ZEHN GRUNDLEGENDE ÜBERLEGUNGEN ZU BYOD

MaaS360
by Fiberlink

MaaS360® by Fiberlink, an IBM company

Zulassen von BYOD im Unternehmen

Die zunehmende Verbreitung von Mobilgeräten am Arbeitsplatz erscheint vielen IT-Führungskräften als Naturgewalt. Es ist, als ob sämtliche Mitarbeiter bestrebt sind, sich möglichst viele Geräte zu kaufen und diese mit Unternehmensdiensten zu verbinden. Bring Your Own Device (BYOD) setzt sich immer weiter durch, und die Mitarbeiter sind begeistert.

Es erscheint wenig sinnvoll, die Augen vor dieser Entwicklung zu verschließen oder sie zu unterbinden. Ihre Mitarbeiter nutzen im Unternehmensnetzwerk bereits eigene, nicht richtlinienkonforme Geräte, und dies wird auch in Zukunft so sein, mit oder ohne Ihrer Erlaubnis. Einer Studie von Forrester zufolge nutzen 37 % aller IT-Beschäftigten in den USA Technologien, bevor für diese formale Genehmigungen oder Richtlinien vorliegen.[1] Des Weiteren ergab eine Umfrage von Gartner CIO, dass bis 2016 80 % aller Beschäftigten zur Nutzung eigener Geräte mit privaten Daten berechtigt sein werden.[2]

Damit wird eine Frage unumgänglich: Wie lässt sich dem Bedürfnis der Belegschaft nach der Verwendung persönlicher Apps und Geräte Rechnung tragen und gleichzeitig die Produktivität und der Schutz von Unternehmensdaten in einer sicheren Umgebung gewährleisten? In zehn grundlegenden Überlegungen zu BYOD erfahren Sie, wie Sie eine störungsfreie, sichere und produktive mobile Umgebung bereitstellen.

Zehn grundlegende Überlegungen zu BYOD

1. Erstellen Sie vor dem Erwerb neuer Technologien entsprechende Richtlinien
2. Verschaffen Sie sich einen Überblick über die Geräte der Belegschaft
3. Sorgen Sie für eine einfache Anmeldung
4. Konfigurieren Sie Geräte per Fernzugriff
5. Ermöglichen Sie Benutzern eine selbständige Verwaltung
6. Schützen Sie persönliche Daten
7. Trennen Sie Unternehmens- von privaten Daten
8. Sorgen Sie für eine automatische Kontrolle
9. Verwalten Sie die Datennutzung
10. Behalten Sie den ROI im Auge

[1] Benjamin Gray und Christian Kane, „Fifteen Mobile Policy Best Practices“, Forrester Research, Januar 2011.

[2] Ken Dulaney und Paul DeBeasi, „Managing Employee-Owned Technology in the Enterprise“, Gartner Group, Oktober 2011.

MaaS360® by Fiberlink, an IBM company

1. Erstellen Sie vor dem Erwerb neuer Technologien entsprechende Richtlinien

Bei allen IT-Projekten sollten vor dem Einsatz der Technologie die jeweiligen Richtlinien festgelegt werden – auch bei Cloud-Projekten. Um eine effektive Nutzung der Mobile Device Management (MDM)-Technologie für mitarbeitereigene Geräte sicherzustellen, bedarf es klarer Richtlinien. Die Auswirkungen dieser Richtlinien gehen weit über die IT hinaus. Sie betreffen die Personal-, Rechts- und Sicherheitsabteilung – also jeden Geschäftsbereich, in dem zu Produktivitätszwecken Mobilgeräte Verwendung finden.

Da BYOD-Richtlinien für alle Unternehmensbereiche gelten, muss die IT das ganze Unternehmen im Auge behalten. Die IT sollte alle Abteilungen in die Richtlinienerstellung einbeziehen, um den vielfältigen Anforderungen gerecht zu werden.

Jede BYOD-Richtlinie ist anders. Die folgenden Fragen bieten Ihnen jedoch einen guten Ausgangspunkt:

- **Geräte**: Welche Mobilgeräte werden unterstützt? Sollen nur bestimmte Geräte oder jegliche Mitarbeitergeräte zugelassen werden?

Der Forrester-Studie zufolge gehören 70 % aller Smartphones den Benutzern selbst, 12 % werden aus einer genehmigten Liste ausgewählt und 16 % werden vom Unternehmen zur Verfügung gestellt. Bei Tablets sind es 65 % benutzereigene Geräte, 15 % werden aus einer Liste ausgewählt und 16 % stammen vom Unternehmen. Anders ausgedrückt: Benutzer verwenden in der Regel ihre eigenen Geräte.

- **Datentarife:** Übernimmt das Unternehmen den Datentarif? Wenn ja, gibt es eine allgemeine Vergütung oder muss der Mitarbeiter eine Spesenabrechnung einreichen?

Wer übernimmt die Kosten für Geräte? Im Fall von Smartphones bezahlten 70 % der Mitarbeiter den vollen Preis, 12 % erhielten einen Rabatt, 3 % zahlten einen Anteil, und bei 15 % der Geräte übernahm das Unternehmen die Kosten vollständig. Bei Tablets erwarben 58 % der Mitarbeiter ihr eigenes Gerät, 17 % erhielten einen Rabatt, 7 % teilten sich die Kosten mit dem Unternehmen, und 18 % wurden von ihren Unternehmen ohne Zuzahlung ausgestattet. (Quelle: Forrester, 2011)

- **Konformität:** Welchen Auflagen unterliegen die zu schützenden Daten Ihres Unternehmens? Beispielsweise ist gemäß des Health Insurance Portability and Accountability Act (HIPAA) auf jedem Gerät mit Daten eine systemeigene Verschlüsselung erforderlich.
- **Sicherheit:** Welche Sicherheitsmaßnahmen sind erforderlich (Passcode-Schutz, Jailbreak-/Root-Erkennung, Antischadsoftware-Apps, Verschlüsselung, Gerätebeschränkung, iCloud-Backup)?
- **Anwendungen:** Welche Apps sind unzulässig? IP-Scanning, Datenfreigabe, Dropbox?
- **Vereinbarungen:** Gibt es ein Acceptable Usage Agreement (AUA) für Mitarbeitergeräte mit Unternehmensdaten?
- **Dienste:** Auf welche Ressourcen dürfen Mitarbeiter zugreifen (z. B. E-Mail)? Wie verhält es sich mit bestimmten Drahtlosnetzwerken oder VPNs? CRM?
- **Datenschutz:** Welche Daten werden von Mitarbeitergeräten erfasst? Welche persönlichen Daten sollen nicht erfasst werden?

Im Zusammenhang mit BYOD sollten Sie Fragen umfassend klären. Fördern Sie einen offenen und ehrlichen Dialog über die Gerätenutzung und die Möglichkeiten der IT, die einzelnen Anforderungen zu erfüllen.

MaaS360® by Fiberlink, an IBM company

2. Verschaffen Sie sich einen Überblick über die Geräte der Belegschaft

Stellen Sie sich folgendes Szenario vor. Zu Beginn Ihrer MDM-Lösung steht die Annahme, dass Ihr Unternehmen etwa 100 Geräte unterstützt. Sie haben sorgfältig alle Gerätetypen und Benutzer erfasst – es sollte also keine Überraschungen geben. Bei dem ersten Bericht werden jedoch über 200 Geräte angezeigt. Dies ist ein realistisches Szenario. Ein vergleichbarer Fall tritt viel öfter ein, als Sie vermuten.

Seien Sie sich dieser Tatsache bewusst. Fehlende Informationen können weitreichende Folgen haben. Verschaffen Sie sich zunächst einen Überblick über die in Ihrem Unternehmen vorhandenen Mobilgeräte, bevor Sie verbindliche Strategien entwickeln. Dazu benötigen Sie ein Tool, das in Echtzeit mit der E-Mail-Umgebung kommuniziert und alle mit dem Unternehmensnetzwerk verbundenen Geräte ermittelt. Sobald ActiveSync für eine Mailbox aktiviert wurde, können mehrere Geräte ohne IT-Fachkenntnisse synchronisiert werden.

Alle Mobilgeräte sollten integriert werden. Außerdem müssen deren Besitzer auf das Inkrafttreten neuer Sicherheitsrichtlinien hingewiesen werden.

3. Sorgen Sie für eine einfache Anmeldung

Komplexität führt besonders schnell zu Nichtkonformität. Ihr BYOD-Programm sollte über eine Technologie verfügen, die eine einfache und benutzerfreundliche Geräteanmeldung ermöglicht. Der Vorgang sollte einfach und sicher durchzuführen sein und gleichzeitig eine geeignete Gerätekonfiguration sicherstellen.

In einem idealen Szenario sollten Benutzer per E-Mail einen Link oder eine Anleitung zu einem auf dem Gerät erstellten MDM-Profil erhalten – einschließlich Annahme des wichtigen AUA.

> Wenn BYOD das Ziel ist, stellt das AUA eine wichtige Vereinbarung auf dem Weg zu diesem Ziel dar.

Die Anweisungen sollten vorhandenen Benutzern die Anmeldung beim BYOD-Programm erleichtern. Vorhandenen Benutzern wird empfohlen, alle ActiveSync-Konten zu löschen, damit Unternehmensdaten auf dem jeweiligen Gerät isoliert und getrennt verwaltet werden können. Neue Geräte sollten mit einem neuen Profil gestartet werden.

Aus Perspektive der IT sollte entweder die Möglichkeit bestehen, mehrere Geräte auf einmal anzumelden, oder Benutzer sollten ihre Geräte selbst registrieren können. Außerdem sollten Sie für Mitarbeiter einen grundlegenden Authentifizierungsprozess bereitstellen, beispielsweise über einen Einmal-Passcode, oder vorhandene Unternehmensverzeichnisse wie Active Directory/LDAP nutzen. Alle neuen Geräte sollten beim Zugriff auf Unternehmensressourcen zunächst isoliert und der IT gemeldet werden. Auf diese Weise kann die IT das betreffende Gerät sperren oder nach der Genehmigung den entsprechenden Anmeldungsworkflow starten, der die Konformität mit Unternehmensrichtlinien gewährleistet.

MaaS360® by Fiberlink, an IBM company

4. Konfigurieren Sie Geräte per Fernzugriff

Sie sollten auf jeden Fall vermeiden, dass durch Ihre BYOD-Richtlinie und die MDM-Lösung mehr Benutzer auf die Supportabteilung angewiesen sind als zuvor. Alle Geräte sollten per Fernzugriff konfiguriert werden, was sowohl für die IT als auch für Geschäftsnutzer eine maximale Effizienz bietet.

Sobald ein Benutzer das AUA angenommen hat, sollten über Ihre Plattform alle Profile, Anmeldedaten und Einstellungen bereitgestellt werden, die der Mitarbeiter benötigt, darunter:

- E-Mail, Kontakte und Kalender
- VPN
- Unternehmensdokumente und -inhalte
- Interne und öffentliche Apps

An diesem Punkt sollten Sie zudem Richtlinien für den Zugriff auf bestimme Anwendungen sowie Warnungen erstellen, die eingeblendet werden, sobald ein Benutzer sein monatliches Datennutzungs- oder Kostenlimit überschreitet.

5. Ermöglichen Sie Benutzern eine selbständige Verwaltung

Sie werden es Ihnen danken. Benutzer sind auf funktionierende Geräte angewiesen, und Sie wünschen sich eine effiziente Supportabteilung. Über eine stabile Selbstbedienungsplattform können Benutzer folgende Aufgaben direkt durchführen:

- Zurücksetzen der PIN und des Kennworts, falls sie die aktuellen Informationen vergessen
- Ortung eines verlorenen Geräts über ein Webportal mit Kartenintegration
- Löschen eines Geräts und Entfernen aller sensiblen Unternehmensdaten per Fernzugriff

Sicherheit, Schutz der Unternehmensdaten und Konformität unterliegen unterschiedlichen Verantwortlichkeiten. Mitarbeiter müssen verstehen, dass Sicherheitsrisiken nur mit ihrer Kooperation vermindert werden können. In einem Selbstbedienungsportal können Mitarbeiter mögliche Nichtkonformitäten besser erkennen.

MaaS360® by Fiberlink, an IBM company

6. Schützen Sie persönliche Daten

Selbstverständlich wird durch eine geeignete BYOD-Richtlinie nicht nur der Schutz von Unternehmensdaten geregelt. Die Sicherheit von Mitarbeiterdaten genießt ebenfalls Priorität. Mithilfe personenbezogener Daten (Personally Identifiable Information, PII) lassen sich Personen identifizieren, kontaktieren und orten. Durch einige Datenschutzregelungen ist es Unternehmen untersagt, diese Daten auch nur anzuzeigen. Setzen Sie Ihre Mitarbeiter über die entsprechenden Datenschutzregelungen in Kenntnis, und verdeutlichen Sie, welche Daten auf Mobilgeräten nicht erfasst werden. Eine MDM-Lösung sollte in der Lage sein, zu analysieren, auf welche Informationen zugegriffen werden kann und auf welche nicht. Zu letzteren zählen etwa:

- Persönliche E-Mails, Kontakte und Kalender
- Anwendungsdaten und SMS
- Anrufverlauf und Voicemails

Setzen Sie Benutzer darüber in Kenntnis, welche Daten erfasst und wie diese verwendet werden und welche Vorteile daraus für die Benutzer entstehen.

Bei einer fortschrittlichen MDM-Lösung lässt sich die allgemeine Datenschutzrichtlinie mittels individueller Datenschutzeinstellungen anpassen, sodass geräteinterne Informationen zu Standort und Software ausgeblendet werden. Auf diese Weise entsprechen Unternehmen den PII-Bestimmungen, und persönliche Informationen von Mitarbeitern können auf Smartphones und Tablets nicht angezeigt werden. Zu diesen Einstellungen zählen beispielsweise:

- Deaktivieren von App-Bestandsberichten, um Administratoren die Einsicht in persönliche Anwendungen zu verwehren
- Deaktivieren von Standortdiensten, um den Zugriff auf Standortindikatoren wie Anschrift, geographische Koordinaten, IP-Adresse und WiFi SSID zu unterbinden

Wichtige Aspekte hierbei sind Transparenz und Klarheit. Wenn alle Voraussetzungen bekannt sind, steigt die Akzeptanz gegenüber der BYOD-Richtlinie.

7. Trennen Sie Unternehmens- von privaten Daten

Damit sowohl die IT als auch die Endbenutzer mit der Vereinbarung bezüglich BYOD zufrieden sind, sollten persönliche Daten wie Geburtstagsfotos oder die private Lektüre und Produktivitäts-Apps voneinander isoliert werden.

Vereinfacht lässt sich festhalten, dass im Falle eines ausscheidenden Mitarbeiters Apps, Dokumente und andere Materialien des Unternehmens von der IT geschützt werden müssen, während dessen persönliche E-Mails, Apps und Fotos unangetastet bleiben sollten.

Nicht nur die Benutzer werden diesen Ansatz zu schätzen wissen. Auch für die IT ergeben sich klare Vorteile. Mit diesem Ansatz lassen sich Unternehmensdaten selektiv löschen, wenn ein Mitarbeiter das Unternehmen verlässt. Im Falle eines Geräteverlusts können unter Umständen auch sämtliche Daten gelöscht werden. Diese Optionen stehen Ihnen jedoch nur bei einer echten MDM-Lösung zur Verfügung.

86 % der Löschvorgänge auf Geräten sind selektiv. Dabei werden nur Unternehmensdaten gelöscht.

MaaS360® by Fiberlink, an IBM company

8. Sorgen Sie für eine automatische Kontrolle

Sobald ein Gerät angemeldet ist, sollten die Rahmenbedingungen geklärt werden. Geräte sollten kontinuierlich hinsichtlich bestimmter Szenarien überprüft werden. Hierfür bieten sich automatisierte Richtlinien an. Versucht der Benutzer das Management zu deaktivieren? Entspricht das Gerät der Sicherheitsrichtlinie? Müssen auf Grundlage der vorliegenden Daten Anpassungen vorgenommen werden? Ausgehend von diesen Fragen können Sie ggf. zusätzliche Richtlinien und Regeln erstellen. Zu den relevanten Aspekten zählen folgende:

- **Jailbreak- und Root-Erkennung:** Gelegentlich versuchen Mitarbeiter mittels Jailbreak oder Root kostenlos an zahlungspflichtige Apps zu gelangen. Dadurch werden Geräte anfälliger für Datendiebstahl durch Schadsoftware. Bei einem Jailbreak-Versuch sollte die MDM-Lösung in der Lage sein, sofortige Maßnahmen wie das selektive Löschen von Unternehmensdaten auf dem entsprechenden Gerät einzuleiten.
- **SMS-Benachrichtigung vor Löschvorgängen:** Die Nutzung zeitintensiver Apps wie Angry Birds entspricht nicht den Unternehmensrichtlinien, stellt jedoch keinen klaren Verstoß dar. In diesem Fall sollte das Löschen von Daten aufgeschoben werden. Mit einer MDM-Lösung lassen sich Richtlinien individuell durchsetzen. Über das MDM kann dem Benutzer eine Nachricht mit einer Frist zum Entfernen der entsprechenden Anwendung gesendet werden, bevor die IT alle Daten löscht.
- **Verfügbarkeit eines neuen Betriebssystems:** Um ein dauerhaft effektives BYOD-Programm sicherzustellen, müssen Benutzer über die Verfügbarkeit eines neuen Betriebssystems informiert werden. Mit der passenden MDM-Lösung lassen sich Betriebssystemupgrades selbständig durchführen. Indem veraltete Betriebssystemversionen eingeschränkt werden, lässt sich die Konformität sowie die optimale Gerätefunktion sicherstellen.

9. Verwalten Sie die Datennutzung

Mithilfe einer BYOD-Richtlinie wird die IT-Abteilung weitgehend von der unternehmensinternen Kommunikation freigestellt. In den meisten Unternehmen benötigen Mitarbeiter jedoch weiterhin Unterstützung beim Verwalten der Datennutzung und Vermeiden übermäßiger Kosten.

Wenn Sie die Kosten eines Datentarifs tragen, möchten Sie möglicherweise auch wissen, wozu die Daten genutzt werden. Bezahlen Sie den Tarif nicht, möchten Sie u. U. die Benutzer bei der Nachverfolgung der Datennutzung unterstützen. Sie sollten in der Lage sein, sowohl netzwerkinterne als auch auf Roaming basierende Datennutzung nachzuverfolgen und Warnungen zu erstellen, wenn ein Benutzer einen Schwellenwert bei der Datennutzung überschreitet.

Sie können Grenzwerte sowohl für netzwerkinterne als auch roamingbasierte Datennutzung festlegen und den Abrechnungstag anpassen, um so Benachrichtigungen gemäß des in Anspruch genommenen Prozentsatzes zu erstellen. Wir empfehlen außerdem, die Benutzer über die Vorteile der Nutzung von verfügbaren WiFi-Netzen in Kenntnis zu setzen. Durch automatische WiFi-Konfiguration wird gewährleistet, dass Geräte an Unternehmensstandorten automatisch eine Verbindung mit dem entsprechenden WiFi-Netz herstellen.

Wenn der Tarif nur eine Datennutzung im Wert von 50 US-Dollar bzw. im Umfang von 200 MB umfasst, ist für Mitarbeiter ein Warnhinweis bei Erreichen des Limits hilfreich.

MaaS360® by Fiberlink, an IBM company

10. Behalten Sie den ROI im Auge

Auch wenn durch das BYOD-Prinzip Geräte von Mitarbeitern erworben werden, sollten Sie Zusammenhänge und langfristigen Kosten für Ihr Unternehmen im Auge behalten.

Bedenken Sie bei der Richtlinienerstellung stets die Auswirkungen auf den ROI. In der folgenden Tabelle finden Sie eine Gegenüberstellung der wesentlichen Aspekte:

Unternehmenseigenes Modell	BYOD
Ausgaben für jedes einzelne Gerät	Anteilige Kosten für einen Datentarif
Vollständige Kosten für einen Datentarif	Keine Kosten für den Geräteerwerb
Kosten für das Geräterecycling im Abstand weniger Jahre	Kosten für eine Plattform zur Mobilgerätverwaltung
Garantievereinbarungen	
Arbeits- und Zeitaufwand seitens der IT zur Programmverwaltung	

Eine allgemeine Lösung kann in einzelnen Punkten kleinere Schwächen aufweisen. Eine sorgfältig entwickelte BYOD-Richtlinie ermöglicht Ihnen jedoch die effektive und effiziente Verwaltung von Mobilgeräten.

Produktivitätszuwächse entstehen bekanntlich häufig bei jederzeit mobilen und vernetzten Mitarbeitern. Dank BYOD profitieren von dieser gesteigerten Produktivität jetzt auch neue Benutzer, denen bislang kein Unternehmensgerät zur Verfügung stand.

BYOD: Sicherheit für mehr Freiräume

BYOD setzt sich als Best Practice zunehmend durch. Mitarbeitern eröffnen sich durch die Nutzung eigener Geräte Freiräume bei der Arbeit, während die IT von wesentlichen finanziellen Belastungen und Verwaltungsaufgaben befreit wird. Die angestrebte Kostenersparnis und die optimierten Verwaltungsabläufe lassen sich jedoch nur mit einer intelligenten Richtlinie und einer stabilen Managementplattform erzielen.

Wenn sich Ihr Unternehmen für BYOD entscheidet, klicken Sie hier, und nutzen Sie MaaS360 30 Tage lang kostenlos. Da MaaS360 Cloud-basiert funktioniert, lässt sich die Testumgebung direkt und ohne Datenverlust in die Produktion überführen.

Wenn Sie sich erst mit der Mobilstrategie vertraut machen, stehen Ihnen mit MaaS360 eine Vielzahl an Schulungsressourcen zur Verfügung. Hier eine Auswahl:

www.maas360.com
http://www.maas360.com/products/mobile-device-management/
MaaSters Center

Weitere Informationen

Weitere Informationen zu unserer Technologie und unseren Dienstleistungen erhalten Sie unter www.maaS360.com.

1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422, USA
Telefon +1 215.664.1600 | Fax +1 215.664.1601 | sales@fiberlink.com