Investmentbank Greenhill & Co. sorgt für sicheres BYOD und schützt hochsensible Kundendaten beim Zugriff über Mobilgeräte

Die Herausforderung

Dan Dougherty, leitender IT-Manager bei Greenhill & Co., war schon früh von Mobile Security überzeugt als er Anfang 2016 in einem Pilotprojekt für das Deployment einer weniger ausgereiften Mobile-Threat-Defense-Lösung verantwortlich war. Allerdings kam es nie zu einem vollständigen Deployment. Ein Grund dafür war die hohe Anzahl falsch-positiver Warnungen bzgl. netzwerkbasierter Angriffe. Darüber hinaus nutzte das Produkt für sämtlichen Datenverkehr von den Enduser-Geräten zu den Servern des Anbieters die „Blackholing"-Methode. Dies war problematisch – sowohl hinsichtlich des Enduser-Datenschutzes als auch in Bezug auf die hochsensiblen Kundendaten.

Dougherty und sein global aufgestelltes Team mussten also eine andere Lösung finden, um Greenhill's Firmen- und Kundendaten abzusichern, wenn diese von Mitarbeitern über deren Privatgeräte abgerufen werden. Außerdem galt es, Datenlecks erzeugende Schadsoftware wie etwa Keylogger aufzuspüren und die Sarbanes-Oxley-Vorschriften zum Schutz sensibler Daten einzuhalten.

Greenhill

Kundenprofil

Greenhill ist eine unabhängige Investmentbank mit Hauptsitz in New York und zählt zu den hochrangigsten und renommiertesten Wall-Street-Firmen. Sie unterhält weltweit 14 Niederlassungen und berät führende Konzerne, Konsortien, Institutionen und Behörden bei Fusionen, Übernahmen und Umstrukturierungen sowie zu Finanzierung und Kapitalbeschaffung.

Branche: Finanzwesen

Mobilitätsrichtlinie: BYOD

EMM-Lösung: Citrix XenMobile

Sicherheitsspezifische Herausforderungen

- Schutz von Finanzdaten der Kunden inkl. sensibler Informationen zu bedeutenden Fusionen und Übernahmen
- Hohe Transparenz über Netzwerkangriffe und Datenlecks durch Malware (z. B. Keylogger)
- Einhaltung der Sarbanes-Oxley-Vorschriften zum Schutz sensibler Daten

Die Lösung

Anfang 2017 entschied sich Greenhill dafür, das Pilotprodukt zur Absicherung seiner BYOD-Geräte durch Lookout Mobile Endpoint Security zu ersetzen. Den Kunden überzeugte vor allem die Lookout Administrator-Konsole, die bei mobilen Risiken handlungsorientierte Warnungen ausgibt und bei der Priorisierung der dringendsten Ereignisse hilft.

Mobile Malware wird immer zahlreicher und raffinierter. Das ist auch Greenhill bewusst. Das Unternehmen fürchtet besonders Keylogger – angesichts der Menge an Kundendaten, die per E-Mail ausgetauscht werden, kein Wunder, denn die 82 Geschäftsführer nutzen hierfür oft ihre Privathandys. Dougherty vertritt hierzu folgende Meinung: „Ohne Lookout wüssten wir nie, ob ein Mitarbeitergerät von Schadsoftware oder einer Daten ausschleusenden App bedroht ist. Ein Keylogger beispielsweise könnte Informationen aus Notizen oder Kontakten abziehen, die mit dem Telefon synchronisiert werden."

> „Als globale Berater bei Fusionen und Übernahmen in Milliardenhöhe sind wir uns bewusst, dass wir attackiert werden und Datenverluste erhebliche Folgen hätten. Deshalb nutzen wir Lookout: Es schützt sensible Daten, auf die unsere Mitarbeiter per Mobilgerät zugreifen, und warnt unsere Administratoren mit handlungsorientierten Hinweisen."

Dan Dougherty, Senior IT Manager, Greenhill & Co.

Des Weiteren überzeugte Dougherty der Umgang mit Netzwerkbedrohungen, da Lookout diese direkt bei der Verbindungsaufnahme entdeckt und Anwender davor warnt, sensible Daten zu übertragen.

Das Team von Greenhill prüft nun, wie sie von der exklusiven engen Integration von Lookout und Microsoft Enterprise Mobility + Security profitieren können. Ziel ist es, mittels Microsoft Intune und Office 365 Richtlinien für den bedingten Zugriff umzusetzen. Hiermit soll der Zugang zu Unternehmensdaten eingeschränkt werden, bis Lookout bestätigt, dass das jeweilige Gerät von keiner mobilen Bedrohung betroffen ist.

Das Ergebnis

Greenhill-Mitarbeitern wurde die Lookout-App über die MDM-Lösung Citrix XenMobile bereitgestellt. Außerdem wurden sie in Sicherheitsschulungen für das Thema Cyberbedrohungen sensibilisiert. Das Greenhill-Team rechnet daher mit einem Rückgang des durch User verursachten Risikos, zum Beispiel durch „sideloaded" Apps oder Jailbreaking, und dafür mit gezielteren Bedrohungen wie etwa Malware.

Zwar sind sicherheitsbewusste Anwender von Vorteil, doch Dougherty weiß, dass dies kein Allheilmittel ist: Greenhill-Mitarbeiter reisen oft geschäftlich in Länder, in denen das Risiko für Angriffe erheblich ist und die Angriffe besonders raffiniert sind. Diese potenziellen Bedrohungen sieht er jedoch pragmatisch: „Als globale Berater bei Fusionen und Übernahmen in Milliardenhöhe sind wir uns bewusst, dass wir attackiert werden und Datenverluste erhebliche Folgen hätten. Deshalb nutzen wir Lookout: Es schützt sensible Daten, auf die unsere Mitarbeiter per Mobilgerät zugreifen, und warnt unsere Administratoren mit handlungsorientierten Hinweisen."