Lookout stoppt Phishing-Angriffe im Rechtswesen

Lookout Phishing- und Content-Protection schützt Anwälte vor mobilen Bedrohungen

Branchenspezifische Sicherheitsherausforderungen

Ohne Mobilgeräte könnten Kanzleien kaum effektiv arbeiten, da ihre Mandanten in kritischen Momenten auf Reaktionen warten müssten. Dementsprechend viele private und vertrauliche Informationen werden außerhalb der Kanzleiräumlichkeiten eingesehen – und damit außerhalb der Reichweite herkömmlicher Sicherheitsmechanismen. Um jederzeit und von überall aus arbeiten zu können, nutzen viele Anwälte ihre Mobilgeräte für Privates wie Berufliches, und so entstehen Konflikte rund um die Sicherheit und den Datenschutz. Zudem stellt eine gemischte Flotte aus Privat- und Firmengeräten Kanzleien vor große Herausforderungen, insbesondere seit immer mehr Mandantendaten in cloudbasierten Diensten gespeichert werden.

Anwendungsfall aus der Praxis – für Kanzleien

Anwälte sind ein begehrtes Ziel von Phishing-Angriffen auf Mobilgeräten, da oft nur mit überholten Sicherheitsmodellen gearbeitet wird. Tatsächlich berichteten 80 % der befragten Kanzleien 2018 Empfänger einer Phishing-Nachricht gewesen zu sein. Die Angreifer haben es auf Anmeldedaten zu Unternehmensressourcen in der Cloud abgesehen, um sensible Mandantendaten abzugreifen. Die IT- und Sicherheitsteams müssen daher mit den richtigen Sicherheitstools Phishing-Links auf Mobilgeräten erkennen können – egal, ob diese per privater oder dienstlicher E-Mail, Messaging-Dienst oder Social-Media-Beiträgen auf die Geräte gelangen.

Branchenspezifische Herausforderungen

1. Deutlicher Anstieg der Mobilgerätenutzung bei allen Kanzleimitarbeitern
2. Schutz sensibler personenbezogener Daten und Falldaten
3. Eine bunte Mischung aus dienstlichen und privat genutzten Apps erhöht das Risiko von Phishing auf Mobilgeräten über Messaging-Dienste und Social-Media-Plattformen.

Unternehmenskritische Lookout-Funktion

Der Phishing- und Content-Schutz von Lookout prüft alle URL-Anfragen aus Firmen- und Privat-E-Mails, SMS, Messaging-Apps und Apps mit URLs zum Download schädlicher Plug-ins. Die Lösung blockiert automatisch URL-Anfragen, die von Lookout als bösartig markiert wurden. Bei Aktivierung dieser Funktion würde Lookout beispielsweise verhindern, dass ein Mitarbeiter seine Anmeldedaten in eine täuschend echte Kopie der Office 365-Anmeldeseite eingibt, auf die er durch Phishing gelangt ist. Damit zudem die Privatsphäre des Nutzers gewahrt bleibt, erhält die MES-Konsole (Mobile Endpoint Security) lediglich eine Meldung über das Vorhandensein des jeweiligen Problems und die Anzahl der Erkennungen. Der Administrator sieht weder den Browserverlauf noch den Datenverkehr des Geräts.

Warum Lookout?

Lookout Mobile Endpoint Security mit Continuous Conditional Access stellt die Sicherheit und Compliance auf jedem Gerät sicher und nutzt dazu einen großen Datensatz, der aus mehr als 170 Millionen Geräten und der Analyse von über 70 Millionen mobilen Anwendungen gespeist wird. Die Lookout Security Cloud vereinfacht die Bereitstellung von Lookout und die Anwendung von Sicherheitsrichtlinien für verwaltete sowie nicht verwaltete Geräte im gesamten Unternehmen. In Echtzeit erhalten Anwender Warnungen und Schritt-für-Schritt-Anleitungen, um beispielsweise bösartige Apps zu deinstallieren, kompromittierte Netzwerke zu verlassen oder Systemanomalien zu beheben. Hinzu kommt die dynamische Analyse des Gerätezustands, sodass ein bedingter Zugang zu Unternehmensanwendungen und -daten gewährleistet ist.

[1]National Cyber Security Centre (Großbritannien): https://www.ncsc.gov.uk/report/-the-cyber-threat-to-uk-legal-sector--2018-report