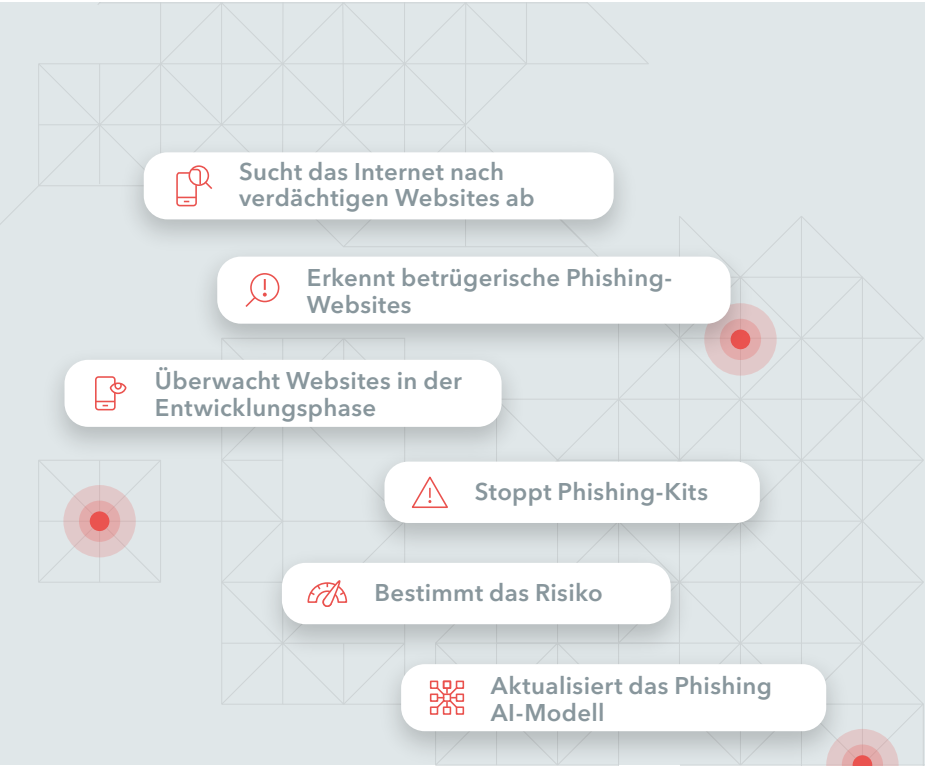
Lookout Phishing AI erkennt aktiv Vorzeichen für Phishing-Websites und warnt Unternehmen

Überblick

Die meisten Cyberangriffe auf Unternehmen beginnen mit Phishing, denn mit nur wenigen Methoden können sich Cyberkriminelle so schnell Zugangsdaten für sensible Daten ergaunern. Um Unternehmen davor zu schützen, hat Lookout Phishing AI entwickelt: Diese Lösung erkennt frühe Anzeichen für Angriffe, bietet Schutzmechanismen für Lookout-Kunden und warnt Organisationen, die in der Schusslinie von Cyberkriminellen stehen, rechtzeitig – ganz gleich, ob sie Kunden von Lookout sind oder nicht. Da Lookout Phishing AI gefährliche Websites bereits in der Entstehungsphase erkennen kann, werden betroffene Unternehmen oft schon vor Beginn der eigentlichen Attacke informiert. Unseren Erkenntnissen können Sie auch auf Twitter folgen, unter @PhishingAI.

So funktioniert es

Phishing AI nutzt hochmoderne Algorithmen der künstlichen Intelligenz, patentierte Technologien zur Mustererkennung und maschinelles Lernen, um im Internet aktiv nach im Aufbau befindlichen Phishing-Websites zu suchen. Sobald es eine potenzielle Phishing-Baustelle entdeckt hat, setzt Phishing AI Agenten ein, die anhand extrahierter Servermerkmale Risikoeinschätzungen vornehmen. So entstehen aussagekräftige Datensätze, die auf der Interaktion mit Milliarden Websites basieren. Die Machine-Learning-Engine überwacht das Phishing-Kit nicht nur in der Anfangsphase, sondern behält dessen gesamten Entwicklungszyklus im Auge. Phishing-Kits tauchen plötzlich auf, schlagen zu und verschwinden dann wieder, um später mit anderen Exploit-Methoden erneut ihr Unwesen zu treiben. Angesichts dieser Wandelbarkeit stehen Phishing-Kits unter ständiger Beobachtung durch Lookout Phishing AI – so lassen sich Angriffe schon im Vorfeld unterbinden.



Die Funktion kurz vorgestellt

Maschinelles Sehen

Phishing AI umfasst maschinelles Sehen – eine Technologie, mit der Lookout den Unterschied zwischen seriösen Websites und betrügerischen Phishing-Nachahmungen erkennen kann. Dadurch ist Phishing AI in der Lage, Logos und Grafiken zu analysieren und so selbst raffinierte Website-Kopien aufzuspüren, die arglose Nutzer zur Eingabe ihrer Nutzerdaten verleiten sollen. Mit der zunehmenden Verbreitung des Phishings imitieren Cyberkriminelle auf tauschend ähnliche Weise Webauftritte, die für das menschliche Auge kaum noch vom Original zu unterscheiden sind.

Warum braucht man Phishing AI, um Angriffe zu unterbinden?

Phishing AI erkennt Tag für Tag über 10.000 aktive Phishing-Websites. Dabei handelt es sich um eine weltweit übliche Betrugsmasche, die sich so schnell entwickeln und erweitern lässt, dass Benutzer diese Bedrohungen nicht in Echtzeit erkennen und darauf reagieren können. Phishing kennt keine Ländergrenzen – die Gefahr lauert also praktisch überall. Wirksame Gegenmaßnahmen übersteigen daher in der Regel die Möglichkeiten einzelner Behörden oder gar Personen. Nur ein KI-basierter Ansatz kann agilen Phishern, die es auf potenziell mehrere Milliarden Internetnutzer weltweit abgesehen haben, auf die Schliche kommen und ihnen das Handwerk legen.

Warum 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.

Phishing im Überblick

- Phishing AI erkennt und verfolgt Tag für Tag über 10.000 aktive Phishing-Websites.
- Phishing AI entdeckt jeden Tag 500 neue, besonders täuschend ähnliche Phishing-Websites.
- Unternehmensanwender fallen dreimal häufiger auf Phishing-Betrug herein, wenn sie ein Mobilgerät nutzen.

Phishing auf Mobilgeräten (60 %) ist ein größeres Sicherheitsrisiko als der physische Verlust/ Diebstahl von Mobilgeräten (30 %).[1]

[1] Phil Hochmuth: „Mobile Security and the Future of Work", IDC 2019

Lookout – der große 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 können Ihre Mitarbeiter 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 Mobilflotte noch heute besser absichern können, kontaktieren Sie uns unter www.lookout.com/de.