IBM Global Technology Services
Thought Leadership White Paper

Februar 2013

Entwicklung von effektiveren Programmen für das mobile Unternehmen

Eine praktische Anleitung zur Erstellung von Programmen für das mobile Unternehmen mit Hilfe von Partnern

IBM

Die immer stärkere Verbreitung von mobilen Endgeräten hat in Verbindung mit zunehmend globalen und mobilen Mitarbeitern, die sofortigen Zugriff auf Unternehmensressourcen verlangen, zu einem enormen Bedarf an Programmen für das mobile Unternehmen geführt. Diese Programme umfassen die Infrastruktur, Technologien und Richtlinien, die Mitarbeitern und weiteren berechtigten Personen die Implementierung von Unternehmensanwendungen und den Zugriff auf Unternehmensressourcen auf mobilen Endgeräten wie Smartphones und Tablets ermöglichen. Während einige Unternehmen ihren Mitarbeitern nur die Arbeit mit unternehmenseigenen mobilen Endgeräten erlauben, setzen andere zunehmend auf BYOD-Programme (Bring Your Own Device), bei denen die Mitarbeiter eigene (d. h. selbst angeschaffte) mobile Endgeräte ihrer Wahl bei der Arbeit verwenden dürfen.

Mit Programmen für das mobile Unternehmen lässt sich erheblicher Wert für Mitarbeiter, Partner und Kunden schaffen. Wenn die Mitarbeiter rund um die Uhr Zugriff auf Unternehmensressourcen haben, können sie praktisch überall arbeiten – und das Unternehmen kann seine Produktivität und Effizienz insgesamt steigern und sich einen Wettbewerbsvorteil sichern. Programme für das mobile Unternehmen bringen jedoch auch große Herausforderungen mit sich. Bisher haben sich nur wenige bewährte Verfahren in der Branche etabliert, bedingt durch das schnelle Wachstum bei Mobiltechnologien in jüngster Zeit. Viele Unternehmen, die Programme für das mobile Unternehmen erstellen wollen, wissen daher nicht, wie sie diesen Plan in die Tat umsetzen und womit sie beginnen sollen. Andere Unternehmen stellen fest, dass die Entwicklung eines Programms in Eigenregie zeitaufwendig, kostenintensiv, kompliziert und mit Risiken verbunden ist.

Dieses White Paper enthält eine praktische Anleitung zur Planung und Implementierung von effektiveren Programmen für das mobile Unternehmen und beschreibt die Fähigkeiten, mit denen Partner des mobilen Unternehmens zur Entwicklung und Unterstützung dieser Programme für unternehmenseigene oder mitarbeitereigene mobile Endgeräte beitragen können. Das White Paper konzentriert sich auf Programme für Mitarbeiter, nicht für Kunden.

Die „Consumerization" der IT

Die große Nachfrage nach mobilen Endgeräten am Arbeitsplatz in Verbindung mit zunehmend geografisch verteilten Mitarbeitern zwingt Unternehmen, die Nutzung von Mobiltechnologie am Arbeitsplatz zu unterstützen. In einer 2012 von IBM durchgeführten Umfrage unter 675 Chief Information Officers (CIOs) und IT-Managern großer Unternehmen weltweit sagten 74 Prozent der Befragten, dass sie der Entwicklung einer flexiblen Arbeitsplatzumgebung in den kommenden zwölf Monaten größere Priorität als anderen Investitionen einräumen werden.[1] Die Mehrzahl der Befragten glaubte zudem, dass eine flexible Arbeitsplatzumgebung zu Produktivitätssteigerungen beitragen wird, und fast die Hälfte der Befragten rechnete mit möglichen Umsatzsteigerungen.[2]

Laut dem Branchenanalysten Gartner werden 80 Prozent der mobilen Mitarbeiter bis 2014 mindestens zwei mobile Endgeräte für den Zugriff auf Unternehmenssysteme und Daten verwenden. Heute sind es nur 40 Prozent.[3] Offensichtlich ist die Nutzung von mobilen Endgeräten am Arbeitsplatz nicht mehr nur ein Trend, sondern bereits Realität in Unternehmen.

„Das IBM BYOD-Programm unterstützt Mitarbeiter dabei, ihre Arbeit nach ihren eigenen Vorstellungen zu gestalten. Sie nutzen das für sie geeignete Tool, um ihre Aufgaben zu erledigen. Ich möchte sie dabei unterstützen, allerdings in einer Weise, die die Integrität unseres Unternehmens sicherstellt."

– IBM CIO Jeanette Horan

Mit Mobiltechnologie verbundene Herausforderungen für Unternehmen

Da Mobiltechnologie neu ist und sich ständig verändert, haben sich bisher nur wenige bewährte Verfahren etabliert, die Unternehmen als Anleitung bei der Umsetzung effektiver Strategien für das mobile Unternehmen verwenden können. Daher wissen viele Unternehmen nicht, wie oder wo sie beginnen sollen.

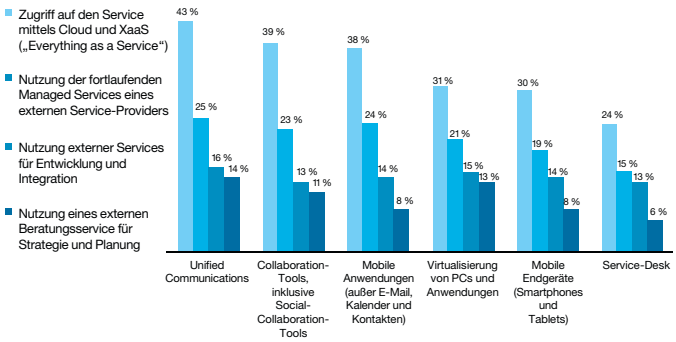
Sicherheit, Datenschutz und die Kontrolle der Nutzung sind ebenfalls wichtige Themen in Anbetracht der Vermischung von privaten Daten und Unternehmensdaten auf vielen mobilen

Endgeräten. Tatsächlich nannten 71 Prozent der befragten CIOs und IT-Manager die Sicherheit als größte Herausforderung für das mobile Unternehmen[6]. Ihre Bedenken sind nicht unbegründet. In seiner siebten jährlichen Studie im Auftrag von Symantec stellte das Ponemon Institute fest, dass sich die Kosten einer Datenschutzverletzung für Unternehmen auf durchschnittlich 5,5 Mio. US-Dollar bzw. 194 US-Dollar pro Datensatz belaufen.[7]

Die Studie zeigte auch, dass 39 Prozent der Unternehmen von einer Datenschutzverletzung betroffen waren, die aus dem Verlust oder Diebstahl eines mobilen Endgeräts eines Mitarbeiters oder Auftragnehmers, das vertrauliche und sensible Daten enthielt, herrührte – darunter Laptops, Smartphones, Tablets und USB-Speichereinheiten. Darüber hinaus machten sich 37 Prozent der Unternehmen Sorgen wegen eines böswilligen oder kriminell motivierten Angriffs und 24 Prozent wegen Systemstörungen, darunter einer Kombination von IT- und Geschäftsprozessausfällen.[8]

Unternehmen können sich die verheerenden Konsequenzen nicht leisten, die entstehen können, wenn sie sich blind in das rasch größer werdende Labyrinth der Mobiltechnologie begeben. Deshalb suchen immer mehr Unternehmen die Unterstützung kompetenter Experten, die ihnen die erforderlichen Ressourcen und Technologien bereitstellen können, mit denen sie Risiken mindern und tragfähige Programme für das mobile Unternehmen implementieren können. Ein Partner für mobile Unternehmen bringt zudem Wissen auf dem Gebiet bewährter Verfahren mit, das er bei der Unterstützung verschiedenster Unternehmen aus zahlreichen Branchen bei der Erstellung erfolgreicher Strategien für das mobile Unternehmen gewonnen hat.

Wie wollen Sie Ihre Strategie für Mobiltechnologie, Onlinezusammenarbeit (Collaboration) und Social Business in die Tat umsetzen und die damit verbundenen Herausforderungen angehen?



Basis: 80 IT-Entscheidungsträger weltweit
Quelle: Eine Studie von Forrester Consulting im Auftrag von IBM, Mai 2012

Anleitung zu Entwicklung, Management und Unterstützung eines Programms für das mobile Unternehmen

Die Implementierung eines effektiven und tragfähigen Programms für das mobile Unternehmen besteht aus vier Schritten:

1. **Definition einer Strategie für das mobile Unternehmen:** Klären Sie Ihre Ziele bezüglich der Nutzung von Mobiltechnologie, entscheiden Sie, was für ein Programm Sie unterstützen wollen (BYOD oder unternehmenseigene mobile Endgeräte) und prüfen Sie die Kostenfaktoren.

2. **Implementierung Ihres Programms für das mobile Unternehmen:** Wählen Sie die Tools aus, die Sie zur Erstellung Ihres Programms für das mobile Unternehmen verwenden wollen, und bereiten Sie Ihr Unternehmensnetzwerk auf die Unterstützung Ihres Programms vor.

3. **Schutz und Management Ihrer mobilen Endgeräte:** Wählen Sie Technologien für den Schutz der mit Ihrem Netzwerk verbundenen mobilen Endgeräte aus und entwickeln Sie eine Richtlinie für die Sicherheit mobiler Endgeräte.

4. **Unterstützung:** Stellen Sie kontinuierlichen Support für mobile Endgeräte bereit.

Jede Phase wird im Folgenden näher beschrieben.

Schritt 1: Entwicklung einer Strategie für das mobile Unternehmen

Einer der wichtigsten Schritte bei der Erstellung eines Programms für das mobile Unternehmen sollte die Definition einer entsprechenden Strategie sein, die festlegt, wie Sie Mobiltechnologie in Ihrer Arbeitsplatzumgebung entwickeln und implementieren. Die Ausarbeitung einer solchen Strategie sollte mit einer genauen Erfassung Ihrer Anforderungen, Wünsche und Ziele beginnen.

Stellen Sie sich folgende Fragen:

- Warum wollen wir ein Programm für das mobile Unternehmen implementieren? Was ist unser oberstes Ziel? Welche Vorteile versprechen wir uns?
- Welche Kostenfaktoren müssen bei einem Programm für das mobile Unternehmen berücksichtigt werden? Überwiegen die Kosten in unserer Situation die Vorteile?
- Stellen wir unseren Mitarbeitern unternehmenseigene mobile Endgeräte zur Verfügung oder sollen unsere Mitarbeiter ihre eigenen mobilen Endgeräte anschaffen und nutzen? Gewähren wir ihnen eine Kostenerstattung und falls ja, in welchem Umfang?
- Wollen wir maßgeschneiderte mobile Anwendungen entwickeln, die Entwicklung mobiler Anwendungen per Outsourcing an einen externen Partner übertragen oder vordefinierte mobile Anwendungen kaufen?

Vorteile von Programmen für das mobile Unternehmen: Programme für das mobile Unternehmen bieten eine Vielzahl von Vorteilen. Die häufigsten sind im Folgenden aufgelistet:

- Höhere Mitarbeiterzufriedenheit – Mitarbeiter arbeiten gerne mit mobilen Endgeräten, vor allem mit Geräten und Plattformen ihrer Wahl. Sie schätzen außerdem die Flexibilität, praktisch überall und nach ihren Vorstellungen arbeiten zu können.
- Einfachere Mitarbeitergewinnung und -bindung – Mitarbeiter arbeiten lieber für Unternehmen, die Mobiltechnologie am Arbeitsplatz unterstützen.
- Höhere Produktivität – Wenn Sie Ihren Mitarbeitern die Möglichkeit geben, praktisch jederzeit und überall zu arbeiten, können diese mehr Aufgaben innerhalb und außerhalb des Büros erledigen. Zudem hilft die Entwicklung individuell angepasster mobiler Anwendungen den Mitarbeitern, auf neue und innovativere Weise zu arbeiten.
- Verbesserte Kundenbeziehungen – Spezialisierte mobile Anwendungen (Apps) ermöglichen es Unternehmen, ihre Produkte über mobile Endgeräte zu vertreiben und ihren Vertriebsmitarbeitern Kundendaten nahezu in Echtzeit bereitzustellen. Dank dieser leistungsfähigen Funktionen können Unternehmen feststellen, wie ihre Kunden „ticken“, schneller auf deren Anforderungen und Wünsche eingehen und ihnen einen besseren Service bieten.

Allgemeine Kostenüberlegungen: Die von Unternehmen erzielten Kosteneinsparungen sind sehr unterschiedlich. Zu den Kostenfaktoren zählen Investitionen in Software, Infrastruktur (einschließlich der mobilen Endgeräte selbst, wenn Sie sich für die Nutzung unternehmenseigener Endgeräte entscheiden), Personalbeschaffung oder zugehörige Support-Services, Anwendungsentwicklung und sogar mögliche Netzwerkupgrades. Sie sollten außerdem die weniger offensichtlichen Kosten berücksichtigen, z. B. Softwarelizenzgebühren, die Kostenerstattung für Mitarbeiter mit privaten mobilen Endgeräten, internationale Nutzungsgebühren, Steuern, Versicherungen und sonstige „weiche“ Kosten. Natürlich sind jedoch viele der Vorteile von Programmen für das mobile Unternehmen von unschätzbarem Nutzen – z. B. höhere Produktivität, Innovation am Arbeitsplatz, Zeitersparnisse und zufriedene Mitarbeiter. Hinzu kommt: Unternehmen, die Services für das mobile Unternehmen von externen Partnern nutzen, profitieren häufig von erheblichen Einsparungen.

CIOs erzielten eigenen Angaben zufolge Produktivitätssteigerungen und Kosteneinsparungen von 20 Prozent durch das Outsourcing von Services für einen flexiblen Arbeitsplatz.[9]

Vergleich von BYOD mit der Nutzung von unternehmenseigenen mobilen Endgeräten: Die Kosten für Programme für das mobile Unternehmen sind auch davon abhängig, was für ein Programm Sie implementieren.

Beispielsweise können BYOD-Programme kostenintensiver und komplexer sein, bedingt durch die Vermischung von Unternehmensdaten und privaten Daten auf mobilen Endgeräten und die komplizierteren Maßnahmen, die erforderlich sind, um die Sicherheit privater mobiler Endgeräte zu gewährleisten. Laut der Aberdeen Group gibt ein Unternehmen mit einem BYOD-Programm, das 1.000 private mobile Endgeräte umfasst, im Durchschnitt 170.000 US-Dollar mehr pro Jahr aus als ein Unternehmen, das alle mobilen Endgeräte zentral beschafft und für alle Aspekte im Zusammenhang mit diesen Geräten verantwortlich ist. Zu den höheren und schwierig zu verfolgenden BYOD-Kosten tragen die folgenden Faktoren bei:

- Rechnungen verschiedener Netzbetreiber
- Höherer Abrechnungsaufwand durch die Kostenerstattung für Mitarbeiter
- Zusätzlicher Aufwand für die IT für das Management und den Schutz von Unternehmensdaten auf privaten mobilen Endgeräten der Mitarbeiter
- Höherer Aufwand für andere Teams, die normalerweise nicht für die Unterstützung von Mobiltechnologie zuständig sind
- Größere Komplexität der mobilen Umgebung und folglich steigende Supportkosten[10]

Die Kontrolle und ein möglichst einfaches Management sind weitere Faktoren, die es zu berücksichtigen gilt. Wenn Sie mobile Endgeräte selbst auswählen, anschaffen und verwalten, ist es in der Regel einfacher, diese Geräte zu schützen und die Einhaltung von unternehmensinternen Richtlinien sicherzustellen – da Sie die Infrastruktur erstellen können, auf deren Basis Sie Unternehmensdaten und -anwendungen bereitstellen. Die größere Kontrolle, die Sie dadurch gewinnen, geht jedoch möglicherweise zu Lasten der Benutzerzufriedenheit – da viele Mitarbeiter unbedingt mit ihren eigenen mobilen Endgeräten arbeiten wollen. Um breite Unterstützung für Ihre Strategie zur Nutzung unternehmenseigener mobiler Endgeräte zu erhalten, sollten Sie Ihre Mitarbeiter nach den Geräten und Anwendungen fragen, die sie verwenden möchten. Ihre Mitarbeiter werden die Einschränkungen eines Programms, an dessen Entwicklung sie selbst mitgewirkt haben, bereitwilliger akzeptieren. Wenn Ihr Unternehmen die mobilen Endgeräte bereitstellt, werden Ihre Mitarbeiter außerdem ein hohes Maß an Endbenutzersupport erwarten. Hierfür benötigen Sie eine ausreichende Anzahl an Mitarbeitern mit dem nötigen Know-how.

Strategische Überlegungen – wie Sie ein Partner für mobile Unternehmen unterstützen kann: Mit Hilfe eines Partners können Sie herausfinden, inwiefern Ihre Mitarbeiter, Kunden und das Unternehmen insgesamt von Mobiltechnologie profitieren können. Ein Partner kann Sie mit Strategie- und Beratungsservices dabei unterstützen, Ihre Anforderungen und Ziele genau zu bestimmen, den materiellen und immateriellen Return-on-Investment (ROI) zu ermitteln und eine in mehrere Phasen unterteilte Roadmap für die Implementierung des Programms zu erstellen. Ein Partner kann sogar Services für das Management der Telekommunikationskosten bereitstellen, um Sie bei der Optimierung und dem besseren Management Ihrer Ausgaben für Mobiltechnologie zu unterstützen. Darüber hinaus kann Ihnen ein Partner praktisch alle Herausforderungen im Zusammenhang mit Forschung und Logistik abnehmen, die anfallen, wenn ein Programm von Anfang an neu erstellt wird – und so dafür sorgen, dass Ihr Programm schneller einsatzbereit ist.

Schritt 2: Implementierung eines Programms für das mobile Unternehmen

Sobald Ihre Ziele im Hinblick auf das Programm feststehen, müssen Sie überlegen, wie Sie das Programm technisch umsetzen werden.

Stellen Sie sich folgende Fragen:

- Welche Geräte wollen wir unterstützen (Mobiltelefone, Tablets, Laptops)? Welche Vor- und Nachteile hat die Unterstützung unterschiedlicher Geräte und Betriebssysteme? Welche Geräte und Betriebssysteme wollen wir ausgehend von dieser Analyse und den Vorlieben der Endbenutzer unterstützen?
- Welche Daten und Anwendungen sollen wir den Endbenutzern zugänglich machen? Sollen wir ihnen vollen oder eingeschränkten Zugriff gewähren?
- Welche Services wollen wir unterstützen?
- Welche Mitarbeiter und sonstigen relevanten Personen benötigen Mobiltechnologie am dringendsten? Sollen wir die Einführung von Mobiltechnologie im Unternehmen auf diese Personen beschränken oder auf alle Mitarbeiter ausweiten?

- Welche Szenarien der Nutzung mobiler Endgeräte rechtfertigen die Entwicklung spezieller mobiler Anwendungen?
- Sollen wir unser Programm für das mobile Unternehmen auf strategische Unternehmensstandorte beschränken oder ein unternehmensweites Programm starten, das mehrere Standorte weltweit unterstützen kann?
- Inwieweit müssen unsere Unternehmenssysteme und mobilen Systeme integriert werden?
- Wie können wir die optimale Leistung unserer Netzwerke unterstützen, um den Erfolg unseres Programms für das mobile Unternehmen sicherzustellen?

Auswahl der Geräte, die unterstützt werden sollen: Es ist nahezu unmöglich, jedes neue Tablet und Smartphone, das auf den Markt kommt, sicher und logistisch zu unterstützen. Daher ist es effektiver, nur bestimmte Geräte und Betriebssysteme zu unterstützen und diese Geräte (und die Begründung für deren Unterstützung) in Ihrer Richtlinie für mobile Endgeräte zu definieren. Auf dieses Thema werden wir später noch näher eingehen. Idealerweise sollte Ihre Entscheidung auf der aktuellen und geplanten Nutzung von mobilen Endgeräten in Ihrem Unternehmen sowie den Vorlieben Ihrer Mitarbeiter basieren.

Im Allgemeinen gilt jedoch: Je mehr Plattformen Sie unterstützen, desto größer die Komplexität. Eine der einfachsten Methoden zur Reduzierung der Komplexität ist daher die Begrenzung der Anzahl an unterstützten Geräten und Plattformen. Sie müssen jedoch auch die Vor- und Nachteile verschiedener Plattformen wie z. B. Research in Motion (RIM) BlackBerry, Apple iOS, Android und Windows® berücksichtigen. Entscheiden Sie bei der Abwägung der Vor- und Nachteile, was mit Blick auf die Sicherheit am ehesten und am wenigsten akzeptabel für Ihr Unternehmen ist. Viele Unternehmen unterstützen die Nutzung von BlackBerry-Geräten wegen ihres sicheren Konzepts. Auch iOS- und Android-Plattformen können ein höheres Maß an Sicherheit bieten, doch für ältere Versionen von Microsoft® Windows und Android gilt dies möglicherweise nicht. Um die Sicherheit, die Kompatibilität von Apps und den Service-Desk-Aufwand zu erleichtern, hat es sich bewährt, die Anzahl an Betriebssystemplattformen und -versionen zu begrenzen. Wenn sich Ihr Programm und die Sicherheitsinfrastruktur mit der Zeit weiterentwickeln, können Sie die Unterstützung für Geräte und Plattformen langsam ausweiten.

Auswahl von Daten und Anwendungen für mobilen Zugriff: Sobald Sie die Geräte und Betriebssysteme eingegrenzt haben, die Sie unterstützen wollen, sollten Sie als Nächstes die Daten und Anwendungen festlegen, die Sie bestimmten Mitarbeitern zugänglich machen wollen. Wenn Sie zum Beispiel im Gesundheitswesen tätig sind, benötigen Ärzte und Pflegepersonal möglicherweise andere Möglichkeiten des mobilen Zugriffs als Mitarbeiter in der Verwaltung. Wir empfehlen Ihnen die Zusammenstellung eines Teams, das für die Erfassung von Informationen von Ihren Mitarbeitern zuständig ist, damit Sie besseren Einblick in deren tatsächliche und wahrgenommene Anforderungen an Mobiltechnologie am Arbeitsplatz erhalten. Diese Informationen helfen Ihnen bei der effektiven Ermittlung von bestimmten Geschäftsprozessen – im gesamten Unternehmen –, die durch den Zugriff auf bestimmte Daten und vorhandene oder individuell erstellte Anwendungen auf mobilen Endgeräten vereinfacht werden könnten. Priorisieren Sie anschließend, welche Benutzer mobilen Zugriff auf diese Unternehmensressourcen erhalten sollen, um die Komplexität zu reduzieren. Stellen Sie sicher, dass Sie zunächst nur Benutzern mit hoher Priorität und nicht gleich allen Mitarbeitern mobilen Zugriff bereitstellen.

Im Allgemeinen sind E-Mail- und Kalenderanwendungen für den Anfang besser geeignet, da sie einfacher sind. Wenn Ihre Mitarbeiter bereits mobile Endgeräte für den Zugriff auf E-Mail und Kalender verwenden, empfiehlt es sich, eine Bestandsaufnahme der verwendeten Geräte und Plattformen durchzuführen, um vor der Aktualisierung oder Ausweitung Ihres Programms für das mobile Unternehmen die Einhaltung von Sicherheitsbestimmungen zu gewährleisten. Wenn Sie ein BYOD-Programm starten, sollten Sie bedenken, dass mobile Messaging-Middleware eingeschränkte Funktionalität bietet (siehe „Löschen und Sperren von Geräten“ auf den Seiten 8 und 9).

Aktivierung von Services für Mitarbeiter: Zusätzlich zur Aktivierung von Anwendungen wollen Sie möglicherweise auch bestimmte Services über mobile Endgeräte aktivieren, darunter Social-Business-Funktionen wie Instant Messaging,

das unternehmensweite Risikomanagement sowie CRM-Systeme (Customer Relationship Management) für den Zugriff auf Vertriebs-, Finanz- und Personaldaten. Legen Sie die Reihenfolge fest, in der Sie Ihren Mitarbeitern diese Services zugänglich machen werden – denn sobald Mobiltechnologien am Arbeitsplatz unterstützt werden, werden Ihre Mitarbeiter nach zahlreichen Funktionen verlangen.

Vorbereitung Ihres Netzwerks: Ein effizientes Netzwerkmanagement ist ein Aspekt, der bei der Planung von Programmen für das mobile Unternehmen häufig außer Acht gelassen wird, jedoch maßgeblich über den Erfolg oder Misserfolg Ihrer Initiativen für Mobiltechnologie entscheiden kann. Im Allgemeinen erfordert ein erweiterungsfähiges Netzwerk, das eine wachsende Zahl von Geräten und enorme Datenmengen unterstützt, eine höhere Bandbreite und leistungsstarke Funktionen für die Netzwerküberwachung. Das bedeutet, Sie benötigen Lösungen für die Automatisierung von Konfigurationsänderungen, die Analyse der Leistung, das Management der Sicherheit, die Bereitstellung einer Vielzahl weiterer Managementfunktionen und die Unterstützung enormer Skalierbarkeit (z. B. Cloud-basierte oder virtualisierte Netzwerktools).

Auch die Verfügbarkeit gewinnt an Bedeutung. Wenn Netzwerke umfangreicher werden, nimmt auch das Risiko von Fehlern und Sicherheitsverstößen zu. Aufgrund dieser größeren Risiken erhöht sich die Notwendigkeit von Funktionen für das zuverlässige und effektive Ereignismanagement, die Ursachenanalyse, das Änderungs- und Konfigurationsmanagement, die Erstellung von Leistungsberichten und das Endgerätemanagement.

Ein einfach umsetzbarer Ansatz in mehreren Phasen für die Implementierung einer Strategie für das mobile Unternehmen

Bei der Entwicklung eines Programms für das mobile Unternehmen sollten Sie der Versuchung widerstehen, alle Aufgaben auf einmal in Angriff zu nehmen – selbst wenn Sie mit einem Partner zusammenarbeiten. Behalten Sie das Gesamtbild im Blick, während Sie sich Ihren Zielen mit kleinen Schritten nähern. Auf diese Weise können Sie auftretende Probleme behandeln und lösen, bevor Sie zu komplexeren Initiativen übergehen.
Im Folgenden ist ein Beispiel des Rollouts eines Programms für das mobile Unternehmen beschrieben, das Sie im Verlauf mehrerer Monate oder eines längeren Zeitraums implementieren können.

1. Verwalten Sie vorhandene Geräte, die auf Ihre E-Mail-, Kalender- und weiteren mobilen Anwendungen zugreifen: Ermitteln Sie mit Hilfe von Tools für das Infrastrukturmanagement oder Software für das Management mobiler Endgeräte die Anzahl an mobilen Endgeräten, die auf Ihr Netzwerk zugreifen. Achten Sie dabei besonders darauf, wie diese Geräte auf Ihr Netzwerk zugreifen (z. B. über ein Virtual Private Network [VPN] oder WLAN) und welche Daten und Anwendungen auf diesen Geräten zugänglich sind. Falls möglich, sollten Sie auch den Sicherheitsstatus dieser Geräte bestimmen, einschließlich Authentifizierungsverfahren und der Anwendungssicherheit. Wenn Sie keinen Zugang zu diesen Informationen haben, weil Sie nicht über Tools für das Management mobiler Endgeräte und Reporting-Tools verfügen, sollten Sie eine Frist setzen, bis zu der die derzeitige Nutzung des mobilen Zugriffs fortgesetzt werden kann, und neue, strengere Richtlinien und Verfahren für Ihre Mitarbeiter ankündigen, wenn Sie die technischen Voraussetzungen für deren Durchsetzung erfüllen.

2. Weiten Sie den kontrollierten Zugriff auf alle Mitarbeiter aus: Die meisten Ihrer Mitarbeiter werden sich mindestens Zugriff auf die E-Mail- und Kalenderanwendungen Ihres Unternehmens wünschen. Wenn Sie diese Funktionen auf alle Mitarbeiter ausweiten, können Sie nicht nur deren Zufriedenheit erhöhen, sondern auch besseren Einblick in die Abläufe der Implementierung eines unternehmensweiten Programms für Mobiltechnologie erhalten. Anhand der dabei gewonnenen Erkenntnisse können Sie entscheiden, ob Sie den unternehmensweiten mobilen Zugriff auch auf andere Daten und Anwendungen ermöglichen wollen.

3. Stellen Sie das Speichern und Synchronisieren von Daten auf Geräten sicher: Sie können das Speichern von Daten nur über das Netzwerk erlauben, um zu vermeiden, dass lokale Kopien auf mobilen Endgeräten gespeichert werden, da dies im Fall eines Verlusts oder Diebstahls des Geräts ein Risiko darstellt. Sie können Methoden wie die Verschlüsselung und die Containerisation für den besseren Schutz von gespeicherten Daten verwenden.

4. Erfassen und priorisieren Sie mobile Standardanwendungen, die für die in Ihrem Unternehmen eingesetzte Software verfügbar sind: Dadurch können Sie die Funktionen bereitstellen, die Ihre Mitarbeiter benötigen, um durch mobilen Zugriff produktiver arbeiten zu können.

5. Entwickeln Sie maßgeschneiderte Apps oder beauftragen Sie Partner mit deren Entwicklung: Überlegen Sie, welche Services und Prozesse die Entwicklung maßgeschneiderter Anwendungen erfordern, und entwickeln Sie diese auf der Basis Ihrer Prioritäten bezüglich der Nutzung von Mobiltechnologie.

6. Implementieren Sie mobile Anwendungen, wenn Ihre Sicherheitsinfrastruktur in Ordnung ist: Die Unternehmensanwendungen, die von mobilen Endgeräten aus zugänglich sind, sollten mindestens dieselbe Sicherheit wie Anwendungen, auf die kein mobiler Zugriff möglich ist, aufweisen. Wenn Sie keine Anwendungen implementieren können, die diesem Sicherheitsstandard entsprechen, sollten Sie Ihre Implementierung auf vertrauenswürdige mobile Anwendungen beschränken.

Schritt 3: Sicherheitsmanagement

Nachdem Sie die Technologie ausgewählt haben, die Sie für die Erstellung und das Management Ihres Programms für das mobile Unternehmen verwenden wollen, benötigen Sie einen Plan, der Sie beim Schutz aller mit dem Netzwerk Ihres Unternehmens verbundenen mobilen Endgeräte unterstützt.

Stellen Sie sich folgende Fragen:

- Wie können wir das Management der Sicherheit von Geräten, Anwendungen und des Datenzugriffs verbessern?
- Wie verwalten wir Daten, wenn ein Mitarbeiter das Unternehmen verlässt oder wenn ein Gerät verloren geht oder gestohlen wird?
- Wie können wir mobile Endgeräte besser vor häufigen Sicherheitsbedrohungen wie Viren, Malware und Angriffen schützen?
- Welches Mindestsicherheitsmaß ist für uns akzeptabel und können wir es im Rahmen unserer Unternehmenskultur erreichen?
- Wie können wir mobile Endgeräte und Unternehmensanwendungen auf sichere Weise verteilen und den Prozess der Integration und Einführung steuern?
- Was genau sollte in eine Richtlinie für die Sicherheit mobiler Endgeräte aufgenommen werden? Wie können wir die Einhaltung von Datenschutzgesetzen besser managen?

Die Sicherheit mobiler Endgeräte ist nach wie vor eines der wichtigsten Themen für Unternehmen. Es gibt jedoch zahlreiche Möglichkeiten für den Schutz der Daten auf mobilen Endgeräten. Wenn Sie bereits die mobilen Endgeräte, die Ihr Unternehmen unterstützen wird, und das Mindestmaß an Sicherheit, das Sie benötigen, ausgewählt haben, ist die Entscheidung über die richtigen Tools für die sicherere Unterstützung Ihres mobilen Unternehmens sehr viel einfacher.

Es gibt eine breite Palette an Ressourcen und Sicherheitsmethoden, aus denen Sie wählen können, darunter:

Management mobiler Endgeräte: Dies ist der traditionelle IT-Ansatz, bei dem ein mobiles Endgerät von einem auf dem Gerät installierten Softwareagenten und einem Server, der entweder vom Unternehmen selbst oder mittels Cloud-Services betrieben wird, überwacht wird. Das Management mobiler Endgeräte ist für praktisch jedes Gerät von Nutzen, das in Berichten dokumentiert oder verifiziert werden muss, und kann Sie zudem bei der Implementierung, dem Management und sogar der Verteilung von Unternehmensanwendungen per Mobilfunk („over the air“) in Ihrem gesamten Unternehmen unterstützen. Das Management mobiler Endgeräte bietet Ihnen sogar die Möglichkeit, die von den Benutzern installierten Anwendungen zu sehen, den Zugriff auf Anwendungen mit Zugriffsbeschränkung zu verbieten und neue Anwendungen oder Updates vorzuschlagen. Einige Tools enthalten außerdem eine Vielzahl verschiedener Self-Service-Portale für Benutzer, mit denen die Mitarbeiter ihren Kenncode zurücksetzen, ihr Gerät sperren und die Daten auf ihrem Gerät per Fernzugriff ganz oder teilweise löschen können („Remote Wipe“), falls sie das Gerät verlieren oder es gestohlen wird. Die Implementierung des Managements mobiler Endgeräte in Eigenregie kann zu hohen Investitionsausgaben für ein Unternehmen führen. Im Gegensatz dazu sind Cloud-basierte SaaS-Systeme (Software as a Service) schneller einzurichten, einfacher zu aktualisieren und kosteneffizienter.

Wenn Sie Ihre Lösung für das Management mobiler Endgeräte konfigurieren, sollten Sie jedoch darauf achten, was Ihre Unternehmenskultur erlaubt, insbesondere mit Blick auf private mobile Endgeräte. Sie können beispielsweise einen Agenten auf einem Android-Smartphone installieren, der eine detaillierte Softwarebestandsaufnahme durchführen, die Kamera deaktivieren, den Standort per GPS verfolgen und die Daten auf dem Smartphone ganz oder teilweise löschen kann. Doch unterstützt Ihre Unternehmenskultur diese Funktionen oder werden sie als zu invasiv angesehen?

Containerisation: Einige Programme für das Management mobiler Endgeräte enthalten Funktionen für die Containerisation, die die Verschlüsselung und andere Methoden nutzen, um eine Hürde zwischen Unternehmensdaten und privaten Daten auf mobilen Endgeräten zu schaffen. Dadurch sind sie für BYOD-Programme besonders geeignet und effektiv. Einige Unternehmen kombinieren aus Gründen von Kosteneinsparungen und des Managements von Anbietern das Management mobiler Endgeräte mit der Containerisation. Wir haben jedoch festgestellt, dass sich die Komplexität deutlich verringern lässt, wenn Containerisation-Methoden und das Management mobiler Endgeräte separat bleiben.

Löschen und Sperren mobiler Endgeräte: Eine der größten Herausforderungen beim Schutz mobiler Endgeräte besteht darin, dass die Geräte mobil sind. Aufgrund ihrer Größe kann man sie leicht verlieren, und da sie mobil eingesetzt werden, sind Tracking- und Managementmechanismen erforderlich, um sensible Unternehmensdaten zu schützen. Das Löschen („Wipe“) aller Daten auf dem mobilen Endgerät nach einer bestimmten Anzahl an Anmeldeversuchen mit ungültigem Kennwort kann dazu beitragen, das Risiko eines Brute-Force-Angriffs zu reduzieren. Wenn ein mobiles Endgerät verloren geht oder gestohlen wird oder ein Mitarbeiter Ihr Unternehmen verlässt oder an eine andere Stelle in Ihrem Unternehmen versetzt wird, empfiehlt sich die Initiierung eines „Local Wipe“ durch einen Endbenutzer oder Administrator. Das Sperren eines Geräts nach einem Inaktivitätszeitlimit kann ebenfalls Sicherheitsrisiken mindern.

Wenn Sie gerade erst ein BYOD-Programm starten und keinen Agenten für das Management mobiler Endgeräte auf den privaten Endgeräten Ihrer Mitarbeiter installieren wollen, sollten Sie bedenken, dass mobile Messaging-Middleware nicht die Möglichkeit bietet, Daten teilweise zu löschen oder zu trennen.

Alternativen für Verschlüsselung und Datenspeicherung: Durch die Verschlüsselung von Daten auf mobilen Endgeräten kann ein höheres Sicherheitsniveau erreicht werden. Dabei bietet die hardwarebasierte Verschlüsselung, eine der am häufigsten eingesetzten Methoden, Vorteile gegenüber der Softwareverschlüsselung, da die Funktionalität in das Endgerät integriert ist und damit die Leistung verbessert werden kann. Browser- und virtualisierte Anwendungen können eine Alternative zur Datenspeicherung auf mobilen Endgeräten bieten. In diesem Fall werden sehr wenige oder keine Daten auf dem Endgerät gespeichert. Stattdessen werden die Daten bei Bedarf abgerufen und angezeigt, wodurch das Risiko eines Datenverlusts sinkt. Allerdings ist dafür Netzwerkzugriff erforderlich, d. h., Benutzer können weder offline noch ohne Netzwerkverbindung auf Daten zugreifen. Darüber hinaus kann die Leistung geringer sein als bei einem nativen Rich Client, der auf lokale Daten auf dem mobilen Endgerät zugreift. Außerdem kann es für die Endbenutzer zu längeren Antwortzeiten kommen.

Benutzerbasierte Authentifizierung und Betrugsvermeidung: Die benutzerbasierte Authentifizierung in zwei Schritten – zunächst für die Anmeldung am Gerät und dann am Unternehmensnetzwerk – kann als absolute Mindestanforderung eingerichtet werden, um zu kontrollieren und zu überwachen, wer auf Ihre Unternehmensdaten und -anwendungen zugreift.

Ein numerischer oder alphanumerischer Standardkenncode kann für die Anmeldung am Gerät verlangt werden, während für den Zugriff auf das Netzwerk eine komplexere Authentifizierungsmethode – z. B. eine Smartcard, ein digitales Zertifikat oder ein Token – verwendet werden kann.

Einige Geräte unterstützen nur Kenncodes, aber BlackBerry bietet auch Smartcard-Unterstützung. Erweiterte Sicherheitsmaßnahmen können jedoch in mobile Anwendungen integriert werden. Beispielsweise können Sie zusätzliche Authentifizierungsverfahren für den Zugriff auf besonders sensible Daten und Anwendungen vorschreiben. Dazu zählen biometrische Indikatoren, z. B. der Stimmenausdruck, die Sie mit den gespeicherten Datensätzen abgleichen können. Ein mehrschichtiges Authentifizierungsverfahren ist eine effektive Methode für die Reduzierung der Zahl von Sicherheitsverletzungen.

Wenn Sie VPN-Zugriff auf das Intranet Ihres Unternehmens erlauben wollen, sollten Sie Funktionen integrieren, die kontrollieren, auf welche IP-Adressen der Zugriff möglich ist.

All diese Methoden können jedoch kostenaufwendig und komplex zu implementieren sein. Daher ist es wichtig, dass Sie bei der Entscheidung über die Methoden der Authentifizierung und Betrugsvermeidung, die Sie implementieren wollen, die richtige Balance aus Kosten und einfachem Management sicherstellen.

Management von Sicherheitsbedrohungen für mobile Endgeräte: Praktisch alle mobilen Endgeräte können mit Malware infiziert werden. Ein wirksamer Ansatz für die Reduzierung von Malware ist die Implementierung von Schutzmaßnahmen, die mit denen für die Desktop- und Laptop-Umgebung vergleichbar sind. Dazu gehört, dass alle

Benutzer Anti-Malware-Software installieren und automatisch ausführen sowie regelmäßige Prüfungen in Echtzeit durchführen müssen. Sie sollten Ihre Mitarbeiter proaktiv anweisen, nur vertrauenswürdige Anwendungen herunterzuladen und zu installieren und entsprechende Maßnahmen zu ergreifen, z. B. Virenprüfungen durchzuführen, wenn verdächtige Anwendungen festgestellt werden. Die Erstellung eines individuell angepassten App-Stores, von dem Ihre Mitarbeiter nur offiziell geprüfte und unterstützte Unternehmens- und sonstige Anwendungen herunterladen können, kann Malware in Ihrem Netzwerk ebenfalls eindämmen.

Richtlinie für die Sicherheit mobiler Endgeräte: Schließlich müssen Sie Richtlinien für den Schutz Ihres Unternehmens vor Haftungs- und Sicherheitsrisiken erstellen und durchsetzen. Bei der Erstellung von Richtlinien für die Sicherheit mobiler Endgeräte sollten Sie sich mit der Rechtsabteilung und den IT-Mitarbeitern Ihres Unternehmens oder mit Partnern beraten, die die technischen Details Ihrer Maßnahmen für die Sicherheit mobiler Endgeräte kennen. Ihre Richtlinie für die Sicherheit mobiler Endgeräte sollte die folgenden wichtigen Punkte beinhalten:

- Die mobilen Endgeräte, die Sie unterstützen werden – darunter unternehmenseigene und private Endgeräte, das Maß an Endbenutzersupport, das Sie bereitstellen werden, und die Art und Weise des Zugangs zu Support. Sie sollten auch erklären, warum Sie bestimmte Plattformen unterstützen und andere nicht. Beispielsweise haben Sie die Möglichkeit, nur Plattformen zu unterstützen, die die Verschlüsselung ermöglichen, wodurch bestimmte mobile Endgeräte ausgeschlossen werden.
- Definitionen aller wichtigen Begriffe, darunter grundlegender Begriffe wie mobiles Endgerät und Management mobiler Endgeräte.
- Wer hat Zugriff auf bestimmte Daten und Anwendungen?
- Daten und Aktivitäten, die Ihr Unternehmen überwachen und verfolgen wird, unterschieden nach unternehmenseigenen und privaten mobilen Endgeräten. Dazu gehören Textnachrichten, E-Mail, Surfen im Internet, Downloads, GPS-Verfolgung, Instant Messaging, das Speichern von Multimediadateien und mehr.
- Eine Datenschutzrichtlinie, die genau festlegt, wofür Sie die Informationen, die auf unternehmens- und mitarbeitereigenen Geräten überwacht und verfolgt werden, verwenden werden und wofür nicht.
- Bestimmte Maßnahmen, die Ihr Unternehmen ergreifen wird, wenn ein Endbenutzer gegen die Nutzungsrichtlinien des Unternehmens verstößt.
- Definition von Schutzmaßnahmen wie z. B. Remote Wipe, die das Unternehmen ergreifen wird, wenn ein Gerät verloren geht oder gestohlen wird oder der Mitarbeiter an ein andere Stelle im Unternehmen versetzt oder gekündigt wird.

Die Vereinbarung sollte sowohl von den Mitarbeitern als auch von ihren Vorgesetzten unterzeichnet werden. Sobald Sie Ihre offizielle Richtlinie für die Sicherheit mobiler Endgeräte entwickelt haben, sollten Sie diese im gesamten Unternehmen bekannt machen und bei jeder Änderung der Richtlinie Updates verteilen. Nutzen Sie für die Bekanntmachung Ihrer Richtlinie für die Sicherheit mobiler Endgeräte Newsletter, soziale Netzwerke Ihres Unternehmens und Ihr Intranet.

Richtlinien von Gartner für Vorgaben für die Sicherheit mobiler Endgeräte[11]

- Stellen Sie sicher, dass das Richtliniendokument möglichst kurz ist. Idealerweise sollte es nur wenige Seiten umfassen.
- Achten Sie sorgfältig darauf, dass Sie anweisende Wörter wie „müssen“, „sollten“ und „dürfen“ richtig verwenden. Standards sind Anweisungen, die befolgt werden müssen. Richtlinien sind Vorschläge, die berücksichtigt werden sollten. Stellen Sie sicher, dass Fragen und Entscheidungskriterien anzeigen, wann ein Standard oder eine Richtlinie anwendbar ist und wann nicht.
- Lagern Sie Prozessdiskussionen und Erläuterungen in Anhänge oder externe Dokumente aus, anstatt das Dokument selbst damit zu überfrachten.
- Duplizieren Sie niemals Material, das in ein anderes Dokument gehört, insbesondere Dokumente, die in die Verantwortung eines anderen fallen. Geben Sie eindeutige Zitate zu externen Dokumenten an. Halten Sie die Kommunikation mit allen Dokumenteignern aufrecht.
- Vermeiden Sie mehrdeutige Konditionalaussagen wie z. B. „immer auf diese Weise, sofern nicht auf jene Weise“ und Aussagen auf der Basis von verschachtelten Negativtests wie z. B. „wenn nicht auf diese Weise, dann nicht auf jene Weise“. Verwenden Sie positive Bedingungen, die klar qualifiziert werden.
- Verwenden Sie absolute Aussagen („immer“) nur, wenn die Bedingung auch wirklich absolut ist.
- Schreiben Sie Akronyme nur einmal beim ersten Vorkommen aus.
- Stellen Sie ein Glossar mit wichtigen Begriffen, einschließlich einer Erklärung der Akronyme, am Ende des Dokuments bereit.

Vergessen Sie die Benutzerzufriedenheit nicht: Achten Sie bei der Definition von Sicherheitsrichtlinien auf die Qualität der Benutzererfahrung. Wenn Sie zum Beispiel unterschiedliche Anwendungen für mobile Endgeräte und Desktop-Geräte verlangen, kann dies den Erfolg Ihres Programms beeinträchtigen. Funktionen zum Sperren von Anwendungen können der Beliebtheit Ihres Programms ebenfalls abträglich sein. Darüber hinaus erwarten die Mitarbeiter automatische Warnmeldungen, wenn ihr Gerät nicht richtlinienkonform ist, und eine Anleitung, wie sie dieses Problem selbst beheben können. Stellen Sie Ihren Mitarbeitern diese Anleitung bereit, indem Sie ihnen Ihre Richtlinien für die Einhaltung von Sicherheitsbestimmungen regelmäßig mitteilen.

Schritt 4: Tägliche Unterstützung

Der letzte Schritt beinhaltet das Management der Sicherheit Ihrer mobilen Endgeräte auf regelmäßiger Basis und die Bereitstellung von Unterstützung für Ihre Endbenutzer.

Stellen Sie sich folgende Fragen:

- Welches Maß an Management und Support können wir für unternehmenseigene oder private Endgeräte bereitstellen?
- Haben wir die nötigen Ressourcen für Implementierung und Support oder sollen wir externe Unterstützung suchen?

Supportmitarbeiter: Mit Tools für das Management mobiler Endgeräte und Software für das Sicherheitsmanagement können Sie die Aktivitäten mobiler Endgeräte in Ihrem Netzwerk verfolgen und überwachen. Sie benötigen jedoch Mitarbeiter, um diese Aufgaben zu unterstützen und Ihr Netzwerk kontinuierlich vor den mit Mobiltechnologien verbundenen Sicherheitsrisiken zu schützen.

Ihr Programm für das mobile Unternehmen sollte zudem den Endbenutzern ein bestimmtes Maß an Support bereitstellen. Beim Start eines Programms für das mobile Unternehmen kann das Verhältnis der Anzahl an Geräten zu Mitarbeitern stark steigen. Deshalb benötigen Sie das entsprechende Personal und Budget, um diese neuen Anforderungen zu unterstützen. Zudem müssen Ihre Mitarbeiter über fundiertes Wissen auf dem Gebiet von Mobiltechnologie verfügen, um neue Supportanfragen von Endbenutzern beantworten zu können.

Methoden der Supportbereitstellung: Sie sollten ein Modell entwerfen, das die Art und Weise der Supportbereitstellung definiert. Einige Unternehmen legen eine bestimmte Zeitspanne – normalerweise eine halbe Stunde bis zu einer Stunde – für die Arbeit an einem Problem mit mobilen Endgeräten fest. Andere stellen nur Support für Netzwerkprobleme und nicht für die mobilen Endgeräte selbst bereit. Wieder andere entwerfen Mailing-Listen, Webportale und Wikis, um die Endbenutzer darin zu bestärken, ihre Erfahrung mit Supportproblemen mit anderen zu teilen. Beispielsweise kann ein Benutzer eine Frage zur Konfiguration von Microsoft ActiveSync auf seinem Gerät stellen, die andere Mitarbeiter beantworten. Eine weitere Möglichkeit besteht darin, den Endbenutzern den Abschluss einer Versicherung vorzuschreiben, die Unterstützung und Schadensersatz im Fall des Verlusts oder der Beschädigung von Geräten abdeckt. In diesem Fall sollte Ihre Richtlinie für mobile Endgeräte akzeptable Versicherungsanbieter definieren.

Implementierung, Sicherheit und Support – wie ein Partner das mobile Unternehmen unterstützen kann: Partner können Ihnen die Fachkompetenz, Technologien, Schulung und Unterstützung bereitstellen, die Sie benötigen, um Programme für das mobile Unternehmen schneller und kosteneffizienter als mit eigenen Lösungen zu implementieren und zu managen. Sowohl Einzellösungen als auch Komplettlösungen sind für folgende Aufgaben verfügbar:

- Beschaffung, Bereitstellung und Konfiguration von mobilen Endgeräten
- Entwicklung einer Strategie für das mobile Unternehmen
- Management mobiler Endgeräte und Anwendungsentwicklung
- Sicherheitsmanagement an einem Hosting-Standort oder beim Kunden
- Entwicklung von Richtlinien für mobile Endgeräte
- Help-Desk-Support für Endbenutzer
- Netzwerkservices für Optimierung, Berichterstellung, Überwachung und Integration
- Verfolgung und Durchsetzung der Einhaltung von Vorschriften
- Wartungs- und Depotservices
- Managed Services für das mobile Unternehmen, die alle Aspekte von der Strategie über die Implementierung bis zur täglichen Unterstützung abdecken

IBM Lösungen und Leistungen für das mobile Unternehmen

IBM Mobile Enterprise Services for Managed Mobility

IBM Mobile Enterprise Services for Managed Mobility bieten erweiterte Services für das Management mobiler Endgeräte sowie für Strategie und Support für eine Vielzahl von mobilen Endgeräten und Betriebssystemen, darunter RIM BlackBerry, Apple iOS- und Google Android-Smartphones und -Tablets sowie viele robuste Geräte mit Microsoft Windows Mobile. Wir können Geräte unterschiedlicher Plattformen beschaffen, installieren, konfigurieren, betreiben und verwalten. Zudem bieten wir ein flexibles nutzungsabhängiges Preismodell, das auf den Voraussetzungen, Nutzungsanforderungen und Serviceoptionen Ihrer Geräte basiert.

Mit Hilfe unserer Strategieservices können Sie überprüfen, ob Ihre Geschäfts- und IT-Umgebung die Voraussetzungen für die Einführung von Mobiltechnologie erfüllt, und einen Plan für das Management mobiler Endgeräte entwerfen. Zu unseren wichtigsten Empfehlungen gehören auf Unternehmen abgestimmte Sicherheitsrichtlinien und Governance-Strukturen, die Sie beim Management von Compliance-Fragen innerhalb und außerhalb Ihres Unternehmens unterstützen. Mit unserer Kompetenz auf dem Gebiet der Strategie und Planung einer Infrastruktur für Mobiltechnologie können wir Ihnen helfen, die richtigen Entscheidungen auf der Basis Ihrer Benutzerprofile und Geschäftsanforderungen zu treffen.

IBM Integrated Communications Services

Integrated Communications Services konzentrieren sich auf Entwurf, Implementierung und Management Ihrer Kommunikations- und Netzwerkumgebung und unterstützen Sie bei deren Optimierung, um praktisch jederzeit und überall die Kommunikation zu Geschäftszwecken zu ermöglichen. Mit diesen Lösungen können Sie wichtige Netzwerkumgebungen unterstützen und einen Wettbewerbsvorteil durch geschäftliche Innovation erreichen.

IBM Telecom Expense Management Services

Telecom Expense Management (TEM) Services beinhalten Beratungsleistungen, Software und Management-Services, die Ihnen schnellen Einblick in Ihre Telekommunikationsausgaben verschaffen und Bereiche aufzeigen, in denen kurz- und langfristige Einsparungen möglich sind.

IBM Mobile Foundation

Das Angebot IBM Mobile Foundation vereint wichtige Komponenten für die Nutzung von Mobiltechnologie in einem einzigen integrierten Paket und hilft Ihnen, das gesamte Spektrum der Herausforderungen und Chancen im Zusammenhang mit Mobiltechnologie abzudecken. IBM Mobile Foundation bietet verschiedene Leistungen für Anwendungsentwicklung, Konnektivität und Management, die eine Vielzahl verschiedener mobiler Endgeräte und mobiler Apps unterstützen.

Das Angebot IBM Mobile Foundation beinhaltet die folgenden Produkte (die auch als eigenständige Produkte erhältlich sind):

- IBM Worklight für Erstellung, Betrieb und Management von plattformübergreifenden mobilen Apps
- IBM WebSphere Cast Iron Hypervisor Edition für die Verbindung von mobilen Apps mit Cloud- und Back-End-Systemen
- IBM Endpoint Manager for Mobile Devices für die Steuerung und das Management der mobilen Geräte der Endbenutzer

IBM Mobile Foundation wird in zwei Konfigurationen angeboten:

- Enterprise Edition – ein B2E-Paket (Business to Enterprise) mit Worklight, WebSphere Cast Iron Hypervisor Edition und Endpoint Manager for Mobile Devices, das von Unternehmen für das Management interner Apps verwendet wird
- Consumer Edition – ein B2C-Paket (Business to Consumer) mit Worklight und WebSphere Cast Iron Hypervisor Edition, das für kommerzielle und kundenorientierte Apps verwendet wird

IBM Sametime

IBM Sametime ist eine exzellente Software, die einfachen und nahtlosen Zugriff auf Funktionen für Unternehmen für Instant Messaging, Anwesenheitsanzeige in Echtzeit, Online-Meetings, Telefonie, Videokonferenzen und mehr ermöglicht – wo immer die Benutzer gerade arbeiten. Die Sametime-Software erlaubt die schnellere und effizientere Interaktion mit Kunden und hilft Teams, schnellere, fundierte Entscheidungen in der Zusammenarbeit mit Personen innerhalb und außerhalb Ihres Unternehmens zu treffen, ohne dass Reisekosten anfallen.

IBM Connections

IBM Connections beinhaltet ausgereifte Analysefunktionen und ermöglicht die Überwachung von Daten nahezu in Echtzeit sowie schnellere Netzwerke für die Zusammenarbeit innerhalb und außerhalb des Unternehmens. Diese Funktionen sind am Kundenstandort, in der IBM SmartCloud oder über eine breite Palette an mobilen Endgeräten verfügbar. IBM Connections integriert Activity Streams, Kalenderfunktionen, Wikis, Blogs, E-Mail und mehr und markiert relevante Daten, die Maßnahmen erfordern. Die Software erlaubt zudem die sofortige Zusammenarbeit – mit nur einem Mausklick – und die Erstellung von sicheren Social Communitys innerhalb und außerhalb des Unternehmens. Dies sorgt für eine bessere Kundenbindung und schnellere Geschäftsergebnisse.

IBM Lösungen für die Sicherheit mobiler Endgeräte

IBM Lösungen für die Sicherheit mobiler Endgeräte unterstützen Sie bei der Abwehr von Malware, der Bereitstellung sicherer Verbindungen, der Bereitstellung des sicheren Zugriffs auf Unternehmensdaten und -systeme sowie der Entwicklung sicherer Anwendungen und einer zuverlässigen Plattform für mobile Apps. Unsere wichtigsten Sicherheitsprodukte umfassen integrierte, übersichtliche Dashboards und Funktionen für den besseren Schutz von praktisch jeder Art von Endgerät oder Netzwerk, ob Smartphone, PC, Server oder Router. Wir bieten:

- IBM Security Access Manager – für die Vereinfachung des Kennwortmanagements, die Verbesserung der Zugriffssicherheit und das bessere Management des Compliance-Nachweises
- Enterprise Wireless Networks – sichere, robuste mobile Netzwerklösungen, mit denen die Benutzer praktisch jederzeit und überall kommunizieren können

- WebSphere DataPower Service Gateway XG45 Appliance – für mehr Sicherheit von Web-Services, Anwendungen und Daten mit individuell anpassbarer, skalierbarer und automatisierter Transparenz und Governance von Services
- Hosted Mobile Device Security Management – für den Schutz Ihrer mobilen Endgeräte vor Malware und anderen Sicherheitsbedrohungen, basierend auf dem Wissen, der Technologie und den Services für das fortlaufende Management, die Ihnen praktisch eine Komplettlösung für die Sicherheit Ihrer mobilen Endgeräte bieten
- IBM AppScan – Lösungen für den Test der Sicherheit von Anwendungen und das Risikomanagement
- IBM Lotus Mobile Connect – für sicherere Verbindungen zwischen gängigen mobilen Endgeräten und Lösungen des Unternehmens

Warum IBM?

Seit mehr als 15 Jahren stellt IBM Lösungen für Mobiltechnologie für Hunderte von Kunden bereit und ist für das Management Hunderttausender von mobilen Endgeräten weltweit verantwortlich. IBM bietet Ihnen Zugang zu einem breiten Angebot an Services und innovativen Lösungen, die den gesamten Lebenszyklus der mobilen Umgebung abdecken – von der Entwicklung und Umsetzung einer Strategie für das mobile Unternehmen über das Sicherheitsmanagement bis zur täglichen Unterstützung. Sie können außerdem unsere zuverlässige globale Infrastruktur nutzen, die mehr als 5.000 Experten für integrierte Kommunikation und Netzwerke, 70 für Workplace Services zuständige Call-Center weltweit, 9 Security Operations Centers, 12 Mobility Delivery and Support Centers und über 30 Forschungslabors, die Mobiltechnologie unterstützen, umfasst.[12] Als eines der führenden Unternehmen der Branche können wir Ihnen zudem helfen, die Komplexität zu reduzieren, indem wir nahezu alle Ihre IT-Anforderungen unterstützen und die Herausforderungen im Zusammenhang mit der Servicebereitstellung durch unterschiedliche Anbieter praktisch ganz vermeiden.

IBM unterstützt die von Mitarbeitern ausgewählten mobilen Endgeräte.

Mehr als die Hälfte der IBM Mitarbeiter weltweit nutzt mobile Endgeräte. IBM musste sein unternehmensweites Programm für die Nutzung von Mobiltechnologie, das 2004 mit einem einzelnen unternehmenseigenen Gerät gestartet wurde, erweitern, um eine Vielzahl neuer mobiler Plattformen am Arbeitsplatz zu unterstützen. Über einen Zeitraum von drei Jahren testete IBM im Rahmen eines Pilotprogramms den mobilen Zugriff mit unterschiedlichen Geräten und Betriebssystemen und nahm neue Geräte wie Tablets in das Programm auf, sobald sie auf dem Markt erschienen. IBM Software für die Onlinezusammenarbeit wurde zu einem wesentlichen Bestandteil der Lösung. Bis 2011 wurde eine groß angelegte Implementierung in der Produktionsumgebung durchgeführt, bei der Mobiltechnologie als zentraler Infrastrukturservice betrachtet wurde. Heute umfasst das Programm 120.000 mobile Benutzer, von denen 80.000 ihre privaten mobilen Endgeräte verwenden – und es wird weiter ausgebaut.[13]

„Die Zunahme von BYOD-Programmen ist die radikalste Änderung im Client-Computing in Unternehmen, seit sich PCs[4] am Arbeitsplatz durchgesetzt haben. Jedes Unternehmen muss eine klare Position zu BYOD formulieren, selbst wenn es seinen Mitarbeitern die Nutzung privater mobiler Endgeräte gar nicht erlaubt.“[5]

– IBM CIO Jeanette Horan

Weitere Informationen

Wenn Sie mehr über IBM Produkte und Services für das mobile Unternehmen erfahren möchten, wenden Sie sich bitte an Ihren IBM Ansprechpartner.

Darüber hinaus kann Ihnen IBM Global Financing Finanzierungslösungen anbieten, die preislich und strategisch auf Ihre individuellen IT-Anforderungen zugeschnitten sind. Mit unseren maßgeschneiderten IT-Finanzierungslösungen helfen wir Kunden dabei, geschäftliche Ziele zu erreichen, ihr Liquiditätsmanagement zu verbessern und die Gesamtbetriebskosten zu senken. IBM Global Financing ist die clevere Wahl, wenn Sie wichtige IT-Investitionen tätigen, um Ihr Unternehmen nach vorne zu bringen. Weitere Informationen finden Sie auf der Website: **ibm.com**/financing/de

[1] IBM: „Achieving success with a flexible workplace“, Mai 2012

[2] Ibid.

[3] Gartner, „Seven Steps to Planning and Developing a Superior Mobile Device Policy“, 5. Oktober 2011

[4] Personal Computer

[5] Gartner, „Gartner Says Bring Your Own Device Programs Herald the Most Radical Shift in Enterprise Client Computing Since the Introduction of the PC“, 29. August 29 2012

[6] IBM, „Achieving success with a flexible workplace“, Mai 2012

[7] Ponemon Institute, „2011 Cost of Data Breach Study: United States“, März 2011

[8] Ibid.

[9] IBM, „Achieving success with a flexible workplace“, Mai 2012

[10] Aberdeen Group, „Hidden Costs, Unseen Value“, 17. August 2012

[11] Gartner, „Seven Steps to Planning and Developing a Superior Mobile Device Policy“, 5. Oktober 2011

[12] Statistiken Stand November 2012

[13] Statistiken Stand 2012

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**

Bitte der Wiederverwertung zuführen

ENW03011-DEDE-00