Proofpoint Impersonation Protection

Schutz für Ihre Kommunikation mit vertrauenswürdigen Partnern, Kunden und Lieferanten

Wichtige Vorteile

- Schutz Ihrer vertraulichen Unternehmenskommunikation vor Nachahmerbedrohungen
- Verhinderung des Missbrauchs Ihrer Identität und Marke durch Nachahmer
- Erkennung von und Schutz vor riskanten Lieferanten, einschließlich kompromittierten Lieferantenkonten
- Absicherung von Anwender- und App-E-Mails, damit diese vertraulich bleiben

Die Geschäftsabläufe der meisten Unternehmen sind auf E-Mails angewiesen. Angreifer haben jedoch Wege gefunden, wie sie Ihre vertrauliche Unternehmenskommunikation missbrauchen und Ihre Identität, Ihre Marke oder die Ihrer Geschäftspartner nachahmen können. Laut dem FBI haben Nachahmerangriffe wie Business Email Compromise (BEC) bereits Schäden in Höhe von mehr als 2,7 Milliarden US-Dollar verursacht. Dabei entstanden bei Datenschutzverletzungen durch kompromittierte Lieferanten pro Vorfall Kosten von fast 5 Millionen US-Dollar.[1]

Taktiken wie gefälschte Domains, Doppelgänger-Domains und kompromittierte Lieferantenkonten werden bei Nachahmerangriffen häufig kombiniert und Sie müssen Ihre Kommunikation mit vertrauenswürdigen Partnern, Kunden und Lieferanten davor schützen. Mit Proofpoint können Sie die Risiken durch diese Bedrohungen verringern, indem Ihre Anwender- und App-E-Mails authentifiziert werden, sodass sie vertrauenswürdig bleiben.

Proofpoint nutzt einen mehrschichtigen Ansatz, um Sie und Ihre Marke vor Missbrauch durch Nachahmer zu schützen. Wir identifizieren Lieferanten, die ein Risiko darstellen und erkennen potenziell kompromittierte Lieferantenkonten sowie Doppelgänger-Domains Ihrer Lieferanten. Außerdem sichern wir Ihre Anwender- und App-E-Mails ab, damit diese vertrauenswürdig bleiben.

Schutz für Sie und Ihre Marke vor Missbrauch durch Nachahmer

Zu den häufigsten Nachahmertaktiken gehört das Domain-Spoofing. Ohne geeignete Kontrollen können Angreifer dabei ganz einfach Ihre vertrauenswürdigen Domains übernehmen und Angriffe gegen Ihre Kunden, Ihre Partner und sogar Ihre Mitarbeiter starten. E-Mail-Authentifizierung bietet hier den besten Schutz. Proofpoint Impersonation Protection implementiert dazu DMARC, damit Ihre Anwender- und App-E-Mails authentifiziert werden können. Um die Umsetzung zu vereinfachen, führen wir Sie beim Rollout durch jeden Schritt. Unsere Experten helfen Ihnen, alle Ihre legitimen Versender zu erkennen, und stellen zudem sicher, dass alle Ihre E-Mails – einschließlich E-Mails von autorisierten externen Dienstleistern – zuverlässig authentifiziert werden.

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

1 IBM: *Cost of a Data Breach Report* (Kosten von Datenkompromittierungen), 2023.

Durch die Integration mit Proofpoint Threat Protection können Sie die DMARC-Authentifizierung für eingehende Nachrichten zuverlässig durchsetzen, sodass Sie zusätzlich vor eingehenden Bedrohungen geschützt werden, die Ihre vertrauenswürdigen Domains missbrauchen. Außerdem können Sie DMARC-Richtlinien außer Kraft setzen, ohne legitime E-Mails zu blockieren oder durch Safelists die Sicherheit zu gefährden. Diese Integration bietet Ihnen einen vollständigen Überblick über ein- und ausgehende E-Mails sowie über alle E-Mails, die Ihre vertrauenswürdige Domain verwenden. Dazu zählen auch Nachrichten von externen Versendern.

Proofpoint Impersonation Protection hilft Ihnen, riskante Lieferanten zu erkennen, und nutzt KI-gestützte Verhaltensanalysen, Machine Learning sowie Bedrohungsdaten aus unserer großen Kundenbasis, um potenziell kompromittierte Lieferantenkonten proaktiv zu identifizieren. Dabei kommen auch adaptive Kontrollen zum Einsatz, bei denen zum Beispiel URLs von kompromittierten Lieferantenkonten automatisch isoliert werden, um Ihr Risiko zu minimieren. Die Integration mit Proofpoint Threat Protection und der Kontext zur Absender-/Empfänger-Beziehung vereinfachen die Reaktion auf Zwischenfälle mit Lieferanten sowie entsprechende Untersuchungen.

Schutz vor kompromittierten Lieferantenkonten

Angreifer missbrauchen die Supply Chain heute als Bedrohungsvektor, indem sie mit kompromittierten Lieferantenkonten die E-Mail-Kommunikation zwischen Ihnen und Ihren Geschäftspartnern kapern. E-Mails von kompromittierten Lieferanten enthalten dabei nicht unbedingt Schaddaten und bestehen zudem die Authentifizierung, was die Erkennung erheblich erschwert. Wenn diese Angriffe erfolgreich sind, können sie jedoch zu hohen finanziellen Verlusten, Datenerpressung oder einer Ransomware-Infektion führen.

Aufdeckung schädlicher Doppelgänger-Domains

Zum Täuschen von E-Mail-Empfängern setzen Bedrohungsakteure auch gern auf Doppelgänger-Domain-Spoofing. Bei dieser Taktik registrieren die Angreifer Domain-Namen, die einer legitimen Marke oder Entität sehr ähnlich sind, und nutzen diese gefälschten Domains bei Angriffen wie Anmeldedaten-Phishing, BEC und auch TOAD (Telephone-Oriented Attack Delivery, Angriff per Telefon).

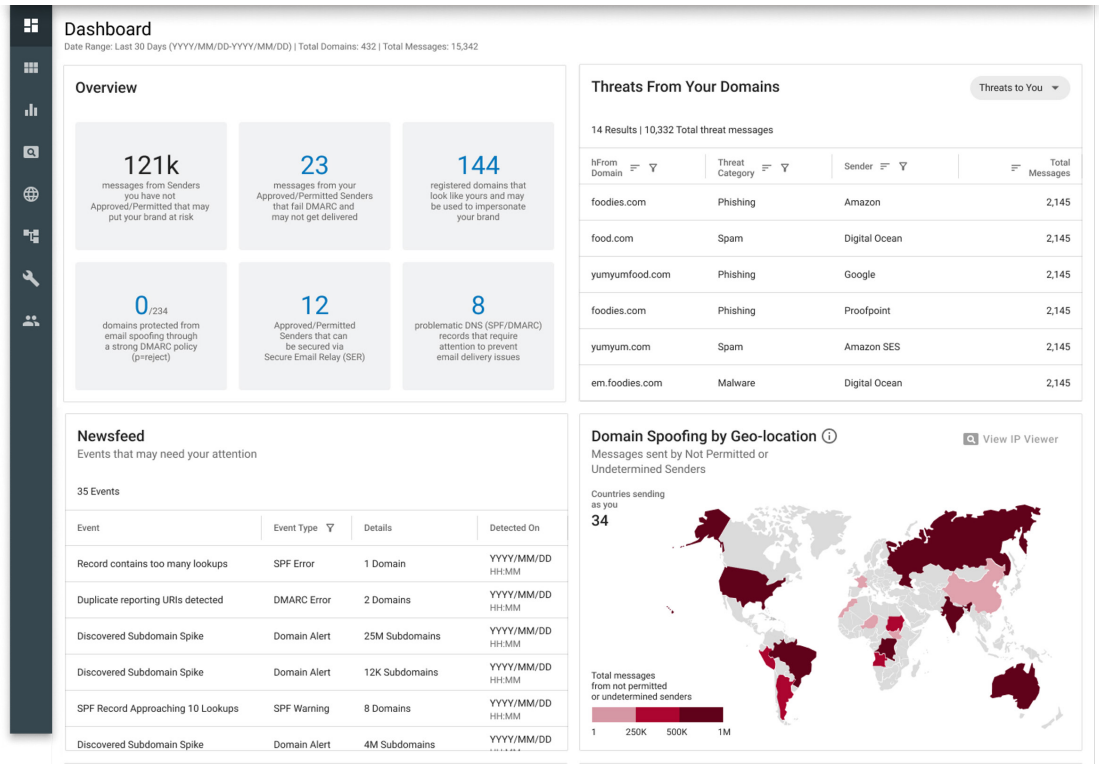

Abb. 1: Proofpoint bietet Ihnen einen Überblick über Domain-Spoofing-Bedrohungen, über schädliche Doppelgänger Ihrer Domains und über E-Mails, die von Ihren vertrauenswürdigen Domains versendet werden.

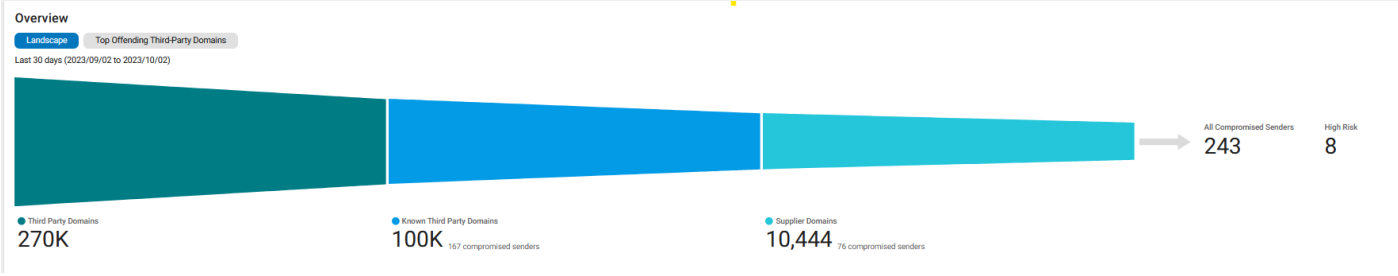

Abb. 2: Proofpoint erkennt potenziell kompromittierte Drittanbieter-Konten, mit denen Sie geschäftlich interagieren, und bietet Ihnen einen Überblick über besonders riskante Lieferanten.

Proofpoint hilft Ihnen, gefährliche Doppelgänger Ihrer vertrauenswürdigen Domains zu finden, und erkennt dynamisch neu registrierte Domains, die bei E-Mail-Betrugsversuchen oder auf Phishing-Websites Ihre Marke imitieren. Wir geben Ihnen einen vollständigen Überblick über verdächtige Domains und helfen Ihnen, gefährliche Doppelgänger der Domains Ihrer Lieferanten zu finden. Sie erhalten einen Überblick über das gesamte Nachrichtenaufkommen und über Nachrichten, die von den Doppelgänger-Domains Ihrer Lieferanten verschickt wurden, damit Sie Probleme mit hochriskanten Lieferanten proaktiv beheben können.

Absicherung von App-E-Mails, die in Ihrem Namen versendet werden

E-Mails, die in Ihrem Namen versendet werden, können von externen Versendern und Anwendungen stammen, sodass Sie keine Kontrolle darüber haben. Eventuell senden Sie per Workday gehaltsbezogene E-Mails an Ihre Mitarbeiter, oder Sie verschicken über Salesforce Newsletter an Ihre Kunden. Falls dabei keine Kontrollmaßnahmen angewendet werden, können diese App-E-Mails Ihre vertrauenswürdigen Domains gefährden. Wenn eine Drittanbieter-App oder ein SaaS-Partner kompromittiert wurde, können Angreifer bei Transaktions-E-Mails, die scheinbar von Ihnen stammen, Malware injizieren. Diese manipulierten Transaktions-E-Mails würden sogar die E-Mail-Authentifizierung bestehen.

Proofpoint Impersonation Protection bietet Schutz für die von Ihnen selbst und in Ihrem Namen versendeten App-E-Mails, indem wir auf Transaktions-E-Mails, die Ihre vertrauenswürdigen Domains verwenden, zuverlässige Sicherheits- und Compliance-Kontrollen anwenden. Wir authentifizieren diese E-Mails und identifizieren mithilfe unserer branchenführenden Bedrohungserkennungstechnologien Malware und andere Bedrohungen. Auf diese Weise wird gewährleistet, dass Ihre Kunden, Partner und Mitarbeiter nur authentische und ungefährliche App-E-Mails von Ihnen erhalten. Außerdem können Sie die Transaktions-E-Mails von Drittanbieter-Apps und SaaS-Partnern zentral kontrollieren und schädlichen App-E-Mail-Datenverkehr, der über die Domains kompromittierter Geschäftspartner gesendet wird, jederzeit stoppen.

WEITERE INFORMATIONEN

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