Wie Lookout Phishing and Content Protection funktioniert?

Phishing und Content-Bedrohungen auf Mobilgeräten

Phishing ist das primäre Mittel, mit dem Angreifer versuchen, sich Zugang zu Ihrem Firmennetzwerk zu verschaffen. Dabei ist es relativ leicht, einen Anwender zum Anklicken eines Links zu verleiten, der zu einer präparierten Website oder ungewollten Downloads führt. In einer exklusiven Studie von Lookout stellte sich heraus, dass bis zu 25 % der Mitarbeiter bei Phishing-Tests auf gefälschte Links hereinfallen. Die Angreifer haben schnell gemerkt, dass E-Mails die kostengünstigste Methode sind, um eine Phishing-Attacke auszuführen. Deshalb haben viele Unternehmen bereits in den Schutz ihrer E-Mails investiert, mit Firewalls, Gateways oder Spam-Filtern, die auch auf Mobilgeräten vor Phishing schützen können, sofern diese ausschließlich für geschäftliche E-Mails verwendet werden. Das ist jedoch mehr oder weniger Wunschdenken, denn viele Mitarbeiter können über ihr Mobilgerät sowohl auf Firmen- als auch private E-Mails sowie Unternehmens- und persönlich genutzte Apps zugreifen.

Phishing auf Mobilgeräten ist nicht nur anders, sondern auch problematischer als herkömmliche Phishing-Attacken, denn es eröffnet Hackern neue Einfallstore über die klassische Firmen-E-Mail hinaus:

Private E-Mails: Eine Phishing-E-Mail kann an ein privates E-Mail-Konto gesendet werden, das die bei vielen kostenlosen E-Mail-Diensten enthaltenen Sicherheitsfunktionen umgeht und den Anwender dazu verleitet, einen Link anzuklicken und damit die Daten auf dem Gerät und die Firmenzugangsinformationen preiszugeben.

SMS: eine SMS, die an einen nichts ahnenden Anwender gesendet wird und einen verkürzten Link enthält, der zu einer präparierten Website führt oder den Download von Malware-Apps oder Surveillanceware auslöst

Präparierte Anzeigennetzwerke: URLs werden in Apps eingebettet, um mit anderen Diensten zu kommunizieren und das Anwendererlebnis zu verbessern – etwa Navigationsdienste, die Verbindung zu Online-Shops oder die Anzeige kontextbezogener Anzeigen. Wenn eine App jedoch so programmiert ist, dass sie auf eine präparierte URL zugreift, kann damit der Download von Plug-ins für Malware oder Spyware ausgelöst werden.

Messaging-Plattformen: eine Nachricht, die über WhatsApp, Facebook Messenger oder Instagram an Anwender gesendet wird, um sie zum Herunterladen von Spyware zu bewegen

Darum müssen sich Unternehmen vor Phishing-Angriffen auf Mobilgeräten schützen

Laut einer IDC-Umfrage berichteten 30 % der befragten Unternehmen davon, dass Mitarbeiter 2018 Ziel von Phishing auf Mobilgeräten gewesen waren.[1] 56 % aller Lookout-Anwender haben sogar bereits Phishing-URLs über ihr Mobilgerät erhalten und aufgerufen. Im Laufe eines Jahres tippten diese Anwender im Durchschnitt sechs Phishing-URLs auf ihren Geräten an.

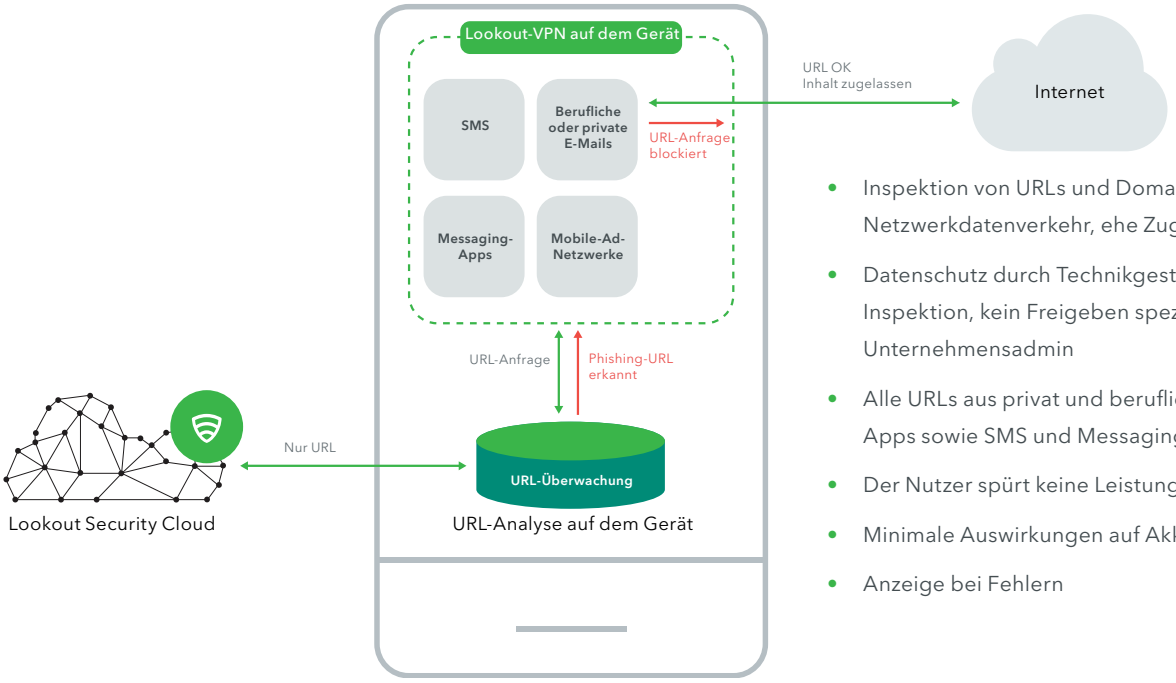
85 %

Seit 2011 ist die Zahl der Lookout-Anwender, die präparierte URLs auf ihren Mobilgeräten antippen, jährlich um durchschnittlich 85 % gestiegen.

[1] Quelle: 2018 U.S. Enterprise Mobility Decision Maker Software Survey, IDC

So funktioniert es

Die KI-Engine (künstliche Intelligenz) von Lookout schützt das Unternehmen vor Zero-Day-Bedrohungen und bekannten Cybersicherheitsrisiken und erkennt Phishing-Attacken in Echtzeit. Lookout Phishing AI durchforstet das Internet auf der Suche nach neuen Phishing-Websites, die gerade im Entstehen sind. Da Lookout dabei fortlaufend aktiv auf der Suche ist, erkennt es präparierte Websites bereits, während sie erstellt werden, also noch bevor der erste Angriff erfolgt.



- Inspektion von URLs und Domainnamen im Netzwerkdatenverkehr, ehe Zugriff erlaubt wird
- Datenschutz durch Technikgestaltung, keine Content-Inspektion, kein Freigeben spezifischer URLs an den Unternehmensadmin
- Alle URLs aus privat und beruflich genutzten E-Mail-Apps sowie SMS und Messaging-Plattformen
- Der Nutzer spürt keine Leistungseinbußen.
- Minimale Auswirkungen auf Akkulaufzeit
- Anzeige bei Fehlern

Der Phishing- und Content-Schutz von Lookout inspiziert auf dem Gerät sämtliche URL-Anfragen, die über E-Mails (berufliche wie private), SMS und Messaging-Apps eingehen oder in App-Browsern eingebettet sind. Erkennt Lookout eine präparierte Website, wird die Anfrage dynamisch blockiert.

Mittels eines lokal gehosteten VPN analysiert der Phishing- und Content-Schutz von Lookout den Datenverkehr und erkennt, wenn ein Browser oder eine App des Geräts versucht, eine verdächtige URL zu öffnen. Damit die Privatsphäre des Nutzers gewahrt bleibt, erhält die MES-Konsole 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. In der „Lookout for Work"-App heißt diese Funktion „Safe Browsing" (Sicheres Surfen).

Datenschutz und Datenerfassung

Bei der Produktentwicklung achtet Lookout von Anfang an auf die datenschutzkonforme Technikgestaltung[2]. Wir erfassen ausschließlich Daten, die zur Erfüllung unseres Sicherheitsversprechens erforderlich sind. Diese Daten sind bei der Übertragung und Speicherung geschützt und wir verfügen über zuverlässige Kontrollmechanismen, die noch weiter einschränken, welche personenbezogenen Daten erfasst und den Administratoren angezeigt werden.

Um Anwendern beruhigende Sicherheit zu bieten und behördliche Vorschriften einzuhalten, verpflichtet sich Lookout, die strengsten Zertifizierungen und Zulassungen zu erlangen. Deshalb ergreifen wir folgende Compliance-Maßnahmen:

- EU-US-Datenschutzschild – abgeschlossen Oktober 2016
- FedRAMP, „In Process" – abgeschlossen März 2017
- ISO 27001 – abgeschlossen Juni 2017
- ISO 27018 – abgeschlossen Dezember 2017
- DSGVO – konform mit der Datenschutz-Grundverordnung EU 2016/679

[2] https://dsgvo-gesetz.de/art-25-dsgvo/

Schwerpunkt URL-Analyse

Der Phishing- und Content-Schutz von Lookout analysiert URLs, die über E-Mails, SMS, Anzeigennetzwerke und Messaging-Plattformen angefragt werden, und zwar mit einer Mischung aus geräte- und cloudbasierten, KI-gesteuerten Technologien. Die Inhalte dieser Apps werden weder erfasst noch gespeichert oder mit Unternehmensadministratoren geteilt. Keine Daten oder Inhalte werden vom Gerät weg durch ein Web-Gateway weitergeleitet.

Lookout und die DSGVO-Konformität

Die Datenschutz-Grundverordnung (DSGVO) regelt den Schutz und die Sicherheit von Daten zu in der EU ansässigen Personen ganz neu. Um der DSGVO (Verordnung [EU] 2016/679) nachzukommen, unternimmt Lookout jeden wirtschaftlich vertretbaren Aufwand, inklusive empfohlener technischer und organisatorischer Maßnahmen.

Die DSGVO bestimmt, wie Organisationen personenbezogene Daten erfassen, speichern, verwenden und absichern sollen. Um dies zu gewährleisten, konzentrieren wir uns auf die folgenden allgemeinen Anforderungen.

Überzeugende Argumente für Lookout

Mit Lookout dehnen Sie Ihren Phishing-Schutz auf Mobilgeräte aus, der dann private E-Mails, SMS, Messaging-Plattformen und Apps abdeckt.

So unterstützen Sie den digitalen Wandel, denn damit steht der Nutzung von Mobilgeräten für die Arbeit nichts mehr im Wege. Ihre Daten und Systeme sind vor schädlichen Inhalten geschützt, unabhängig davon, ob sich der Mitarbeiter innerhalb des geschützten Unternehmensnetzwerks befindet oder nicht.

Lookout bietet umfassenden Schutz vor allen Facetten mobiler Risiken, einschließlich des Web- und Content-Bedrohungsvektors, der von Angreifern am häufigsten genutzt wird, um Unternehmensdaten über Mobilgeräte auszuspähen.

Lookout – der feine Unterschied

- Dank unserer globalen Ausrichtung und unserer Konzentration auf Mobilgeräte verfügt Lookout über einen der weltweit größten Datensätze zur mobilen Sicherheit. Lookout hat Sicherheitsdaten von über 170 Millionen Geräten weltweit sowie über 70 Millionen Apps erfasst. Täglich kommen bis zu 90.000 neue Apps hinzu.
- Dank dieses globalen Sensorennetzwerks kann unsere Plattform Bedrohungen im Voraus erkennen. Wir setzen dafür maschinelle Intelligenz ein, um komplexe Muster zu identifizieren, die auf Risiken hindeuten. Diese Muster wären für menschliche Analysten nicht erkennbar.
- Die Mobilität hat eine neue Ära der Datenverarbeitung eingeläutet. Benötigt wird eine neue Generation von Sicherheitslösungen, die speziell für diese Plattform entwickelt wurden. Lookout spezialisiert sich bereits seit 2007 auf mobile Sicherheit und verfügt über das gebotene Expertenwissen in diesem Bereich.

Mithilfe von Lookout kann Ihr Unternehmen sicher mobil unterwegs sein. Und zwar ohne Einbußen bei der Produktivität, denn Lookout versorgt die IT- und Sicherheitsteams mit der erforderlichen Transparenz. Um zu erfahren, wie Sie Ihre mobile Flotte noch heute sichern können, kontaktieren Sie uns unter lookout.com/de.