Kurzvorstellung

Schutz vor SSL-Schwachstellen in Mobilgeräte-Apps

Heutzutage, wo es für alles eine App gibt und neue, innovative Ideen noch aufregendere Apps versprechen, verschwenden die Benutzer kaum noch Gedanken daran, wie angreifbar ihre vertraulichen Daten durch MITM-Angriffe („Man-In-The-Middle“) sind. So tragen sie selbst mit dazu bei, dass ihre vermeintlich sicheren Apps kompromittiert werden können. Auch die Entwickler der Apps nehmen den Datenschutz und die Sicherheit ihrer Kunden auf die leichte Schulter. Aber gerade die App-Entwickler sind dafür verantwortlich, dass die privaten Daten der Benutzer vor der steigenden Anzahl kryptographischer Schwachstellen (z. B. BERserk oder Heartbleed) geschützt werden.

Im September 2014 veröffentlichte das erste Computer Emergency Response Team (CERT) der Carnegie Mellon University eine Liste von Mobilgeräte-Apps, die für MITM-Angriffe verwundbar sind, da sie SSL-Zertifikate nicht ordnungsgemäß validieren und somit Benutzernamen sowie Kennwörter für potenzielle Angreifer einsehbar machen.[1] Im Januar 2015 – fünf Monate später – stellte McAfee® Labs fest, dass dieses Problem bei 18 der 25 am häufigsten heruntergeladenen Apps aus dieser Liste noch nicht behoben wurde. Diese Apps sind immer noch über eine der häufigsten SSL-Schwachstellen angreifbar: die fehlerhafte Validierung digitaler Zertifikate.

Da die App-Entwickler dem wachsenden Bedarf an Datenschutz und Sicherheit nur unzureichend folgen, liegt es bei den Benutzern und Unternehmen, alle erdenklichen Sicherheitsmaßnahmen zur Absicherung ihrer Apps zu treffen.

Schutz vor Schwachstellen in Mobilgeräte-Apps

Mit diesen empfehlenswerten Maßnahmen können Sie Angriffen über Schwachstellen in Apps vorbeugen:

- Sie sollten nur solche Apps herunterladen und installieren, die allgemein verbreitet sind, über eine hohe Bewertung verfügen und aus vertrauenswürdigen Quellen stammen.
- Richten Sie Anmeldekonten nur dann ein, wenn Sie so deutlich mehr Leistungen als ein normaler Gastbenutzer erhalten. Verwenden Sie für jedes Konto ein anderes Kennwort.

intel Security

- Testen Sie regelmäßig Mobilgeräte-Apps, die in der Unternehmensumgebung eingesetzt werden, damit keine sensiblen Informationen aufgrund von Schwachstellen kompromittiert werden können.
- Vor dem Download einer App sollten Sie deren Datenschutzrichtlinie sorgfältig durchlesen und besonders darauf achten, auf welche Daten die App zugreifen kann (z. B. auf Informationen über Ihren aktuellen Standort oder auf Anmeldeinformationen für Ihre sozialen Netzwerke) und wie diese Daten dann weiter verwendet werden.

So kann Intel Security vor Schwachstellen in Mobilgeräte-Apps schützen

McAfee VirusScan® Mobile

McAfee VirusScan Mobile ist ein System zum Schutz vor Malware. Es scannt sowie bereinigt mobile Daten und verhindert so eine Beschädigung der Daten durch Viren, Trojaner sowie anderen böswilligen Code. McAfee VirusScan Mobile schützt Ihre mobilen Geräte an den kritischsten Stellen: ein- und ausgehende E-Mails, Textnachrichten, E-Mail-Anhänge und Internet-Downloads.

- **Bedrohungserkennung in Echtzeit:** Blockieren Sie Malware in E-Mails, Textnachrichten und Anhängen ohne merkbare Verzögerung. McAfee VirusScan Mobile scannt Geräte innerhalb von weniger als 200 Millisekunden auf zahlreiche Bedrohungen und bietet automatischen und umfassenden Schutz für Smartphones.
- **Datenschutz in Anwendungen:** Sie müssen wissen, auf welche personenbezogenen Informationen Ihre installierten Anwendungen zugreifen können. Nur dann können Sie auch sicher sein, dass Ihre Daten geschützt sind und nicht unnötig offen gelegt werden.
- **Verringerung der Risiken durch SSL-Schwachstellen:** McAfee VirusScan Mobile stellt Warnbenachrichtigungen bereit, wenn Anwendungen vertrauliche Informationen über verwundbare Verbindungen senden, und stuft Anwendungen mit Schwachstellen als potenziell unerwünschte Programme (PUP) ein.

McAfee Complete Endpoint Protection-Suites

Die **McAfee Complete Endpoint Protection-Suites** integrieren sich nahtlos in die preisgekrönte Verwaltungslösung **McAfee® ePolicy Orchestrator® (McAfee ePO™)**. Mit McAfee Complete Endpoint Protection und McAfee ePO können Unternehmen ihre mobilen Benutzer verwalten und deren Mobilgeräte vor Malware, Datenkompromittierung und anderen Bedrohungen schützen.

- **Zentral verwaltete Virenschutz- und App-Reputations-Scans:** In weniger als 200 Millisekunden wird festgestellt, wie vertrauenswürdig eine Anwendung ist und ob sie gefährliche Bedrohungen enthält. So sind Smartphones automatisch und umfassend geschützt.
- **Zentrale Übersicht:** Verwalten und schützen Sie Smartphones mit Google Android, Apple iOS und Microsoft Windows sowie herkömmliche Endgeräte mithilfe von McAfee ePO, und nutzen Sie dessen automatisierte Funktionen zur Durchsetzung von Richtlinien auf jedem beliebigen Smartphone oder Endgerät.
- **Richtlinienerzwingung:** Blockieren Sie den Zugriff auf Firmen-E-Mails, wenn auf Benutzergeräten Apps Malware oder potenziell unerwünschte Programme gefunden werden. Zusätzlich können Sie McAfee ePO auch weitere Aktionen automatisch durchführen lassen (z. B. Daten löschen oder an eine andere Stelle in der Systemstruktur verschieben, in der Zugriffe auf das Unternehmens-VPN verweigert werden).

Intel Security True Key

True Key von Intel Security bietet einen einfachen und sicheren Weg, sich bei Mobilgeräte-Apps anzumelden. Das Tool identifiziert den Benutzer über mehrere individuelle Faktoren und meldet ihn dann umgehend bei Apps, Webseiten und Geräten an. Dadurch muss der Benutzer nicht mehr unzählige Kennwörter selbst verwalten.

- **Entsperrung über biometrische Faktoren:** Die Anmeldung erfolgt über Faktoren, die für jeden Benutzer individuell sind. Das können biometrische Daten sein (z. B. der Abstand zwischen Augen und Nase) oder die Geräte, die die Benutzer besitzen.
- **Einfachere Erstellung und Verwaltung einmaliger Kennwörter:** True Key merkt sich die Kennwörter der Benutzer und meldet sie unverzüglich in Webseiten und Apps an. Dadurch muss sich niemand mehr all seine Kennwörter merken.
- **Mehrfachfaktor-Identifizierung:** Benutzer können ihre Profile mit verschiedenen Faktoren ergänzen, deren Kombination eindeutig auf den Benutzer verweist. Je mehr Faktoren angegeben werden, desto sicherer ist der Schutz.

Schützen Sie Ihre mobilen Mitarbeiter vor schlecht implementierten Anwendungen, damit vertrauliche Informationen Ihres Unternehmens nicht unnötig offen gelegt werden. Mit der Technologie von Intel Security kann sich Ihr Unternehmen präventiv vor Schwachstellen schützen, die das traditionelle Vertrauensmodell unterlaufen.

1. **http://www.kb.cert.org/vuls/id/582497**

Intel und das Intel-Logo sind eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern. McAfee, das McAfee-Logo, ePolicy Orchestrator, McAfee ePO und VirusScan sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2015 McAfee, Inc. 61737brf_mobile-users-exposed_0215

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com