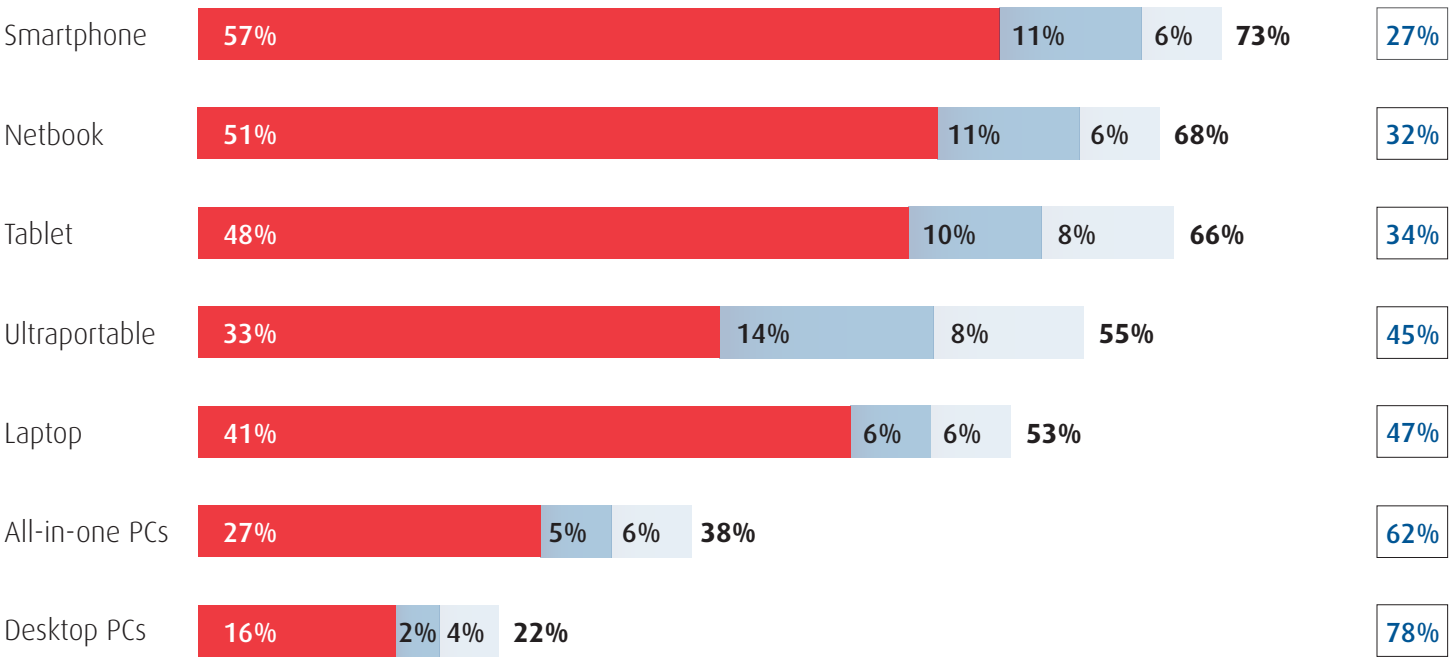
Das Ziel dieses Leitfadens besteht darin, Ihnen praktische, konkrete Maßnahmen an die Hand zu geben, um private Geräte effizient in Ihre Umgebung einzubinden und gleichzeitig sicherzustellen, dass Infrastruktur und Daten des Unternehmens sicher und geschützt bleiben.

SCHRITT 1 – DEFINIEREN SIE IHRE IT-ANFORDERUNGEN GERÄTE UND FORMFAKTOREN

Geräte und Formfaktoren

Im Folgenden finden Sie die Formfaktoren, die laut der Forrsights-Umfrage von Forrester Research, Inc. von Arbeitnehmern eingesetzt werden. Die Umfrage zeigt aktuelle Trends bei privaten Geräten von IT-Mitarbeitern am Arbeitsplatz, einschließlich der Option einer vollständigen oder teilweisen Kostenübernahme.

VIELE IT-MITARBEITER IN NORDAMERIKA/EUROPA WÄHLEN IHRE ARBEITSGERÄTE SELBST AUS UND TRAGEN DIE AUFWENDUNGEN DAFÜR SELBST



Befragte: IT-Mitarbeiter in Nordamerika und Europa

Quelle: Forrsights Workforce Employee Survey, 4. Quartal 2011

FORRESTER®

Zunächst müssen Sie die Geräte und Betriebssysteme festlegen, die Sie unterstützen möchten (und können). Eine standardisierte Verwaltung von mobilen Geräten ist nicht möglich, weil jedes Betriebssystem und sogar die Hardware selbst Einfluss auf die IT-Funktionen haben können. Im Folgenden finden Sie grundlegende Kriterien für Ihre Richtlinie für mobile Geräte, die Sie zur Bewertung von Betriebssystemen und Gerätetypen heranziehen können:

Sicherheit	• Integrierte Verschlüsselung • Identifizierung von Geräten mit Jailbreak und Rooting • Durchsetzbare Kennwörter • Geolocation-Funktionen • Remote-Sperrung / -Löschung
Verwaltbarkeit	• Eine API zur Verwaltung von mobilen Geräten und/oder Anwendungen • Erweiterte MDM-API über den Hardware-Anbieter • Unterstützung von Exchange ActiveSync-Richtlinien, die mit Unternehmensstandards konform sind
Apps	• Umfassende Auswahl kommerziell erhältlicher Produktivitäts-Apps • Support für die Entwicklung und Implementierung eigener Apps • Verfügbarkeit wichtiger, Formfaktor-spezifischer Apps

Mithilfe dieser Kriterien sollten Sie in der Lage sein, eine Liste mit Formfaktoren und Betriebssystemen zu definieren, die Sie unterstützen werden.

Netzwerkzugriff

Als Nächstes müssen Sie eine Umgebung implementieren, die eine Registrierung privater Geräte unterstützt. Die einfachste Lösung ist die Einrichtung eines vom internen Netzwerk getrennten Gast-WLANs. Dieses kann als Registrierungsnetzwerk für private Geräte dienen. Nach der Registrierung sollte Ihre MDM-Lösung anhand der von Ihnen erstellten Richtlinien automatisch die entsprechenden Berechtigungen und Einschränkungen zuweisen.

Zu den grundlegenden Berechtigungen gehören der Zugriff auf Unternehmens-E-Mails, das Unternehmens-Wi-Fi und VPN-Konfigurationen. Diese Berechtigungen sollten an eine Richtlinie gebunden sein, in der die Sicherheitsanforderungen des Unternehmens festgelegt sind. Geräte, die nicht den Sicherheitsrichtlinien entsprechen, sollten blockiert werden. Dazu gehören z. B.: Geräte mit Jailbreaks, Rooting oder verbotenen Anwendungen.

Eine Bereitstellung des Zugriffs über Ihre MDM-Lösung kommt sowohl Ihrer Organisation als auch Ihren Mitarbeitern zugute:

- Mitarbeiter erhalten unmittelbar Zugriff
- IT-Abteilung muss Geräte nicht manuell aktivieren
- Wi-Fi-Kennwörter werden nicht an Mitarbeiter weitergegeben
- Maßnahmen bei zukünftigen Sicherheitsverletzungen erfolgen automatisch, weil der Zugriff an die Sicherheitsrichtlinie gebunden ist

Verwaltungsrichtlinien

Der letzte Schritt zur Vorbereitung der IT-Umgebung bezieht sich auf Verwaltungsrichtlinien und Einschränkungen für private Geräte. Er lässt sich in drei grundlegende Aspekte aufteilen:

Richtlinienbasierte Verwaltung: Mitarbeiterinformationen sind bereits in Verzeichnissystemen wie Active Directory oder Open Directory organisiert, einschließlich Abteilungen, Standorte und Positionen. Sie können sich viel Zeit sparen, wenn Sie Ihre Geräterichtlinien an diesen Gruppierungen ausrichten.

Sicherheit: Erstellen Sie eine grundlegende Sicherheitsrichtlinie, die automatische Maßnahmen vorsieht, wenn Geräte nicht mehr konform sind. Weitere Kriterien wie z. B. Unternehmenskennwörter und App-Blacklists sollten identifiziert und implementiert werden.

Dokumentmanagement: Wenn Sie Mitarbeitern keine Möglichkeit zur Verfügung stellen, sicher auf Unternehmensdokumente zuzugreifen, werden sie nach einer eigenen Lösung suchen. Das beste Verfahren besteht darin, ein zentral verwaltetes Dokument-Repository einzurichten, in dem Dateiverfügbarkeiten nach Richtlinien bestimmt werden. Gleichzeitig hat die IT-Abteilung die Möglichkeit, Dateien gegebenenfalls zu löschen. Dies ist das beste Modell, um Unternehmensdaten zu sichern, gleichzeitig die Besitzverhältnisse von Geräten zu berücksichtigen und die Lösung benutzerfreundlich zu machen.

SCHRITT 2 – DEFINIEREN SIE IHRE RECHTLICHEN ANFORDERUNGEN

Die größte Herausforderungen einer BYOD-Lösung besteht darin, dass die IT-Abteilung zwischen einem angemessenen Umgang mit der Privatsphäre eines Mitarbeiters und der Sicherung des Unternehmensnetzwerks sowie der auf dem Gerät enthaltenen Daten abwägen muss.

Da es sich dabei im Wesentlichen um eine Form der Zusammenarbeit zwischen Mitarbeiter und Organisation handelt, ist die beste Lösung, die Bedingungen dafür schriftlich festzuhalten.

Richtlinie für mobile Geräte

Dabei handelt es sich um ein umfassendes Dokument, das die spezifischen Anforderungen Ihrer Organisation berücksichtigen sollte. Dabei sind Aspekte verschiedener interner Interessengruppen (z. B. Rechtsabteilung, IT-Abteilung, Personalabteilung und Mitarbeiter) zu berücksichtigen.

Jede Richtlinie wird individuell ausgestaltet, sollte aber im Allgemeinen einige oder alle der folgenden Aspekte umfassen:

Kriterien

- Definiert Verantwortlichkeiten
- Definiert Vorgehensweise bei Richtlinienverletzungen, einschließlich Konsequenzen
- Gibt vor allem allgemeine Standards vor, ohne auf Details wie Gerätetyp und Betriebssystem einzugehen
- Formuliert die Erwartung, dass Standards regelmäßig aktualisiert werden

Benutzer und Finanzierung

- Definiert, wie Geräte von Mitarbeitern verwendet werden
- Definiert, wie Mitarbeitern Sicherheitsanforderungen kommuniziert werden
- Legt fest, ob ein Technologie-Finanzierungsprogramm benötigt wird und woher die Mittel dafür stammen
- Definiert gegebenenfalls den Erstattungsvorgang für die laufenden Kosten von Mitarbeitern
- Support für Auftragnehmer, die ihre eigenen Geräte im Unternehmensnetzwerk verwenden

Rechtliches

- Durchsetzbarkeit
- Beschränkungen der der IT-Abteilung zur Verfügung stehenden Sicherheitsmaßnahmen durch regionale oder landesspezifische Datenschutzgesetze und Erfordernis von Einverständniserklärungen
- Rechte, Aktivitäten auf privaten Geräten zu prüfen und zu überwachen, und Einschränkungen dieser Rechte durch lokale Gesetze und Regulierungen
- Möglichkeit, bei der Haftung bezüglich der Verwendung von Funktionen, Lizenzen, Apps usw. zwischen Anwendern und der Organisation zu unterscheiden
- Einverständniserklärung, dass das Unternehmen zu geschäftlichen Zwecken auf das Gerät zugreifen kann
- Festlegung, wie sich Geräte aus dem System entfernen lassen und wie vertrauliche Daten und Unternehmens-Assets entfernt werden
- Verpflichtung des Mitarbeiters, einen Verlust des Geräts zu melden, und Recht des Arbeitgebers, alle Daten darauf zu löschen

Personalabteilung

- Details zur Kontrolle der auf Geräten von Mitarbeitern gespeicherten Unternehmensinformationen
- Richtlinien der Personalabteilung, die die Verwendung privater Geräte für den privaten Gebrauch während der Arbeitszeit und Nicht-Arbeitszeit sowie in der Arbeitsumgebung und Nicht-Arbeitsumgebung festlegensolute.com
- Vertragssprache zur Einbindung unabhängiger Auftragnehmer und Lieferanten und ihre Compliance mit der Richtlinie für mobile Geräte
- Mitarbeitersensibilisierung und Schulungen
- Details des Auszahlungsplans für Mitarbeiter, wenn diese das Gerät zunächst selber bezahlen und vom Arbeitgeber ratenweise erstattet bekommen

Vereinbarung über mobile Geräte von Arbeitnehmern

Dabei handelt es sich um ein einfacheres Dokument mit dem einzigen Zweck, das Einverständnis des Arbeitnehmers mit der Richtlinie des Unternehmens für mobile Geräte schriftlich einzuholen. Wenn der Arbeitnehmer die Bedingungen akzeptiert, erkennt er damit an, dass die IT-Abteilung das Recht und die Möglichkeit hat, das Gerät und die darauf enthaltenen Daten gegebenenfalls zu schützen. In Anhang A finden Sie ein Beispiel einer solchen Vereinbarung.

Es ist wichtig, dass Mitarbeiter der Vereinbarung aktiv zustimmen. Damit wird zukünftig vermieden, dass Mitarbeiter eine Kenntnis der Richtlinie abstreiten. Eine Zustimmung gibt der IT-Abteilung das Recht, Sicherheitsmaßnahmen einschließlich des Löschens einiger oder aller Daten auf dem Gerät durchzuführen und (je nach Ausführung der Unternehmensrichtlinie) das Gerät potenziell zu beschlagnahmen. Es ist daher wichtig, dass das Unternehmen sein Recht nachweisen kann, diese Art von Sicherheitsmaßnahmen durchzuführen.

Mitarbeitervereinbarungen sollten sicher aufbewahrt werden und bei Bedarf zur Verfügung stehen.

SCHRITT 3 – IMPLEMENTIEREN SIE DIE MDM MANAGEMENT SOFTWARE

Jetzt, da Ihnen sämtliche internen Anforderungen bekannt sind, müssen Sie eine geeignete Softwareanwendung auswählen, die es Ihnen ermöglicht, private und unternehmenseigene mobile Geräte auf geeignete Weise zu verwalten und zu sichern.

Ähnlich wie bei den Kriterien, die Sie angewandt haben, um verschiedene Betriebssysteme und Formfaktoren zu bewerten, müssen Sie sicherstellen, dass die von Ihnen gewählte Lösung einige grundlegende und zusätzliche Funktionen bereitstellen kann:

Plattformflexibilität	• Einfach in der vorhandenen Umgebung installierbar • Nutzt vorhandene Sicherheits- und Netzwerkinfrastruktur • Erfordert nur minimale Anpassungen • Konsolidierung: Kann alle IT-Formfaktoren und Betriebssysteme über eine einzige Konsole verwalten (idealerweise einschließlich Desktop- und Laptop-Computern)
Verwaltung	• Rollenbasierte Administration, sodass sich Techniker spezifischen Benutzergruppen mit definierten Verwaltungsberechtigungen zuweisen lassen
Verwaltung mobiler Apps	• Distribution innerbetrieblicher und kommerzieller Apps • Apps-Management-Funktionen zur Unterstützung und Automatisierung von Selbstbedienungsfunktionen für Anwender • Unterstützung für das Apple ASVPP-Programm (wenn Sie Apple Apps erwerben möchten)
Sicherheit	• Anwendung mehrerer Richtlinien pro Gerät, z. B. einer gemeinsamen grundlegenden Sicherheitsrichtlinie für alle Geräte, jedoch unterschiedlicher Berechtigungen oder Restriktionen je nach Abteilung und Nutzerrolle • Automatische Anpassung nicht konformer Geräte • Sichere Dokumentenweitergabe und -verwaltung • Remote-Funktionen zur Sperrung und Löschung • Unterstützung für Unternehmenskennwörter

ABSOLUTE MANAGE FÜR BYOD

Absolute® Manage für mobile Geräte hat die mit BYOD verbundenen Arbeitsabläufe für Mitarbeiter erfolgreich automatisiert.

Dadurch können IT-Administratoren auf eine manuelle Registrierung privater Mitarbeitergeräte und Erfassung einzelner Vereinbarungen, in denen jeder Mitarbeiter die Bedingungen der Richtlinien für mobile Geräte anerkennt, verzichten. Der Ablauf ist wie folgt:

1. Sobald ein Mitarbeiter ein Gerät registriert, erhält er eine Mitteilung auf dem Gerät, in der er gefragt wird, ob das Gerät dem Unternehmen oder dem Mitarbeiter gehört.
2. Sollte das Gerät dem Mitarbeiter gehören, erscheint die Vereinbarung über mobile Geräte von Mitarbeitern auf dem Bildschirm. Der Mitarbeiter muss die Vereinbarung lesen und die Option „Zustimmen" wählen, um mit der Registrierung fortzufahren.
3. Der Mitarbeiter erhält anschließend eine Bestätigungs-E-Mail, in der seine Zustimmung zu den Bedingungen bestätigt wird. Diese E-Mail enthält zudem weitere Informationen zur Richtlinie des Unternehmens für mobile Geräte. Eine Kopie dieser E-Mail geht gegebenenfalls an die Personalabteilung, die die Kopie in der jeweiligen Mitarbeiterakte ablegt.
4. Nachdem das Gerät als privat identifiziert ist, lassen sich BYOD-spezifische Richtlinien und Profile automatisch und unmittelbar auf dem Gerät installieren.

ist eine Lebenszyklusmanagement- und Mobilgerätelösung, mit der IT-Administratoren PC-, Mac®-, iOS-, Android- und Windows®-Mobiltelefone von einer einzigen Konsole aus verwalten können. Kunden können ihre Implementierung per Fernzugriff ansteuern und typische Wartungsaufgaben erledigen sowie strategische und taktische Maßnahmen für jedes verwaltete Gerät ergreifen.

Weitere Informationen über Absolute Manage für mobile Geräte finden Sie unter:
www.absolute.com/mdm

Anhang A

VEREINBARUNG ÜBER MOBILE GERÄTE VON ARBEITNEHMERN

Diese Vereinbarung ist rechtlich bindend und gerichtlich durchsetzbar. Im Gegenzug dafür, dass das Unternehmen Ihnen gestattet, Ihr privates Gerät in unserer Unternehmensumgebung einzusetzen, stimmen Sie den folgenden Bedingungen zu:

Ihre Zustimmung zu dieser Vereinbarung ist eine Bedingung dafür, dass Sie Ihr privates Gerät in unserer Unternehmensumgebung einsetzen dürfen. Sie erklären sich zudem damit einverstanden, die Richtlinie des Unternehmens für mobile Geräte (URL ergänzen) und jegliche von Zeit zu Zeit eingeführten Ergänzungen und Änderungen einzuhalten. Die Richtlinie für mobile Geräte ist Teil dieses Vertrags.

Sollte Ihr Gerät verloren gehen oder gestohlen werden, sind Sie verpflichtet, diesen Verlust umgehend per E-Mail (E-Mail ergänzen) oder Telefon (Tel. ergänzen) an (Nachrichtenempfänger ergänzen) zu melden.

Bedingungen, die Sie kennen sollten:

- Das Unternehmen kann während des Zeitraums, in dem das Gerät registriert ist, auf alle auf Ihrem privaten Gerät gespeicherten Informationen, Anwendungen und Daten zugreifen. Sie stimmen einem solchen Zugriff im Rahmen der Datenschutzrichtlinien des Unternehmens unwiderruflich zu, bis Ihr privates Gerät aus dem Programm entfernt wird.
- Das Unternehmen ist berechtigt, Daten (einschließlich persönlicher Daten, sofern notwendig) auf privaten Geräten gegebenenfalls per Fernzugriff zu löschen. Dies kann aus Sicherheitsgründen geschehen, oder wenn das Arbeitsverhältnis vom Arbeitgeber oder Arbeitnehmer gekündigt wird.
- Im Fall einer Verletzung der Richtlinie des Unternehmens für mobile Geräte hat das Unternehmen das Recht, u. a. die folgenden Maßnahmen zu ergreifen:
    - Spezielle Schulungen, um Ihnen ein Verständnis für die Sicherheitsmaßnahmen zu vermitteln
    - Entziehung der Berechtigungen für mobile Geräte
    - Einziehung des Geräts und/oder Löschung des Geräts per Fernzugriff
    - Beendigung des Arbeitsverhältnisses

Das Gerät muss den Richtlinien des Unternehmens für mobile Geräte entsprechen, damit der Mitarbeiter zum Zugriff auf das Unternehmensnetzwerk, E-Mails, Adressbuch und andere Unternehmensinformationen berechtigt ist.

Sollten Sie Ihr privates Gerät nicht mehr in unserer Unternehmensumgebung einsetzen möchten, müssen Sie sich an (Kontakt ergänzen) wenden, um das Gerät entfernen zu lassen. Das Unternehmen kann alle auf Ihrem privaten Gerät enthaltenen Informationen löschen, bevor das private Gerät aus dem Programm entfernt wird.

(Zustimmen) Ich habe die Richtlinie des Unternehmens für mobile Geräte gelesen und stimme dieser zu. Ich bin mit den Bedingungen einverstanden und möchte mit der Registrierung meines privaten Geräts fortfahren.