

KnowBe4

Der außergewöhnliche ROI für das Security Awareness Training von KnowBe4



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, Eindringenschutz 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.

Zusammenfassung für Führungskräfte

Die Gefahr von Ransomware-Angriffen wird immer größer. Ist ein solcher Angriff erfolgreich, drohen Netzwerkausfälle und Datendiebstahl.

Sie können das Risiko reduzieren. Ein wirksames Mittel hierzu ist Security Awareness Training (SAT), denn zwei Drittel aller Ransomware-Infektionen lassen sich auf Phishing zurückführen. Laut Forrester ergaben sich bei einem Großunternehmen durch die Einführung von Security Awareness Training von KnowBe4 über einen Zeitraum von drei Jahren folgende Kosteneinsparungen, Produktivitätszuwächse und Geschäftsvorteile:¹

1. **ROI von 276 %**, Einsparungen in Höhe der Anschaffungskosten innerhalb von nur drei Monaten
2. **Schutz von Vermögenswerten im Wert von 432.300 USD (392.800 EUR)** über drei Jahre durch den Aufbau einer starken Sicherheitskultur mithilfe von Security Awareness Training und Phishing-Simulationen
3. **Einsparungen in Höhe von 411.300 USD (373.800 EUR)**, da die IT-Abteilung proaktiv auf Bedrohungen reagieren kann
4. **Einsparungen in Höhe von 164.200 USD (149.200 EUR) durch Nutzung** der in 35 Sprachen zur Verfügung stehenden Trainingsbibliothek und Phishing-Simulationen
5. **Einsparungen bei Versicherungskosten**, da es zu weniger Ausfällen und Betriebsunterbrechungen kommt

Fazit: Die Investition in die KnowBe4-Plattform ist vor dem Hintergrund begrenzter InfoSec-Budgets extrem lohnend. Es stehen leistungsstarke Add-ons für Phishing-Abwehr, Echtzeit-Coaching und Compliance-Training zur Verfügung. Unternehmen, und Organisationen berichten immer wieder von dem herausragenden Return on Investment bei KnowBe4.

“

Wir haben vor etwa drei Jahren KnowBe4 eingeführt. **Seitdem gab es keinen vergleichbaren Sicherheitsvorfall mehr.**

– IT Security Awareness Program Manager

“

1 [Forrester, Total Economic Impact von KnowBe4](#)

Social Engineering wird ein immer größeres Problem

Sie müssen Ihr InfoSec-Budget optimal nutzen und Netzwerke sowie Daten schützen. Diese Ziele erreichen Sie mit dem Einsatz wirkungsvoller Sicherheitslösungen.

Ein einziger erfolgreicher Cyberangriff kann Umsatz, Ausgaben und Cashflow beeinträchtigen. Als IT-Verantwortlicher übernehmen Sie eine wichtige Rolle bei der Bewältigung dieses Risikos.

Schätzungen zufolge steigen die Kosten von Cybercrime zwischen 2023 und 2028 weltweit um 5,7 Billionen USD (5,2 Billionen EUR).² Vor dem Hintergrund dieses exorbitanten Anstiegs müssen Sie sich bewusst machen, dass Ihre Belegschaft das größte Sicherheitsrisiko darstellt. Laut dem Data Breach Investigations Report von Verizon gehen 74 % der Datenpannen auf den Faktor Mensch zurück. Dabei starten 91 % der Cyberangriffe mit einem Spear-Phishing-Angriff. Darüber hinaus lassen sich zwei Drittel aller Ransomware-Infektionen auf Phishing zurückführen.³

Diese Statistiken machen deutlich, wie wichtig ein wirkungsvolles SAT-Programm ist, dank dem Ihre Belegschaft intelligentere Entscheidungen treffen, Ihre Sicherheitskultur stärken und Risiken durch menschliche Fehler reduzieren kann. Der ROI von Security Awareness Training lässt sich anhand der folgenden Punkte ermitteln:

- Risiken/Kosten ohne Training
- Kosten für die Bereitstellung, Implementierung und Verwaltung eines eigenen SAT-Programms
- Vorteile der SAT-Plattform von KnowBe4

Risiken/Kosten ohne Training

Bei SAT geht es um die Minimierung von Risiken. Ohne Security Awareness Training können Ihnen enorme Kosten entstehen. 2023 beliefen sich die Kosten einer Datenpanne im Schnitt auf etwa 4,05 Millionen EUR.⁴ Im Folgenden sind die sechs wichtigsten Kostenpunkte aufgeführt:

- Zeitaufwand für die Wiederherstellung des Normalzustands nach einem Cybervorfall oder einer ausgewachsenen Datenpanne (häufig nur durch teure externe Angebote möglich)
- Ausfallzeiten und Verlust von Geschäftsfeldern
- Finanzielle Verluste (Diebstahl, Lösegeldzahlungen und Betrug)
- Rufschädigung
- Verlust von geistigem Eigentum
- Erhöhung der Versicherungsprämien für Cyberbedrohungen und mögliche Geldbußen aufgrund der Nichteinhaltung von Branchenstandards/Vorschriften

91 % der Cyberangriffe starten mit einem Spear-Phishing-Angriff und zwei Drittel aller Ransomware-Infektionen lassen sich auf Phishing zurückführen.

2 [Statista, Cost of Cybercrime Worldwide](#)
3 [Verizon, Data Breach Investigations Report](#)
4 [IBM, Cost of Data Breach Report](#)

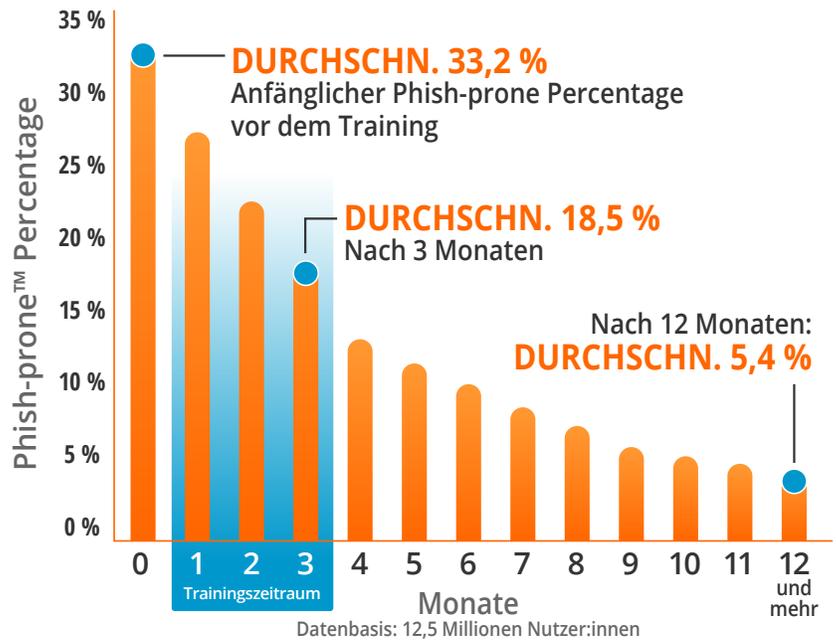
Darüber hinaus ist auch mit deutlichen Umsatzeinbußen zu rechnen. 2023 haben beispielsweise einige Cybervorfälle in der Glücksspielbranche und der Konsumgüterbranche Aufsehen erregt – mit einem geschätzten Umsatzverlust der betroffenen Unternehmen von über 1 Mrd. EUR.

Kosten für die Bereitstellung, Implementierung und Verwaltung eines eigenen SAT-Programms

Können Sie einschätzen, wie viele Stunden, Teammitglieder und Ressourcen Sie benötigen würden, um ein attraktives, effektives SAT-Programm in mehreren Sprachen mit Phishing-Simulationen, Reports und stets aktuellen Inhalten aufzubauen? Je nach Größe Ihres Unternehmens oder Ihrer Organisation liegen die Kosten um 200 % bis 300 % höher als ein Jahresabonnement für die KnowBe4-Plattform.

Vorteile und ROI der SAT-Plattform von KnowBe4

Bei einem wirkungsvollen SAT-Programm wird proaktiv versucht, die Risiken von Phishing- und Social-Engineering-Angriffen abzuwenden, bevor Ihnen ein Schaden aus einem Cyberangriff oder einer Datenpanne entsteht. Laut Cost of a Data Breach Report 2023 von IBM war Training von Mitarbeitenden einer der drei wichtigsten Faktoren, um Datenpannen effektiv abzuwenden. Im Schnitt können Unternehmen und Organisationen dadurch 232.867 USD (211.615 EUR) einsparen.



Quelle: KnowBe4 – Phishing-Risiko nach Branchen: Benchmarking-Report 2023

Anmerkung: Der anfängliche Phish-prone Percentage wird auf Grundlage aller evaluierten Nutzer:innen berechnet. Diese Nutzer:innen wurden vor der Evaluierung nicht mithilfe der KnowBe4-Konsole geschult. Nachfolgende Zeiträume geben den Phish-Prone Percentage für die Untergruppe der Nutzer:innen wieder, die mithilfe der KnowBe4-Konsole geschult wurden.

Hervorragender Schutz vor Social-Engineering-Angriffen

Im Benchmarking-Report von KnowBe4 zum Phishing-Risiko nach Branchen wird der Phish-prone™ Percentage (Phishing-Anfälligkeit) von Millionen von Nutzern und Nutzerinnen analysiert. Aus dem Report geht hervor, wie wichtig es für Unternehmen, Unternehmen und Organisationen ist, in die Belegschaft als menschliche Verteidigungslinie zu investieren sowie die Sicherheitskultur zu stärken. Mit der Plattform für Security Awareness Training und Phishing-Simulationen von KnowBe4 lässt sich die Phishing-Anfälligkeit um unglaubliche 82 % reduzieren.⁵

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

MEHR ERFAHREN