Cofense PhishMe™

MITARBEITER FÜR PHISHING-ANGRIFFE SENSIBILISIEREN

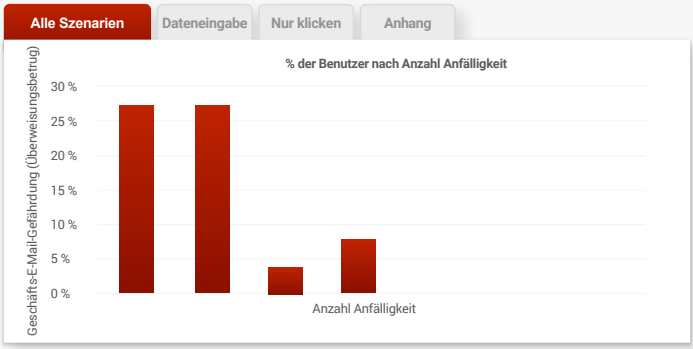
Die Forschungsabteilung von Cofense hat ermittelt, dass 2016 über 97 % aller Phishing-E-Mails Ransomware enthielten. Diese Zahlen sind beunruhigend. Doch was können Sie tun, um Ihr Unternehmen davor zu bewahren, selbst Opfer solcher E-Mails zu werden? Cofense PhishMe nutzt bewährte Methoden der Verhaltenssteuerung, damit Mitarbeiter als letzte Verteidigungslinie auf bösartige Phishing-Versuche besser vorbereitet sind und diese eher erkennen.
Damit werden Ihre Mitarbeiter, die bisher eine der größten Schwachstellen in Ihrem Unternehmen waren, zum wertvollsten Schutzmechanismus.

Warum sollten Sie sich für Cofense PhishMe™ entscheiden?

Cofense reduziert erwiesenermaßen die Gefahr, dass Mitarbeiter Opfer raffinierter Cyberangriffe werden, um bis zu 95 %. Ihre letzte Verteidigungslinie wird so ermächtigt, trickreiche Phishing-Angriffe zu erkennen und zu umgehen.

Wichtigste Vorteile

- Reduzierung der Anfälligkeit für Phishing-Angriffe im Unternehmen um mehr als 95 % durch praxisnahes Mitarbeitertraining
- Simulation aktueller Angriffstaktiken mit anpassbaren Szenarien und Trainingsvorlagen
- Einsatz vielseitiger Schulungsmethoden aus einer umfassenden Bibliothek mit Inhalten in mehreren Sprachen
- Bewertung der Effizienz des Programms und Ermittlung von Risikobereichen anhand von detaillierten Berichten

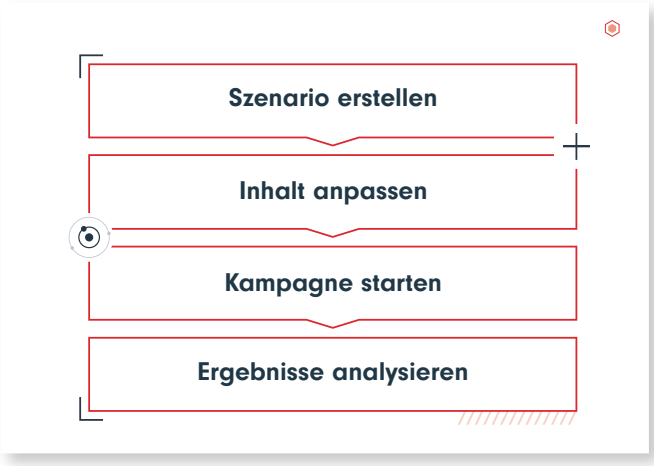


Was ist Cofense PhishMe™?

Cofense PhishMe ist eine spezielle SaaS-Trainingsplattform, mit der Ihre Mitarbeiter in realistische Spear-Phishing-Szenarien versetzt werden, damit sie besser auf Phishing-Angriffe reagieren und sofort Informationen zu verdächtigen Aktivitäten weiterleiten können. Die Lösung umfasst benutzerdefinierbare Szenarien, in denen die wichtigsten Bedrohungen simuliert werden. Dabei erhalten die Beteiligten unmittelbares Feedback und lernen, wie sie sich in diesen Situationen verhalten sollen.

Unsere patentierte Technologie umfasst eine breite Palette an verschiedenen Arten von Cyberattacken, Inhalten sowie Anpassungsmöglichkeiten und liefert detaillierte Analysen und Berichte für jedes Szenario. Mit dem erstklassigen Kunden-Support von Cofense wird sichergestellt, dass die Übungen kontrolliert ablaufen, keine Sicherheitslücken verursachen und keine anderen negativen Auswirkungen haben.

Funktionsweise



> Die verbesserten Analyseberichte von Cofense sind von unschätzbarem Wert. Mithilfe dieser Daten konnten wir unsere Phishing-Abwehrprogramme anpassen und insbesondere Mitarbeiter, die oft auf Phishing-E-Mails klicken, gezielt schulen, um sie für diese Gefahr zu sensibilisieren.
>
> **Jim Stewart, CISO, United Community Bank**

Anpassbare Inhalte und praxisorientierte Trainings

Mit Cofense PhishMe werden in einzelnen Szenarien verschiedene Angriffsmethoden simuliert. Dazu zählen neben Drive-by-Downloads, Malware- und Social Engineering-Attacken auch komplexere Taktiken, wie Conversational-Phishing und das gezielt auf einzelne Personen zugeschnittene Spear-Phishing. Darüber hinaus können Sie die Szenarien auch zur Bewertung Ihrer Fortschritte im Vergleich zu anderen Cofense-Kunden verwenden.

Sie haben die Möglichkeit, eigene Szenarien zu entwickeln oder eine der anpassbaren vordefinierten Vorlagen aus unserer umfassenden Inhaltsbibliothek zu wählen. Diese enthält zahlreiche Themen rund um das Thema Sicherheit – u. a. Phishing, das Bewusstsein für Gefahren aus dem Internet, Compliance und Social Media. Diese stehen in verschiedenen Formaten, z. B. als HTML5-Vorlagen, Videos und als Game-Modul, zum Abruf bereit. Mit Inhalten und Schulungsmaterialien in mehreren Sprachen richtet sich Cofense an die mitunter auch kulturell bedingten unterschiedlichen Anforderungen nationaler und internationaler Unternehmen.

Für Unternehmen, die eine umfassendere Schulung benötigen, bietet Cofense vollständig SCORM-kompatible Lerninhalte, die allgemeine Sicherheitsthemen abdecken. Die verfügbare Schulung deckt die folgenden Themen ab:

- **Bewusstsein für Spear-Phishing**
- **Bösartige Links**
- **Malware**
- **Passwortsicherheit**
- **Datenschutz**
- **Mobilgeräte**
- **Sicherere Internetnutzung**
- **Social Engineering**
- **Soziale Netzwerke**
- **Physische Sicherheit**
- **Arbeit außerhalb des Büros**
- **Melden von verdächtigen Aktivitäten**
- **Ransomware**
- **Business Email Compromise (BEC)**
- **Erweitertes Spear-Phishing**

Sichere Plattform

Unsere SaaS-Plattform befindet sich in einem nach Tier III SOC 2 und SOC 3 zertifizierten Rechenzentrum in den Vereinigten Staaten und einem nach ISO9001:2008 zertifizierten Rechenzentrum in Europa. Beide werden regelmäßig externen Penetrationstests unterzogen und sind mit robusten Zugriffskontrollen ausgestattet. Alle Daten werden mit Data-at-Rest-Verschlüsselung gesichert. Darüber hinaus erfasst Cofense während den Dateneingabeszenarien keine vertraulichen Kundendaten.

Detaillierte Analysen

Jedes Szenario bietet Kennzahlen für die Erfassung einer Vielzahl an Datenpunkten, die nach einer Langzeitanalyse Aufschluss über die Schwachstellen eines Unternehmens und Möglichkeiten zur kontinuierlichen Verbesserung liefern.

Mit den Reporting-Funktionen in Cofense PhishMe werden u. a. folgende Informationen erfasst:

- **Geolokation**
- **Zeitstempel**
- **Reaktionen der einzelnen Benutzer**
- **Trends**
- **Trainingsdauer**
- **Dauer bis zur Erstmeldung (Reporter erforderlich)**
- **Browser-Enumeration**
- **Widerstandskraft des Unternehmens (Reporter erforderlich)**

Maximaler Erfolg für unsere Kunden

Benutzer mit einer Cofense PhishMe-Lizenz erhalten Zugriff auf unseren erstklassigen Kunden-Support. Neben der zuverlässigen Bereitstellung von E-Mail-basierten Szenarien unterstützen die Experten in unserem Support-Team Sie bei der Implementierung von Cofense PhishMe und der Bewertung von E-Mail-Szenarien im Vergleich zu branchenspezifischen Best Practice-Standards. Ebenfalls im Serviceumfang enthalten ist die Anpassung des Programms an Unternehmenskultur, Vorgaben der Unternehmensleitung und Benutzeranforderungen. Darüber hinaus erhalten Sie Unterstützung beim Einsatz neuer Funktionen und Szenarien.

Sollten in Ihrem Unternehmen keine entsprechenden Mitarbeiter zur Verfügung stehen, können Sie Cofense PhishMe auch als teilweise oder vollständig verwaltete Lösung nutzen. Bei dieser Option werden die Kampagnen durch einen für Ihr Unternehmen zuständigen Account-Verantwortlichen erstellt, ausgeführt und analysiert. Darüber hinaus werden die Programme auf die Anforderungen und kulturellen Gegebenheiten in Ihrem Unternehmen angepasst.

COFENSE

W: cofense.com/contact **T:** 703.652.0717
A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175

Weitere Informationen finden Sie unter **www.cofense.com.**