Lookout für Finanzdienstleistungen in der EU

Europäische Finanzinstitute müssen mobile Arbeitnehmer schützen, da immer Daten in der Cloud abgelegt werden

Branchenspezifische Sicherheitsherausforderungen

Europäische Finanzdienstleister setzen immer häufiger Clouddienste ein und arbeiten mittlerweile auch verstärkt mit sensitiven Daten in Microsoft Office 365. Durch diesen Service können Mitarbeiter jederzeit über ihre eigenen Geräte auf Unternehmensressourcen zugreifen. Obwohl diese Flexibilität Kosten- und Effizienzvorteile birgt, werden Unternehmen dadurch auch attraktiver für mobile Bedrohungen wie Phishing, schadhafte Apps und Schwachstellen im jeweiligen Betriebssystem. Zukunftsorientierte Unternehmen sehen zahlreiche Vorteile im sicheren mobilen Arbeiten und integrieren Lookout in Microsoft Office 365, um ihre sensiblen Daten vor Cyber-Bedrohungen zu schützen.

Branchenspezifische Herausforderungen

1. Deutlicher Anstieg der Mobilgerätenutzung
2. Strenge Datenschutzvorschriften
3. Hauptziel von Cyberangriffen

Anwendungsfall aus der Praxis – Finanzwesen

Die NIS-Richtlinie der Europäischen Kommission, der erste EU-weite Rechtsakt zur Cybersicherheit, musste bis November 2018 in das nationale Recht aller EU-Mitgliedstaaten umgesetzt sein. Von dieser Richtlinie verspricht man sich ein hohes Maß an Netzwerk- und Informationssicherheit. Mit der Einführung von Cybersicherheitsstandards können Finanzdienstleister in der EU Transaktionen durchführen, ohne um die Sicherheit sensibler Daten besorgt sein zu müssen. Da finanzielle Transaktionen auch zunehmend über Mobilgeräte getätigt werden, haben europäische Geldinstitute nun die Aufgabe, Daten vor raffinierten Cyberbedrohungen zu schützen und dabei die strengen Vorgaben der Datenschutz-Grundverordnung einzuhalten. Insbesondere Phishing auf Mobilgeräten muss zuverlässig abgewehrt werden, da die diesbezüglichen Methoden oft zum Ziel führen – und immer häufiger Mobilgeräte ins Visier nehmen.

Unternehmenswichtige Lookout-Funktion

Der Phishing- und Content-Schutz von Lookout inspiziert sämtliche URL-Anfragen, die über E-Mails (berufliche wie private), SMS und Messaging-Apps eingehen oder in App-Browser eingebettet sind. Erkennt Lookout eine präparierte Website, wird die Anfrage dynamisch blockiert. 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 stellt die kontinuierliche Sicherheit und Compliance auf jedem Mobilgerät 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. Gewarnt wird vor bösartigen Apps und Netzwerkverbindungen sowie Systemanomalien auf Betriebssystemebene. Die Warnungen erfolgen in Echtzeit und enthalten einfache Beseitigungsmaßnahmen zur direkten Anwendung auf dem Gerät. Europäischen Finanzinstituten bietet Lookout sowohl die Sicherheit als auch die Sichtbarkeit, die für umfassende Compliance und Transparenz über jeden Aspekt der Bedrohungen für Mobilgeräte erforderlich sind, ohne die Privatsphäre der Gerätenutzer einzuschränken.