Was macht die Proofpoint-Lösung zur Abwehr von BEC- und EAC-Angriffen so besonders?

DIE FAKTEN

- Bis 2023 wird sich die Zahl der BEC-Angriffe jedes Jahr verdoppeln und bei Unternehmen erhebliche finanzielle Verluste in Höhe von 5 Milliarden US-Dollar verursachen.[1]
- Die Verluste durch BEC- und EAC-Betrug belaufen sich inzwischen auf weltweit 26 Milliarden US-Dollar (potenzielle und tatsächliche Verluste einberechnet).[2]
- Fast 90 % der Unternehmen haben 2019 BEC- und Spearphishing-Angriffe erlebt.[3]
- Der durchschnittliche Verlust durch einen Banküberfall beläuft sich auf 3.000 US-Dollar – bei einem erfolgreichen BEC-Angriff entsteht ein Schaden von fast 130.000 US-Dollar.[4]

E-Mail-Betrug umfasst vor allem zwei Bedrohungsformen: Während die Angreifer bei Business Email Compromise (BEC, auch als Chefmasche oder CEO-Betrug bezeichnet) lediglich Ihren Namen missbrauchen, sich also als Sie ausgeben, übernehmen sie bei Email Account Compromise (EAC) Ihr E-Mail-Konto.

BEC und EAC sind komplexe, facettenreiche Probleme, die sich nur schwer abwehren lassen. Cyberkriminelle setzen eine große Vielfalt an Taktiken und Kanälen ein, nehmen Ihre Mitarbeiter dabei aber ganz gezielt ins Visier. Zu den Taktiken und Kanälen zählen das geschäftliche E-Mail-Konto, private Webmail Accounts, aber auch Cloud-Anwendungen und sogar die Lieferkette.

Erstklassiger Schutz mit Proofpoint

Da BEC und EAC zusammenhängen, müssen Sie beide Betrugsformen mit einer gemeinsamen, umfassenden Sicherheitslösung adressieren. Wenn Sie nur BEC, aber nicht EAC berücksichtigen, ist Ihr Unternehmen weiterhin gefährdet.

Proofpoint ist der einzige Anbieter mit einer integrierten, Ende-zu-Ende-Lösung, die BEC- und EAC-Angriffe tatsächlich stoppen kann. Wir bieten den effektivsten Bedrohungsschutz und berücksichtigen alle bei diesen Angriffen eingesetzten Taktiken.

Unsere einzigartige, umfassende Lösung bietet folgende Vorteile:

- Erkennung und Blockierung von Impostor- und Phishing-E-Mails und Verhinderung des Missbrauchs Ihrer Domäne
- Detaillierte Einblicke in die menschliche Angriffsfläche, indem wir Ihnen aufzeigen, welche Anwender per Impostor- und Phishing-E-Mails angegriffen werden und wer für diese Bedrohungen anfällig ist
- Nutzung adaptiver Kontrollen für risikobehaftete Anwender, um BEC/EAC-Risiken zu minimieren
- Schulung der Anwender mit bewährten Trainings zur Steigerung des Sicherheitsbewusstseins, damit sie Täuschungen zuverlässig erkennen
- Schnellere Reaktion auf Bedrohungen und verbesserte operative Effektivität durch automatisierte Erkennung und Reaktion auf Bedrohungen, damit Sie Zeit und Geld sparen

Schnellere Abwehr von mehr Bedrohungen

Mit unserer fortschrittlichen Lösung können Sie BEC- und EAC-Angriffe effektiv abwehren. Die meisten Anbieter beschränken sich auf statische Regeln und andere Methoden, die umfangreiche manuelle Anpassungen erfordern. Das bedeutet einen großen Aufwand

1 „Protecting Against Business Email Compromise“ (Schutz vor BEC), Gartner, 2020
2 Öffentliche Service-Bekanntmachung, FBI, 2019
3 „State of the Phish-Bericht“, Proofpoint, 2019
4 US-amerikanischer Secret Service, 2019

für Ihr Team. Wir optimieren unsere Lösung zusätzlich mit Machine Learning, damit Impostor- und Phishing-E-Mails, die häufig ohne schädliche Payloads auskommen, dynamisch klassifiziert und erkannt werden. Dank mehrerer Erkennungstechniken identifizieren und blockieren wir zuverlässig E-Mail-Bedrohungen, die andere Lösungen übersehen. Dadurch bleiben Sie den sich ständig ändernden Taktiken der Angreifer stets einen Schritt voraus.
Nur wir bieten umfassende E-Mail-Sicherheit mit diesen Funktionen:

- Erkennung und Blockierung von Bedrohungen, noch bevor sie Ihr Unternehmen erreichen
- Verwertbare Einblicke in die menschliche Angriffsfläche
- Authentifizierung von E-Mails per DMARC, damit Ihre vertrauenswürdigen Domänen nicht von Betrügern missbraucht werden können
- Identifizierung verdächtiger Cloud-Aktivitäten wie fehlgeschlagene Anmeldeversuche, Brute-Force-Angriffe und kompromittierte Cloud-Konten
- Adaptive Kontrollen wie Browser-Isolierung, damit Ihre Mitarbeiter sicher auf private Webmails zugreifen können, zusätzlich Trainings zur Steigerung des Sicherheitsbewusstseins

Einzigartige Transparenz

BEC- und EAC-Angriffe zielen nicht auf Schwachstellen in Ihrer kritischen Infrastruktur, sondern auf Menschen ab. Um Ihre tatsächliche Gefährdung für diese Angriffe zu besser zu verstehen, müssen Sie über Ihre menschliche Angriffsfläche Bescheid wissen.

Für den Aufbau einer optimalen Abwehr müssen Sie Ihre Mitarbeiter genau kennen. Dazu erhalten Sie einen einzigartigen Überblick darüber, welche Anwender von Impostor- und Phishing-Angriffen ins Visier genommen werden, wer Ihre Very Attacked People (VAPs) sind und welche Mitarbeiter für Ihr Unternehmen ein Risiko darstellen. Kein anderer Anbieter bietet seinen Kunden diese personenorientierte Transparenz.

Außerdem müssen Sie über verdächtige Ereignisse in Ihrem E-Mail-Datenverkehr und in Cloud-Konten informiert werden. Wir bieten Einblicke in B2B- und B2C-E-Mail-Datenverkehr sowie in alle E-Mails, die von Ihren Domänen versendet werden. Das schließt E-Mails von vertrauenswürdigen externen Versendern ein.

Zudem liefert eine zentrale Verwaltungsoberfläche Informationen zu allen verdächtigen Cloud-Konto-Aktivitäten wie mehrfache Anmeldeversuche und andere Aktionen, die als frühe Anzeichen eines EAC-Angriffs gelten. Außerdem korrelieren wir Bedrohungsaktivitäten bei E-Mails und in der Cloud, um Verbindungen zwischen Anmeldedaten-Phishing und verdächtigen Anmeldeversuchen herzustellen. Für noch höhere Sicherheit melden wir Ihnen Registrierungen betrügerischer Doppelgänger-Domänen, damit Sie Angriffe mit gefälschter Identität proaktiv verhindern können.

Verbesserte operative Effizienz

Da Proofpoint das Durchkommen der meisten Bedrohungen verhindert, werden die operativen Kosten gesenkt. Wenn eine Bedrohung die Sicherheitsmaßnahmen überwindet, erhalten Sie den nötigen Kontext, um schnell reagieren und die Untersuchung sowie Problembehebung automatisieren zu können.

- **Verhindern von Bedrohungen:** Wir erkennen mehr Bedrohungen als unsere Mitbewerber. In einem Fall konnte ein weltweit tätiger Hersteller der Fortune 250 die Zahl der untersuchungsbedürftigen Sicherheitszwischenfälle um 81 % reduzieren – und das allein in den ersten drei Monaten ab der Einführung unserer Lösung.
- **Bereitstellen von Kontext:** Wir liefern verwertbare Einblicke zu allen Sicherheitskontrollpunkten und Bedrohungsdaten. Dadurch können Sie die bereitgestellten Informationen einfach nutzen und sparen Zeit, die Sie andernfalls für die manuelle Aufarbeitung benötigen würden. Unsere Mitbewerber bieten diese Einblicke nicht, sodass deren Kunden die eigenen Bedrohungen selbst einschätzen und die Mitarbeiter und Verteilerlisten darauf überprüfen müssen, wer zusätzlich geschützt werden muss.
- **Automatisierte Erkennung und Reaktion:** Unsere Produkte sind eng miteinander vernetzt, damit die Bedrohungserkennung und Problembehebung automatisiert werden. Zudem stellen wir Verbindungen zwischen verschiedenen Kontrollpunkten wie E-Mail, Cloud-Anwendungen und Anwendern her, um den Schutz zusätzlich zu verbessern. Die Ausbreitung von Bedrohungen lässt sich mithilfe automatisierter Reaktionen schnell eindämmen:
  - Embedded URL-Rewriting, um Anwender in eine Web-Isolierungsumgebung umzuleiten
  - Durchsetzung von E-Mail-Authentifizierung per DMARC
  - Automatische Suche und Entfernung von E-Mails mit URLs, die nach der Zustellung in den Posteingang „scharf geschaltet“ werden
  - Zurücksetzung kompromittierter Cloud-Konten

Diese enge Integration ermöglicht schnellere Reaktionen auf Bedrohungen, da weniger manuelle Schritte erforderlich sind und mehrere, punktuell ansetzende Produkte konsolidiert werden.

Erfahren Sie, wie wir Ihnen helfen können

Informieren Sie sich darüber, wie unsere integrierte, durchgängige E-Mail-Sicherheitslösung Ihre Abwehr gegen BEC- und EAC-Angriffe stärken kann. Sind Sie bereit, Ihre Optionen auszuloten? Kontaktieren Sie uns, um eine kostenlose Bewertung Ihrer aktuellen Sicherheitsumgebung zu erhalten. Wir können diese Bewertung mit nur minimaler Konfiguration umsetzen.

Registrieren Sie sich hier: proofpoint.com/de/free-trial-request

WEITERE INFORMATIONEN

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