

KURZDARSTELLUNG

Scam auf dem Vormarsch: warum E-Mails der Bedrohungsvektor Nummer eins sind

Auch heute noch starten die schlimmsten Datenlecks mit einer einzigen E-Mail.

Zusammenfassung

Beim Phishing geht es Hackern nicht einfach nur darum, dass Sie einen mit Malware infizierten Link anklicken. Ihr eigentliches Ziel ist, Anmeldedaten von Power-Usern zu stehlen. Damit erhalten sie Zugriff auf alle Daten und Systeme, für die der Benutzer autorisiert ist: Sie können E-Mails versenden, Geldüberweisungen anfordern und ihren bösartigen Code verbreiten.

E-Mails gehören nach wie vor zu den größten Bedrohungsvektoren. Daher müssen Unternehmen wachsam sein und ihre Mitarbeiter vor ausgeklügelten Phishing- und Malware-Angriffen in Form von Business-E-Mail-Compromise (BEC), Vortäuschung falscher Identitäten (Impersonation) und Betrug schützen.

Einführung

Jeden Tag werden knapp 320 Milliarden E-Mails versendet. E-Mails gehören immer noch zu den meistgenutzten Methoden, um Informationen – und Bedrohungen – auszutauschen. COVID-19 und Home-Office-Initiativen haben diesen Trend verstärkt. E-Mails sind heute daher das größte Einfallstor für alle möglichen Phishing- und Ransomware-Angriffe.

Wir haben in der Vergangenheit aus großen Datenlecks gelernt, dass bei hoch entwickelten Angriffen häufig unterschiedliche Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs) zum Einsatz kommen, um Benutzern zu schaden. In der Regel dienen E-Mails als Sprungbrett für Social-Engineering-Attacken wie BEC oder Credential-Phishing-Angriffe.

Laut dem Verizon Data Breach Report 2020 kam etwa in 22 Prozent der Sicherheitsvorfälle Social Engineering zum Einsatz, wobei 96 Prozent davon durch E-Mails ausgelöst wurden. Weitere 22 Prozent der Vorfälle sind dem Bericht zufolge auf menschliches Versagen zurückzuführen, etwa weil sensible Daten unabsichtlich an den falschen Empfänger weitergeleitet werden.

Eine weitere Studie von 451 Research ergab, dass 87 Prozent der Organisationen bereits ein E-Mail-Security-Produkt nutzen; doch 46 Prozent geben zu, dass von E-Mails immer noch das größte Risiko für Daten ausgeht. Außerdem meinen 46 Prozent, dass E-Mails die größte Schwachstelle sind – das Risiko schätzen sie fünfmal höher ein als bei der ihrer Ansicht nach nächstgrößeren Bedrohung.

Microsoft und Google dominieren den globalen cloudbasierten E-Mail-Markt mit ihren breiteren Office-Suite-Angeboten. So teilen sich die beiden Konzerne den weltweiten Marktanteil bei Office-Suite-Technologien. Mit mehr als 1,8 Milliarden Benutzern ist Gmail die beliebteste E-Mail-Plattform auf der Welt. Und Microsoft Office 365 wurde Ende 2020 von über einer Million Unternehmen rund um den Globus genutzt – 650.000 Unternehmen allein in den USA.

Dieser massive Pool potenzieller Opfer ist für Cyberkriminelle ein gefundenes Fressen: Ständig tüfteln sie an neuen Methoden, um Nutzer dieser cloudbasierten E-Mail-Services zu hacken. Somit sind cloudbasierte E-Mails einer der beliebtesten und lukrativsten Angriffsvektoren für opportunistische Hacker.



Phishing und E-Mail-Betrug: eine Erfolgsgeschichte

Phishingmails, die von gestohlenen, gefälschten oder gestohlenen bekannten Identitäten gesendet werden, sehen mittlerweile so authentisch aus, dass selbst versierte und sicherheitsbewusste Nutzer darauf hereinfallen. Trotz Bemühungen, Mitarbeiter für das Thema Sicherheit zu sensibilisieren, führen Phishing-Angriffe immer noch zu vielen Schwachstellen. Laut unseren interviewten Sicherheitsexperten klicken immer noch viele Benutzer auf gezielte themen- und ereignisbasierte Phishingmails, die seriösen E-Mails zum Verwechseln ähnlich sehen. Viele sind nicht in der Lage, seriöse E-Mails von gefälsch-

ten zu unterscheiden, verdächtige Links zu erkennen oder Vorsichtsmaßnahmen zu treffen, etwa indem sie URL, Identität des Senders und Unternehmenswebsite prüfen.

Hinzu kommt, dass eine Verbreitung kaum zu vermeiden ist. E-Mails und Anhänge von Mitarbeitern, Partnern und Kunden – und erst recht von Familienmitgliedern und Freunden – sind in dieser mobilen, kollaborativen Arbeitswelt gang und gäbe. Wir hinterfragen sie nicht, weil sie von vertrauenswürdigen Identitäten stammen und weil wir Zugriff auf Inhalte und Informationen für unsere Arbeit benötigen.

Business-E-Mail-Compromise

Wenn es um die Vortäuschung falscher Identitäten und Betrug geht, steht BEC ganz oben auf der Liste. Bei dieser Art von Angriff wird in der Regel ein kompromittiertes E-Mail-Konto eines CEO oder einer anderen hochrangigen Führungskraft genutzt. Über das kompromittierte Konto fordern die Betrüger die Opfer auf, bestimmte finanzielle Transaktionen durchzuführen, wie zum Beispiel eine gefälschte Rechnung zu bezahlen oder eine Geldüberweisung für den Abschluss einer erfundenen Geschäftsvereinbarung zu tätigen.

In den meisten Fällen greifen Cyberkriminelle auf Social Engineering oder Whaling-Attacken zurück, um die Konten der oberen Führungskreise für ihre Zwecke zu kapern. Dem Internet Crime Complaint Center (IC3) des FBI zufolge erlitten Unternehmen im Jahr 2020 einen Schaden von über 4,1 Milliarden USD infolge von Cyberangriffen. Mit 1,8 Milliarden USD verursachte BEC den größten finanziellen Schaden als einzelner Bedrohungsvektor.

Wenn Sie bemerken, dass das Nutzerkonto einer Führungskraft kompromittiert wurde, ist es schon zu spät. Es braucht nur ein kompromittiertes Konto, um eine virale Reaktion zwischen Nutzern, Geräten und Apps zu verursachen, die sich unmöglich eindämmen lässt – der Schaden ist meist vorprogrammiert.

Native Cloud-Sicherheit reicht nicht aus

Entwickler von E-Mail-Security-Lösungen haben bereits Methoden entworfen, um Nutzer vor schädlichen Links zu schützen, die Vorfilter umgehen und im Postfach landen. Dazu zählen etwa Click-Time-Schutz, Rückruf bereits gesendeter E-Mails und Webbrowser-Filter. Allerdings investieren Angreifer ebenso viel Mühe in die Entwicklung von Techniken, um ihr Ziel trotzdem zu erreichen.

Dem jüngsten Microsoft ATP Report 2020 zufolge schafft es mehr als eine von zehn gezielten Phishingmails in das Postfach der angegriffenen Person. Jede einzelne Attacke nutzt verschiedene Kombinationen von Verschleierungsmethoden, die explizit dazu konzipiert sind, die Microsoft-Dienste Exchange Online Protection (EOP) und Advanced Threat Protection (ATP) zu überlisten.

Einige weitverbreitete E-Mail-Bedrohungen können E-Mail-Security-Filter äußerst erfolgreich umgehen. Ein Beispiel für einen solchen Angriff ist eine ausgeklügelte kleinvolumige Phishingmail, die Office 365 oder Gmail imitiert und gezielt eingesetzt wird. Sie ist gut gestaltet, personalisiert und wird nicht wie üblich im Rahmen einer groß angelegten Kampagne verschickt, sondern an eine kleine Gruppe von Nutzern versendet. Diese Angriffe sind sehr ausgeklügelt – sowohl was die Benutzererfahrung im Back-End betrifft als auch ihre Fähigkeit, sich einen Weg in das Postfach zu verschaffen. Jeder Link enthält in der Regel die E-Mail-Adresse des Nutzers, so dass die Anmeldeseite wie die zweite Seite einer Authentifizierung mit dem Challenge-Response Verfahren aussieht, ähnlich wie bei einer Anmeldung wenn Sie versuchen auf eine Verwaltungsseite zu gelangen. Sie weiß, wer Sie sind, und führt im Hintergrund Analysen aus.

Das Innovative an dieser Phishingmail ist, dass der eigentliche Angriff erst erfolgt, nachdem die E-Mail in das Postfach gelangt. Mit anderen Worten: Anstatt die schädliche URL in der E-Mail zu platzieren, fügen die Phisher einen Link zu einem Redirect-Server (Umleitungsserver) ein, der als Gateway fungiert und Anfragen von einem Sicherheitsunternehmen an eine harmlose Website sendet. Dagegen werden Anfragen der Opfer an den Phishing-Server weitergeleitet.

Obwohl Microsoft ATP im Wesentlichen vier Policy-Engines für Anti-Phishing, Spoof-Intelligence, sichere Links und sichere Anhänge anwendet, handelt es sich immer noch um eine regelbasierte Sicherheitstechnologie. Der Sicherheitsscan nutzt ausschließlich statische reputationsbasierte Filter, die Hacker so lange durch Reverse Engineering zurückentwickeln können, bis sie Wege zur Umgehung dieser Filter finden. Aufgrund dieser Schwachstelle in der Sicherheitsschicht sind Unternehmen einem ständigen Risiko ausgesetzt, etwa wenn ein Mitarbeiter die falsche Datei öffnet, auf eine schädliche URL klickt oder ein Passwort an der falschen Stelle eingibt.

Die Gruppe von Cloud-E-Mail-Benutzern ist heute sehr groß und sichtbar, was sie zu einfachen Zielen für jeden Hacker macht. Nie zuvor gab es so viele Benutzerkonten und Postfächer mit identischer Sicherheit. Ein weiterer Vorteil für Hacker: Über diese Cloud-Konten können sie sich auch für andere unternehmenseigene SaaS-Apps authentifizieren, um Malware zu verbreiten oder Daten zu stehlen. Das ist die echte und akute Gefahr der Cloud-Security-Monokultur – wenn ein Sicherheitsmechanismus umgangen wird, können alle umgangen werden.

SiteCloak ist ein gutes Beispiel für eine solche Technik. Aktuell kommt diese zum Einsatz, um die Funktion „sichere Links" in Microsoft 365 ATP – auch bekannt als Click-Time-Schutz – zu umgehen. Durch verschiedene Taktiken und Techniken, um die echte Absicht der Zielseite zu verbergen (dies ist oft eine Credential-Harvesting-Seite), setzt SiteCloak neue Maßstäbe bei der Phishing-Verschleierung.

Opfer von SiteCloak müssen ihre E-Mail-Adresse nicht eingeben. Sie werden direkt zur Passworteingabe geleitet, wo die Credential-Harvesting-Seite die Zero-Font-Technik einsetzt, um die E-Mail-Scanner von Microsoft auszutricksen. Hierbei werden beliebige Zeichen der Schriftgröße null zwischen die Zeichen auf der Seite eingefügt, sodass die Natural-Language-Filter von Microsoft den Zufallstext sehen, während menschliche Leser nur das sehen, was die Angreifer möchten. Mit anderen Worten: Die Funktion „sichere Links" hält die Seite für harmlos, während es sich in Wahrheit um eine authentisch wirkende Credential-Harvesting-Seite handelt. Die Angreifer aktivieren den schädlichen Content erst, nachdem die E-Mail im Postfach gelandet ist.

Fazit

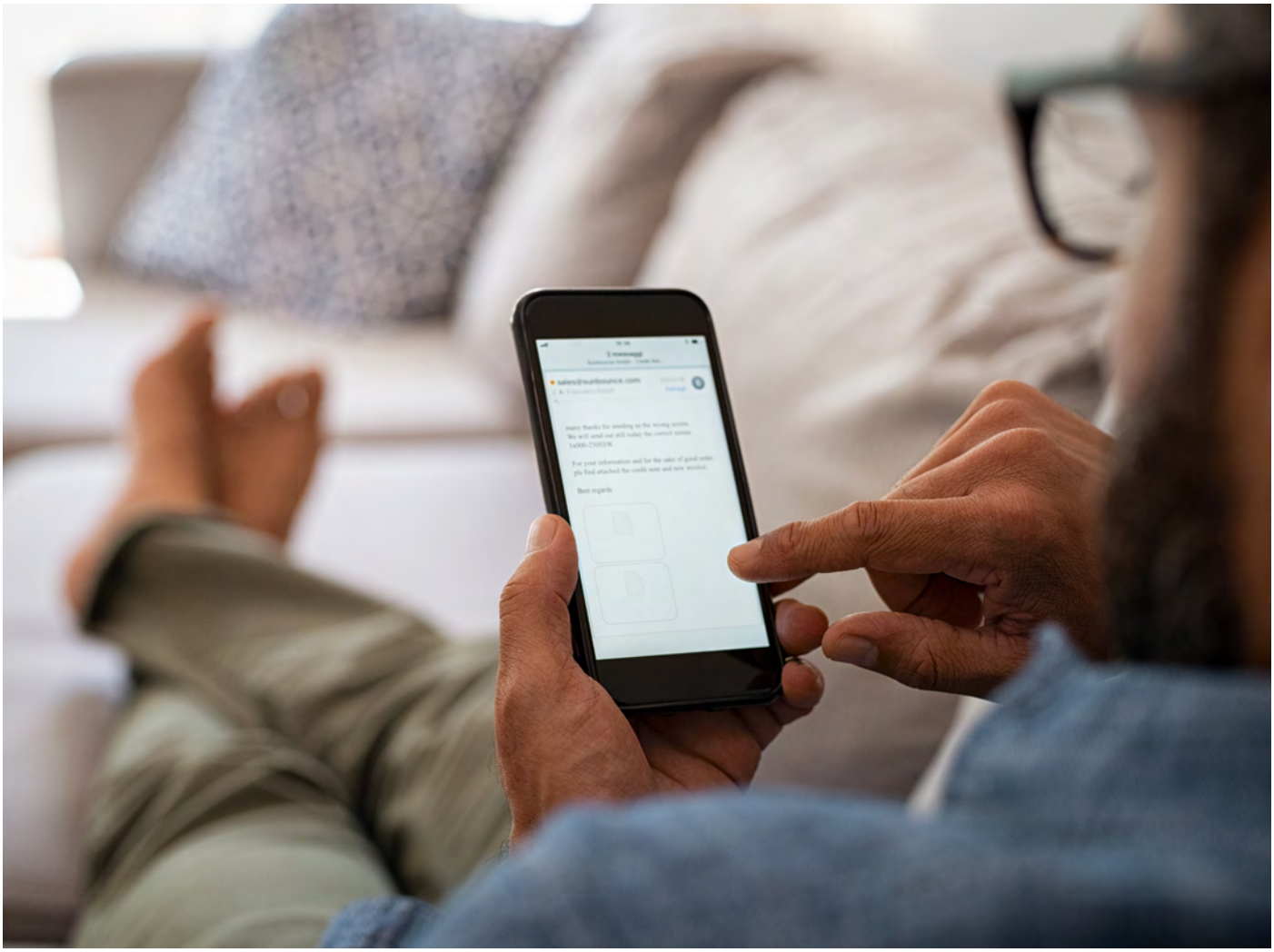
SiteCloak und andere Formen betrügerischer E-Mails sind ein gutes Beispiel dafür, dass Hacker mithilfe gut konzipierter, vorbereiteter und personalisierter Phishing-Angriffe ihre Aktivitäten verbergen können. Das werden nicht die letzten Angriffe sein, die unbemerkt durch die Sicherheitsfilter von Cloud-Anbietern schlüpfen. Diese Beispiele machen klar: Unternehmen benötigen zusätzliche Schutzschichten, die über die integrierte Sicherheit von Cloud-Office-Systemen hinausgehen.

SonicWall Email Security lässt sich als robuste virtuelle Appliance, Softwareanwendung, gehosteter Service oder gehärtete physische Appliance implementieren – ideal für Organisationen, die eine dedizierte lokale Lösung benötigen. Die mehrschichtige Lösung von SonicWall bietet umfassenden Schutz vor ausgeklügelten ein- und ausgehenden E-Mail-Bedrohungen wie Ransomware, Zero-Day-Bedrohungen, Spear-Phishing und Business-E-Mail-Compromise (BEC).

Weitere Informationen finden Sie auf www.sonicwall.com/email-security.

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.



SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

© 2021 SonicWall Inc. ALLE RECHTE VORBEHALTEN.

SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber. Die Informationen in diesem Dokument werden in Verbindung mit den Produkten von SonicWall Inc. und/oder deren Tochtergesellschaften bereitgestellt. Sie erhalten durch dieses Dokument oder in Verbindung mit dem Verkauf von SonicWall-Produkten keine Lizenz (weder ausdrücklich noch stillschweigend, durch Rechtsverwirkung oder anderweitig) für geistige Eigentumsrechte. SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN ÜBERNEHMEN KEINE HAFTUNG UND KEINERLEI AUSDRÜCKLICHE, STILLSCHWEIGENDE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR DEREN PRODUKTE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE NICHTVERLETZUNG VON RECHTEN DRITTER, SOWEIT SIE NICHT IN DEN BESTIMMUNGEN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT NIEDERGELEGT SIND. SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN HAFTEN NICHT FÜR IRGENDWELCHE UNMITTELBAREN, MITTELBAREN, STRAFRECHTLICHEN, SPEZIELLEN, ZUFÄLLIGEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG ODER VERLUST VON INFORMATION), DIE AUS DER VERWENDUNG ODER DER UNMÖGLICHKEIT DER VERWENDUNG DIESES DOKUMENTS ENTSTEHEN, SELBST WENN SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Gewährleistungen in Bezug auf die Genauigkeit oder Vollständigkeit dieses Dokuments und behalten sich das Recht vor, Spezifikationen und Produktbeschreibungen jederzeit ohne Vorankündigung zu ändern. SonicWall Inc. und/oder deren Tochtergesellschaften übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

ExecBrief-EmailThreatVector-A4-COG-5264