Lookout

DAS SPEKTRUM 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.

DIE MATRIX FÜR MOBILE RISIKEN

Risikokomponenten

Vektoren

	APPS	GERÄT	NETZWERK	WEB UND CONTENT
BEDROHUNGEN	**App-Bedrohungen** 1 Bösartige Apps können Informationen ausschleusen, die Gerätehardware beschädigen und unberechtigten Fernzugriff gewähren.	**Gerätebedrohungen** Gerätebedrohungen können zu einem katastrophalen Datenverlust führen, da sich Angreifer auf diese Weise umfassendere Berechtigungen verschaffen.	**Netzwerk-bedrohungen** 5 Daten sind Angriffen über WLAN- oder Mobilfunkverbindungen ausgesetzt.	**Web- und Content-bedrohungen** Die Bedrohungen umfassen bösartige URLS, die in Phishing-E-Mails oder SMS-Nachrichten angeklickt werden.
SOFTWARE-SCHWACHSTELLEN	**App-Schwachstellen** Auch namhafte Softwarefirmen veröffentlichen mitunter Apps, die Sicherheitslücken enthalten und Unternehmens- und Userdaten gefährden.	**Geräte-schwachstellen** 2 Unternehmenseigene Geräte bieten „Angriffsfenster", d. h. sie sind in dem Zeitraum von der Veröffentlichung eines neuen Patches bis zur Implementierung des Updates gefährdet.	**Netzwerk-schwachstellen** Mobilgeräte sind einer deutlich größeren Zahl bösartiger Netzwerke ausgesetzt als Laptops und verfügen nicht über das gleiche Schutzniveau.	**Web- und Content-schwachstellen** Manipulierte Inhalte wie Webseiten, Videos und Fotos können einen unbefugten Gerätezugriff gestatten.
VERHALTEN UND KONFIGURATIONEN	**App-Verhalten und -konfigurationen** 3 Mobile Apps können den Verlust von Daten, beispielsweise von Kontaktdaten, begünstigen.	**Geräteverhalten und -konfigurationen** 4 Zahlreiche Verhaltensweisen gefährden die Sicherheit von Unternehmensdaten, wie beispielsweise das Aktivieren von USB-Debugging für Android oder das Installieren von Apps aus nicht offiziellen App-Stores.	**Netzwerkverhalten und -konfigurationen** Das Herstellen einer Verbindung zu einem falsch konfigurierten Router, einem unbekannten Captive Portal oder einem Netzwerk, das den Datenverkehr zwecks Inhaltsfilterung entschlüsselt.	**Web-/ Contentverhalten und -konfigurationen** Der Besuch von Websites mit "geringer Reputation", die Anmeldedaten nicht verschlüsseln sowie Unternehmensdaten ungewollt abfließen lassen und die Wahrscheinlichkeit böswilliger Aktivitäten erhöhen.

HÄUFIGKEIT VON RISIKEN FÜR MOBILE PLATTFORMEN

47 VON 1000 UNTERNEHMENSEIGENEN ANDROID-GERÄTEN WAREN APP-BASIERTEN BEDROHUNGEN AUSGESETZT

In zwei aufeinanderfolgenden Quartalen (Q4 2016 – Q1 2017) waren 47 von 1.000 durch Lookout Mobile Endpoint Security abgesicherte unternehmenseigene Android-Geräte App-basierten Bedrohungen ausgesetzt. 1

57 % DER IOS-USER HABEN IHRE BETRIEBSSYSTEME LEDIGLICH BIS ZUR VERSION 10.3 AKTUALISIERT

Von der Veröffentlichung von iOS 10.3 am 27. März 2017 bis zum 14. April 2017 hatten nur 43 % aller User ihre Geräte auf die neueste iOS-Version aktualisiert. Dies ist besorgniserregend, da die Version 10.3.1 einen Codeausführungsfehler behebt, der über WLAN ausgenutzt werden kann. Diese Information basiert auf Daten von iOS-Anwendern, die Lookout Personal nutzen. 2

30 % DER APPS AUF UNTERNEHMENSEIGENEN IOS-GERÄTEN GREIFEN AUF KONTAKTE ZU

75 % aller von Lookout Mobile Endpoint Security abgesicherten iOS-Geräte in Unternehmen haben Kamerazugriff, 38 % haben Zugriff auf GPS, 8 % auf Kalender und 10 % auf das Mikrofon. 43 % aller iOS-Unternehmens-Apps sind mit Facebook und 14 % mit Twitter verbunden. 3

5 VON 1000 UNTERNEHMENSEIGENEN ANDROID-GERÄTEN SIND GEROOTED

Nur 1 von 1.000 unternehmenseigenen iOS-Geräten ist von Jailbreaking betroffen. 4

BIS ZU 1 % DER UNTERNEHMENSEIGENEN MOBILGERÄTE WAR NETZWERKBASIERTEN BEDROHUNGEN AUSGESETZT

Forschungsergebnisse von Lookout belegen, dass im vergangenen Jahr etwas weniger als 1 % der unternehmenseigenen Mobilgeräte netzwerkbasierten Bedrohungen ausgesetzt war. 5

METHODIK:

Die analysierten Daten stammen aus einer großen globalen Teilmenge an privat und im Unternehmen genutzten Geräten, die von Lookout abgesichert werden. Die Daten wurden zwischen dem 15. April 2016 und 16. April 2017 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 100 Millionen Android- und iOS-Geräte weltweit. Die Datenerfassung erfolgte anonym, Unternehmensdaten oder Daten aus Netzwerken oder Systemen wurden nicht erfasst.

ÜBER LOOKOUT:

Das Unternehmen Lookout bietet Cybersicherheitslösungen an, die es Millionen Privatpersonen, Unternehmen und Regierungsbehörden ermöglichen, für mobile Sicherheit zu sorgen. Lookout verfügt über eine Datenbank, die fast alle mobilen Codes weltweit umfasst – derzeit 40 Millionen Apps, zu denen ständig neue dazukommen. Damit kann die Lookout Security Cloud Netzwerkverbindungen identifizieren, die andernfalls unbemerkt blieben, und mobile Angriffe vorhersehen und stoppen, bevor sie Schaden anrichten können. Lookout ist die bevorzugte mobile Sicherheitslösung der weltweit führenden Mobilfunkbetreiber, darunter AT&T, die Deutsche Telekom, EE, KDDI, Orange, Sprint, T-Mobile und Telstra. Auch führende Unternehmen wie AirWatch, Ingram Micro, Microsoft und MobileIron haben Lookout als Partner gewählt. Lookout hat seinen Hauptsitz in San Francisco und verfügt über Niederlassungen in Amsterdam, Boston, London, Sydney, Tokio, Toronto und Washington, DC. Weitere Informationen finden Sie unter www.lookout.com. Abonnieren Sie den Lookout-Newsletter oder folgen Sie Lookout auf Facebook, Twitter und LinkedIn.