

AUSGABE 2023

# Echte Verhaltens- änderungen erreichen

Leitfaden für den Aufbau eines effektiven  
Programms zur Sensibilisierung für Sicherheit



# Der Mensch steht im Mittelpunkt aller Cybersicherheitsmaßnahmen

Die größte Cyberbedrohung geht heutzutage nicht von Zero-Day-Schwachstellen, neuer Malware oder aktuellen Exploit-Kits aus, sondern von den Anwendern in Ihrem Unternehmen.

Heutige Angriffe zielen auf die menschliche Schwachstelle ab, nicht auf IT-Infrastruktur. Fakt ist: Die meisten Cyberangriffe werden erst durch das mehrheitlich arglose Handeln eines im Unternehmen tätigen Anwenders zum Erfolg. So werden Mitarbeiter zum Beispiel dazu verleitet, schädliche Anhänge auszuführen, auf unsichere Links zu klicken, Anmeldedaten in gefälschte Formulare einzugeben oder gar selbst aktiv zu werden, indem sie etwa Geld überweisen oder vertrauliche Daten weiterleiten.

## Warum Anwenderschulungen so wichtig sind

Laut dem Verizon Data Breach Investigations Report 2022 gehen 82 % aller Datenschutzverletzungen mit einer menschlichen Komponente einher. In diesem Bericht heißt es: „Malware und gestohlene Anmeldedaten sind ein lohnenswerter zweiter Schritt, sobald ein Angreifer per Social Engineering einen Fuß in die Tür bekommen hat. Das zeigt, wie wichtig ein wirkungsvolles Programm zur Sensibilisierung für Sicherheit ist.“<sup>1</sup>

Security-Awareness-Schulungen gehören zu den wichtigsten Maßnahmen, mit denen Sie die Sicherheit in Ihrem Unternehmen verbessern können. Wenn Sie Ihre Anwender zur Erkennung, Vermeidung und Meldung von Phishing-Versuchen schulen, können Sie eine starke letzte Verteidigungslinie gegen die größten aktuellen Cyberbedrohungen schaffen.

## Das bietet dieser Leitfaden

Ein neues Schulungsprogramm auf den Weg zu bringen, mag zunächst wie eine Mammutaufgabe wirken. Wenn Ihr Ziel zudem darin besteht, Ihre Anwender zur engagierten Mitarbeit zu motivieren und ihr Verhalten nachhaltig zu ändern, damit Ihr Unternehmen besser vor Bedrohungen geschützt ist, liegt die Messlatte noch einmal ein Stück höher.

Wir helfen Ihnen dabei.

Dieser Leitfaden zeigt auf, wie Sie ein nachhaltiges, effizientes und effektives Schulungsprogramm für Cybersicherheit auf die Beine stellen – unabhängig davon, wie ausgereift Ihr derzeitiges Schulungsangebot ist, mit welchem Anbieter Sie zusammenarbeiten und welche Hürden es zu überwinden gilt. In unserem Leitfaden erhalten Sie die wichtigsten Fakten, effektive Strategien, wertvolle Materialien und Praxistipps für Sicherheitsverantwortliche. Dabei werden alle Phasen des Wegs zu mehr Sicherheitsbewusstsein abgedeckt.

Hier finden Sie Antworten auf diese Fragen:

- Wie erhalte ich in meinem Unternehmen die benötigte Unterstützung? Mit wem arbeite ich intern zusammen?
- Was ist zu tun – und wie oft?
- Wie spreche ich die Anwender an?
- Wie kann ich den Erfolg einschätzen und präsentieren?

**82 %**

der Datenschutzverletzungen gehen mit einer menschlichen Komponente einher<sup>1</sup>

<sup>1</sup> Verizon: „2022 Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen 2022), Juni 2022.

## Ein personenzentriertes Modell zur Bewertung und Verringerung von Anwenderrisiken

So wie jeder Mensch einzigartig ist, ist auch sein Wert für die Cyberangreifer individuell – und damit das Risiko, das er für Ihr Unternehmen darstellt. Wir von Proofpoint haben das Very Attacked People (VAP)<sup>TM</sup>-Modell entwickelt, mit dem wir die drei verschiedenen Aspekte von Anwenderrisiken für besonders häufig angegriffene Personen messen und minimieren.

Bei Security-Awareness-Schulungen geht es vor allem darum, die Anfälligkeit der Anwender zu reduzieren. Ihr Schulungsprogramm sollte jedoch auch die Angriffsprofile und Berechtigungen Ihrer Anwender berücksichtigen. Der personenzentrierte Ansatz zur Sensibilisierung Ihrer Anwender sollte maßgeschneiderte, proaktive Schulungen sowie zielgerichtete Nachschulungen umfassen.

V

### Vulnerability

(Schwachstelle)

Dieser Aspekt bemisst, mit welcher Wahrscheinlichkeit Anwender aufgrund ihrer Anfälligkeit für die Taktiken von Angreifern oder ihres eigenen risikoreichen Verhaltens Opfer von Angriffen werden. Dies lässt sich durch Wissenstests, Quizfragen innerhalb der Schulungsinhalte sowie simulierte Phishing-Angriffe messen.

A

### Attack Profile

(Angriffsprofil)

Dieser Aspekt berücksichtigt den Umfang und die Raffinesse des gegen Anwender gerichteten Angriffs. Hier können auch Beziehungen zu anderen Anwendern innerhalb und außerhalb eines Unternehmens in die Bewertung einfließen.

P

### Privilege

(Berechtigungen)

Dieser Aspekt bemisst Wert und Vertraulichkeitsgrad von Daten, Systemen und Ressourcen, zu denen Anwender Zugang haben. Damit wird das Schadenspotenzial eines gegen bestimmte Anwender gerichteten Angriffs bemessen.

## Inhaltsverzeichnis

<b>1</b>	Das müssen Sie wissen, bevor Sie loslegen . . . . .	5
<b>2</b>	Die zeitliche Planung . . . . .	8
<b>3</b>	Warum ist die Mitarbeit der Anwender so wichtig . . . . .	13
<b>4</b>	Ohne Daten geht es nicht . . . . .	18
<b>5</b>	Die richtigen Kennzahlen: Erfolg ist messbar . . . . .	23
<b>6</b>	Über Schulungen hinaus: Aufbau einer Sicherheitskultur . . . . .	27
<b>7</b>	Schlussfolgerungen und Empfehlungen . . . . .	32

## ABSCHNITT 1

# Das müssen Sie wissen, bevor Sie loslegen

Sie haben es geschafft. Der Vertrag ist unterschrieben und Sie können endlich starten. Ihr neuer Anbieter für Sicherheitsschulungen schickt Ihnen einen Link für Ihre Software und Sie können loslegen. Sie sind bereit, simulierte Phishing-Angriffe zu starten, Daten zu erfassen, Schulungen zuzuweisen und überhaupt all die spannenden Funktionen und Inhalte zu nutzen, die Sie in den Demos gesehen haben.

Sie informieren Ihre User also, dass Sie demnächst ein Programm zur Sensibilisierung für Sicherheit starten werden. Prompt quillt Ihr Posteingang über:

- „Wer hat das genehmigt?“
- „Da muss ich erst mal meinen Chef fragen.“
- „Muss ich daran unbedingt teilnehmen?“

Das sind die üblichen Hürden, mit denen sich unsere Kunden gleich zu Beginn herumschlagen müssen. Gleichzeitig zeigt sich damit, dass Sie einen wichtigen ersten Schritt bewältigen müssen, damit Ihr Programm zur Sensibilisierung für Sicherheit zum Erfolg werden kann: Sie benötigen die aktive Mitarbeit der Anwender.





Immer wieder hören wir von Kunden, dass sich einige Anwender weigern, sich an Sicherheitsschulungen zu beteiligen.

## Die Anwender auf Ihre Seite bringen

Immer wieder hören wir von Kunden, dass sich einige Anwender weigern, sich an Sicherheitsschulungen zu beteiligen. Möglicherweise fühlen sich einige Anwender durch simulierte Angriffe bloßgestellt, während andere die Schulungen als lästige Pflicht empfinden, die sie von ihrer „echten Arbeit“ abhält.

Deshalb hier einige Vorschläge dazu, wie Sie diese Hürde überwinden können:

**Machen Sie den Nutzen für den Einzelnen deutlich.** Wenn Sie Nachrichten an Ihre Anwender verfassen, bedenken Sie, dass diese sich wahrscheinlich fragen: „Und was habe ich davon?“ Liefern Sie daher konkrete und echte Beispiele für Identitätsdiebstahl, gestohlene Kreditkartendaten, kompromittierte Konten usw. und machen Sie deutlich, dass die Teilnehmer auch privat von der Schulung profitieren. Dadurch bekommen Anwender eher einen Bezug zur Schulung und die Schulung mehr Zuspruch.

**Finden Sie die richtige Balance zwischen Tests und Schulung.** Simulierte Phishing-Angriffe sind ein beliebter Programmteil, sollten allerdings nicht übermäßig eingesetzt werden. Von vielen Kunden bekommen wir die Rückmeldung, dass sich Tests, Schulungen und Sensibilisierungsmaßnahmen die Waage halten müssen. Ein Kunde sagte zum Beispiel: „Wenn ich ständig nur Phishing-Angriffe starte, glauben die Anwender irgendwann, wir wollen sie austricksen.“ Sie sollten Ihr Programm also möglichst ausgewogen gestalten und immer wieder auch Aktivitäten wie kleine Wettbewerbe einbauen.

**Stellen Sie sich auf Firmenveranstaltungen vor.** Computer-basierte Tests und Schulungen wirken oft unpersönlich. Ein eigener „Cybersecurity“-Stand auf einem Firmen-Event oder virtuelle Treffen schaffen hingegen eine persönlichere Verbindung. Fangen Sie mit einer Auftaktveranstaltung für Mitarbeiter an, bieten Sie Kurse an und stellen Sie weiterführendes Material bereit. Verteilen Sie kleine Geschenke oder geben Sie zumindest einen Kaffee aus. Auf diese Weise wird das neue Schulungsprogramm mit einem freundlichen menschlichen Gesicht und einem Namen assoziiert.

## Widerstände abbauen

Aus Gesprächen mit unseren Kunden wissen wir, dass sich Schulungsverweigerer grundsätzlich in zwei Gruppen unterteilen lassen.

- **Wiederholungstäter:** Anwender, die wiederholt auf Phishing-Simulationen hereinfliegen oder andere Tests nicht bestehen
- **Nichtteilnehmer:** Anwender, die sich der Teilnahme an Schulungen verweigern

Sie haben wahrscheinlich schon alles Mögliche versucht, um diese Personen zu erreichen: E-Mails, ein informeller Plausch, ein offizielles Gespräch mit Vorgesetzten oder sogar Entzug von Netzwerkzugangsrechten. Wenn all das noch keine Verhaltensänderung bewirkt, ist trotzdem noch nicht aller Tage Abend.

Einer unserer Kunden versuchte es beispielsweise mit einem 15-minütigen Termin zwischen dem betreffenden Anwender und dem CISO des Unternehmens. Dabei wurden folgende Themen angesprochen:

- Warum sind Anwenderverhalten und Sicherheitsbewusstsein so wichtig?
- Wie versucht die IT-Sicherheitsabteilung, das Unternehmen zu schützen und welche positiven Konsequenzen hat das für jeden einzelnen Mitarbeiter?
- Welche Vorteile erhält der betreffende Mitarbeiter, wenn er wachsamer wird und an einer Schulung teilnimmt?

Solche Interaktionen machen einen starken Eindruck. Sie machen auf persönliche, greifbare Weise deutlich, wie wichtig es ist, sich korrekt zu verhalten und mitzuziehen.

## Von Anwendern gemeldetes Phishing: Ein zweiseitiges Schwert

Auf einer unserer jährlichen Konferenzen gab es nach einer Präsentation folgende Wortmeldung:

„Bei uns werden Phishing-E-Mails einfach nicht an das Abuse-Postfach gemeldet. Immer heißt es, es handele sich entweder um Spam oder um wirklich erwünschte Nachrichten. Unser Team kommt gar nicht nach. Wie sollen wir vorgehen?“

Abuse-Postfächer, an die potenzielle Phishing-Nachrichten gemeldet werden können, sind eine hervorragende Möglichkeit, um das Risiko zu minimieren. Die Verwaltung ist jedoch recht zeitaufwändig. Für dieses häufig auftretende Problem haben wir zwei Lösungen gefunden:

- Unterstützen Sie Ihre Anwender dabei, echte Phishing-E-Mails zu erkennen.
- Automatisieren Sie die Analyse und Reaktion auf gemeldete Phishing-E-Mails.

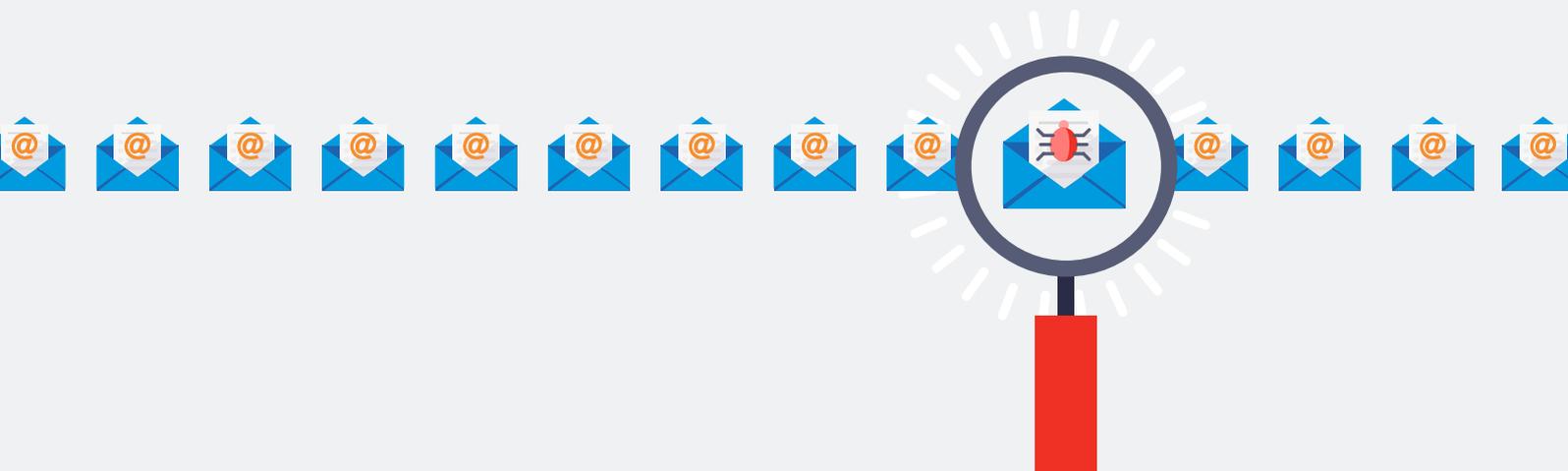
Ein effektives Programm zur Sensibilisierung für Sicherheit zieht in der Regel auch eine Verbesserung bei der Qualität der Meldungen nach sich. Bei vielen Kunden stellt sich die Verbesserung der Meldungen – mehr echte schädliche Nachrichten und weniger False Positives – etwa sechs bis zwölf Monate nach der Einführung eines kontinuierlichen Schulungsprogramms zur Identifizierung von Phishing-E-Mails ein.

Wenn E-Mails mittels Sandbox-Analysen automatisiert ausgewertet, mit Bedrohungsdaten unterfüttert und beantwortet werden, kann das den Arbeitsaufwand erheblich verringern. Das reduziert den Mehraufwand für die IT erheblich, da schädliche Inhalte automatisch aus den Posteingängen der Anwender entfernt werden können.

Ein weiterer Vorteil automatisierter Incident Response besteht darin, dass die Anwender individuelles Feedback erhalten können und so erfahren, ob die von ihnen gemeldete Nachricht wirklich schädlich war. Dieser Schritt trägt zur weitergehenden Schulung der Anwender bei und verbessert die Sicherheit zusätzlich, indem positives Verhalten mit einem einfachen Dankeschön für die Meldung tatsächlich schädlicher E-Mails verstärkt wird.



Ein effektives Programm zur Sensibilisierung für Sicherheit zieht in der Regel auch eine Verbesserung bei der Qualität der Meldungen nach sich.



## ABSCHNITT 2

# Die zeitliche Planung

Die Zeitplanung ist kein isoliertes Detail Ihres Security-Awareness-Schulungsprogramms, sondern die Summe all Ihrer Bemühungen. Die richtige Schulung, die richtigen Personen und viele andere taktische, organisatorische und strategische Elemente ergeben im Gesamtergebnis den buchstäblich „richtigen Zeitpunkt“.

Jedes Unternehmen ist einzigartig und kein Schulungsprogramm ist wie das andere. Folgende Punkte sollten allerdings unbedingt in Ihr Schulungsprogramm einfließen:

- Definition des Schulungsbedarfs
- Identifizierung von Anwendern mit speziellem Schulungsbedarf
- Definition der Aktivitäten
- Erstellung und Verwaltung von Zeitplänen
- Test und Kommunikation der ersten Schritte
- Definition von Häufigkeit und Zeitplanung der Programmaktivitäten



## Empfohlene Reihenfolge der Aktivitäten: Eine Checkliste



Ein zentraler Grundsatz der personenzentrierten Cybersicherheit lautet: Jeder Anwender ist anders.

Je mehr Sorgfalt und Planung Sie in Ihr Programm fließen lassen, desto erfolgreicher wird es letztlich werden. Folgende Schritte haben sich dabei für unsere Kunden als hilfreich erwiesen.

### 1. Definition des Schulungsbedarfs

Personenzentrierte Cybersicherheit beginnt mit einer Bewertung der Anwenderrisiken. Über **Anwendertests** erfahren Sie, in welchen Bereichen Anwender möglicherweise besonders anfällig sind – und welche Schulungsaufgaben sie benötigen, um ihre Kenntnisse zu wichtigen Themen wie Phishing, Datenschutz, mobile Sicherheit usw. zu verbessern.

Risiken existieren nicht im luftleeren Raum. Erst wenn Sie die aktuelle Bedrohungslage kennen, können Sie die richtigen Schulungsschwerpunkte setzen. Hier kommen **Bedrohungsdaten** ins Spiel. Mithilfe realer Bedrohungsdaten verstehen Sie, welche aktuellen und aufkommenden Bedrohungen sich gegen Ihre Anwender richten.

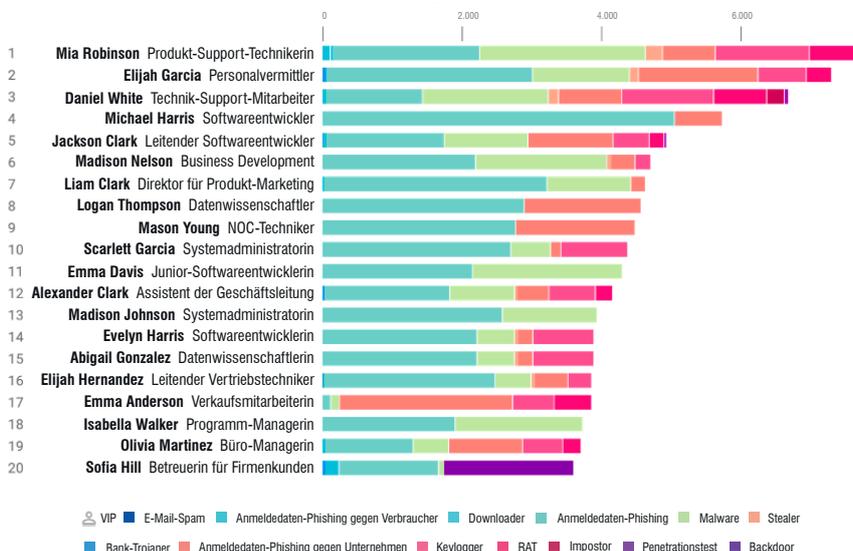
### 2. Identifizierung von Anwendern und Gruppen, die möglicherweise anders getimte oder maßgeschneiderte Schulungen benötigen

Ein zentraler Grundsatz der personenzentrierten Cybersicherheit lautet: Jeder Anwender ist anders. Einheitsschutz funktioniert in der heutigen Welt nicht mehr – und das gilt auch für Programme zur Sensibilisierung für Sicherheit.

Diese Gruppen benötigen eventuell maßgeschneiderte oder themenspezifische Schulungen:

- **VAPs:** Diese Anwender sind stärker gefährdet als andere, weil sie etwa für die Taktiken von Cyberangreifern besonders anfällig oder besonders oft Ziel von Angriffen sind oder Zugriffsrechte für wertvolle Daten, Systeme oder Ressourcen haben.

Ein VAP-Bericht in Proofpoint Targeted Attack Protection



- **VIPs:** Das sind die oberste Führungsebene, Vorstand, Aufsichtsrat und andere Führungskräfte, die aufgrund ihrer Bedeutung für das Unternehmen eine spezifische Schulung und Anleitung benötigen. Viele VIPs sind zugleich VAPs.
- **Führende Positionen und Abteilungen:** Das sind Anwender aus der Personalabteilung, der Finanzabteilung, der Rechtsabteilung, der Compliance, der Entwicklung oder andere Mitarbeiter, für die bestimmte Schulungen zum Teil sogar gesetzlich vorgeschrieben sind. Im weiteren Verlauf Ihres Schulungsprogramms sollten Sie für diese Gruppen verschiedene Wissenstests und Simulationen in Erwägung ziehen.

### 3. Definition wichtiger Programmaktivitäten

Ein erfolgreiches Schulungsprogramm besteht aus der richtigen Mischung aus Tests, Schulung, ergänzendem Material, Kommunikation sowie Präsenz- und virtuellen Aktivitäten. Diese Punkte sollten Sie dabei in Erwägung ziehen:

- Tests, mit denen Sie den Wissensstand und eventuelle Schwachstellen der Anwender ermitteln, z. B. Wissenstests sowie simulierte Phishing-, USB- und Smishing-Angriffe.
- Computer-basierte Schulungen auf Grundlage des Bedarfs der Anwender und der aktuellen Bedrohungslage.
- Aktivitäten zur Sensibilisierung (Poster, Webinare, Newsletter, Videos), mit denen Sie die Konzepte vorstellen und die zentralen Botschaften untermauern.
- Präsenzveranstaltungen wie informelle „Lunch&Learn“-Angebote oder virtuelle Aktivitäten wie Webinare. Werden Sie kreativ. Einige unserer Kunden waren zum Beispiel mit Escape Rooms für Cybersicherheit äußerst erfolgreich.

### 4. Test und Kommunikation der ersten Schritte

Für viele Unternehmen stellt eine umfassende Anwenderschulung eine große Veränderung dar. Fangen Sie deshalb lieber mit einer kleinen Gruppe an, um die Kinderkrankheiten auszumerzen. Geben Sie allen Beteiligten früh und oft Informationen zu den ersten Schritten. Sorgen Sie dafür, dass es möglichst wenige Überraschungen gibt.

#### *Zwei Monate vor Beginn*

Schicken Sie einer kleinen Gruppe von „Eingeweihten“ eine Phishing-Simulation als Test, um technische Probleme aufzudecken. Senden Sie dann einen mittelschweren Phishing-Test an alle Mitarbeiter.

In dieser Phase genügt es, wenn Sie alle, die auf den Phishing-Köder hereinfallen, auf eine 404-Fehlerseite weiterleiten („Seite nicht gefunden“). (In späteren Phasen können Sie diese Anwender an eine Landing Page weiterleiten, die auf das Phishing-Problem hinweist.)

#### *Ein Monat vor Beginn*

Kündigen Sie das Programm an. Wenn Sie beabsichtigen, die [Schaltfläche zum Melden von Phishing-E-Mails](#) direkt im E-Mail-Client zu implementieren, erklären Sie den Zweck und die Bedienung. Wenn Ihnen Poster, Bilder oder ähnliches Material zur Verfügung stehen, verteilen Sie es im Büro oder stellen Sie es im Intranet zur Verfügung.

### 5. Definition von Häufigkeit und Zeitplanung der Programmaktivitäten

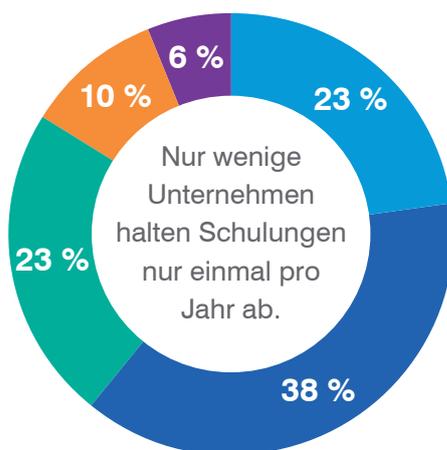
Auch hier gilt: Richtiges Timing ist entscheidend. Wir empfehlen für Ihre Sensibilisierungsaktivitäten folgende Reihenfolge:

- Senden Sie alle vier bis sechs Wochen einen Phishing-Test und wechseln Sie dabei immer wieder Themen und Köder.
- Melden Sie Anwender mindestens einmal pro Vierteljahr bei einem Phishing-Test an. Setzen Sie je nach Art des gestarteten Angriffs ein zielgerichtetes Modul zur Folgeschulung ein.
- Überprüfen Sie die VAP-Berichte monatlich, spätestens aber alle zwei Monate. Entscheiden Sie anhand dieser Berichte, wer zielgerichtete Schulungen erhalten sollte und welche Inhalte dafür zum Einsatz kommen sollten.
- Setzen Sie mindestens vierteljährlich unternehmensweite Schulungen an.
- Wiederholen Sie die allgemeinen Wissenstests und Phishing-Tests mindestens einmal jährlich und vergleichen Sie die neuen Ergebnisse mit denen der ersten Tests.
- Um das Gelernte zu festigen, setzen Sie mindestens zweimal im Jahr Aktivitäten zur Sensibilisierung für Sicherheit an. Das können Webinare, Wettbewerbe oder auch (falls möglich) Präsenzveranstaltungen sein.

Erstellen Sie einen Rahmenplan für die jährlichen Schulungsaktivitäten. Bleiben Sie dabei flexibel und passen Sie die Termine der jeweiligen Bedrohungslage an.

Aus unserem [State of the Phish-Bericht 2020](#) geht hervor, dass Security-Awareness-Schulungen längst nicht mehr nur jährlich oder vierteljährlich stattfinden, sondern inzwischen eher alle zwei Monate, wenn nicht gar monatlich. Wir empfehlen, Schulungen (einschließlich gezielte Schulungen, Sensibilisierungskampagnen und Wissenstests) mindestens einmal im Monat durchzuführen.

#### Häufigkeit von Security-Awareness-Schulungen



- Zweimal im Monat
- Einmal im Quartal
- Einmal im Jahr
- Einmal im Monat
- Zweimal im Jahr

Quelle: State of The Phish 2020

## Wann Änderungen notwendig sind



Die Bedrohungslandschaft entwickelt sich ständig weiter. Deshalb muss auch Ihr Programm zur Sensibilisierung für Sicherheit auf Kontinuität ausgelegt sein.

Die Bedrohungslandschaft entwickelt sich ständig weiter. Deshalb muss auch Ihr Programm zur Sensibilisierung für Sicherheit auf Kontinuität ausgelegt sein. Ausgehend von den ersten Testergebnissen – der Startlinie, wenn Sie so möchten – können Sie anhand nachfolgender Tests feststellen, wie sich die Kenntnisse der Anwender weiterentwickeln, und die weitere Vorgehensweise entsprechend anpassen.

Es gibt allerdings Situationen, die eine Änderung der Häufigkeit oder Reihenfolge der Schulungsaktivitäten erfordern. Dazu gehören:

- **Bestimmte Anwenderbedrohungen nehmen überhand oder Angreifer setzen auf bestimmte Marken oder Köder.** Ändern Sie die Inhalte der Tests (z. B. die Vorlagen für simulierte Phishing-Kampagnen) oder verwenden Sie bedrohungsgesteuerte Schulungsinhalte, um das Risiko zu verringern.
- **In Ihrem Unternehmen kommt es zu einem Zwischenfall, zum Beispiel zu einer Datenschutzverletzung.** In diesem Fall sollten Sie Ihre geplanten Aktivitäten und die Häufigkeit der Kommunikation, Tests und Schulungen in Bezug auf diesen konkreten Zwischenfall überdenken.
- **Es treten neue Gesetze oder Vorschriften in Kraft, die mehr Schulungen vorschreiben.** Stellen Sie mit einem angepassten Wissenstest fest, wie gut die Anwender die Schulungsinhalte behalten haben.
- **Ihr Unternehmen veröffentlicht oder aktualisiert eine Richtlinie oder es kommen Zweifel daran auf, dass die Anwender eine bestehende Richtlinie kennen.** Starten Sie einen angepassten Wissenstest, um Lücken im Wissen der Anwender zu identifizieren und die Schulungen entsprechend anzupassen.
- **Ein Programm zur Sensibilisierung für Sicherheit wurde über einen Zeitraum von mehr als einem halben Jahr ausgesetzt.** In diesem Fall kann es sinnvoll sein, das Programm noch einmal von vorne zu beginnen, damit die Teilnehmer Zusammenhang und Bedeutung verstehen.

Wir empfehlen, die Häufigkeit der Schulungen nicht zu sehr zu erhöhen – auch nicht bei Wiederholungstätern, die bei Tests schlecht abschneiden. Monatliche Phishing-Tests und die gezielte Zuweisung von „durchgefallenen“ Anwendern zu einer einzigen Schulung ist ein vernünftiger, zielgerichteter Ansatz. Wenn Sie diesen Anwendern stattdessen vier Schulungseinheiten zuweisen, könnten sie die Maßnahme als Strafe empfinden und das Programm ablehnen.

Versuchen Sie vor allem nicht, alles auf einmal zu schaffen. Beginnen Sie im Vorfeld mit einer gründlichen Analyse, die sich auf Bedrohungsdaten und Tests stützt. Erstellen Sie anschließend einen realistischen Plan, der von allen Mitarbeitern akzeptiert wird.



### ABSCHNITT 3

# Warum ist die Mitarbeit der Anwender so wichtig

Es gibt sicher keinen Zweifel daran, dass bei Security-Awareness-Schulungen immer der Mensch im Mittelpunkt steht. Die Schulungen sollen Menschen in die Lage versetzen, gegen sie gerichtete Angriffe zu erkennen und ihr Verhalten zu ändern.

Deshalb kann das Programm nur erfolgreich sein, wenn die Anwender mitmachen. Auch ein mit der besten Absicht erstelltes Programm wird als anstrengend wahrgenommen, wenn die Inhalte nicht wertvoll und relevant sind.





Bedenken Sie: Ihr Programm ist nur dann erfolgreich, wenn Ihre Anwender es akzeptieren und annehmen.

### Erfolgreiche Programme zeichnen sich durch Folgendes aus:

- Sie haben einen Namen, der ihre Relevanz verdeutlicht.
- Sie wenden wissenschaftlich bestätigte Lernprinzipien an, um Verhaltensänderungen zu bewirken.
- Sie festigen die Schulungsinhalte mit einer abwechslungsreichen Mischung aus Inhalten und Medien.
- Sie haben mehrere Fürsprecher im ganzen Unternehmen, die Unterstützung und Verbesserungsvorschläge bieten.
- Sie setzen auf eine ausgewogene Mischung aus Anreizen und Konsequenzen.

Ein erfolgreiches Programm, das Ihre Anwender schätzen werden, ruht auf diesen fünf Säulen. Kunden aus einer Vielzahl von Branchen nutzen diese Konzepte, um Security-Awareness-Schulungsprogramme zu entwickeln, die Risiken verringern, Kosten senken und die Einhaltung der Datenschutzvorgaben unterstützen.

## Dem Programm einen Namen geben

Mit dem richtigen Namen ist sofort klar, worum es in Ihrer Security-Awareness-Schulung geht und warum das Programm für die Teilnehmer relevant ist.

Wenn die Mitarbeiter Ihres Unternehmens beispielsweise zur Einhaltung der Datenschutzgrundverordnung (DSGVO) Kundendaten aus der Europäischen Union mit äußerster Vorsicht behandeln müssen, ruft ein Name wie „DSGVO-Schulung“ nicht unbedingt positive Emotionen hervor, die für eine Verhaltensänderung benötigt werden.

Besser klingt da schon: „Werden Sie zum Verteidiger des Datenschutzes!“ Der Titel unterstreicht deutlich den Zweck des Programms (Datenschutz) und die Rolle des Anwenders (aktiver Beitrag zum Datenschutz).

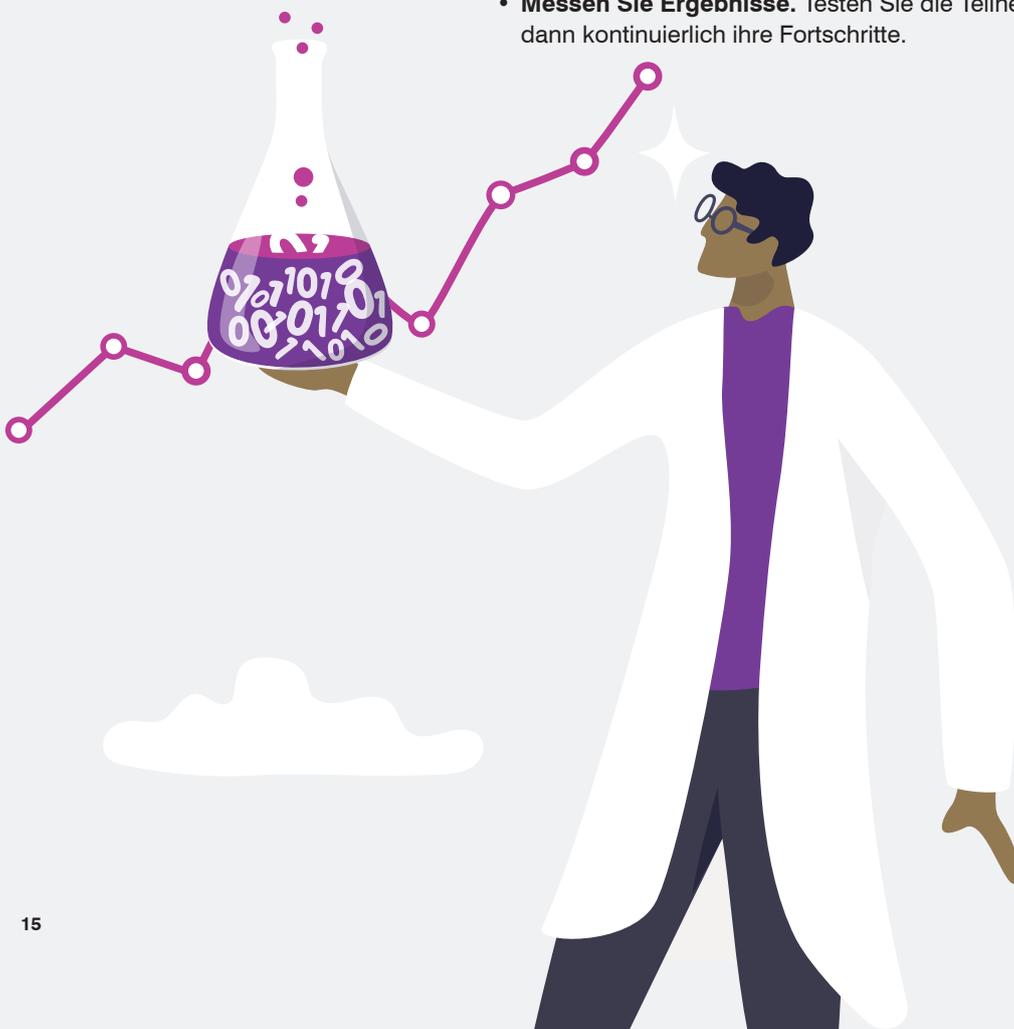
Wenn Ihre Unternehmenskultur eine direktere Herangehensweise mit eher praktisch orientierten Themen vorgibt, ist die Benennung Ihrer Programme nach bestimmten Themen (Phishing, Social Engineering, E-Mail, Arbeit im Homeoffice usw.) bereits eine Verbesserung.



## Wissenschaftlich bestätigte Lernprinzipien anwenden

In der Wissenschaft wird seit Jahrzehnten erforscht, wie man effektiv lernt, Gelerntes vertieft und Verhaltensänderungen bewirkt. Diese Erkenntnisse sollten sich in Ihrem Programm widerspiegeln. Ein gut ausgearbeitetes Programm vermittelt sowohl theoretisches als auch praxisorientiertes Wissen. Dazu erhalten die Teilnehmer zunächst einen allgemeinen Überblick und anschließend spezifische Lektionen. Folgende Vorgehensweisen haben sich bewährt:

- **Servieren Sie mundgerechte Häppchen.** Schulungen sollten sich eher in Minuten als in Stunden bemessen lassen und so oft wie möglich nur ein Thema behandeln.
- **Festigen Sie das Gelernte.** Geben Sie Rückmeldung, halten Sie die Aufmerksamkeit für die Schulungsinhalte aufrecht und führen Sie die Schulungen regelmäßig durch.
- **Schulen Sie im Kontext.** Ihre Schulungen sollten sowohl in Bezug auf die Bedrohungen als auch die Position der Anwender im Unternehmen relevant sein.
- **Geben Sie sofort Rückmeldung.** Geben Sie die Ergebnisse von Schulungen oder Phishing-Übungen zeitnah bekannt.
- **Lassen Sie die Teilnehmer das Tempo bestimmen.** Jeder ist ein Individuum und lernt unterschiedlich schnell.
- **Erzählen Sie eine Geschichte.** Bringen Sie konkrete Beispiele.
- **Variieren Sie die Botschaft.** Achten Sie darauf, dass zu den Themen verschiedene Inhalte verfügbar sind, die sich in ihren Formulierungen unterscheiden.
- **Binden Sie die Teilnehmer ein.** Interaktive Inhalte und Übungen sorgen dafür, dass Gelerntes besser behalten wird.
- **Bringen Sie die Teilnehmer zum Nachdenken.** Übungen sollten zeigen, wie gut Teilnehmer ihr Wissen anwenden können.
- **Messen Sie Ergebnisse.** Testen Sie die Teilnehmer im Vorfeld und verfolgen Sie dann kontinuierlich ihre Fortschritte.



## Durch Abwechslung bleibt die Schulung interessant

In der Werbung gibt es eine „7-Kontakte-Regel“, der zufolge eine Botschaft siebenmal beim Adressaten ankommen muss, ehe sie haften bleibt. Beim Lernen ist es ähnlich.

Unabhängig davon, welche Lösung Sie für Ihre Security-Awareness-Schulungen nutzen, die Lerninhalte sollten über unterschiedliche Kanäle und Aktivitäten vermittelt werden. Hier einige Beispiele für Aktivitäten und Kanäle, die Sie dazu nutzen können:

AKTIVITÄTEN	KANÄLE
Angriffssimulationen (Phishing, USB, SMS usw.)	Tools zur Sensibilisierung für Sicherheit
Wissenstests	Tool zur Sensibilisierung für Sicherheit oder Umfrage-Tool
Identifizieren und Überwachen der VAPs	Bedrohungsdaten/E-Mail-Gateway
Computer-basierte Schulungen	Module für Security-Awareness-Schulungen über eine Online-Plattform oder andere Learning-Management-Systeme (LMS)
Sensibilisierungskampagnen	Poster, Videos, Podcasts, Webinare, Gastredner, Infografiken
Sensibilisierungs- und Schulungsübungen als virtuelle Events oder Präsenzveranstaltungen	Lunch&Learn-Angebote, Webinare, Stände auf Firmenveranstaltungen, Präsentationen auf Firmen-Events, Präsenzs Schulungen, Escape Room-Aktionen
Wettbewerbe/Spiele	Anerkennung positiver Verhaltensänderungen über einen bestehenden Unternehmenskanal, z. B. Newsletter oder Intranet
Informationen zur Sensibilisierung für Sicherheit	Unternehmens-Wiki, Intranet oder gemeinsamer Unternehmenskalender
Aktuelle Informationen zur Sensibilisierung für Sicherheit	Newsletter des Unternehmens, Chat-App-Kanal (z. B. Microsoft Teams und Slack) oder über die Kommunikation anderer Abteilungen
Teilnehmer-Feedback zu den Security-Awareness-Schulungen	Umfragen oder gemeinsamer Posteingang
Phishing-Meldungen von Anwendern	Schaltfläche für den E-Mail-Client oder eigenes Abuse-Postfach

## Andere Abteilungen und Mitarbeiter in wichtigen Positionen mit an Bord holen

IT-Sicherheit, Marketing, Personalabteilung und Führungskräfte können in Ihrem Programm wichtige Funktionen übernehmen. Nutzen Sie deren Kompetenzen zur Unterstützung und Verbesserung Ihres Ansatzes, der Inhalte und der Bereitstellung.

### Hier einige Beispiele dafür, wie andere Abteilungen helfen können:

- Das **IT-Sicherheitsteam** kann Ihnen Inhalte empfehlen, die für Ihre Unternehmensrichtlinien relevant sind (z. B. Kennwörter). Das Team weiß unter Umständen auch, welche Anwender weiter geschult werden müssen, weil sie besonders häufig Ziel von Cyberangriffen sind oder mit vertraulichen Daten zu tun haben.
- Das **Marketingteam** kann helfen, Materialien und Inhalte zur Sensibilisierung so zu gestalten, dass sich darin die Markenelemente Ihres Unternehmens wiederfinden.
- Die **Personalabteilung** kann in Fragen der Organisationsdynamik beraten und Einblicke in die Arbeit mit Führungskräften und Bereichsleitern geben.
- Der **CISO** (oder ein anderes Mitglied der obersten Führungsebene) kann seine Unterstützung deutlich machen und die Bedeutung des Programms betonen.



Wenn Anwender schlecht über die Security-Awareness-Schulung in ihren Unternehmen denken, können sie gleichgültig werden und sich vielleicht sogar dagegen wehren.

## Mit Zuckerbrot und Peitsche zu besserem Verhalten

Wenn Anwender schlecht über die Security-Awareness-Schulung in ihren Unternehmen denken, können sie gleichgültig werden und sich vielleicht sogar dagegen wehren. Bisher haben wir Schritte skizziert, mit denen die Voraussetzungen für ein Programm geschaffen werden können, das gut ankommt und echten Mehrwert besitzt. Bei der Frage nach „Zuckerbrot“ oder „Peitsche“ bevorzugen die meisten unserer Kunden eindeutig das Zuckerbrot.

Doch es kommt immer wieder vor, dass das Zuckerbrot bei ein paar wenigen uneinsichtigen Schulungsteilnehmern nicht zum Erfolg führt. In diesen seltenen Fällen kann ein klares Konsequenzmodell helfen, die Einhaltung der Schulungsrichtlinien zu gewährleisten. Unsere Kunden haben als letztes Mittel beispielsweise zu folgenden Maßnahmen gegriffen:

- Anwender, die dreimal auf simulierte Phishing-E-Mails geklickt hatten, wurden zum Vorgesetztengespräch gebeten, bekamen vorübergehend nur begrenzten Netzwerkzugang oder verloren ihre Zugriffsrechte ganz
- Weitergehende Konsequenzen können sein: Abmahnung durch Personalabteilung, Kürzung bei Gehalt, Boni oder Leistungen, in seltenen Fällen Kündigung

Es hat sich allerdings bewährt, in erster Linie auf Anreize und Bestärkung zu setzen und nur als letztes Mittel zu Konsequenzen zu greifen. Unsere Kunden haben festgestellt, dass allzu viel Härte nur dazu führt, dass die Teilnehmer das Programm insgesamt ablehnen. Wenn Sie allerdings in einer gesetzlich stark regulierten oder besonders sensiblen Branche tätig sind, kommen Sie an der Einführung eines strikten Konsequenzmodells unter Umständen nicht vorbei.

## ABSCHNITT 4

# Ohne Daten geht es nicht

Wenn es Ihnen so geht wie vielen unserer Kunden, können Sie es vermutlich kaum abwarten, simulierte Phishing-Angriffe zu starten.

Es ist jedoch wichtig, von Anfang an einen Plan zu haben. Um die Vorteile (weniger Anwenderrisiken) zu maximieren und die Kosten (Zeitaufwand der Anwender) zu minimieren, sollten Ihre ersten Schritte darin bestehen, grundlegendes Wissen zu vermitteln, die Schwachstellen der Anwender zu verstehen und die Schulung auf die dringendsten Bereiche zu konzentrieren.



Was ist  
**PHISHING?**



Richtig

**61%**



Falsch

**24%**



Weiß nicht

**15%**

- Nur 49 % der Angestellten in den USA beantworteten diese Frage richtig.
- Deutsche Angestellte lagen mit 66 % am häufigsten richtig.

Was ist  
**RANSOMWARE?**



Richtig

**31%**



Falsch

**31%**

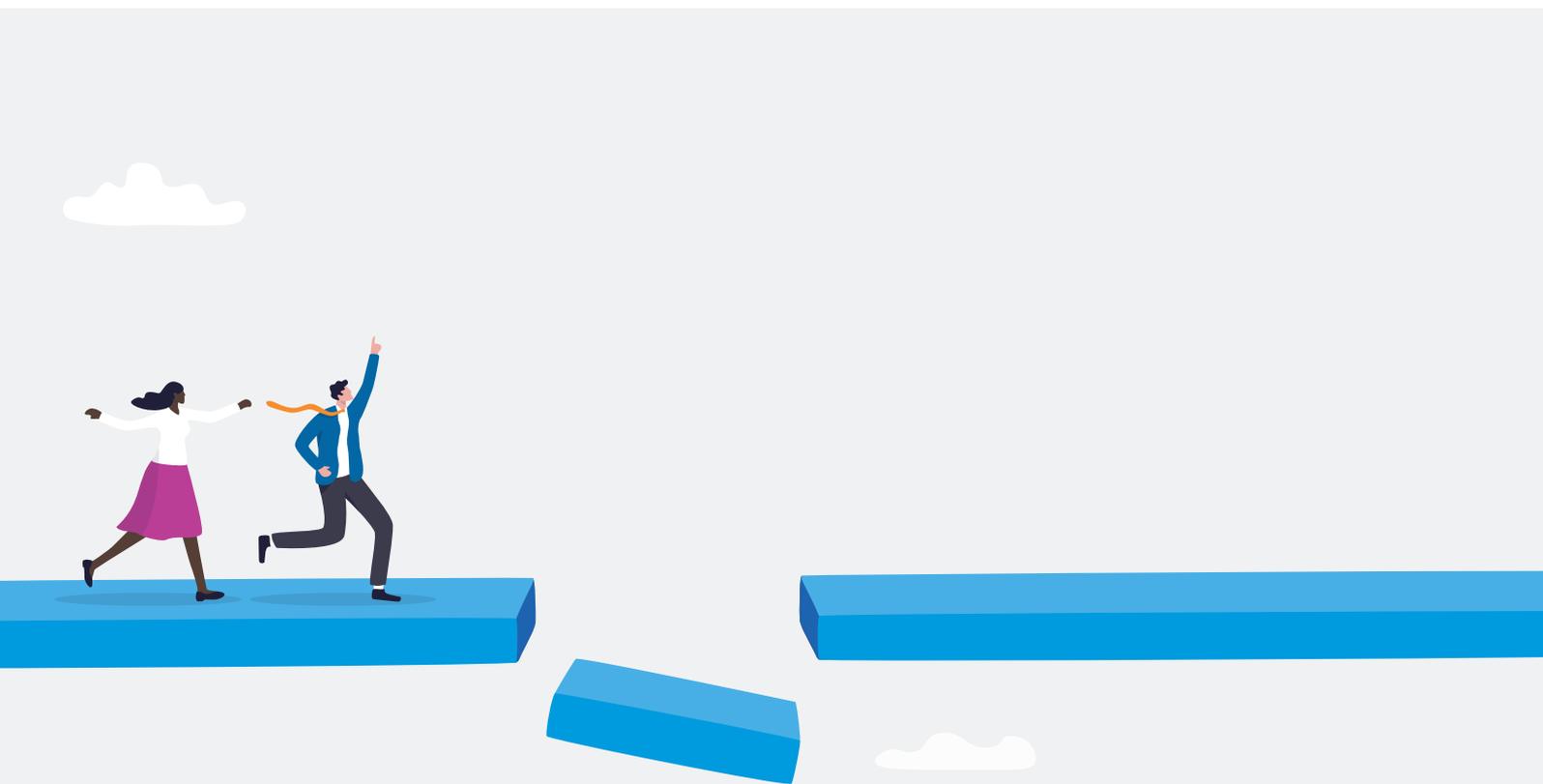


Weiß nicht

**38%**

- Im vergangenen Jahr konnten 45 % der Angestellten in aller Welt diese Frage richtig beantworten. Dieser Rückgang beim Wissen könnte daraus resultieren, dass Ransomware-Angriffe im Jahr 2018 erheblich zurückgingen. Möglicherweise haben Sicherheitsteams dieses Thema deshalb seltener gegenüber den Anwendern thematisiert.

Quelle: State of The Phish-Bericht 2020



## Gefährdete Anwender und VAPs identifizieren

Unter Verwendung des in der Einleitung beschriebenen VAP-Modells sollte Ihr Programm den Anwendern besondere Aufmerksamkeit schenken, die folgende Kriterien erfüllen und daher ein erhöhtes Risiko bergen:

- Sie sind besonders anfällig für die Taktiken von Cyberangreifern.
- Sie sind besonders häufig Ziel von Angriffen.
- Sie haben Zugangsrechte für wertvolle Daten, Systeme oder Ressourcen.

(Siehe „[Ein personenzentriertes Modell zur Bewertung und Verringerung von Anwenderrisiken](#)“ auf Seite 3.)

## Schwachstellen, Angriffe und Berechtigungen bewerten

Zur Identifizierung von Schwachstellen sind simulierte Phishing-Angriffe und Wissenstests unverzichtbar. So erfahren Sie, wer mehr Schulung benötigt, auf welche Taktiken die Anwender bevorzugt hereinfließen und welche Bereiche abzudecken sind.

Mit Blick auf Angriffe müssen Sie wissen, welche Anwender wie und von wem am stärksten ins Visier genommen werden. Dazu benötigen Sie die Bedrohungsdaten Ihres Sicherheitsteams. Wir identifizieren VAPs anhand unseres Attack Index, der sich aus folgenden Faktoren zusammensetzt:

- **Krimineller Akteur:** Gibt an, wie raffiniert der Angreifer ist und wie groß damit die Gefahr für das Unternehmen. Ein staatlich unterstützter Angreifer erhält zum Beispiel einen deutlich höheren Wert als ein Kleinkrimineller.
- **Angriffstyp:** Gibt an, wie gezielt der Angriff ist. War der Angriff auf einen Nutzer zugeschnitten oder wurde er auf breiter Front ausgerollt? War der Angriff auf einen bestimmten Anwender bzw. eine bestimmte Firma, Branche oder Region gerichtet? Oder handelte es sich um eine volle Breitseite, die um die halbe Welt ging? Je gezielter der Angriff erfolgt, desto höher ist der Wert.
- **Bedrohungstyp:** Bei dieser Komponente geht es darum, welche Art von Malware am Angriff beteiligt war. In den meisten Fällen deutet die bei einem Angriff eingesetzte Malware darauf hin, wie gefährlich eine Bedrohung ist und wie viel Aufwand in die Entwicklung dieser Bedrohung gesteckt wurde. So erhalten zum Beispiel ein Remote-Zugriffs-Trojaner (RAT) oder ein Informationsdieb eine höhere Punktzahl als ein Phishing-Versuch, der ganz allgemein auf Anmeldedaten von Verbrauchern aus ist.

Für die Bewertung der Berechtigungen müssen Unternehmen zunächst erfassen, auf welche potenziell wertvollen Daten die Nutzer Zugriff haben bzw. auf welche Systeme sie zugreifen können. Bedenken Sie auch Befugnisse finanzieller Natur (das Recht, Überweisungen vorzunehmen oder Bankdaten zu aktualisieren) oder das Vorhandensein wichtiger Beziehungen im Unternehmen usw.

Die Position des Anwenders im Organigramm ist natürlich ein wichtiger Faktor bei der Bewertung der Berechtigungen. Sie ist jedoch nicht der einzige Faktor – und häufig noch nicht einmal der wichtigste. Wenn der Angreifer auf Wirtschaftsspionage aus ist, sind Assistenten möglicherweise ein interessanteres Ziel als andere Mitarbeiter im mittleren Management, da sie Zugriff auf die Kalender der Chefetage haben. Im Krankenhaus ist die Situation ähnlich: Krankenschwestern mit Zugriff auf Patientenakten sind für Identitätsdiebe eventuell nützlicher als der Vorstandschef.



Durch die Quantifizierung der Anwenderrisiken im Rahmen des VAP-Modells können Sie Ihr Schulungsprogramm passgenau gestalten und Risiken schneller verringern.

### Kennwort-Gewohnheiten



nutzen einen Kennwort-Manager.



wechseln zwischen fünf bis zehn unterschiedlichen Kennwörtern.



geben bei jeder Anmeldung manuell ein anderes Kennwort ein.



verwenden die gleichen ein oder zwei Kennwörter für alle Konten.

Quelle: State of The Phish-Bericht 2020

## VAP-Daten über Schulungen hinaus nutzen

Durch die Quantifizierung der Anwenderrisiken im Rahmen des VAP-Modells können Sie Ihr Schulungsprogramm passgenau gestalten und Risiken schneller verringern. Außerdem liefert das Modell möglicherweise Erkenntnisse darüber, warum Angreifer bestimmte Anwender auswählen. Mit diesen Erkenntnissen können Sie die fraglichen Anwender sowie Anwender mit ähnlichen Positionen besser im Auge behalten und bei Bedarf adaptive Steuerelemente wie die Sperrung von Browser-Aktivitäten oder die Erhöhung der Authentifizierungsanforderungen einsetzen.

Wenn Sie diese Informationen mit Bedrohungsdaten (z. B. den umfassenden Erkenntnissen aus Proofpoint Targeted Attack Protection (TAP)) verknüpfen, können Sie feststellen, ob Anwender überhaupt Ziel schädlicher Inhalte sind.

Es ist hilfreich zu wissen, ob Anwender auf simulierte Phishing-E-Mails klicken. Noch wichtiger ist es zu wissen, ob sie auf echte schädliche Inhalte klicken – selbst wenn dieser Klick ohne Folgen bleibt. Die entsprechenden Daten können potenzielle Sicherheitsrisiken und -lücken offenbaren.

## Nicht nur Phishing: Andere brandgefährliche Bedrohungen

Phishing ist sicher das meistdiskutierte Thema in Security-Awareness-Schulungen. Doch wenn Sie Ihr Programm ausschließlich auf E-Mail-basierte Bedrohungen ausrichten, können sich in anderen wichtigen Themenbereichen große Lücken auf tun.

Erwägen Sie einen breit angelegten Wissenstest, um die Kenntnisse der Anwender zur Cybersicherheit und zu den Richtlinien oder Vorgaben Ihres Unternehmens besser zu verstehen.

In unserem [State of the Phish-Bericht 2020](#) zeigten sich verschiedene gefährliche Verhaltensmuster. Hier nur einige der Ergebnisse:

- 45 % der berufstätigen Erwachsenen geben zu, dasselbe Kennwort für mehrere Konten zu verwenden.
- Lediglich 49 % verschlüsseln den Zugang zu ihrem heimischen WLAN-Netzwerk mit einem Kennwort.
- 26 % glauben, dass die Verwendung eines kostenlosen WLAN-Netzwerks an einem vertrauenswürdigen Ort (z. B. einem Café oder Flughafen) sicher ist.
- 17 % sind sich nicht sicher, ob Open-Access-Netzwerke an diesen Standorten sicher sind.

Solche Verhaltensmuster setzen Ihr Unternehmen ernsthaften Gefahren aus. Diversifizieren Sie Ihr Programm, damit diese und andere potenzielle Schwachstellen thematisiert werden, um Ihre Angriffsfläche zu verringern.

Wenn Sie diese Themen behandeln, verwenden Sie wahre Begebenheiten und anschauliche Beispiele. Relevante, konkrete Details helfen den Anwendern zu verstehen, wie Angreifer arbeiten – und warum das wichtig ist.

## Ihr Programm flexibel gestalten

Jedes Unternehmen hat eine einzigartige Bedrohungslandschaft, Anwenderbasis und Kultur des Sicherheitsbewusstseins. Und so wichtig Planung auch ist, ebenso wichtig ist Flexibilität.

Ein flexibles Programm passt sich an veränderte Umstände an und richtet Ihre Schulung zur richtigen Zeit auf die richtigen Personen aus. Mit Flexibilität können Sie sicherstellen, dass Ihr Programm umfassend, wirkungsvoll und effizient ist und die Anwenderisiken verringert. Außerdem trägt sie dazu bei, dass Unternehmen aus den ein oder zwei Stunden pro Jahr, die typischerweise für Security-Awareness-Schulungen angesetzt werden, das Maximum herausholen.

Die erfolgreichsten Programme stimmen Schulungsübungen mit realen und potenziellen Bedrohungen ab. Passen Sie Ihr Programm an die Umstände an. Das Leben ist unvorhersehbar und plötzliche Veränderungen können neue Wissenslücken und Anwenderisiken schaffen.

Hier sind einige Beispiele für Situationen, in denen Sie Ihren Plan unter Umständen ändern müssen, weil sich ein neuer Bedarf ergibt oder neue Schwachstellen aufgedeckt werden:

- Ihre Phishing-Tests zeigen, dass Anwender zwar Link-basierte Angriffe verstehen, aber Probleme haben, Angriffe mit E-Mail-Anhängen zu erkennen.
- Ihr Unternehmen sieht sich einer wachsenden Zahl von BEC-Angriffen gegenüber.
- Ihr E-Mail-Sicherheitsteam beobachtet Angreifer, die eine bestimmte Art von Phishing-Köder oder einen bestimmten Angriffstyp verwenden.
- Aus Ihren Wissenstests geht hervor, dass eine bestimmte Abteilung Probleme bei einem wichtigen Thema hat.

## Automatisierte Folgeschulungen

Automatisierung kann Ihnen zu noch mehr Flexibilität verhelfen. So nutzen unsere Kunden beispielsweise die Auto-Enrollment-Funktion unserer Lösung, um Anwendern je nach Abschneiden bei simulierten Angriffen und Wissenstests automatisch Schulungen zuzuweisen. Diese Funktion weist Anwendern jene Schulungen zu, die sie am dringendsten benötigen, zwingt sie aber nicht dazu, sie sofort zu absolvieren.

Die automatisierte Folgeschulung ist eine gute Möglichkeit, die Schulung auf tatsächliche Schwachstellen und Lücken zuzuschneiden, anstatt einen pauschalen Ansatz zu verwenden, der allen Anwendern die gleiche Schulung zuweist. Zielgerichtete Schulungen sparen die Zeit der Anwender und machen es allen Beteiligten einfacher, sie zu akzeptieren.

## Chance, den Schulungserfolg zu beweisen

Sie können Schulungen auch maßschneidern, indem Sie Anwendern Gelegenheit geben, den Schulungserfolg zu beweisen und zu zeigen, dass sie Cybersicherheitskonzepte verstehen und gutes Verhalten an den Tag legen. Wenn Anwender ihre Grundschulung absolviert haben, simulierte Phishing-Angriffe konsequent abwehren (oder melden) und beim Wissenstest gut abschneiden, benötigen sie unter Umständen insgesamt weniger Schulung.

Durch die Aussicht darauf, ihren Schulungserfolg beweisen zu können, nehmen Anwender die Schulung eher als besser wahr. Zudem verschafft das einen Anreiz, Wissenstests ernster zu nehmen.

ABSCHNITT 5

# Die richtigen Kennzahlen: Erfolg ist messbar

Wenn Sie ein Programm zur Sensibilisierung für Sicherheit nutzen, sind Sie wahrscheinlich mit den Begriffen „Klickrate“ bzw. „Fehlerquote“ vertraut. Das ist die erste und wichtigste Statistik, die unsere Kunden zum Messen des Programmerfolgs verwenden. Damit wir uns nicht missverstehen: Sie ist wichtig.



## Meldungsrate

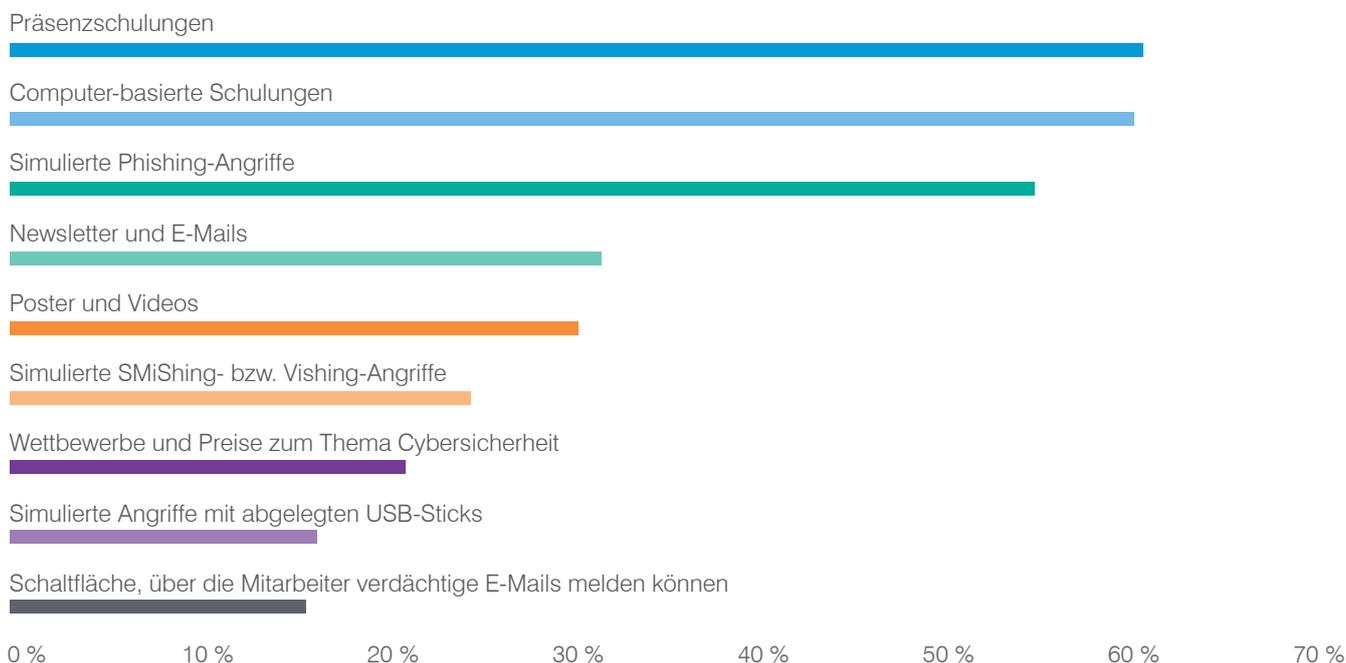
Doch Sie sollten auch noch andere Kennzahlen auf dem Schirm haben. Die Messung der Rate, mit der Anwender aktiv (tatsächliche und simulierte) schädliche E-Mails melden, kann ebenfalls wichtige Erkenntnisse liefern.

Mit einer integrierten Schaltfläche im E-Mail-Client für das Melden schädlicher E-Mails können Anwender ihr Sicherheitsteam problemlos auf verdächtige E-Mails aufmerksam machen. Mit diesen Tools lässt sich auch messen, wie viele Anwender eine erhaltene simulierte Phishing-E-Mail melden. Diese Kennzahl ist als Meldungsrate bekannt.

Leider verwenden nur 15 % der Unternehmen diese Werkzeuge in ihrem Sensibilisierungsprogramm. Das geht aus unserer Umfrage zum [State of the Phish-Bericht 2020](#) hervor.

Unsere Daten ergaben mehr Schwankungen in der Meldungsrate als in den Klickraten, was darauf schließen lässt, dass die Meldungsrate insgesamt ein besserer Indikator für Verhaltensänderungen ist.

### Von Unternehmen eingesetzte Maßnahmen\*



\* Mehrere Antworten waren zulässig.

Quelle: State of The Phish 2020

## Der Wissensstand

Weitere Erkenntnisse kann der Wissensstand liefern. Mit Klickrate und Meldungsrate lässt sich messen, wie gut (oder schlecht) Anwender Phishing-Angriffe als solche erkennen können. Doch mit Wissenstests lässt sich zusätzlich messen, wie gut sie andere Themen wie Datenschutz, Kennwörter und mobile Sicherheit verstehen.

So können für stark regulierte Unternehmen oder Abteilungen beispielsweise spezielle Schulungen erforderlich sein. Es ist wichtig, den Kenntnisstand der Anwender zu kennen und zu wissen, ob er sich verbessert oder verschlechtert.

## Benchmark-Analysen der Klick- und Meldungsraten

Was gilt als „gute“ Klickrate, wenn Sie eine simulierte Phishing-E-Mail versenden? Bei der Beantwortung dieser Frage kommt es hauptsächlich auf zwei Faktoren an:

- Wie raffiniert und zielgerichtet ist die simulierte Phishing-E-Mail?
- Wie erfahren sind Ihre Anwender?

In der Regel gelten Klickraten (oder Fehlerquoten) von unter 5 % als gut. Ein genaueres Maß ist jedoch, wie weit über oder unter der durchschnittlichen Fehlerquote in einem breiteren Spektrum von Unternehmen Ihre Rate liegt.

Proofpoint gehört zu den vielen Anbietern, die die durchschnittliche Fehlerquote verschiedener [simulierter Phishing](#)-Vorlagen zur Verfügung stellen. Wie in diesem Screenshot zu sehen ist, liegt eine Fehlerquote von 5 % bei einigen Vorlagen unter dem Durchschnitt.



In der Regel gelten Klickraten (oder Fehlerquoten) von unter 5 % als gut.

### Vergleich der durchschnittlichen Fehlerquote mittels ThreatSim® (in Grün).

Jump in this quick meeting	Corporate	8%
FREE GDPR Readiness Tools - Targets Legal or HR	Commercial	3%
College Admissions Help	Consumer	2%
Online dating - Message waiting	Proofpoint - Consumer	5%

Deshalb bietet der Vergleich Ihrer Ergebnisse mit diesen durchschnittlichen Fehlerquoten bessere Erkenntnisse über die Sensibilisierung Ihrer Anwender für Phishing. Je mehr Unternehmen bestimmte Vorlagen nutzen, desto eher ändern sich durchschnittliche Fehlerquoten mit der Zeit.

In Bezug auf die Meldungsrate (also Anwender, die eine simulierte Phishing-E-Mail erkennen und melden) sollten Sie eine Quote von 70 % anstreben. Etliche unserer Kunden erreichten Meldungsraten von über 80 % bei gleichzeitig niedriger Fehlerquote.

Einer unserer Kunden hat durch den Einsatz einer Komponente unserer Lösung CLEAR

**345.000 US-Dollar**

an Personalkosten gespart.

## Messbare Wirkung

Kennzahlen zum Sicherheitsbewusstsein sind wichtig und sollten daher in der entsprechenden Software leicht zu finden sein. Doch das eigentliche Ziel jeder Security-Awareness-Schulung ist die Verringerung der Anwenderrisiken.

Daher können Sie Ihr Programm mit externen Kennzahlen bewerten und so seinen Wert beweisen. Einige der wichtigsten Zahlen sind dabei:

- Die Anzahl der Malware-Infektionen und der Aufwand für notwendige Arbeiten an den Rechnern der Anwender
- Die Zeit und Mittel für die Verwaltung des Abuse-Postfachs
- Die Anzahl tatsächlich erfolgreicher Phishing-Angriffe
- Die Ausfallzeiten für Anwender

Diese Kennzahlen können zudem helfen, die dauerhafte Unterstützung der wichtigsten Projektbeteiligten für Ihr Programm zu erhalten. Einer unserer Kunden hat durch den Einsatz einer Komponente unserer Lösung Proofpoint Closed-Loop Email Analysis and Response (CLEAR) 345.000 US-Dollar an Personalkosten gespart. (Weitere Informationen dazu erhalten Sie im Forrester-Bericht [The Total Economic Impact Of Proofpoint Advanced Email Protection](#) (Die wirtschaftlichen Auswirkungen von Proofpoint Advanced Email Protection)).

## Mit Daten zur Erfolgsgeschichte

Viele Kennzahlen, die für Security-Awareness-Schulungen verwendet werden (z. B. „Fehlerquote“ oder „Klickrate“) klingen unterbewusst negativ, weil sie eher Fehler als Erfolge hervorheben. Andere Kennzahlen (z. B. Meldungsraten und Wissensstand) betonen hingegen eher positive Verhaltensweisen und zeigen besser auf, wie sich Anwender als Verteidigungslinie gegen heutige gezielte Angriffe schlagen.

Verwenden Sie diese Daten, um Erfolgsgeschichten darüber zu erzählen, wie Anwender die Sicherheit Ihres Unternehmens verbessern. Ein Beispiel: Ein Anwender meldete eine tatsächlich schädliche Nachricht und Ihr Team konnte auf den Zwischenfall reagieren, bevor die E-Mail Schaden angerichtet hat. Geschichten wie diese können dabei helfen, Ihr Programm intern gegenüber den wichtigsten Projektbeteiligten zu bewerben und die Sicherheitskultur in Ihrem Unternehmen zu verbessern.

ABSCHNITT 6

# Über Schulungen hinaus: Aufbau einer Sicherheitskultur

Rund 99 % der Unternehmen sagen, dass sie ihren Anwendern Schulungen zur Sensibilisierung für Phishing bieten.<sup>2</sup> Gleichzeitig geben 43 % an, dass sie nur einen Teil ihrer Anwender schulen. Es verwundert daher nicht, dass Phishing-Betrug nach wie vor die Bedrohungsart ist, die am ehesten zu einer Datenschutzverletzung führt.

Was können wir besser machen? Die Antwort liegt im Aufbau einer systematischen, nachhaltigen und individuellen Sicherheitskultur, die sich durch das gesamte Unternehmen und alle digitalen Aktivitäten zieht.

Dazu sind gezielte Investitionen von Zeit, Energie und Ressourcen sowie unternehmensweite Unterstützung nötig. Das Ergebnis jedoch ist unbezahlbar, da eine robuste Sicherheitskultur die Sicherheit Ihres Unternehmens, die Einhaltung von Vorschriften und das Geschäftsergebnis verbessern kann. Richtig umgesetzt lässt sich damit sogar die Motivation und Produktivität der Mitarbeiter steigern.



<sup>2</sup> Proofpoint: „State of the Phish 2022“, Februar 2022.

## Wie sieht eine Sicherheitskultur aus?

Den MIT-Forschern Keman Huang und Keri Pearlson zufolge besteht eine Sicherheitskultur aus „den Überzeugungen, Werten und Einstellungen, die die Anwender dazu bewegen, das Unternehmen vor Cyberangriffen zu schützen“.<sup>3</sup>

Mit anderen Worten: Alle Ihre Mitarbeiter sind beim Schutz der Daten, Systeme und Ressourcen des Unternehmens aktive Akteure.

Für den Aufbau einer Sicherheitskultur sind Lösungen erforderlich, die bei den Mitarbeitern ein Umdenken beim Thema Sicherheit auslösen. Diese Sicherheitskultur sollte in die Unternehmenskultur eingebettet sein. Sie muss inspirieren – und zwar nachhaltig.

### Faktoren einer Kultur

Eine Cybersicherheitskultur besteht aus drei sich überschneidenden Faktoren:

- **Die Verantwortung für die Cybersicherheit.** Die Mitarbeiter fühlen sich gemeinsam verantwortlich dafür, so zu handeln, dass Sicherheitszwischenfälle vermieden werden.
- **Das Wissen, warum Cybersicherheit wichtig ist.** Die Mitarbeiter sind davon überzeugt, dass Cyberbedrohungen ein erhebliches Risiko für den Erfolg des Unternehmens sind und persönliche Folgen für sie haben könnten.
- **Die Fähigkeit zu handeln.** Die Mitarbeiter fühlen sich durch ihr Cybersicherheitswissen gestärkt, verstehen die Sicherheitsrichtlinien und vertrauen darauf, dass das Unternehmen sie unterstützt, wenn sie unabsichtlich einen Fehler begehen.

### Eigenschaften einer starken Sicherheitskultur

Eine starke Sicherheitskultur hat folgende Merkmale:

- **Sie ist ganzheitlich und kontinuierlich.** Eine Sicherheitskultur darf nicht nur aus Schulungen und gelegentlichen Phishing-Simulationen bestehen. Das Ziel ist, die Moral zu heben und die Mitarbeiter dazu zu motivieren, sich für die Sicherheit im Unternehmen einzusetzen. Dies lässt sich auf vielen Wegen erreichen. Eine Sicherheitskultur fördert das Lernen und Sicherheitsbewusstsein durch relevante und maßgeschneiderte Inhalte sowie Updates zur sich verändernden Bedrohungslandschaft. Die Anwender erhalten E-Mails und andere Erinnerungen, die als Stütze dienen und ihnen bewusst machen, warum sie am Programm teilnehmen und wie es ihnen bei ihrer Arbeit – und im Privatleben – hilft. Zudem werden sie ermutigt, verdächtige digitale Ereignisse vorbehaltlos und entschlossen zu melden.
- **Sie hat positionsübergreifende Fürsprecher.** Die Unterstützung beginnt bei der Unternehmensführung und geht über die Abteilungsleiter bis hin zu den Endnutzern. Abgesehen von den Führungskräften können sich Fürsprecher unter anderem in der Sicherheits-, IT-, Personal-, Compliance- und Audit- sowie der Marketing- und Presse-Abteilung finden.<sup>4</sup>
- **Sie erzeugt Erwartungen und erhält sie aufrecht.** Dazu gehört die Entwicklung und Durchsetzung von Sicherheitsrichtlinien, die kulturelle Normen bestimmen.

<sup>3</sup> Keman Huang and Keri Pearlson (MIT): „For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture“ (Technologie kann nicht alles beheben: Aufbau eines Modells einer Cybersicherheitskultur für Unternehmen), Januar 2019.

<sup>4</sup> SANS Institute: „2021 Security Awareness Report: Managing Human Cyber Risk“ (Bericht zum Sicherheitsbewusstsein 2021: Verwaltung menschlicher Cyberrisiken), November 2021.

## Die Vorteile

Eine starke Sicherheitskultur kann zu den geschäftlichen Zielen des Unternehmens beitragen und sinnvolle sowie messbare Vorteile mit sich bringen, zum Beispiel:



### Verbesserte Agilität und Resilienz

Eine Sicherheitskultur spornt die Anwender dazu an, potenzielle Bedrohungen zu erkennen. Zudem ermöglicht sie dem Sicherheitsteam, schneller auf Bedrohungen zu reagieren und diese zu beheben. Agilität und Resilienz verbessern sich, wenn durch motivierte, geförderte und sich gegenseitig unterstützende Anwender ein Netzwerkeffekt entsteht. Die Vorteile wirken sich auf das gesamte Unternehmen aus.



### Unternehmensweite Minimierung von Risiken

Wir leben in einer Zeit mit immer mehr Remote- und Hybrid-Arbeitsplätzen, in der Unternehmen auf die Cloud setzen und verstärkt private Geräte genutzt werden. Das führt meist zu wachsenden Risiken. Wenn es eine starke Sicherheitskultur gibt, können sich die Führungskräfte unbesorgt um andere Bereiche des Unternehmens kümmern.



### Unkomplizierte Compliance

Die Einhaltung von gesetzlichen Vorschriften, Branchenstandards und internen Sicherheitsrichtlinien wird einfacher, womit sich die Wahrscheinlichkeit von Strafen und Geldbußen verringert.



### Wettbewerbsvorteil

Wenn Kunden und Partner den Eindruck haben, dass Ihr Unternehmen mehr Sicherheit bietet, werden sie sich für Sie anstatt für Ihre Mitbewerber entscheiden. Sicherheit sollte als Grundwert kommuniziert werden.

## Häufige Hindernisse

Unternehmen geben Millionen für Sicherheitstools, Services und Personal aus. Doch selbst mit diesen Investitionen übersehen viele den größten Risikofaktor: den Menschen.

Der Faktor Mensch spielt beim Schutz des Unternehmens die größte Rolle – und ist ein Problem, das sich nur schwer bewältigen lässt. Aktivitäten zur Sensibilisierung für Sicherheit werden häufig als störend und ablenkend empfunden. Einige Mitarbeiter haben das Gefühl, dass sie dadurch von ihrer „richtigen“ Arbeit abgehalten werden. Viele stellen sich gegen die zusätzlichen Anforderungen wie das Melden von verdächtigen E-Mails oder die Schulungs-Webinare. Zudem können die technischen Fachkräfte und Mitarbeiter der Personalabteilung zurückhaltend auf den Aufbau einer Sicherheitskultur reagieren, da sie dafür nicht gerüstet sind.

#### Folgende Herausforderungen stellen sich:

- Die Unternehmensführung vom Konzept überzeugen
- Die Rendite überzeugend quantifizieren
- Die Anwender davon überzeugen, dass Schulungen und Sicherheitsbewusstsein etwas Positives sind und sie dabei mitmachen sollten
- Das Anwenderverhalten ändern

## Umsetzung mithilfe des ACE-Frameworks

Motivation ist der Schlüssel zur Entwicklung einer starken Sicherheitskultur und besteht aus drei wichtigen Bestandteilen. Der erste ist Autonomie. Das bedeutet individuell gestaltetes und selbstbestimmtes Lernen für jeden Anwender. Der zweite ist die Entwicklung von Kompetenz. Das heißt, den Anwendern die Tools und Zeit zu geben, die sie benötigen, um sich weiterzuentwickeln und Cybersicherheitswissen und Fähigkeiten anzueignen bzw. zu erlernen. Der letzte Bestandteil ist der Sinn und Zweck. Die Anwender sollen das Gefühl bekommen, dass sie Teil einer umfassenden Mission sind.

### Verwenden des ACE-Frameworks

Der Aufbau einer nachhaltigen Sicherheitskultur kann mit drei Schritten unterstützt werden. Dieser fortlaufende Prozess, den wir als ACE-Framework bezeichnen, gliedert sich wie folgt:

#### **A** Assess: Bewertung der Anwenderschwachstellen

Jedes Unternehmen hat seine individuellen Risiken und Sicherheitsprioritäten.

##### **Stellen Sie sich folgende Fragen:**

- Was wissen meine Anwender?
- Wer von ihnen wird gezielt angegriffen? Welchen Arten von Angriffen sind meine Anwender ausgesetzt?
- Wie würden sich diese Anwender bei einem Angriff verhalten?
- Was sind glauben sie? Wie stehen sie zum Thema Cybersicherheit?

Anhand dieser und anderer Fragen können Sie ermitteln, wo die Schwachstellen liegen.

#### **C** Change: Änderung des Anwenderverhaltens

Der Aufbau einer Sicherheitskultur ist ein fortlaufender Prozess und kein einmaliges Ereignis. Wählen Sie einen ganzheitlichen Ansatz.

Wenden Sie sich dazu regelmäßig über verschiedene Kommunikationskanäle an Ihre Mitarbeiter, zum Beispiel in regelmäßigen Newslettern, über interne Blog-Artikel und durch aktuelle Informationen über die neuesten Bedrohungen und Angriffsvektoren.

Sorgen Sie für eine bunte Mischung an Inhalten und gestalten Sie sie individuell. Jeder ist unterschiedlich und reagiert bzw. lernt anders. Denken Sie daran, immer wieder auf positive Art und Weise auf die Bedeutung von Sicherheit hinzuweisen.

#### **E** Evaluate: Bewertung und Beobachtung des Fortschritts

Geben Sie Kennzahlen weiter, die den Fortschritt, die kontinuierliche Verbesserung und die Rendite zeigen. Diese quantifizierbaren Bewertungen bestätigen Ihre Investition und zeigen der Geschäftsleitung sowie dem gesamten Unternehmen, wie wertvoll eine Sicherheitskultur ist.

Lassen Sie niemals eine gute Krise ungenutzt verstreichen. Zeigen Sie nach einem Angriff, wie durch eine starke Sicherheitskultur der Zeit- und Arbeitsaufwand sowie die Finanzmittel zur Behebung verringert oder der Angriff völlig vermieden werden konnte.

Es gibt viele Möglichkeiten, das Sicherheitsbewusstsein in Ihrem Unternehmen zu messen und einzuschätzen, wie sich die Sicherheitskultur auf das Anwenderverhalten ausgewirkt hat.

**Dazu gehören:**

- Klickraten für die am meisten gefährdeten Anwender
- Meldungsraten bei Phishing-Simulationen
- Zuverlässigkeit, mit der Anwender echte Bedrohungen erkennen

## Warum das wichtig ist

Der Aufbau einer lebendigen Sicherheitskultur wirkt sich auf alle Ihre Anwender positiv aus – von der Geschäftsleitung über die Abteilungsleiter bis hin zu den Endnutzern.

Es gibt jedoch keine universelle Vorlage, um dies zu erreichen. Jedes Unternehmen hat einen eigenen Charakter und individuelle Anforderungen. Einige dieser Unterschiede hängen vom Unternehmen ab, andere wiederum von der Branche. Zudem wird jede Kultur durch eine ganze Reihe an internen und externen Faktoren bestimmt.

Durch den Aufbau eines langfristigen Programms, das von allen Beteiligten getragen wird, kann Sicherheitsbewusstsein zu den festen Grundwerten Ihres Unternehmens werden. Eine echte Sicherheitskultur besteht nicht aus einmaligen Schulungen. Sie ist geprägt von einer inneren Einstellung, die sich auf die alltäglichen Aktivitäten im Unternehmen und im privaten Bereich auswirkt.

An dieser Stelle möchten wir nur eine allgemeine Einführung in den Aufbau einer Sicherheitskultur geben.

Einen umfassenden Überblick zu Sicherheitskulturen und zum ACE-Framework erhalten Sie in unserem E-Book [Mehr als nur Cybersicherheits-Schulungen: Der Aufbau einer nachhaltigen Sicherheitskultur – und warum sie wichtig ist](#).



ABSCHNITT 7

# Schlussfolgerungen und Empfehlungen

Ihr Security-Awareness-Schulungsprogramm sollte das Ziel haben, die Verhaltensweisen zu verbessern, die für Ihr Unternehmen die größte Bedeutung haben. Die beste Möglichkeit dazu ist eine Mischung aus allgemeinen und gezielten Schulungen, die Mitarbeiter mit umsetzbaren Empfehlungen unterstützen.



Sofern Sie bislang noch keinen personenzentrierten Ansatz für Sicherheitsschulungen umgesetzt haben, sollten Sie das umgehend tun. Das sind die fünf Säulen eines erfolgreichen und effizienten Programms:

## Rücken Sie den Menschen in den Fokus

Jeder Mitarbeiter in Ihrem Unternehmen kann ins Visier der Angreifer geraten. Zu jedem Zeitpunkt kann jeder Angestellte in Ihrem Unternehmen die Sicherheitslage verbessern oder beeinträchtigen.

Security-Awareness-Schulungen gehören zu den wichtigsten Maßnahmen, mit denen Sie die Sicherheit in Ihrem Unternehmen verbessern können. Wenn Sie Ihre Anwender zur Erkennung, Vermeidung und Meldung von Phishing-Versuchen schulen, können Sie eine starke letzte Verteidigungslinie gegen die größten aktuellen Cyberbedrohungen schaffen.

## Geplant an den Start

Jedes Unternehmen ist einzigartig und kein Schulungsprogramm ist wie das andere. Folgende Punkte aus Abschnitt 2 sollten allerdings unbedingt in Ihr Schulungsprogramm einfließen:

- Definition des Schulungsbedarfs
- Identifizierung von Anwendern mit speziellem Schulungsbedarf
- Definition der Aktivitäten
- Erstellung und Verwaltung von Zeitplänen
- Kommunikation und Test der ersten Schritte
- Definition von Häufigkeit und Zeitplanung der Programmaktivitäten

Je mehr Sorgfalt und Planung Sie in Ihr Programm fließen lassen, desto erfolgreicher wird es letztlich werden.

## Die Mitarbeiter müssen mitmachen

Bedenken Sie: Ihr Programm ist nur dann erfolgreich, wenn Ihre Anwender es akzeptieren und annehmen. Auch ein mit der besten Absicht erstelltes Programm wird als anstrengend wahrgenommen, wenn die Inhalte nicht wertvoll und relevant sind.

Erfolgreiche Programme zeichnen sich durch Folgendes aus:

- Sie haben einen Namen, der ihre Relevanz verdeutlicht.
- Sie wenden wissenschaftlich bestätigte Lernprinzipien an, um Verhaltensänderungen zu bewirken.
- Sie festigen die Schulungsinhalte mit einer abwechslungsreichen Mischung aus Inhalten und Medien.
- Sie haben mehrere Fürsprecher im ganzen Unternehmen, die Unterstützung und Verbesserungsvorschläge bieten.
- Sie setzen auf eine ausgewogene Mischung aus Anreizen und Konsequenzen.

## Nutzen Sie Daten, um gefährdete Anwender zu ermitteln, Schwerpunkte für Schulungen zu setzen und flexibel zu bleiben

Ihre ersten Schritte sollten darin bestehen, grundlegendes Wissen zu vermitteln, die Schwachstellen der Anwender zu verstehen und die Schulung auf die dringendsten Bereiche zu konzentrieren. Hier können simulierte Phishing-Angriffe und fragenbasierte Wissenstests wertvolle Erkenntnisse darüber liefern, worauf Sie Ihre Schulungsmaßnahmen konzentrieren sollten. Durch Bedrohungsdaten, die Aufschluss über die Angriffe geben, denen sich Ihre Anwender gegenübersehen, können Sie Schulungsinhalte mit realen Bedrohungen abstimmen. Das Wissen, welche Anwender Zugang zu den vertraulichsten Daten des Unternehmens haben, kann Ihnen bei der zielgerichteten Gestaltung der Schulungen ebenso helfen wie beim Anwenden anderer Sicherheitskontrollen auf Anwender mit weitreichenden Rechten.

Mit automatisierten Folgeschulungen und der Möglichkeit, sachkundige und risikoarme Anwender von Schulungen ausnehmen zu können, können Sie flexibel handeln.

## Erfolgsmessung mit internen und externen Kennzahlen

Klickraten oder Fehlerquoten für simulierte Phishing-E-Mails sind wichtig. Doch der Anteil der gemeldeten E-Mails ist möglicherweise ein noch besserer Maßstab dafür, wie gut Ihre Anwender Angriffen widerstehen können.

Mithilfe von Wissenstests lässt sich ermitteln, wie gut sie andere Themen verstehen.

Unterm Strich helfen externe Kennzahlen wie Malware-Infektionen und Ausfallzeiten dabei, Wirkung und Wert Ihres Programms aufzuzeigen.

Diese Kennzahlen können zudem helfen, die dauerhafte Unterstützung der wichtigsten Projektbeteiligten für Ihr Programm zu erhalten. Verwenden Sie diese Daten, um hervorzuheben, wie Anwender die Sicherheit Ihres Unternehmens verbessern. Die Daten helfen nicht nur, Ihr Programm intern gut zu verkaufen, sondern verbessern auch die Sicherheitskultur in Ihrem Unternehmen.



## Weitere Informationen

Wenn Sie mehr über Stärken, Schwächen und Cybersicherheitswissen Ihrer Anwender erfahren wollen – und darüber, wie Sie Verhaltensänderungen bewirken können –, registrieren Sie sich unter [proofpoint.com/de/people-risk-assessment](https://proofpoint.com/de/people-risk-assessment) für unsere kostenlose Risikoanalyse Ihrer Mitarbeiter.



### Gründe für Proofpoint

 Wir analysieren täglich mehr als:

**2,6 Mrd.**  
E-MAILS

**49 Mrd.**  
URLs

**1,9 Mrd.**  
ANHÄNGE

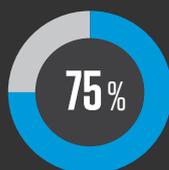
**1,7 Mrd.**  
MOBILGERÄTE-  
NACHRICHTEN

**430 Mio.**  
WEB-DOMAINS

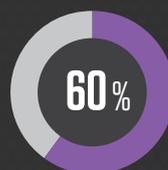
**143.000**  
SOCIAL-MEDIA-KONTEN



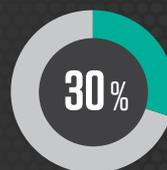
Auf unsere Lösungen vertrauen mehr als:



DER FORTUNE 100



DER FORTUNE 1000



DER FORTUNE  
GLOBAL 2000



**8.000**  
GROSSUNTERNEHMEN



**200.000**  
KLEINE UNTERNEHMEN

## WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://www.proofpoint.com/de).

---

### INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter [www.proofpoint.de](https://www.proofpoint.de).

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.