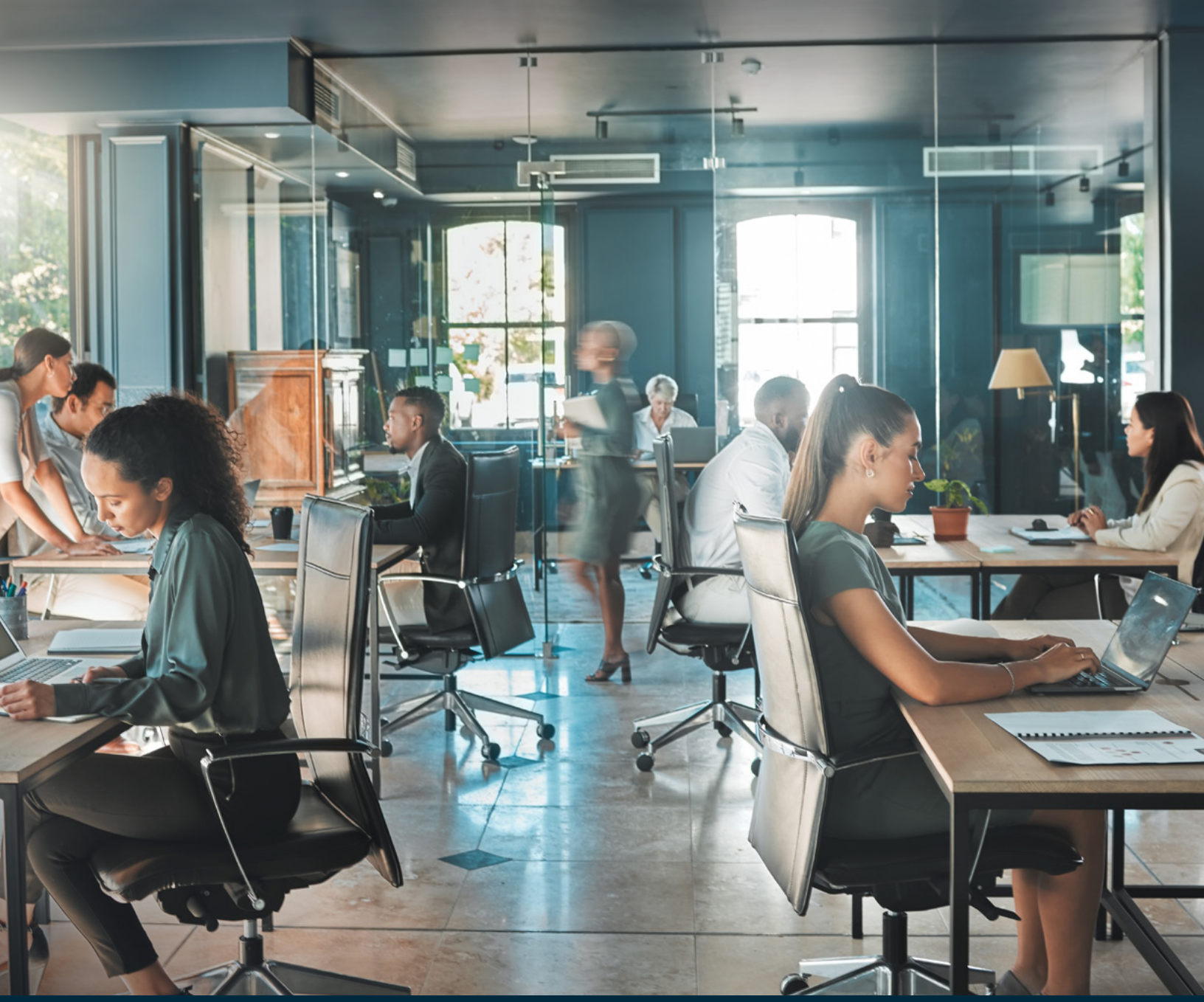
knowbe4

Wichtige Funktionen, auf die Sie bei der Beurteilung von Plattformen für Human Risk Management unbedingt achten sollten

WWW.KNOWBE4.DE

KnowBe4 Germany | Rheinstr. 45/46, 12161 Berlin – Deutschland |
KnowBe4.de | +49 30 34 64 64 60 | kontakt@knowbe4.com

04431025



Einführung

Human Risk Management (HRM) ist viel mehr als ein einfacher Entwicklungsschritt in Bezug auf Security Awareness Training (SAT). HRM verändert den Umgang von Organisationen mit durch den Faktor Mensch verursachten Sicherheitsrisiken grundlegend. Herkömmliches SAT konzentriert sich auf die Vermittlung von Wissen. HRM ist ein ganzheitlicher, datengestützter Ansatz zur Ermittlung, Messung und Minderung der durch menschliches Verhalten verursachten Risiken. Mitarbeitende werden nicht einfach nur auf Bedrohungen aufmerksam gemacht. HRM bewirkt eine Verhaltensänderung und optimiert die Entscheidungsfindung.

Die meisten Angebote auf dem Markt gehen noch immer auf rein technisch geprägte Konzepte zurück, mit denen sich nur ein Teil des Problems angehen lässt. Sie sind jedoch weit von einem echten HRM-Ansatz oder an Menschen orientierten Sicherheitsprodukten entfernt. HRM muss an der Wurzel des Problems ansetzen. Unsere Plattform rückt den Faktor Mensch, d. h. Gewohnheiten, Bewusstsein und Entscheidungsfindung, in den Mittelpunkt.

Identifizierung und Beurteilung von Risiken

Eine solide HRM-Plattform ermöglicht die Identifizierung und Beurteilung von Cyberrisiken in Bezug auf den Faktor Mensch. Es werden nicht einfach grundlegende Kennzahlen zum Sicherheitsbewusstsein bereitgestellt, sondern echte Erkenntnisse über das Verhalten der Mitarbeitenden, Schwachstellen und tägliche Bedrohungen geliefert. Damit eine HRM-Plattform das Human Risk effektiv bestimmen und messen kann, muss diese die folgenden fünf Funktionen aufweisen:

KI-gestützte Verhaltensanalyse

Die Interaktionen der Nutzerinnen und Nutzer werden über Systeme und Plattformen hinweg mithilfe von fortschrittlichen Analysen ausgewertet. Dadurch können Risikoprofile der Mitarbeitenden erstellt werden und der jeweilige Lernbedarf kann ermittelt werden. Bei der KI-gestützten Verhaltensanalyse werden die Aktionen der Nutzerinnen und Nutzer kontinuierlich überwacht und potenziell riskantes Verhalten erkannt sowie erfasst (z. B. wiederholte Klicks bei Phishing-Versuchen oder Download unsicherer Dateien). Mit diesem proaktiven Ansatz können Mitarbeitende mit hohem Risiko ermittelt und individuelle Sicherheitstrainings zusammengestellt werden.

Anpassungsfähiges Assessment

Es werden ausgefeilte Social-Engineering-Simulationen und Assessments durchgeführt, die auf den aktuellen Wissensstand und die Verhaltensmuster der Nutzerinnen und Nutzer abgestimmt sind. Diese Assessments sollten auf tatsächlichen Bedrohungen basieren und wertvolle Lerngelegenheiten bereitstellen. Indem der Schwierigkeitsgrad und die Angriffsvektoren abhängig von den Reaktionen und Antworten der Mitarbeitenden angepasst werden, wird sichergestellt, dass das Training relevant und anspruchsvoll bleibt. Mitarbeitende mit ausgeprägtem Sicherheitsbewusstsein erhalten andere Szenarien als Mitarbeitende, die sich mit den grundlegenden Konzepten schwer tun. Diese Personalisierung steigert den Lerneffekt und verhindert zugleich die Überschätzung der eigenen Fähigkeiten.

Umfassende Risikoüberwachung

E-Mails, Cloud-Anwendungen und andere Systeme werden kontinuierlich auf potenzielle Risiken überwacht, wodurch Probleme frühzeitig erkannt und Sicherheitsvorfälle verhindert werden. Bei einer effektiven Risikoüberwachung werden keine rein statischen Berichte bereitgestellt, sondern Kommunikationsmuster, Zugriffsverhalten und Gerätenutzung aktiv im Hinblick auf Abweichungen analysiert.

Auswertung des Sicherheitsstatus

Der Sicherheitsstatus der Organisation wird regelmäßig ausgewertet. Dazu gehören die Wirksamkeit von Richtlinien, die Implementierung von Technologien sowie kulturelle Faktoren in Bezug auf das Human Risk. Es werden beispielsweise Foren und Marktplätze im Internet, Deep Web und Dark Web nach offengelegten Anmeldedaten oder sensiblen Daten durchsucht, die für Angriffe gegen die Mitarbeitenden oder die Organisation genutzt werden können.

Integration von Bedrohungsdaten

Indem externe Bedrohungsdaten und von Nutzerinnen und Nutzern erfasste Sicherheitsdaten einbezogen werden, lassen sich neue Angriffsvektoren und Taktiken erkennen, die speziell auf menschliche Schwächen abzielen. Da Cyberkriminelle ihre Taktiken fortlaufend anpassen, sind Echtzeitdaten unerlässlich, um in Bezug auf Cyberbedrohungen einen Schritt voraus zu bleiben. HRM-Plattformen analysieren Daten aus globalen Bedrohungsmeldungen, Dark-Web-Aktivitäten und branchenspezifischen Angriffsmustern. So können Organisationen frühzeitig vor gezielten Phishing-Kampagnen, Credential Stuffing und Social-Engineering-Betrugsmaschen gewarnt werden.

Personalisierte Trainingsinhalte

HRM bietet mehr als ein herkömmliches SAT. Es werden stets ansprechende und personalisierte Trainingsinhalte bereitgestellt, die auf die Lernpräferenzen und Verhaltensweisen der Nutzerinnen und Nutzer abgestimmt sind. Effektives Sicherheitstraining funktioniert nicht mit einer Standardlösung – das individuelle Risikoprofil der Mitarbeitenden muss stets berücksichtigt werden. Eine solide HRM-Plattform gestaltet mithilfe von KI ein dynamisches Training, das sich basierend auf den jeweiligen Anforderungen und Verhaltensweisen weiterentwickelt. Sechs wichtige HRM-Funktionen für eine personalisierte und anpassungsfähige Lernerfahrung:

KI-gestützte Trainingsempfehlungen

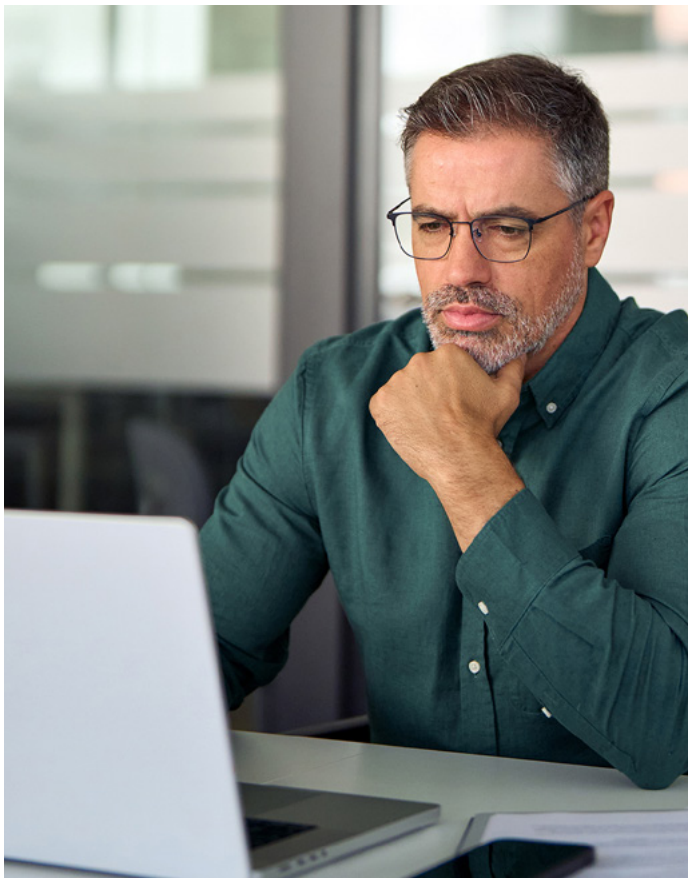
Mithilfe von KI werden relevante Trainingsinhalte automatisch ausgewählt und bereitgestellt. Dabei werden das Risikoprofil, die Rolle und der Trainingsverlauf der Mitarbeitenden berücksichtigt. Das Training ist dadurch stets anspruchsvoll, bleibt jedoch auch bewältigbar. Durch die Analyse von Verhaltensdaten und Daten zu riskanten Interaktionen in der Vergangenheit werden die KI-Empfehlungen mit der Zeit immer besser und die dringendsten Risiken priorisiert. Personalisierte Lernpfade sorgen dafür, dass die Mitarbeitenden stets motiviert sind und sich proaktiv vor neuen Bedrohungen schützen. Darüber hinaus können Sicherheitsteams anhand von KI-gestützten Erkenntnissen Trends erkennen und ihre Strategien proaktiv anpassen.

Echtzeit-Sicherheitscoaching

Mithilfe von Just-in-Time-Learning und sofortiger Rückmeldung bei riskantem Verhalten werden kontextbezogene Lerninhalte genau in dem Moment bereitgestellt, wenn ein Fehler passiert ist oder riskantes Verhalten festgestellt wird. Durch diesen proaktiven Ansatz werden das Sicherheitsbewusstsein gestärkt und sichere Verhaltensweisen verinnerlicht, ohne die Produktivität zu beeinträchtigen. Da sich das Sicherheitsbewusstsein im Laufe der Zeit immer weiter ausprägt, reduziert sich die Wahrscheinlichkeit von Fehlern, die Sicherheitsvorfälle zur Folge haben können.

Microlearning

Es werden kurze, relevante und praxisnahe Trainingsinhalte in verschiedenen Formaten bereitgestellt. Das soll Informationsüberflutung verhindern und den Lernerfolg verbessern. Komplexe Themen werden in kurzen, prägnanten Lektionen aufgegriffen, die den Mitarbeitenden wichtige Sicherheitskonzepte vermitteln, ohne sie dabei zu überfordern. Microlearning-Module lassen sich problemlos in tägliche Arbeitsabläufe integrieren. Die Mitarbeitenden beschäftigen sich dann regelmäßig mit Themen rund um Security Awareness.



Kontinuierliche Verstärkung

Anstelle von einmaligen Trainingssitzungen wird ein Prozess des kontinuierlichen Lernens und Anpassens etabliert. Dazu gehören regelmäßige Aktualisierungen, Auffrischungskurse und Beispiele aus der Praxis. Durch kontinuierliche Verstärkung wird sichergestellt, dass die Mitarbeitenden die wichtigen Lerninhalte nicht vergessen. Das Training umfasst Quizfragen, realitätsnahe Übungen und regelmäßige Erinnerungen. Gamification-Elemente wie Bestenlisten, Abzeichen und interaktive Herausforderungen fördern zusätzlich die Motivation.

Kommunikation über mehrere Kanäle

Sicherheitstipps werden über unterschiedliche Kommunikationskanäle (E-Mail, Teams, Slack, LMS, Google Chat) bereitgestellt. Trainingskonzepte werden direkt in der Umgebung verstärkt, in der sich die Mitarbeitenden befinden. Dadurch wird Security Awareness in die täglichen Arbeitsabläufe integriert und nicht isoliert behandelt. Kurze Erinnerungen, ein schnelles Quiz und interaktive Diskussionen helfen dabei, die wichtigsten Lektionen natürlich und interaktiv zu vertiefen. Darüber hinaus können Hinweise zu riskantem Verhalten über bevorzugte Kanäle bereitgestellt werden. Die Mitarbeitenden erhalten so zeitnah relevante Sicherheitsanweisungen.

Tests und simulierte Angriffe

Es werden ausgefeilte Phishing- und Social-Engineering-Simulationen durchgeführt, die auf aktuellen Bedrohungen beruhen, den Mitarbeitenden zu Übungszwecken jedoch in einer sicheren Lernumgebung präsentiert werden. Durch solch realistische Simulationen werden die Mitarbeitenden mit den neuesten Social-Engineering-Taktiken vertraut gemacht und lernen, schädliche Angriffe zu erkennen und souverän darauf zu reagieren.

Integration und Automatisierung

Eine solide HRM-Plattform bietet mehr als lose miteinander verknüpfte Tools. Sie stellt eine vollständig integrierte Umgebung für das Human Risk Management bereit. Achten Sie bei der Bewertung von HRM-Plattformen auf eine anpassungsfähige Sicherheitsarchitektur, die sich nahtlos in Ihr vorhandenes Ökosystem an Sicherheitsprodukten einfügt. Diese fünf wesentlichen Produkte/Funktionen gewährleisten Effektivität:

Sicherheitsorchestrierung und automatisierte Reaktion (Security Orchestration and Automated Response, SOAR)

Ein SOAR-Produkt automatisiert Incident-Response-Prozesse und verkürzt die Zeit zwischen der Erkennung einer Bedrohung und deren Abwendung. Gleichzeitig wird ein konsistenter Umgang mit Sicherheitsereignissen gewährleistet. Darüber hinaus kann ein HRM-basiertes SOAR-Produkt aus realen Bedrohungen sichere Trainingsmöglichkeiten generieren. SOAR-Plattformen erkennen Zusammenhänge zwischen Human-Risk-Daten und Sicherheitsvorfällen und können gezielt Maßnahmen einleiten, z. B. Just-in-Time-Training bereitstellen oder eine zusätzliche Authentifizierung anfordern. Diese nahtlose Integration von HRM und SOAR erhöht die Resilienz und ermöglicht Sicherheitsteams eine schnellere und präzisere Reaktion.

Integrierte E-Mail-Sicherheit in der Cloud (Integrated Cloud Email Security, ICES)

Es gibt einen erweiterten E-Mail-Schutz, der Verhaltensmuster der Nutzerinnen und Nutzer mit KI-gestützten Analysen kombiniert, um ausgefeilte Phishing- und Social-Engineering-Angriffe abzuwehren. Wenn ICES in HRM-Plattformen integriert ist, können schädliche E-Mails blockiert und kann ein risikobasiertes Training für Nutzerinnen und Nutzer bereitgestellt werden, die mit verdächtigen Mitteilungen interagieren. Mit diesem proaktiven Ansatz werden die Mitarbeitenden nicht nur vor E-Mail-Bedrohungen geschützt, sondern auch kontinuierlich über neue Angriffstaktiken informiert, sodass das allgemeine Sicherheitsbewusstsein gestärkt wird.

Risikominderung in Echtzeit

Artificial Intelligence Defense Agents bieten sofortigen Schutz vor neuen Bedrohungen und leisten zugleich das kontextbezogene Coaching der Nutzerinnen und Nutzer. Wenn riskantes Verhalten erkannt wird (z. B. Eingabe von Anmeldedaten auf einer mutmaßlichen Phishing-Website oder Download eines nicht verifizierten Anhangs), können Risikominderungstools in Echtzeit eingreifen und Aktionen blockieren, Warnungen senden oder weitere Verifizierungen anfordern. So entwickeln die Mitarbeitenden im Laufe der Zeit sichere Verhaltensweisen. Außerdem sinkt die Wahrscheinlichkeit, Opfer von Bedrohungen zu werden. Auch der allgemeine Sicherheitsstatus der Organisation verbessert sich.

Plattformübergreifende Integrationen

Durch die Verknüpfung mit vorhandenen Sicherheitsinfrastrukturen (Microsoft 365, CrowdStrike, Cisco, Netskope usw.) werden Bedrohungsdaten weitergegeben und es wird ein einheitliches Ökosystem an Sicherheitsprodukten aufgebaut. Eine solide HRM-Plattform agiert nicht isoliert, sondern fügt sich in Ihr vorhandenes Ökosystem ein und optimiert dieses. Durch die Integration von Endpoint Detection and Response (EDR), Identity Access Management (IAM) und Security Information and Event Management (SIEM) können HRM-Plattformen ein umfassendes Bild des Risikofaktors Mensch bereitstellen.

Automatisierte Reaktion

Bedrohungen werden automatisch unter Quarantäne gestellt und erkannte schädliche E-Mails aus dem gesamten Netzwerk der Organisation entfernt. Automatisierte Reaktionsmechanismen helfen Sicherheitsteams dabei, Bedrohungen einzudämmen, bevor sie sich ausbreiten. Der Schutz der Organisation ist somit nicht allein von manuellen Eingriffen abhängig. Wird ein Phishing-Versuch gemeldet oder erkannt, kann das System ähnliche E-Mails sofort aus allen Posteingängen entfernen und so eine weitere Gefährdung verhindern. Da automatisierte Sicherheitsmaßnahmen nicht von einer schnellen Reaktion der Nutzerinnen und Nutzer oder Sicherheitsteams abhängig sind, können Bedrohungen und Risiken deutlich besser abgewehrt werden.

Kontinuierliche Überwachung und Verbesserung

Datengestützte Erkenntnisse und anpassungsfähige Sicherheitsmechanismen sind heute unerlässlich. Der Faktor Human Risk gewinnt zunehmend an Bedeutung. Eine HRM-Plattform muss daher in der Lage sein, anhand von Echtzeitdaten dynamische Anpassungen vorzunehmen und die Risikomanagementstrategie Ihrer Organisation kontinuierlich zu stärken. Diese fünf wichtigen Funktionen sorgen dafür:

Risikobewertung

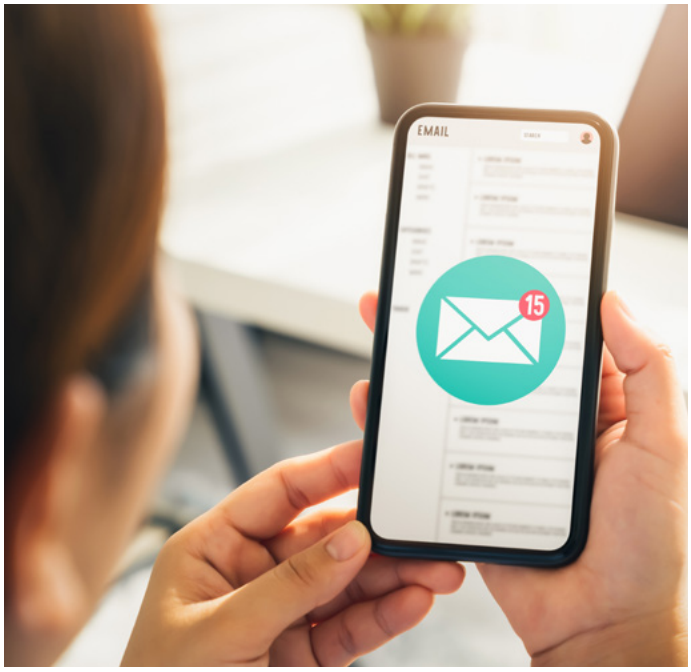
Es ist wichtig, dass dynamische Risikoprofile für alle Mitarbeitenden, Teams und Abteilungen auf der Grundlage von Verhaltensweisen, Trainingsleistungen und Sicherheitsvorfällen erstellt werden. Im Gegensatz zu statischen Bewertungen werden Echtzeit-Risikobewertungen kontinuierlich und abhängig von den Nutzeraktivitäten angepasst. Sie erhalten so stets ein aktuelles und vollständiges Bild vom Human Risk in Ihrer Organisation. Fehler in Phishing-Simulationen, die Teilnahme an Sicherheitstrainings sowie Reaktionen auf tatsächliche Sicherheitsvorfälle werden berücksichtigt. Eine solide HRM-Plattform kann die Mitarbeitenden mithilfe dieser Daten in Risikostufen einordnen, sodass Sicherheitsteams sofort erkennen, wo der größte Handlungsbedarf besteht.

Anpassungsfähige Sicherheitskontrollen

Sicherheitskontrollen und Trainingsanforderungen werden abhängig von den jeweiligen Risikostufen und Verhaltensweisen automatisch angepasst. Wenn sich Mitarbeitende wiederholt riskant verhalten, beispielsweise auf Phishing-Simulationen hereinfallen, Assessments nicht bestehen oder Sicherheitsrichtlinien nicht beachten, kann das System weitere Schutzmaßnahmen einleiten: Durchsetzung der Multi-Faktor-Authentifizierung (MFA), eingeschränkter Zugriff auf sensible Daten oder kürzere Abstände von obligatorischen Trainings. Umgekehrt kann die Häufigkeit von Trainings bei Mitarbeitenden, die sich konsequent sicherheitsbewusst verhalten, reduziert werden, da sich so Frustration verhindern und die Effizienz erhöhen lassen. Durch dynamische und responsive Sicherheitskontrollen können Organisationen einen stärker personalisierten, risikobasierten Ansatz entwickeln, der in Echtzeit auf das Verhalten der Mitarbeitenden abgestimmt wird.

Verhaltenskennzahlen und -analysen

Trainingsabschlussraten liefern keine Erkenntnisse. Kennzahlen zu tatsächlichen Verhaltensänderungen schon. Zu den aussagekräftigen Kennzahlen gehören z. B. der Phish-prone™ Percentage (der Auskunft über die jeweilige Phishing-Anfälligkeit gibt), das Level des Sicherheitsbewusstseins, die Rate der Richtlinieneinhaltung, die Rate der gemeldeten Vorfälle (einschließlich der Zeit bis zur Entdeckung) und Echtzeit-Risikoindikatoren.



Regelmäßige Neubewertung von Risiken

Indem das Human-Risik-Profil der Organisation regelmäßig neu bewertet wird, lassen sich neue Schwachstellen, aufkommende Bedrohungen und verbesserungsfähige Bereiche ermitteln. Dazu gehört auch die Bewertung, wie gut die Sicherheitskontrollen auf die Verhaltensweisen und Arbeitsabläufe abgestimmt sind. Cyberbedrohungen entwickeln sich kontinuierlich weiter. Die Effektivität von Trainings, das Verhalten der Mitarbeitenden und die Einhaltung von Richtlinien müssen regelmäßig überprüft werden. Bei einer Neubewertung von Risiken ist es ratsam, Daten zu Phishing-Simulationen, Richtlinienverstößen sowie tatsächlichen Sicherheitsvorfällen zu berücksichtigen und das Training damit kontinuierlich zu verbessern. Außerdem können Organisationen durch den Vergleich aktueller Risikotrends mit Verlaufsdaten die Effektivität ihrer Sicherheitsprogramme messen und ihre Strategien auf neue Herausforderungen anpassen.

Anpassung an Wandel

Strategien zur Bewältigung neuer Herausforderungen wie die Arbeit im Homeoffice, Generationswechsel in der Belegschaft, neue Cyberbedrohungen und der zunehmende Einsatz von KI und Automatisierung müssen immer wieder neu abgestimmt werden. Mit dem Wandel von Arbeitsumgebungen und Technologie ändern sich auch die Taktiken von Cyberkriminellen. Organisation müssen in der Lage sein, Sicherheitstrainings, Kommunikationsstrategien und Risikobewertungen auf dem neuesten Stand zu halten und neue Angriffsvektoren und Verhaltenstrends einzubinden. Da KI-gestützte Phishing-Angriffe zunehmen, müssen auch Deepfake- und Voice-Phishing-Bedrohungen in das Training einbezogen werden. Eine wirklich effektive HRM-Plattform stellt sicher, dass Sicherheitsstrategien stets relevant, proaktiv und auf die aktuelle Cyberlandschaft abgestimmt sind.

Eine solide HRM-Plattform kombiniert Risikobewertung, personalisiertes Lernen, Automatisierung und kontinuierliche Überwachung zu einem anpassungsfähigen Ökosystem an Sicherheitsprodukten, das sich mit aufkommenden Bedrohungen weiterentwickelt.
Durch den Einsatz von KI und Verhaltensanalysen überführt HRM Security Awareness von einer statischen Trainingsübung in eine dynamische, datengestützte Strategie.

Cyberbedrohungen entwickeln sich ständig weiter. Um sich zu schützen, müssen Organisationen nicht nur das Sicherheitsbewusstsein im Blick behalten, sondern danach streben, tatsächliche Verhaltensänderungen zu bewirken. Die richtige HRM-Plattform verringert nicht nur das Human Risk, sondern schafft eine stärkere Sicherheitskultur.

Lernen Sie die Vorteile von KnowBe4 für Ihre Organisation kennen:

KnowBe4.de aufrufen

Kostenloser Phishing Security Test

Wie anfällig sind Ihre Mitarbeitenden gegenüber Phishing? Unser kostenloser Phishing Security Test verrät es Ihnen.

Kostenloses Automated Security Awareness Program

Erstellen Sie ein auf Ihr Unternehmen, Ihre Institution oder Ihre Organisation abgestimmtes Security Awareness Program.

Kostenloser Phish Alert Button

Mit diesem Tool können Mitarbeitende ab sofort Phishing-Angriffe mit nur einem Klick sicher melden.

Kostenloser Email Exposure Check

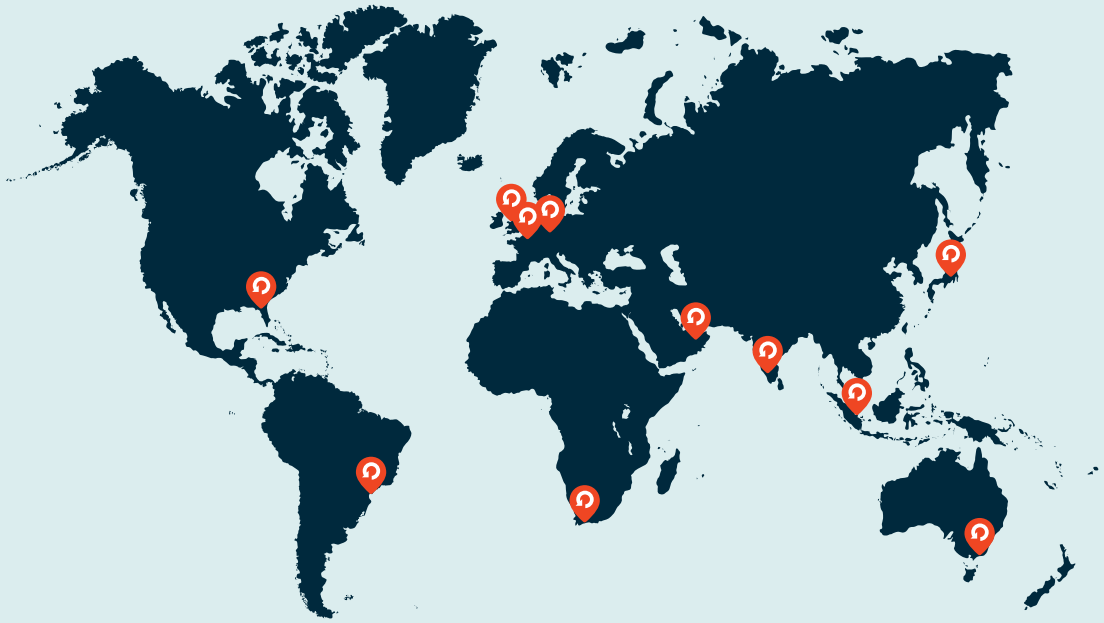
Welche Ihrer E-Mail-Anmeldedaten wurden bereits offengelegt? Werden Sie aktiv, bevor es Kriminelle tun.

Kostenloser Domain Spoof Test

Finden Sie heraus, ob Hacker E-Mail-Adressen Ihrer Domain spoofen können.

Über KnowBe4

Mit KnowBe4 treffen Belegschaften Tag für Tag bessere Sicherheitsentscheidungen. Mehr als 70.000 Organisationen nutzen KnowBe4 zur Stärkung ihrer Sicherheitskultur und zur Minderung durch den Faktor Mensch verursachter Risiken. Die umfassende und führende Plattform mit KI-Unterstützung für Human Risk Management von KnowBe4 ermöglicht den Aufbau einer flexiblen Verteidigungsinfrastruktur, die Nutzerinnen und Nutzer auf die Abwehr aktueller Cyberbedrohungen vorbereitet. In der Plattform HRM+ sind Module für Awareness and Compliance Training, Cloud-/E-Mail-Sicherheit, E-Mail-Coaching, Phishing-Abwehr durch Meldungen von Nutzerinnen und Nutzern, KI-Abwehragenten und weitere Features enthalten. Mit personalisierten und relevanten Inhalten, Tools und Methoden aus dem Kontext der Cybersicherheit transformiert KnowBe4 als einzige Sicherheitsplattform weltweit Belegschaften von der größten Angriffsfläche in die wichtigste Verteidigungslinie einer Organisation. Weitere Informationen finden Sie auf www.KnowBe4.de



knowbe4

KnowBe4 Germany | Rheinstr. 45/46, 12161 Berlin – Deutschland | KnowBe4.de |
+49 30 34 64 64 60 | kontakt@knowbe4.com