IBM Security
Thought Leadership White Paper

Das ABC des Managements mobiler Geräte

Die Grundlagen für die erstmalige Implementierung von Mobile Device Management (MDM)

IBM

A steht für Android, Fragmentierung ist beängstigend

Hunderte von Modellen, verschiedene Netzbetreiber, Betriebssysteme von Gingerbread bis Marshmallow und viele andere Dinge – die Fragmentierung von Android versetzt die IT-Abteilungen regelrecht in Angst und Schrecken. Mit Mobile Device Management (MDM) besteht jedoch kein Grund zur Sorge. Wenn Sie eine Minimalkontrolle im Betriebssystembereich sicherstellen, Sicherheitslücken bei Features in den Griff bekommen und eine wirksame E-Mail-Verschlüsselung durchsetzen, ist Android keine Angst verbreitende Technologie mehr.

B steht für BYOD (Bring Your Own Device), das Arbeiten mit mitarbeitereigenen Geräte. Was sich auf diesen Geräten befindet, lässt sich kaum kontrollieren.

BYOD ist ein einfaches Konzept, für die IT ist es jedoch ein verdächtiges Element. Mobile Mitarbeiter erwarten, dass sie eigene Smartphones und Tablets zum Arbeiten, aber auch zum Spielen verwenden können. Mit Mobile Device Management sind in diesem Zusammenhang Sicherheitsbedenken in der Regel kein Thema mehr.

C steht für die Cloud, die für jedes Gerät verwendet wird

In einer Welt, in der neue Gerätetypen und Software-Updates in unvorhersehbaren Zyklen angekündigt werden, sind cloudbasierte MDM-Implementierungen zum Stützpfeiler wirksamer mobiler Sicherheitsmechanismen im modernen Unternehmen geworden. In der Cloud stehen tägliche Updates sofort zur Verfügung. Sie hilft, die Gesamtbetriebskosten zu senken und bietet flexible Skalierbarkeit. Sofortige Einsatzbereitschaft ist das Schlagwort von heute.

D steht für Dokumente, die mit hoher Sicherheit gemeinsam genutzt werden können

Die gemeinsame Nutzung von Dokumenten auf mobilen Geräten ist einfach. Die sichere gemeinsame Nutzung von Dokumenten hingegen gestaltet sich etwas schwieriger. Verbraucher-Apps wie Dropbox haben ihren Platz in der Benutzergemeinschaft, jedoch nicht im Unternehmen. Unternehmen brauchen eine Dokumentmanagementlösung, die Unternehmensinformationen ausreichend schützt. Gleichzeitig muss eine solche Lösung Mitarbeitern die Möglichkeit bieten, auf einfache Weise über ihre mobilen Geräte sofort auf aktuelle Dokumente zugreifen zu können.

E steht für Enrollment, die einfache und schnelle Registrierung

Die IT ist sich über die Vorteile von MDM durchaus bewusst, viele Benutzer vielleicht eher weniger. Wenn Sie die MDM-Registrierung einfach gestalten – einfach per Mausklick – werden die Benutzer gerne ihre Geräte registrieren, um auf Netzressourcen zugreifen zu können.

F steht für frei, kostenfrei! Testen Sie 30 Tage lang kostenlos die IBM MaaS360-Lösung!

Kaufen Sie ein Fahrzeug, ohne es vorher Probe zu fahren? Kaufen Sie ein Haus, bevor Sie es sich genau angesehen haben? Ihr MDM-Service muss ebenso transparent sein. Anbieter, die keine Vorabtests ihrer Lösungen anbieten, haben möglicherweise etwas zu verbergen. Fragen Sie nach einer kostenlosen 30-Tage-Testversion. Sie haben es verdient! Ihre MaaS360-Testversion steht Ihnen in wenigen Minuten zur Verfügung unter **ibm.com**/maas360

G steht für geniale E-Mail- und WiFi-Funktionalität

Mobilität soll Ihr Leben einfacher und nicht komplizierter machen. Mitarbeiter wollen sich nicht mit Dingen wie dem Verbinden von Ressourcen befassen. Sie wollen einfach mit verbundenen Ressourcen arbeiten. Mit einer MDM-Lösung können Sie Geräte so konfigurieren, dass Mitarbeiter auf sichere Weise auf die Ressourcen zugreifen können, die sie brauchen und wann sie sie brauchen.

H steht für Hilfe, die mit einer intuitiven Benutzeroberfläche praktisch nicht benötigt wird

Bei Mobile Device Management geht es nicht nur um Benutzer. Es geht auch um Vereinfachungen, die den IT-Abteilungen das Leben leichter machen. Es gibt Lösungen, die komplexe Setups erfordern und bei denen Benutzerhandbücher fast den Umfang einer Enzyklopädie haben. Die richtige MDM-Lösung ist leistungsfähig, ohne kompliziert zu sein. Optimierte Arbeitsabläufe mithilfe einer einfachen, klar strukturierten Benutzeroberfläche lautet die Devise, mit der sich zeit- und ressourcenintensive MDM-Aufgaben automatisieren lassen.

iOS ist das zentrale Element

Die iOS Mobile-Plattform ist mit einigen der besten Sicherheitsfunktionen für Unternehmen ausgestattet. Hierzu zählen native Verschlüsselung, leistungsfähige MDM-APIs und ein umfangreicher App Store. Speziell für kontrollierte drahtlose Konfigurationen, das effiziente Sicherheitsrichtlinienmanagement und die gemeinsame Nutzung von Apps und Dokumenten ist Mobile Device Management in der Regel die einzig mögliche Antwort.

Jailbroken-Geräte können IT-Abteilungen große Sorgen bereiten

Trotz der hervorragenden sofort einsatzfähigen Features von Apple iOS wollen viele Benutzer mit „Jailbreaking“, also dem Hacken von Geräten und Betriebssystemen, mehr Kontrolle über ihr Gerät bekommen. Für dieses Mehr an Flexibilität müssen Sie in der Regel einen hohen Preis bezahlen. Und dieser Preis heißt Malware! Mit einer Mobile Device Management lassen sich solche Sicherheitsprobleme erkennen und blockieren.

K steht für Kenntnis jedes einzelnen Kostenfaktors für mehr Mobilität

Je mehr sich das Thema Konnektivität verbreitet, desto öfters beginnen Mitarbeiter damit, Inhalte im Datenstrom zu übertragen. Das ist die perfekte Lösung, wenn es auf eigene Kosten geschieht; sie eignet sich aber überhaupt nicht, wenn es zu Lasten des Unternehmens geht. Und denken Sie dabei nicht einmal an die vielen Geschichten, ob wahr oder unwahr, die zum Thema Roaming kursieren. Halten Sie Ihre Ausgaben immer im Blick und definieren Sie Richtlinien im Rahmen Ihrer MDM-Lösung, um die Datennutzung immer unter Kontrolle zu haben.

Lokalisieren Sie Ihre Geräte – anstatt Ihre IT-Abteilung nervös zu machen

Je kleiner die Geräte werden, desto einfacher gehen sie verloren. Die Hoffnung müssen Sie jedoch nicht verlieren. Und auch die IT muss keinen übermäßig hohen Aufwand für die Suche nach den Geräten investieren. Mit Mobile Device Management können Mitarbeiter die Gerätesuche von ihrem eigenen Self-Service-Portal aus einleiten. Die integrierten Karten zeigen ganz genau, wo sich das Gerät befindet.

Mobile Device Management – auf jeden Fall ein Muss

Auch wenn es native Apps gibt, die die grundlegenden Anforderungen an das Mobile Device Management erfüllen, kann nur eine echte MDM-Lösung den IT-Abteilungen das Leben erleichtern. Konfigurationen über drahtlose Verbindungen, vollständiges und selektives Löschen, App-Management, sichere gemeinsame Dokumentnutzung und Sicherheitseinrichtungen zum Schutz personenbezogener Mitarbeiterdaten sind die Merkmale eines wahren Mobile Device Management.

Neue „Verbesserungen“ am Betriebssystem, denen man nicht immer trauen kann

Es hat oft den Anschein, dass es jeden Tag neue Betriebssystem-updates für die populären mobilen Plattformen gibt. Auch wenn Benutzer sehr schnell durch diese neuen Extras beeindruckt sein können, sind sich die IT-Abteilungen über die Probleme, die diese Extras mit sich bringen können, sehr wohl bewusst. Mit Mobile Device Management lassen sich Geräte blockieren, die die Unternehmensstandards nicht erfüllen. Zudem werden Mitarbeiter durch die Möglichkeit einer kontinuierlichen Kommunikation immer darüber informiert, wenn es an der Zeit ist, eine Rollback-Operation durchzuführen.

OTA, die drahtlose Art der Konfiguration

Mobile Geräte haben es uns ermöglicht, auch von unterwegs aus miteinander zu kommunizieren. Warum sollte dies also nicht auch für das Management der Geräte möglich sein? Wenn Mitarbeiter ihr Gerät für die Registrierung oder Konfiguration zur IT-Abteilung bringen müssen, machen Sie etwas falsch. Eine MDM-Lösung funktioniert dann und dort, wo die IT-Abteilungen und Benutzer sie brauchen.

Probleme mit dem Schutz vertraulicher Daten werden immer größer

Selbst vor der Verbreitung des BYOD-Konzepts hatten Mitarbeiter bereits Probleme mit dieser Thematik, wobei die IT oft als Big Brother betrachtet wurde. Mit Mobile Device Management können Sicherheitsexperten im Unternehmen Richtlinien definieren, um den Möglichkeiten der IT-Abteilungen Grenzen zu setzen.

Quantensprung bei der Geschwindigkeit – die Cloud macht es möglich

On-Premises war in den 90er Jahren top-aktuell. Warum soll man Wochen oder Monate für die Bereitstellung einer lokalen MDM-Lösung aufwenden, wenn die Cloud dieselben Sicherheits- und Steuermechanismen ohne zusätzliche Kosten und Komplexitäten bei der Hardware- und Softwarebereit-stellung bietet? Außerdem sind keine zusätzlichen speziellen Ressourcen erforderlich, um die Lösung dauerhaft zu unterstützen.

R steht für RIM. BlackBerry ist nicht so schlecht wie sein Ruf

BlackBerry musste in letzter Zeit einiges einstecken. Es lässt sich jedoch nicht verleugnen, dass wir BlackBerry Anerkennung für eine der populärsten Apps zollen müssen, die das Unternehmen geschaffen hat: E-Mail. Aber die Zeit steht nicht still. Die Menschen wollen weitere und andere Optionen. Wenn Sie einerseits ein BlackBerry-Fan sind und andererseits die Vorzüge von Android und iOS zu schätzen wissen, brauchen Sie eine MDM-Lösung, um beides über eine einzelne Konsole verwalten zu können. Mit MaaS360 können Sie alle drei Plattformen über eine Konsole handhaben.

S steht für Self-Service: Mitarbeitern helfen, sich selbst zu helfen

Die IT muss nicht jedes einzelne Problem aus dem Mobilbereich selbst bearbeiten. Mit einer MDM-Lösung lässt sich das in die Tat umsetzen. Einfache Funktionen wie das Zurücksetzen von Kennwörtern, das Auffinden von Geräten und das Überprüfen der Datennutzung lassen sich allesamt über die MDM-Self-Serviceportale ausführen.

T steht für Termineinhaltung durch Zeiteinsparung

MDM erfüllt Ihnen auch diesen Wunsch! Mit einer cloud-basierten MDM-Lösung sind Sie in wenigen Minuten einsatzbereit. Die Zeiteinsparungen setzen sich auch nach der Installation der Lösung fort. Drahtlose Registrierung und Verwaltung, Dokumentverteilung und Anwendungssteuerung können zu hohen Zeiteinsparungen und damit zu mehr Produktivität bei den Benutzern führen. Außerdem können sich die IT-Abteilungen dadurch auf für das Unternehmen wichtigere Aktivitäten konzentrieren.

U steht für unbedingtes Verständnis Ihrer Mitarbeiter und der Geräte, die sie verwenden

Sie können nichts schützen, was Sie nicht kennen. Smartphones und Tablets machen es für Benutzer ganz einfach, eine Verbindung zu Ihren E-Mail-Servern ohne Eingriff der IT-Abteilung herzustellen. Fragen Sie sich selbst, wie viele Geräte mit Ihren Unternehmenssystemen verbunden sind, und untersuchen Sie das dann genauer. Die Anzahl wird sehr wahrscheinlich deutlich höher liegen als erwartet. Mit Mobile Device Management können Sie feststellen, wer wo verbunden ist.

VPP: Apps in großen Mengen kaufen; der hohe Nutzen daraus ist bekannt

Über das Volume Purchasing Program (VPP) von Apple können Sie öffentlich verfügbare Apps oder von Drittanbietern speziell entwickelte Apps in großen Mengen kaufen. MDM lässt sich problemlos in das Apple VPP integrieren, um die Auftragsverwaltung und die Verfolgung von Kaufmengen zu verbessern. Hinzu kommen weitere Möglichkeiten wie die Verteilung von anwendungsspezifischen Einlösecodes und Lizenzen, die Anwendungsinstallation und die Complianceüberwachung. Einer der größten Vorteile ist, dass VPP-Käufe nicht mehr in Kurznotizen festgehalten werden müssen.

W steht für Wiping, das Löschen von Unternehmensdaten oder allen Datenbeständen

Die Menschen lieben ihre Smartphones. Es ist in der Regel aber nicht die Hardware, die uns begeistert – es sind die persönlichen Erlebnisse oder Erfahrungen mit Apps, Fotos oder der Stimme des eigenen Kindes als Klingelton. Niemand will, dass diese persönlich wertvollen Dinge in irgendeiner Form zu Schaden kommen. Mit der richtigen MDM-Lösung gehen Sie bei persönlichen Daten und Unternehmensdaten keine Kompromisse ein. Verlässt ein Mitarbeiter das Unternehmen, werden die Unternehmensdaten einfach vom Gerät gelöscht, ohne die persönlichen Daten zu beeinträchtigen.

X steht für X-Ray und andere Apps, die begeistern

Medizin, Ausbildung, Einzelhandel, Finanzen und viele andere Branchen haben bereits ihr Anwendungskonzept umgestellt: Apps kosten keine Zeit mehr, sie helfen, Zeit einzusparen. Dann wären noch die Apps zu nennen, für die es im Unternehmen keinen Platz gibt. Mit Mobile Device Management können Sie genau kontrollieren, welche Apps auf dem Gerät installiert werden können, und welche Apps im App Store verbleiben müssen, weil sie keinen geschäftlichen Nutzen haben.

Y steht für die Generation Y, die junge Generation, die Auswahlmöglichkeiten im Mobilbereich fordert

Die Generation Y und die Millennials drängen massiv in den Arbeitsmarkt. Diese Digital Natives können sich ein Leben ohne ihre mobilen Geräte nicht vorstellen. Dieser nächsten Generation an Arbeitskräften werden Sie sicherlich nicht sagen wollen, dass sie durch die bisherigen Geschäfts- und Kommunikationsmöglichkeiten in ihrer Arbeit eingeschränkt sind! Profitieren Sie stattdessen von den Geräten, die diese Generation am besten kennt und nutzen kann.

Z steht für Zufriedenheit und Begeisterung

Benutzer und IT-Abteilungen sind gleichermaßen erfreut, wenn mobile Arbeitsprozesse reibungslos funktionieren und einfach zu verwalten sind. Mobile Device Management wird sich in den kommenden Jahren immer weiterentwickeln und immer präsenter werden. Vereinfachen Sie Ihre eigenen Prozesse und die Prozesse der von Ihnen unterstützten Personen – durch die Handhabung aller Mobilitätsaspekte mit MaaS360 in nur wenigen Minuten.

Informationen zu IBM MaaS360

IBM MaaS360 ist die unternehmensweite Plattform für das Mobilitätsmanagement, mit der Sie die Produktivität und Datenschutz bei den Arbeitsprozessen verbessern. Tausende von Unternehmen vertrauen bereits auf MaaS360 als Grundlage für ihre Mobilitätsinitiativen. MaaS360 ermöglicht umfassende Managementprozesse mit leistungsfähigen Sicherheitsmechanismen für Benutzer, Geräte, Apps und Inhalte und damit eine optimale Bereitstellung von Mobilumgebungen. Weitere Informationen zu IBM MaaS360 und zur kostenlosen 30-Tage-Testversion erhalten Sie hier: **ibm.com**/maas360

Informationen zu IBM Security

Die IBM Security-Plattform überzeugt durch die Bereitstellung von Sicherheitsdaten, die Unternehmen helfen, mit einem ganzheitlichen Ansatz Mitarbeiter, Daten, Apps und Infrastruktur ausreichend zu schützen. IBM bietet zudem eine große Anzahl von Lösungen für die unterschiedlichsten Bereiche: Identitäts- und Zugriffsmanagement, Sicherheitsinformationen, Ereignismanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Manipulationsschutz der nächsten Generation und vieles mehr. IBM betreibt darüber hinaus eines der weltweit größten Forschungs-, Entwicklungs- und Bereitstellungszentren zum Thema Sicherheit. Weitere Informationen finden Sie hier: **ibm.com**/security

Bemerkungen

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

Die in diesem Dokument enthaltenen Informationen sind zum Datum der Erstveröffentlichung des Dokuments aktuell und können von IBM jederzeit geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist.

Die genannten Leistungsdaten und Kundenbeispiele dienen nur zur Veranschaulichung. Die tatsächlichen Leistungsergebnisse können je nach Konfigurationen und Betriebsbedingungen variieren. Die Verantwortung für die Auswertung und Prüfung des Betriebs von Produkten oder Programmen anderer Anbieter mit IBM Produkten und Programmen liegt beim Benutzer.

Die Informationen in diesem Dokument werden auf der Grundlage des gegenwärtigen Zustands (auf „as-is“-Basis) ohne jegliche ausdrückliche oder stillschweigende Gewährleistung zur Verfügung gestellt, einschließlich, aber nicht beschränkt auf die Gewährleistungen für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

Der Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. IBM erteilt keine Rechtsberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit den geltenden Gesetzen und gesetzlichen Bestimmungen.

Jegliche Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Erklärung zu geeigneten Sicherheitsvorkehrungen: Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Prävention, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht oder veruntreut werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt und keine einzelne Sicherheitsmaßnahme können einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme und Produkte werden als Teil eines umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keine Gewähr dafür, dass Systeme und Produkte vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter geschützt sind.

Bitte der Wiederverwertung zuführen

WGW03116-DEDE-01