Phishing- und Content-Schutz von Lookout

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.

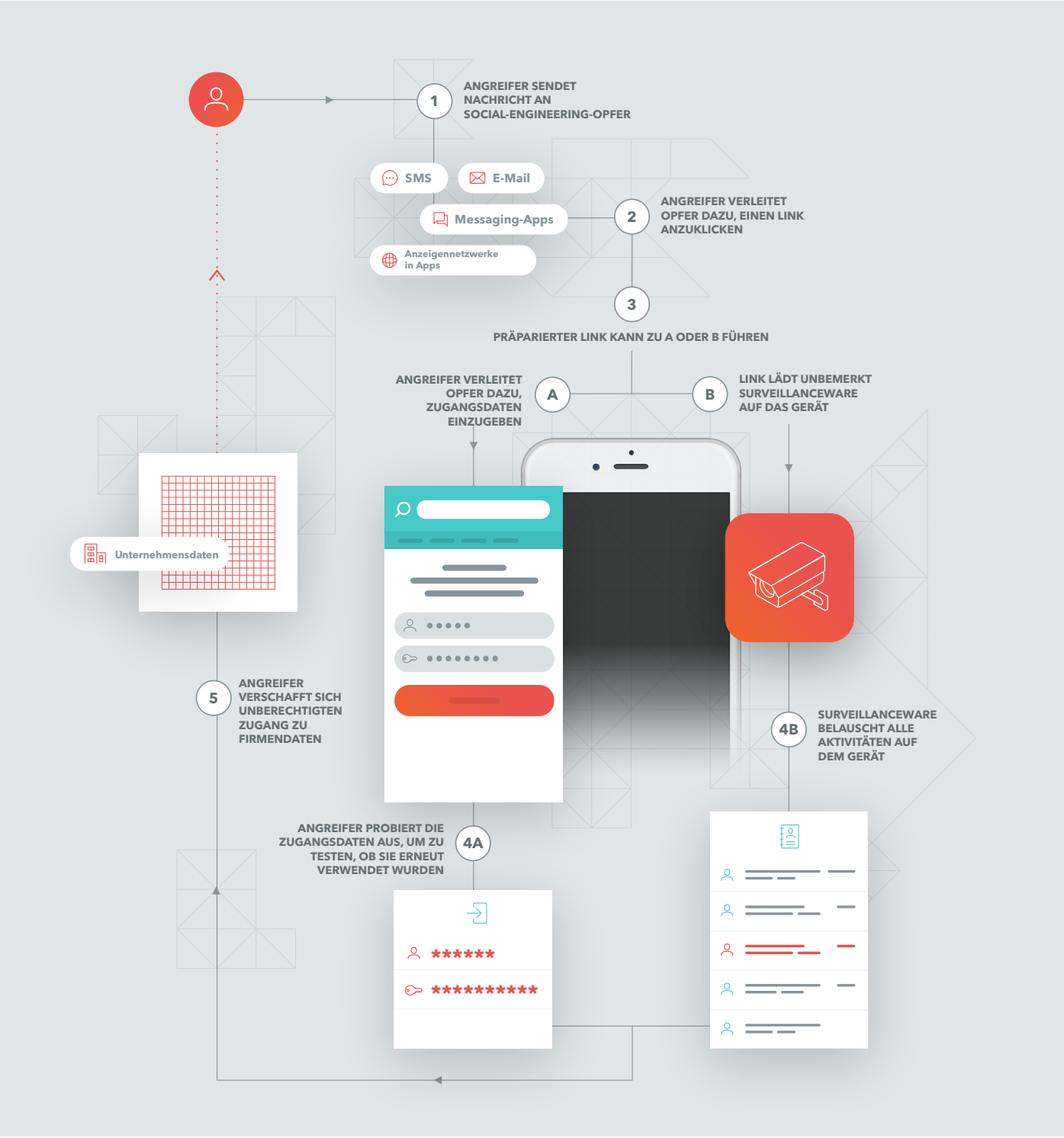
Messaging-Plattformen: eine Nachricht, die über WhatsApp, Facebook Messenger oder Instagram an Anwender gesendet wird, um sie zum Herunterladen von Spyware zu bewegen

Best Practices für den Schutz vor Phishing und Content-Bedrohungen

1. Sorgen Sie für einen angemessenen Desktop- und Web-Gateway-Schutz für geschäftliche E-Mail-Konten, um Infektionen durch schädliche Anhänge und URLs zu vermeiden.
2. Stellen Sie einen umfassenden Phishing-Schutz auf Android- oder iOS-Mobilgeräten bereit, der private E-Mails, SMS, Messaging-Plattformen und Apps abdeckt.
3. Schulen Sie Ihre Mitarbeiter im Erkennen von Phishing- und Social-Engineering-Angriffen auf verschiedenen Kanälen wie E-Mail, SMS und soziale Medien.

Wie läuft ein Phishing-Angriff auf Mobilgeräten ab?

Phishing-Angreifer geben sich längst nicht mehr mit E-Mails zufrieden, sondern setzen vermehrt auf Mobilgeräte, die sich schnell zu einem primären Vektor für Phishing-Angriffe entwickelt haben, um Surveillanceware einzuschleusen und Zugang zu Unternehmensdaten und -netzwerken zu erhalten.



Darum müssen sich Unternehmen vor Phishing-Angriffen auf Mobilgeräten schützen

Laut IBM fallen Mobilgerätenutzer dreimal eher auf Phishing-Betrug herein. 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 %

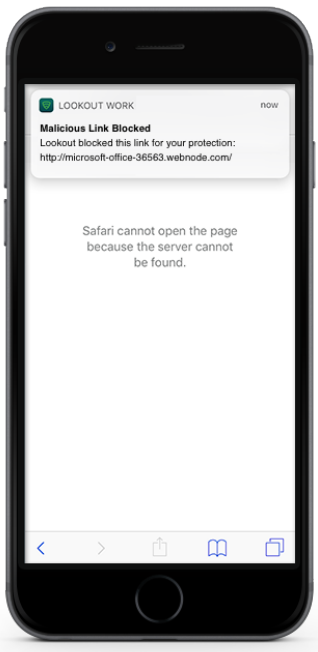
Seit 2011 ist die Zahl der Lookout-Anwender, die präparierte URLs auf ihren Mobilgeräten antippen, jährlich um durchschnittlich 85 % gestiegen.

Wenn es einem Angreifer gelingt, einen Anwender dazu zu verleiten, Firmenzugangsdaten preiszugeben, erhält er unbefugten Zugriff auf die Unternehmenssysteme, sodass er sich ungehindert durch Ihre Infrastruktur bewegen und Ihre Daten ausspionieren kann.

So schützt Lookout vor Phishing-Angriffen

Der Phishing- und Content-Schutz von Lookout ist eine umfassende Funktion von Lookout Mobile Endpoint Security, die Unternehmen vor Phishing-Angriffen über sämtliche Kanäle wie E-Mail (geschäftlich und privat), SMS, Messaging-Apps und in Apps eingebettete URLs schützt.

Sobald ein Anwender versucht, eine Verbindung herzustellen, überwacht Lookout sämtliche ausgehenden Verbindungen des Mobilgeräts und alle installierten Apps auf Netzwerkebene. Da dabei der Inhalt von Nachrichten nicht überprüft wird, bleibt die Privatsphäre des Endnutzers gewahrt. Dadurch unterscheidet sich unser Ansatz von herkömmlichen Lösungen. Lookout vergleicht die URL, die geöffnet werden soll, mit bekannten präparierten URLs aus der Lookout Security Cloud und warnt den Anwender im Ernstfall, bevor eine Verbindung hergestellt wird. Diese Echtzeitwarnungen verhindern, dass der Anwender gefährliche Inhalte wie infizierte Apps oder Websites mit bekannten Schwachstellen öffnet.



Über die Lookout-Konsole können Administratoren Nutzer blockieren, die versuchen, auf dem Mobilgerät eine Verbindung zu bekannten schädlichen URLs herzustellen, die über präparierte Websites gehostet werden und möglicherweise versuchen, Zugangsdaten auszuspähen.

Als schädliche URLs gelten betrügerische Anzeigen, Botnets, Command and Control Center (C&C), infizierte Anzeigen-Links zu Malware, Call Home, Malware-Verbreitungspunkte, Phishing/Betrug, Spam-URLs und Spyware.

In Lookout Mobile Endpoint Security ist diese Funktion standardmäßig deaktiviert. Ein Administrator muss den Phishing- und Content-Schutz erst in der Konsole aktivieren und der Anwender muss auf dem Gerät die nötigen Berechtigungen erteilen.

Administratoren haben auch die Möglichkeit, Anwender vor gefährlichen Websites zu warnen, bevor diese sie öffnen. Und wenn der Phishing- und Content-Schutz auf einem Gerät deaktiviert ist, können Administratoren dieses Gerät als nicht konform markieren, bis der Schutz wieder aktiviert wird.

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 150 Millionen Geräten weltweit sowie über 50 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 info@lookout.com