**IBM Security**
Whitepaper – Thought Leadership

# Wenn das Geschäft eine App ist, dann ist die App das Geschäft

*Teil 2: Vier Elemente einer soliden Mobile App-Strategie*

IBM

## Einführung

IBM Security, ein führender Anbieter von Enterprise-Mobile-Management-(EMM-)Lösungen, präsentiert Teil 2 einer dreiteiligen Serie, in der es um die zunehmende Bedeutung von Apps in Unternehmen sowie die Rolle der IT als wichtiger Förderer geht.

In diesem Teil erfahren Sie, wie Sie eine App-Strategie zum Erreichen Ihrer geschäftlichen Ziele entwickeln können – ohne Daten und Netzwerk Ihres Unternehmens zu gefährden.

---

*Bei der Verwendung geschäftlicher Apps spielen Erkennung, Skalierbarkeit, Nachhaltigkeit und Sicherheit eine wichtige Rolle.*

---

## Vier Elemente einer soliden Mobile App-Strategie

Wie wir in „*Teil 1: Die zunehmende Bedeutung von Apps in Unternehmen*“[1] bereits erörtert haben, verändern mobile Anwendungen von Grund auf die Art und Weise, wie Unternehmen mit Kunden und Mitarbeitern interagieren und Geschäfte erledigen. Die Entwicklung einer effektiven Strategie ist Voraussetzung dafür, dass Apps Ihrem Unternehmen reale Vorteile bieten können, während Daten und das Netzwerk geschützt bleiben. Ein angemessener Ansatz für die Verwendung von Apps muss die Aspekte Erkennung, Skalierbarkeit, Nachhaltigkeit und Sicherheit beinhalten.

## Entwickeln Sie Apps, die Ihre Benutzer benötigen

Laut einer Umfrage unter 300 Führungskräften aus dem Bereich Enterprise Mobility, die von Enterprise Mobility Exchange (EME) durchgeführt wurde[2], konzentrieren Unternehmen ihre Investitionen in Mobilität vor allem auf mobile Apps, die der Verbesserung der Mitarbeiterproduktivität dienen.

Das klingt nach einem alten Hut – nur auf einer anderen Plattform. Führungskräfte von Unternehmen haben folgende Ziele: produktivere Mitarbeiter, eine verbesserte Kundeninteraktion sowie vereinfachte Geschäfts- und Arbeitsabläufe. IT-Abteilungen müssen sicherstellen, dass Mitarbeiter im Netzwerk kein Unheil anrichten sowie keine größeren Sicherheitsrisiken (sowie Kosten) verursachen können.Bei der Entwicklung eines auf mobilen Apps basierenden Betriebs geht es jedoch nicht um die Frage Geschäft versus IT. Vielmehr kommt es darauf an, dass IT- und Geschäftsabteilungen gemeinsam an der Entwicklung einer effektiven Strategie arbeiten.

Zum einen muss die IT die übergeordneten Ziele von App-basierten Initiativen kennen. Zum anderen muss sie zusammen mit der Geschäftsführung und Benutzern herausfinden, wie Personen – sowohl Kunden als auch Mitarbeiter – Geräte nutzen, um miteinander zu kommunizieren und auf benötigte Informationen zuzugreifen. Zudem muss ermittelt werden, welche Informationen sie nutzen und teilen und welche Probleme dabei auftreten können. Dieser Prozess sollte alle Geschäftseinheiten und Anwendungsfälle beinhalten – schon bei der Entwicklung einer einzigen App –, damit sich Lücken und Inkonsistenzen im fertigen Produkt verhindern lassen. Gemeinsam mit geschäftlichen Mitarbeitern muss die IT-Abteilung folgende Fragen klären:

- Wie soll die App genutzt werden? Wird sie der direkten Kundeninteraktion dienen?
- Auf welche Funktionen kommt es besonders an?
- Wie lassen sich diese Funktionen implementieren?
- Auf welche Systeme wird zugegriffen?
- Welche Sicherheitsrisiken werden mit der App verbunden sein? Was würde geschehen, wenn ein unbefugter Benutzer darauf zugreifen kann?
- Gibt es Datenschutzvorschriften, die eingehalten werden müssen?
- Welchen Nutzen soll die App haben?

## Skalierbarkeit in kürzester Zeit

Nach Fertigstellung der anfänglichen Analyse kann die IT einen Plan für die Entwicklung und Bereitstellung der App erzeugen. Unabhängig von der ursprünglich skizzierten Größe oder Nutzung ist es wichtig, eine mobile App zu erstellen, die sich problemlos skalieren lässt und gleichzeitig hohen Komfort bietet. Bei der Auswahl der Technologien, die als Grundlage für Ihre Apps dienen sollen, müssen Sie folgende Aspekte hinsichtlich der fertigen Infrastruktur beachten:

- Wir können wir sicherstellen, dass unsere App über unterschiedliche Geräte und Betriebssysteme hinweg für ein konsistentes Benutzererlebnis sorgt?
- Kann unsere Anwendungsarchitektur variable Nutzerzahlen unterstützen?
- Was geschieht mit unserem Netzwerk, wenn die Back-End-Schnittstellen mit zusätzlichen Systemen und/oder Datenbanken verknüpft werden?
- Ist unser Netzwerk leistungsfähig genug, um eine steigende Zahl an gleichzeitig verbundenen Geräten zu unterstützen?
- Wie können wir Engpässe bei der Planung, Bereitstellung und Nutzung verhindern?

## Wandel ist unvermeidlich

Mit der Zeit müssen Apps aktualisiert werden. Darum müssen Sie langfristig planen. Im Gegensatz zu Webanwendungen, die auf einem Server bereitgestellt werden, befinden sich mobile Apps auf den Geräten selbst. Das bedeutet, dass regelmäßige und rasche Änderungen an einer App nicht möglich sind. Egal ob aufgrund von schwankender Benutzernachfrage oder Betriebssystemupdates sind Änderungen jedoch erforderlich. Darum muss die IT bei der Entwicklung von Apps auch deren Nachhaltigkeit berücksichtigen.

- Sind die Front-End-Funktionen der App anpassungsfähig genug, um von Benutzern geforderte neue Funktionen unterstützen zu können?
- Können wir Benutzern sofort nach Aktualisierung ihrer Betriebssysteme Zero-Day-Updates bereitstellen?
- Wie sieht unser Verfahren für die Kollaboration und Erkennung von Benutzer-Apps aus?
- Können wir Feedback von Benutzern berücksichtigen, um eine kontinuierliche Planung und Entwicklung zu ermöglichen?

## Sicherheit bei jedem Schritt – . . nicht erst im Nachhinein!

Im nächsten Teil mit dem Titel „*Sicherheitsrisiken bei der Verwendung mobiler Apps bewältigen*“ werden wir auf den letzten – aber definitiv nicht unwichtigen – Aspekt eingehen: die Verbesserung der Sicherheit mobiler Apps.[3] Mobile Apps sind immer öfter Ursache für Sicherheitsrisiken in Unternehmen – durch unzureichende Datenspeicherverfahren, Schadsoftware, unbefugte Zugriffen, fehlende Verschlüsselung und Datenlecks bei der Synchronisation.

Gartner geht davon aus, dass 75 Prozent aller mobilen Apps 2015 bei einfachen Sicherheitstests versagen werden und Hackern, die versuchen, in ein Unternehmensnetzwerk einzudringen, als Einfallstor dienen können.[4] Beim kürzlichen Masque Attack[5] wurde die offizielle App eines Unternehmens mit einer schädlichen App überschrieben, die auf Benutzergeräten nicht erkennbar war, da sie sich als die ursprüngliche App ausgab.

Im Zuge der zunehmenden Verbreitung von Apps in Unternehmen werden auch sich die Risiken für geschäftliche Daten und Netzwerke erhöhen. Sicherheitsaspekte müssen in jeder Stufe der Entwicklung und Bereitstellung berücksichtigt und implementiert werden.

Gemeinsam mit anderen Lösungen aus dem IBM® MaaS360® Portfolio kann MaaS360 Ihnen dabei helfen, eine Strategie für mobile Apps zu entwickeln, die Ihr Unternehmen voranbringt und gleichzeitig für die erforderliche Skalierbarkeit, Nachhaltigkeit und Sicherheit sorgt. Wenden Sie sich noch heute an IBM, um zu erfahren, wie Sie die Welt der mobilen Apps optimal nutzen können.

Wollen Sie Apps zur Verbesserung Ihrer Geschäftsabläufe verwenden? Dann sehen Sie sich den Rest der Serie an:

- **Teil 1:** ***Die zunehmende Bedeutung von Apps in Unternehmen.*** Erforschen Sie die zunehmende Bedeutung von Apps in Unternehmen, inklusive der Rolle der IT als wichtiger Förderer App-basierter Mitarbeiterproduktivität und Kollaboration, geschäftlichen Wachstums und verbesserter Kundeninteraktion.
- **Teil 3:** ***Sicherheitsrisiken bei der Verwendung mobiler Apps bewältigen.*** Verschaffen Sie sich Informationen über technische und praktische Aspekte einer effektiven Unterstützung und Sicherung Ihres Unternehmens hinsichtlich der Entwicklung und Implementierung App-basierter Geschäftsabläufe.

## Verwandte Ressourcen

- Mobilität für Ihre Unternehmensinhalte und Apps[6]
- Gute Apps, schlechte Apps: Der Nutzen einer Schaffung einzigartiger mobiler Momente[7]
- Vier Tipps zum Schutz Ihres Unternehmens vor Bedrohungen durch mobile Apps
- Best Practices für das Mobile Application Lifecycle Management[8]
- Webinar: Planung, Entwicklung und Bereitstellung mobiler Apps
- IBM® MaaS360® Mobile Application Management

## Über IBM MaaS360

IBM MaaS360 ist eine Enterprise-Mobility-Management-Plattform, die bei mobilen Geschäften für hohe Produktivität und maximalen Datenschutz sorgt. Tausende von Unternehmen nutzen MaaS360 bereits als Grundlage für mobile Initiativen. MaaS360 ermöglicht eine umfassende Verwaltung mit zuverlässigen Sicherheitskontrollen für alle Benutzer, Geräte, Apps und Inhalte und unterstützt die Entwicklung einer optimalen mobilen Strategie. Wenn Sie weitere Informationen erhalten und IBM MaaS360 30 Tage lang kostenlos testen möchten, besuchen Sie www.ibm.com/maas360

## Über IBM Security

Die Sicherheitsplattform von IBM stellt Sicherheitsinformationen bereit, damit Unternehmen ihre Mitarbeiter und Kunden, Daten, Anwendungen und Infrastruktur umfassend schützen können. Wir bieten Lösungen für Identitäts- und Zugriffsmanagement, Sicherheitsdaten- und Vorfallmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Intrusion Protection der nächsten Generation und vieles mehr an. IBM verfügt über eines der größten Forschungs-, Entwicklungs- und Bereitstellungsteams für Sicherheitslösungen weltweit. Weitere Informationen hierzu finden Sie im Internet unter **ibm.com**/security

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

Hergestellt in den Vereinigten Staaten von Amerika,
März 2016



Bitte der Wiederverwertung zuführen

WGW03106-DEDE-01

1 IBM Security, *Wenn das Geschäft eine App ist, dann ist die App das Geschäft – Teil 1: Die zunehmende Bedeutung von Apps in Unternehmen*, 2015, **ibm.com**/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03105USEN&attachment=WGW03105USEN.PDF

2 Westacott, Robbie, *The Global State of Enterprise Mobility Report 2014/2015*, Enterprise Mobility Exchange, 3. Dezember 2014, http://www.enterprisemobilityexchange.com/the-global-state-of-enterprise-mobility-report

3 IBM Security, *Wenn das Geschäft eine App ist, dann ist die App das Geschäft – Teil 3: Sicherheitsrisiken bei der Verwendung mobiler Apps bewältigen*, 2015, **ibm.com**/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03107USEN&attachment=WGW03107USEN.PDF

4 „Gartner Says More than 75 Percent of Mobile Applications will Fail Basic Security Tests Through 2015“, Gartner, 14. September 2014, http://www.gartner.com/newsroom/id/2846017

5 IBM Security Intelligence, Vier Tipps zum Schutz Ihres Unternehmens vor Bedrohungen durch mobile Apps, 11. Februar 2015, https://securityintelligence.com/four-tips-for-protecting-the-enterprise-against-mobile-app-threats/

6 IBM Security, *Mobilität für Ihre Unternehmensinhalte und Apps*, 2015, **ibm.com**/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03111USEN&attachment=WGW03111USEN.PDF

7 „Gute Apps, schlechte Apps: Der Nutzen einer Schaffung einzigartiger mobiler Momente“, Studie von Forrester im Auftrag von IBM, IBM MobileFirst, 2014, http://www.ibm.com/mobilefirst/us/en/good-apps-bad-apps.html

8 IBM Security, *Best Practices für das Mobile Application Lifecycle Management*, 2015, **ibm.com**/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03110USEN&attachment=WGW03110USEN.PDF