KnowBe4
Human error. Conquered.

# Was Sie bei der Auswahl eines Anbieters von Security Awareness Training (SAT) unbedingt beachten müssen

# Was Sie bei der Auswahl eines Anbieters von Security Awareness Training (SAT) unbedingt beachten müssen

## Inhaltsverzeichnis

# EINFÜHRUNG

Security Awareness Training (SAT) wird von vielen innovativen Anbietern bereitgestellt. Die Branche hat sich in den vergangenen Jahren deutlich gewandelt. Denn CISOs und Sicherheitsverantwortliche möchten heute sicherstellen, dass ein SAT-Programm das Verhalten von Nutzer:innen tatsächlich verändert. Außerdem soll das Cyberrisiko, das von Mitarbeitenden ausgeht, ermittelt, reduziert und im Blick behalten werden können.

Folgendes muss die Plattform eines SAT-Anbieters leisten:

- Bewusstsein hinsichtlich der Sicherheitskultur stärken und Human Risk Management verbessern
- Notwendige Mittel zur Durchsetzung und Messung von Verhaltensänderungen bereitstellen
- Sicherstellen, dass Mitarbeitende des Unternehmens, der Institution oder der Organisation als Human Firewall und letzte Verteidigungslinie agieren und Cyberangriffe sowie Datenpannen verhindern

In diesem Whitepaper erfahren Sie, was Sie vor der Beurteilung von SAT-Plattformen wissen müssen, und lernen sieben kritische Komponenten kennen, die bei einem SAT-Anbieter nicht fehlen dürfen, damit Sie Ihre Ziele erreichen.

# BEURTEILUNG VON PLATTFORMEN FÜR SECURITY AWARENESS TRAINING

Viele herkömmliche SAT-Programme haben ein Problem: Sie können die Intentions-Verhaltens-Lücke nicht schließen. Einfach ausgedrückt: Nur weil Sie Nutzer:innen Informationen und Daten zu Security Awareness bereitstellen, bedeutet das noch lange nicht, dass diese daraus lernen und/oder das Erlernte anwenden.

Durch Informationen allein werden keine Verhaltensänderungen erzielt. Menschen neigen dazu, den Weg des geringsten Widerstands zu gehen oder an gewohnten Verhaltensweisen festzuhalten. Stellen Sie sicher, dass wichtige Entscheidungsträger:innen innerhalb Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation vor der Auswahl eines SAT-Anbieters mit folgenden drei Tatsachen vertraut sind.

- **Informationen allein reichen nicht aus, um eine Verhaltensänderung zu bewirken.**
  Wenn Sie Mitarbeitende mit unzähligen Informationen, Daten und Verfahren überhäufen, bedeutet das nicht, dass sich dadurch das Sicherheitsbewusstsein verändert. Eine Sicherheitsempfehlung werden die meisten Mitarbeitenden als gutgemeinten Ratschlag verbuchen und gegen andere Prioritäten abwägen.

- **Richtlinien, die gegen die menschliche Natur gehen, werden nicht befolgt.**
  Wenn sich Richtlinien nicht am tatsächlichen Verhalten orientieren, bleibt Ihr SAT-Programm wahrscheinlich weit hinter den Erwartungen zurück. Sie dürfen nicht außer Acht lassen, dass es um Menschen geht, die im Gegensatz zu Computern nicht einfach programmiert werden können.

- **Es kommt auf das Verhalten der Mitarbeitenden an. Dieses ist viel wichtiger als das, was Ihre Mitarbeitenden wissen.**
  Durch Wissen allein können Datenpannen in Unternehmen, Institutionen und Organisationen nicht verhindert werden. Es ist das Verhalten, das die Sicherheit eines Unternehmens, einer Institution oder einer Organisation stärken oder andererseits eben zu einer Datenpanne führen kann. Konzentrieren Sie sich darauf, eine Verhaltensänderung zu bewirken, und stellen Sie nicht nur Informationen und Richtlinien bereit.

# SIEBEN KRITISCHE KOMPONENTEN, DIE BEI EINEM SAT-ANBIETER NICHT FEHLEN DÜRFEN

Achten Sie bei der Auswahl eines SAT-Anbieters darauf, dass die folgenden sieben Komponenten bereitgestellt werden. Sie stellen dadurch nicht nur sicher, dass Ihr SAT-Programm in kurzer Zeit zum Erfolg führt, sondern sorgen auch für eine erfolgreiche Zukunft vor.

## 1. Vielfältiger und spannender Content

*Nutzer:innen sollten das Training auch auf Mobilgeräten absolvieren können.*

Selbstverständlich kommt es vor allem auf den Content an. Er bildet die Grundlage der Wissensvermittlung bei jedem SAT-Programm. Achten Sie auf Vielfalt. Nutzer:innen werden von ganz unterschiedlichen Inhalten angesprochen und lernen besonders effektiv, wenn der Content zu ihren persönlichen Lernpräferenzen passt. Achten Sie also auf den Content, wenn Sie SAT-Plattformen beurteilen. Um Verhaltensänderungen zu bewirken und eine starke Sicherheitskultur in Ihrem Unternehmen, Ihrer Institution oder Ihrer Organisation aufzubauen, benötigen Sie Content, der so vielfältig ist wie Ihre Mitarbeitenden. Entscheiden Sie sich für eine SAT-Plattform mit einer großen Bibliothek, deren Trainingsinhalte kontinuierlich aktualisiert werden und in mehreren Sprachen zur Verfügung stehen. Außerdem sollten interaktive Module, Videos, Spiele, Poster, Newsletter, Assessments usw. bereitgestellt werden.

Genauso wichtig sind Trainingsangebote, die auf spezifische Rollen oder Präferenzen abgestimmt sind. Ihr Callcenter-Team benötigt vermutlich ein anderes Training als Ihr IT-Team. Dies muss sich im Content widerspiegeln. Nutzer:innen lernen darüber hinaus ganz unterschiedlich: Manche verinnerlichen Inhalte aus drei- bis fünfminütigen lustigen Videos, während für andere ein solcher Ansatz möglicherweise irritierend ist. Entscheidend für die Auswahl einer SAT-Plattform ist, ob diese die Möglichkeit bietet, grundlegende Trainingsinhalte flexibel, d. h. passend zu den jeweiligen Präferenzen, zu vermitteln.

Achten Sie nicht zuletzt darauf, wie die Trainingsinhalte bereitgestellt wird. Nutzer:innen sollten das Training auch auf Mobilgeräten absolvieren können. Genauso wichtig ist eine benutzerfreundliche Verwaltung. Das Training muss einfach zugewiesen, verfolgt und in Zahlen gefasst werden können. Reports, aus denen aussagekräftige und nützliche Schlussfolgerungen gezogen werden können, dürfen nicht fehlen. Sie benötigen Aufschluss darüber, ob sich das Risiko erhöht oder verringert hat und in welchen Bereichen Ihr Unternehmen, Ihre Institution oder Ihre Organisation stärker intervenieren muss. Die SAT-Plattform sollte Ihnen darüber hinaus die Möglichkeit bieten, benutzerdefinierten Content und Content von Drittanbietern einzubinden.

## 2. Lokalisierung

Lokalisierung bedeutet, dass der Content in verschiedene Sprachen übersetzt wird und länder- bzw. regionsspezifische Beispiele, Bilder sowie interaktive Elemente enthalten sind. Lokalisierung geht über einfache Übersetzungstätigkeit hinaus und ist wichtig für international tätige Unternehmen, Institutionen und Organisationen mit Mitarbeitenden unterschiedlicher Muttersprache.

Entscheiden Sie sich für die Partnerschaft mit einem SAT-Anbieter, der Ihren Nutzer:innen die Möglichkeit bietet, die Sprache/Region selbst auszuwählen. Das ist entscheidend für den Lernerfolg. Ein SAT-Anbieter muss hochwertige Lokalisierungen bereitstellen und die Relevanz der Beispiele von lokalen Expert:innen überprüfen lassen.

## 3. Struktur und Automatisierung

Ein SAT ist nicht nach einer Sitzung erledigt. Um eine Sicherheitskultur aufzubauen, sind kontinuierliches Training, fortlaufende Tests und die Wiederholung der Inhalte erforderlich. Denken Sie beim Konzipieren eines SAT-Programms daran, dass Lernen auf drei unterschiedlichen Ebenen erfolgt. Es ist wichtig, dass eine SAT-Plattform den Content und die Tools bietet, mit denen Sie jede der Ebenen gezielt unterstützen können.

- **Formelles, strukturiertes Lernen (10 %)**: Frontalunterricht, Onlineunterricht über ein Learning Management System (LMS), Trainingstage usw.
- **Informelles Lernen (20 %)**: Nachfrage bei Teammitgliedern, Zusammenarbeit, Videos, eigenständige Lektüre usw.
- **Experimentelles Lernen (70 %)**: alltägliche Lernchancen, die sich durch Training on the Job, den Austausch mit anderen oder im Rahmen von Arbeitsabläufen oder der Unternehmens- und Abteilungskultur usw. bieten.

*Lernen findet zu 90 % außerhalb formeller, strukturierter Umgebungen statt.*

Laut diesem Modell findet Lernen zu 90 % außerhalb formeller, strukturierter Umgebungen statt. Viele SAT-Programme erzielen nicht die gewünschte Wirkung, da sie sich auf die ersten 10 % konzentrieren. Stellen Sie sicher, dass in Ihrem SAT-Programm alle drei Ebenen berücksichtigt werden und die ausgewählte SAT-Plattform über die dafür notwendigen Tools verfügt. Beispielsweise sollte es möglich sein, ein kurzes Video über die Anforderungen an Passwörter auf der Seite zum Zurücksetzen von Passwörtern einzubinden, damit es im Bedarfsfall sofort zur Verfügung steht.

Automatisierung ist ebenfalls eine wichtige Komponente. Sie vereinfacht die Nutzerbereitstellung und ermöglicht eine frühzeitige Planung von Trainingskampagnen bereits Wochen im Voraus, ohne dass die Programmadministrator:innen direkt eingreifen müssen. Automatisierung erhöht die Benutzerfreundlichkeit und die Kapitalrendite, da Sie weniger Zeit für die Programmverwaltung benötigen und Content effektiver bereitstellen können. Schließlich sollte es auch möglich sein, mithilfe von Automatisierung relevante Trainingsinhalte direkt nach einem Fehlverhalten einzublenden und Management und Führungskräften planmäßige Reports bereitzustellen.

## 4. Tests

Training bildet zwar die Grundlage eines SAT-Programms, Nutzer:innen sollten jedoch auch getestet werden. Mithilfe von Phishing-Simulationen können Sie herausfinden, ob sich das Sicherheitsverhalten ändert und Fehler reduziert werden. Klicken Nutzer:innen auf die E-Mail, melden Sie sie oder tun sie nichts? Achten Sie auch darauf, ob Phishing-E-Mails einfach gemeldet werden können.

Dadurch erhöht sich die Resilienz Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation. Ihr IT-Team erfährt, ob Ihr Unternehmen, Ihre Institution oder Ihre Organisation derzeit von Angriffen bedroht wird, und kann alle Betroffenen rechtzeitig warnen.

Die meisten SAT-Plattformen bieten zwar verschiedene Simulationen und Phishing-Vorlagen sowie Reporting-Tools an, hier kommt es jedoch aufs Detail an. Entscheiden Sie sich für einen SAT-Anbieter als Partner, der die Bedrohungslage genau im Auge behält und Phishing-E-Mail-Vorlagen bereitstellt, die auf realen Bedrohungen basieren.

Wenn Mitarbeitende einen simulierten Phishing-Test nicht bestehen, sollten sie umgehend Training zum entsprechenden Thema erhalten. Der Lerneffekt ist größer, wenn ein spezifischer Vorfall noch frisch im Gedächtnis ist.

Automatisierung und maschinelles Lernen sind nicht nur bei der Bereitstellung von Content und der Entwicklung von Programmen von Vorteil, auch Phishing-Simulationsprogramme profitieren hiervon. Eine Phishing-Simulationsplattform sollte durch maschinelles Lernen und auf Basis von Trainingsdaten und Phishing-Verlauf der Nutzer:innen in der Lage sein, fundierte und personalisierte Phishing-Vorlagen zu empfehlen und bereitzustellen. Wenn die Plattform darüber hinaus echte Phishing-E-Mails erkennen und diese in Phishing-Vorlagen umwandeln kann, sind Sie auf der sicheren Seite.


## 5. Kennzahlen und Reports

Kennzahlen und Reports sind wichtige Indikatoren dafür, ob Ihr SAT-Programm zu Verhaltensänderungen und weniger menschlichen Fehlern führt. Solche Kennzahlen und Reports dienen außerdem als Erfolgsnachweis für Ihr Security Awareness Program gegenüber Führungskräften.

Wenn Sie wissen, ob Sie durch Ihr Programm die gewünschten Ziele erreichen, und in der Lage sind, eine Verbesserung zu belegen, können Sie sich die Unterstützung der Führungskräfte sichern. Ein guter SAT-Anbieter verfügt über eine solide Reporting- und Analyseplattform und stellt Ihrem Unternehmen, Ihrer Institution oder Ihrer Organisation wichtige Kennzahlen bereit, aus denen beispielsweise Reports für Führungskräfte erstellt werden können.

Entscheiden Sie sich für einen SAT-Anbieter, der den Faktor Mensch und die Sicherheitskultur berücksichtigt. Herkömmliche SAT-Programme bieten in der Regel lediglich Kennzahlen zu Abschlussquoten, Quizleistungen, Beteiligung usw. Um datengestützte Entscheidungen bezüglich der weiteren Trainingsmaßnahmen treffen zu können, benötigen Sie jedoch ein Risikoprofil von allen Nutzer:innen bzw. jeder Abteilung. Sie sollten beurteilen können, wie sich das Risiko Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation im Laufe der Zeit verändert und was Ihr Trainingsprogramm tatsächlich bewirkt. Nur so finden Sie heraus, wo Sie ansetzen müssen, um die Human Firewall weiter zu stärken.

## 6. Umfragen und Assessments

Möglicherweise verstehen nicht alle Mitarbeitenden, warum sie sich einem kontinuierlichen Security Awareness Training unterziehen müssen, da sie Cybersicherheit als Angelegenheit der IT-Abteilung betrachten. Sie sollten daher die Einstellungen innerhalb Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation verstehen und wissen, wie sie sich durch das SAT verändern. Dann können Sie Bereiche ermitteln, in denen bereits gute Leistungen erzielt werden, sowie Bereiche, in denen noch Trainingsbedarf besteht. Sie erfahren auch, wie sich Ihre Sicherheitskultur entwickelt. Da Vorlieben, Meinungen und Einstellungen analysiert werden, reichen die bereits erwähnten Kennzahlen nicht aus.

In Umfragen und Assessments sollten nicht nur Stimmungen und Einstellungen gemessen, sondern auch Kenntnisse und Fähigkeiten abgefragt werden. Wählen Sie eine SAT-Plattform aus, über die Sie Assessments zu den Fähigkeiten und Umfragen zur Sicherheitskultur durchführen können, um Ihre Nutzer:innen besser einschätzen und die allgemeine Sicherheitskultur Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation besser beurteilen zu können. Sie können ermitteln, welche Nutzer:innen in einer bestimmten Situation kompetent reagieren und was es bedeutet, das Richtige zu tun. Sie sollten auch die Möglichkeit haben, Ihr Unternehmen, Ihre Institution oder Ihre Organisation im Branchenvergleich zu betrachten und mithilfe wissenschaftlich fundierter Assessments die erzielten Fortschritte präzise zu messen.

Dazu gehört auch ein individueller Risk Score für alle Mitarbeitenden. Oberstes Ziel ist ein verbessertes Human Risk Management. Sobald Sie das Risikoprofil einer Person oder einer Abteilung kennen, können Sie das Training anpassen und wertvolle Erkenntnisse darüber gewinnen, wo Sie Ihr Sicherheitsprogramm verbessern können.

## 7. Weitere Inhalte, die über SAT hinausgehen

Die Branche hat sich in den vergangenen Jahren grundlegend verändert. Führende Anbieter haben sich weiterentwickelt und bieten nicht mehr nur Training für Nutzer:innen an, sondern stellen auch Plattformen bereit, die beim Aufbau einer Sicherheitskultur und der Verbesserung des Human Risk Management helfen.

Suchen Sie sich einen SAT-Anbieter als Partner, der nicht nur Ihre unmittelbaren Ziele erreicht, sondern mit dem Sie auch in Zukunft gut aufgestellt sind. Beachten Sie bei der Beurteilung von SAT-Anbietern diese wichtigen Punkte:

- **Fokus auf Bewusstsein, Verhalten und Sicherheitskultur**
  Ziel sollte sein, menschliche Fehler weitestgehend auszuräumen. Laut Forrester Research sind Anbieter zu bevorzugen, die Kennzahlen zum Faktor Mensch anbieten und das Risiko auf der Grundlage des Nutzerverhaltens berechnen.* Das SAT wird dann zum Eckpfeiler für die Gestaltung Ihrer Sicherheitskultur.

- **Von welchen zusätzlichen Angeboten kann Ihr Unternehmen, Ihre Institution oder Ihre Organisation neben dem SAT noch profitieren?**
  Wie bereits erwähnt, ist das SAT der grundlegende Eckpfeiler für den Aufbau einer Sicherheitskultur in einem Unternehmen, einer Institution oder einer Organisation, aber nicht unbedingt die einzige Komponente. Andere Komponenten wie individuelles Verhalten, SOAR-Plattformen, Reagieren auf Vorfälle und Bedrohungsdaten sind weitere Schlüsselkomponenten, die in Zukunft in Ihre Sicherheitskultur aufgenommen werden könnten. Suchen Sie sich einen Partner, der nicht nur Ihre aktuellen, sondern auch Ihre zukünftigen Anforderungen erfüllt.

* The Forrester Wave: Security Awareness And Training Solutions, Q1 2022

# CHECKLISTE ZUR AUSWAHL EINES SAT-ANBIETERS

- ☐ Umfangreiche und vielfältige Lernbibliothek
- ☐ Lokalisierung
- ☐ Automatisierte Trainings- und Phishing-Plattform
- ☐ Haben Sie die Möglichkeit, eigene Trainingsinhalte hochzuladen oder Content von der Plattform herunterzuladen?
- ☐ Plattform zur Bereitstellung von Training mit Automatisierungsfunktionen
- ☐ Möglichkeit, Inhalte von Drittanbietern auf die Trainingsplattform bzw. in das Lernmanagementsystem hochzuladen
- ☐ Flexible simulierte Phishing-Plattform mit vielfältigen, anpassbaren und lokalisierten Phishing-Vorlagen
- ☐ Automatisierung, künstliche Intelligenz und maschinelles Lernen als integrale Bestandteile der Trainings- und Phishing-Plattform
- ☐ Solide Funktionen zum Testen und Bewerten der Nutzer:innen, Kennzahlen über den Kenntnisstand und die Auswirkungen des Trainings
- ☐ Intuitive Metriken und Reporting-Funktionen zur Darstellung der Kapitalrendite
- ☐ Reports für Führungskräfte

# FAZIT

Letztlich bilden diese Funktionen die Grundlage dafür, dass das SAT-Programm Ihres Unternehmens, Ihrer Institution oder Ihrer Organisation das Nutzerverhalten verändert und Sie die Möglichkeit haben, Cyberrisiken zu verstehen, zu reduzieren und zu überwachen. Das SAT dient als Plattform für die Entwicklung eines umfassenderen Verständnisses von Sicherheitskultur und Human Risk Management und macht aus Ihren Nutzer:innen eine Human Firewall.

## Weitere Ressourcen

**Kostenloser Phishing Security Test**
Wie anfällig sind Ihre Mitarbeitenden für Phishing? Unser kostenloser Phishing Security Test verrät es Ihnen.

**Kostenloses Automated Security Awareness Program**
Erstellen Sie ein auf Ihr Unternehmen abgestimmtes Security Awareness Program.

**Phish Alert Button (kostenlos)**
Mit diesem Tool können Mitarbeitende ab sofort Phishing-Angriffe mit nur einem Klick sicher melden.

**Email Exposure Check (kostenlos)**
Welche Ihrer E-Mail-Anmeldedaten wurden bereits offengelegt? Werden Sie aktiv, bevor es die Kriminellen tun.

**Domain Spoof Test (kostenlos)**
Finden Sie heraus, ob Hacker E-Mail-Adressen Ihrer Domain spoofen können.


## Über KnowBe4

KnowBe4 ist die weltweit größte integrierte Plattform für Security Awareness Training und Phishing-Simulationen. Der Faktor Mensch wurde bei Sicherheitsschulungen bisher deutlich vernachlässigt. In den umfangreichen KnowBe4-Programmen werden Mitarbeitende über die fortlaufenden Gefahren von Social Engineering aufgeklärt und erfahren, wie sie ihr Unternehmen schützen können.

Der neue Ansatz kombiniert elementare Tests auf Basis realer Angriffsszenarien, kurzweilige interaktive Trainings, kontinuierliches Assessment anhand von Simulationen sowie aussagekräftige Reports, um Unternehmen durch sicherheitsbewusstes Handeln besser vor tatsächlichen Angriffen zu schützen.

Weltweit nutzen Zehntausende von Unternehmen aus unterschiedlichsten Branchen – darunter auch stark reglementierte Bereiche wie das Finanzwesen, das Gesundheitswesen, die Energiebranche, die öffentliche Verwaltung und das Versicherungswesen – die KnowBe4-Plattform, um Nutzer:innen in die Lage zu versetzen, kompetente Entscheidungen hinsichtlich Cybersicherheit zu treffen.

**Weitere Informationen finden Sie auf www.KnowBe4.de.**

KnowBe4
Human error. Conquered.

KnowBe4 Germany | Rheinstr. 45/46 | 12161 Berlin – Deutschland | knowbe4.de |
Tel.: +49 30 34 64 64 60 | E-Mail: kontakt@knowbe4.com

04D03K01