Proofpoint Email Fraud Defense

Wichtige Vorteile

- Einfache DMARC-Implementierung, da Sie durch jeden Schritt geführt werden
- Schutz Ihrer Marke vor E-Mail-Betrugsversuchen, ohne legitime E-Mails zu blockieren
- Automatische Identifizierung Ihrer Lieferanten und der mit ihnen verbundenen Risiken
- Übersicht über E-Mails, die über vertrauenswürdige und Doppelgänger-Domains gesendet wurden
- Zuverlässiges Hosting von SPF-, DKIM- und DMARC-Datensätzen dank Proofpoint-gehosteter Authentifizierungsdienste
- Integration mit branchenführendem Proofpoint-E-Mail-Gateway, um DMARC zuverlässig und flexibel durchzusetzen
- Anzeige von DMARC-Passraten für unternehmenseigene Domains, die über Microsoft 365 verwaltet werden

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

Proofpoint Email Fraud Defense vereinfacht die DMARC-Implementierung mit geführten Workflows und wird von erfahrenen Experten begleitet und unterstützt. Unser Produkt schützt den Ruf Ihres Unternehmens vor Schäden durch E-Mail-Betrugsversuche, indem es Ihnen einen Überblick über die unternehmenseigenen und Doppelgänger-Domains bietet, über die E-Mails versendet werden. Zudem werden Ihre Lieferanten und deren Doppelgänger-Domains identifiziert, sodass Lieferantenrisiken effektiv minimiert werden können.

Proofpoint Email Fraud Defense führt Sie durch den gesamten DMARC-Bereitstellungsprozess, damit Sie Ihre Kunden, Geschäftspartner und Mitarbeiter vor Betrugsversuchen mit Business Email Compromise (BEC) schützen können. Proofpoint Email Fraud Defense verhindert, dass Ihre Marke für E-Mail-Betrugsversuche verwendet wird, und minimiert das Risiko von Impostor-Bedrohungen durch eingehende E-Mails. Wir authentifizieren alle zugestellten und von Ihrem Unternehmen versendeten E-Mails – ohne legitime E-Mails zu blockieren.

Anwenderfreundlichkeit

Spezialisierte Berater und Unterstützung durch Experten

Bei der Einrichtung der E-Mail-Authentifizierung unterstützt Sie Proofpoint mit der Erstellung eines Projektplans mit geführten Workflows, die den Einrichtungsprozess vereinfachen. Unsere Berater unterstützen Sie in jeder Phase der Implementierung. Wir arbeiten mit Ihnen zusammen, um alle E-Mail-Versender zu identifizieren, die legitim unter Verwendung Ihrer Domains E-Mails versenden (dazu zählen auch externe Dienstleister und Schatten-IT), sodass diese alle ausgehenden E-Mails zuverlässig authentifizieren. Wir analysieren zudem Ihre individuelle E-Mail-Umgebung, um Ihren Bedarf sowie Kriterien wie E-Mail-Aufkommen und die häufigsten Versender festzustellen und Sie bei der Priorisierung von Aufgaben zu unterstützen.

Gehostete Authentifizierungsdienste

Proofpoint Email Fraud Defense umfasst Proofpoint-Services für gehostetes SPF, gehostetes DKIM und gehostetes DMARC, die Sie bei der Einrichtung und Verwaltung von Richtlinien für die Standards Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) und DMARC unterstützen. Zudem bieten die geographisch verteilten und fehlertoleranten Services hohe Zuverlässigkeit.

Gehostetes SPF

- Umgehung der SPF-Beschränkung auf 10 DNS-Abfragen
- Reduzierung des Aufwands für Änderungen am SPF-Datensatz
- Aktualisierung der Datensätze in Echtzeit, mit ordnungsgemäßer Syntaxprüfung
- Verbesserte SPF-Sicherheit dank Verschleierung der Versandinfrastruktur
- Vereinfachte Verwaltung mehrerer Domains, die dieselbe Versandinfrastruktur verwenden

Gehostetes DKIM

- Vereinfachte Konfiguration und Verwaltung der DKIM-Selektoren und -Schlüssel
- Flexible Hosting-Optionen für DKIM-Selektoren (delegiert oder nicht delegiert)
- Unterstützt DNS Security Extensions (DNSSEC)
- Einfacher Import von DKIM-Selektoren und öffentlichen Schlüsseln

Gehostetes DMARC

- Vereinfachte Konfiguration und Verwaltung der DMARC-Datensätze für Ihre Domains
- Unterstützt DNSSEC
- Einfacher Import vorhandener DMARC-Datensätze

Umfassender Markenschutz

Um Ihre Marke zu schützen, verhindert Proofpoint Email Fraud Defense, dass betrügerische E-Mails über Ihre vertrauenswürdigen Domains verschickt werden.

Identifizierung von Doppelgänger-Domains

Proofpoint Email Fraud Defense verwendet die Domain-Registrierungsdaten aus Proofpoint Domain Discover und erkennt Domains, die Ihre Marke in E-Mail-Betrugsversuchen oder auf Phishing-Websites imitieren. Proofpoint analysiert Millionen Domains und verknüpft die Registrierungsdaten mit unseren eigenen Daten zu E-Mail-Aktivitäten und aktiven Angriffen. So können wir Ihnen verdächtige Domains aufzeigen und Sie darüber informieren, wie sich Angreifer Ihrer Marke bedienen. Zudem warnt die Lösung Sie, sobald verdächtige Domains aktiv werden.

Mit dem Proofpoint Takedown-Add-on reduzieren Sie das Risiko für Ihre Kunden, Partner und Mitarbeiter durch Doppelgänger-Domains. Zusätzlich haben Sie die Möglichkeit, die Entfernung von schädlichen Domains beim Registrar oder dem zuständigen Content Delivery Network (CDN)- bzw. E-Mail-Anbieter zu beantragen. Außerdem können Sie Domains exportieren, die vom Proofpoint-E-Mail-Gateway blockiert werden sollen.

Vollständiger Überblick über Ihr gesamtes E-Mail-Ökosystem

Dank Proofpoint Email Fraud Defense sehen Sie alle E-Mails, die über Ihre vertrauenswürdigen Domains verschickt werden. Dazu gehören auch E-Mails, die für Verbraucher-Postfächer, Business-Gateways und Ihr eigenes Gateway bestimmt sind.

Im Dashboard finden Sie eine Übersicht der Domains, für die Angriffe registriert wurden, sowie Angaben zur Missbrauchsquote für jede Domain. Darüber hinaus finden Sie dort die autorisierten Absender und deren DMARC-Datensätze sowie Ihre Richtlinien und Passraten für SPF, DKIM und DMARC.

Proofpoint Email Fraud Defense bietet verwertbare Erkenntnisse und Empfehlungen, damit Sie sich keine Sorgen um fehlgeschlagene DMARC-Prüfungen oder blockierte legitime E-Mails machen müssen und gleichzeitig Angreifer stoppen.

Transparenz über Risiken durch Lieferanten

Proofpoint Email Fraud Defense hilft Ihnen nicht nur bei der DMARC-Einrichtung, sondern gibt Ihnen zudem einen Überblick über Ihre Lieferantenrisiken. Proofpoint Nexus Supplier Risk Explorer identifiziert Ihre Lieferanten, überprüft deren DMARC-Datensätze und zeigt die damit verbundenen Risiken auf. Die Lösung zeigt Ihnen, welche Nachrichten über Doppelgänger-Domains versendet wurden. Dank der risikobasierten Priorisierung der Warnmeldungen können Sie sich auf die wichtigsten Vorfälle konzentrieren.

Integration mit Proofpoint-E-Mail-Gateway

Zusammen mit dem Proofpoint E-Mail-Gateway sorgt Proofpoint Email Fraud Defense für eine zuverlässige Durchsetzung der DMARC-Authentifizierung eingehender Nachrichten. Die Lösung unterstützt Sie bei der Überprüfung der Reputation der DMARC-Adresse einer Domain, um zu verhindern, dass Ihr Gateway legitime E-Mails blockiert. Außerdem unterstützt sie Sie beim Erstellen von Außerkraftsetzungsrichtlinien für legitime E-Mails, ohne dabei Ihre Sicherheit zu beeinträchtigen.

DMARC-Transparenz für Microsoft 365

Proofpoint Email Fraud Defense kann die DMARC-Konformität Ihrer Domains auch dann anzeigen, wenn Sie Microsoft 365 verwenden und Ihre MX-Datensätze (Mail eXchange) auf die Posteingangsserver von Microsoft verweisen. Diese Transparenz hilft Ihnen bei der Durchsetzung einer zuverlässigen DMARC-Authentifizierung für eingehende Nachrichten, die über Ihre Domains versendet werden.

MEHR ERFAHREN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 85 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.