SONICWALL

PHISHING IM ZEITALTER VON SAAS

Ein Leitfaden für Unternehmen und Anwender

Einführung

Phishing-Attacken sind zur wichtigsten Hacking-Methode gegen Organisationen aufgestiegen. Früher schob man hauptsächlich dem Anwender die Schuld in die Schuhe, aber inzwischen wirken diese Attacken so echt, dass selbst die in Sachen Sicherheit erfahrensten Empfänger darauf hereinfallen. Phishing-Angriffe haben kürzlich mit der Verbreitung von SaaS am Arbeitsplatz neue Erfolge erzielt.

Was ist Phishing?

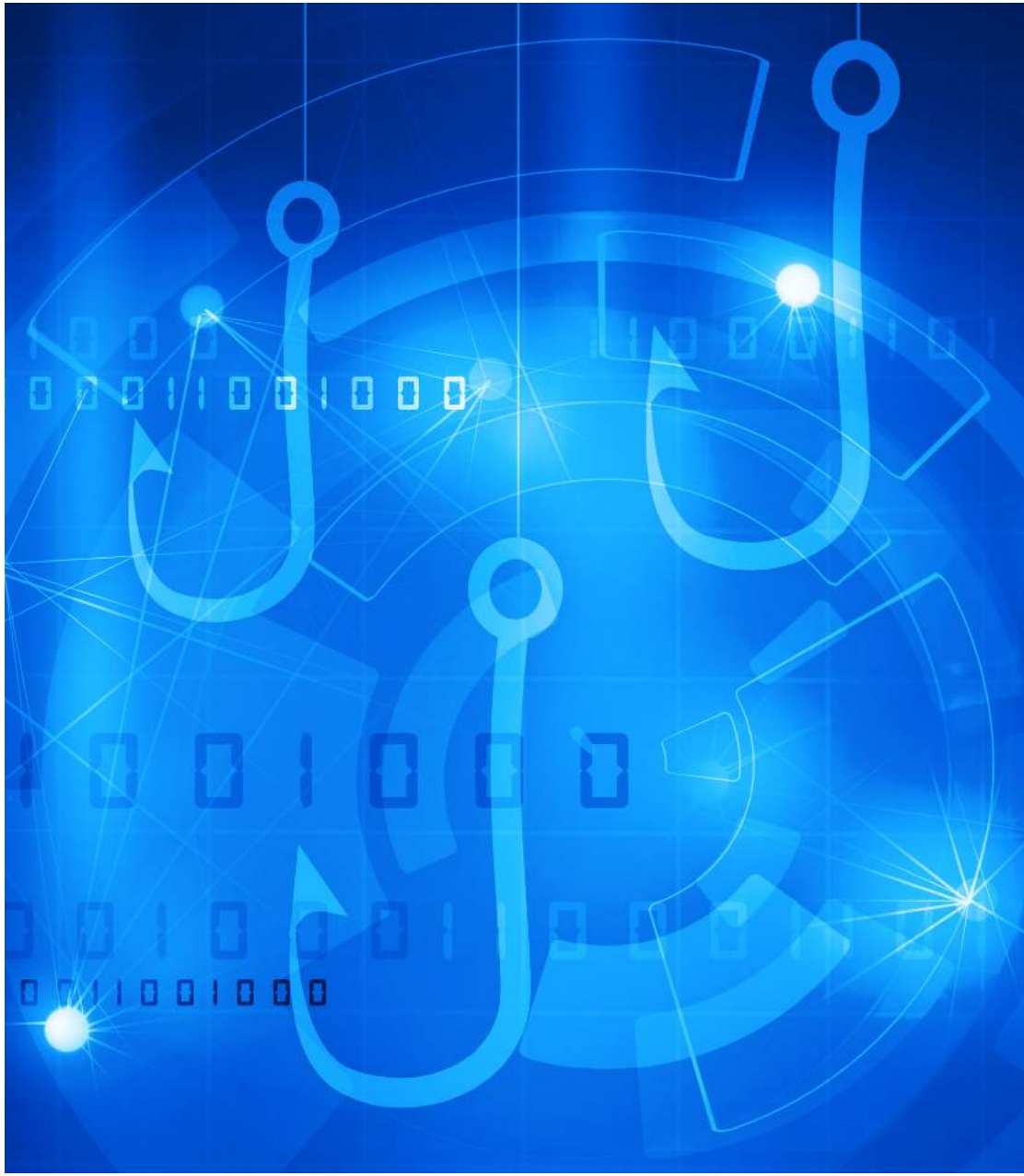
Phishing ist eine Hacker-Methode, bei der der Angreifer in böser Absicht eine Nachricht versendet – meist eine E-Mail, manchmal aber auch über SMS, Skype- oder Slack-Nachricht. Der Angreifer gibt sich als vertrauenswürdige Person aus und will den Empfänger dazu bringen, vertrauliche Daten preiszugeben, Geld zu überweisen oder die Verbindung zu einer Betrugsseite herzustellen.

Phishing ist aus mehreren Gründen nach wie vor eine sehr wirksame Hacking-Methode.

1. Weil sie die üblichen Kommunikationskanäle nutzen, haben Hacker direkten Zugang zu allen Benutzern in der Organisation.
2. Computerbasierte Filter verlieren irgendwann ihre Wirkung, weil Hacker mit ständigem Reverse Engineering schließlich den richtigen Algorithmus für den Zugang zum Netzwerk finden.

Phishing-Attacken können sich wie ein Computer-Wurm ausbreiten.

Wenn ein Account einmal infiziert ist, können über den Angriff Mitteilungen an alle Kontakte des Account-Inhabers geschickt werden, sodass künftige E-Mail-Attacken aus einer vertrauenswürdigen Quelle und ihrem rechtmäßigen Account stammen.



Wer wird nachgeahmt?

Generell versuchen Hacker sich als vertrauenswürdige Person oder legitimer Service auszugeben. Damit sie echt wirken, passen das Format und die Sendezeit oft zum beabsichtigten Opfer. Zum Beispiel:

Jemand gibt sich als Mitarbeiter der Organisation aus

1. Der CEO bittet den CFO um Überweisung von Geldern
2. Die Personalabteilung bittet um Personendaten, besonders zum Jahresabschluss oder wenn die Steuererklärung fällig ist
3. Ein „neuer“ Mitarbeiter in einer Außenstelle hat Fragen

Fälschung einer automatisierten Mitteilung, die vorgeblich von einem vertrauenswürdigen Service stammt

1. Ein Link auf ein geteiltes Google Doc
2. Der Einzahlungsbeleg von der Bank
3. Eine Versandbestätigung von FedEx

SONICWALL®

Worauf sind sie aus?

Letzten Endes wollen Hacker Geld machen. Es handelt sich um finanziell gut ausgestattete Gruppen mit „Investoren“, die eine Rendite erwarten.

Direktes Geld

Zum Beispiel falsche Überweisungen oder Erpressersoftware, die eine Zahlung zur Entschlüsselung verschlüsselter Daten verlangt.

Fälschung einer automatisierten Mitteilung, die vorgeblich von einem vertrauenswürdigen Service stammt

Verkauf von Benutzerdaten zu kompromittierten Accounts, Kreditkartennummern, personenbezogene Daten usw. im Darknet an andere Kunden, die sie zu Geld machen.

Warum ist Phishing auf SaaS-Plattformen einfacher?

Die Wurzeln der Phishing-Attacken lassen sich bis in die Anfangszeit der E-Mail zurückverfolgen, aber die allgemeine Verbreitung von SaaS hat zu einem Wiederaufleben dieser Hacking-Methode geführt. SaaS-Anwendungen sind besonders anfällig für diese Verletzungen, weil sie bei jeder Form von Phishing-Attacke eingesetzt werden können.

Zugang

Sich als eine andere Person auszugeben ist einfacher, wenn die SaaS der vertrauenswürdige Kommunikationskanal ist und das Login von überall stammen kann. Gelingt Hackern der Diebstahl von Benutzerdaten, haben sie unmittelbaren Zugriff auf den Account.

Verhalten

Der Diebstahl von Benutzerdaten über SaaS-Anwendungen ist einfach, weil **Endnutzer ständig aufgefordert werden, sich neu zu authentisieren**, und gewöhnlich Nachrichten mit Links zu einem Login bekommen. Eine Bitte um Anmeldedaten erregt nicht viel Verdacht, auch wenn sie in skrupelloser Absicht verschickt wurde.

Einheitlichkeit

Ein weiterer Aspekt von SaaS, der die Anfälligkeit gegenüber Phishing-Attacken erhöht, ist ihre **Einheitlichkeit**. Hacker können einen Account öffnen und ihre Methoden testen, bis es ihnen gelingt, an den Standardfiltern vorbei zu kommen. Und wenn sie dann einmal ungehindert Zugang zum E-Mail-Postfach haben, besteht die einzige Hürde im unaufmerksamen Endnutzer.

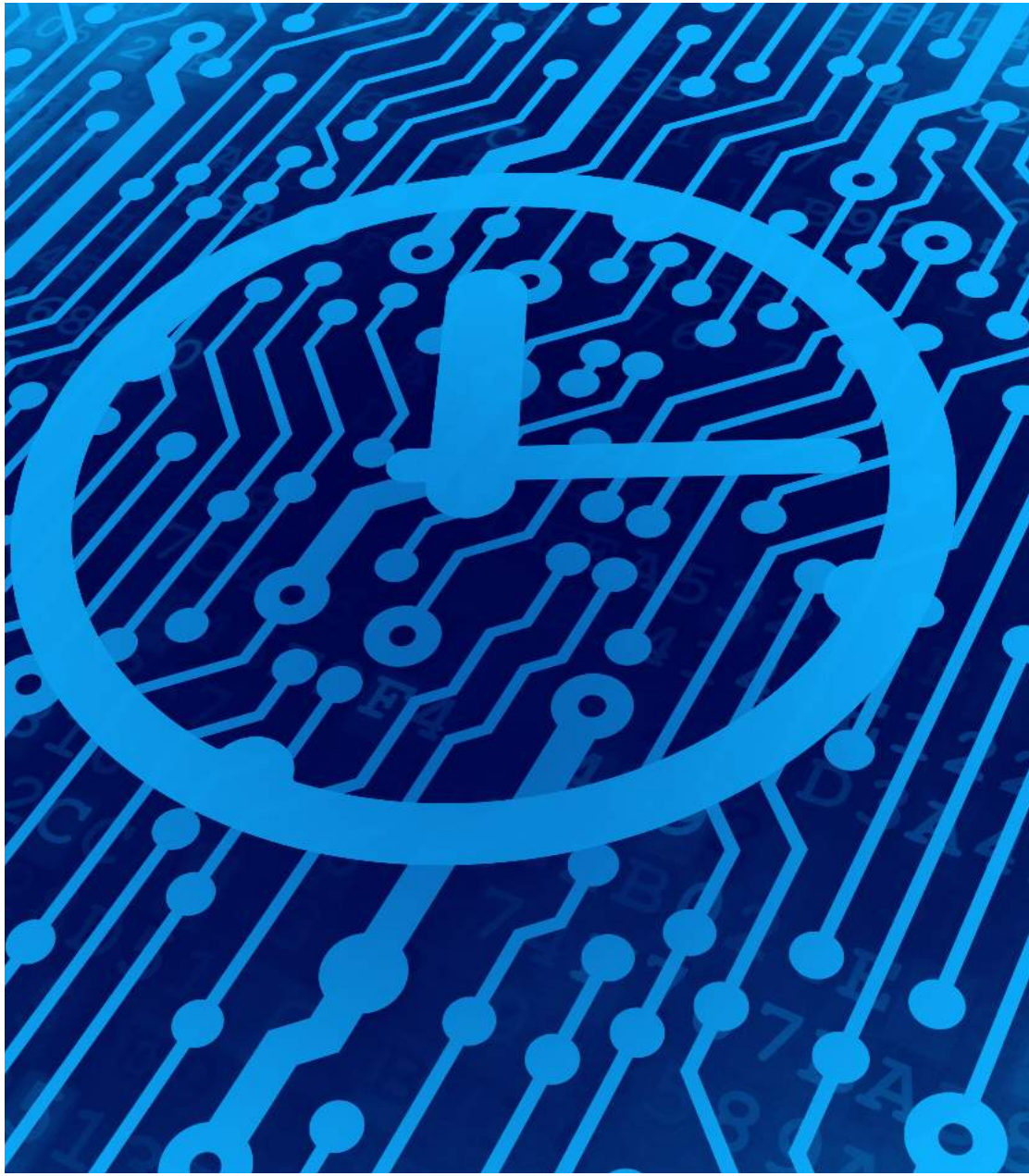
Frühere Verteidigungs-maßnahmen

Wer Phishing bekämpfen will, braucht zusätzliche Sicherheits-vorkehrungen, die über den Standardschutz der SaaS hinaus gehen. Bis vor kurzem liefen die meisten Lösungen extern – entweder stellvertretend für eingehende Nachrichten (MTA, Mail Transfer Agent) oder als Gateway zwischen Endnutzer und Service (Forward- oder Reverse-Proxy). Weil diese Lösungen an der Netzwerkgrenze eingesetzt wurden, waren sie gewöhnlich blind gegenüber Bedrohungen von innen – infizierte Accounts oder der Verkehr unter Kollegen.

Was Sie tun können

Die SonicWall Cloud App Security wurde zur Verteidigung gegen alle Formen von SaaS-Phishing-Attacken und zur Beseitigung der Schwachstellen konzipiert, die es mit den früheren Schutzvorkehrungen an der Netzwerkgrenze gab.

Die eingebaute Anti-Phishing-Technologie bietet die Sicherheits-schichten, die man zur Bekämpfung der zunehmenden SaaS Phishing-Attacken in allen Formen der SaaS-Kommunikation braucht – von der E-Mail bis zur Chat-Nachricht.



Lösungen

Nachahmungsanalyse – Mithilfe von Big-Data-Analyse

Absender und Inhalt der Nachricht werden auf Nachahmung untersucht. Die eingesetzten KI-Algorithmen zu Aufdeckung von und Schutz vor Nachahmung suchen nach:

Nachahmung eines Benutzers

Cloud App Security prüft, ob es in der Organisation einen ähnlichen Absender mit einer anderen E-Mail-Adresse gibt. Wir identifizieren den Absender durch die Prüfung von Querverweisen an verschiedenen Stellen der E-Mail, wie Absender, E-Mail-Signatur usw.

Nachahmung einer Domäne

Cloud App Security prüft, ob der Absender von einer Domäne aus sendet, die einer bekannten Domäne ähnelt, aber einen anderen Sendeweg, eine andere Quell-IP usw. hat.

Nachahmung einer Marke

Cloud App Security erkennt, wenn die E-Mail von einer vertrauenswürdigen Marke (FedEx, Microsoft usw.) zu kommen scheint, der Sendeweg der E-Mail aber nicht zu diesem Absender passt.

Lösungen

URL- und Dateianalyse – Mithilfe von Capture ATP

Weil viele Phishing-Attacken sich über eine schädliche URL verbreiten oder eine Schaddatei enthalten, muss dieser Inhalt unbedingt untersucht werden, bevor er den Endnutzer erreicht. Mit Capture ATP enttarnt und blockiert Cloud App Security sogenannte Advanced Threats (AT, fortgeschrittene Bedrohungen), bis ein Urteil darüber gefällt werden kann. Dieser Service zur Aufdeckung fortgeschrittener Bedrohungen kombiniert als einziger mehrschichtiges Sandboxing, einschließlich RealTime Deep Memory Inspection™ (RTDMI™), die Nachbildung des gesamten Systems und Virtualisierungsverfahren zur Analyse verdächtigen Code-Verhaltens in E-Mails, damit Kunden gegen die zunehmenden Gefahren von Zero-Day-Bedrohungen geschützt sind.
Zum Service gehört der fortgeschrittene URL-Schutz mit dynamischer Analyse eingegliederter URLs, womit Nachrichten mit schädlichen URLs bereits im Vorfeld blockiert und unter Quarantäne gestellt werden, damit die Benutzer erst gar nicht darauf klicken und Schaden erleiden.

Lösungen

Zur Umgehung der Standard-Sicherheitseinstellung in SaaS haben Hacker Angriffe erfunden, deren Entdeckung sich den üblichen Methoden entzieht. Es ist deshalb wichtig, diese Kombinationen zu testen und rekursiv nachzubilden, zum Beispiel, indem man eine URL in einer Datei findet, dem Link folgt und die Datei untersucht, die heruntergeladen werden könnte.

KI-Baselining für verdächtigen E-Mail-Verkehr

Durch Betrachtung verschiedener Kennzahlen vom Alter der verknüpften Domänen oder Überprüfung des Absenders kann Cloud App Security dem Endnutzer einen Hinweis schicken und fragen, ob dieser Absender bekannt oder vertrauenswürdig ist, ohne den Verkehr zu blockieren. Dank diesem Austausch mit dem Endnutzer kann der Algorithmus lernen, was legitim und was schädlich ist.

Dynamische Quarantäne- und Nachrichtenkontrolle

Cloud App Security prüft, ob der Absender von einer Domäne aus sendet, die einer bekannten Domäne ähnelt, aber einen anderen Sendeweg, eine andere Quell-IP usw. hat.

Überwachung kompromittierter Accounts

Cloud App Security erkennt, wenn die E-Mail von einer vertrauenswürdigen Marke (FedEx, Microsoft usw.) zu kommen scheint, der Sendeweg der E-Mail aber nicht zu diesem Absender passt.

Zusammenfassung

Es besteht eine Korrelation zwischen der Verbreitung von Phishing-Attacken und der zunehmenden Nutzung von SaaS. SonicWall Cloud App Security sorgt mit einem mehrschichtigen Ansatz für SaaS-Sicherheit und bietet den modernsten Schutz gegen Phishing mit verschiedenen Technologien und Anbietern in synchroner Arbeitsweise. Wir sorgen dafür, dass jede Organisation selbst vor den raffiniertesten Attacken geschützt ist.

Wollen Sie Ihre Organisation vor Phishing-Attacken schützen?

WENDEN SIE SICH AN UNSEREN VERTRIEB

Über uns

Seit über 27 Jahren verteidigt SonicWall kleine und mittelständische Unternehmen weltweit im Kampf gegen Cyberkriminalität. Unsere Kombination von Produkten und Partnerschaften liefert Echtzeit-Cyberschutzlösungen, die auf die spezifischen Bedürfnisse der über 500.000 Unternehmen in mehr als 215 Ländern und Gebieten abgestimmt sind. Das Ergebnis: Sie können sich beruhigt ganz auf Ihr Geschäft konzentrieren. Weitere Informationen finden Sie auf **www.sonicwall.com** oder folgen Sie uns auf Twitter, LinkedIn, Facebook und Instagram.

Wenn Sie Fragen zu den Nutzungsmöglichkeiten dieses Materials haben, wenden Sie sich bitte an:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

SONICWALL®

Ebook-PhishingInTheAgeOfSaaS-US-KJ-MKTG4123