proofpoint.

Proofpoint Secure Email Relay

Eine bessere Lösung zur Kontrolle und Absicherung von Transaktions-E-Mails von Anwendungen und SaaS-Partnern

Wichtige Vorteile

- Schutz für Transaktions-E-Mails von internen Anwendungen und externen SaaS-Anbietern (z. B. Salesforce, ServiceNow, Workday)
- Schnellere DMARC-Implementierung durch DKIM-Signaturen für E-Mails aus allen Quellen noch vor dem Versand
- Schutz Ihrer vertrauenswürdigen Domain vor Missbrauch durch kompromittierte externe Versender und anfällige E-Mail-Service-Anbieter, deren IP-Adressen in Ihren SPF-Datensätzen registriert sind
- Schutz vertraulicher Informationen (wie personenbezogene und Gesundheitsdaten) in App-E-Mails durch Inhaltsverschlüsselung und DLP
- Sichere Cloud-basierte Alternative für lokale Relays
- Isolierung von App-E-Mails, um Unterbrechungen bei E-Mails von Anwendern zu vermeiden

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.

Proofpoint Secure Email Relay (SER) konsolidiert und schützt Transaktions-E-Mails und verhindert, dass kompromittierte externe Versender schädliche E-Mails von Ihrer Domain senden können. Durch Signieren Ihrer E-Mails per DKIM können Sie DMARC-Compliance erzielen. Da Proofpoint SER als gehostete Lösung bereitgestellt wird, unterstützt sie Ihre Migration in die Cloud.

Anwendungen wechseln von lokalen Systemen in die Cloud. Durch diese Migration wächst die Angriffsfläche Ihres Unternehmens, da in Ihrem Namen versendete E-Mails von externen Versendern und Anwendungen stammen können, über die Sie keine Kontrolle haben. Dies macht E-Mail-Identitäten für Spoofing anfällig, wobei Angreifer ohne geeignete Kontrollen auf Ihrer Seite ganz einfach die Identität Ihres Unternehmens übernehmen können. Indem Cyberkriminelle die Cloud-Umgebungen autorisierter Versender missbrauchen, sind sie in der Lage, schädliche E-Mails von Adressen zu versenden, die von Ihnen autorisiert wurden. Diese Nachrichten können sogar SPF-, DKIM- und DMARC-Prüfungen bestehen und werden daher ungehindert an Ihre Kunden, Partner und Mitarbeiter weitergeleitet.

Mit Proofpoint SER erhalten Sie Sicherheits- und Compliance-Kontrollen für Transaktions-E-Mails, die Ihre Identität verwenden. Diese E-Mails stammen von internen Anwendungen oder externen SaaS-Partnern (z. B. Salesforce, ServiceNow und Workday) und können Rechnungen, Authentifizierungscodes, Bestätigungen und ähnliche Inhalte haben. Proofpoint SER trennt diese E-Mails von Anwender-E-Mails, bietet jedoch den gleichen Schutz.

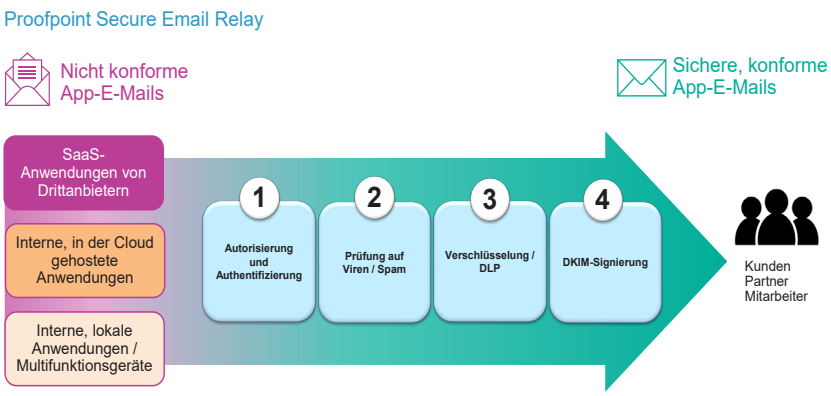

Abb. 1: Gewährleistung sicherer, sauberer und konformer Transaktions-E-Mails

Weitere Beispiele für transaktionsbezogene E-Mails:

- Statusberichte
- Benachrichtigungen für Paketlieferungen
- Bestellbestätigungen
- Elektronische Kaufbelege
- Automatisch generierte Versicherungsangebote
- Bitten um Erfahrungsberichte oder Feedback
- Aufgabenbenachrichtigungen
- IoT- oder Gerätealarm-Benachrichtigungen
- Verwaltung von Warnmeldungen/Zwischenfällen

Proofpoint SER vereinfacht DMARC, indem alle E-Mails per DKIM signiert werden. E-Mails werden mit Spam- und Virenschutz-Technologien geprüft. Zudem werden Risiken durch vertrauliche Daten dank Inhaltsverschlüsselung und E-Mail-DLP minimiert. Mit Proofpoint SER haben Sie die Kontrolle über Ihre E-Mail-Identität. Sie können gewährleisten, dass Ihre Kunden, Partner und Mitarbeiter nur authentische E-Mails von Ihrer Domain erhalten.

Sichere E-Mails von anfälligen Umgebungen

Anbieter von App-E-Mails und E-Mail-Services sind möglicherweise autorisiert, E-Mails mit Ihrer Domain zu versenden, halten aber häufig nicht die Best Practices für Sicherheit ein, was zu Kontenkompromittierung und zum Missbrauch Ihrer Plattform führen kann. In beiden Fällen können kriminelle Akteure mit Ihren vertrauenswürdigen Domains schädliche E-Mails versenden, die Authentifizierungsprüfungen bestehen.

Proofpoint SER setzt auf ein geschlossenes System, bei dem nur verifizierte Geschäftsentitäten Ihren E-Mail-Weiterleitungsdienst nutzen können – Einzelpersonen können keine kostenlosen Konten auf unserer Plattform registrieren. Das senkt das Risiko anfälliger oder kompromittierter E-Mail-Dienstleister enorm.

Proofpoint SER verwendet außerdem SMTP-Authentifizierung und TLS (STARTTLS), um E-Mails auf sichere Weise von autorisierten Anwendungen zu akzeptieren. Dabei wird jede Nachricht von Proofpoint auf Spam und Viren geprüft.

Proofpoint SER blockiert alle in Ihrem Namen versendeten E-Mails, die als autorisiert, aber schädlich eingestuft werden. Sie können auch App-E-Mails konsolidieren, die vertrauenswürdige, namhafte IP-Adressen verwenden und möglicherweise Versender verschleiern, die E-Mails in Ihrem Namen von böswilligen Akteuren senden.

Beschleunigte DMARC-Implementierung

Manche Anwendungs- oder SaaS-Anbieter unterstützen keine DKIM-Signaturen. Wenn Sie Single-Pass-DMARC festlegen und dabei ausschließlich auf SPF setzen, fehlt Ihren legitimen E-Mails ohne DKIM jedoch die erforderliche Redundanz bei der Authentifizierung, sodass zum Beispiel sichere Weiterleitungen schwierig sind. Mit Proofpoint SER erzielen diese Transaktions-E-Mails jedoch vollständige DMARC-Compliance, da sie vor dem Versand per DKIM signiert werden. Auf diese Weise können Sie die DMARC „Reject"-Richtlinie schneller umsetzen – und böswillige Akteure können Ihre Domain nicht mehr per Spoofing missbrauchen.

Einhaltung gesetzlicher Vorschriften für App-E-Mails

Anwendungen wechseln in die Cloud und Unternehmen stehen in diesem Fall aus Compliance-Sicht vor suboptimalen E-Mail-Optionen. Einige leiten ihre App-E-Mails über lokale Systeme, was zu Risiken durch externe Umgebungen führt. Andere fügen Cloud-basierte Einzellösungen zusammen, bei denen jedoch ein konsolidierter Überblick über Aktivitäten fehlt.

Mit Proofpoint SER können Sie für Ihre App-E-Mails gesetzliche Compliance-Vorgaben einhalten. E-Mails aus Anwendungen mit Zugriff auf personenbezogene Daten und personenbezogene Gesundheitsdaten können per Transport- und Inhaltsverschlüsselung geschützt werden. Proofpoint SER bietet zudem die Möglichkeit, Ihre App-E-Mails mit Lösungen für Datenverlustprävention (DLP) und Archivierung zu schützen, damit Sie die Vorgaben von SEC/FINRA einhalten.

Proofpoint bietet optional Unterstützung für Anwendungsverantwortliche, Services zur Planung und Umsetzung von Migrationen sowie zur Gewährleistung der Zustellbarkeit nach der Implementierung von Proofpoint Secure Email Relay.

MEHR ERFAHREN

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

0102-012-04-05 5/24

proofpoint.