IBM Security
Whitepaper – Thought Leadership

Sorgen Sie für den Schutz von Android-Geräten

Reichen Updates zur Verbesserung der Geräte- und Datensicherheit, die den Namen von Süßigkeiten tragen, für Unternehmen aus?

IBM

Android ist bereit für den Einsatz in Unternehmen. Doch ist Ihr Unternehmen bereit für Android?

Einführung

Android dominiert bereits seit längerem den Verbrauchermarkt. Aktuelle Sicherheitsverbesserungen von Google und Geräteherstellern sowie Unterstützung für Android durch führende EMM-Lösungsanbieter sorgen nun für eine zunehmende Verbreitung in Unternehmen. Zur Förderung der Sicherheit und Einhaltung von Branchenstandards sowie rechtlichen Vorgaben benötigen Unternehmen Lösungen, mit denen sie das breite Spektrum an verfügbaren Geräten, Versionen und Eigenarten des weltweit populärsten mobilen Betriebssystems schützen und verwalten können.

Dafür gibt es keine Standardlösung. Die IT muss ihre Geräte- und Anwendungslandschaft analysieren und entscheiden, welche Sicherheits- und Verwaltungsfunktionen für die individuelle Mobilitätsstrategie des Unternehmens essentiell sind. Mithilfe von Plattformen wie MaaS360®, die einen flexiblen EMM-Ansatz bieten, können Unternehmen native Geräte- und OS-Kontrollen, Datencontainerisierung und Cloud-gestützte Skalierbarkeit nutzen, damit sich Android ruhigen Gewissens einsetzen lässt.

Unternehmen erlauben Mitarbeitern die Verwendung privater oder branchenspezifischer Geräte. Die IT-Abteilung muss jedoch konkrete Probleme lösen, um Unternehmensdaten zu schützen und eine standardisierte Verwaltung zu erreichen.

Android ist überall: Vor- oder Nachteil?

Mit einem Anteil von 84 Prozent am weltweiten Mobilgerätemarkt[1] dient Android als Grundlage für Hunderte von Millionen mobiler Endgeräte – die geschäftlich und privat genutzt werden – in über 190 Ländern weltweit. Das Betriebssystem weist die größte Installationsbasis aller mobilen Plattformen auf und wächst kontinuierlich weiter.

Die breite Palette an verfügbaren Android-Geräten eignet sich besonders für Programme mit unternehmenseigenen Geräten. So benötigen Außendienstmitarbeiter robuste Android-Geräte, die widerstandsfähig gegen Schmutz, Stöße, Vibrationen, Regen, Feuchtigkeit, Sonneneinstrahlung, Höhe oder Temperaturextreme sind. Andere Benutzer benötigen Android-Geräte mit Datenerfassungsfunktionen, die sich für Bestandskontrollen und Lagerhaltungsaktivitäten verwenden lassen.

Das Wachstum hat einige unerwünschte Konsequenzen und auch Folgen für die IT. Unternehmen erlauben Mitarbeitern den Einsatz privater und branchenspezifischer Geräte. IT-Abteilungen müssen jedoch konkrete Probleme lösen, um Unternehmensdaten schützen und eine standardisierte Verwaltung erreichen zu können.

Die populärste mobile Plattform der Welt weist eine durchmischte Sicherheitsbilanz auf[2]; die neuesten Android-Versionen 4.0 (Ice Cream Sandwich, Jelly Bean und KitKat), 5.0 (Lollipop) und 6.0 (Marshmellow) tragen jedoch nicht nur Namen von Süßigkeiten, sondern haben auch die größten Sicherheitslücken der Vergangenheit geschlossen. Auf der Betriebssystemseite unterstützt Android 4.0 Verschlüsselung, ein neues öffentliches Keychain-Framework für das Authentifizierungsmanagement sowie Schutz vor ausgefeilten Angriffen (zum Memory Exploits). In Android 5.0 sind viele der wichtigsten Sicherheitsfunktionen für Benutzer bereits automatisch aktiviert, darunter die Bildschirmsperre, Geräteverschlüsselung und der Gerätemanager (zur Suche nach verlorenen Geräten oder zum Remotelöschen von Daten auf Geräten). Google hat zudem durchgesetzt, dass Security Enhanced Linux (SELinux) standardmäßig implementiert ist, um zum Schutz vor Sicherheitsverletzungen die Berechtigungen von Anwendungen und Benutzern in einem System zu begrenzen. Ein neues verwaltetes Bereitstellungsverfahren unter Android 5.0 erzeugt ein geschütztes Arbeitsprofil auf dem Gerät und ebnet damit den Weg für BYOD in Unternehmensumgebungen. Im Launcher werden Apps mit einer Arbeitsplakette gekennzeichnet, um anzuzeigen, dass App und Daten innerhalb des Arbeitsprofils von einem IT-Administrator verwaltet werden.

Benachrichtigungen zum privaten Profil und Arbeitsprofil werden in einer zentralen Ansicht angezeigt. Die Daten der beiden Profile werden getrennt voneinander gespeichert – auch dann, wenn dieselbe App in beiden Profilen genutzt wird.

Android 5.0 bietet zudem einen Gastzugang für Telefone und Tablets, in dem Apps angeheftet (oder gesperrt) werden können, damit Benutzer nicht auf andere Bereiche des Geräts zugreifen können. Dies ist eine hervorragende Option, um Apps im Kiosk-Modus auf Geräten bereitzustellen, die z. B. im Handel ausliegen.

Android for Work

Google hat auf Unternehmen und ihre Bedürfnisse reagiert. Um Android für den geschäftlichen Einsatz vorzubereiten, ermöglicht Google IT-Abteilungen nun eine Verwendung von Containerisierung und Sicherheitskontrollen der Enterprise-Klasse. Die neue Enterprise-Management-Plattform namens Android for Work bietet IT-Abteilungen Folgendes:

- Trennung von geschäftlichen und privaten Daten auf Android-Smartphones
- Einfache Verwaltung und Verteilung von kostenlosen und kostenpflichtigen Google Play-Apps

Android for Work wird automatisch in Lollipop integriert und steht für Geräte, die mit Android 4.0 oder höher arbeiten, als App zur Verfügung.

Hersteller: integrierte Sicherheit und EMM-Einbindung

Viele führende Android-Gerätehersteller – wie Samsung, HTC, LG und Amazon – haben ihre neuesten Geräte um Schutzmechanismen für den Unternehmenseinsatz erweitert. Integrierte Funktionen wie ferngesteuertes Löschen von SD-Karten und Dateiverschlüsselung, WLAN-Sicherheit der Enterprise-Klasse, VPN-Zugang und die Fähigkeit, offene und verschlüsselte Informationen gleichzeitig auf einem Gerät zu unterstützen, sorgen dafür, dass eine große Zahl von Android-Geräten bereit für den Unternehmenseinsatz ist.

- Samsung KNOX bietet einen geschützten Container für Verwaltung, Pflege und Schutz von Unternehmensdaten.
- HTCpro-zertifizierte Geräte verfügen über Datenverschlüsselung auf dem Sicherheitsniveau von Regierungen sowie über VPN- und weitere fortschrittliche Sicherheitsfunktionen.
- Amazon Fire-Geräte sind mit Verschlüsselung, VPN, Single Sign-On und Funktionen zur Registrierung von Zertifikaten ausgestattet.
- LG GATE-fähige mobile Geräte bieten eine umfangreichere Sicherheitsverwaltung mit Unterstützung für erweitertes Microsoft Exchange ActiveSync, Datenverschlüsselung und VPN.

Diese vier und weitere Android-Gerätehersteller haben neben wesentlichen Sicherheitsfunktionen auch Partnerschaften mit branchenführenden Anbietern von Enterprise-Mobility-Management-(EMM-)Lösungen entwickelt. EMM-Integrationen und APIs bieten Unternehmen solide Verwaltungs- und Sicherheitsfunktionen über ein einheitliches Portal.

Best Practices und Funktionen

Angesichts der umfangreichen Sicherheitserweiterungen in den Android-Versionen 4 und 5 sollte die IT für alle Geräte mindestens Android 4.0 sowie Kennwortschutz vorschreiben. So lassen sich klassische Android-Risiken, die aus Fragmentierung und fehlender Verschlüsselung entstehen, signifikant reduzieren. Android überzeugt Unternehmen (und Benutzer) durch Flexibilität und vielfältig einsetzbare Geräte. Damit verbunden sich jedoch Risiken durch Rooting und mobile Malware, gegen die die IT zum Schutz von Unternehmensdaten Maßnahmen ergreifen muss.

Rooting: immense Risiken für Unternehmen

Benutzer können Android-Geräte durch Zugriff auf den UNIX-Kern rooten und damit praktisch beliebige Anwendungen – darunter auch Malware – installieren sowie Kontrollen auf der Anwendungsebene unterlaufen. Ein gerootetes Gerät kann Unternehmensnetzwerke derselben Malware aussetzen, die auf das Gerät geladen wurde, und so Maßnahmen zum Schutz vor Datenverlusten umgehen.

Datenverluste: das ganze Unternehmen in Ihrer Tasche

Erinnern Sie sich an die guten alten Tage? Als die Desktops auf unseren Schreibtischen noch sicher waren? Heute wandern Daten von Gerät zu Gerät und sind damit äußerst anfällig. Bei Geräten mit austauschbaren SD-Karten und USB-Anschlüssen können leicht Daten verlorengehen, auch wenn sie verschlüsselt sind. Daten, die in einem unsicheren Funknetzwerk übertragen werden, sind ebenfalls gefährdet. Verluste oder Manipulationen von Unternehmensdaten können empfindliche Strafen sowie den Verlust von Vertrauen und Loyalität der Kundschaft nach sich ziehen.

Mobile Malware: gefährlich bei beabsichtigter sowie auch unbeabsichtigter Verbreitung

In der Studie „State of Mobile App Security“[3] hat Arxan Technologies, Inc. herausgefunden, dass 97 Prozent der beliebtesten gebührenpflichtigen Android-Apps und 80 Prozent der beliebtesten kostenlosen Android-Apps bereits gehackt wurden. Da Android-Benutzer beliebige Apps aus jedem App Store installieren können (nicht nur aus Google Play), gibt es im Vergleich zu anderen mobilen Betriebssystemen einen wesentlich größeren Anteil an Apps, die mit Malware oder Social Engineering manipuliert wurden, um sie mit Malware zu verknüpfen. Das Wachstum App-basierter Innovationen in Unternehmen sowie die zunehmende Nutzung mobiler Technologien durch Mitarbeiter führt laut Arxan zu einer steigenden Zahl an gehackten mobilen Apps.

Selbst vermeintlich harmlose Apps aus dem Google Play Store können Netzwerken und Marken beträchtlichen Schaden zufügen sowie Umsatzeinbußen, unbefugte Zugriffe auf kritische Daten, Diebstahl geistigen Eigentums, Betrug und manipulierte Benutzererfahrungen zur Folge haben. Wenn einem Ihrer Kinder beispielsweise Ihr Gerät in die Hände fällt und es das beliebte Spiel Temple Run herunterlädt, kann dessen Code auf Ihr Root-Dateisystem zugreifen und den Inhalt des Cache oder auch der SD-Karte, die Sie in Ihr Gerät eingelegt haben, herunterladen. Zudem kann es Audiodateien direkt über das Mikrofon Ihres Geräts aufzeichnen und Ihren Standort ermitteln. Mit IBM® MaaS360® App Risk Management werden sämtliche (zum Teil unschönen) Sicherheitsdetails der App Temple Run sichtbar.

Zum Schließen solcher Sicherheitslücken muss die IT wissen, welche Software installiert wurde, sowie mobile Malware und gerootete Geräte erkennen, Blacklists erstellen und entsprechende Compliance-Regeln durchsetzen können.

Verwendung von EMM in einer Android-Umgebung

Egal ob unternehmenseigene oder private Geräte vorhanden sind: Viele IT-Abteilungen müssen unterschiedliche Gerätetypen, zahllose Apps und wahrscheinlich mehr als ein Betriebssystem verwalten.

Best Practices für EMM: genaue Anpassung an die jeweilige Umgebung und Sicherheitsrichtlinien.

Die IT sollte Investitionen in die Mobilitätsverwaltung auf unterschiedliche Klassen von Benutzern, Abteilungen, Regionen, Geräten und Anwendungen zuschneiden und jene Technologie wählen, die den jeweiligen Anforderungen am besten entspricht. Beispielsweise benötigen Vertriebsmitarbeiter Zugriff auf Kundenkontakte und Produktdaten, während die Personalabteilung mit deutlich sensibleren Daten umgeht, was bei Missbrauch Compliance-Haftung zur Folge haben kann. EMM ist keine Standardlösung.

MaaS360 sorgt für sichere Android-Geräte

Als Technology Preview Partner arbeitet IBM eng mit Google und anderen Herstellern wie Samsung zusammen, um Kunden eine bestmögliche Android-Erfahrung zu bieten. MaaS360 lässt sich direkt in Samsung KNOX und Android for Work integrieren. Mit MaaS360 erhalten Sie eine zusammenhängende, robuste Umgebung zur Verwaltung Ihrer verschiedenen Geräte über unterschiedliche Plattformen hinweg.

Durch Verwendung der Funktionen von Google, Geräteherstellern und MaaS360 können IT-Abteilungen vielfältige mobile Sicherheitsoptionen und eine einheitliche Plattform für die Entwicklung, Verwaltung und Skalierung eines gestaffelten oder schichtweisen Sicherheitsansatzes nutzen. Mit MaaS360 wird nur implementiert, was Sie tatsächlich benötigen. Sie wählen die individuellen Lösungen zum Schutz Ihrer mobilen Umgebung mit genau den Kontrollen aus, die Sie für Ihre Umgebung benötigen.

MaaS360	Einsatzbereiche
IBM® MaaS360® Mobile Device Management Alle Funktionen für den Lebenszyklus von Geräten, die Sie benötigen	• Zugangskontrolle und Isolierung von einzelnen Geräten oder Android OS-Versionen nach Bedarf • Schutz von Daten bei der Übertragung mit Durchsetzung von Kennwörtern, Geofencing-Regeln und kontextbezogener Verwaltung • Schutz und Beschränkung von gerooteten Geräten • Ferngesteuerte Suche, Sperrung und Löschung von verlorenen oder gestohlenen Geräten
IBM® MaaS360® Mobile Application Management Für ein intelligentes mobiles Unternehmen	• Schutz von Unternehmens-Apps durch Containerisierung • Zentrale Verwaltung mobiler Apps mit einer webbasierten Konsole • Blacklists, Whitelists und Festlegung obligatorischer Apps zur Verhinderung von Datenlecks und Netzwerkangriffen
IBM® MaaS360® Productivity Suite Erstklassiger Schutz auf individueller Ebene	• Trennung privater und geschäftlicher Daten • Einrichtung von Persona-Richtlinien auf der Benutzerebene • Online- und Offline-Compliance-Prüfungen • Löschen von Suite-Containern, App-Containern, Unternehmensprofilen oder des gesamten Geräts
IBM® MaaS360® Content Suite Kontrollierte Kollaboration	• Zentrale Verwaltung der Dokumentverteilung oder geschützter Zugriff auf vorhandene Unternehmensdateispeicher wie SharePoint, Windows-Dateifreigaben, IBM Connections, Box, Google Drive, CMIS-Quellen und viele mehr • Sicheres Anzeigen, Erstellen, Bearbeiten und Speichern von Dokumenten auf Android-Geräten in einem verschlüsselten Container • Synchronisierung von Inhalten auf unterschiedlichen Gerätetypen wie iOS-, Android- und Windows-Geräten
IBM® MaaS360® Gateway Suite Schutz Ihres Zugangs	• Geschützter mobiler Zugriff auf Unternehmensdaten ohne VPN auf dem Gerät • Mobilisierung von SharePoint, Windows-Dateifreigaben und Intranetseiten • Verwendung von In-App-VPN-Tunneln zu Ihren Unternehmenssystemen

MaaS360	Einsatzbereiche
IBM® MaaS360® Mobile Threat Management Abwehr von Angriffen, bevor sie geschehen	• Erkennung von Apps mit Malware-Signaturen aus einer regelmäßig aktualisierten Datenbank • Aktivierung einer nahezu echtzeitbasierten Engine mit Compliance-Regeln zur automatisierten Fehlerbehebung • Entdeckung von versteckten Schadprogrammen, die versuchen, die Erkennung von gerooteten Geräten zu verbergen
MasS360 App Risk Management Ermöglicht die Beseitigung riskanter Aktivitäten aus Ihren Apps	• Identifikation von Hunderten von Code-Sicherheitslücken und riskantem App-Verhalten durch umfassende automatisierte Analysen • Design und Test von App-Regeln vor der Einführung in Geschäftseinheiten, Regionen oder Arbeitsgruppen • Durchsetzung von App-Sicherheitsrichtlinien auf Benutzergeräten und in Enterprise App Stores

Android ist nun offiziell bereit für den Einsatz im Unternehmensbereich. Kontaktieren Sie uns, um zu erfahren, wie MaaS360 Ihr Unternehmen auf Android vorbereiten kann. Schützen Sie Ihre Unternehmensdaten und bieten Sie Ihren Benutzern nahtlosen Zugang zu geschäftlichen Informationen auf ihren Geräten. Nutzen Sie alle Vorteile von einheitlichen Richtlinien, Risikomanagement, App-Verteilung, Geräteverwaltung und Standardbedingungen für eine konsistente Erfahrung auf allen Android Geräten. Lernen Sie IBM MaaS360 mit unserer Testversion 30 Tage lang kostenlos kennen: **ibm.com**/maas360.

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

1 „Worldwide Smartphone Shipments Edge Past 300 Million Units in the Second Quarter; Android and iOS Devices Account for 96% of the Global Market, According to IDC“, IDC Worldwide Mobile Phone Tracker, 14. August 2014 (Paywall), http://www.businesswire.com/news/home/20140814005599/en/Worldwide-Smartphone-Shipments-Edge-300-Million-Units

2 ebd., 2014.

3 „State of Mobile App Security (Research), Apps Under Attack„ Vol. 3 (früherer Titel: „State of Security in the App Economy“), 17. November 2014, Arxan Technologies, Inc., https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

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

WGW03108-DEDE-01