Solution Brief

mimecast

Email Security 3.0

Die Erweiterung Ihrer Sicherheit über die Unternehmensgrenzen hinaus

Zone 3

Gerade was Sie nicht kennen kann eine große Gefahr darstellen

Angriffe, die Ihre Marke imitieren, die Ihren guten Namen ausnutzen, um Kunden und Partner zu kompromittieren, sind verheerend. Sie zerstören das Vertrauen, sind schwierig aufzudecken und noch schwieriger abzuschalten. Und leider sind sie für Kriminelle nur allzu leicht zu kreieren. Sogar wenig erfahrene Angreifer können schnell und mühelos ähnliche Domains registrieren und Websites hosten, die darauf abzielen, ahnungslose Besucher zu täuschen und den Markenwert zu schädigen, für dessen Aufbau Sie vielleicht Jahre oder Jahrzehnte gebraucht haben.

Es ist an der Zeit, von der Verteidigung zum Angriff überzugehen. Der Schutz Ihrer Organisation vor Markenmissbrauch ist die Grundlage der E-Mail-Sicherheitsstrategie von Mimecast in Zone 3 - über Ihren Perimeter hinaus. Zu den wesentlichen Schritten gehört die Implementierung von DMARC zum Schutz Ihrer Domains, während Sie gleichzeitig proaktiv nach Angriffen suchen, die sich auf betrügerische, ähnliche Domains stützen, und diese vom Netz nehmen.

Email Security 3.0

Mimecast Email Security 3.0 hilft Ihnen dabei, sich von einer auf dem Perimeter basierenden Sicherheitsstrategie zu einer umfassenden und allgegenwärtigen Strategie zu entwickeln, die Schutz in drei Zonen bietet. Diese Schutzmaßnahmen werden durch ein breites Portfolio an ergänzenden Lösungen, umsetzbar Threat Intelligence und eine wachsende Auswahl an APIs ergänzt.

Zonen-basierte Abwehr	Erweiterungen
Zone 1 am E-Mail-Perimeter	Kontinuität & Wiederherstellung
Zone 2 innerhalb Ihres Netzweks & Unternehmens	Webbedrohungen & Schatten-IT
Zone 3 außerhalb des Perimeters	Datenschutz & Verschlüsselung
	Governance & Compliance
Ecosystem & Threat Intelligence	

Schützen Sie sich gegen Missbrauch Ihrer Marke

Wenn es um Angriffe auf Markenimitationen geht, haben Cyber-Kriminelle in der Vergangenheit immer am Steuer gesessen. Diese Angriffe finden jenseits der eigenen Grenzen statt, wo die Sichtbarkeit gering oder nicht vorhanden ist und wo Abhilfemaßnahmen schwierig und zeitaufwendig sind. Mimecast Brand Exploit Protect wurde entwickelt, um die Macht wieder in Ihre Hände zu legen.

Durch eine Kombination aus maschinellem Lernen und Billiarden von gezielten Scans, die selbst unbekannte Angriffsmuster erkennen können, hilft Ihnen Brand Exploit Protect, Angriffe in ihrem frühen Stadium zu erkennen und zu blockieren, bevor sie live gehen. Wenn Live-Angriffe entdeckt werden, können diese schnell behoben werden, um Schaden zu minimieren. Die Lösung wurde entwickelt, um Sie beifolgenden Szenarien zu unterstützen:

- Schützen Sie Kunden, Partner und Mitarbeiter vor Phishing-Betrügereien, die ähnliche Domains verwenden.
- Identifizieren Sie Angriffe, die Ihre Website klonen, unabhängig von der Hosting-Domäne.
- Blockieren und beseitigen Sie sowohl verdächtige Websites als auch aktive Betrügereien.

Ein Beispiel aus der Praxis

Eine Universität in Australien wurde von Angreifern betrogen, die eine gefälschte Website einrichteten, Phishing-E-Mails an Studenten verschickten und beim Einloggen unerlaubt Zugangsdaten sammelten. Die Universität selbst hat diesen Vorfall nie bemerkt. Obwohl die Universität nicht zu den Kunden von Mimecast zählte, hat Mimecast den Angriff entdeckt und die Situation aufgedeckt. Die Universität entschied sich zunächst dafür, die Sache selbst in die Hand zu nehmen; einige Tage später war die Website jedoch immer noch aktiv. Sie wandten sich an Mimecast und baten um Hilfe und die gefälschte Website wurde in kurzer Zeit vom Netz genommen. Und als einige Wochen später eine weitere gefälschte Website online war, entdeckte Mimecast diese, noch bevor jemand anders auf den Betrug hereinfiel.

Schützen Sie Ihr größtes Kapital

Wechseln Sie von Verteidigung auf Angriff mit einem Markenschutz, der Sie effektiv unterstützt:

- Verteidigen Sie sich gegen auf Nachahmung basierende Bedrohungen, die auf Kunden, Lieferanten und Partner abzielen.
- Erweitern Sie den Phishing-Schutz über Ihre Grenzen hinaus.
- Verhindern Sie Angriffe auf Ihre Marke.
- Beheben Sie schnell Angriffe in Echtzeit.
- Erhalten Sie Sichtbarkeit über den E-Mail-Verkehr über Ihre eigenen Domains, sowohl aktive als auch ruhende.
- Wechseln Sie schneller und sicherer zu einer DMARC-Ablehnungsrichtlinie.
- Ergreifen Sie proaktiv Maßnahmen bei verdächtigen und aktiv böswilligen Domains und URLs.

Die Integration mit den E-Mail- und Web-Sicherheitsdiensten von Mimecast stärkt diese Abwehr noch weiter, indem sie es Ihnen ermöglicht, alle potenziell bösartigen Domains und URLs in Ihrer Mimecast-Lösung mit einem Klick zu blockieren.

Verteidigung eigener Domains

Eine Schlüsselkomponente von Angriffen auf Marken ist häufig der Missbrauch von eigenen Domains. Da Organisationen meist viele aktive und ruhende Domains haben, ist es schwierig, diese zu verfolgen und zu kontrollieren. Angreifer nutzen diese Komplexität aus, um E-Mails zu versenden, die scheinbar von einer vertrauenswürdigen Quelle stammen. DMARC ist ein E-Mail-Authentifizierungsprotokoll nach Industriestandard, welches es Organisationen ermöglicht, DMARC-Einträge für alle ihre eigenen Domänen bei ihrem DNS-Provider zu veröffentlichen. Mimecast DMARC Analyzer ist ein Cloud-basiertes Tool, das zur Vereinfachung der Implementierung, Verwaltung und Berichterstattung über DMARC-Richtlinien entwickelt wurde und Ihnen dabei hilft:

- eine bessere Sichtbarkeit über die eigenen Domains – sowohl der aktiven als auch der inaktiven – zu gewinnen.
- DMARC Einträge einfacher zu veröffentlichen.
- zu sehen, wer in ihrem Namen E-Mails versendet – sowohl erlaubt als auch unerlaubt.
- DMARC Ablehnungs-Richtlinien zu implementieren, um die Zustellung von E-Mails aus unerlaubten Quellen zu verhindern.
- sicherzustellen, dass legitime E-Mails nicht durch DMARC-Richtlinien blockiert werden.

Einer der Hauptvorteile von Mimecast DMARC Analyzer ist die Möglichkeit, das Vertrauen in Ihre Domains aufrechtzuerhalten. Wenn Kunden regelmäßig gefälschte E-Mails erhalten, die eigentlich so aussehen, als ob sie von Ihrem Unternehmen verschickt wurden, ist die Wahrscheinlichkeit hoch, dass sie diese ignorieren oder misstrauisch werden. Mimecast DMARC Analyzer hilft Ihnen, die Sichtbarkeit, die Analysen und die Werkzeuge zu erhalten, die für eine einfache und sichere Anwendung der DMARC-Richtlinien erforderlich sind.

Mimecast unterstützt Sie mit einem integrierten Ansatz

Durch die Kombination von vollständiger DMARC-Sichtbarkeit, Reporting und der Möglichkeit Markenangriffe proaktiv zu verfolgen, hilft Mimecast Ihnen, sich gegen böswillige Nutzung eigener Domains sowie gegen Spoofing zu schützen, die ähnliche oder gleich aussehende Domains verwenden, um Ihre Mitarbeiter zum Klicken zu verleiten.