Global-2000-Bank sichert 9.000 Android-Smartphones zur Erfüllung interner Compliance-Anforderungen

Die Anforderung

Für die Einführung ihrer COPE-Mobilitätsrichtlinie (Corporate Owned, Personally Enabled) benötigte die führende Bank eine mobile Sicherheitslösung, die ihren internen Datenschutzrichtlinien entsprach, eine Vernetzung mit VMware AirWatch ermöglichte und dem Unternehmen Transparenz über die mobilen Bedrohungen verschaffte, mit denen ihre internationale Belegschaft in Kontakt kam.

Das IT-Team beschloss, eine COPE-Mobilitätsrichtlinie einzuführen, um durch die somit begrenzte Anzahl von Gerätemodellen und Android-Versionen den Supportaufwand zu reduzieren. Darüber hinaus entwickelte die Bank eine eigene Unternehmensanwendung, die es den Beschäftigten ermöglicht, Bankdienstleistungen für ihre Kunden über mobile Endgeräte zu erbringen. Da das IT-Mobilitätsteam keinen Einblick in die Bedrohungen oder den Datenverlust auf den mobilen Geräten hatte wusste es, dass ihre ungeschützten Endgeräte Angriffsflächen boten, die ein ernsthaftes Sicherheitsrisiko darstellten.

Kundenprofil

Der Finanzdienstleister mit Firmensitz im Nahen Osten verfügt über ein internationales Netzwerk von weltweit 1.400 Filialen und ist im Forbes-Global-2000-Ranking vertreten.

Branche: Finanzdienstleistungen

Mobilitätsstrategie: COPE

EMM-Lösung: VMware AirWatch

Die Lösung

- Lookout Mobile Endpoint Security

Das Ergebnis

- Einhaltung der internen Richtlinien für den Schutz von Endgeräten
- Transparenz über Bedrohungen mit hohem Risiko
- Gesteigerte Produktivität der Beschäftigten, ohne die Anzahl der Support-Tickets zu erhöhen

> „Lookout bietet eine Lösung, die Daten zu Bedrohungen aus aller Welt sammelt und uns Transparenz über sämtliche Risiken für unsere mobilen Daten gibt."
>
> Manager, IT-Infrastruktur-Abteilung

Als Finanzdienstleistungsunternehmen gehört die Bank einer regulierten Branche an. Nationale Compliance- und Datenschutzregeln für mobile Geräte sind aber noch neu und im Heimatland der Bank nicht klar definiert. Dennoch unterscheidet das IT-Mobility-Team nicht zwischen mobilen Geräten und Laptops - aus seiner Sicht handelt es sich in beiden Fällen um ein Endgerät, von dem aus auf Unternehmensressourcen zugegriffen werden kann. Um die internen Richtlinien zum Schutz aller Endgeräte einhalten zu können, suchte die Bank daher nach einer Lösung für die Sicherheit ihrer mobilen Plattformen. Diese sollte AirWatch ergänzen, die bankeigenen Verschlüsselungsrichtlinien einhalten und das Sicherheitsbewusstsein der Beschäftigten erhöhen.

Die Lösung

Um die Herausforderungen für die Sicherheit der mobilen Plattformen der Bank zu bewältigen, evaluierte das IT-Team eine Reihe von Lösungen. Dabei kamen die Mitarbeiter zu dem Ergebnis, dass traditionelle Anbieter von Endgerätesicherheit entweder gar keine Unterstützung für Android anboten oder aber signaturbasierte Schutzmechanismen verwendeten, die nicht mit den sich rasant entwickelnden Bedrohungen für mobile Plattformen mithalten können.

Das IT-Team entschied sich schließlich für Lookout, da es einzigartige Informationen zu mobilen Bedrohungen bereitstellt und dafür Daten auf der ganzen Welt sammelt. Das Team kam zu dem Schluss, dass Lookout Mobile Endpoint Security die richtige Lösung war, um ihrer mobilen Belegschaft die Möglichkeit zu bieten, frei auf Produktivitäts-Apps zuzugreifen. Zudem war es mit Lookout nicht mehr notwendig, Anwendungen manuell in „Blacklists" bzw. „Whitelists" einzutragen, um sie zu sperren oder freizuschalten. Das Team arbeitete dann gemeinsam mit Lookout daran, Lookout Mobile Endpoint Security auf rund 9.000 Samsung Galaxy Smartphones bereitzustellen und zu aktivieren. Die „Lookout for Work-App" konnte dabei mühelos via AirWatch direkt auf die Geräte der Belegschaft übertragen werden – ohne dass die Mitarbeiter selbst etwas tun mussten.

Das Ergebnis

Die Bank ist sehr zufrieden damit, wie schnell Lookout bereitgestellt werden konnte: Am Ende des Prozesses wurde die Lookout for Work-App auf 2.000 Geräte pro Tag übertragen.

Im Rahmen der Bereitstellung identifizierte Lookout Mobile Endpoint Security eine große Anzahl von Hochrisiko-Apps sowie Auto-Rooting Malware und Man-in-the-Middle-Angriffe auf die Mobilgeräte der Belegschaft. Das Erkennen dieser erheblichen Bedrohungen bestätigte die Bank in ihrer Entscheidung, der Einhaltung ihrer internen Richtlinien für den Schutz von Endgeräten eine hohe Priorität beizumessen.

Das Fazit

Zur Zufriedenheit der Bank hat sich seit der Bereitstellung von Lookout die Anzahl der Support-Tickets nicht erhöht: die Beschäftigten beseitigen mobile Bedrohungen einfach selbst, sobald sie eine Benachrichtigung der „Lookout for Work-App" auf ihrem Gerät vorfinden.

Nun, da das IT-Team der Bank seine Ziele bezüglich Compliance und Transparenz über mobile Bedrohungen und riskante Apps auf den Mobilgeräten der Belegschaft erreicht hat, konzentriert es sich bereits auf die nächsten Schritte: So möchten die Mitarbeiter etwa die Vernetzung zwischen Lookout und AirWatch nutzen, um für von Lookout erkannte Bedrohungen automatische Beseitigungsmaßnahmen in AirWatch einzuleiten. Damit soll der Zeitraum zwischen Erkennung und Beseitigung noch weiter verkürzt werden.

Die Zahlen: Erkannte Bedrohungen

Trojaner

16 Trojaner erkannt 5 Shedun-Alarme	Shedun ist eine Art von Android-Malware, die im Jahr 2015 erstmals von Lookout erkannt wurde. Shedun gibt vor, eine legitime Anwendung zu sein. Sie ist in Wahrheit aber bösartig und versucht Dritten mittels Rooting zu ermöglichen, zusätzliche Anwendungen zu installieren. Dadurch kann auch weitere Malware auf dem Gerät installiert werden.

Infizierte Geräte

37 „Root Enablers" erkannt	Mit dem „Rooting" eines Geräts erlangen potenzielle Angreifer Zugriff auf erweiterte Administratorrechte und können systemeigene Sicherheitsfeatures wie etwa App-Sandboxing beeinträchtigen.

Netzwerkangriffe

91 Man-in-the-Middle-Angriffe	Angreifer können eine Reihe von Methoden anwenden, um den Netzwerkverkehr zu und von Mobilgeräten abzufangen. Befindet sich ein Angreifer in unmittelbarer Nähe eines Zielgeräts, kann er für Zugriffszwecke ein falsches WLAN- oder Mobilfunknetz vortäuschen. Ein standortferner Angreifer kann Malware oder Social Engineering einsetzen, um User dazu zu bewegen, ein Gerät so zu konfigurieren, dass der gesamte Netzwerkverkehr über eine bösartige Proxy- oder VPN-Verbindung geroutet wird.

App-basierte Bedrohungen

172 Riskware-Programme erkannt 61 Adware-Programme erkannt 3 Chargeware-Programme erkannt	Bei Riskware-Programmen handelt es sich um Code, Libraries oder Netzwerkdienste, die aufgrund von bekannten Schwachstellen oder dem schlechten Ruf der von der App verwendeten Dienstleister ein Geräterisiko darstellen. Chargeware führt zu unerwünschten Gebühren. Adware aktiviert störende Werbung oder übermittelt übermäßig viele personenbezogenen Daten an Anzeigennetzwerke, und zwar in einem Ausmaß, das gängige Werbepraktiken weit überschreitet.