DATASHEET

Mimecast Advanced BEC Protection

Blockieren Sie Business Email Compromise (BEC) mit einer KI-gestützten E-Mail-Sicherheitslösung, die integrierten Schutz für Ihre Kommunikation bietet.

Das Problem:

E-Mail ist essenziell für geschäftliche Abläufe, sei es beim Austausch sensibler Informationen oder bei der Abwicklung wichtiger Transaktionen. Aufgrund dieser starken Abhängigkeit wird E-Mail zum idealen Ziel für Business Email Compromise (BEC), das darauf abzielt, diese kritischen Phasen auszunutzen. Da sich BEC-Angriffe ständig weiterentwickeln, sind Werkzeuge erforderlich, die nicht auf Signaturen oder Heuristiken angewiesen sind, weshalb KI-basierte Lösungen zum Einsatz kommen. Die Herausforderung bei der Nutzung dieser Technologien liegt in der Komplexität und der großen Menge an Daten, die interpretiert werden müssen. Zudem sind ständige Anpassungen und menschliche Überwachung notwendig, um die Vielzahl an Fehlalarmen zu bewältigen, die von rein KI-gesteuerten Lösungen erzeugt werden.

Die Lösung:

Um BEC-Bedrohungen zu verhindern, benötigen Sicherheitsteams einen Ansatz, der mehrere bewährte Lösungen integriert, statt sich nur auf eine einzelne Methode zu verlassen. Diese integrierte Strategie sollte Bedrohungsfeeds, E-Mail-Authentifizierungsprotokolle und fortschrittliche, KI-gesteuerte Funktionen kombinieren, um Anomalien zu erkennen und verdächtige E-Mails zu identifizieren.

Da Angriffe ohne Payload zunehmend raffinierter werden, ist es entscheidend, dass Ihre Schutzmethoden kontinuierlich lernen und sich verbessern. Blockieren Sie fortgeschrittene Business Email Compromise-Angriffe mit KI, die auf Milliarden von Signalen basiert und darauf ausgelegt ist, sich entwickelnde Bedrohungen zu erkennen. Unsere integrierte Plattform schützt Ihre Kommunikation und gewährleistet Schutz vor jeder Art von Angriff – nicht nur BEC. Ermöglichen Sie Administratoren, Einblick in Bedrohungen zu erhalten, die auf Ihre Benutzer abzielen, und nutzen Sie umsetzbare Erkenntnisse für fundierte Entscheidungen durch intuitive Dashboards und Richtlinienmodellierung.

Verluste von 2,9 MILLIARDEN Dollar durch Business Email Compromise im Jahr 2023*

25% der finanziell motivierten Angriffe nutzen Business Email Compromise**

Der Mehrwert von Mimecast

- **Erkennen Sie Angriffe ohne Nutzlast.** Stoppen Sie fortschrittliche Business Email Compromise-Bedrohungen mit modernster KI.
- **Stärken Sie Ihre Abwehr durch integrierten Schutz.** Eine Plattform schützt Ihre Zusammenarbeit umfassend – unabhängig von der Art des Angriffs.
- **Verschaffen Sie sich Einblick in Bedrohungen, die Ihre Benutzer anvisieren.** Ermöglichen Sie Administratoren, fundierte Entscheidungen mit umsetzbaren Erkenntnissen zu treffen.

*https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
** https://www.verizon.com/business/resources/reports/dbir/

Feature	Details
Social Graph	• Analysiert die Beziehung zwischen Absender und Empfängern innerhalb der Organisation. • Bewertet die Vertrauenswürdigkeit eingehender und ausgehender Kommunikation sowie von gemeldeten Nachrichten. • Überprüft Domains von Freemail-Anbietern, neu registrierten Domains und Tippfehler-Domains bekannter Marken.
Message Analysis	• Erkennung von bedrohungsspezifischer Sprache in E-Mails, die mit bestimmten BEC-Bedrohungskategorien zusammenhängt, wie z.B. Hilfsgesuche, gefälschte Überweisungen, Dringlichkeit, Kanalwechsel in der Kommunikation sowie Betrügereien mit Geschenkkarten, Bank- und Finanztransaktionen. • Fokus auf das Verständnis des Kontextes, der Nuancen und der Implikationen der Nachricht, um die wahre Absicht genau zu interpretieren.
Betreffzeilenanalyse	• Erkennung von bedrohungsspezifischer Sprache in der Betreffzeile im Zusammenhang mit bestimmten BEC-Bedrohungskategorien. • Konzentration auf das Verständnis des Kontexts, der Nuancen und der Implikationen der Betreffzeile, um die wahre Absicht genau zu interpretieren.
Administration	• Organisierte und konsolidierte Übersicht wichtiger Informationen. • Detaillierte Erklärungen zur Bedrohungserkennung mit Beweisen und betroffenen Nutzern. • Übersicht der am häufigsten angegriffenen Nutzer, die oft BEC-Bedrohungen erhalten. • Durchsuchbarkeit von Bedrohungen zur Bestimmung von Umfang und Schwere. • Unterstützung für anpassbare BEC-Richtlinien und Maßnahmen zur Unterstützung der Risikotoleranz der Organisation.
Richtlinienmodellierung	• Die Auswirkungen einer Anpassung des Sensitivitätsniveaus bewerten. • Bearbeitete E-Mails vergleichen, um den Status der verschiedenen Sensitivitätsniveaus zu bestimmen.

Advanced BEC Protection Anwendungsfälle:

Schutz vor BEC-Bedrohungen
BEC-Bedrohungen beseitigen, indem anomale Aktivitäten identifiziert und ein soziales Netzwerk der Benutzerinteraktionen erstellt wird. Risikobehaftete Formulierungen und die semantische Absicht analysieren, um den Zweck einer E-Mail zu bestimmen.

Umfassender BEC-Schutz
Der Schutz vor BEC-Bedrohungen kann sich nicht nur auf KI verlassen, um Muster und Abweichungen zu erkennen. Er erfordert einen Ansatz, der KI mit bewährten Indikatoren aus Signaturen und Bedrohungsfeeds kombiniert. So wird sichergestellt, dass Angriffe bereits bei der Erkennung gestoppt werden und nicht ausschließlich auf KI als letzte Verteidigungslinie angewiesen sind.

Verstehen, was blockiert wird und warum
Es ist wichtig, eine BEC-Erkennung einfach überprüfen zu können. Jede Erkennung von Mimecast's Advanced BEC Protection zeigt nicht nur die Richtlinie an, die die Erkennung ausgelöst hat, sondern auch die riskanten Merkmale, die zur Entscheidung geführt haben. Dadurch verbringen Administratoren weniger Zeit damit, die Ursache zu ermitteln.

Richtlinienmodellierung leicht gemacht
Das ständige Anpassen von BEC-Richtlinien ist auf Dauer nicht tragbar. Durch die historische Analyse von Nachrichten können die Auswirkungen einer Richtlinienänderung ermittelt und die potenziellen Nachrichten identifiziert werden, die bei jedem Sensitivitätsniveau erfasst werden.