Data Sheet

mimecast

Mimecast DMARC Analyzer

Gewinnen Sie die Kontrolle über Ihre Domain und setzen Sie Spoofing-Angriffen mit E-Mail-Kanalanalyse und DMARC-Berichten ein Ende

Identitätsmissbrauchs- und Spoofing-Angriffe sind für die meisten Unternehmen ein großes Problem und nehmen viel schneller zu als normale Malware-Angriffe, da Cyberkriminelle menschliche Schwächen ausnutzen.

Angreifer haben es auf Ihr eigenes Unternehmen und Ihre Mitarbeiter, Kunden und Lieferanten abgesehen, wodurch die Gefahr einer Schädigung Ihrer Marke wächst. Es ist nicht einfach, diese Angriffe zu stoppen, die oft ohne Schadsoftware ablaufen, und um dabei möglichst effektiv zu sein, sollten mehrere Schutzebenen kombiniert werden.

Der Mimecast DMARC Analyzer hilft Ihnen, Ihre Marke zu schützen, indem er Ihnen die notwendigen Werkzeuge zur Verfügung stellt, um Spoofing und Missbrauch Ihrer eigenen Domains zu stoppen. Die zeit- und ressourcenschonende Self-Service Lösung bietet die erforderlichen Analytics-Tools und Berichte, um volle Transparenz über Ihre E-Mail-Kanäle zu gewinnen und somit erfolgreich DMARC-konform zu werden.

Vorteile:

- Effektivere Abwehr von Identitätsmissbrauch, Phishing- und Malware-Angriffe durch die Kombination von Transparenz und Reporting mit DMARC-Richtlinien und Targeted Threat Protection für Ihre Domains.
- Schnellere Umsetzung von DMARC-Richtlinien durch Self-Service-Tools und benutzerfreundliche Diagramme und Berichte.
- Schützen Sie Ihr eigenes Unternehmen, sowie Ihre Marke, Kunden, Partner und Lieferanten.
- 100% SaaS Lösung für schnellen Einsatz und Kosteneffizienz.

Wieso DMARC

Der Einsatz von DMARC (Domain-based Message Authentication, Reporting and Conformance) zur Unterbindung von Domain Spoofing schützt vor Markenmissbrauch und Betrug, der Ihren Ruf schädigen und zu direkten Verlusten für Ihr Unternehmen, Ihre Kunden und Partner führen kann. Eine effektive DMARC-Implementierung ermöglicht es Ihnen, die Kontrolle über Ihre eigenen Domains zu erlangen und besser zu bestimmen, wer im Namen Ihres Unternehmens E-Mails versenden darf und wer nicht.

Allerdings kann die Umsetzung ohne die richtigen Tools schwierig und zeitaufwändig sein. Bevor Sie eine DMARC-Richtlinien durchsetzen, müssen Sie unbedingt einen vollständigen Einblick in Ihre eingehenden und ausgehenden E-Mail-Kanäle gewinnen, um sicherzustellen, dass legitime E-Mails nicht abgelehnt werden. Wenn Ihr Unternehmen viele aktive und inaktive Domains hat oder Drittanbieter in Ihrem Namen E-Mails versenden, kann die Sicherstellung einer effektiven DMARC-Konfiguration eine besondere Herausforderung darstellen.

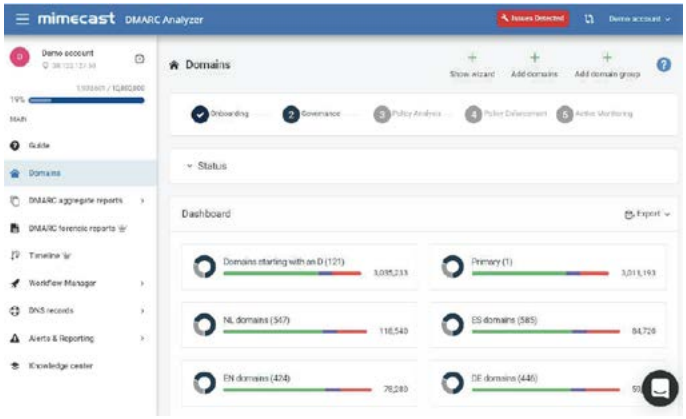

Abb. 1: Domain dashboard

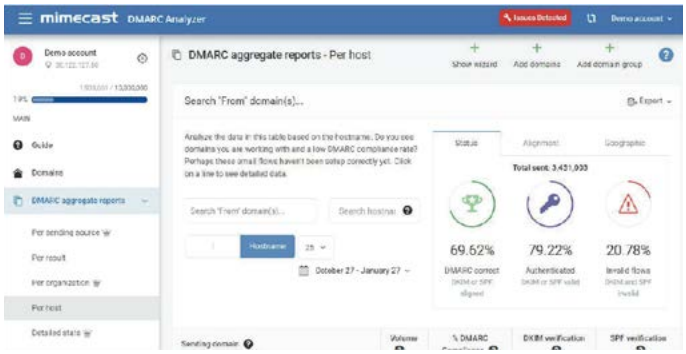

Abb. 2: Aggregierter Bericht gruppiert nach Hostname der versenden IP-Adressen

Hier hilft DMARC Analyzer weiter

- Eine einfach zu bedienende SaaS-Lösung zur Verwaltung komplexer DMARC Use-Cases.
- 360-Grad-Transparenz -und Governance über alle E-Mail Domains hinweg.
- Self-Service-E-Mail-Intelligence-Tools zur Implementierung von DMARC-Richtlinien auf dem Gateway.
- Warnmeldungen, Berichte und Diagramme, um die DMARC-Durchsetzung schneller zu erreichen und die laufende Leistung überwachen zu können.
- Ein DNS-Delegationsdienst, der Ihnen zur Verfügung steht, um Probleme bei der Begrenzung von Suchanfragen zu lösen.

Im Gegensatz zu anderen DMARC-Lösungen, die oft eine professionelle Beratung benötigen, um vollumfänglich zu funktionieren, ist der Mimecast DMARC Analyzer für eine einfache und effektive Selbstbedienung konzipiert, um den Zeitaufwand, die Mühe und die Kosten für die Abwehr von Domain-Spoofing-Angriffen zu reduzieren. Zusätzliche Dienstleistungen und Support sind bei Bedarf verfügbar.

Die Kombination ist der Schlüssel zum Erfolg

Der Schutz vor direktem Domain-Spoofing allein kann nicht alle Identitätsmissbrauchs-Angriffe verhindern. Die Kombination der Mimecast DMARC Analyzer Reporting- und E-Mail-Sicherheitslösung mit unserer Targeted Threat Protection bietet Schutz sowohl an Ihrem Perimeter als auch darüber hinaus, um Ihr Unternehmen, Ihre Beziehungen und Ihren Ruf zu schützen.

Als Teil von Targeted Threat Protection bietet Impersonation Protect einen wirksamen Schutz vor Identitätsmissbrauchs-Angriffen, indem es Kombinationen von Schlüsselindikatoren in einer E-Mail identifiziert, um festzustellen, ob der Inhalt oder der Absender verdächtig sind, selbst wenn keine bösartige URL oder Anlage vorhanden ist. Zu diesen Indikatoren gehören:

- Neu erfasste und neu registrierte Domains.
- Spoofing des Anzeigenamens und Unstimmigkeiten der Antwortadresse.
- Ähnlich aussehende Domains einschließlich der Verwendung nicht-westlicher Zeichensätze.
- Schlüsselwörter, die mit denen in unserem Threat-Wörterbuch übereinstimmen.

Zusammen bieten Mimecast E-Mail-Sicherheit und DMARC Analyzer einen umfassenden Schutz vor Identitätsmissbrauchs-Angriffen und Domain Spoofing. Mimecast schützt Ihre Mitarbeiter, Kunden, Lieferkette und das gesamte Unternehmen vor gezielten Angriffen und Markenmissbrauch.

"Impersonation Protect arbeitet mit Mimecast URL Protect, Attachment Protect und Internal Email Protect zusammen und bietet so umfassenden Schutz vor fortschrittlichen E-Mail-Bedrohungen. Data Leak Prevention (DLP) hilft, das Abfließen sensibler und persönlicher Daten zu verhindern."

Mehr erfahren

Um mehr über den Mimecast DMARC Analyzer zu erfahren, besuchen Sie mimecast.com/products/dmarc-analyzer