

PhishER PLUS

PhishER Plus ist Phishing-Abwehr der nächsten Dimension

Wesentliche Vorteile

- Automatische Priorisierung von nicht bedrohlichen E-Mails über den Phish Alert Button von KnowBe4
- Übersicht im IR-Posteingang – schnelle und effiziente Reaktion auf tatsächliche Bedrohungen
- Freimachen von IR-Ressourcen, Zeit und Kapazitäten zur Überprüfung von Spam-E-Mails und legitimen Anfragen (90 % der Nachrichten), da weniger E-Mails bei Ihrem SOC-Team (Security Operations Center) eingehen
- Blockieren von E-Mail-Bedrohungen, die alle anderen E-Mail-Sicherheitsfilter oder Sicherheitssysteme umgangen haben, bevor diese in den Posteingängen Ihrer Nutzer und Nutzerinnen landen
- Isolieren von schädlichen E-Mails, die es bereits durch Ihre E-Mail-Filter geschafft haben – durch die automatische Quarantäne mit der globalen PhishRIP-Funktion
- Zusammenführen von Bedrohungsdaten von mehr als 10 Millionen geschulten KnowBe4-Nutzern und -Nutzerinnen
- Nutzen dreifach validierter Bedrohungsdaten zum Schutz Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation vor neuen Angriffen
- Anzeigen von Nachrichtenclustern oder -gruppen mit ähnlichem Muster zur Erkennung von großflächigen Phishing-Angriffen auf Ihr Unternehmen, Ihre Institution oder Ihre Organisation
- Informieren Ihrer Mitarbeitenden bezüglich der für die Arbeit benötigten E-Mails mithilfe von automatischen E-Mail-Antwortvorlagen
- Entlasten Ihres IR-Teams durch benutzerdefinierte Workflows für Aufgaben (z. B. Priorisierung und Warnungen)

E-Mail-Bedrohungen lassen sich mit jedem Jahr schwieriger erkennen und ein beunruhigender Prozentsatz schafft es durch Ihr sicheres E-Mail-Gateway (SEG) in die Posteingänge der Nutzer und Nutzerinnen. Auch Social-Engineering-Angriffe auf Nutzer und Nutzerinnen mit hohem Risiko nehmen weiter zu. Laut dem 2023 Verizon Data Breach Investigations Report gehen Datenpannen am häufigsten auf E-Mail-Bedrohungen zurück. Und laut dem Team von ArmorBlox umgehen 56 % aller Angriffe veraltete Sicherheitsfilter. Das Fazit? Aufgrund veralteter E-Mail-Sicherheitsfilter gelangen diese digitalen Zeitbomben in die Posteingänge Ihrer Nutzer und Nutzerinnen.

Revolutionäre und proaktive Phishing-Abwehr

PhishER Plus ist der stärkste Phishing-Schutz der Welt. PhishER Plus basiert auf einem einzigartigen KnowBe4-Feed zu globalen Bedrohungen. Dieser dreifach validierte Feed zu Phishing-Bedrohungen blockiert Phishing-Angriffe automatisch mithilfe der folgenden Komponenten, bevor diese in den Posteingängen Ihrer Nutzer und Nutzerinnen landen:

1. Globales KnowBe4-Netzwerk mit mehr als 10 Millionen bestens geschulten Endnutzern und Endnutzerinnen sowie PhishER-Administratoren und -Administratorinnen
2. PhishML, eine einzigartige KI-Engine, gespeist mit Phishing-E-Mails, die alle anderen Filter nicht erkannt haben
3. Von Menschen ausgewählte Bedrohungsdaten aus dem Threat Research Lab von KnowBe4

KnowBe4 erkennt Bedrohungen wie kein anderes Unternehmen, da Nutzer und Nutzerinnen die Angriffe melden, die es durch die Sicherheitsfilter geschafft haben. Genau von diesen im Umlauf befindlichen Social-Engineering-Bedrohungen geht täglich die größte Gefahr aus.

So funktioniert PhishER Plus

PhishER Plus wurde entwickelt, um die E-Mail-Sicherheit Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation zu stärken. Es bildet eine zusätzliche letzte Sicherheitsebene, sofern Ihre vorhandenen SEG- und anderen Cybersicherheitstool versagen.

PhishER Plus ermöglicht einen wichtigen Arbeitsablauf, mit dem Ihre IR-Teams (Incident Response) gemeinsam die Risiken von Phishing-Angriffen mindern können. Das Tool eignet sich für alle Unternehmen, Institutionen und Organisationen, die nach einer präzisen und schnellen Lösung zum automatischen Priorisieren und Verwalten potenziell schädlicher Nachrichten suchen. PhishER Plus ist als eigenständige Lösung oder als optionales Add-on für KnowBe4-Kunden erhältlich.



So funktioniert PhishER Plus



Automatische Nachrichtenvorriorisierung

Mit PhishER Plus weisen Sie jede gemeldete Nachricht einer von drei Kategorien zu: Sicher, Spam oder Bedrohung. Sie weisen anhand von YARA-Regeln die wichtigsten Inhalte zu und PhishER Plus schlägt Prozesse vor, um automatisch so viele Nachrichten wie möglich ohne Nutzereingriff zu priorisieren. Mithilfe von PhishER Plus kann Ihr Team schneller auf die gefährlichsten Bedrohungen reagieren, indem es die Attribute gemeldeter Nachrichten überprüft und die bedenklichsten Nachrichten nach Priorität einstuft.

Emergency Rooms

In den Emergency Rooms befinden sich ähnliche, von Nutzern und Nutzerinnen gemeldete Nachrichten. Diese Nachrichten werden von PhishER Plus nach bestimmten Eigenschaften gruppiert. Die gefilterten Ansichten führen Nachrichten nach „Häufigste Betreffzeilen“, „Häufigste Absender“, „Häufigste Anhänge“ und „Häufigste URLs“ auf. Die einzelnen Emergency Rooms sind interaktiv. Sie können die gefilterten Ansichten der Inbox eingehender untersuchen und Maßnahmen für alle zugehörigen Nachrichten in die Wege leiten.

Integrationen

Dank API-Integration von PhishER Plus und Syslog-Unterstützung lässt sich PhishER Plus mit Ihren vorhandenen Sicherheitsprodukten verknüpfen, um Daten in gängige E-Mail-Sicherheits-, Threat Intelligence-, Ticketing- und SIEM-Plattformen zu übertragen. Darüber hinaus können Sie Ereignisse von PhishER Plus aus senden und zu den Zeitleisten der Nutzer und Nutzerinnen in Ihrer KnowBe4-Plattform hinzufügen. Erstellen Sie anhand dieser Ereignisse spezifische Phishing- und Trainingskampagnen, damit Ihre Nutzer und Nutzerinnen verdächtige E-Mails besser erkennen und über den Phish Alert Button melden. PhishER Plus bietet auch Integrationen in externe Dienste wie VirusTotal, um Anhänge und schädliche Domains zu analysieren.

Von der Community gemeldete Bedrohungsdaten

Alle für alle. Das Threat Research Lab von KnowBe4 und das Netzwerk aus KnowBe4-Endnutzern und -Endnutzerinnen bilden ein gutes Team. Nutzen Sie deren gemeinsame Power, um sich vor neuen und aktuellen Phishing- und Social-Engineering-Angriffen zu schützen.

Globale Blockliste von Microsoft 365

Erstellen Sie über die globale PhishER Plus-Blockliste eine individuelle Liste mit gesperrten Einträgen für Ihr Unternehmen, Ihre Institution oder Ihre Organisation und verbessern Sie Ihre Microsoft 365-E-Mail-Filter direkt in Ihrer PhishER Plus-Konsole. Mithilfe von Blocklisteneinträgen von validierten Bedrohungen – gemeldet von mehr als 10 Millionen geschulten Nutzern und Nutzerinnen – werden übereinstimmende neue eingehende Nachrichten automatisch blockiert, bevor Sie in den Posteingängen Ihrer Nutzer und Nutzerinnen landen.

Dieser fortlaufend aktualisierte Bedrohungsfeed wird von KnowBe4 verwaltet und mit Ihrem Microsoft 365-E-Mail-Server synchronisiert. Sie können für Microsoft 365 stattdessen jedoch auch Ihre eigene private Blockliste verwenden.

PhishML™

PhishML ist ein PhishER Plus-Modul für maschinelles Lernen, mit dem Sie verdächtige Nachrichten, die von Nutzern und Nutzerinnen gemeldet werden, am Anfang des Priorisierungsprozesses identifizieren und bewerten können. PhishML analysiert jede auf der PhishER Plus-Plattform eingehende Nachricht und stellt Ihnen Informationen für einen schnellen, genauen und einfachen Priorisierungsprozess bereit.

PhishML entwickelt sich basierend auf den Nachrichten, die von Ihnen und anderen Nutzern und Nutzerinnen der PhishER Plus-Community getaggt werden, kontinuierlich weiter. Das Modul wird dank der neu bereitgestellten Daten immer besser und genauer. So können in PhishER Plus noch mehr Nachrichten automatisch kategorisiert werden.

Globale PhishRIP™-Funktion

Die globale PhishRIP-Funktion ist eine Quarantänefunktion für E-Mails mit Unterstützung für Microsoft 365 und Google Workspace, dank der Ihr IR-Team schnell reagieren und Maßnahmen ergreifen kann.

Mithilfe der globalen PhishRIP-Funktion lassen sich identifizierte Bedrohungen aus allen Posteingängen Ihrer Nutzer und Nutzerinnen entfernen, nicht gemeldete Bedrohungen isolieren und zukünftige Bedrohungen vermeiden, indem legitime E-Mails gelöscht, unter Quarantäne gestellt oder wiederhergestellt werden. Nachrichten, die mit einer von anderen PhishER Plus-Kunden erkannten Phishing-Bedrohung übereinstimmen und aus den Posteingängen dieses Unternehmens, dieser Institution oder dieser Organisation entfernt wurden, werden im Anschluss vom Threat Research Lab von KnowBe4 überprüft. Diese Nachrichten werden automatisch in Quarantäne verschoben und aus allen Posteingängen Ihrer Nutzer und Nutzerinnen entfernt.

PhishFlip™

PhishFlip ist eine Funktion von PhishER Plus, bei der von Nutzern und Nutzerinnen gemeldete tatsächliche Phishing-Angriffe in einer sicheren Simulation für Phishing-Kampagnen auf Ihrer KnowBe4-Plattform eingesetzt werden. Mit PhishFlip können Sie einen gefährlichen Angriff unmittelbar in wirklichkeitsnahes Training „verwandeln“.

Integration der CrowdStrike Falcon Sandbox

Mit dieser Integration können Administratoren und Administratorinnen, die über eine Lizenz für CrowdStrike Falcon Sandbox verfügen, potenziell schädliche Dateien schneller und effizienter untersuchen – alles über eine einzigen Konsole. Das Malware-Analysetool CrowdStrike Falcon Sandbox bietet die Möglichkeit, Dateien und URLs in einer geschützten Sandbox-Umgebung auf schädliche Inhalte hin zu analysieren.

PhishER Plus integriert KI-validierte Daten von bestens geschulten und technisch versierten Nutzern und Nutzerinnen weltweit – es handelt sich um den Kundenstamm von KnowBe4 mit mehr als 65.000 Unternehmen, Institutionen und Organisationen und über 55 Millionen Nutzern und Nutzerinnen insgesamt. **Ganz einfach. Zusammen sind wir stärker.**