Mobile Apps: Trends und Vorgehensweisen

Know-how Der Wunsch nach vermehrter Verwendung von Anwendungen aller Art auch auf mobilen Geräten ist mit Herausforderungen verbunden. Welches sind die Treiber, Lösungsansätze und zu berücksichtigende Themenbereiche beim Mobile Application Management?

Von Patrick Trevisan

Smartphones und Tablets durchdringen immer mehr die Nutzung der Endgeräteflotte in den Unternehmen. Denn zunehmend werden nicht mehr nur E-Mail oder Kalenderfunktionen von mobilen Mitarbeitenden zur Zusammenarbeit genutzt. Immer häufiger kommen auch Unternehmens-Apps oder der mobile Zugriff auf Firmeninfrastrukturen zum Einsatz – ganz abgesehen von dem vermehrten Wunsch nach der Auslagerung von Teilen der IT in die Cloud. Dies sowie der Wunsch nach der Nutzung privater Geräte (Bring Your Own Device, BYOD) oder von Geräten, die vom Unternehmen zur Verfügung gestellt werden und gleichzeitig für die private Verwendung zugelassen sind (Company Owned Personal Enabled, COPE), stellt IT-Sicherheitsverantwortliche und -Administratoren gleichermassen vor Herausforderungen. Hinzu kommt, dass der Benutzer – anders als beim User herkömmlicher PC oder Laptops – auch Administratorenrechte besitzt, mobile Betriebssysteme regelmässig und mittlerweile automatisiert Versions- und Funktionsupdates erhalten und damit insgesamt die IT nur noch über limitierte Einschränkungs- und Kontrollfunktionen verfügt. Nicht zuletzt werden Smartphones und Tablets deshalb immer häufiger auch Ziele für Hacker, Man-in-the-Middle-Angriffe, Data Mining, Crypto-Angriffe und vieles mehr.

Trends im Mobile Application Management

Mobile Application Management (MAM), also das Verwalten mobiler Apps, ist wie das mobile Gerätemanagement (Mobile Device Management, MDM) Teil eines gesamtheitlichen Enterprise Mobility Managements (EMM). Es empfiehlt sich, Unternehmens-Apps mittels EMM-Plattformen wie beispielsweise von Blackberry, Citrix, IBM Maas360, Microsoft Intune, Mobileiron, Sophos oder Vmware in die Architektur und Umgebung des Unternehmens zu integrieren. Dies ermöglicht beispielsweise den Benutzern die Suche nach intern entwickelten Apps und genehmigten öffentlichen Business-Apps. Unternehmen können damit via EMM-Appstore ihre Apps direkt aus den Appstores von Apple, Google und Microsoft veröffentlichen oder die App-Lizenzverwaltung skalieren. Darüber hinaus können Konfiguration von App-Einstellungen und Richtlinien automatisiert, Unter-

nehmensdaten abgesichert und gleichzeitig der Datenschutz für private Daten der Nutzer respektiert werden. Gartner zufolge sollen bis ins Jahr 2021 60 Prozent der in Unternehmen verwendeten mobilen Apps mindestens ein Management-Steuerelement auf App-Ebene verwenden – und zwar unabhängig davon, ob es sich dabei um verwaltete oder nicht verwaltete Geräte handelt. Einer im Jahr 2015 durchgeführten Umfrage des MAM-Herstellers Apperian zufolge sollen Produktivitäts-Apps (wie z.B. Notiz- und andere Office-Apps) die grösste Auswirkung auf die Leistungsfähigkeit der Mitarbeitenden respektive den Return on Investment haben. An zweiter Stelle nannten die Befragten Apps für Aussendienstler wie zum Beispiel für Wartungspersonal, gefolgt von Verkaufs-Tools (etwa für Bestellprozesse), HR-Apps (etwa für die Zeiterfassung) und Reise-Apps (für Reservationen oder Spesen-Reporting).

MAM Standalone-Tools

Anstatt das Management der mobilen Apps mit bestehenden EMM-Plattformen zu bewerkstelligen, besteht auch die Möglichkeit, sogenannte Standalone-MAM-Werkzeuge wie solche von Appaloosa, App47, Apperian, Oracle oder Pulse Secure sowie App-zentrierte Sicherheits- und Policy-Tools von Appdome, Better Mobile Security oder Blue Cedar Networks zu verwenden. Insbesondere erstere kommen vermehrt zum Einsatz, etwa wenn Apps auf unverwalteten Geräten wie solchen von Lieferanten oder in BYOD-Szenarien verwaltet werden müssen. Oder sei dies, weil damit tiefere Lizenzkosten pro Nutzer erzielt werden können, was zweckdienlich sein kann in Anwendungsfällen, die lediglich App-Management erfordern. Denn mit MAM-Standalone-Tools lassen sich lediglich Apps und App-Lizenzen verwalten und kundenspezifische Anwendungen betreiben. Die Mehrzahl dieser Lösungen ist infolgedessen schlank angelegt und als Software as a Service beziehbar. Ob standalone oder integriert in das EMM, gewisse Themenbereiche bedürfen der vertieften Beachtung durch IT- und Sicherheitsverantwortliche. Die App Config Community (ein Verbund mehrerer EMM Hersteller, siehe Kasten) stellt Funktionalitäten und Vorgehensweisen in den vier folgenden Feldern zur Verfügung.

App-Konfiguration

Bei vielen Anwendungen müssen Benutzer im Rahmen einer einmaligen Einrichtung einer App URL, Port, E-Mail-Adresse, Server-Adresse etcetera und verschiedene Konfigurationen eingeben. Diese manuellen Konfigurationen können sich auf die Akzeptanz und den Erfolg der Initiativen eines Unternehmens für mobile Apps auswirken, die Belastung für den Helpdesk erhöhen, welcher Anrufe von Benutzern entgegennimmt, und den Aufwand für die Verwaltung der Dokumentation steigern, die häufig aktualisiert werden muss, wenn neue Updates für die Anwendung verfügbar gemacht werden. Durch die Nutzung von APIs (Application Programming Interface, dt. Anwendungsprogrammierschnittstelle) der Betriebssystem- oder EMM-Hersteller können diese Konfigurationen vom EMM-Server remote festgelegt werden, um den Einrichtungsprozess für Endbenutzer zu vereinfachen und den durch die manuelle Einrichtung verursachten Helpdesk- und Dokumentationsaufwand zu verringern. App-Entwickler wiederum können eine Reihe von Konfigurationsschlüsseln definieren, die sie von einem EMM-Server akzeptieren. Des Weiteren können IT-Administratoren die Schlüssel und Werte einfach in der Verwaltungskonsole des EMM-Anbieters festlegen, sodass sie in die App übertragen werden.

App Tunnel / VPN pro App

Möglicherweise erfordert eine Anwendung den Zugriff auf Web-Dienste, die sich hinter einer Unternehmens-Firewall befinden. Dies erfordert eine sichere App-Tunnel-Verbindung zwischen der App auf dem Gerät und den Backend-Diensten. Ein häufiger Anwendungsfall für Cloud-basierte öffentliche Apps ist die Möglichkeit, die Authentifizierung mit dem Identity Provider (IDP) eines Unternehmens über SAML (Security Assertion

APP CONFIG COMMUNITY

Die App Config Community optimiert die Einführung und Bereitstellung mobiler Unternehmensanwendungen indem sie Entwicklern einen Standardansatz für die App-Konfiguration und -Verwaltung bietet, der auf den umfassenden App-Sicherheits- und -Konfigurations-Frameworks aufbaut, die in iOS und Android verfügbar sind. Gemeinsam erleichtern die Mitglieder Entwicklern die Implementierung einheitlicher Steuerelemente, sodass Unternehmens-IT-Administratoren Apps von jeder teilnehmenden EMM-Plattform aus problemlos konfigurieren und verwalten können. Weitere Informationen: **www.appconfig.org**

Markup Language), ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen oder einen ähnlichen Standard zusammenzufassen. Da einige Organisationen die SAML-Identitätsanbieter lokal auf eine Weise bereitstellen, auf die nicht öffentlich zugegriffen werden kann, ist ein sicherer App-Tunnel erforderlich, um sich bei der App zu authentifizieren und anzumelden. Mobile Betriebssysteme aktivieren dabei eine Funktion, die allgemein als Per-App VPN bezeichnet wird. Mehrere gängige kommerzielle VPN-Anbieter unterstützen die Per-App-VPN-Funktionen. Viele EMM-Anbieter bieten auch ihre eigenen Per-App-VPN-Funktionen an. Unabhängig davon, welcher Per-App-VPN-Anbieter bevorzugt wird, kann der EMM-Anbieter das Per-App-VPN in der Regel automatisch auf Geräten verteilen und aktivieren.

Single Sign On

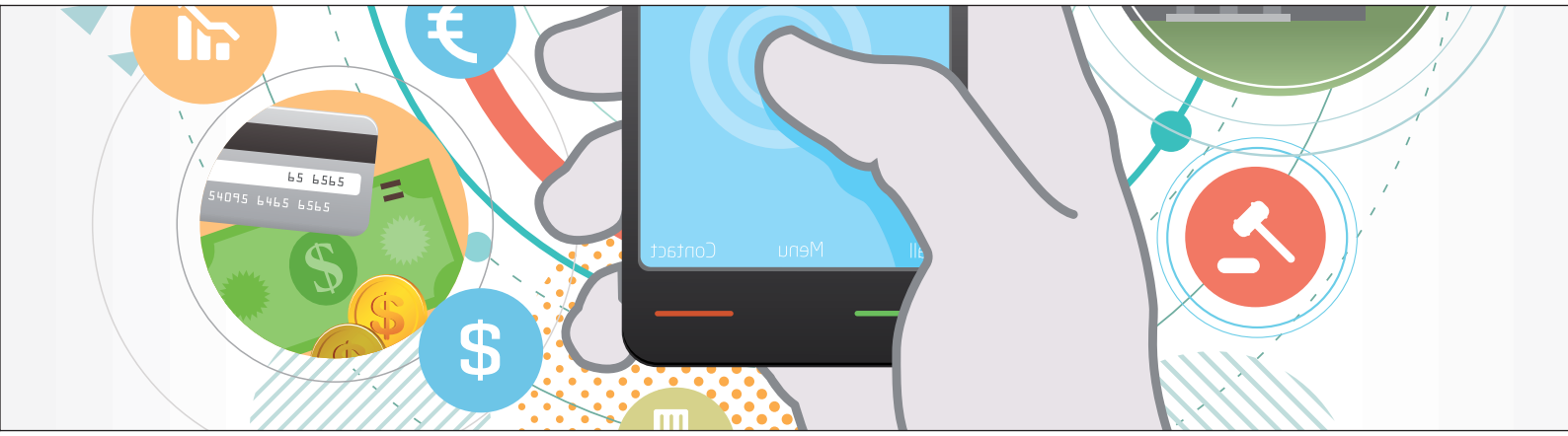
In gewissen Fällen möchten Unternehmen ihren Benutzern ermöglichen, sich mit ihren vorhandenen Arbeitsanmeldeinformationen bei einer Anwendung anzumelden und die Sicherheit für die Anmeldung so anzupassen, dass verschiedene Authentifizierungsfaktoren erforderlich sind. Sobald sich ein Benutzer erfolgreich bei einer Anwendung angemeldet hat, sollte dieser Anmeldevorgang automatisch in andere Anwendungen übertragen werden, damit die Nutzer ihre Anmeldeinformationen nicht mehrmals eingeben müssen. Viele Organisationen verwenden für diese Einmalanmeldung (engl. Single Sign-on, SSO) die Verbundauthentifizierung für einen Identitätsanbieter. Dieser unterstützt in der Regel standardisierte Protokolle (wie OAuth, Kerberos, zertifikatsbasiert oder SAML), die von vielen App-Entwicklern implementiert werden. Die von der App Config Community dokumentierte Funktion für die einmalige Anmeldung gibt eine bewährte Methode an, mit der App-Entwickler die Mandantenerkennung durchführen sollten, um den IDP über die App aufzurufen und eine einmalige Anmeldung zu ermöglichen.

Sicherheitsrichtlinien / DLP (Data Loss Prevention)

Organisationen benötigen einen detaillierten Schutz in Sachen Sicherheit und Datenverlust in Unternehmensanwendungen, um zu verhindern, dass vertrauliche Daten und Dokumente ausserhalb der Kontrolle des Unternehmens verloren gehen. Eine App kann beispielsweise eine Funktion enthalten, die ein Unternehmen aus Sicherheitsgründen deaktivieren möchte, wie etwa die Möglichkeit, Daten mit einem öffentlichen Cloud-Dateispeicherdienst zu synchronisieren. Einige Sicherheitsfunktionen werden nativ vom Betriebssystem bereitgestellt, ohne dass Code-Änderungen an der App erforderlich sind. Andere Funktionen erfordern hingegen die Implementierung einer App-Konfiguration, um eine Sicherheitsfunktion zu aktivieren. Bei der App Config Community findet sich eine Zusammenfassung einiger der Funktionen. Ein App-Entwickler kann auch eine benutzerdefinierte Sicherheitsrichtlinie implementieren.

Fazit

Bei all den unterschiedlichen Anwendungsszenarien und Anwendungsfällen gilt es insbesondere, den Spagat zwischen der Einhaltung der Sicherheit und der Gewährung eines bestmöglichen Nutzererlebnisses zu meistern. Die sichere Verwaltung mobiler Apps und die Bereitstellung entsprechender Services ist deshalb eine Herausforderung, weil sich das Know-how in Unternehmen nach wie vor hauptsächlich auf die Verwaltung der herkömmlichen PC-Infrastruktur beschränkt. Hinzu kommt erschwerend die Tatsache, dass der Wunsch nach der Verlegung möglichst vieler Services in die Cloud einhergeht mit der Vorstellung des Managements, damit vor allem Investitions-, aber auch Personalkosten einsparen zu können. Allein schon deshalb empfiehlt sich, die unabhängige Beratung eines dediziert auf das Thema sichere Bereitstellung von mobilen Services spezialisierten Experten in Betracht zu ziehen.



Eine Analyse der Bestandssituation im Unternehmen und der anstehenden Anforderungen im Bereich mobiler Apps sowie ein darauf abgestimmter Machbarkeitsnachweis (Proof of Concept) dürften den Beschaffungsentscheid entsprechend erleichtern. ■

DER AUTOR

Patrick Trevisan ist Mobile Security Consultant bei Nomasis, einem Anbieter von Dienstleistungen für den sicheren Einsatz von Tablets und Smartphones in Unternehmen. Als Spezialist in der Umsetzung von mobilen IT-Infrastrukturen betreut Nomasis über 200 aktive Kunden aus der Finanzbranche, den öffentlichen Diensten, Industrie, Gesundheitswesen, Handel und Bildung.