Der 2023 Leitfaden zur Reduzierung des menschlichen Cyber-Risikos

Erfahren Sie, wie Sie die Mitarbeitersicherheit Ihres Unternehmens gegen menschliches Versagen und sich entwickelnde Cyber-Bedrohungen verbessern können.

SPIE

Menschen vom 'schwächsten Glied' umwandeln ....

Mitarbeiter gelten seit langem als das 'schwächste Glied' in der Cyber-Sicherheitskette eines Unternehmens, und da menschliches Versagen immer noch die häufigste Ursache für Datenschutzverletzungen ist, wurde diese unerwünschte Krone zu Recht seit geraumer Zeit behoben.

Auch wenn Organisationen mehr Zeit und Geld für die Bekämpfung menschlicher Cyberrisiken aufwenden, plagen mitarbeiterbezogene Sicherheitsvorfälle die Unternehmen auch im Jahr 2022. Aber warum war das so?

Einfach ausgedrückt: Viele Unternehmen tun einfach nicht genug, um sich entwickelnde Bedrohungen zu bekämpfen. Da Cyberkriminelle fortschrittlichere Techniken verwenden, um Menschen auszunutzen, reicht die traditionelle Methode der einmal jährlich stattfindenden Sicherheitsbewusstseinsschulung einfach nicht aus, um die heutigen Unternehmen vor dem Verlust sensibler Informationen, Reputationsschäden und finanziellen Folgen zu schützen.

95%

According to IBM, 95% of cyber security breaches result from human error.

$4.5M

IBM also reports the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

36%

Verizon's 2023 DBIR found that 36% of all data breaches involved phishing.

...in ein Cyber Security Asset.

Die gute Nachricht ist, dass sich die Lösung für benutzerorientierte Sicherheit in den letzten Jahren durch die Einführung von Human Risk Management (HRM) weiterentwickelt hat und ein viel robusteres Schutzniveau für Unternehmen aller Größen und Branchen bietet. In diesem Leitfaden erfahren Sie, warum Mitarbeiter eine Insider-Bedrohung darstellen und wie Sie sicheres menschliches Verhalten in Ihrem Unternehmen fördern können.

Menschen vom 'schwächsten Glied' umwandeln ....

Mitarbeiter gelten seit langem als das 'schwächste Glied' in der Cyber-Sicherheitskette eines Unternehmens, und da menschliches Versagen immer noch die häufigste Ursache für Datenschutzverletzungen ist, wurde diese unerwünschte Krone zu Recht seit geraumer Zeit behoben.

Auch wenn Organisationen mehr Zeit und Geld für die Bekämpfung menschlicher Cyberrisiken aufwenden, plagen mitarbeiterbezogene Sicherheitsvorfälle die Unternehmen auch im Jahr 2022. Aber warum war das so?

Einfach ausgedrückt: Viele Unternehmen tun einfach nicht genug, um sich entwickelnde Bedrohungen zu bekämpfen. Da Cyberkriminelle fortschrittlichere Techniken verwenden, um Menschen auszunutzen, reicht die traditionelle Methode der einmal jährlich stattfindenden Sicherheitsbewusstseinsschulung einfach nicht aus, um die heutigen Unternehmen vor dem Verlust sensibler Informationen, Reputationsschäden und finanziellen Folgen zu schützen.

95%

According to IBM, 95% of cyber security breaches result from human error.

$4.5M

IBM also reports the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

36%

Verizon's 2023 DBIR found that 36% of all data breaches involved phishing.

...in ein Cyber Security Asset.

Die gute Nachricht ist, dass sich die Lösung für benutzerorientierte Sicherheit in den letzten Jahren durch die Einführung von Human Risk Management (HRM) weiterentwickelt hat und ein viel robusteres Schutzniveau für Unternehmen aller Größen und Branchen bietet. In diesem Leitfaden erfahren Sie, warum Mitarbeiter eine Insider-Bedrohung darstellen und wie Sie sicheres menschliches Verhalten in Ihrem Unternehmen fördern können.

Menschen — Die Ursache Nr. 1 für Cyber-Sicherheitsverletzungen

74 % der Datenschutzverletzungen betreffen die menschliche Komponente

Verizon 2023 Untersuchungsbericht zu Datenschutzverletzungen

Fahrlässige Mitarbeiter verursachen etwa 62 % der Sicherheitsvorfälle

60 % der Unternehmen haben mehr als 20 Vorfälle von Insider-Angriffen in einem Jahr

82 % der IT-Führungskräfte sehen ein größeres Risiko von Insider-Bedrohungen, wenn ihr Unternehmen eine dauerhafte hybride Arbeitsstruktur einführt

98 % der Unternehmen geben an, dass sie sich in gewissem Maße anfällig für Insider-Bedrohungen fühlen

Was sind die wichtigsten Arten von Insider-Bedrohungen?

Fahrlässige Insider

Fahrlässige Insider - z.B. ein Mitarbeiter, der eine E-Mail fehlleitet oder versehentlich die falsche Datei anhängt – stellen die häufigste Bedrohung für Ihr Unternehmen dar und sind für 62 % aller Sicherheitsvorfälle verantwortlich.

Fahrlässige Insider, denen ihre Zugangsdaten gestohlen wurden

Fahrlässige Insider mit gestohlenen Zugangsdaten - z.B. ein Mitarbeiter, dessen Benutzername und Passwort im Dark Web preisgegeben werden – machen 25 % aller Sicherheitsvorfälle aus.

Böswillige Insider

Böswillige Insider – z. Mitarbeiter oder ehemalige Mitarbeiter mit böswilligen Motiven gegenüber dem Unternehmen, wie z. B. ein verärgerter Mitarbeiter, der kürzlich entlassen wurde, machen 13 % der Vorfälle aus.

Warum sind Mitarbeiter eine Insider-Bedrohung?

1

Menschen machen Fehler

Wir alle machen Fehler. Tatsächlich sagen 43 % der Mitarbeiter, dass sie bei der Arbeit einen Fehler gemacht haben, der die Cybersicherheit gefährdet hat, wie z. B. die Fehlleitung einer E-Mail. Das Problem ist, dass diese Art von ‚kleinen" Fehlern dazu führen können, dass vertrauliche Daten offengelegt werden, die Angreifer Experten für deren Ausnutzung sind.

2

Menschen sind Ziele

Viele Ihrer Unternehmensinformationen können online gefunden werden, einschließlich Ihrer Lieferanten, Auftragnehmer und Kunden. Dies macht es Angreifern leicht, sich als interne und externe Kontakte auszugeben, und es genügt, wenn eine Person erfolgreich hinters Licht geführt wird, damit Ihr Unternehmen einem ernsthaften Angriff ausgesetzt ist.

3

Menschen brechen die Regeln

Menschen in jedem Geschäft sind in der Lage, die Regeln zu brechen, sei es böswillig oder versehentlich. Aber ein großer Teil der Regelverstöße geht über die Nichteinhaltung von Passwortrichtlinien hinaus – einige Mitarbeiter können sogar so weit gehen, Unternehmensdaten zu stehlen und diese im Darknet zu verkaufen.

88%

Die Stanford University führt 88 % der Datenschutzverletzungen auf menschliches Versagen zurück, sogar mehr als Verizon.

Im Jahr 2022 Phishing Angriffe waren mit 36 % der Verstöße verbunden, ein Anstieg von 11 %.

45%

der Mitarbeiter wären bereit, Unternehmensinformationen an Personen außerhalb ihrer Organisation zu verkaufen.

43 % der Mitarbeiter sagen, dass sie bei der Arbeit einen Fehler gemacht haben, der die Sicherheit gefährdet hat.

25 % der Mitarbeiter glauben, dass sie bei der Arbeit auf eine Phishing-E-Mail geklickt haben.

70%

von böswilligen Insider-Verstößen sind finanziell motiviert, hauptsächlich durch den Verkauf von Anmeldeinformationen im Dark Web.

4 Hauptursachen für eine benutzerbezogene Datenschutzverletzung

Menschlicher Fehler

Ein Mitarbeiterfehler, wie ein einfacher Tippfehler, kann klein erscheinen … aber die Auswirkungen können enorm sein. Für viele Unternehmen hat ein durch menschliches Versagen verursachter Verstoß zu Bußgeldern, dem Verlust des Kundenvertrauens und dem Verlust des Zugriffs auf Daten geführt.

Häufige Wege, wie riskantes Mitarbeiterverhalten zu einem Sicherheitsvorfall führen kann

- Passwörter über mehrere Konten hinweg teilen, aufschreiben oder wiederverwenden
- Sorgloser Umgang mit Daten, wie Eingabe des falschen E-Mail-Empfängers oder Anhängen der falschen Datei
- Mangelndes Bewusstsein für gängige Bedrohungen wie Spear-Phishing-E-Mails
- Nicht verstanden haben, dass Sicherheit in der Verantwortung aller Mitarbeiter liegt und nicht nur ein Problem der IT-Abteilung

Mitarbeiter fällt auf einen Phishing-Angriff herein

Die häufigste Art und Weise, wie ein Mitarbeiter eine Sicherheitsverletzung verursacht, besteht darin, auf einen Phishing-Angriff hereinzufallen.

Und da Phishing zielgerichteter und ausgeklügelter denn je ist, fällt es Mitarbeitern immer schwerer, diese Angriffe zu erkennen.

Die cleveren Techniken, mit denen Angreifer Ihre Mitarbeiter anlocken

- **Spear Phishing —** Diese hyperpersonalisierten Angriffe zielen auf eine bestimmte Person oder Gruppe ab, wobei der Angreifer zuvor Nachforschungen über ein oft hochrangiges Ziel anstellt.
- **Unternehmens-E-Mail-Kompromittierung –** Wenn ein Angreifer Zugriff auf ein legitimes E-Mail-Konto erhält, kann er ‚Kollegen" ausnutzen, indem er sich über einen BEC-Angriff als vertrauenswürdige Quelle ausgibt.
- **Domain-Spoofing –** Ein Angreifer kann den Anzeigenamen und die Absenderadresse einer E-Mail fälschen, damit es so aussieht, als käme sie aus dem Unternehmen oder von einem vertrauenswürdigen Anbieter.

Missbrauch von Anmeldeinformationen durch Mitarbeiter

Das Kennwortverhalten von Mitarbeitern spielt eine große Rolle bei Sicherheitsvorfällen, wobei 61 % der Sicherheitsverletzungen gestohlene Zugangsdaten betreffen und Unternehmen durchschnittlich 4,37 Millionen US-Dollar kosten.

Durch die Wiederverwendung desselben Passworts für mehrere Konten kann ein Angriff eines Drittanbieters ein Portal für menschliche Risiken für Ihr Unternehmen schaffen.

Der Weg zu kompromittierten Anmeldeinformationen

1. Mitarbeiter melden sich mit derselben geschäftlichen E-Mail-Adresse und demselben Kennwort für mehrere Dienste von Drittanbietern an.
2. Ein Drittanbieterdienst erleidet eine Datenpanne, wodurch die Anmeldedaten des Benutzers offengelegt werden.
3. Die Zugangsdaten werden im Dark Web verkauft, mit denen Angreifer potenziell Zugriff auf mehrere Konten erhalten können.

Im Darknet

- Das Dark Web ist 500x größer als das Surface Web.
- Seit 2017 ist die Dark-Web-Aktivität um 300 % gestiegen.
- Im Jahr 2020 wurden dem Dark Web mehr als 22 Milliarden Datensätze hinzugefügt.
- 60 % der im Dark Web verfügbaren Informationen könnten Unternehmen potenziell schaden.

Ein Mangel an Sicherheitsrichtlinien und -prozessen

Informationssicherheitsrichtlinien helfen, das Verhalten der Mitarbeiter beim Umgang mit Unternehmensinformationen und der Sicherheit von IT-Systemen zu lenken.

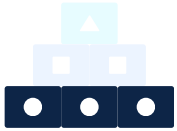
Ohne diese Richtlinien ist es unwahrscheinlicher, dass Mitarbeiter wissen, wem sie Phishing-Angriffe melden sollten oder wer auf welche sensiblen Daten zugreifen darf.

Richtlinien können zur Risikominderung beitragen?

- Sie schützen die kritischen Informationen Ihres Unternehmens, indem sie die Sicherheitsverantwortlichkeiten der Mitarbeiter klar umreißen.
- Sie verhindern unbefugte Offenlegung, Unterbrechung, Verlust, Zugriff, Verwendung oder Änderung der Informationsbestände einer Organisation.

Gute Politikbeispiele

- Richtlinie zur akzeptablen Nutzung
- Richtlinie zu vertraulichen Daten
- E-Mail-Richtlinie
- Richtlinie zur Reaktion auf Vorfälle
- Netzwerksicherheitsrichtlinie
- Kennwortrichtlinie
- Physische Sicherheitsrichtlinie



Etablieren Sie eine sicherheitsorientierte Kultur — Die Grundlagen

Eine ‚Sicherheitskultur" zielt darauf ab, alle Mitarbeiter zu ermutigen, über Sicherheit nachzudenken und sie mit denselben Werten anzugehen, und Menschen zu ermutigen, die gewünschten Verhaltensweisen zu befolgen, die die Sicherheit von Mitarbeitern, Kunden und Lieferanten gewährleisten. Der Aufbau dieser Kultur erfordert eine Reihe von Faktoren, darunter Beständigkeit, Zeit und Mühe. Hier sind einige der wichtigsten Bausteine für die Schaffung einer sicherheitsbewussten Belegschaft.

Holen Sie sich Unterstützung von oben

Die Unterstützung durch die Geschäftsleitung ist entscheidend für den Erfolg jeder Human Risk Management-Initiative. Wir meinen nicht nur eine ‚Send-to-all"-E-Mail des CEO – wir meinen das Führungsteam, das seine volle Unterstützung für diese Initiative durch regelmäßige Mitteilungen an die Mitarbeiter, die Zuweisung des erforderlichen Budgets und die Schaffung spezifischer Geschäftsrollen demonstriert.

Konstanz und Engagement sind entscheidend

Der Schlüssel zum Aufbau und zur Aufrechterhaltung einer sicherheitsbewussten Belegschaft liegt in Form einer konsistenten und langfristigen Benutzerschulung, wie in einem Bericht von Keepnet Labs hervorgehoben wird, in dem eine konsequente Schulung des Sicherheitsbewusstseins nachweislich die Phishing-Anfälligkeit der Mitarbeiter um insgesamt 60 % reduziert den Weg nach unten auf 10 % innerhalb der ersten 12 Monate.

Zeit, nicht Budget, ist der Blocker, den es zu schlagen gilt

Laut dem Bericht ‚Managing Human Cyber Risk" von SANS verbringen 75 % der Sicherheitsexperten weniger als die Hälfte ihrer Zeit mit Sicherheitsbewusstsein, obwohl ein größeres Engagement für Schulungen mit einer Zunahme positiver Verhaltensänderungen korreliert.

Behandeln Sie die Sicherheit als die Verantwortung aller

Mitarbeiter müssen verstehen, dass Cybersicherheit in der Verantwortung jedes Mitarbeiters liegt, nicht nur der IT-Abteilung. Mitarbeiter erhalten mehr Zugriff auf Computer und Online-Ressourcen als je zuvor und werden weithin als das größte Risiko eines Unternehmens angesehen. Es ist wichtig, dass die Menschen wissen, wie wichtig es ist, zusammenzuarbeiten, um letztendlich Cybersicherheit zu erreichen.

Gehen Sie über die Schulung des Sicherheitsbewusstseins hinaus

Schulungen zum Sicherheitsbewusstsein sind eine großartige Möglichkeit, das menschliche Cyberrisiko zu verringern, da 80 % der Unternehmen bei der Schulung von Mitarbeitern eine Verringerung der Phishing-Schwachstelle feststellen. Um jedoch eine wirklich widerstandsfähige Belegschaft gegen sich entwickelnde Bedrohungen aufzubauen, müssen Richtlinien implementiert und regelmäßig praktische Bewertungen wie Phishing-Simulationen durchgeführt werden.

Entscheidend ist die strategische Ausrichtung

SANS berichtet auch, dass Führungskräfte langfristige, strategische Investitionen in Menschen tätigen müssen, genau wie sie es bei anderen Sicherheitsbemühungen wie Schwachstellenmanagement, Reaktion auf Vorfälle oder Sicherheitsbetriebszentren tun würden, um menschliche Risiken effektiv zu managen.

Human Risk Management (HRM) implementieren — Die Grundlagen

Human Risk Management (HRM) ermöglicht es Unternehmen, ihre laufende Sicherheitslage für Mitarbeiter gegen sich entwickelnde Cyber-Bedrohungen und menschliches Versagen zu bewerten, zu reduzieren und zu überwachen. Da diese Bedrohungen immer komplexer und ausgefeilter werden, bietet HRM eine umfassende Lösung, um sicheres menschliches Verhalten zu fördern, anstatt sich nur auf Benutzerschulungen zu verlassen, in der Hoffnung, dass etwas hängen bleibt. Es gibt vier Schlüsselelemente für HRM:

Fördern Sie ein sicheres Benutzerverhalten

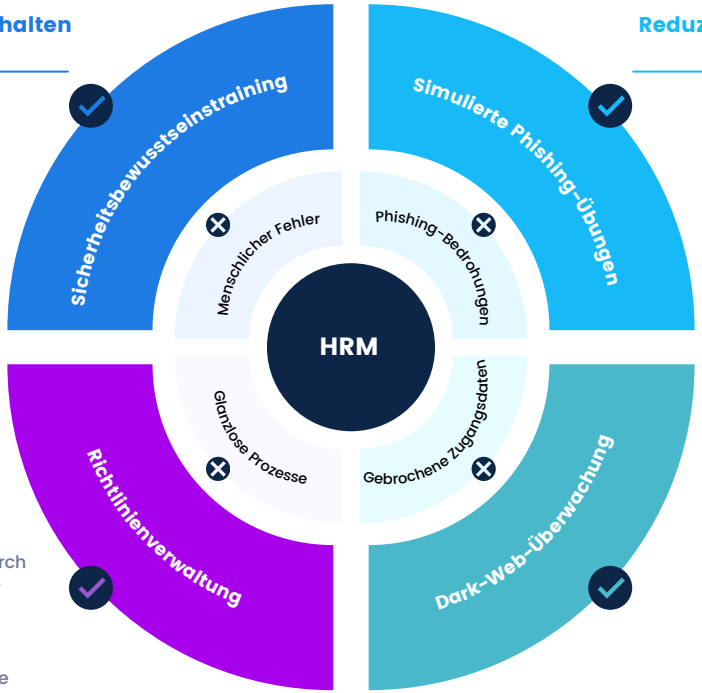
Das **Sicherheitsbewusstseinstraining** ist einer der effektivsten Ansätze zur Reduzierung des menschlichen Cyberrisikos, wobei Unternehmen einen ROI zwischen 69 und 562 % erwarten (Osterman Research).

Diese Sitzungen, die über computergestützte Schulungen durchgeführt werden, sollten regelmäßig und kurz sein und eine Vielzahl von Kernthemen der Informationssicherheit und Compliance abdecken.

Sicherheitsprozesse verbessern

Die Implementierung eines **Richtlinienverwaltungsprozesses** hilft den Mitarbeitern, ihre Verantwortlichkeiten zu verstehen und entsprechend zu handeln, wodurch der Schutz von Geschäftsinformationen und IT-Systemen verbessert wird.

Die Richtlinien sollten eine Reihe von Schlüsselbereichen ansprechen (siehe Beispiele auf der nächsten Seite) und sollten mindestens einmal jährlich aktualisiert und von den Mitarbeitern unterzeichnet werden, um die Prozesse auf dem neuesten Stand zu halten.



Reduzieren Sie die Phishing-Anfälligkeit

Phishing-Simulationen ermöglichen es Unternehmen nicht nur, die menschliche Anfälligkeit für häufige Angriffe zu bewerten, sondern bieten auch die Möglichkeit, die Benutzerschulung zu verstärken und den Fortschritt jedes Benutzers zu messen.

Idealerweise sollten Simulationen vierteljährlich durchgeführt werden, um neue und aktuelle Angriffe zu testen und gleichzeitig das Risikoniveau neuer Mitarbeiter zu bewerten.

Mindern Sie externe Bedrohungen

Da jedes Jahr Millionen von Benutzernamen, Passwörtern und Zahlungsdetails in das Dark Web geworfen werden, warnt die laufende **Dark Web-Überwachung** Unternehmen, wenn Mitarbeiterdaten kompromittiert werden.

Das Erkennen dieser frühen Bedrohungen kann letztendlich einen gezielten Angriff – und eine potenzielle Datenpanne – später verhindern.

Decken Sie das Wesentliche ab, um den Erfolg zu maximieren — Die besten Praktiken

9 Tipps zum Umgang mit langfristigen menschlichen Risiken

Erfahren Sie, was die wichtigsten Zutaten für einen erfolgreichen Human Risk Management-Ansatz sind.

- **Gestalten Sie Schulungen kurz und ansprechend** – Verwenden Sie kurze Videoschulungen, um Mitarbeiter einzubinden
- **Behandeln Sie das Wesentliche** – Stellen Sie sicher, dass wichtige Sicherheitsthemen behandelt werden (siehe diese weiter unten)
- **Mitarbeiter regelmäßig schulen** – Monatliche Schulungen halten das Wissen frisch im Gedächtnis
- **Vermeiden Sie Fachjargon** – Viele Mitarbeiter verstehen die Fachausdrücke nicht
- **Replizieren Sie häufige Phishing-Bedrohungen** – Testen Sie Ihre Mitarbeiter auf Betrugsversuche, denen sie wahrscheinlich ausgesetzt sind
- **Stellen Sie vierteljährliche Phishing**-Simulationen bereit – Dies hilft, Risiken ohne Overkill zu überwachen
- **Grundlegende Policen abdecken** – Stellen Sie sicher, dass Ihre Policenbibliothek das Wesentliche enthält (siehe unten)
- **Halten Sie die Richtlinien auf dem neuesten Stand** – Überprüfen / aktualisieren Sie die Richtlinien jedes Jahr
- **Messen Sie die Wirkung** – Verfolgen Sie die Trainingsleistung und Simulationen im Laufe der Zeit

Die wichtigsten Schulungsthemen für Ihr Personal

- Phishing-Angriffe
- Passwörter und Authentifizierung
- Sicheres Arbeiten von zu Hause aus
- Sichere Internet- und E-Mail-Nutzung
- Physische Sicherheit
- Soziale Entwicklung
- Sicherheit mobiler Geräte
- Öffentliches WLAN

Häufige Phishing-Betrügereien, die Sie an Ihren Mitarbeitern testen können

- Neue Microsoft Teams-Anfrage
- Warnung vor Coronavirus-Beratungswarnung
- Ablauf des Office 365-Kennworts
- Deaktivierung des alten OneDrive-Kontos
- Benachrichtigung über freigegebene OneDrive-Kontakte
- Starbucks-Bonus
- Informationen zur Coronavirus-Sicherheit
- Benachrichtigung über Voicemail-Nachricht

Grundlegende Sicherheitsrichtlinien zur Implementierung in Ihrem Unternehmen

- Richtlinie zur akzeptablen Nutzung
- Richtlinie zu vertraulichen Daten
- E-Mail-Richtlinie
- Richtlinie für Mobilgeräte
- Richtlinie zur Reaktion auf Vorfälle
- Netzwerksicherheitsrichtlinie
- Kennwortrichtlinie
- Physische Sicherheitsrichtlinie

Beginnen Sie noch heute mit der Reduzierung des menschlichen Cyber-Risikos

Beleuchten Sie die aktuellen menschlichen Risikobereiche Ihres Unternehmens und beginnen Sie mit dem Aufbau einer sicherheitsbewussten Belegschaft mit unserem vollständig verwalteten HRM-Service.

Wir wissen, dass Zeit, Budget und einfach nicht zu wissen, wo man anfangen soll, oft die Haupthindernisse für die Einführung eines neuen internen Prozesses sind.

Aus diesem Grund haben wir einen kostengünstigen und vollständig verwalteten Human Risk Management-Service eingeführt, der schnell implementiert und unterbrechungsfrei ist und zudem alle Schlüsselelemente für die Förderung eines sicheren Benutzerverhaltens abdeckt:

- Ansprechende und massgeschneiderte Schulungsprogramme für das Sicherheitsbewusstsein
- Regelmäßige simulierte Phishing-Bewertungen
- Kontinuierliche Darknet-Überwachung
- Grundlegende Richtlinienimplementierung mit nachvollziehbaren Mitarbeitersignaturen
- Laufendes Human Risk Scoring und regelmäßige zusammenfassende Berichte
- Vorgefertigte Kurse, Phishing-Vorlagen und Richtliniendokumente

Kontaktieren Sie uns

Nehmen Sie eine proaktive Haltung ein und beginnen Sie mit der Bekämpfung menschlicher Cyberrisiken, bevor es zu einer benutzerbezogenen Datenschutzverletzung kommt.

Anruf: +41 58 301 11 11
Email: info.ch@spie.com
Webseite: https://spie.ch/securityawareness

SPIE

Vorteile auf einen Blick

- **Steigern Sie die Widerstandsfähigkeit der Benutzer gegenüber Phishing-Angriffen**
- **Reduzieren Sie benutzerbezogene Sicherheitsvorfälle**
- **Demonstrieren Sie die Einhaltung wichtiger Standards wie ISO 27001 und GDPR**
- **Verstehen Sie die Sicherheitslage Ihrer Mitarbeiter mit einem Human Risk Score**
- **Tauchen Sie mit Schulungen, Phishing und Richtlinienberichten tief in die laufenden menschlichen Risiken ein**
- **Sparen Sie Zeit mit vorgefertigten Kursen, Phishing-Kampagnen und Richtlinienvorlagen**
- **Einfache Einrichtung, schnelle Bereitstellung und automatische Erinnerungen an Mitarbeiterschulungen**