Proofpoint Email Fraud Defense

WICHTIGE VORTEILE

- Einfachere DMARC-Implementierung, da Sie durch jeden Schritt geführt werden
- Schutz Ihrer Marke bei E-Mail-Betrugsversuchen, ohne legitime E-Mails zu blockieren
- Automatische Identifizierung Ihrer Lieferanten und der mit ihnen verbundenen Risiken
- Überblick über Doppelgänger-Domänen und E-Mails, die über Ihre vertrauenswürdigen Domänen verschickt werden
- Integration mit branchenführendem Proofpoint-Gateway, um DMARC zuverlässig und flexibel durchzusetzen

Proofpoint Email Fraud Defense vereinfacht die DMARC-Implementierung mit einem geführten Workflow und wird von spezialisierten Experten begleitet und unterstützt. Die Lösung schützt den Ruf Ihres Unternehmens vor Schäden durch E-Mail-Betrugsversuche und bietet volle Transparenz über Doppelgänger-Domänen und alle E-Mails, die über Ihre Domänen verschickt werden – auch von externen Versendern. Email Fraud Defense hilft zudem bei der Verringerung von Risiken durch Lieferanten, indem Ihre Lieferanten und von Dritten registrierte Doppelgänger-Domänen automatisch identifiziert werden.

Der seit 2016 entstandene Schaden durch E-Mail-Betrugsversuche für Unternehmen jeder Größe und in allen Branchen beläuft sich auf mehr als 26 Milliarden US-Dollar. Die Angreifer verwenden dabei eine Reihe an Taktiken zur Identitätstäuschung (z. B. Domänen-Spoofing und Doppelgänger-Domänen), um die Opfer dazu zu bewegen, betrügerische Banküberweisungen zu tätigen. Unter den verschiedenen Arten von E-Mail-Angriffen verursacht der Betrug mit Lieferantenrechnungen zudem oft die größten finanziellen Schäden, da große B2B-Zahlungen im Spiel sind.

E-Mail-Authentifizierung bietet zwar Schutz vor Impostor-Bedrohungen, doch die Implementierung von DMARC (Domain-based Message Authentication, Reporting & Conformance) kann zu einem langwierigen und komplexen Prozess werden, bei dem auch die Gefahr besteht, dass der legitime E-Mail-Verkehr unterbrochen wird.

Email Fraud Defense vereinfacht diesen Prozess, da Sie von Anfang bis Ende durch die Bereitstellung geführt werden. Wir authentifizieren alle zugestellten und von Ihrem Unternehmen versendeten E-Mails, ohne legitime E-Mails zu blockieren. Auf diese Weise schützen wir Ihre Marke vor E-Mail-Betrugsversuchen und verringern das Risiko für eingehende Impostor-Bedrohungen. Mit Email Fraud Defense können Sie Ihre Kunden, Geschäftspartner und sogar Ihre Mitarbeiter vor Betrugsversuchen mit Business Email Compromise (BEC) schützen – und so das Vertrauen in Ihre E-Mails wiederherstellen.

Anwenderfreundlichkeit

Spezialisierte Consultants und geführter Workflow

Als Email Fraud Defense-Kunde erhalten Sie eine branchenführende Lösung mit erstklassigem Support. Gleich am ersten Tag erstellen wir für Sie ein Projekt mit geführtem Workflow. Unsere Berater, die stets mit hervorragenden Net Promoter Scores (NPS)[1] bewertet werden, unterstützen Sie in jeder Phase des Rollouts.

Wir arbeiten mit Ihnen zusammen, um alle E-Mail-Versender zu identifizieren, die legitim unter Verwendung Ihrer Domänen E-Mails versenden (dazu zählen auch externe Dienstleister), sodass diese alle ausgehenden E-Mails zuverlässig authentifizieren. Unsere Consultants geben Empfehlungen für die Priorisierung von Aufgaben. Dazu analysieren sie Ihre individuelle E-Mail-Umgebung, um Ihren Bedarf, Kriterien wie E-Mail-Aufkommen und die häufigsten Versender festzustellen. Mit unserer bewährten Implementierung lässt sich vollständige E-Mail-Authentifizierung erreichen, ohne dass negative Konsequenzen zu befürchten sind. Zudem können Sie so den Wert Ihrer Investition in Proofpoint schneller erkennen.

1 NPS ist eine weltweit genutzte Kennzahl zur Messung von Kundenzufriedenheit und Kundentreue. Laut globalen Benchmark-Daten beträgt der NPS-Durchschnittswert +32. Proofpoint Email Fraud Defense-Berater erzielen einen NPS von +90.

Hosted SPF

Email Fraud Defense umfasst den Hosted SPF-Dienst, mit dem Sie das bestehende DNS-Lookup-Limit von 10 Suchvorgängen umgehen und den Mehraufwand für Änderungen am SPF-Datensatz minimieren können. Die standardmäßige Verzögerungszeit für die globale Verbreitung beträgt 72 Stunden. Hosted SPF aktualisiert die Datensätze dagegen in Echtzeit. Der Dienst sorgt außerdem für bessere Sicherheit, indem er Angreifer daran hindert, Ihre Domäne über Ihren öffentlich einsehbaren SPF-Datensatz zu missbrauchen.

Umfassender Markenschutz

E-Mail-Spoofing und Doppelgänger-Domänen sind häufig genutzte Taktiken bei BEC-Angriffen (Business Email Compromise, auch als Chefmasche bezeichnet). Die Angreifer missbrauchen dabei den Markennamen eines Unternehmens, um die Opfer zur Herausgabe von Geld oder vertraulichen Informationen zu bewegen. Email Fraud Defense verhindert, dass betrügerische E-Mails über Ihre vertrauenswürdigen Domänen verschickt werden, und schützt Ihre Marke und den Ruf Ihres Unternehmens auf diese Weise vor Schäden durch E-Mail-Betrugsversuche.

Identifizierung von Doppelgänger-Domänen

Über Informationen aus Proofpoint Domain Discover identifiziert Email Fraud Defense automatisch Doppelgänger Ihrer Domäne. Wir erkennen dynamisch neu registrierte Domänen, die bei E-Mail-Betrugsversuchen oder auf Phishing-Websites Ihre Marke imitieren. Wir analysieren Millionen Domänen, verknüpfen die Registrierungsdaten mit unseren eigenen Daten zu E-Mail-Aktivitäten und aktiven Angriffen und bieten so einen vollständigen Überblick über verdächtige Domänen. Wir zeigen zudem, wie Angreifer Ihre Marke imitieren. Sobald verdächtige Domänen von einem geparkten Status aus aktiv oder „scharf geschaltet“ werden, erhalten Sie sofort eine Warnmeldung.

Mit dem Virtual Takedown-Add-on können Sie schnell die Anfälligkeit von Verbrauchern, Geschäftspartnern und Mitarbeitern durch schädliche Doppelgänger-Domänen verringern und das Entfernen der Domäne beim Registrar oder Hosting-Anbieter beantragen. Außerdem können Sie Domänen exportieren, die vom Proofpoint-E-Mail-Gateway blockiert werden sollen.

Vollständiger Überblick über Ihr gesamtes E-Mail-Ökosystem

Dank Email Fraud Defense erhalten Sie einen einzigartigen Überblick über alle E-Mails, die über Ihre vertrauenswürdigen Domänen verschickt werden. Dazu gehören auch E-Mails, die für Verbraucher-Postfächer, Business-Gateways und Ihr eigenes Gateway bestimmt sind. Keine anderen Sicherheitstools oder öffentlichen Datenquellen können diesen Überblick bieten.

Unser Dashboard liefert umfassende Informationen:

- Welche Ihrer Domänen haben Angreifer versucht zu kapern
- Die Missbrauchsrate jeder Domain
- Ihre DMARC-, SPF- und DKIM-Passrate und Richtlinien
- Autorisierte Absender und deren DMARC-Einträge

Im Gegensatz zu anderen Lösungen, die nur Zahlen auf einem Dashboard anzeigen, bietet Email Fraud Defense verwertbare Erkenntnisse und Empfehlungen, damit Sie offene Aufgaben besser verfolgen, verwalten und geeignete Maßnahmen ergreifen können. So müssen Sie sich keine Sorgen um ein fehlerhaftes DMARC oder blockierte legitime E-Mails machen, während Sie Angreifer vom Spoofing Ihrer Domänen abhalten.

Transparenz über Risiken durch Lieferanten

Email Fraud Defense bietet zusätzlich zur DMARC-Implementierung auch Transparenz über die Risiken durch Ihre Lieferanten. Die Nexus Supplier Risk Explorer-Funktion identifiziert automatisch Lieferanten, validiert deren DMARC-Datensätze und macht die damit verbundenen Risiken für Ihr Unternehmen, z. B. Impostor-Bedrohungen, Phishing, Malware und Spam, sichtbar. Sie erhalten einen Überblick über das gesamte Nachrichtenaufkommen und über Nachrichten, die über die Doppelgänger-Domänen Ihrer Lieferanten verschickt wurden, und können außerdem jede potenzielle Bedrohung näher untersuchen. Dank der Priorisierung der Risikostufen jeder Domäne eines Lieferanten sorgen wir dafür, dass Sie sich auf die wichtigsten Zwischenfälle konzentrieren können.

Enge Integration mit dem Proofpoint-E-Mail-Gateway

Wir sind der einzige Sicherheitsanbieter, der E-Mail-Authentifizierung und ein sicheres E-Mail-Gateway miteinander verknüpft. Wenn Sie Email Fraud Defense zusammen mit dem branchenführenden Proofpoint-E-Mail-Gateway einsetzen, können Sie durch die zuverlässige und flexible Durchsetzung von DMARC für Ihren eingehenden Datenverkehr Risiken durch Impostor-Angriffe verringern. Wir helfen Ihnen, die Reputation der DMARC-Adresse einer bestimmten Domäne zu verifizieren, sodass Ihr Gateway keine legitimen E-Mails blockiert, die aus irgendwelchen Gründen die DMARC-Prüfung nicht bestehen. Wir unterstützen Sie außerdem beim Erstellen von Außerkraftsetzungsrichtlinien für legitime E-Mails, ohne dabei Ihre Sicherheit zu beeinträchtigen. Dadurch sind Ihre Mitarbeiter besser vor E-Mail-Betrug geschützt.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de/products/email-fraud-defense**.