IBM Security
Whitepaper – Thought Leadership

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

Teil 3: Sicherheitsrisiken bei der Verwendung mobiler Apps bewältigen

IBM

Einführung

IBM Security, ein führender Anbieter von Enterprise-Mobile-Management-(EMM-)Lösungen, präsentiert Ihnen Teil 3 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 lernen Sie zentrale Sicherheitsrisiken mobiler Apps in Unternehmen kennen und erfahren, wie Sie Bedrohungen im App-basierten Geschäftsumfeld abwehren können.

Sie erhalten Informationen über technische und praktische Aspekte einer effektiven Unterstützung und Sicherung Ihres Unternehmens bei der Entwicklung und Implementierung App-basierter Geschäftsabläufe.

Sicherheitsrisiken bei der Verwendung mobiler Apps bewältigen

Wie in Teil 1 und 2 (siehe Fußnoten 4 und 5) dieser Serie beschrieben bringen mobile Anwendungen bei der Ausführung von Geschäften radikale Veränderungen mit sich. Um die Vorteile einer zunehmenden Verwendung von Apps richtig nutzen zu können, müssen IT-Abteilungen eine effektive Strategie entwickeln, die die Aspekte Erkennung, Skalierbarkeit, Nachhaltigkeit und Sicherheit umfasst.

Apps stellen eine hervorragende Methode zur Verbesserung der Produktivität und Kundeninteraktion dar, sind jedoch auch mit großen Risiken verbunden, die von der IT-Abteilung bewältigt werden müssen. IDC sagt voraus, dass sich die Zahl der für Mobilität optimierten Unternehmensanwendungen bis 2016 vervierfachen wird – angetrieben vom steigenden Wettbewerbsdruck und neuen Technologien, die eine schnellere und sicherere Verbreitung von geschäftlichen Apps ermöglichen.[1] Dabei darf Sicherheit nicht einfach nur ein Element sein, das hinzugefügt wird, wenn eine App fertig für die Bereitstellung ist – vielmehr muss dieser Aspekt in jeder Phase der App-Entwicklung berücksichtigt und implementiert werden.

Egal ob ruhend oder aktiv – App-bezogene Daten sind stets Gefahren ausgesetzt

Enterprise-Anwendungen sind besonders anfällig für Datenlecks, da sie direkt auf Informationssysteme und Dateien von Unternehmen zugreifen können. Die Sicherheit von in Apps genutzten Daten – egal ob diese ruhen oder aktiv sind – muss bereits bei der Planung und Entwicklung berücksichtigt werden.

Wie im Whitepaper „*Best Practices für das Mobile Application Lifecycle Management*“[2] erörtert müssen IT-Abteilungen jeden Schritt der Planung und Entwicklung von Apps unterstützen, um im gesamten Lebenszyklus für maximale Sicherheit sorgen zu können. Hier ein kurzer Überblick über die absoluten Grundlagen:

Bei ruhenden Daten:

• **Authentifizierung:** Neben Authentifizierung für mobile Geräte sollten Sie Authentifizierung auch in Ihre Apps integrieren, damit ausschließlich befugte Benutzer auf spezifische Apps und Daten zugreifen können, selbst wenn diese aus Versehen an unbefugte Benutzer verteilt werden.

- **Single Sign-On:** Bei der Entwicklung von Apps können IT-Abteilungen Benutzern mit einem zentralen Kennwort Zugriff auf alle zugelassenen Unternehmens-Apps bieten (eine Funktion, wie sie die meisten Benutzer wünschen und erwarten). Diese Funktion sorgt für einen stärker benutzerzentrierten Ansatz, wenn mobile Apps mithilfe einer Entwicklungsplattform erzeugt werden.
- **Data Loss Prevention (DLP) mit einem Dual-Persona-Ansatz:** Entwickler und MDM-Administratoren können einen geschützten Container wie IBM® MaaS360® Trusted WorkPlace, verwenden, um Datenlecks, eine Vermischung geschäftlicher und privater Daten sowie Datenschutzprobleme bei Mitarbeitern zu verhindern. IBM MaaS360 Trusted WorkPlace erlaubt es, das Kopieren und Einfügen von Daten außerhalb des Containers zu deaktivieren (und bei solchen Versuchen die IT-Abteilung zu alarmieren). Dank „Open-in“-Kontrollen können Benutzer Dokumente und Dateien im Container ausschließlich mit vom Unternehmen genehmigten Apps öffnen.

Bei aktiven Daten:

Durch einen Schutz von aktiven Daten wird das Risiko von Man-in-the-Middle-Angriffen deutlich reduziert, wenn Daten zwischen Unternehmensservern und einem mobilen Gerät übertragen werden. Wenn Sie die IBM® MaaS360® Gateway Suite verwenden, ist dies ohne VPN-Infrastruktur möglich. Außerdem können App-Entwickler mit Funktionen für eine automatische Überwachung der Sicherheit Richtlinien einrichten, um Benutzer am Öffnen von Apps auf einem Gerät zu hindern, das den Richtlinien nicht entspricht.

Diese Sicherheitsmaßnahmen klingen gut, erschweren sie aber nicht das Entwicklungsverfahren?

In der Community, die sich mit mobiler Sicherheit befasst, wird viel darüber diskutiert, was besser ist – App-Wrapping oder Containerisierung. Beide Ansätze sind mit unterschiedlichen Erfahrungen für Entwickler, Administratoren und Benutzer verbunden. App-Wrapping setzt keine Codeänderungen voraus, während dies bei einer codebasierten Containerisierung der Fall ist. Containerisierung bietet aber genauere Kontrollmöglichkeiten als das App-Wrapping. Ein kürzliche Umfrage von Forrester[3] hat ergeben, dass App-Wrapping mit leichtem Vorsprung die bevorzugte Wahl ist. Welche Technologie besser geeignet ist, hängt jedoch in Wahrheit von Prioritäten und Ressourcen des jeweiligen Unternehmens ab. Die IBM® MaaS360® Productivity Suite bietet Entwicklern und Administratoren mobiler Lösungen beide Optionen:

- **App-Wrapping:** IBM® MaaS360® Mobile Application Security, das in die Mobile Application Management Plattform integriert ist, bietet Workflows in einem Fenster, in dem Sie ganz einfach Kontrollkästchen aktivieren können, um automatisch Sicherheitskontrollen beim Hochladen und Bereitstellen von Apps zu integrieren.
- **Containerisierung:** Mit dem MaaS360 Mobile Application Security Software Development Kit (SDK) können Entwickler Sicherheit der Enterprise-Klasse direkt im App-Code aktivieren und private sowie öffentliche Apps in kürzester Zeit um Containerisierungsfunktionen erweitern.

Bis zur Bereitstellung… und darüber hinaus

Im Anschluss an die sichere Entwicklung Ihrer App ist diese fertig zur Bereitstellung an Benutzer. Eine der einfachsten und sichersten Methoden zur Verteilung und Kontrolle ist ein Enterprise App Store. Mit dem IBM® MaaS360 Katalog können Administratoren sowohl öffentliche Apps als auch intern entwickelte Unternehmens-Apps verwalten.

Die Sicherheit von Apps endet jedoch nicht bei der Bereitstellung. Durch eine Anwendung „passiver“ Best Practices für Anwendungssicherheit können Sie Apps mit geringem Aufwand verwalten und schützen – durch:

- Whitelisting und Blacklisting von Anwendungen
- Konfiguration von Sicherheit und Einschränkungen
- Automatische Durchsetzung von Aktionen bei fehlender Compliance (Warnhinweise, Sperrung des Geräts, selektives oder vollständiges Löschen des Geräts)
- Automatische Überwachung von Jailbreak-, gerooteten und anderweitig nicht konformen Geräten
- Kontinuierliche Sichtbarkeit des Compliance-Status für alle Geräte
- Berichte zum Sicherheits- und Compliance-Verlauf

Verwendung von Apps in Ihrem Unternehmen

Wie bereits in Teil 1 und 2 erörtert (siehe Fußnoten 4 und 5) können es sich Unternehmen nicht mehr leisten, keine sicheren Apps bereitzustellen. Bei dieser Aufgabe kommt Ihnen eine Schlüsselrolle zu. Wenn es darum geht, eine App-Strategie zu entwickeln, mit der sich die Mitarbeiterproduktivität, Kundeninteraktion und Umsätze verbessern sowie Geschäftsabläufe vor Malware, Datenlecks und anderen ernsthaften Bedrohungen schützen lassen, ist Ihr Unternehmen auf Ihre Unterstützung angewiesen.

Diese Aufgabe müssen Sie jedoch nicht allein bewältigen. Zusammen mit anderen Lösungen aus dem IBM IBM MobileFirst Portfolio kann Ihnen MaaS360 bei der Entwicklung von Apps zur Seite stehen. Wenden Sie 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**[4] 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 2: Vier Elemente einer soliden Mobile App-Strategie.**[5] Entwickeln Sie zusammen mit Ihren Benutzern eine App-Strategie, die den Anforderungen Ihres Unternehmens gerecht wird.

Verwandte Ressourcen

- Mobilität für Ihre Unternehmensinhalte und Apps[6]
- Gute Apps, schlechte Apps: Der Nutzen einer Schaffung einzigartiger mobiler Momente[7]
- Malware, Masque und mehr: Schützen Sie Endbenutzer vor ihren Apps (MaaS360)
- Webinar: Planung, Entwicklung und Bereitstellung mobiler Apps (MaaS360)
- MaaS360 Mobile Application Security
- 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 www.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

WGW03107-DEDE-01

1 „*IDC Reveals Worldwide Mobile Enterprise Applications and Solutions Predictions for 2015*“, BusinessWire, 18. Dezember 2014, http://www.businesswire.com/news/home/20141218006258/en/IDC-Reveals-Worldwide-Mobile-Enterprise-ApplicationsSolutions#.VSfAlig0qVh

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

3 Shields, T., *Mobile Application Security – The Fight Results*, Forrester Research, Inc. Blog, 7. Juli 2014, http://blogs.forrester.com/category/application_wrapping/

4 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

5 IBM Security, *Wenn das Geschäft eine App ist, dann ist die App das Geschäft – Teil 2: Vier Elemente einer soliden Mobile App-Strategie*, 2015, ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03106USEN&attachment=WGW03106USEN.PDF

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