IBM Security
Whitepaper – Thought Leadership

Mobile Lösungen sind der neue Spielplatz für Diebe

So können Sie Ihr Unternehmen vor mobiler Malware schützen

IBM

Zusammen mit mobilen Lösungen wachsen auch die Gefahren

Einführung

Mobilität sorgt in Unternehmen für einzigartigen Wandel – durch die fortgesetzte Verbreitung intelligenter Geräte, das explosionsartige Wachstum mobiler Apps und den zunehmenden Zugang zu Arbeitsdateien. Mitarbeiter werden von ihren Unternehmen dabei unterstützt, praktisch jederzeit und überall produktiv zu sein. Hierfür richten sie BYOD-Richtlinien ein und erlauben sogar die Nutzung privater Apps für arbeitsbezogene Aufgaben.

Untrenehmen schaffen es jedoch nicht, mit der mobilen Explosion Schritt zu halten und Sicherheitslösungen der Enterprise-Klasse bereitzustellen, die ihre sensiblen Daten zuverlässig schützen. Hacker und Diebe nutzen diese Gelegenheit, um in Netzwerke einzudringen und sich sensible geschäftliche Daten von mobilen Endgeräten zu verschaffen. IT- und Sicherheitsverantwortliche brauchen zeitgemäße, solide Sicherheitslösungen, die mobile Bedrohungen proaktiv erkennen, analysieren und entfernen.

Zu jedem Zeitpunkt sid geschätzte 16 Millionen mobile Geräte mit Malware infiziert.

Mobile Explosion im Unternehmen

Die mit dem mobilen Wachstum verbundenen Zahlen sind atemberaubend. Prognosen zufolge wird es 2014 mehr Mobiltelefone (7,3 Milliarden) auf unserem Planeten geben als Menschen (7 Milliarden).[1]

Laut Arxan Technologies wurden 2014 138 Milliarden mal mobile Apps heruntergeladen – und diese Zahl soll sich bis 2017 auf 268 Milliarden fast verdoppeln.[2]

Konsumenten waren mit der Einführung von intelligenten Geräten und Apps zur privaten Verwendung die Triebkräfte dieser mobilen Entwicklung; heute profitieren davon jedoch auch Unternehmen. Der BYOD-Trend am Arbeitsplatz setzt sich weiter fort, sodass Unternehmen ihre gesamte Belegschaft mobilisieren und ihre Beschaffungs- und Supportkosten reduzieren können. So sagt Gartner voraus, dass die Häfte aller Mitarbeiter in Unternehmen bis 2017 nach BYOD verlangen wird.[3]

Mobile Apps sorgen für neue, effiziente Workflows für Mitarbeiter. Nahtloser Zugriff auf geschäftliche Daten, E-Mails und Inhalte nimmt ebenfalls zu, was zu einer höheren Produktivität führt. Unternehmen denken bei ihren einzelnen Prozessen immer öfter zuerst an mobile Lösungen, was das Wachstum von Mobilität weiter antreibt.

Wenn mobile Apps angreifen

Hacker und Diebe stellen jedoch eine Bedrohung für die signikante Beschleunigung des geschäftlichen Wandels dar. Infektionen mobiler Geräte nehmen immer schneller zu – mit einer Steigerung von 25 Prozent 2014 im Vergleich zu 20 Prozent 2013 – zu jedem Zeitpunkt sind geschätzte 16 Millionen mobile Geräte mit Malware infiziert.[4]

Bei mobiler Malware handelt es sich um schädliche Software, die speziell auf mobile Geräte abzielt und dabei die Schwachstellen bestimmter Betriebssysteme nutzt.

Verletzungen der Datensicherheit können teuer werden, wobei sich zu den finanziellen Verlusten die Beschädigung des Unternehmensrufs gesellt. Das Ponemon Institute hat geschätzt, dass eine einzige Datenschutzverletzung 2014 im Durchschnitt 3,5 Millionen Dollar gekostet hat – 15 Prozent mehr als noch ein Jahr zuvor.[5]

Abbildung 1: Führende bezahlte Android- und iOS-Apps, die bereits gehackt wurden

Durch schädliche mobile Apps kompromittierte Geräte stellen in praktisch allen Unternehmen die größte Gefahrenquelle dar. Wenn Benutzer Verbindungen mit unsicheren Netzwerken herstellen oder riskante Apps aus nicht vertrauenswürdigen Quellen installieren, sind mobile Geräte anfällig für Malware, berichtet Arxan Technologies. 97 bzw. 87 Prozent der beliebtesten bezahlten Android- und iOS-Apps wurden bereits gehackt und in anderen App Stores bereitgestellt.[6]

Wie eine andere Studie des Ponemon Institute[7] ergeben hat, können selbst Apps vertrauenswürdiger Unternehmen, die in traditionellen App Stores verfügbar sind, enorme Risiken aufweisen. 82 Prozent der Befragten gaben an, dass mobile Apps am Arbeitsplatz die Sicherheitsrisiken sehr stark (50 Prozent) oder stark (32 Prozent) erhöht haben. Die meisten Mitarbeiter „nutzen Apps häufig“ (66 Prozent), während über die Hälfte (55 Prozent) angibt, dass ihr Unternehmen keine Richtlinien implementiert haben, in denen eine akzeptable Nutzung mobiler Apps am Arbeitsplatz definiert wird.

Lediglich 20 Prozent der Befragten erklärten, dass ihr Unternehmen einen Enterprise App Store bereitgestellt hat. Gleichzeitig gibt jedoch eine Mehrheit (67 Prozent) der Befragten an, dass Mitarbeiter nicht geprüfte mobile Apps aus anderen Quellen nutzen können, selbst wenn es einen App Store gibt. Außerdem gaben 55 Prozent der Unternehmen an, dass Mitarbeiter geschäftliche Apps aus dem Enterprise App Store auf ihre privaten Geräte herunterladen und verwenden dürfen.

Deraktuelle Stand mobiler Malware

Was ist mobile Malware?

Bei mobiler Malware handelt es sich um Schadsoftware, die für Angriffe auf mobile Geräte entwickelt wurde und dabei Schwachstellen bestimmter Betriebssysteme nutzt. Es gibt drei verbreitete Arten von Schadprogrammen:

- Spyware – Diebe und Spione, die bestimmte Arten von Daten auf Geräten entwenden und an Hacker verkaufen.
- Trojaner – Malware, die die Funktionalität von Geräten oder Apps einschränkt, automatische Transaktionen ausführt oder ohne Wissen des Benutzers Kommunikation initiiert.
- Jailbreak- oder Root-Malware – bietet Hackern bestimmte Administratorrechte für Beräte sowie Zugriff auf Dateien.

Um die jeweilige Bedrohung zu verstehen und zu erkennen, warum sie sich auf ein mobiles Endgerät konzentriert, sollten wir uns den Denkansatz der Cyberkriminellen ansehen. Mobile Geräte stellen eine der einfachsten Zugriffsmethoden auf vertrauliche Daten dar. Während Back-End-Systeme von Unternehmen mit Firewalls, Intrusion-Prevention-Systemen und Antivirus-Gateways geschützt werden, weisen weder unternehmenseigene noch private mobile Geräte den gleichen Schutz auf. Private BYOD-Geräte sind besonders anfällig, da sie sich außerhalb des Perimeters und meist außerhalb der Kontrolle des Unternehmens befinden.

Wenn Hacker den Endpunkt angreifen, können sie Malware für ein Social Engineering des Benutzers verwenden, um personenbezogene Daten sowie Anmeldedaten zu erfassen. Anschließend können sie das Konto des Benutzers übernehmen und authentifizierte Sitzungen verwenden, um private Daten zu sammeln sowie betrügerische Transaktionen auszuführen.

Angst vor Android ist reichlich vorhanden

Laut IDC dominierte Android 2014 den Markt für mobile Geräte mit einem Marktanteil von 81,2 Prozent und über 1 Milliarde ausgelieferter Geräte.[8] Das Betriebssystem beherrscht den Verbaruchermarkt, die Verbreitung in Unternehmen hingegen ist eher gering.

Das grundlegende Design sowie die Offenheit von Plattform und App-Ökosystem sind die Ursachen dafür, dass Android besonders anfällig für mobile Malwareinfektionen ist.

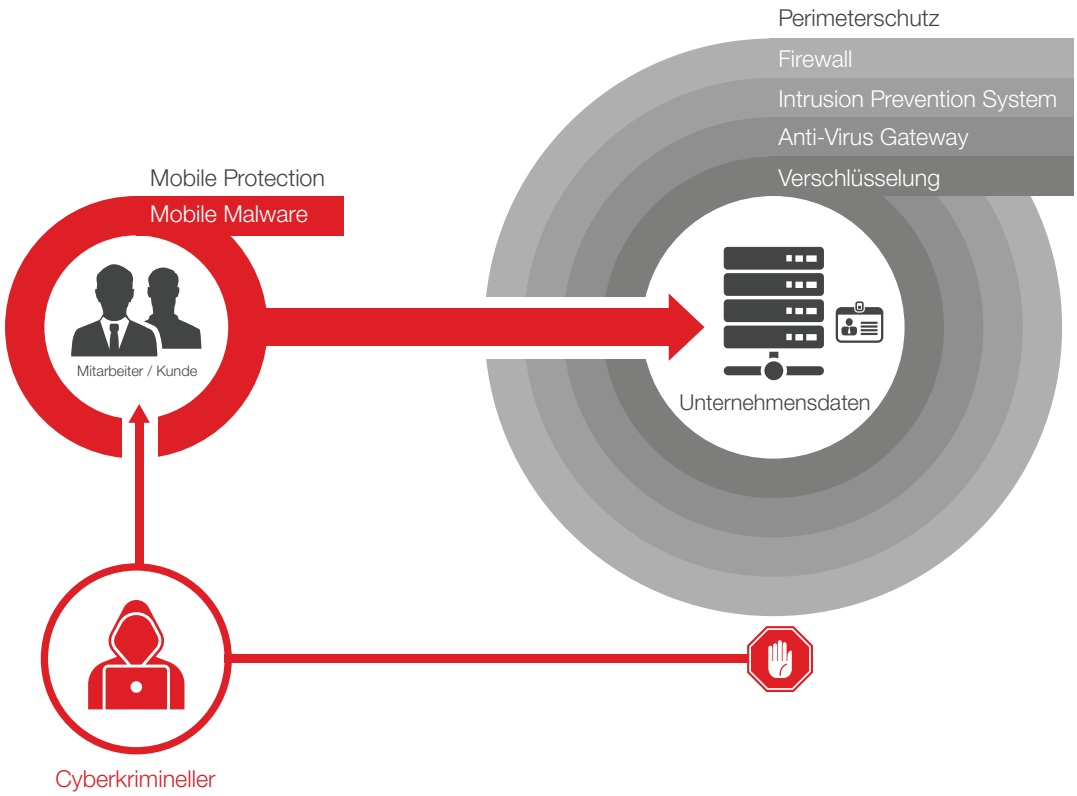

Abbildung 2: Kriminelle greifen das schwächste Glied an, um sich Zugriff auf vertrauliche Daten zu verschaffen

Das grundlegende Design sowie die Offenheit von Plattform und App-Ökosystem sind die Ursachen dafür, dass Android besonders anfällig für mobile Malwareinfektionen ist. Zu den Eigenschaften, die Android zu einem besonders leichten Ziel für Hacker und Diebe machen, gehören:

- Android-Apps können von App Stores und Websites anderer Anbieter heruntergeladen und installiert werden.
- Im Google Play Store werden Apps nicht umfassend geprüft und genehmigt, wie Apple es tut, bevor eine iOS-App in iTunes veröffentlicht wird.
- Es gibt keine Kontrolle digitaler Zertifikate zur Signierung von Android-Apps. Die Apps sind in der Regel selbstsigniert und lassen sich nicht auf den App-Entwickler zurückführen. So ist es einfach, eine Android-App zu hacken, Malware zu injizieren und eine Neusignatur vorzunehmen.

Cyberkriminelle suchen ständig nach neuen und kreativen Wegen, um die Schwachstellen mobiler OS-Plattformen, die sich von PCs unterscheiden, auszunutzen.

Google hat Sicherheitsverfahren implementiert, um schädliche Apps im Google Play Store auszusortieren. Das Unternehmen scannt Apps beim Hochladen in den Store und führt sie einzeln aus, um Malware, Spyware und Trojaner zu erkennen und zu entfernen. Wenn Google neue Malware identifiziert, können seine Systeme den gesamten Google Play Store durchsuchen und verdächtige Dateien entfernen. Google deaktitiviert Apps und Konten von Entwicklern, wenn sie die Bedingungen und Inhaltsrichtlinien des Unternehmens verletzen.

Wie jedoch bereits erwähnt wurden 97 Prozent der beliebtesten bezahlten Android-Apps gehackt und lassen sich in anderen App Stores oder Websites finden. Wenn Ihre Mitarbeiter – oder deren Kinder – also die neueste Premium-Spiele-App aus einer dieser inoffiziellen Quellen kostenlos auf ein unternehmenseigenes oder privates Android-Gerät herunterladen, können Sie davon ausgehen, dass dieses Gerät mit Malware infiziert wird. Ihr Unternehmen kann Richtlinien und Benutzerschulungen einführen, um solche Praktiken zu verhindern. Android-Geräte können jedoch ohne automatisierte Schutzebene anfällig bleiben.

Ein Beispiel für Android-Malware ist ein Banking-Trojaner namens SVPENG, der bei Angriffen auf russische und europäische Finanzinstitute entdeckt wurde. SVPENG stellt im Rahmen mobiler Malware einen deutlichen Schritt nach vorne dar. Der Angriff richtet sich direkt gegen Benutzer mobiler Banking-Apps, indem Opfer durch Verwendung eines verbreiteten Malware-Verfahrens auf PCs namens Overlay-Angriff dazu verleitet werden, ihre Anmeldedaten anzugeben.

Bei diesem Angriff wartet die Malware auf dem infizierten Gerät, bis der Benutzer die mobile App seiner Bank öffnet. Sobald die Malware erkennt, dass die Sitzung einer mobilen Banking-App startet, zeigt sie über der App (daher der Begriff „Overlay“) ein Fenster an, das das Aussehen der Banking-App imitiert, in Wahrheit jedoch eine gefälschte Seite ist. Dies zwingt den Benutzer dazu, unwissentlich mit der von der Malware erzeugten Seite zu interagieren. Er denkt, dass er es mit der echten Seite seiner Bank zu tun hat, und gibt seine Anmeldedaten ein.

Ähnliche Overlay-Anrgiffe können auch vertrauliche Unternehmensdaten bedrohen. Ein Mitarbeiter könnte unwissentlich seine geschäftlichen Anmeldedaten eingeben und Dieben damit liefern, was sie zur Anmeldung im Unternehmenssystem benötigen, sodass sie mit Ihren Daten großes Unheil anrichten können.

Vor kurzem hat das IBM X-Force® Application Security Research Team eine Schwachstelle im Dropbox SDK für Android entdeckt, über die Angreifer Apps auf mobilen Geräten mit einem Dropbox-Konto verknüpfen können, das vom Angreifer kontrolliert wird – ohne Wissen oder Zustimmung des Opfers.[9] Diese Schwachstelle namens DroppedIn lässt sich auf zwei Arten nutzen: als böswillige auf dem Benutzergerät installierte App oder als Drive-by-Methode von einer Website.

Dies stellte einen schweren Fehler im Authentifizierungsverfahren der Andoird-App dar (Dropbox SDK Version 1.5.4 bis 1.6.1). Nachdem das IBM Security Team das Problem an Dropbox gemeldet hatte, wurde es jedoch innerhalb von vier Tagen im Dropbox SDK für Android v1.6.2 behoben. Einen Überblick über den DroppedIn-Exploit finden Sie in einem Blog-Post (siehe Fußnote 9) auf SecurityIntelligence.com.

Hackers konnten den DroppedIn-Exploit aufgrund der Leichtigkeit einer Installation bösartiger Apps auf Android-Geräten nutzen. Cyberkriminelle suchen ständig nach neuen und kreativen Wegen, um die Schwachstellen mobiler OS-Plattformen, die sich von PCs unterscheiden, auszunutzen.

Zwar gibt es weiterhin Herausforderungen bei der Implementierung von Android in Unternehmen, die letzten Sicherheitsverbesserungen von Google und Geräteherstellern sowie Unterstützung führender Enterprise-Mobility-Management-(EMM-) Anbieter haben jedoch dafür gesorgt, dass die Präsenz des Betriebssystems in Unternehmen und Behörden zunimmt. Wenn sich Privatkunden und damit Ihre Mitarbeiter für eine Verwendung von Android-Geräten entscheiden, muss Ihr Unternehmen die erforderlichen Schutzmaßnahmen ergreifen, um mobile Malware abwehren zu können.

iOS ist nicht unangreifbar

iOS-Geräte waren auf dem Enterprise-Markt bislang aus verschiedenen Gründen vorherrschend. Als das iPhone 2007 auf den Markt kam, verwendeten Angestellte anstelle ihrer firmeneigenen Smartphones eigene iPhones für geschäftliche Aufgaben. Die Sandbox-Architektur und das Verhalten von iOS-Apps haben für ein grundlegend sicheres Design der Plattform gesorgt, das es Hackern erschwert, das gesamte Geräte inklusive aller Apps zu infizieren, solange Benutzer deren Sicherheitssysteme nicht absichtlich umgehen.

Nach anfänglichem Fokus auf dem Verbrauchermarkt erkannte Apple schnell das Potenzial auf dem Enterprise-Markt. Das Unternehmen sorgte mit Unterstützung von Mobile-Device-Management-(MDM-) Lösungsanbietern für eine rasche Integration von Kontrollen, um IT-Managern eine bessere Sicherung und Verwaltung von Geräten, Apps und Daten zu ermöglichen.

Im Gegensatz zur offenen App-Architektur und dem offenen Ökosystem von Android weist Apple eine deutlich geschlossenere Geräte- und App-Umgebung auf. Öffentliche iOS-Apps lassen sich ausschließlich über den iTunes App Store herunterladen und installieren, solange bei einem iOS-Gerät kein Jailbreak vorgenommen wurde. Apps, die auf iTues hochgeladen werden, durchlaufen ein intensives Prüfungsverfahren, bevor sie von Apple offiziell freigegeben werden. Außerdem werden zur Signierung von iOS-Apps digitale Zertifikate benötigt, sodass sich Apps zu ihrem Entwickler zurückverfolgen lassen.

Alle diese Gründe haben zur Beliebtheit und Nutzung von iPhones und iPads in Unternehmen, Behörden und Bildungseinrichtungen beigetragen. Diese umfangreichen Sicherheitsmaßnahmen haben Cyberkriminelle jedoch nicht davon abhalten können, auch iOS-Geräte zu hacken. So gab es verschiedene Fälle, in denen Hacker iPhones und iPads auf kreative Weise infiziert haben – darunter mit neuer Malware namens WireLurker und Masque Attack.

WireLurker ist eine neue Klasse an Malware, mit der sowohl Mac OS- als auch iOS-Geräte angegriffen werden.[10] Das Besondere an WireLurker ist, dass die Malware auch iOS-Geräte inifizieren kann, bei denen kein Jailbreak vorgenommen wurde – und zwar dann, wenn sie per USB-Kabel mit einem infizierten Mac OS-Gerät verbunden werden.

Dies ist die generelle Funktionsweise von WireLurker:

- Der Benutzer lädt eine mit Malware infizierte OS X-App auf sein Mac OS-Gerät herunter (meist aus einem inoffiziellen anderen App Store) und installiert sie.
- Anschließend führt der Benutzer die infizierte App aus und gewährt ihr Root-Berechtigungen. Hierfür wird das Administratorkennwort auf dem Mac OS-Gerät benötigt.
- Nach der Ausführung lädt die mit Malware infizierte OS X-App weitere iOS-Apps herunter und wartet darauf, dass ein iOS-Gerät, das dem Computer vertraut, per USB-Kabel angeschlossen wird.
- Nach dem Anschluss eines Geräts, das dem infizierten Mac OS-Gerät vertraut, lädt die Malware-App die bösartigen iOS-Apps auf das iPhone oder iPad herunter.
- Bei den iOS-Apps selbst handelt es sich um von Unternehmen signierte Apps, was bedeutet, dass die Cyberkriminellen entweder das Konto eines anderen Unternehmens manipuliert haben oder sich die eigenen iOS-Apps von Apple haben genehmigen lassen. Diese Apps verfügen zudem über Bereitstellungsprofile, sodass sie von iOS-Geräten als vertrauenswürdig eingestuft werden.

Sobald die schädlichen iOS-Apps auf die iOS-Geräte (auf denen kein Jailbreak vorgenommen wurde) der ahnungslosen Benutzer hochgeladen wurden, können sie Daten stehlen und regelmäßig mit den Servern der Angreifer kommunizieren.

Vielleicht noch gemeiner als WireLurker ist eine vor kurzem entdeckte Malware namens Masque Attack[11] , die ebengalls iOS-Geräte ohne Jailbreak angreifen kann, ohne jedoch eine Verbindung mit einem infizierten Mac OS-Gerät zu benötigen. Bei diesem Angriff kann eine per Enterprise-/Ad-hoc-Bereitstellung installierte iOS-App eine zugelassene App aus dem iTunes App Store ersetzen, solange beide Apps den gleichen Bundle Identifier aufweisen.

So kann Masque Attack authentische Apps von Benutzern ersetzen und Daten stehlen:

- Der Benutzer klickt über eine beliebige Website auf einen Link, um die schädliche App herunterzuladen und zu installieren. Sie ist mt einem Enterprise-Zertifikat signiert und kann einen Namen wie zum Beispiel „Neues Angry Bird“ tragen.
- Die bösartige App ersetzt eine legitime App (zum Beispiel eine Banking- oder E-Mail-App), die den gleichen Bundle Identifier aufweist.
- Angreifer können die Anmeldeoberfläche der ursprünglichen App imitieren, um so die Anmeldedaten des Benutzers zu stehlen.
- Außerdem kann die App lokale Daten-Caches nutzen, um die Funktionen der ersetzten App zu simulieren (zum Beispiel E-Mails bei einer E-Mail-App).

Sobald die Cyberkriminellen Zugriff auf die Anmeldedaten und lokal zwischengespeicherten Daten haben, sind vertrauliche Daten und Finanzinformationen des Benutzers dem Risiko von Angriffen und Datenverlusten ausgesetzt.

Malware-Schutz trifft auf Enterprise Mobility Management

IBM® MaaS360® Mobile Threat Management

IBM bietet mit der Integration von IBM Security Trusteer® ein neues Maß an Sicherheit für EMM und schützt vor mobiler Malware sowie manipulierten Geräten (zum Beispiel Smartphones oder Tablets mit Jailbreak bzw. Rooting).

Die spezielle Integration und Synergie bieten effektiven Schutz vor Hackern und Dieben, die versuchen, geschäftliche und private Daten für kriminelle Zwecke zu entwenden.

Erkennen und analysieren Sie iOS- und Android-Apps mit Malware-Signaturen aus einer regelmäßig aktualisierten Datenbank.

Trusteer, das von Hunderten von Millionen von Benutzern verwendet wird, um Unternehmen von Betrug und Datenverletzungen zu schützen, sorgt in MaaS360 für Risiko- und Sicherheitsinformationen.

Erkennung und Beseitigung mobiler Malware:

- Erkennen und analysieren Sie iOS- und Android-Apps mit Malware-Signaturen aus einer regelmäßig aktualisierten Datenbank.
- Fügen Sie für eine individuelle Anpassung der erlaubten App-Nutzung App-Ausnahmen hinzu.
- Richten Sie detaillierte Richtlinien für Gegenmaßnahmen ein.
- Nutzen Sie eine Engine mit Compliance-Regeln in nahezu Echtzeit zur automatisierten Problembehebung.
- Alarmieren Sie Benutzer und Verantwortliche bei Erkennung von Malware.
- Zeigen Sie betroffene Geräte in My Alert Center und Vorfällen in My Activity Feed Dashboards an.
- Sorgen Sie für eine automatische Deinstallation von Apps, die Malware enthalten (bei ausgewählten Android-Geräten wie Samsung SAFE).
- Sperren Sie den Zugang und nehmen Sie eine selektive oder komplette Gerätelöschung vor.
- Erfassen und zeigen Sie Attribute von Gerätebedrohungen an, wie z. B.:
  - Erkannte Malware
  - Verdächtige Systemkonfigurationen wie unbekannter SMS-Listener oder Startpaket
  - Verbindung mit unsicherem WLAN-Hotspot
  - Erlaubte Installation von nicht marktüblichen Apps
  - Betriebssystemversion
- Anzeige des Verlaufs mit Malware-Erkennungsereignissen

Abbildung 3: MaaS360 arbeitet mit Trusteer zusammen, um mobile Malware und kompromittierte Geräte zu erkennen, zu analysieren und abzuwehren bzw. zu korrigieren

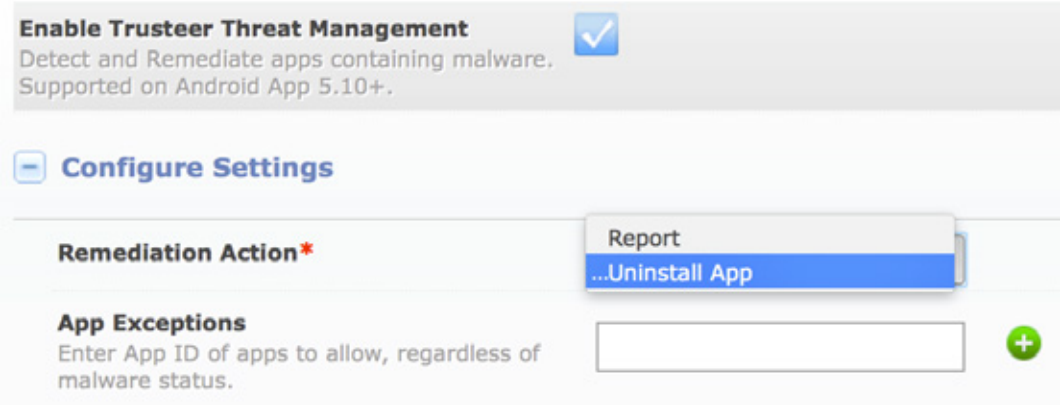

Abbildung 4: Einige der Einstellungen von MaaS360

Ergänzende Jailbreak- und Root-Erkennung:

- Erkennung angegriffener und gefährdeter mobiler Geräte
- Schutz vor iOS-Geräten mit Jailbreak und gerooteten Android-Geräten, die Angreifern erhöhte Zugriffsrechte auf das Betriebssystem verschaffen können (was verschiedene Angriffsvektoren möglich macht)
- Erkennung von versteckten Schadprogrammen und aktiven Versteckmethoden, mit denen eine Erkennung von Jailbreak- oder gerooteten Geräten zu verhindert werden soll
- Anwendung einer automatisch aktualisierten Erkennungslogik ohne App Schnellere Updates im Hinblick auf flinke Hacker
- Einrichtung von Sicherheitsrichtlinien und Compliance-Regeln zur automatisierten Problembehebung
- Sperrung von Zugang, selektives oder vollständiges Löschen von Geräten bzw.Entfernen der Gerätekontrolle

Geräte und Daten von Benutzern lassen sich auch mit dieser Sicherheitsebene schützen, die Konsumenten im Normalfall nicht zur Verfügung steht.

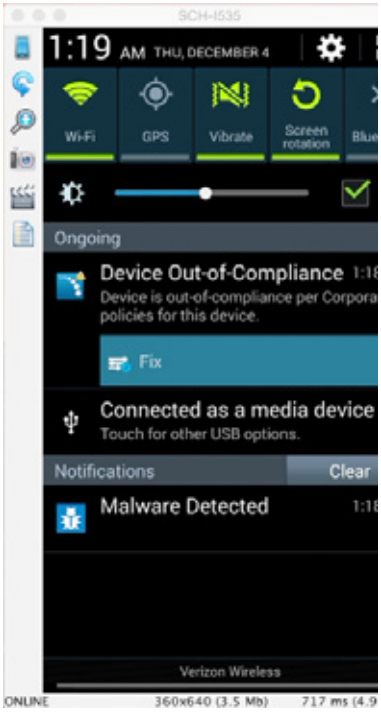

Abbildung 5: Screenshot, der erkannte mobile Malware und nicht konforme Geräte aufzeigt

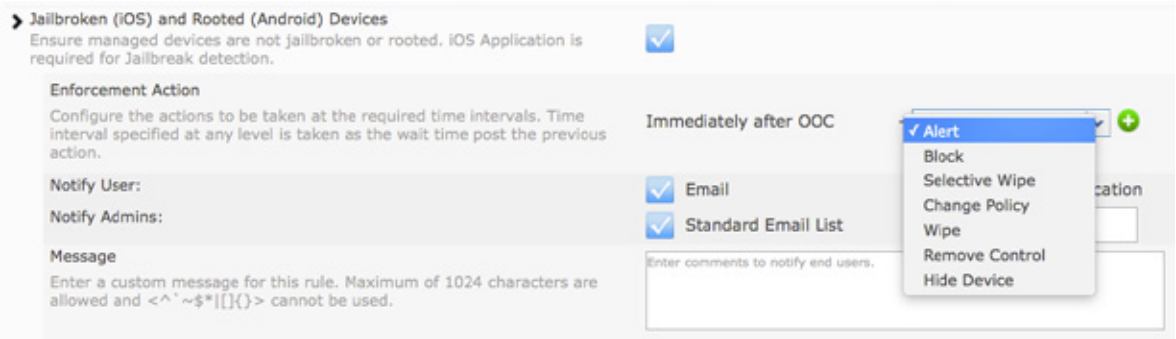

Abbildung 6: Konfiguration von Aktionen zur Compliance-Durchsetzung auf Jailbreak- oder gerooteten Geräten

Die Trusteer Mobile Risk Engine bietet Schutzschichten und Informationen über Cyberkriminalität für flexiblen Malware-Schutz, sodass sich das Verhalten neuer Angriffe schneller erkennen und abwehren lässt. So hat Malware kaum eine Gelegenheit, um Schaden anzurichten. Die Engine wird kontinuierlich aktualisiert, um neueste Malware, Jailbreaks und Roots erkennen zu können, und nimmt anhand von Geräten und Risikofaktoren von Apps eine nahezu echtzeitbasierte Bewertung der mobilen Risiken vor.

Die wichtigsten Vorteile

Der Nutzen der MaaS360 Mobile Threat Management Lösung geht weit über den Schutz geschäftlicher Geräte und Daten hinaus. Geräte und Daten von Benutzern lassen sich mit einer Sicherheitsebene schützen, die Konsumenten im Normalfall nicht zur Verfügung steht.

Unternehmen können mehr tun, um ihre Benutzer aufzuklären und Daten zu schützen.

- Sichere Unterstützung von privaten und unternehmenseigenen Geräten
- Schützen Sie private Daten als zusätzlichen Vorteil für Mitarbeiter bei BYOD
- Proaktive Behandlung mobiler Bedrohungen fast in Echtzeit
- Reduzierung des Risikos hinsichtlich der Offenlegung sensibler Daten und personenbezogener Informationen
- Höhere Attraktivität einer Android-Einführung in Unternehmen – besonders im Rahmen von BYOD
- Automatisierte Maßnahmen zur Reduzierung mobiler Sicherheitsrisiken

Auflöärung und Schutz von Benutzern

Zusätzlich zur MaaS360 Mobile Threat Management Lösung können Unternehmen ihre Benutzer besser aufklären und Daten effektiver schützen.

Unternehmen sollten überlegen, folgende Aktivitäten für mobile Sicherheit anzuwenden:

- Aufklärung von Mitarbeitern über Anwendungssicherheit: Klären Sie Mitarbeiter über die Gefahren eines Herunterladens von Anwendungen anderer Anbieter sowie die potenziellen Risiken auf, die durch eine Verwendung schwach geschützter Geräte entstehen.
- Schutz von BYOD-Geräten: Nutzen Sie Enterprise-Mobilty-Management-Funktionen, um Mitarbeitern die Verwendung ihrer eigenen Geräte zu ermöglichen und gleichzeitig für maximale Sicherheit zu sorgen.
- Gestatten Sie es Mitarbeitern, Apps ausschließlich aus autorisierten App Stores herunterzuladen: Erlauben Sie es Angestellten, Anwendungen ausschließlich aus genehmigten App Stores wie Google Play, dem Apple App Store oder ggf. dem App Store Ihres Unternehmens herunterzuladen.
- Reagieren Sie schnell, wenn ein Gerät kompromittiert wurde: Richten Sie automatische Richtlinien für Smartphones und Tablets ein, die automatische Aktionen auslösen, wenn ein Gerät kompromittiert wurde oder bösartige Apps entdeckt werden. Mit diesem Ansatz werden die Daten Ihres Unternehmens geschützt und das Problem behoben.

Warum MaaS360?

Für MaaS360 hat IBM erweiterten Schutz vor integrierter Malware mit branchenführenden Enterprise-Mobility-Management- und Sicherheitsfunktionen integriert. Die Lösung lässt sich schnell und einfach einrichten und bietet Sicherheit für Daten auf unternehmenseigenen und privaten mobilen Geräten.

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

1 World to have more cell phone accounts than people by 2014, Januar 2013 International Telecommunications Union, http://www.siliconindia.com/magazine_articles/World_to_have_more_cell_phone_accounts_than_people_by_2014-DASD767476836.html

2 State of Mobile App Security, November 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

3 Bring Your Own Device: The Facts and the Future, Mai 2013, Gartner, http://www.gartner.com/newsroom/id/2466615

4 Motive Security Labs Malware Report, H2 2014, Motive Security Labs, http://www.gartner.com/newsroom/id/2466615

5 2014 Cost of Data Breach Study: Global Analysis, Mai 2014, Ponemon Institute, http://www-03.ibm.com/security/data-breach/

6 State of Mobile App Security, November 2014, Arxan Technologies, https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

7 The State of Mobile Application Insecurity, Februar 2015, Ponemon Institute, https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=swg-WW_Security_Organic&S_PKG=ov33432&S_TACT=102PW2CW

8 IDC Worldwide Quarterly Mobile Phone Tracker, Februar 2015, IDC, http://www.idc.com/getdoc.jsp?containerId=prUS25450615

9 DroppedIn: Remotely Exploitable Vulnerability in the Dropbox SDK for Android, März 2015, IBM Security, http://securityintelligence.com/droppedin-remotely-exploitable-vulnerability-in-the-dropbox-sdk-for-android/#.Vb-1_SisG8W

10 Wirelurker: A new Era in OS X and iOS Malware; Blog, PaloAlto Networks, 5. November 2014, http://researchcenter.paloaltonetworks.com/2014/11/wirelurker-new-era-os-x-ios-malware/

11 Xue, H., Wie, T., Yulong, Z.; Masque: All Your iOS Apps Belong to Us; Fire Eye; 10. November 2014, https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html