sosafe

Behavioral Security

Mit verhaltensbasierten Daten die Security Awareness steigern

Inhaltsverzeichnis

01 Einleitung

Das Zusammenspiel von Cyber Security und Verhaltenspsychologie

Informationssicherheit ist heute eine der größten Herausforderungen für Organisationen weltweit. Cyberattacken werden nicht nur häufiger, sondern auch immer ausgeklügelter, da sich viele Cyberkriminelle die Macht des Social Engineering zunutze machen. Ihre Angriffe werden so immer schwieriger zu erkennen und noch schwieriger abzuwehren.

Die Social-Engineering-Strategien, die Angreifende zur emotionalen Manipulation ihrer Opfer nutzen, basieren dabei auf grundlegenden menschlichen Verhaltensmustern. Dasselbe muss daher auch für die Sicherheitsmaßnahmen gelten, die Organisationen vor genau solchen Attacken schützen sollen. Die dynamische Cyber-Bedrohungslage zwingt deshalb viele Sicherheitsbeauftragte dazu, ihre Schutzmaßnahmen zu überdenken – weg von rein technischen Maßnahmen und hin zu einem ganzheitlichen Ansatz, bei dem der Faktor Mensch im Vordergrund steht. Im Zuge dieses Wandels wurde „sicheres Verhalten“ zu einem der Schlüsselbegriffe – wenn nicht sogar zu dem zentralen Begriff – auf den heute viele Organisationen zur Stärkung ihrer Sicherheitskultur setzen. In einer Sicherheitskultur, in der Mitarbeitende überlegt

handeln und sichere Gewohnheiten festigen, haben Cyberkriminelle weitaus weniger Erfolgschancen.

Wenn Organisationen das Verhalten von Angreifenden und Nutzenden verstehen, können sie Angriffe frühzeitig erkennen und abwehren. Dabei helfen aussagekräftige verhaltensbasierte Daten: Sie zeigen den Verantwortlichen auf, wie Mitarbeitende auf verschiedene Bedrohungen reagieren, welche Lernmethoden besonders effektiv sind, und ermöglichen ihnen zudem, ihre Awareness-Maßnahmen entsprechend zu optimieren. Weist ein bestimmtes Team zum Beispiel eine geringere Phishing-Meldequote als andere Teams auf, kann den Mitarbeitenden durch zusätzliche gezielte E-Learning-Einheiten vermittelt werden, wie sie verdächtige E-Mails erkennen und melden können. Zu guter Letzt veranschaulichen verhaltensbasierte Kennzahlen eindrucksvoll, welchen Einfluss Lernprogramme auf die gesamte Sicherheitskultur der Organisation haben. Sie sind somit handfeste Argumente, um Entscheidungsträgern von der Führungsebene bis hin zu den Mitarbeitenden die Relevanz der Maßnahmen zu vermitteln.

Das bringt zwei Fragen auf

Welche Daten sind für Organisationen besonders aussagekräftig, um zu beurteilen, wie wirkungsvoll ihre Awareness-Maßnahmen ihre Sicherheitskultur stärken?

Und **welche psychologisch fundierten Ansätze** können die Effizienz dieser Maßnahmen steigern?

Um diese Fragen zu beantworten, sehen wir uns zunächst genauer an, wie Verhaltenswissenschaft bzw. Psychologie und Informationssicherheit in Verbindung stehen. Danach beleuchten wir die Dimensionen, die eine ganzheitliche Sicherheitskultur ausmachen, sowie die wichtigsten Kennzahlen, die die Effektivität der verschiedenen Sicherheitsmaßnahmen aufzeigen.

02 Warum sich bei Cyber Security ein Blick auf die Änderung von Verhalten lohnt

Für Cyber-Security-Expertinnen und -Experten ist es nichts Neues: Technologie allein reicht nicht mehr aus, um Organisationen vor den immer ausgefeilteren Angriffen und Betrugsmaschen der Cyberkriminellen zu schützen. Social Engineering ist für Angreifende inzwischen die Betrugstaktik Nummer eins, denn die Erfolgsrate dieser Angriffe ist schockierend hoch. **Tatsächlich spielt bei mehr als 82 Prozent aller Datenschutzverletzungen der menschliche Faktor eine Rolle, so Verizon in seinem neuesten Data Breach Investigations Report**.[1] Auch IBM nennt gestohlene E-Mail-Credentials und Phishing als zwei der häufigsten Angriffstaktiken – beide zielen stark auf menschliche Schwachstellen ab. [2]

Die neuen Maschen der Cyberkriminellen kommen Organisationen teuer zu stehen

Die verschärfte Bedrohungslage hatte bereits kostspielige Folgen für Unternehmen weltweit, darunter bekannte Größen wie Twilio, Cisco und Uber. Sie alle haben zuletzt die unmittelbare Bedrohung durch Social-Engineering-Taktiken selbst erlebt.

Im Falle von Twilio gelang es Hackern durch einen ausgeklügelten Social-Engineering-Angriff, sich Zugriff auf mehr als 120 Kundenaccounts zu verschaffen, indem sie durch gezielte Manipulation an E-Mail-Daten von Mitarbeitenden gelangten. Dabei erhielten Mitarbeitende personalisierte Phishing-Benachrichtigungen in Form von SMS („Smishing"), die sie dazu verleiteten, sensible Daten preiszugeben. [3]

Das Threat-Intelligence-Unternehmen Cisco Talos berichtete von einem ähnlichen Angriff durch die Ransomwaregruppe Yanluowang, bei dem knapp 3 GB Daten gestohlen wurden.[4] Dabei gelang es den Angreifenden, die Kontrolle über das Google Konto eines Mitarbeitenden zu übernehmen, in dem sensible Login-Daten gespeichert waren. Per Voice Phishing („Vishing") brachten sie daraufhin Personen in der Organisation dazu, eine Multifaktor-Authentifizierung zu durchlaufen und drangen so in die Unternehmenssysteme ein.

1 Verizon (2022). Data Breach Investigations Report.
2 IBM (2022). Die Kosten von Datenschutzverletzungen – Bericht 2022.
3 Twilio (2022). Incident Report: Employee and Customer Account Compromise.
4 Cisco Talos (2022). Cisco Talos shares insights related to recent cyber attack on Cisco.

Am schockierendsten war vermutlich der Social-Engineering-Angriff, der im September 2022 von einem angeblich 18-jährigen Hacker auf Transport-Dienstleister Uber verübt wurde.[5] Bei dem Man-in-the-Middle-Angriff nutzte der Angreifer gezielt eine Schwachstelle in der Multifaktor-Authentifizierung aus und brachte einen Admin dazu, unwissentlich Login-Daten weiterzugeben. Die Folge: Der Angreifer erhielt so Zugriff auf die internen Systeme von Uber, einschließlich Datenspeicher und Kommunikationsplattformen.

Remote Work und neue Technologien verschärfen die Cyber-Bedrohungslage

Die Innovationskraft der Cyberkriminellen ist aber nur eine Seite der Medaille. Es gibt viele weitere Faktoren, die dafür sorgen, dass sich immer mehr Cybercrime-Trends auf den Faktor Mensch fokussieren. Mit der Vielfalt an Homeoffice-Modellen entstanden in den letzten zwei Jahren beispielsweise neue Prozesse und Kollaborationstools – und mit ihnen eine neue Angriffsfläche für Cyberkriminelle. Denn sie bieten nicht nur neue Chancen für den Zugriff auf Unternehmenssysteme. Neue Tools und Prozesse bringen auch eine Übergangsphase mit sich, die Mitarbeitende verunsichert und sie somit zur perfekten Zielscheibe werden lässt. Gleichzeitig bergen auch technologische Entwicklungen ein zusätzliches Risiko für die Informationssicherheit. Dabei ist auch die Rolle der künstlichen Intelligenz (KI) nicht zu unterschätzen. Strategien wie das sogenannte „Voice Cloning“, bei dem Angreifende bei Phishing-Attacken die Stimme einer Person künstlich imitieren, lassen sich immer einfacher umsetzen. AI-as-a-Service-Tools machen diese neuen Angriffstaktiken möglicherweise bald sogar für Laien zugänglich und verleihen gängigen Strategien wie Spear Phishing eine völlig neue Dynamik.

Die entscheidende Frage: Wie können wir uns vor solchen Bedrohungen schützen?

Auch wenn Security Awareness schon seit Langem ein maßgeblicher Faktor in den Sicherheitsstrategien von Unternehmen aller Größen und Branchen ist, findet derzeit ein grundlegender Paradigmenwechsel statt. Alte Trainingsansätze, die nur darauf ausgelegt sind, Compliance-Anforderungen zu erfüllen und auf statische Content-Bibliotheken setzen, können mit der professionellen Cybercrime-Industrie nicht mithalten und Organisationen nicht mehr ausreichend schützen. Worauf es heute ankommt, ist eine starke Sicherheitskultur und ein ganzheitlicher Ansatz bei Security Awareness. Statt allein auf Compliance zu setzen, sollten Awareness-Maßnahmen sicheres Verhalten bei den Mitarbeitenden festigen, damit diese im Arbeitsalltag Bedrohungen erkennen und korrekt darauf reagieren. Indem Organisationen psychologisch fundierte Awareness-Programme nutzen, können sie einmaligen, kurzfristigen Maßnahmen endlich den Rücken kehren und ein kontinuierliches Sicherheitsmanagement aufbauen, das effektiven Schutz vor Social-Engineering-Taktiken bietet.

[5] CSO Online (2022). 18-Jähriger hackt Uber.

Welche Vorteile hat es, die Änderung von Verhalten zu messen?

Um an diesen Punkt zu gelangen, führt kein Weg an der Analyse relevanter Kennzahlen vorbei, die wichtige Einblicke in die Entwicklung der Sicherheitskultur und in die Verhaltensweisen der Mitarbeitenden liefern. Für CISOs und andere IT-Sicherheitsexpertinnen und -experten sind verhaltensbasierte Daten also wertvolle Tools. **Diese bei der Entwicklung von Strategien und im Reporting zu berücksichtigen, hat gleich mehrere Vorteile:**

Sie bieten Einblicke in die Verhaltensmuster der Mitarbeitenden, zum Beispiel im Falle eines Angriffs: Wie reagieren sie? Für welche Angriffstaktiken sind sie am gefährdetsten? Was verbessert ihren Lernerfolg – und was hält sie beim Lernen zurück?

Sie ermöglichen den Verantwortlichen, gezielt auf Schwachstellen zu reagieren und Sicherheitsmaßnahmen anzupassen. Brauchen Mitarbeitende mehr motivierende Anreize, um Schulungen abzuschließen? Bei welchen Themen haben sie gegebenenfalls noch Aufholbedarf?

Sie dienen als handfeste Argumente in Diskussionen mit Entscheidungsträgern von der Führungsebene bis hin zu Mitarbeitenden. Sie zeigen auf, wie sich sicheres Verhalten auf die gesamte Informationssicherheit und sogar auf die wirtschaftlichen Erfolge der Organisation auswirken kann. Inwieweit hat das Awareness-Programm dazu beigetragen, sicheres Verhalten zu stärken und das Risiko kostspieliger Cyberattacken zu reduzieren?

Die wichtigsten Kennzahlen für Ihre Organisation

Die Frage, welche verhaltensbasierten Kennzahlen für eine Organisation relevant sind, lässt sich nicht allgemeingültig beantworten. In jedem Fall gilt: Sicherheitsbeauftragte sollten sich jene KPIs genauer ansehen, die für ihre Anforderungen und Situation besonders aussagekräftig sind – zum Beispiel je nach Branche. Diese Metriken gehen normalerweise weit über Melde- oder Abschlussquoten hinaus. Unter Umständen sind nicht nur die während des Awareness-Trainings gesammelten Daten zum Verhalten der Mitarbeitenden von Interesse. Auch ihr generelles Online-Verhalten im Internet, etwa die Nutzung eines Passwortmanagers, die Akzeptanz interner Security-Richtlinien oder ob sie sich vor dem Download einer App erst die Genehmigung der IT-Abteilung einholen, sind Aspekte, die berücksichtigt werden können. So ermöglichen es detaillierte verhaltensbasierte Daten schlussendlich, die bestehenden Cyberrisiken besser einzuschätzen und sich durch entsprechende Maßnahmen proaktiv zu schützen.

INFOBOX

Von traditionellen Awareness-KPIs zur nächsten Generation: verhaltensbasierte Metriken

Im Zuge des Paradigmenwechsels tun Organisationen gut daran, bei ihren Awareness-Maßnahmen über „traditionellere" Leistungskennzahlen (wie Phishing-Klickraten) hinaus auch auf verhaltensbasierte Daten (wie die Phishing-Melderate) zu achten. Zusammen veranschaulichen sie deutlich, wie sich die Maßnahmen auf das sichere Verhalten der Mitarbeitenden auswirken.

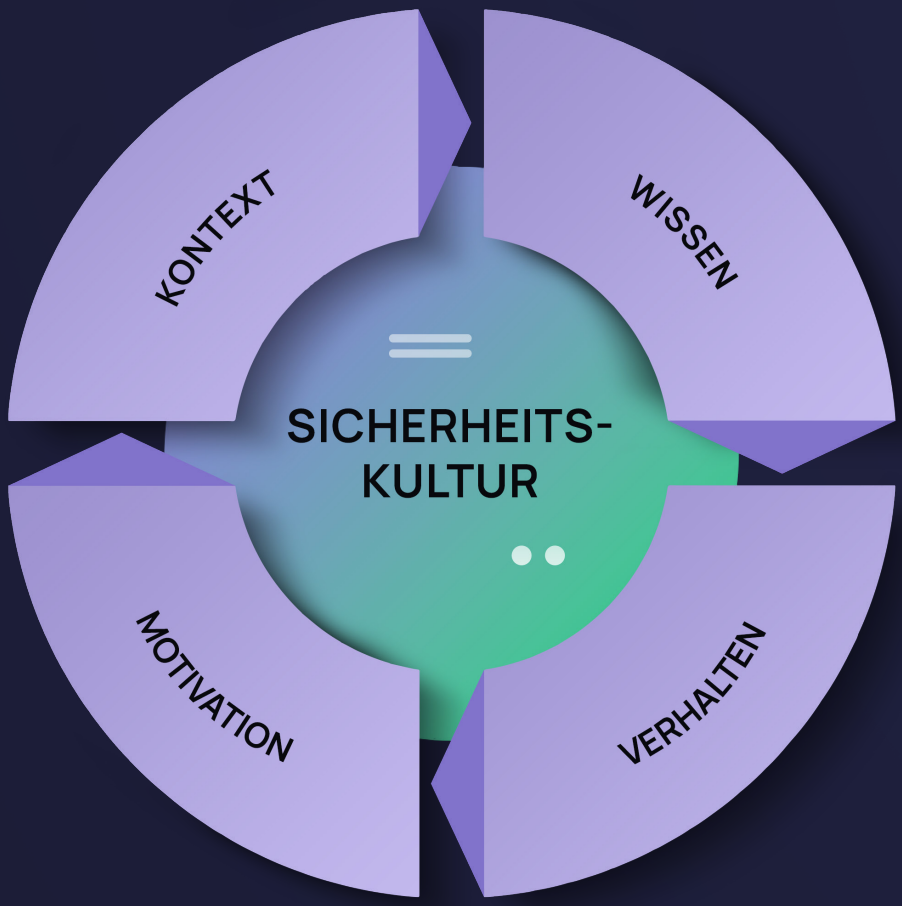
In der folgenden Tabelle finden sich einige Beispiele für die verschiedenen Arten von Kennzahlen:

Traditionelle Awareness-Kennzahlen	Moderne, verhaltensbasierte Kennzahlen
Klickraten in Phishing-Simulationen	Phishing-Melderaten mittels integrierter Reporting-Tools
Öffnungsrate in Phishing-Simulationen	Interaktionsraten mit simulierten Phishing-Mails und -Webseiten
Abschlussquote eines Kurses zur Passwortsicherheit	Tägliche/wöchentliche Nutzungsraten eines Passwortmanagers
Abschlussquote eines Kurses zu vertraulichen Daten	Anzahl an Datenelementen im Intranet, die mit ihrer Vertraulichkeitsstufe gekennzeichnet wurden
Anzahl der Ansichten eines Videos zum Thema Schatten-IT	Anzahl der an die IT gestellten Software-Freigabeanfragen

Wie in den vorherigen Absätzen bereits deutlich wurde, ist die Integration verhaltenswissenschaftlicher bzw. psychologischer Erkenntnisse in Cyber-Security-Strategien kein geradliniger Prozess. Vielmehr können je nach Organisation ganz unterschiedliche Richtlinien gelten. Werfen wir also zuerst einen Blick auf die Elemente, die eine starke Sicherheitskultur ausmachen – sowie auf einige verhaltensbasierte Kennzahlen und Methoden, mit denen Organisationen ihre Sicherheitskultur festigen können.

03 Das Behavioral-Security-Modell:

Sicherheitskultur um den Faktor Mensch aufbauen



Cyberbedrohungen entwickeln sich stetig weiter – und so auch die damit verbundenen Herausforderungen. Es steht außer Zweifel, dass inzwischen ein Großteil der Cyberattacken an menschlichen Schwachstellen ansetzt. Technische Maßnahmen alleine reichen nicht mehr aus. Solange Organisationen ihre Mitarbeitenden nicht als Teil der Lösung des Billionen-Dollar-Problems betrachten, das Cybercrime heute ist, sind sie nicht ausreichend geschützt. Nachhaltige und effektive Lernprogramme sind der Schlüssel, um die Mitarbeitenden aktiv in die Verteidigung einzubinden.

Das **Behavioral-Security-Modell** beschreibt, welche vier Dimensionen bei einer auf den Faktor Mensch ausgerichteten Sicherheitsstrategie im Fokus stehen sollten. Jede einzelne dieser Komponenten spielt eine wichtige Rolle, um das übergreifende Ziel zu erreichen: den Aufbau einer starken Sicherheitskultur. Die Komponenten stehen dabei nicht für sich, sondern treiben die jeweils anderen an. Denn gemeinsam fördern sie sicheres Verhalten zur Verteidigung gegen Cyberangriffe. In jeder dieser Dimensionen helfen Ihnen die richtigen Kennzahlen, den Stand Ihrer Sicherheitskultur zu beurteilen, Sicherheitsrisiken zu erkennen und proaktiv gegen diese vorzugehen.

3.1 Wissen: Klare Insights für nachhaltig sichere Gewohnheiten

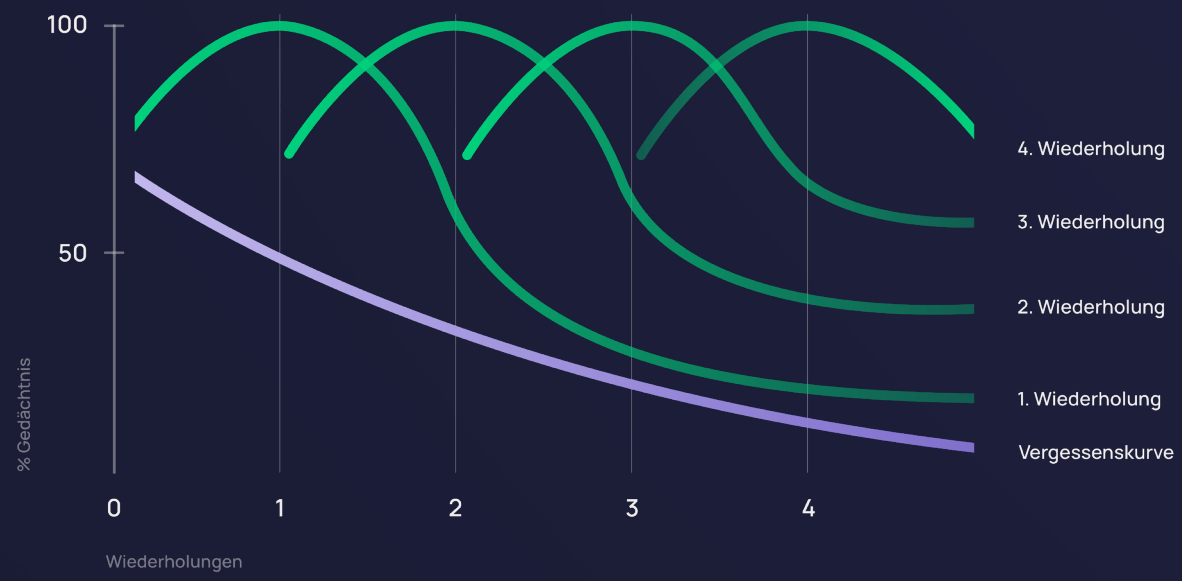
Wird der Faktor Mensch bei Schulungen außer Acht gelassen, fördert dies in Bezug auf Cybersicherheit ungewollt unachtsames Verhalten: Haben Mitarbeitende keinen Spaß am E-Learning, fehlt ihnen die Motivation, auf Cyberattacken proaktiv zu reagieren. Das gefährdet sowohl ihre eigene Sicherheit als auch die der Organisation – eine klare No-Win-Situation. Awareness-Trainings sollten so aufgebaut sein, dass sie Mitarbeitenden ihre entscheidende Rolle bei der Erkennung und Abwehr möglicher Angriffe klar vermitteln. Doch um sicheres Verhalten zu festigen, brauchen sie zunächst das nötige Wissen darüber, was sichere Verhaltensweisen eigentlich ausmacht.

Hacker hören nie auf zu lernen – das sollte unsere größte Motivation sein, auch selbst immer weiter zu lernen. Es verdeutlicht aber auch, wie wichtig stetige Weiterbildung innerhalb von Organisationen ist. In der Vergangenheit wurde Wissen dabei häufig sehr linear und in „hoher Dosis" vermittelt. Wir wissen jedoch alle nur zu gut, dass langatmige Workshops und eintönige Schulungen meist nicht die gewünschten Resultate liefern: Wissen, das im Gedächtnis bleibt. Das liegt daran, dass das angeeignete Wissen mit der Zeit von Natur aus exponentiell schwindet – eine der größten Herausforderungen im Bereich Learning und Development.

Der Vergessenskurve nach Dr. Ebbinghaus [6] zufolge vergessen Lernende schon innerhalb der ersten sieben Tage 90 Prozent des Erlernten. Das gilt insbesondere dann, wenn User ihre Lernroutine und -häufigkeit unterbrechen. Es gibt jedoch Möglichkeiten, die Mitarbeitenden dazu zu motivieren, beim Lernen am Ball zu bleiben und sich Wissen so nachhaltiger einzuprägen. Beim „Spaced Learning" wird Wissen kontinuierlich über verschiedene Kanäle vermittelt und so immer wieder aktiv wiederholt. In Kombination mit interaktiven, motivierenden Elementen, wie kurzen Quiz, lässt dies die Vergessenskurve abflachen.

SPACED TRAINING

Beispiel eines Lernpfads, der den Wissenserhalt unterstützt



[6] NeuoNation (2022). Die Vergessenskurve nach Dr. Ebbinghaus.

Durch Nudging wird die Engagement-Rate kontinuierlich um 30 %, in der Einführungsphase sogar um bis zu 90 % erhöht.

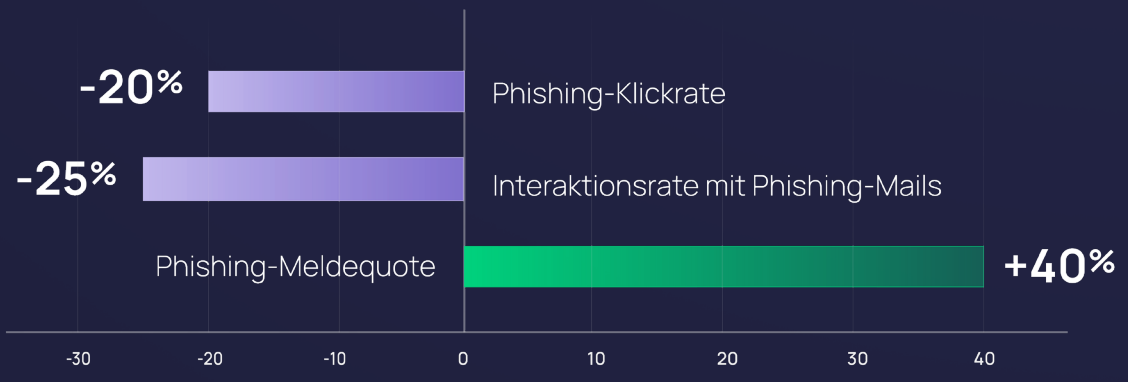
Eine Methode, die als Teil des Spaced Learning eine nachhaltige Lernerfahrung unterstützt, sind sogenannte „Nudges“. Wie in unserem Human Risk Review 2022 erwähnt: „Durch Nudging wird die Engagement-Rate kontinuierlich um 30 Prozent, in der Einführungsphase sogar um bis zu 90 Prozent, erhöht.“ [7] Nudging in Form von regelmäßigen, automatisierten System-E-Mails steigert die Interaktion der Nutzenden und sorgt dafür, dass das Thema der Cybersicherheit immer präsent ist. Nudges können kleine Anstupser zur Motivation, zur Erinnerung oder ein Update zum Lernfortschritt sein, die dafür sorgen, dass die User beim Awareness-Training auf der Spur bleiben.

Wissen, das durch Methoden wie Spaced Learning oder Nudging positiv bestärkt wird, ist essentiell, um eine starke Sicherheitskultur aufzubauen. Die Daten von der SoSafe-Plattform zeigen: Personen, die Lernmodule im Bereich Cybersicherheit und Datenschutz abgeschlossen haben, sind besser darin, E-Mails als bedrohlichen Phishing-Angriff zu identifizieren und abzuwehren. Bei diesen Mitarbeitenden ist die Wahrscheinlichkeit, dass sie solche Phishing-Angriffe melden, 40 Prozent höher als bei anderen mit geringerer Abschlussquote.

Mitarbeitende, die genau wissen, wie sie sich digital schützen können, reduzieren das Risiko der gesamten Organisation, einem Angriff zum Opfer zu fallen. Ein solides Lernprogramm bzw. Awareness-Training, bei dem kontinuierlich kontextbezogenes Wissen vermittelt wird, kann das effektiv unterstützen.

PRODUKTNUTZUNG

Ergebnisse von Nutzenden mit einer hohen Abschlussquote der Lernmodule



Beispiele für verhaltensbasierte Kennzahlen in der Dimension „Wissen“

- → E-Learning-Abschlussquoten
- → Einfluss von Nudging auf die Engagement-Rate
- → Einfluss der E-Learning-Abschlussquote auf Phishing-Meldequoten

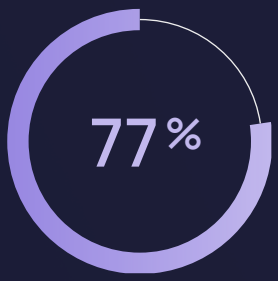
[7] SoSafe (2022). Human Risk Review 2022.

3.2 Kontext: Auf individuelle Risikofaktoren abgestimmte Lernprogramme

Ein weiterer Faktor spricht gegen eine allgemeingültige Lösung bei Cyber-Security-Trainings: Kontext. Nicht jede Person innerhalb einer Organisation hat dieselbe Ausgangslage. Die individuelle Rolle beeinflusst maßgeblich, wie sich Cyberrisiken gestalten. Angestellte in Führungspositionen und Personen mit Diensthandy sind beispielsweise stärkeren Gefahren ausgesetzt als Praktikantinnen und Praktikanten.

Cyberkriminelle werden verschiedene Positionen innerhalb der Organisation zielgerichtet angreifen. Das heißt nicht, dass manche Personen keinem Risiko ausgesetzt sind – denn das sind wir alle. Die Lernerfahrungen sollten aber entsprechend auf die Mitarbeitenden und ihre individuellen Positionen und Aufgaben abgestimmt werden.

Personalisierte Lernpfade machen Erlerntes beispielsweise greifbar und relevant und minimieren Cyberrisiken auf effiziente Weise. Laut einer Studie von Towards Maturity wünschen sich 77 Prozent der Lernenden Inhalte, die für ihre Position relevant sind.[8] Dieser verhaltensbasierte Ansatz legt den Fokus auf die Mitarbeitenden, spricht ihre individuellen Herausforderungen an und stellt Informationen bereit, die auf ihre Positionen, Profile und ihr Awareness-Level abgestimmt sind.



der Lernenden wünschen sich Inhalte, die für ihre Position relevant sind.

8 Towards Maturity (2017). Modern learning content for modern workers.

Die Branche eines Unternehmens hat ebenso Einfluss auf das Risiko. Das Gesundheitswesen, Banken und der öffentliche Sektor gehören beispielsweise zu den besonders gefährdeten Sektoren. Interne Richtlinien auf die Security-Training-Plattform hochzuladen, kann deshalb etwa entscheidend dazu beitragen, das Bewusstsein der Mitarbeitenden zu schärfen. Je kontextueller das Erlernte ist, desto nachhaltiger lässt es sich einprägen.

Kontext ist zugleich noch auf eine andere Art und Weise zu verstehen: So sollten Organisationen nicht nur personalisierte Lernerfahrungen anbieten, sondern auch einen Kontext schaffen, der sicheres Verhalten generell begünstigt. Durch die Integration bestimmter Komponenten und Tools in die bestehende Infrastruktur wird das sichere Verhalten der Mitarbeitenden begünstigt. Einfacher geht das mit einer datenbasierten Awareness-Plattform, die das Erkennen und Melden verdächtiger Aktivitäten erleichtert. Zum Beispiel weisen Mitarbeitende, die Zugriff auf den SoSafe Phishing-Meldebutton haben, eine 30 Prozent niedrigere Interaktionsrate mit Phishing-Mails auf als andere Mitarbeitende, denen dieses Feature nicht zur Verfügung steht. Das heißt, die Wahrscheinlichkeit, dass ein Angriff größere Schäden anrichtet, wird durch ein solches kontextuelles Feature reduziert. Ein Meldebutton hat weitere nachweisliche Vorteile:

DIE EFFIZIENZ EINES PHISHING-MELDEBUTTONS

Akzeptanzrate von E-Learnings

Modul-Abschlussquote

Damit sich Mitarbeitende relevantes Wissen zu sicheren Verhaltensweisen aneignen und pflegen können, sollten Organisationen also zum einen personalisierte Lernerfahrungen bieten und zum anderen die passenden kontextuellen Tools bereitstellen, die sicheres Verhalten begünstigen. Die Mitarbeitenden erkennen so, wie wichtig ihr Verhalten für die Sicherheit der Organisation ist, werden dadurch in ihrem Verantwortungsgefühl bestärkt und sind eher gewillt, an ihren Lernfortschritt anzuknüpfen.

Beispiele für verhaltensbasierte Kennzahlen in der Dimension „Kontext“

- → Engagement-Rate mit/ohne personalisierte Lernpfade
- → Phishing-Meldequote mit integrierten Reporting-Tools
- → Einfluss der Nutzung von Reporting-Tools auf die E-Learning-Abschlussquote

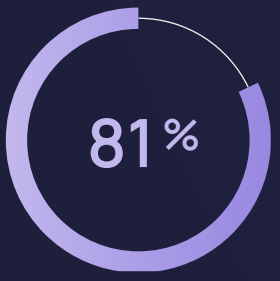
3.3 Motivation: Mitarbeitende motivieren für besseren Lernerfolg

Die Befähigung, Motivation und Kenntnisse der Mitarbeitenden tragen maßgeblich zu einer starken Sicherheitskultur bei. Neben dem Zugang zu E-Learning-Tools ist es wichtig, eine aufgeschlossene Umgebung zu fördern und die gesamte Organisation, unabhängig von Positionen und Zuständigkeiten, mit einzubeziehen. Das Sicherheitsbewusstsein sollte von der Führungsebene vorgelebt werden und auf alle Teams übergehen – Vorgesetzte sollten es sich zur Mission machen, eine ganzheitliche Sicherheitskultur zu beflügeln, anstatt Sicherheitslücken nur punktuell zu schließen. Unter internen und externen Faktoren, die eine nachhaltige Sicherheitskultur ausmachen, hebt sich die Motivation besonders ab.

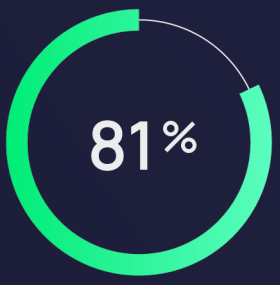
Man könnte die Motivation als qualitativen Faktor betrachten, der sich mit Zahlen nicht bemessen lässt. Doch sie kann dennoch durch verschiedene angrenzende Faktoren, wie Fortschritt, Leistung und Erfolg der User, bewertet werden. Motivation, die mit Gamification einhergeht, wirkt sich beispielsweise positiv auf das direkte Engagement aus. Im Vergleich zu traditionellen Trainings im Präsentationsstil begünstigen interaktive E-Learning-Module mit spielerischen Elementen das Interesse und die Beteiligung der Mitarbeitenden. Und diese steigern wiederum die Motivation. Bei einer von Talent LMS durchgeführten Studie gaben mehr als 80 Prozent der Teilnehmenden an, dass Gamification ihre Kreativität begünstige, sie damit besser lernten, einen besseren Bezug herstellen konnten und dass sie insgesamt ihre Zielstrebigkeit steigere.

Durch das Verfolgen der Fortschritte und das Aneignen von Wissen werden die Mitarbeitenden wie von selbst nebenbei motiviert. Zwischen der Motivation und dem Lernen besteht eine wechselseitige Beziehung – und User werden gleichzeitig dazu befähigt, richtig auf Bedrohungen zu reagieren.

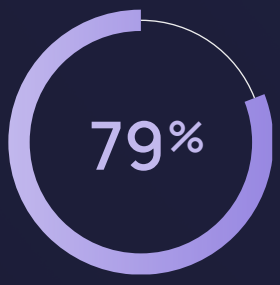
Gamification spornt zu mehr **Kreativität, Freiheit** und **Verantwortungsbewusstsein** an



Gamification hilft mir, mich **sozial besser integriert** zu fühlen und schafft ein **Gefühl der Zugehörigkeit**



Gamification hilft mir, zu **lernen** und mich persönlich und beruflich **weiterzuentwickeln**



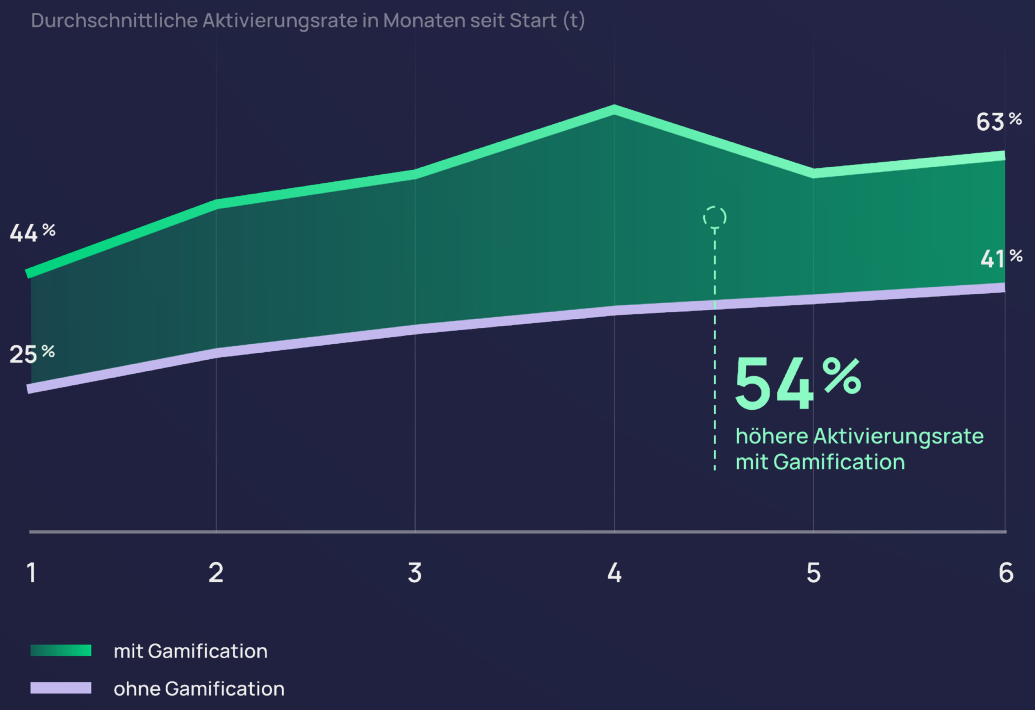
Gamification schafft ein **Gefühl der Sinnhaftigkeit** am Arbeitsplatz

Quelle:
TalentLMS (2018). The 2018 Gamification At Work Survey.

Moderne Awareness-Plattformen wie SoSafe, die auf verhaltenspsychologischen Prinzipien basieren, haben sich in dem komplexen Themenbereich der Cybersicherheit als äußerst motivierend erwiesen. Gamification nimmt Mitarbeitende mit auf einen Weg durch eine spannende Geschichte, durch Challenges auf verschiedenen Levels und versüßt diesen Weg mit wohlverdienten Belohnungen. Das Ergebnis? Eine um mehr als 50 Prozent erhöhte Aktivierungsrate. Wenn Mitarbeitende Sicherheitsthemen langweilig und kompliziert finden, fehlt ihnen die intrinsische Motivation, mehr darüber zu lernen. Hinzu kommt, dass in der heutigen, geschäftigen Arbeitswelt viele das Gefühl haben, keine Zeit für solche Themen zu haben. Die Integration typischer Videospielelemente in die Lernerfahrung steigert den Spaßfaktor und motiviert dazu, immer weiter zu lernen.

PRODUKTNUTZUNG

Gamification steigert Motivation und Security Awareness – und macht Spaß



Durch eine immersive Lernerfahrung erhalten Mitarbeitende Feedback in Echtzeit, damit sie nicht nur verstehen, wie sie handeln müssen, sondern auch die Gründe dafür kennen. Und ihre Motivation wird durch Belohnungen während ihres Lernprozesses aufrechterhalten.

Beispiele für Kennzahlen in der Dimension „Motivation“

- → E-Learning-Aktivierungsrate
- → Einfluss von Gamification auf E-Learning-Abschlussquoten

3.4 Verhalten: Sicheres Verhalten geht „in Fleisch und Blut“ über

Sicheres Verhalten ist das zentrale Element einer starken Sicherheitskultur – was die zuvor erläuterten Kennzahlen bestätigen. Der Schutz Ihrer Organisation steht und fällt mit den sicheren Gewohnheiten Ihrer Mitarbeitenden; sei es, dass sie ihren Bildschirm sperren, wenn sie den Schreibtisch verlassen, ihre E-Mails auf verdächtige Aktivitäten scannen oder die IT-Abteilung zeitnah über Risiken und Zwischenfälle informieren. Indem wir auswerten, inwieweit das Awareness-Training Verhaltensweisen beeinflusst, können wir die Maßnahmen kontinuierlich anpassen und Cyberrisiken somit effektiv minimieren.

Inzwischen sollte deutlich geworden sein, wie stark tägliche digitale Gewohnheiten am Arbeitsplatz von den anderen drei Dimensionen abhängen: Nur wenn sich Mitarbeitende mit Informationssicherheit auskennen, wenn sie im richtigen Kontext lernen und wenn sie intrinsisch motiviert sind, werden sie zuverlässig sichere Gewohnheiten pflegen. Sei es der gesteigerte Wissenserhalt durch Spaced Learning, der Einfluss von Motivation auf die Engagement-Rate oder die Phishing-Meldequote, die ansteigt, indem wir Mitarbeitende zu sicherem Verhalten befähigen: All diese Kennzahlen veranschaulichen, dass eine starke Sicherheitskultur einen ganzheitlichen Ansatz erfordert. Sich allein auf eine der vier Dimensionen zu fokussieren oder mit dem Ziel der Compliance punktuell Präsentationen zum Thema Sicherheit abzuhalten, ist bei der heutigen dynamischen Cyber-Bedrohungslage wenig erfolgreich.

Stattdessen sollten Verantwortliche Insights aus allen vier Dimensionen des Behavioral-Security-Modells nutzen, um ihr Awareness-Training so anzupassen, dass sicheres Verhalten bei Mitarbeitenden „in Fleisch und Blut“ übergehen kann.

Beispiele für Kennzahlen in der Dimension „Verhalten“

- → Phishing-Meldequote via Reporting-Tools
- → Interaktionsraten mit Phishing-Mails und -Webseiten
- → Tägliche/wöchentliche Nutzungsraten des Passwortmanagers
- → Differenzierte Phishing-Klickraten nach psychologischen Taktiken
- → „Time to reporting“ (Zeit bis zur Meldung eines Vorfalls)

04 Warum es sich rentiert, sicheres Verhalten zu messen

Die Stärke der organisationseigenen Sicherheitskultur hängt von verschiedenen Faktoren ab, die sichere Gewohnheiten beeinflussen. Um die Security Awareness Ihrer Mitarbeitenden nachhaltig zu stärken, sollten Sie ihnen auf ihrem Risiko- und Wissenslevel begegnen. Die vier Dimensionen unseres Behavioral-Security-Modells – Wissen, Kontext, Motivation und Verhalten – stehen in ständiger Wechselwirkung beim Aufbau dieser Security Awareness jenseits standardisierter Checklisten.

Mitarbeitende über immersive Lernerfahrungen zu befähigen, ist nicht nur äußerst motivierend, sondern auch effektiv. Eine Tatsache, die sich auch beim Bemessen ihres Verhaltens bestätigt. Mit einem Blick auf die richtigen verhaltensbasierten Kennzahlen erkennen Sie, welche Gewohnheiten gestärkt wurden und wo es noch Nachholbedarf gibt. Anstatt die Wichtigkeit von Awareness-Trainings zu ignorieren, sollten Organisationen ihren Mitarbeitenden proaktiv mit gutem Beispiel vorangehen und die Weichen für das Training stellen.

Wie viel Mitarbeitende über Informationssicherheit wissen und wie sie bei einer Cyberbedrohung reagieren, sollte nicht auf Vermutungen basieren. Ein Security-Awareness-Programm, das Wissen vermittelt und festigt und dadurch Unachtsamkeit in sichere Gewohnheiten umwandelt, ist vielmehr der richtige Ansatz. Messen Sie die erzielten Veränderungen, um Bereiche zu identifizieren, in denen Ihre Organisation Nachholbedarf hat. Und währenddessen erweitern Ihre Mitarbeitenden ihre Kenntnisse und eignen sich Wissen an, das außer Ihren Daten vor allem eines schützt: ihren Lernerfolg.

Moderne Awareness-Lösungen wie SoSafe bieten verhaltensbasierte Daten, die über den Lernerfolg Auskunft geben und gleichzeitig bestehende Schwachstellen aufzeigen, an denen dringender Handlungsbedarf besteht. Außerdem zeigen Ihnen auf Sicherheitsrisiken bezogene Empfehlungen auf, wie Sie mögliche Bedrohungen erkennen, verstehen und effektiv abwehren können.

Stärken Sie die Sicherheitskultur Ihrer Organisation!

SoSafe hilft Organisationen, ihre Sicherheitskultur aufzubauen und menschliche Cyberrisiken zu minimieren. Die psychologisch fundierte und DSGVO-konforme Awareness-Plattform setzt auf personalisierte Lerninhalte und intelligente Angriffssimulationen. Mitarbeitende lernen so, sich aktiv vor Online-Bedrohungen zu schützen. Die Plattform ist einfach implementier- und skalierbar; umfassende Analysen messen den ROI und zeigen Schwachstellen auf. Damit fördert SoSafe das sichere Verhalten aller Mitarbeitenden.

Motivierendes Micro-Learning

Eine psychologisch fundierte Lernplattform, die Mitarbeitende lieben:

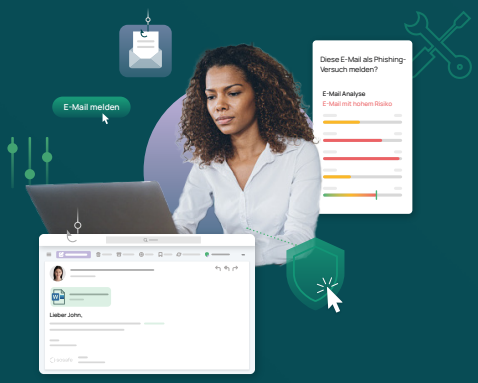
Stärken Sie die Resilienz Ihrer Organisation gegenüber Cybergefahren und erfüllen Sie Compliance-Anforderungen mit dynamischen und effektiven Lernerfahrungen, die nachhaltig das sichere Verhalten Ihrer Mitarbeitenden fördern.

- → Story-basierte, gamifizierte Lerninhalte, die im Gedächtnis bleiben
- → Stets aktualisierte Bibliothek mit sorgfältig ausgewählten Lernmodulen
- → Content-Management-Optionen und einfache Anpassung der Plattform an Ihre Bedürfnisse

Smarte Angriffssimulationen

User-zentrierte Phishing-Simulationen, die sicheres Verhalten fördern:

Helfen Sie Ihrem Team mit automatisierten Spear-Phishing-Simulationen Cyberangriffe zu erkennen und sorgen Sie für kontinuierliche Awareness-Momente – damit Cyberrisiken und entscheidende Reaktionszeit bei Vorfällen reduziert werden können.



- → Personalisierte und realistische Phishing-Angriffssimulationen
- → Kontextbasierte Lernseiten, die sichere Verhaltensweisen festigen
- → Reporting von Angriffen mit nur einem Klick via Phishing-Meldebutton

Strategisches Risk Monitoring

Umfassendes Human Risk Dashboard, um Schwachstellen proaktiv zu begegnen:

Nutzen Sie umfassende Analytics-Optionen, um die Cyberrisiken in Ihrer Organisation zu verstehen, zu minimieren und den Erfolg Ihrer Awareness-Maßnahmen zu interpretieren – für datengestützte Entscheidungen.

- → Tracking von kontextuellen Daten inklusive technischer und psychologischer KPIs
- → Branchen-Benchmarking und klare Handlungsempfehlungen für Optimierungen
- → Basierend auf ISO/IEC-27001-Anforderungen und einem Privacy-by-Design-Ansatz

SoSafe GmbH
Lichtstrasse 25a
50825 Köln

info@sosafe.de
www.sosafe-awareness.com/de
+49 221 65083800

Haftungsausschluss: Die Inhalte dieses Dokuments wurden mit größtmöglicher Sorgfalt recherchiert. Eine Haftung für die Richtigkeit, Vollständigkeit und Aktualität kann jedoch nicht übernommen werden. SoSafe übernimmt insbesondere keinerlei Haftung für eventuelle Schäden oder Konsequenzen, die durch die direkte oder indirekte Nutzung entstehen.

Copyright: SoSafe räumt das kostenlose, räumlich und zeitlich unbeschränkte, nichtexklusive Recht an der Nutzung, Vervielfältigung und Verbreitung des Werkes oder Teilen davon ein, sowohl zu privaten als auch zu kommerziellen Zwecken. Nicht gestattet ist die Änderung oder Abwandlung des Werkes, sofern diese nicht technisch notwendig sind, um die zuvor genannten Nutzungen zu ermöglichen. Dieses Recht steht unter der Bedingung, dass stets die Urheberschaft der SoSafe GmbH und, insbesondere bei ausschnittweiser Nutzung, dieses Werk unter seinem Titel als Quelle angegeben werden. Soweit möglich und zweckmäßig soll außerdem die URL, unter der SoSafe das Werk zur Verfügung stellt, angegeben werden.