KnowBe4

Der außergewöhnliche ROI von PhishER Plus

Ich bin Stu Sjouwerman, Gründer und CEO von KnowBe4. KnowBe4 ist mein fünftes Start-up. Ich bin seit mehr als 40 Jahren in der IT-Branche tätig und beschäftige mich bereits seit 25 Jahren mit Informationssicherheit. In meinem letzten Unternehmen haben wir eine Antivirus-Engine mit Angriffserkennung, Eindringschutz und einer Firewall entwickelt. Ein Problem wurde damals in der Branche jedoch kaum beachtet – die Manipulation der Nutzer und Nutzerinnen durch Cyberkriminelle. Aus diesem Grund wurde KnowBe4 gegründet: Wir möchten IT-Teams dabei helfen, die allgegenwärtige Gefahr durch Social Engineering in den Griff zu bekommen. Im April 2021 sind wir an die NASDAQ gegangen und 2023 wurde KnowBe4 dann zu einem privaten Unternehmen.

Schutzwall gegen die verheerende Flut von Phishing-Angriffen

91 % der Cyberangriffe starten mit einem Spear-Phishing-Angriff und zwei Drittel aller Ransomware-Infektionen lassen sich auf Phishing zurückführen. Durch den Einsatz von KI werden Phishing-Angriffe noch ausgefeilter und effektiver. Daher ist es wichtig, dass Sie Ihren IT- und InfoSec-Teams Tools bereitstellen, mit denen Phishing-Bedrohungen präzise und schnell abgewendet werden können, BEVOR diese Schaden anrichten.

> “PhishER hat sich für uns ausgezahlt. Unser Risiko hat sich reduziert, unsere IT-Teams haben mehr Zeit und das Produkt ist extrem einfach zu konfigurieren und anzupassen.”
>
> – George Schneider, Information Security Manager

Wenn Ihr Unternehmen oder Ihre Organisation Phishing-Bedrohungen manuell bekämpft, erhöht sich das Risiko, das Phishing darstellt, drastisch. Eine manuelle Bekämpfung ist mit vier großen Herausforderungen verbunden:

- **HOHE ANZAHL AN WARNMELDUNGEN**

  IT- und InfoSec-Teams, die nicht auf automatisierte Workflows vertrauen, benötigen im Schnitt 27 Minuten, um eine Phishing-E-Mail manuell zu überprüfen.[1] Dies erhöht das Phishing-Risiko für das Unternehmen oder die Organisation enorm.

- **ÜBERLASTUNG UNTERBESETZTER IT-TEAMS**

  61 % der mittelgroßen Unternehmen und Organisationen haben kein eigenes Cybersecurity-Team. Im Schnitt befasst sich nur eines von 10 Mitgliedern des IT-Teams ausschließlich mit dem Thema Cybersicherheit.[2]

- **DURCHBRECHEN DES SCHUTZWALLS**

  Immer mehr Phishing-E-Mails gelangen über sichere E-Mail-Gateways in die Posteingänge Ihrer Nutzer und Nutzerinnen: Bei 56 % der E-Mail-Angriffe im Jahr 2022 wurden veraltete Sicherheitsfilter umgangen[3] und 18,8 % der Phishing-E-Mails wurden von Microsoft Exchange Online Protection und Microsoft Defender nicht erkannt[4].

- **LANGSAME REAKTION AUF GEZIELTE ANGRIFFE**

  Wenn Sie gezielte Phishing-Angriffe wie Spear-Phishing-Kampagnen nicht in Echtzeit abwenden können, ist Ihr Unternehmen oder Ihre Organisation gefährdet. Dabei erhalten mehrere Nutzer und Nutzerinnen gleichzeitig dieselbe Phishing-E-Mail. Ihrem Team bleibt nur wenig Zeit, diese Phishing-E-Mails aus den Posteingängen zu entfernen, bevor ein schädlicher Link angeklickt wird.

[1]The Business Cost of Phishing, 2022 Report
[2]State of Cybersecurity for Mid-Sized Businesses, 2023
[3]ArmorBlox
[4]Check Point Email Research Team

Aus diesem Grund gibt es das Security, Orchestration, Automation and Response (SOAR)-Produkt von KnowBe4, das speziell für die Abwehr und die Beseitigung von Phishing-Bedrohungen konzipiert wurde: PhishER Plus.

Die Vorteile und der ROI von PhishER Plus/PhishER von KnowBe4

Laut Forrester ergaben sich bei einem Großunternehmen durch die Einführung von PhishER von KnowBe4 über einen Zeitraum von drei Jahren folgende Kosteneinsparungen, Produktivitätszuwächse und geschäftlichen Vorteile.[5]

Die Mitarbeitenden melden über den Phish Alert Button von KnowBe4 bis zu 2.000 verdächtige E-Mails pro Monat in PhishER. Etwa 88 % der gemeldeten E-Mails sind Spam oder Bedrohungen. Das Unternehmen kann einen großen Teil dieser Meldungen mit der E-Mail-Quarantänefunktion PhishRIP abarbeiten. Die gemeldeten Phishing-E-Mails werden automatisch unter Quarantäne gestellt und aus den Posteingängen betroffener Nutzer und Nutzerinnen gelöscht.

Aufgrund der Automatisierung von E-Mail-Warnungen und -Antworten konnte das Unternehmen den Zeitaufwand reduzieren und 411.302 USD (378.988 EUR) einsparen.

PhishER Plus reduziert den Zeitaufwand für die Analyse und Abwehr für das IR-Team im Schnitt um 25 Minuten pro E-Mail.

Durch die engere Zusammenarbeit zwischen den Nutzern und Nutzerinnen und dem SOC-Team kann letzteres proaktiv auf Bedrohungen reagieren. Dadurch verringern sich die Anzahl der IT-Helpdesk-Tickets und der Aufwand für das IT-Team.

Dank automatisierter E-Mail-Antworten an die Mitarbeitenden kann die Arbeit schnell wieder aufgenommen werden.

Weitere Beispiele für die Zeitersparnis von Unternehmen und Organisationen:

- **In einem kritischen Infrastrukturbereich in den USA tätiges Unternehmen**

  Zeitersparnis von 7 Wochen pro Jahr für das IT-Team durch automatisierte Analyse, Quarantäne und Entfernung schädlicher E-Mails

- **Marketingfirma**

  Zeitersparnis von 12,5 Stunden pro Monat, da die Anzahl der verdächtigen E-Mails, die manuell überprüft werden müssen, von etwa 70 auf 20 reduziert werden konnte

- **Tech-Unternehmen**

  Zeitersparnis und Freisetzung von Personal- und Budgetkapazitäten, da die KI-gesteuerte Analyse von PhishER 70 % aller von Nutzern und Nutzerinnen gemeldeten E-Mails automatisch identifiziert

- **Non-Profit-Organisation**

  Schnellere Reaktion auf Phishing-Angriffe und Freisetzung von IT-Ressourcen und Personal für andere sicherheitsrelevante Aufgaben

- **Bildungseinrichtung**

  Entfernung von mehr als 150.000 schädlichen E-Mails aus den Posteingängen der Nutzer und Nutzerinnen durch PhishER

Mehr als 65.000 Unternehmen und Organisationen setzen die Plattform bereits erfolgreich ein.

Mehr erfahren

[5] Forrester Total Economic Impact of KnowBe4

ELOVADE

Kontaktdaten für DE/AT:

ELOVADE Deutschland GmbH
knowbe4@elovade.com
DE: +49 6441 67118 842
AT: +43 820 0010 36
elovade.com/knowbe4

Kontaktdaten für CH:

ELOVADE Swiss AG
sales@elovade.ch
CH: +41 55 552 27 92
elovade.ch/knowbe4