proofpoint.

WHITEPAPER

Vertrauen in Transaktions-E-Mails

Empfohlene Vorgehensweisen für den Schutz des Anwendervertrauens und das Unterbrechen der Angriffskette

Einführung

Die meisten Unternehmen haben Lösungen implementiert, um die von ihren Anwendern versendeten und empfangenen E-Mails abzusichern. Doch für jede E-Mail, die von einer Person geschrieben wird, werden mindestens sechs E-Mails – sogenannte Transaktions-E-Mails – von Systemen generiert. Das sind Kennwortrücksetzungen, Empfangsbestätigungen, einmalige Passcodes, Lieferstatusmeldungen, Erinnerungen usw.

Erst Transaktions-E-Mails machen den modernen Geschäftsbetrieb möglich. Sie tragen den digitalen Stempel Ihrer vertrauenswürdigen E-Mail-Domain und werden von den meisten Empfängern nicht infrage gestellt.

Leider werden diese E-Mails größtenteils ungesichert versendet, da sie sich – aus nachvollziehbaren technischen und geschäftlichen Gründen – außerhalb Ihrer geschützten E-Mail-Infrastruktur befinden. Sie sind also in Gefahr, von Cyberkriminellen kompromittiert zu werden, die Ihre Domain – und das Vertrauen Ihrer Anwender – auszunutzen versuchen.

Was sind Transaktions-E-Mails?

Transaktions-E-Mails sind automatisierte Nachrichten, die im Rahmen eines Geschäftsprozesses an Kunden gesendet werden. Dazu gehören:

- E-Mails zur Kennwortrücksetzung
- Bestellbestätigungen
- Digitale Kaufbelege
- Follow-up-E-Mails
- Einmalige Zugangscodes

Diese E-Mail-Typen werden meist durch Anwenderaktionen ausgelöst, für jeden Empfänger individuell generiert und in bestehenden Geschäftsbeziehungen zwischen Kunden und Anbietern verwendet. Diese E-Mail-Kategorie umfasst keine E-Mails, die individuell an einen bestimmten Empfänger oder, wie etwa Marketing-Kampagnen, an eine große Adressliste gesendet werden.

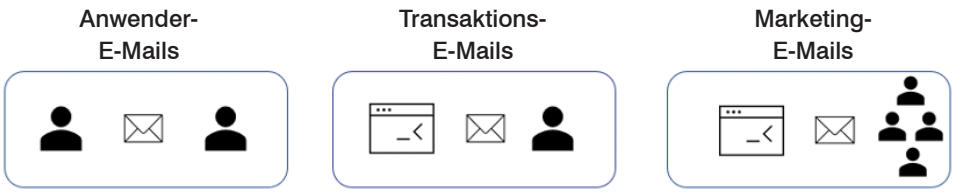

Abb. 1: Unterschiedliche E-Mail-Typen.

Schlagzeilen nach Kompromittierungen von E-Mail-Relays

- **Mailchimp says it was hacked—again** (Mailchimp erneut gehackt) (*TechCrunch,* Januar 2023)
- **HMRC phishing scam abuses mail service to bypass spam filters** (HMRC-Phishing-Betrug missbraucht E-Mail-Dienst zum Umgehen von Spam-Filtern) (*BleepingComputer,* Dezember 2020)
- **Sendgrid Under Siege from Hacked Accounts** (Sendgrid durch gehackte Konten angegriffen) (*KrebsOnSecurity,* August 2020)
- **Rackspace security vulnerability leaves customers open to cyberattack: SMTP Multipass** (Sicherheitslücke bei Rackspace ermöglicht Cyberangriffe auf Kunden: SMTP Multipass) (*Hacking,* Juli 2020)

Ein gutes Beispiel ist der E-Mail-Automatisierungsdienst Mailchimp. Von April 2022 bis Januar 2023 verzeichnete das Unternehmen drei Social-Engineering-Angriffe, wobei die Angreifer Anmeldedaten von Mitarbeitern missbrauchten, um Zugriff auf den internen Support sowie Kontoadministratortools zu erlangen. Durch die Kompromittierung hatten sie Zugang zu den E-Mail-Domains von Mailchimp-Kunden, was ihnen die Möglichkeit gab, die Personen in den E-Mail-Marketinglisten dieser Unternehmen ins Visier zu nehmen.

Einige der kompromittierten Konten gehörten Mailchimp-Kunden mit hunderttausenden – oder sogar mehreren Millionen – E-Mail-Adressen in der Datenbank. Einer der betroffenen Kunden war WooCommerce, ein häufig genutztes E-Commerce-Plugin für WordPress mit 5 Millionen Kunden.[1] Ein anderer war FanDuel, eine beliebte Glücksspiel-Website.[2]

Gründe für Angriffe auf Transaktions-E-Mails

Es ist leicht nachvollziehbar, warum Angreifer Transaktions- und andere anwendungsgenerierte E-Mails attackieren:

- Damit erhalten sie Zugriff auf Infrastrukturen, die für den Massenversand von E-Mails konzipiert wurden.
- Kompromittierte Konten können schädliche E-Mails über eine vertrauenswürdige Domain versenden, die alle grundlegenden Sicherheitstests bestehen. Selbst sicherheitsbewusste Empfänger können davon getäuscht werden.
- Diese Kanäle werden für routinemäßige Geschäftsprozesse genutzt und existieren außerhalb der geschützten E-Mail-Umgebung, was das Umgehen normaler Sicherheitskontrollen ermöglicht.

Warum sind Transaktions-E-Mails oft ungeschützt?

Wenn Transaktions-E-Mails ein so attraktives Ziel darstellen, warum bemühen sich so wenige Unternehmen um ihre Absicherung?

Erstens werden diese E-Mail-Kanäle häufig außerhalb der geschützten E-Mail-Umgebung des Unternehmens implementiert, meist aus nachvollziehbaren technischen und geschäftlichen Gründen.

Die meisten Transaktions-E-Mails kommen von einer dieser drei Quellen:

- Interne, lokale Anwendungen
- Interne, in der Cloud gehostete Anwendungen
- Externe SaaS-Partner (Software-as-a-Service), die im Namen Ihrer Domain E-Mails versenden

Unternehmen, die immer noch lokale E-Mail-Relays für Transaktions-E-Mails nutzen, vermeiden dadurch die Vermischung mit E-Mails, die von ihren Anwendern versendet werden, da Transaktions-E-Mails in großen Mengen auftreten können. Doch wenn alles durch das gleiche Relay gesendet wird, kann das die Leistung für alle senken. Schwerwiegender ist jedoch, dass Anwendungen ihre Transaktions-Nachrichten in großen und plötzlichen Aktivitätsspitzen versenden – was fälschlicherweise als Spam eingestuft werden kann. Das Blocklisting einer IP-Adresse, die gleichermaßen für Anwender- und Transaktions-E-Mails genutzt wird, würde sämtliche ausgehenden E-Mails blockieren und damit bei den meisten Unternehmen den Geschäftsbetrieb zum Erliegen bringen.

Viele Legacy-Anwendungen wurden lokal bereitgestellt. Immer häufiger migrieren Unternehmen jedoch zu Web-Anwendungen und Cloud-Hostern mit PaaS-Plattformen (Platform-as-a-Service) wie Microsoft Azure. Auch in diesem Fall empfiehlt sich die Trennung von Anwender- und Transaktions-E-Mails aus vielen der oben genannten Gründe.

Immer mehr Transaktionsnachrichten werden im Namen eines Unternehmens gesendet und stammen von externen SaaS-Anwendungen wie Salesforce, ServiceNow oder Workday. Wenn Sie externe SaaS-Anwendungen nutzen, die in Ihrem SPF-Eintrag (Sender Policy Framework) für die gemeinsame Nutzung vorgesehene Versand-IP-Adressen verwenden, entstehen weitere Risiken für Ihre Marke. Das Geschäftsmodell der SaaS-Anbieter konzentriert sich meist auf die zuverlässige Zustellung von E-Mails – und nicht auf ihren Schutz.

1 Zack Whittaker (*TechCrunch*): „Mailchimp says it was hacked — again." (Mailchimp erneut gehackt), Januar 2023.
2 Lawrence Abrams (*Bleeping Computer*): „FanDuel warns of data breach after customer info stolen in vendor hack." (FanDuel warnt vor Datenschutzverletzung, nachdem Kundeninformationen bei Hacking-Angriff gestohlen wurden), Januar 2023.

Gleicher Schutz: Ein dreistufiger Plan zur Absicherung von Transaktions-E-Mails

Bei der Einrichtung der richtigen Umgebung zum Versenden und Verwalten von Transaktions-E-Mails muss Sicherheit einen hohen Stellenwert haben. Dies sind einige wichtige Faktoren und Empfehlungen, die Sie bei der Konzeption und Pflege Ihrer Transaktions-E-Mail-Umgebung berücksichtigen sollten:

Schritt 1: Zentrale Transparenz und Kontrolle

Die Absicherung von Transaktions-E-Mails beginnt mit zentraler Transparenz und Kontrolle für interne Anwendungen sowie alle Drittanbieter, die Nachrichten in Ihrem Namen versenden. Die Quellen sollten genehmigt sowie validiert werden, wofür wir die Verwendung einer sicheren Verbindung (z. B. SMTP-Authentifizierung) zwischen den Quellen und Ihrer Versandumgebung empfehlen.

Durch die Verwendung einer stark begrenzten Anzahl von Versand-IP-Adressen in Ihrem SPF-Eintrag minimieren Sie das Risiko, dass jemand Ihre Domain fälschen kann. Der Versand von Datenverkehr über dedizierte IP-Adressen grenzt dieses Risiko sogar noch weiter ein.

Schritt 2: Scannen von Nachrichten vor dem Versand

Jede aus Ihrer Domain versendete Nachricht wirft ein Licht auf Ihr Unternehmen. Damit niemand Kunden oder Geschäftspartner in Ihrem Namen ausnutzen kann, sind Scans von Nachrichten auf Spam oder Malware unabdingbar. Besser noch ist die Verwendung von DLP-Regeln (zum Schutz vor Datenverlust) oder Verschlüsselung. Das gilt vor allem in dann, wenn Sie Finanzdaten, Patienteninformationen oder andere personenbezogene Daten verarbeiten.

Damit demonstrieren Sie, dass Sicherheit und Datenschutz für Sie einen hohen Stellenwert haben, und bauen Vertrauen bei Kunden und Partnern auf.

Schritt 3: Signieren von Nachrichten mit DKIM (Domain Keys Identified Mail)

Eine der wichtigsten Maßnahmen, um die Sicherheit und Authentizität aller ausgehenden E-Mails mit Ihrer Domain sicherzustellen, ist das Signieren mit dem DKIM-Protokoll (Domain Keys Identified Mail). Damit verhindern Sie nicht nur Spoofing, Phishing und Spam, sondern verbessern zusätzlich Ihre Versender-Reputation und Zustellbarkeit.

Wenn Ihre externen SaaS-Partner kein DKIM bieten, sollten Sie eine Umgebung beschaffen oder aufbauen, in der Nachrichten vor dem Versand eine DKIM-Signatur erhalten. DMARC (Domain-Based Message Authentication, Reporting and Conformance), das auf SPF und DKIM aufbaut, ist für den Schutz von Marken mittlerweile unverzichtbar.

Vorteile von Proofpoint Secure Email Relay

Proofpoint Secure Email Relay schafft eine separate und gleichermaßen geschützte Versandumgebung für Transaktions-E-Mails. Die Lösung bietet vielen Teams vielfältige Vorteile, zum Beispiel:

Messaging-Teams

Mit Proofpoint Secure Email Relay können Messaging-Teams sicherstellen, dass Nachrichten zuverlässig zugestellt werden, ohne sich über externe kompromittierende Faktoren Gedanken machen zu müssen.

Sie haben die Sicherheit, dass der Anwendungs-datenverkehr die Reputation Ihrer Versand-IP-Adressen nicht beeinträchtigen wird, da Probleme mit einer Anwendung sich nicht auf Anwender- oder Marketing-E-Mails auswirken. Ihre Markenreputation ist von Problemen der Drittanbieter losgelöst, die E-Mails über ihre Domain senden.

Proofpoint Secure Email Relay verbessert nicht nur die Zustellbarkeit, sondern schützt auch die Reputation Ihrer Domain und Marke.

Sicherheitsteams

Für Sicherheitsteams minimiert Proofpoint Secure Email Relay die Risiken durch einen zu großzügigen SPF-Eintrag. (Zu viele IP-Adressen in Ihrem SPF-Datensatz können Spoofing- und Phishing-Angriffe auf Ihre Domain ermöglichen.)

Sicherheitsteams können mithilfe zentraler Kontrollen in Ihrem Auftrag (Drittanbieter-)Anwendungen deaktivieren, wenn Zweifel daran auftreten. Das ist besonders für externe SaaS-Anbieter wichtig, die gemeinsam genutzte IP-Adressen verwenden und daher anfällig sind.

Mit Proofpoint Secure Email Relay können Sie sicherstellen, dass nur legitime und vertrauenswürdige Versender Ihren Domain-Namen nutzen können, und damit Ihre Domain und die Anwender schützen.

Infrastrukturteams

Als Cloud-basierter Service macht Proofpoint Secure Email Relay eine lokale Infrastruktur überflüssig und vereinfacht den E-Mail-Zustellungsprozess. Sie können sicher sein, dass Ihre E-Mails die Kunden zuverlässig und sicher erreichen.

Gleichzeitig können dadurch Entwickler in Ihrem Unternehmen Transaktions-E-Mails aus ihren Anwendungen versenden. Entwicklern stehen so standardisierte Methoden für die Absicherung von Transaktions-E-Mails zur Verfügung, sodass die Nutzung nicht genehmigter und potenziell unsicherer Tools verringert wird.

Nächste Schritte: Weitere Informationen

Proofpoint ist ein Branchenführer im E-Mail-Sicherheits-bereich. Wir verfügen über die Ressourcen, Technologien und Expertise, die Sie zur Trennung und Absicherung Ihrer Transaktions-E-Mails benötigen. Die Einrichtung eines solchen Prozesses ist schneller und kostengünstiger, als Sie vielleicht denken. Mit Proofpoint Secure Email Relay sind Sie im Handumdrehen einsatzbereit.

Weitere Informationen dazu, wie Sie mit Proofpoint Secure Email Relay Ihre Transaktions-E-Mails absichern können, finden Sie hier: **https://www.proofpoint.com/de/products/email-security-and-protection/secure-email-relay**

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.