mimecast

Wie Sie Ihr Unternehmen vor Business Email Compromise (BEC)-Betrugsmaschen schützen

Die aktuelle Lage

25%
der gezielten Angriffe sind BEC.[1]

$50.000
Der durchschnittliche Schaden durch BEC Angriffe.[1]

60 Sekunden
Die Zeit, die benötigt wird, um auf einen Phishing-Angriff hereinzufallen.[2]

Das Risiko?

Kleine Unternehmen haben begrenzte Ressourcen, um gegen hochvolumige oder komplexe E-Mail-Betrügereien vorzugehen.

5 kritische Schutzschichten zur Verteidigung gegen BEC

Entdecken Sie, wie ein mehrschichtiger, KI-gestützter Ansatz vor BEC schützt.

Checkliste:

- ☑ **Prefiltering** – Blockieren Sie bekannte schadhafte E-Mails und lassen Sie bekannte sichere E-Mails an die Endnutzer durch.
- ☑ **KI-gestützt** - Die Natural Language Processing (NLP)- und Machine Learning (ML)-Funktionen analysieren den E-Mail-Inhalt und erkennen subtile Anomalien sowie verdächtige Aktivitäten.
- ☑ **Integrierte Erkennung** – Mehrere Signale und Technologien schaffen eine umfassende Sicht auf Bedrohungen, wodurch eine Blockierung bereits an der Erkennungsstelle ermöglicht wird.
- ☑ **Kontinuierliches Lernen** – Reduzieren Sie manuelle Eingriffe mit Modellen, die kontinuierlich lernen und sich verbessern.
- ☑ **Security Awareness Training** – Ermöglichen Sie es Ihren Mitarbeitern, sicherheitsbewusster zu sein und identifizieren sie risikoreichere Nutzer.

Erfahren Sie, wie Sie sich vor Business Email Compromise schützen können

1: FBI Internet Crime Report 2023 2: 2024 Data Breach Investigations Report