Lookout®

DIE BANDBREITE MOBILER RISIKEN

Ein Überblick über die gesamte Bandbreite mobiler Risiken für Unternehmensdaten

Lookout hat eine Matrix für mobile Risiken entwickelt, die Unternehmen einen Überblick über die Komponenten und Vektoren der gesamten Bandbreite mobiler Risiken vermittelt. Durch die Bereitstellung entsprechender Daten hilft Lookout ihnen außerdem, die Häufigkeit und Auswirkungen mobiler Bedrohungen und Schwachstellen besser zu verstehen.

MATRIX FÜR MOBILE RISIKEN

Risikokomponenten

Vektoren

	WEB & CONTENT	APPS	GERÄT	NETZWERK
BEDROHUNGEN	• Phishing • Drive-by-Download • Bösartige Websites und Dateien	• Spyware und Surveillanceware • Trojaner • Sonstige bösartige Apps	• Privilegienerweiterung • Remote-Jailbreaking/ Rooting	• Man-in-the-Middle-Angriffe • Gefälschte Mobilfunkmasten • Root-CA-Installation
SOFTWARE-SCHWACHSTELLEN	• Kompromittierte Inhalte, die Betriebssystem- oder App-Schwachstellen auslösen	• Veraltete Apps • SDKs, die Schwachstellen enthalten • Mangelhafte Praktiken zum Verfassen von Code	• Veraltete Betriebssysteme • Dead-End-Hardware • Anfällige vorinstallierte Apps	• Netzwerkhard-wareschwachstellen • Schwachstellen im Protokollstapel
VERHALTEN UND KONFIGURATIONEN	• Öffnen von Anhängen und Besuchen von Links zu potenziell unsicheren Inhalten	• Apps, die Daten ungewollt abfließen lassen • Apps, die die Sicherheit des Unternehmens verletzen • Apps, die gegen gesetzliche Vorschriften verstoßen	• Durch User initiiertes Jailbreaking/Rooting • Keine PIN/Kein Kennwort • USB-Debugging	• Proxies, VPNs, Root-CAs • Automatisches Verbinden unverschlüsselter Netze

HÄUFIGKEIT MOBILER RISIKEN

203 VON 1000 AUF UNTERNEHMENSEIGENEN GERÄTEN SIND URL-BASIERTE BEDROHUNGEN AUFGETRETEN

203 von 1000 unternehmenseigenen Geräten (Android und iOS) waren von URL-basierten Bedrohungen betroffen (Q1-Q3 2021).

17 % DER APPS AUF UNTERNEHMENSEIGENEN GERÄTEN GREIFEN AUF DIE KONTAKTE DES GERÄTS ZU

Auf Unternehmensgeräten, die durch Lookout Mobile Endpoint Security geschützt sind, greifen 25 % der Apps auf die Kamera, 38 % auf GPS, 2 % auf Kalender und 5 % auf das Mikrofon zu. 4 % aller Unternehms-Apps sind mit Facebook und 2 % mit Twitter verbunden.

16 VON 1000 UNTERNEHMENSEIGENE ANDROID-GERÄTE WAREN APP-BASIERTEN BEDROHUNGEN AUSGESETZT

In zwei aufeinanderfolgenden Quartalen (Q1-Q3 2021) waren 16 von 1000 unternehmenseigenen Android-Geräten appbasierten Bedrohungen ausgesetzt.

58 % VON iOS-USER HABEN IHRE BETRIEBSSYSTEME LEDIGLICH BIS ZUR VERSION 15.0 AKTUALISIERT

Von der Veröffentlichung der Version 15.0 am 20. September 2021 bis zum 17. November 2021 hatten nur 42 % aller User ihre Geräte auf die neueste iOS-Version aktualisiert.

2 VON 1000 UNTERNEHMENSGERÄTE WAREN NETZBASIERTEN BEDROHUNGEN AUSGESETZT

2 von 1000 unternehmenseigenen Mobilgeräten waren im vergangenen Jahr netzwerkbasierten Bedrohungen ausgesetzt.

ÜBER DIE DATEN:

Die analysierten Daten stammen aus einer großen globalen Teilmenge an privat und in Unternehmen genutzten Geräten, die von Lookout gesichert werden. Die Daten wurden zwischen dem 1. Januar 2021 und 31. Oktober 2021 von Android- und iOS-basierten Geräten erhoben, die bei Finanzdienstleistern, Healthcare-Organisationen, Behörden sowie in anderen Branchen im Einsatz sind. Die Daten zum privaten Einsatz beziehen sich auf mehr als 185 Millionen Android- und iOS-Geräte weltweit. Die Datenerfassung erfolgte anonym. Unternehmensdaten oder Daten aus Netzwerken oder Systemen wurden nicht erfasst.

ÜBER LOOKOUT:

Lookout ist ein Anbieter für integrierte Sicherheit von Endgerät zu Cloud. In einer Welt, in der Datenschutz höchste Priorität hat und Mobilität und Cloud bei der Arbeit und in der Freizeit unverzichtbar geworden sind, haben wir es uns zur Aufgabe gemacht, Sie sicher in die digitale Zukunft zu führen. Wir geben Verbrauchern und Mitarbeitern die Möglichkeit, ihre Daten zu schützen und sicher miteinander in Verbindung zu bleiben, ohne ihre Privatsphäre oder ihr Vertrauen zu verletzen. Millionen von Verbrauchern, weltweit führende Unternehmen und Behörden sowie Partner wie AT&T, Verizon, VMware, Vodafone, Microsoft, Google und Apple vertrauen auf Lookout. Lookout hat seinen Hauptsitz in San Francisco und verfügt über Niederlassungen in Amsterdam, Boston, London, Sydney, Tokio, Toronto und Washington, D.C. Um mehr zu erfahren, besuchen Sie www.lookout.com/de und folgen Sie Lookout im unternehmenseigenen Blog, sowie auf LinkedInund Twitter.