mimecast

THE STATE OF HUMAN RISK

2026

ZUSAMMENFASSUNG

Seit 2024 ist die größte Herausforderung von Cybersicherheitsexperten nicht mehr ein Mangel an Technologien, sondern das menschliche Risiko. Obwohl Unternehmen Milliarden in die Verstärkung ihrer Technologie-Stacks investieren, nimmt die Zahl an Sicherheitsverletzungen nicht ab. Die eigentliche Schwierigkeit ist allerdings nicht, dass der Mensch das schwächste Glied in der Sicherheitskette ist. Problematisch ist eher die Tatsache, dass bestehende Sicherheitsstrategien nicht weiterentwickelt wurden, um die Arbeitsweise moderner Belegschaften zu schützen.

Die meisten Sicherheitsvorfälle sind heute auf Insiderbedrohungen, Zugangsdatenmissbrauch und benutzerbedingte Fehler zurückzuführen. Angreifer hacken sich also nicht einfach so ein – zunehmend zielen sie bewusst auf die Vulnerabilität „Mensch“ ab. Sie nutzen KI-gestütztes Phishing, missbrauchen Tools für die Zusammenarbeit und umgehen die üblichen Authentifizierungsmethoden. Dadurch entstehen größere, kostspieligere Sicherheitsverletzungen, die schwieriger zu erkennen und einzudämmen sind.

In diesem neunten jährlichen „State of Human Risk“-Bericht untersuchen wir, wie Unternehmen auf diesen Wandel der Bedrohungslandschaft reagieren. Eine Umfrage unter 2.500 IT-Sicherheitsverantwortlichen und -Entscheidungsträgern aus neun Ländern zeigt, wo Unternehmen aktuell Fortschritte machen und wo es noch kritische Lücken gibt. Das Wichtigste schon einmal vorweg: 2026 reicht es für Unternehmen nicht aus, aktiv bekämpfen.

Das Problem des menschlichen Risikos: Warum Unternehmen 2026 aktiv werden müssen

Die Beweislage ist eindeutig: Die meisten Sicherheitsvorfälle sind heute auf Insiderbedrohungen, Zugangsdatenmissbrauch und benutzerbedingte Fehler zurückzuführen. Die Teilnehmer unserer Umfrage schätzen, dass ein einziger von Insidern verursachter Datenverlust, Datenabfluss oder Datendiebstahl ihr Unternehmen im Durchschnitt 11.4 Mio. EUR. USD kosten würde. Bei durchschnittlich sechs derartigen Vorfällen pro Monat, denen Unternehmen heute ausgesetzt sind, entspricht dies einem monatlichen Schadensrisiko von 68.2 Mio. EUR – oder etwa 818.0 Mio. EUR pro Jahr.

Die Lücke zwischen Sicherheitsbewusstsein und Handlungsbereitschaft

Unsere Untersuchung zeigt zwar, dass in den befragten Unternehmen allgemein ein gutes Sicherheitsbewusstsein vorhanden ist, doch die Umsetzung entsprechender Maßnahmen nur fragmentiert stattfindet. 91 % der Befragten haben Schwierigkeiten, die Compliance in ihrer Belegschaft zu gewährleisten, und 96 % beschreiben ihre Schutzmaßnahmen als unvollständig. Trotzdem implementieren nur 28 % der Unternehmen sowohl regelmäßige Schulungen zum Sicherheitsbewusstsein als auch eine kontinuierliche Überwachung auf Richtlinienverstöße. Dies sind zwei grundlegende Maßnahmen, die jedes Unternehmen ergreifen sollte, das sich ernsthaft mit menschlichen Risiken befassen möchte. Diese Diskrepanz zwischen Bewusstsein und Handlungsbereitschaft birgt ein großes Risiko,

dessen sich Unternehmen ebenfalls bewusst sind. 71 % der Befragten erwarten nämlich, dass Angriffe auf ihre Collaboration-Tools im Jahr 2026 Auswirkungen auf ihr Geschäft haben werden. Trotzdem verlassen sich 38 % immer noch ausschließlich auf native Sicherheitskontrollmaßnahmen – obwohl 64 % zustimmen, dass solche Sicherheitsvorkehrungen unzureichend sind.

Fünf kritische Lücken, die das Jahr 2026 prägen werden

2026 müssen sich Unternehmen mit fünf Sicherheitslücken auseinandersetzen, die alle eng miteinander zusammenhängen. Diese Gefahren sind mit traditionellen Abwehrmechanismen nur schwer zu bewältigen. Das große Problem ist nicht ein fehlendes Bewusstsein für diese Sicherheitslücken, sondern eine mangelnde Reaktion darauf. Unternehmen gelingt es nicht, Schwachstellen durch koordinierte Maßnahmen zu beheben, bevor die Lücke zwischen Bewusstsein und Handeln katastrophale Ausmaße annimmt.

1. Eine starke Ausweitung der Angriffsfläche:
Bedrohungen lauern heute im E-Mail-Verkehr, auf Collaboration-Plattformen und in internen Kommunikationskanälen. Leider verlassen sich 38 % der Unternehmen immer noch ausschließlich auf die nativen Sicherheitskontrollmaßnahmen dieser Tools.

2. Insiderrisiken:
Nur 8 % der Mitarbeiter sind für 80 % der Sicherheitsvorfälle verantwortlich1. Unternehmen unterscheiden drei Risikoprofile (fahrlässig, kompromittiert und böswillig), versäumen es jedoch, entsprechende Präventionsstrategien umzusetzen. Nur 28 % von ihnen kombinieren regelmäßige Schulungen zum Sicherheitsbewusstsein mit einer kontinuierlichen Überwachung.

3. Das Integrationsparadox:
65 % der befragten Unternehmen empfinden die Integration von Sicherheitstools als zu kompliziert. Doch eine erfolgreiche Implementierung führt zu einer 40 % schnelleren Bedrohungsbeseitigung und verschafft Unternehmen eine gute Einsicht in alle sicherheitsrelevanten Aspekte. Wenn ein Unternehmen seine Sicherheitstools nicht miteinander integrieren kann, entsteht früher oder später ein Chaos aus fragmentierten Tools. Und genau diese Fragmentierung hätte die Integration eigentlich lösen bzw. verhindern sollen.

4. Eine mangelnde Governance:
Die befragten Unternehmen erkennen allgemein an, wie wichtig eine gute Governance ist. Dennoch sind 59 % von ihnen nicht zuversichtlich, dass sie zeitnah die nötigen Kommunikationsdaten finden könnten, um regulatorischen Anforderungen gerecht zu werden. Wenn Unternehmen sich immer noch auf manuelle Prozesse verlassen (36 % für die Überwachung und 23 % für das Richtlinienmanagement) und die Datenmengen in ihren fragmentierten Systemen immer weiter ansteigen, werden sie früher oder später zwangsläufig mit Engpässen konfrontiert.

5. Die KI-Bereitschaftslücke:
69 % der befragten Unternehmen denken, dass sie innerhalb von 12 Monaten KI-gestützte Angriffe erleben werden. Doch nur 55 % unserer Teilnehmer nutzen KI-gestützte Tools zur Bedrohungserkennung und Echtzeitüberwachung. Unternehmen setzen eher KI-gestützte Überwachungs- und Schutztools ein (48 %) als Schulungen für Mitarbeiter zur Erkennung von KI-gestützten Angriffen (44 %) oder spezifische KI-Nutzungsrichtlinien (41 %).

[1]Diese 8 %/80 %-Statistik stammt aus dem Mimecast-Whitepaper “The Size and Shape of Workforce Risk

Der Weg in die Zukunft: Integriertes Human Risk Management

Um eine erfolgreiche Sicherheitsstrategie umzusetzen, müssen Unternehmen sich von ihren fragmentierten Systemen abwenden. Sie sollten integrierte Plattformen schaffen, die ihre menschenorientierten Initiativen, technologieorientierten Kontrollmechanismen und Governance-Rahmen effektiv miteinander koordinieren und sich gleichzeitig kontinuierlich an die Bedrohungslage anpassen. Unternehmen mit starken Sicherheitsprogrammen haben einige Gemeinsamkeiten. Sie identifizieren Hochrisikonutzer mithilfe von Verhaltensanalysen, sie passen ihre Kontrollmechanismen an die individuellen Risikoprofile der Benutzer an, sie setzen einheitliche Schutzmaßnahmen über alle Kommunikationskanäle hinweg ein, sie automatisieren die Durchsetzung von Richtlinien und sie bereiten sich mit defensiven KI-Maßnahmen sowie einer entsprechenden Governance auf KI-gestützte Bedrohungen vor.

Ein klarer Business Case

Unternehmen müssen in der Lage sein, Sicherheitsvorfälle zu verhindern, ihre Erkennungs- und Reaktionszeiten zu reduzieren, ihre Compliance-Quoten zu verbessern, die Effizienz ihrer Sicherheitsteams zu steigern und ihren Vorständen sowie Führungskräften eine messbare Risikominimierung nachzuweisen. Zusätzlich zu dem oben genannten jährlichen Insiderrisiko von 818.0 Mio. EUR sollten sie auch behördliche Strafen, ihre rechtliche Haftbarkeit und Reputationsschäden in ihren Berechnungen der potenziellen Kosten von Sicherheitsvorfällen berücksichtigen. Angesichts dieser kostspieligen Abhilfemaßnahmen für Sicherheitsvorfälle ist der ROI von Ausgaben für das Human Risk Management unbestreitbar.

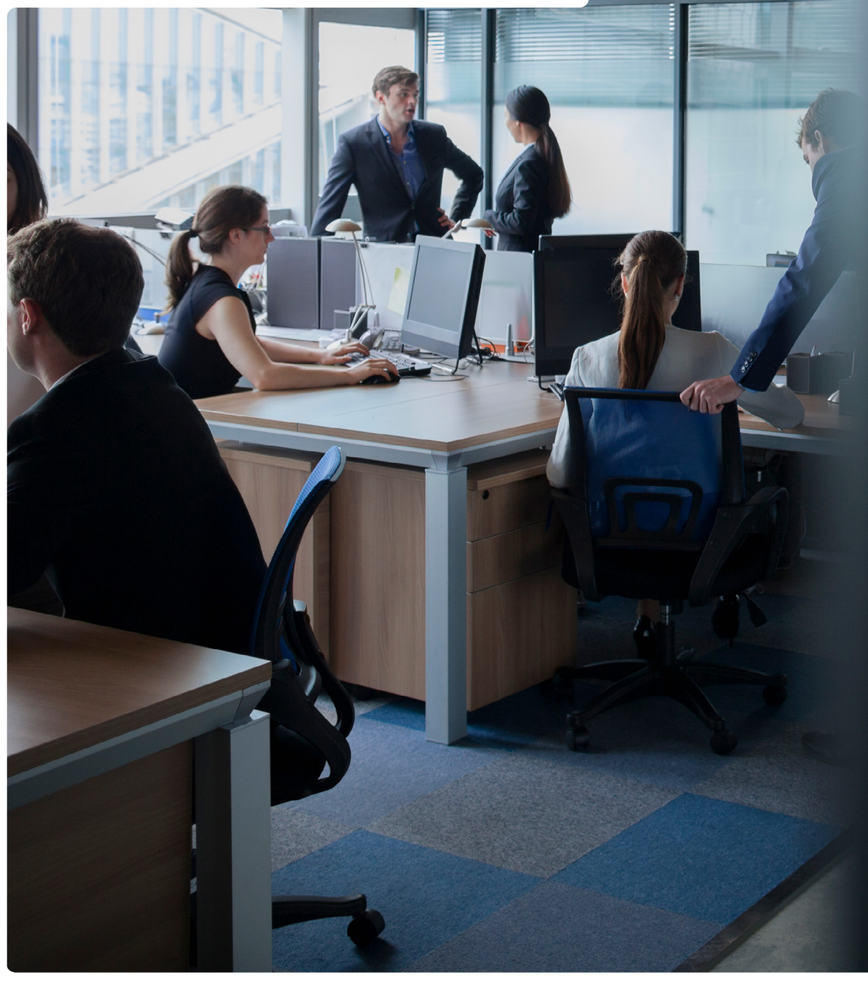
Das Jahr 2026 stellt Unternehmen vor eine wichtige Wahl

Die zentrale Sicherheitsfrage für 2026 lautet nicht, ob Unternehmen in Lösungen für den Umgang mit menschlichen Risiken investieren sollten. Die Frage ist, ob sie investieren, bevor es zum nächsten potenziell sehr kostspieligen Vorfall kommt. Diejenigen Unternehmen, die das Human Risk Management als integrierte strategische Priorität behandeln, werden sich hervortun. Diejenigen, die weiterhin mit fragmentierten Lösungen arbeiten, werden viele Herausforderungen erleben.

Methodik: Wir haben 2.500 Teilnehmer befragt (1.922 IT-Entscheider, 578 IT-Sicherheitsentscheider) in neun Ländern im November und Dezember 2025. Alle Unternehmen hatten mehr als 250 Mitarbeiter und mehr als 250 E-Mail-Nutzer. Die Unternehmensgrößen reichten von 250 bis über 10.000 Mitarbeiter.

Geografische Abdeckung: USA (500), UK (300), Deutschland (300), Frankreich (300), Spanien (200), Italien (200), Südafrika (200), Singapur (250), Australien (250)

Beteiligte Branchen: Finanzdienstleistungen, Gesundheitswesen (öffentlich und privat), IT/ Technologie/Telekommunikation, Fertigung, Einzelhandel, öffentlicher Sektor, Energie/Versorgung, Unternehmensdienstleistungen, Bauwesen, Verbraucherdienstleistungen, Medien/Unterhaltung.



Die wichtigsten Erkenntnisse

- Befragung unter 2.500 Unternehmen mit zwischen 250 und über 10.000 Mitarbeitern
- In 9 Ländern
- In 10 Branchen
- 1.922 IT-Entscheider / 578 IT-Sicherheitsentscheider

11.4 Mio. EUR

USD an durchschnittlich geschätzten Kosten pro Vorfall, der durch Insider verursacht wurde × 6 Vorfälle/Monat = 818.0 Mio. EUR an jährlichem Risiko

Nur **28 %** kombinieren regelmäßige Schulungen für das Sicherheitsbewusstsein (53 %) mit einer kontinuierlichen Überwachung (52 %)

69 % sind der Meinung, dass KI in den nächsten 12 Monaten bei Angriffen gegen ihr Unternehmen eingesetzt wird

71 % erwarten negative Geschäftsauswirkungen durch Angriffe auf Collaboration-Tools im Jahr 2026

65 % finden die Integration von Cybersicherheitstools und -lösungen kompliziert

59 % fehlt die Zuversicht, dass sie Daten für regulatorische/ gesetzliche Anforderungen schnell auffinden können

91 % erleben Governance- und Compliance-Herausforderungen

EINE STARKE AUSWEITUNG DER ANGRIFFSFLÄCHE

Vom exklusiven E-Mail-Risiko zum Omni-Channel-Risiko
Den traditionellen Sicherheitsperimeter gibt es nicht mehr. Heute sind Unternehmen Bedrohungen über E-Mail, Slack, Microsoft Teams, Zoom und Dutzende anderer Plattformen für die Zusammenarbeit ausgesetzt. Jede davon ist ein potenzielles Einfallstor für raffinierte Bedrohungsakteure, und die nativen Sicherheitskontrollmechanismen dieser Plattformen erweisen sich gegen solche Angriffe als unzureichend. In diesem Kontext sollten sich Sicherheitsteams nicht auf seltene Zero-Day-Schwachstellen fokussieren, sondern auf die Abwehr von Angreifern, die systematisch und in erheblichem Umfang das menschliche Vertrauen ausnutzen.

Was ursprünglich vor allem eine Herausforderung der E-Mail-Sicherheit darstellte, hat sich mittlerweile zu einer komplexen, alle Kanäle umfassenden Bedrohungslandschaft entwickelt. 96 % der Unternehmen rechnen für das Jahr 2026 mit Herausforderungen im Bereich der E-Mail-Sicherheit. Und bemerkenswerte 71 % erwarten nun auch konkrete negative Auswirkungen für ihr Geschäft durch gezielte Angriffe auf Collaboration-Tools. Die Angriffsfläche wächst also, und es gibt keinerlei Anzeichen einer Verlangsamung.

Zunehmende Multi-Channel-Bedrohungen

Wir beobachten in allen Kanälen eine Zunahme der Bedrohungen. Dabei bleibt der E-Mail-Verkehr ein primäres Angriffsziel. 53 % melden ein erhöhtes Phishing-Volumen mit schädlichen Links oder Anhängen. 48 % haben einen Anstieg der Business-Email-Compromise-Angriffe (BEC-Angriffe) festgestellt. Tools für die Zusammenarbeit stehen ebenfalls unter Beschuss. 45 % der Unternehmen verzeichnen nun auch dort eine Zunahme der Cyberangriffe. Gleichzeitig nehmen die internen Risiken zu. 42 % unserer Befragten berichten von vermehrten Datenlecks durch kompromittierte Mitarbeiter. Ebenfalls 42 % erleben mehr Datenlecks durch böswillige Insider.

Eine Sicherheitslücke durch native Sicherheitstools

Wir sehen eine gefährliche Diskrepanz zwischen den Gefahren, derer Unternehmen sich bewusst sind, und ihrer Reaktion darauf. 38 % verlassen sich ausschließlich auf die nativen Sicherheitsmaßnahmen ihrer Collaboration-Tools. Doch 71 % erwarten, dass Angriffe auf diese Tools im Jahr 2026 negative Auswirkungen auf ihr Geschäft haben werden. 2025 waren 67 % der Meinung, dass die nativen Sicherheitsvorkehrungen von Tools für die Zusammenarbeit unzureichend seien – eine Vorhersage, die sich als zutreffend erwiesen hat.

Diese nativen Sicherheitsvorkehrungen sind nicht darauf ausgelegt, ausgeklügelte Angriffe abzuwehren, bei denen psychologische Taktiken angewandt und das Vertrauen der Mitarbeiter ausgenutzt werden. Es fehlen ihnen die dafür erforderlichen kontextabhängigen Erkennungsfunktionen, die feststellen können, ob es sich bei legitim aussehenden Mitteilungen in Wirklichkeit um sorgfältig ausgearbeitete Social-Engineering-Versuche handelt. Wenn sich Unternehmen ausschließlich auf diese nativen Kontrollinstrumente verlassen, stellt jede Collaboration-Plattform einen ungeschützten Angriffsvektor dar.

Reale geschäftliche Konsequenzen

Wenn bei einem Sicherheitsvorfall die Abwehr eines Unternehmens erfolgreich durchbrochen wird, sind die finanziellen Folgen verheerend. Bei den meisten Unternehmen (71 %) kommt es monatlich zu ein bis zehn durch Insider verursachten Datenlecks. Datenschutzverletzungen sind somit keine Ausnahme mehr, sondern Routine.

Diese Erkenntnis wird durch Berichte über Sicherheitslücken bestätigt. Der Cyberangriff auf Change Healthcare im Jahr 2024 zeigt beispielsweise, wie menschliches Versagen katastrophale Konsequenzen haben kann. Bei diesem Angriff wurden die Anmeldedaten eines Mitarbeiters durch eine Phishing-E-Mail kompromittiert. Angreifer hatten dadurch Netzwerkzugriff auf Systeme, die keine Multifaktor-Authentifizierung erforderten. United Healthcare schätzt die Gesamtkosten für die Reaktion auf diesen Vorfall auf 1.99 bis 2.12 Mrd. EUR.

Die Größenordnung moderner Bedrohungen

Die Bedrohungserkennung von Mimecast identifizierte in den ersten neun Monaten des Jahres 2025 9,13 Milliarden individuelle Bedrohungen. Dies verdeutlicht sehr gut die schiere Menge an Angriffen, mit denen Unternehmen täglich konfrontiert sind.

Angreifer haben ausgeklügelte Taktiken entwickelt, um die Vertrauensbasis der Geschäftskommunikation ausnutzen. Sie generieren automatisierte Konversationsketten für BEC-Angriffe, mit denen über einen längeren Zeitraum ein glaubwürdiger Austausch simuliert wird. Dabei werden absichtlich die Kommunikationskanäle gewechselt. Opfer werden zunächst per E-Mail, dann per Telefon und schließlich über Microsoft Teams angesprochen. Dadurch gelingt es Angreifern, Sicherheitskontrollmaßnahmen zu umgehen, die nicht plattformübergreifend greifen. Darüber hinaus nutzen Cyberkriminelle vertrauenswürdige Unternehmensdienste wie DocuSign und SharePoint als Angriffsvektoren. Sie wissen, dass die systemeigenen Sicherheitskontrollmaßnahmen ihrer Opfer so konfiguriert sind, dass diesen weit verbreiteten Plattformen automatisch vertraut wird.

Unternehmen können es sich nicht länger leisten, die Sicherheit von E-Mail- und Collaboration-Plattformen als separate Anliegen zu behandeln. Noch können sie sich weiterhin auf native Kontrollmaßnahmen verlassen, die nie darauf ausgelegt waren, menschenorientierte Angriffe in großem Umfang zu stoppen.

Externe Bedrohungen machen sich zunutze, dass 8 % der Mitarbeiter für 80 % der Sicherheitsvorfälle verantwortlich sind.1 Können Sie Ihre 8 % identifizieren, bevor Angreifer es tun?

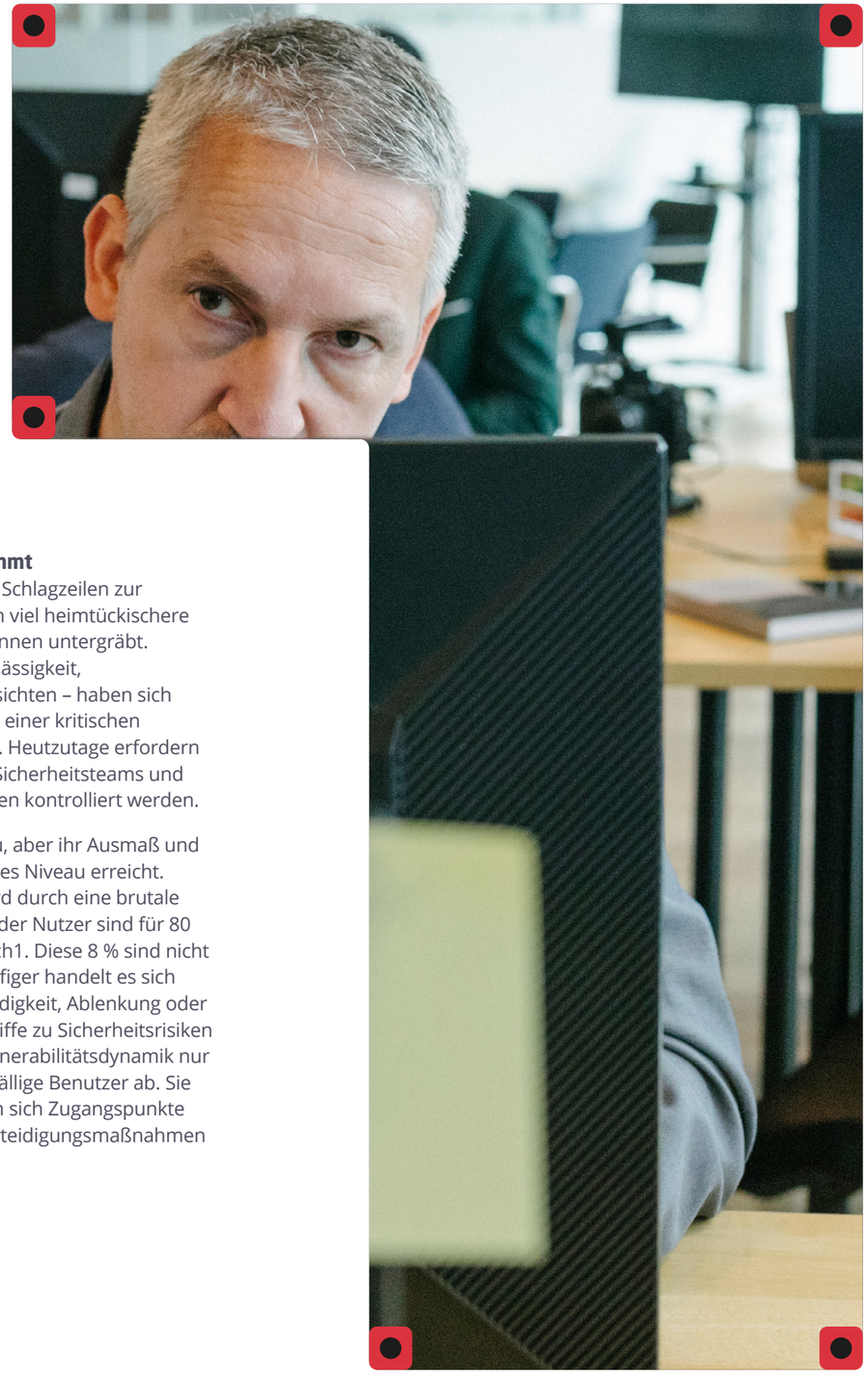
KI kann äußerst realistische E-Mails, Nachrichten und Stimm-Deepfakes erstellen, die für Benutzer schwerer zu erkennen sind.

Techniken wie ClickFix zeigen, wie Angreifer Benutzer dazu bringen, schädliche Befehle direkt auszuführen und dabei technische Kontrollen vollständig zu umgehen.

„Mitarbeiter klicken trotz Schulungen häufig auf bösartige Links, was das Risiko von unternehmensweitem Phishing und der Kompromittierung von Zugangsdaten erhöht."
(Südafrika, Gesundheitswesen)

[1] Diese 8 %/80 %-Statistik stammt aus dem Mimecast-Whitepaper "The Size and Shape of Workforce Risk".

– „Das menschliche Risiko ist eines unserer komplexesten Probleme. Es beruht auf Social Engineering, und dagegen kommt man nur schwer an. Wir führen daher aktive Schulungen durch und nutzen Tools, die menschliches Handeln blockieren, kontrollieren und überwachen. Unter anderem nutzen wir hierfür KI-Tools zur Mustererkennung."
(Spanien, Finanzdienstleistungen)



INSIDERRISIKEN

Wenn die Bedrohung von innen kommt
Externe Bedrohungen dominieren die Schlagzeilen zur Cybersicherheit, aber es gibt eine noch viel heimtückischere Gefahr, die Sicherheitsstrategien von innen untergräbt. Insiderrisiken – verursacht durch Fahrlässigkeit, Kompromittierung oder böswillige Absichten – haben sich von einer bekannten Schwachstelle zu einer kritischen Geschäftsbedrohung weiterentwickelt. Heutzutage erfordern sie die sofortige Aufmerksamkeit der Sicherheitsteams und müssen durch strategische Maßnahmen kontrolliert werden.

Die Herausforderung ist also nicht neu, aber ihr Ausmaß und ihre Komplexität haben ein beispielloses Niveau erreicht. Die heutige Bedrohungslandschaft wird durch eine brutale mathematische Realität definiert: 8 % der Nutzer sind für 80 % der Sicherheitsvorfälle verantwortlich1. Diese 8 % sind nicht unbedingt böswillige Akteure. Viel häufiger handelt es sich um ehrliche Mitarbeiter, die durch Müdigkeit, Ablenkung oder ausgeklügelte Social-Engineering-Angriffe zu Sicherheitsrisiken werden. Angreifer verstehen diese Vulnerabilitätsdynamik nur allzu gut und zielen absichtlich auf anfällige Benutzer ab. Sie setzen auf menschliches Versagen, um sich Zugangspunkte zu verschaffen, die technologische Verteidigungsmaßnahmen allein nicht blockieren können.

Drei unterschiedliche Benutzerrisikoprofile

Sicherheitsteams müssen drei grundlegend verschiedene Benutzerrisikokategorien erkennen und ansprechen. Jede davon erfordert eine maßgeschneiderte Präventionsstrategie:

Der Unaufmerksame: Die unbeabsichtigte Bedrohung
Diese Mitarbeiter stellen nicht durch böswillige Absichten, sondern durch unachtsames Verhalten ein Risiko dar. Unternehmen nutzen verschiedene Ansätze, um dieser Herausforderung zu begegnen. Mehr als die Hälfte führt regelmäßige Sicherheitsschulungen und Aufklärungskampagnen durch (53 %) oder fahndet kontinuierlich nach Richtlinienverstößen bzw. schlechten Datenverarbeitungspraktiken (52 %). Fast die Hälfte (48 %) setzt auf rollenbasierte Zugriffskontrollmaßnahmen und Zugriffsberechtigungen. Lediglich 37 % geben Mitarbeitern kontextbezogene Hinweise oder „Anstöße", um riskante Aktionen in Echtzeit zu verhindern.

Der Missbrauchte: Das Risiko einer Kompromittierung
Sogar sicherheitsbewusste Mitarbeiter können zur Gefahr werden, wenn Angreifer sie gezielt ins Visier nehmen. Um zu verhindern, dass anvisierte Nutzer kompromittiert werden, sieht fast die Hälfte der Unternehmen eine automatisierte Blockierung oder Isolierung von mutmaßlich kompromittierten Konten vor (47 %). 46 % setzen eine KI-gestützte Erkennung gezielter oder ungewöhnlicher Nutzeraktivitäten ein. Darüber hinaus nutzen 46 % Echtzeit-Warnmeldungen und Handlungsanweisungen für Benutzer mit hohem Risiko.

Der Böswillige: Die absichtliche Bedrohung
Manche Nutzer missbrauchen ihre Zugangsberechtigungen bewusst, um sich persönlich zu bereichern, Rache zu nehmen oder äußeren Zwang auszuüben. Diese Art der Bedrohung nimmt im gleichen Maße zu wie die unbeabsichtigten Risiken. Im vergangenen Jahr erlebten 42 % der Unternehmen eine Zunahme der Bedrohungen durch böswillige Insider. Ebenso viele verzeichneten einen Anstieg der Vorfälle durch fahrlässiges Handeln. Diese Tatsache offenbart eine wichtige Realität: Unternehmen können das Insiderrisiko nicht durch Schulungen beseitigen. Sie benötigen technische Kontrollmaßnahmen, die sowohl unachtsame Fehler als auch eine kalkulierte Ausnutzung erkennen und verhindern.

Die kritische Koordinationslücke

Die besorgniserregendste Erkenntnis unserer Umfrage betrifft nicht die Sicherheitslösungen der Unternehmen, sondern deren Umsetzung. Obwohl Sicherheitsteams umfangreiche Kontrollmaßnahmen für Mensch und Technologien durchführen, kombinieren nur 28 % von ihnen Schulungen zum Sicherheitsbewusstsein (53 %) mit einer kontinuierlichen Überwachung (52 %). Das bedeutet, dass viele Unternehmen womöglich mit fragmentierten Verteidigungsansätzen arbeiten, bei denen Präventivmaßnahmen isoliert und nicht als ein einheitliches System funktionieren.

Die Folgen dieses Ansatzes sind gravierend: Nutzerrisikoprofile werden nicht verwendet, um individuelle Kontrollmaßnahmen umzusetzen;

– „Wir versuchen unsere Mitarbeiter aufzuklären und sie mit dem Thema Risiko vertraut zu machen. Diese Art der Aufklärung ist in der heutigen Zeit sehr wichtig geworden."
(Deutschland, Finanzdienstleistungen)

[1]Diese 8 %/80 %-Statistik stammt aus dem Mimecast-Whitepaper "The Size and Shape of Workforce Risk".

Verhaltensanalysen lösen keine automatischen Systemblockaden aus; und Systemwarnungen führen nicht zu gezielten Schulungsmaßnahmen. Jede Sicherheitsebene arbeitet im Wesentlichen unabhängig von den anderen. Dadurch entstehen ausnutzbare Schwachstellen, die zunehmend von raffinierten Angreifern ausgenutzt werden.

Wie ein Sicherheitsverantwortlicher aus dem italienischen Finanzdienstleistungssektor demonstrierte, ist eine gute Systemkoordination durchaus möglich: „Jeder Mitarbeiter ist wie ein Sensor: Verdächtige Klicks lösen sofortige Mikroschulungen aus, und nach zwei Fehlern in einem Quartal werden die Kontoprivilegien der Person gesperrt, bis ein Videointerview mit dem CISO stattgefunden hat.“ Dieser Ansatz zeigt, wie effektiv die 28 % unserer Befragten, die über gut koordinierte Sicherheitsmaßnahmen verfügen, sich schützen können: Ihre Verhaltensanalysen führen zu sofortigen Konsequenzen; die Erkennung eines verdächtigen Musters löst eine Zugriffskontrollmaßnahme aus; und vor der Wiederherstellung der Zugriffsrechte erfolgt eine Prüfung durch einen Menschen. Ohne eine sinnvolle Koordination besteht selbst in Unternehmen mit gutem Ressourcenaufgebot das Risiko, dass Kontrollmaßnahmen isoliert voneinander umgesetzt werden. Die Sicherheitsmaßnahmen existieren dann zwar, sind aber nicht effektiv miteinander verbunden.

“Menschliches Versagen ist eines der Hauptrisiken. Unsere Benutzer müssen entsprechend geschult werden und sich der Risiken voll bewusst sein.“

(Frankreich, IT/Technologie/ Telekommunikation)

Die Beschleunigung der aktiven Überwachung

Unternehmen überwachen zunehmend ihre internen Aktivitäten, um Insiderbedrohungen vorherzusehen, noch bevor diese sich konkretisieren. 59 % unserer Befragungsteilnehmer verwenden integrierte Verhaltensanalysen (im Vergleich zu 50 % im Jahr 2025). 56 % führen Stimmungsanalysen durch. Und 48 % nehmen manuelle Prüfungen von Mitteilungen vor, die als verdächtig markiert wurden.

Diese Mischung aus manuellen und automatisierten Ansätzen lässt darauf schließen, dass viele Unternehmen noch immer aktiv an der Entwicklung ihrer Sicherheitsprogramme für Insiderbedrohungen arbeiten.

Der Weg nach vorn

Insiderrisiken sind heute kein periodisches Problem mehr. Sie sind zu einer permanenten operativen Realität geworden, die eine koordinierte, auf Erkenntnissen basierende Reaktion erfordert. Mit Blick auf die Zukunft äußern 66 % unserer Umfrageteilnehmer die Sorge, dass Datenverluste durch Insider in den nächsten 12 Monaten in ihren Unternehmen zunehmen werden. Ebenso viele befürchten, dass Mitarbeiter Schwierigkeiten bei der sicheren Handhabung von Daten haben werden, während sie versuchen, regulatorische Anforderungen einzuhalten.

Wenn Unternehmen unter diesen Umständen trotzdem erfolgreich sind, heißt das nicht unbedingt, dass sie mehr Tools einsetzen oder mehr Schulungen durchführen als andere. Sie verschaffen sich einen Vorteil, indem sie menschenorientierte Initiativen mit technologischen Kontrollmaßnahmen verknüpfen. So sorgen sie dafür, dass Verhaltensanalysen Zugriffsentscheidungen beeinflussen und dass Sicherheitsvorfälle automatisch zu einem menschlichen Eingreifen führen.

DAS INTEGRATIONSPARADOXON WENN DER ÜBERFLUSS AN TOOLS ZUM PROBLEM WIRD

Die Asymmetrie zwischen Angreifer und Angriffsziel

Die Sicherheitsteams von Unternehmen haben Schwierigkeiten damit, ihre Systeme miteinander zu verknüpfen. Angreifer haben diese Probleme nicht: Moderne Angriffsketten kombinieren nahtlos CAPTCHA-geschützte Phishing-Seiten, in SVG eingebettetes JavaScript und legitime Fernverwaltungstools in koordinierten Angriffssequenzen, die Lücken zwischen isolierten Sicherheitskontrollmaßnahmen ausnutzen.

Wenn es Unternehmen gelingt, ihre Tools miteinander zu integrieren, profitieren sie eher von einer schnelleren Bedrohungsneutralisierung (40 %), umfassender Transparenz (40 %) und vereinfachten Sicherheitsabläufen (37 %). Doch die meisten sind nicht in der Lage, ihre fragmentierten Sicherheitssysteme sinnvoll miteinander zu verbinden.

Die Koordinationskrise

Fragmentiert sind allerdings nicht nur die Tools der Unternehmen, sondern auch ihre Sicherheitsstrategien. Nur 28 % unserer Umfrageteilnehmer kombinieren regelmäßige Schulungen zum Sicherheitsbewusstsein mit kontinuierlichen Überwachungsmaßnahmen. Die Konsequenzen: Verhaltensanalysen werden nicht für die Anwendung von Kontrollmaßnahmen hinzugezogen, Erkennungsmechanismen lösen keine gezielten Benutzerinterventionen aus und Sicherheitsmaßnahmen werden in Silos ausgeführt statt als einheitliche Strategie. Genau diese Schwächen nutzen Angreifer aus.

Den Kreislauf durchbrechen

Unternehmen stoßen auf ein Paradox: Sie benötigen integrierte Sicherheitsmaßnahmen, um die Komplexität der Bedrohungslandschaft zu bewältigen, doch die eigentliche Integration erweist sich für viele als zu komplex. Kompetenzlücken, veraltete Strukturen, Anbietereinschränkungen und organisatorische Silos schaffen Barrieren, die die meisten Teams nicht alleine überwinden können.

Unternehmen mit gut integrierten Sicherheitsmaßnahmen haben enorme Vorteile. Wer allerdings an der Integration scheitert, bleibt im eigenen Tool-Chaos gefangen und fokussiert sich auf seine Dashboards, während Angreifer die Lücken zwischen isolierten Verteidigungsmechanismen ausnutzen. In Zukunft benötigen Unternehmen Plattformen, die von vornherein die Integration ihrer Sicherheitsmaßnahmen unterstützen, statt einzelner Punktlösungen, die eine spätere Integration versprechen.

65% **unserer Befragten empfinden die Integration von Cybersicherheitstools als kompliziert. Doch diejenigen, die es schaffen, profitieren von fünf Hauptvorteilen:**

- **Eine bessere Kommunikation von Bedrohungsinformationen für eine stärkere Sicherheitslage**
- **Eine umfassendere Sicht auf die Sicherheitsumgebung**
- **Eine schnellere Neutralisierung von Bedrohungen**
- **Eine verbesserte Compliance und Audit-Bereitschaft**
- **Bessere Funktionen zur Untersuchung sicherheitsrelevanter Ereignisse**

DIE GOVERNANCE-KRISE

Mangelnde Zuversicht in Compliance-Prozesse
Es gibt immer mehr Sicherheitsvorschriften und immer mehr Daten. Sicherheitsteams sind dadurch zu einer Art digitaler Archäologen geworden, die eilig versuchen, Daten zu finden, bevor gesetzliche Fristen ablaufen oder Geldstrafen verhängt werden. Trotz massiver Investitionen in SIEM-Plattformen, DLP-Lösungen und verwaltete Sicherheitsdienste fehlt 59 % der Unternehmen die Zuversicht, dass sie Kommunikationsdaten schnell finden und abrufen können, wenn Aufsichtsbehörden dies von ihnen verlangen. Wenn 91 % der Unternehmen Governance-Probleme erleben, ist das kein isoliertes Scheitern, sondern ein systemisches Versagen.

Der Risikofaktor „Mensch“

Neben Standortherausforderungen müssen sich Unternehmen mit menschlichen Risikofaktoren und einer Reihe neuer Risiken auseinandersetzen. Ganze 66 % äußern die Besorgnis, dass ihre Mitarbeiter beim Versuch eines regelkonformen Vorgehens einen nachlässigen Datenumgang zeigen. Die zunehmende Nutzung von Tools mit generativer KI hat zudem neue Ängste hervorgerufen. 80 % der Befragten befürchten nun, dass über diese Plattformen sensible Daten durchsickern könnten.

Die möglichen Auswirkungen wären keine bloßen Unannehmlichkeiten. Im Rahmen von behördlichen Untersuchungen, der Datensicherung bei Rechtsstreitigkeiten und Audit-Anfragen müssen Unternehmen einen schnellen Datenabruf gewährleisten können. Sind sie dazu nicht in der Lage, drohen finanzielle Strafen, rechtliche Haftbarkeit und Rufschädigung. In einem Umfeld, in dem Angreifer nach einer erfolgreichen Kompromittierung unkontrollierte Collaboration-Kanäle, Schatten-IT-Repositorys und falsch konfigurierte Cloud-Speicher zur Datenexfiltration ausnutzen können, führen Governance-Mängel zu ernsthaften Sicherheitslücken.

Der Fortbestand manueller Prozesse

Obwohl es heutzutage ausgeklügelte Automatisierungstechnologien gibt, verlassen sich viele Unternehmen weiterhin auf manuelle Prozesse, die nicht skalierbar sind.

Im Bereich der Compliance und Datenspeicherung zeigt unsere Umfrage: Nur 37 % der Befragten verfügen über automatisierte, kanalübergreifende Compliance-Tools; 23 % verwalten ihre Richtlinien manuell über IT- oder Compliance-Teams; 21 % verlassen sich auf die nativen Sicherheitsfunktionen ihrer Kommunikationsplattformen; und 18 % setzen ausschließlich für den E-Mail-Verkehr automatisierte Compliance-Tools ein.

Wie ein Sicherheitsexperte im spanischen Gesundheitsweisen bemerkte: „Sicherheitsrichtlinien sollten nicht statisch sein. Sie sollten regelmäßig überprüft und aktualisiert werden. Dabei sollten sowohl die jeweils aktuelle Bedrohungslandschaft wie auch Gesetze und Vorschriften berücksichtigt werden.“ Mit manuellen Prozessen ist eine solche kontinuierliche Anpassung nahezu unmöglich.

59 % haben kein Vertrauen in ihre Datenabfrage + 36 % verlassen sich auf eine manuelle Überwachung = Compliance-Krise

„Wir nutzen KI„ um die schlimmsten Konsequenzen menschlicher Risiken zu minimieren. Allerdings versuchen wir immer noch herauszufinden, ob wir ohne KI besser dran wären und lieber manuell weitermachen sollten.“

(UK, Einzelhandel/Vertrieb/Transport – Veranschaulichung der Unsicherheit bei der Umsetzung von Automatisierungsmaßnahmen)

Konvergierende Compliance-Herausforderungen

Unternehmen erleben mehrere Herausforderungen gleichzeitig. Insgesamt 80 % der Befragten äußern Bedenken hinsichtlich Datenlecks durch GenAI-Tools. 91 % haben Probleme dabei, die konsequente Einhaltung von Compliance-Standards durch ihre Mitarbeiter zu gewährleisten.

Parallel dazu gelingt es Unternehmen nur begrenzt, ihre Governance-Ziele durch die Integration ihrer Technologien umzusetzen. Lediglich 40 % der Befragten berichten von einer verbesserten Compliance und Audit-Bereitschaft infolge der Integration ihrer Sicherheitstools. Die verbleibenden 60 % haben ihre integrationsbasierten Compliance-Ziele noch nicht vollständig erreicht.

Ein eskalierendes Problem

Wenn Governance-Systeme unter dem großen Bedrohungsvolumen und einer hohen Datenwachstumsrate zusammenbrechen, werden KI-gestützte Angriffe alles zerstören, was noch übrig ist. Dieses Problem lässt sich nicht durch die Implementierung zusätzlicher Tools bewältigen, sondern erfordert einen grundlegend neuen Ansatz zur Daten-Governance. Unternehmen sollten sich auf die Automatisierung, die Zentralisierung sowie auf einheitliche, skalierbare Richtlinienrahmen fokussieren. Ohne ein solches Umdenken wird die aktuelle Governance-Krise von einem Compliance-Problem zu einem existenziellen Geschäftsrisiko eskalieren.

Die vier Säulen einer ineffektiven Governance

Eine ineffektive Governance resultiert aus der Kombination mehrerer Mängel:

1. Eine unzureichende Automatisierung:
Die Hälfte aller Unternehmen ist auf manuelle Compliance-Prozesse angewiesen, die nicht skalierbar sind. Dies führt zu einer uneinheitlichen Anwendung von Richtlinien, verzögerten Reaktionen auf Verstöße und einer starken Abhängigkeit vom menschlichen Urteilsvermögen.

2.Uneinheitliche Aufbewahrungsrichtlinien:
Richtlinien für ihre E-Mail-Tools und ihre Cloud-Speicher, und es gibt keinen einheitlichen Plan für die Datenaufbewahrung. Das führt dazu, dass Daten entweder zu lange aufbewahrt werden (wodurch das Risiko von Datenlecks steigt) oder zu früh gelöscht werden (was zu Verstößen gegen die Vorschriften führt). Die Schatten-IT verschärft dieses Problem. Sie schafft unkontrollierte Repositorys, in denen die offiziellen Richtlinien nicht greifen.

3. Schwierigkeiten bei Audits und Untersuchungen:
In vielen Unternehmen liegen Daten über mehrere Plattformen hinweg verstreut und es gibt keine zentrale Suchfunktion. Lückenhafte Metadaten und eine unvollständige Indexierung zwingen Teams dazu, Kommunikationsverläufe manuell zu rekonstruieren.

4. Eine fragmentierte Verantwortung:
Viele Unternehmen legen die Verantwortlichkeit für die Governance ihrer Kommunikation nicht in die Hände einer einzelnen Person. Die Zuständigkeiten verteilen sich auf IT-, Rechts-, Compliance- und Sicherheitsteams.

KI ALS ZWEISCHNEIDIGES SCHWERT

Eine übereilte Implementierung schwächt die Verteidigung

Für Unternehmen ist KI paradoxerweise sowohl ihr vielversprechendstes Verteidigungsmittel als auch ihre größte Bedrohung. Während Milliarden in KI-gestützte Sicherheitstools fließen, klafft weiterhin eine gefährliche Lücke zwischen dem Akquisitionszeitpunkt und der vollen Einsatzbereitschaft der neuen Lösungen.

Unsere Daten zeigen den Umfang dieser Lücke: 82 % der Sicherheitsverantwortlichen äußern Besorgnis darüber, dass ihre KI-Lösungen als Angriffsvektor missbraucht werden könnten, und ein ähnlich großer Anteil (71 %) hat Bedenken, dass seine Mitarbeiter Opfer von KI-gestützten Social-Engineering-Angriffen werden. Datenlecks in Tools mit generativer KI verstärken diese Ängste: 80 % unserer Teilnehmer fürchten die Offenlegung sensibler Informationen. Besonders auffallend ist, dass 69 % es sogar für unvermeidlich halten, dass KI in den nächsten 12 Monaten bei einem Angriff auf ihr Unternehmen eingesetzt wird.

Allerdings geben nur 40 % an, durch spezifische Strategien vollständig auf KI-gestützte Bedrohungen vorbereitet zu sein. Diese 29-Prozent-Lücke zwischen Bewusstsein und Bereitschaft stellt eine kritische Schwachstelle dar, die raffinierte Angreifer heute bereits ausnutzen.

Eine fragmentierte Verteidigung

Die Einführung von KI-gestützten Abwehrtools nimmt zu, ist aber nach wie vor nicht in allen Unternehmen vorgesehen. Etwas mehr als die Hälfte der befragten Unternehmen (55 %) nutzt mittlerweile KI zur Bedrohungserkennung und Echtzeitüberwachung – im Vergleich zu 46 % im Vorjahr. Genau die Hälfte unserer Befragten setzt KI für die Phishing-Analyse und -Reaktion, den Schutz ihrer Endpunkte und die automatisierte Reaktion auf Sicherheitsvorfälle ein. Die Verwendung KI-gestützter Verhaltensanalysen und Vorkehrungen zur Erkennung von Insiderbedrohungen ist auf 49 % angestiegen – gegenüber 43 % im Vorjahr.

Im Umkehrschluss sind unsere Umfrageergebnisse ebenso aussagekräftig: Fast die Hälfte unserer Teilnehmer setzen noch keine KI-Tools zur grundlegenden Bedrohungserkennung ein, die Hälfte hat keine KI-gestützten Phishing-Abwehrsysteme und 51 % verwenden keine KI-gestützten Verhaltensmusteranalysen oder Vorkehrungen zur Erkennung von Insiderbedrohungen. Daraus ergeben sich zwei unterschiedliche Kohorten – diejenigen, die mit einer umfassenden KI-Abwehr vorpreschen, und diejenigen, die noch zögern, während die Bedrohungen um sie herum zunehmen.

Das Ungleichgewicht zwischen Tools und Schulungen

Die Investitionsmuster unserer Befragten offenbaren eine gravierende Fehlausrichtung. Fast die Hälfte der Unternehmen (48 %) implementiert KI-gestützte Überwachungs- und Schutztools (die Kategorie mit den höchsten Investitionen). Weniger investiert wird hingegen in Mitarbeiterschulungen zur Erkennung von KI-Angriffen (44 %), die Erstellung spezifischer KI-Nutzungsrichtlinien (41 %) und die Durchführung simulierter KI-gestützter Phishing-Angriffe (40 %). Unternehmen priorisieren demnach die Akquisition neuer Technologien gegenüber der Kompetenzentwicklung und Governance-Rahmenwerken. Dieses Ungleichgewicht schafft strategische blinde Flecken. Zwar werden heute intelligentere Systeme eingesetzt, doch das Personal bleibt anfällig für KI-gestütztes Social Engineering.

69 % sagen, KI-Angriffe seien unvermeidlich, doch nur 40 % sind vollständig darauf vorbereitet. Es gibt demnach eine Diskrepanz von 29 % zwischen Bewusstsein und Bereitschaft.

“Unkontrollierte KI stellt ein sehr hohes Sicherheitsrisiko dar.”
(Spanien, Energie/Öl/Gas/Versorgung)

“Wir setzen KI kontinuierlich zur Überwachung menschlicher Risiken ein.”
(US, IT/Technologie/Telekommunikation)

“Wir nutzen überhaupt keine KI.”
(UK, öffentlicher Sektor)

“Angreifer erhöhen das Risiko unbeabsichtigter Datenlecks, indem sie mithilfe von KI hochgradig personalisierte E-Mails erstellen, die Mitarbeiter leichter täuschen.”
(Frankreich, Finanzdienstleistungen)

Drei Faktoren lassen Unternehmen zögern

Obwohl unsere Umfrageteilnehmer die Unvermeidbarkeit von KI-Angriffen erkannt haben, verzögern viele den Einsatz von defensiver KI. Wir haben drei Hauptgründe dafür identifiziert:

1. Governance-Bedenken

Unternehmen haben Probleme mit der rasanten Entwicklung der KI. Sie sind sich unsicher, wie sie Kontrollmechanismen implementieren sollen, die dauerhaft greifen. Regulatorische Unklarheiten – insbesondere in Regionen wie der Europäischen Union, in denen die sogenannte KI-Verordnung umgesetzt wurde – schaffen Hindernisse, die den Einsatz von KI verlangsamen.

2. Sicherheitsrisiken:

Führungskräfte haben die Sorge, dass durch ihre Sicherheitssysteme neue Schwachstellen entstehen. Sie befürchten zum Beispiel einen Datenabfluss durch Tools mit generativer KI, eine Modellvergiftung oder eine externe Manipulation ihrer KI-Systeme.

3. Anforderungen an den Wertnachweis (unklarer ROI):

Unternehmen haben Schwierigkeiten, die Wirksamkeit ihrer KI zu quantifizieren. Auch das führt zu Verzögerungen bei der Implementierung.

Die aktuelle Bedrohungslandschaft

Moderne Angriffe demonstrieren heute bereits die offensiven Fähigkeiten der KI. Automatisierte BEC-Konversationsketten können wochenlang glaubwürdige Austausche aufrechterhalten. KI-generiertes sprachbasiertes Phishing kann Führungskräfte authentisch nachahmen. Und CAPTCHA-geschützte Phishing-Seiten überlisten automatisierte Analysen.

Traditionelle Indikatoren für Phishing – schlechte Grammatik, unpersönliche Begrüßungen, offensichtliche Formatierungsfehler – sucht man in KI-gestützten Inhalten vergebens. Künstliche Intelligenz senkt die Hürden für überzeugende Angriffe und ermöglicht es so auch Bedrohungsakteuren mit begrenzten technischen Fähigkeiten, in großem Umfang ausgeklügelte Kampagnen durchzuführen.

Strategische Imperative

Governance-Frameworks implementieren, werden sie bestens positioniert sein, um neue Bedrohungen zu erkennen und abzuwehren. Wenn sie hingegen auf eine perfekte Lösung warten, sind sie ausgeklügelten Angriffen ohne angemessene Verteidigung ausgesetzt.

In Zukunft müssen Unternehmen ausgewogen investieren: Sie benötigen ausgefeilte Tools und umfassende Schulungen; sie müssen sich gute technische Fähigkeiten aneignen und diese durch klare Richtlinien unterstützen; und sie brauchen eine angemessene Governance, mit der sie neue Tools nicht nur schnell, sondern auch sicher implementieren. Kurzum: Die Bedrohungslandschaft erfordert, dass sie jetzt aktiv werden.

UNTERSCHIEDE IN HUMAN RISK AUF VERSCHIEDENEN GLOBALEN MÄRKTEN

Globale Muster, lokale Nuancen

Menschliche Risiken gibt es in jedem Land, das Teil unserer Befragung war. Doch der regionale Umgang mit diesen Risiken unterscheidet sich markant je nach regulatorischem Umfeld, Bedrohungslandschaft, kulturellen Normen und Ressourcenverfügbarkeit. Dieser Schnappschuss zeigt wichtige Ergebnisse aus neun wichtigen Märkten. Eine detaillierte länderspezifische Analyse finden Sie unter **https://www.mimecast.com/de/digital/sohr/**

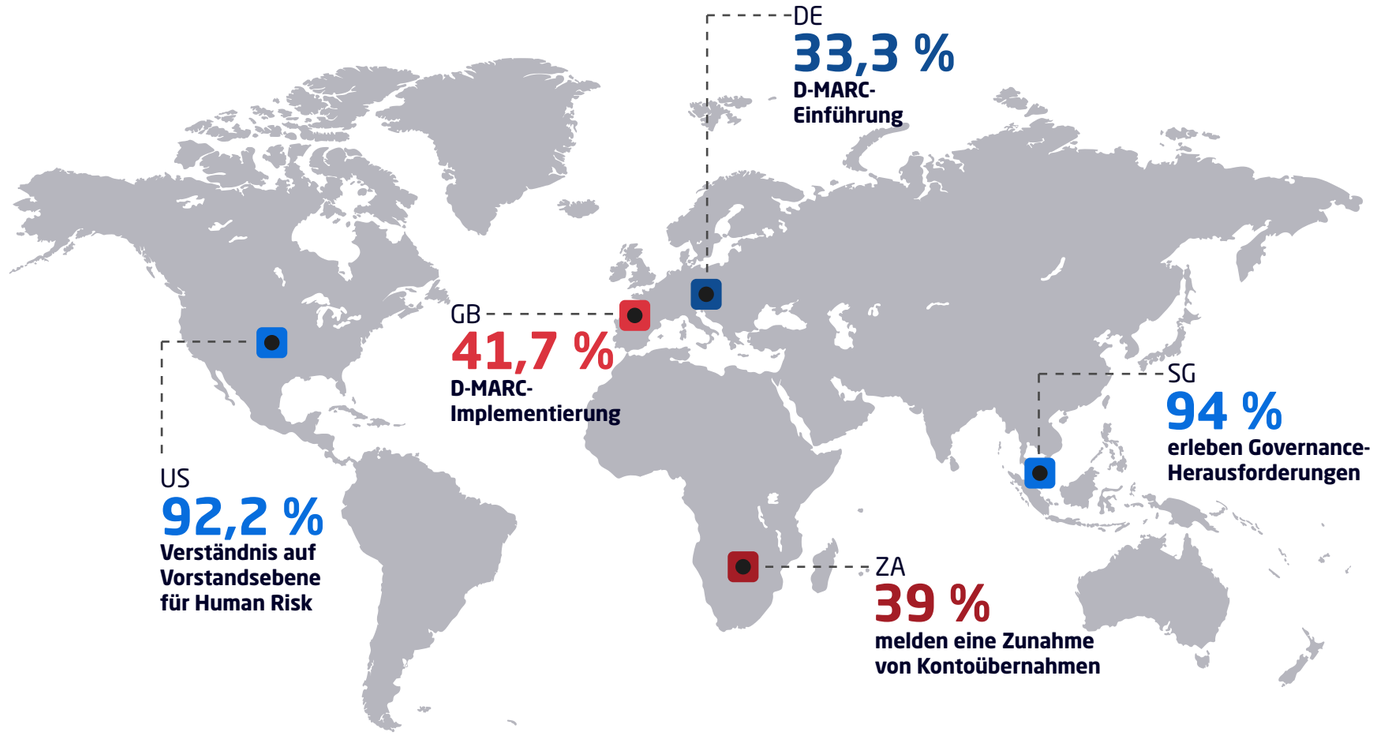
Drei Reifegrade

Bei der Umsetzung von Human-Risk-Management-Strategien gibt es drei Reifegrade:

KI-Anwender (USA, Singapur): Hohes Bewusstsein + hohe Nutzung + belegter ROI. Führend im defensiven KI-Einsatz; starke Integration zwischen Mensch und Technologie; Unterstützung auf Vorstandsebene; Bereitschaft zum Experimentieren und Iterieren.

Vorsichtige Pragmatiker (UK, Deutschland, Frankreich): Hohes Bewusstsein + maßvolle Nutzung + Fokus auf die Compliance. Datenschutz- und Governance-Überlegungen beeinflussen das Implementierungstempo; es gibt starke Sicherheitsgrundlagen; bewährte Technologien werden bevorzugt eingesetzt; Lösungen werden vor der Bereitstellung systematisch evaluiert.

Aufstrebende Exponenten (Spanien, Südafrika, Australien): Wachsendes Bewusstsein + selektive Nutzung + Fokus auf Ressourcen. Rasante Erhöhung des Reifegrads; Innovation mit Rücksicht auf die vorhandenen Einschränkungen; ROI-orientierte Entscheidungsfindung; Beachtung der Lehren aus reifen Märkten bei gleichzeitiger Anpassung an den lokalen Kontext.



Regionale Highlights

US Vereinigte Staaten: 92,2 % der Verständnis für menschliche Risiken auf Vorstandsebene (weltweit höchster Prozentsatz); 38,4 % nutzen DMARC; 85,4 % fürchten KI-Angriffe (weltweit höchster Prozentsatz); führend in der Koordination zwischen Mensch und Technologie. Herausforderung: Tool-Chaos trotz größerer Budgets. Lektion: Eine frühe KI-Nutzung erfordert keine Perfektion.

GB Vereinigtes Königreich: 41,7 % DMARC-Einsatz (höchster Wert in Europa); 83 % fürchten KI-Angriffe, doch KI wird langsamer eingeführt; starke DSGVO-orientierte Compliance-Grundlagen. Herausforderung: Lücke zwischen Bewusstsein und Handlungsbereitschaft in der Verteidigung gegen KI-Angriffe. Lektion: Datenschutz durch Technologiegestaltung schafft nachhaltige Sicherheitsprogramme.

DE Deutschland: 33,3 % DMARC-Einführung; 81 % erleben immer komplexere Angriffe; methodischer „Untersuchen-testen-bereitstellen"-Ansatz; starker Fokus auf Datensouveränität. Herausforderung: Systematisches Testen verzögert die Bereitstellung. Lektion: Strenge Tests schaffen robuste Sicherheitsprogramme.

FR Frankreich: Eine starke Finanzbranche setzt KI-Standards; hervorragendes Verständnis von KI-Bedrohungen; selektive Nutzung, mit entsprechenden Datenschutzschutzmaßnahmen. Herausforderung: Gleichgewicht zwischen Innovation und Datenschutz. Lektion: Eine gut durchdachte Einführung mit einem klaren Verständnis der Bedrohungslage funktioniert.

ES Spanien: Schnelle Reife des Sicherheitsprogramms; „Erst beweisen, dann skalieren"-Ansatz für KI; Schwerpunkt auf kontinuierlichen Richtlinien-Updates; aktives Experimentieren mit Bewusstsein für die Governance. Herausforderung: Nachweis des Nutzens im Vorfeld einer skalierten Anwendung. Lektion: Eine kontinuierliche Anpassung der Richtlinien schafft agile Programme.

ZA Südafrika: 39 % berichten von erhöhten Kontoübernahmen; große Besorgnis über Lücken in der Schulungseffektivität; Fokus auf die Maximierung des ROI unter Ressourcenbeschränkungen. Herausforderung: Fachkräftemangel auf dem wettbewerbsintensiven globalen Markt. Lektion: Eine Ressourcenknappheit führt zu innovativen Effizienzsteigerungen.

SG Singapur: Einer von nur zwei Märkten weltweit, der als „KI-Anwender" eingestuft wird; führend beim defensiven Einsatz von KI und bei der Koordinierung zwischen Mensch und Technologie; übertrifft APAC-Konkurrenten in einer Region, in der 94 % der Unternehmen Governance-Herausforderungen erleben. Herausforderung: Beibehaltung der Führungsrolle, während die Konkurrenz aufholt. Lektion: Die Zusammenarbeit zwischen Regierung und Unternehmen beschleunigt den Reifeprozess.

AU Australien: Starke Grundlagen für die E-Mail-Sicherheit; Anforderungen für kritische Infrastruktur treiben Investitionen voran; von der Regierung entwickelte Rahmenwerke (Essential Eight) bieten klare Richtlinien. Herausforderung: Der Remote-Betrieb schafft einzigartige Sicherheitsherausforderungen. Lektion: Klare regulatorische Vorgaben beschleunigen den Reifeprozess.

Universelle Herausforderungen trotz regionaler Unterschiede: In allen Regionen erleben 91–93 % der Unternehmen Governance-Herausforderungen, mehr als 65 % Integrationskomplexität, mehr als 69 % unvermeidbare KI-gestützte Angriffe – doch nur 28 % kombinieren regelmäßige Sicherheitsbewusstseinsschulungen mit einer kontinuierlichen Überwachung

Strategisches Fazit: Obwohl die konkreten Taktiken je nach Region variieren, verfolgen alle das gleiche strategische Imperativ. Der Umgang mit menschlichen Sicherheitsrisiken erfordert integrierte Plattformen zur Koordinierung von menschenorientierten Initiativen, technologieorientierten Kontrollmaßnahmen, Governance-Rahmenwerken und kontinuierlichen Anpassungen. Einzellösungen und isolierte Initiativen scheitern unabhängig von der Region. Link zur detaillierten regionalen Analysse.

WICHTIGE ERKENNTNISSE UND EMPFEHLUNGEN

Was sind Ihre nächsten Schritte?

Unsere diesjährigen Umfragedaten zeigen fünf kritische Bereiche, in denen vorausschauende Sicherheitsverantwortliche gerade messbare Fortschritte erzielen. Im Folgenden erklären wir, wie auch Sie die Erkenntnisse aus dieser Forschung mit bewährten Lösungsansätzen in organisatorische Maßnahmen umsetzen:

1. Sichere E-Mail- und Collaboration-Kanäle

Die Herausforderung: 71 % der Unternehmen erwarten negative Auswirkungen durch einen Angriff auf ihre Collaboration-Tools. 96 % rechnen mit Herausforderungen im E-Mail-Verkehr. 64 % stimmen zu, dass die meisten nativen Sicherheitstools unzureichend sind.

Maßnahmen: Setzen Sie einheitliche Schutzmaßnahmen für Ihre gesamte Angriffsfläche um. Betrachten Sie die Sicherheit Ihres E-Mail-Verkehrs und Ihrer Collaboration-Tools nicht als separate Probleme. Setzen Sie einen einheitlichen Bedrohungsschutz für E-Mail- UND Collaboration-Plattformen ein. Implementieren Sie KI-gestützte Maßnahmen für die adaptive Erkennung von Bedrohungen (55 % der Befragten nutzen diese bereits). Erweitern Sie Ihre E-Mail-Sicherheitsmaßnahmen auf Teams/Slack/Zoom. Überwachen Sie alle Kanäle auf BEC-Angriffe und Identitätsdiebstahl.

Worauf Sie achten sollten: Einheitliche Plattformen, die sowohl den E-Mail-Verkehr als auch Ihre Tools für die Zusammenarbeit schützen. KI-gestützte Erkennungsmaßnahmen, die sich in Echtzeit an neue Bedrohungen anpassen. Keine vierteljährlichen Schulungen, sondern ein Sicherheitsbewusstsein, das in risikoreichen Momenten greift. Eine integrierte, kanalübergreifende Compliance-Berichterstattung.

Erfolgskennzahlen: Reduzierung erfolgreicher Angriffe; Zeit bis zur Erkennung/Behebung in allen Kanälen; Abdeckungsprozentsatz; Benutzer-Melderaten.

2. Die Implementierung des Human Risk Management

Die Herausforderung: Nur 28 % der Unternehmen kombinieren regelmäßige Schulungen zum Sicherheitsbewusstsein mit einer kontinuierlichen Überwachung. 8 % der Mitarbeiter verursachen 80 % der Sicherheitsvorfälle1. Insidervorfälle können bei sechs monatlichen Ereignissen 111.4 Mio. EUR kosten.

Maßnahmen: Identifizieren und bewerten Sie riskante Nutzer mithilfe von Verhaltensanalysen. Erstellen Sie drei Nutzerrisikoprofile (fahrlässig, kompromittiert, böswillig). Überwachen Sie kontinuierlich alle Ihre Kommunikationsplattformen. Finden Sie das Gleichgewicht zwischen Produktivität und Risiko anhand adaptiver Richtlinien. Konzentrieren Sie

Ihre Ressourcen auf die risikoreichsten 8 % der Nutzer.

Worauf Sie achten sollten: Plattformen, die Verhaltensdaten kanalübergreifend korrelieren; Risikobewertung in Echtzeit; Integration mit einer Schulungsplattform; Automatisierung der Reaktion auf Vorfälle; Einsicht in Benutzerrisiken.

Erfolgskennzahlen: Reduzierung von Insidervorfällen; Verbesserung der Nutzer-Risikobewertungen; Reduzierung der Zeit bis zur Erkennung von Bedrohungen; Schulungswirksamkeit (Verhaltensänderung); Prävention ist kostengünstiger als Sicherheitsvorfälle.

3. Eine stärkere Compliance und Maßnahmen zur Verhinderung von Datenverlusten

Die Herausforderung: 59 % haben kein Vertrauen in die Qualität ihrer Datenabfragen; 91 % erleben Governance-Herausforderungen; 66 % sorgen sich um den Verlust von Daten durch Insider; 80 % befürchten GenAI-Datenlecks.

Maßnahmen: Setzen Sie automatisierte Compliance-Prozesse um. Schaffen Sie einheitliche Aufbewahrungsrichtlinien für alle Systeme. Implementieren Sie integrierte DLP-Lösungen (derzeit verwenden nur 47 % spezielle DLP-Lösungen). Gewährleisten Sie einen schnellen Datenabruf für Audit-Zwecke. Vermeiden Sie GenAI-Datenlecks durch eine entsprechende Überwachung und genehmigte Alternativen.

Worauf Sie achten sollten: Eine vereinheitlichte Governance für alle Plattformen; automatisierte Compliance-Workflows; Erkennung von Insiderrisiken; eine Audit-taugliche Berichterstattung; DSGVO-/CCPA-Unterstützung; SIEM/SOAR-Integration.

Erfolgskennzahlen: Verkürzung der Datenabrufzeit; Erhöhung des Automatisierungsgrades; Reduzierung von Datenlecks; Reduzierung von Audit-Feststellungen; gesteigertes Vertrauen.

4. Die Konsolidierung und Integration von Sicherheitstools

Die Herausforderung: 65 % empfinden die Integration als zu kompliziert. Das Tool-Chaos behindert eine effektive Reaktion. Nur 28 % kombinieren regelmäßige Sicherheitsbewusstseinsschulungen mit einer kontinuierlichen Überwachung.

Maßnahmen: Prüfen Sie Ihre Tools auf Redundanzen und Lücken. Priorisieren Sie Plattformen mit mehreren Fähigkeiten gegenüber Punktlösungen. Suchen Sie Anbieter mit offenen APIs für die SIEM/SOAR/IAM-Integration. Schaffen Sie eine zentrale Einsicht in Ihre Systeme. Koordinieren Sie Personal- und Technologieinitiativen (verbinden Sie Schulungen mit der Bedrohungserkennung und Risikobewertungen mit Zugriffskontrollmaßnahmen).

Worauf Sie achten sollten: Plattformen mit mehreren Fähigkeiten, bewährten API-Ökosystemen, SIEM/SOAR-Integrationen, einer zentralen Systemeinsicht und Kundenreferenzen, die eine erfolgreiche Konsolidierung belegen.

Erfolgskennzahlen: Der ROI ist eindeutig, doch die meisten Unternehmen arbeiten nach wie vor mit fragmentierten Lösungen. Dadurch können sie keine einheitliche Reaktion auf Angriffe umsetzen, die den E-Mail-Verkehr, Collaboration-Tools und Datenspeicher umfassen. Die Vorteile der Konsolidierung und Integration von Sicherheitstools sind eine Reduzierung der Anzahl an Tools, ein höherer Integrationsgrad, Zeitgewinne bei der Erkennung von Bedrohungen in der gesamten Umgebung, eine höhere Effizienz von Sicherheitsteams (Verhältnis von Warnungen zu Vorfällen) und reduzierte Gesamtbetriebskosten.

[1]Diese 8 %/80 %-Statistik stammt aus dem Mimecast-Whitepaper "The Size and Shape of Workforce Risk".

5. Eine gute Vorbereitung auf KI-gestützte Bedrohungen

Die Herausforderung: 669 % sehen KI-Angriffe als unvermeidlich an, doch nur 40 % sind vollständig darauf vorbereitet. 80 % sind besorgt über KI-Angriffsvektoren und Social Engineering. Investitionen priorisieren Überwachungs- und Schutztools (48 %) gegenüber Mitarbeiterschulungen zur Vermeidung von Schwachstellen (44 %) und der Erstellung von Richtlinien zur KI-Nutzung (41 %).

Maßnahmen: Einsatz einer KI-gestützten Erkennung (55 % nutzen diese bereits für Bedrohungen, 50 % für Phishing); Richtlinien und Governance für die KI-Nutzung (derzeit verfügen nur 41 % über solche Richtlinien); Schulung von Mitarbeitern zu KI-gestütztem Social Engineering (nur 44 % bieten Schulungen an); Entwicklung interner KI-Tools zur Abwehr von Bedrohungen (nur 46 % entwickeln solche Tools); Gleichgewicht zwischen dem KI-Einsatz und der Schulung des menschlichen Urteilsvermögens.

Worauf Sie achten sollten: KI-Tools, die KI-generierte Inhalte erkennen; Verhaltensmodelle, die KI-gestütztes Social Engineering erkennen; Governance-Rahmenwerke für die Nutzung von GenAI; Schulungen zu KI-Angriffstechniken, Erklärbarkeit und Transparenz.

Erfolgskennzahlen: Erkennung von KI-generierten Angriffen; Meldung von mutmaßlichen KI-Angriffen durch Mitarbeiter; Compliance-Quoten; Abschluss von Schulungen (mit Verhaltensänderungen); Verhinderung von Vorfällen.

Der Business Case

- Erwartete durchschnittliche Kosten von 11.4 Mio. EUR pro Insidervorfall
- Im Durchschnitt 6 Vorfälle pro Monat
- 818.0 Mio. EUR an jährlichem Kostenrisiko durch Insiderrisiken
- 71 % erwarten negative Geschäftsauswirkungen durch Angriffe auf Collaboration-Tools im Jahr 2026
- 1.99 - 2,45 Mrd. USD Kosten für die Change-Healthcare-Sicherheitslücke nach der Kompromittierung der Anmeldeinformationen eines einzigen Mitarbeiters

Die Kosten der Untätigkeit übersteigen die Investitionskosten für Human-Risk-Management-Lösungen.

FAZIT: DIE KONSEQUENZEN DES MENSCHLICHEN RISIKOS

Die Daten der 2.500 Unternehmen aus neun Ländern, die an unserer Umfrage teilgenommen haben, vermitteln eine unmissverständliche Botschaft: Menschliche Risiken sind heute die größte Herausforderung für die Cybersicherheit und erfordern sofortiges, koordiniertes Handeln.

Die Statistiken liefern klare Beweise

Dieser Bericht soll Ihnen Einblick in das menschliche Risiko geben und Sicherheitsverantwortlichen dabei helfen, die nächsten Schritte für die Weiterentwicklung ihres Sicherheitsprogramms zu planen. Unsere diesjährigen Statistiken sind ein klarer Beweis dafür, dass jetzt gehandelt werden muss.

Die Diskrepanz zwischen Bewusstsein und Handlungsbereitschaft

Das Problem bei unseren Umfrageteilnehmern ist nicht ein fehlendes Bewusstsein für ihre aktuellen Sicherheitsrisiken, sondern eine mangelnde Umsetzung der eigentlich erforderlichen Sicherheitspraktiken. Unternehmen wissen sehr wohl, welche Cyberbedrohungen es gibt, doch nur 28 % kombinieren regelmäßige Sicherheitsschulungen mit kontinuierlichen Überwachungsmaßnahmen. Genau hier, in dieser Diskrepanz zwischen Bewusstsein und Handlungsbereitschaft, liegt das Problem.

91 % unserer Befragten haben Schwierigkeiten mit der Compliance ihrer Mitarbeiter, und 96 % wissen, dass ihre Sicherheitsmaßnahmen unvollständig sind. Dennoch arbeiten fast drei Viertel der Unternehmen immer noch mit fragmentierten Verteidigungsmechanismen, bei denen menschenorientierte und technologieorientierte Kontrollmaßnahmen nicht miteinander koordiniert werden. Angreifer müssen sich also nicht darauf verlassen, dass Unternehmen Bedrohungen übersehen. Sie nutzen einfach die Tatsache aus, dass ihre Opfer Bedrohungen zwar erkennen, aber keine einheitliche Abwehr dagegen einsetzen.

Fünf miteinander verbundene Prioritäten für 2026

Die kritischen Lücken, die wir in diesem Bericht aufgezeigt haben, sind keine isolierten Probleme, die separate Lösungen erfordern. Es handelt sich um Schwachstellen, die eng miteinander verbunden sind. Sie entstehen alle aus dem grundlegenden Versäumnis, menschliche Risiken als integrierte strategische Priorität zu behandeln:

1. Sichern Sie alle Kommunikationskanäle mit einheitlichen Schutzmaßnahmen ab.
2. Reduzieren Sie das menschliche Risiko anhand von Verhaltensanalysen und nutzerzentrierten Kontrollmaßnahmen.
3. Setzen Sie eine Daten-Governance mit automatisierten Compliance-Prozessen und einem schnellen Datenabruf um.
4. Integrieren Sie Sicherheitstools ineinheitliche Plattformen.
5. Bereiten Sie sich mit defensiver KI und einer entsprechenden Governance auf unvermeidliche KI-gestützte Bedrohungen vor.

Mit der richtigen Herangehensweise können diese fünf Prioritäten sich gegenseitig verstärken: Einheitliche Schutzmaßnahmen für all Ihre Kanäle liefern Ihnen umfangreichere Daten für verhaltensbasierte Analysen; eine effektivere Bewertung menschlicher Risiken dient als solide Grundlage für Governance-Maßnahmen; integrierte Plattformen ermöglichen die betriebliche Umsetzung dieser Maßnahmen; und die KI-Bereitschaft bildet das Fundament für all diese Ebenen. Wenn Unternehmen diese fünf Prioritäten separat betrachten, werden sie genau die Fragmentierung erzielen, vor der dieser Bericht warnt.

Unternehmen müssen handeln

Behandeln Unternehmen das Human Risk Management als integrierte strategische Priorität, wird es ihnen gelingen, Sicherheitsverletzungen zu verhindern, ihren Ruf zu schützen und ein effektives Sicherheitsprogramm umzusetzen. Wenn sie hingegen weiterhin fragmentierte Ansätze nutzen, werden sie Schwierigkeiten dabei haben, ihre Kosten einzudämmen, ihre Compliance aufrechtzuerhalten und sich gegen Angreifer zu verteidigen, die Lücken zwischen isolierten Systemen ausnutzen.

2026 ist das Jahr, in dem Unternehmen von der Bewusstseins- zur Umsetzungsphase übergehen sollten. Nicht etwa, weil die Daten dies nahelegen, sondern weil sie es geradezu diktieren. Wenn Unternehmen die Lücke zwischen Bewusstsein und Umsetzung schließen, werden sie selbst die nächste Ära der Cyber Resilience definieren. Alle anderen werden zu Fallstudien für gescheiterte Unternehmen, die ihr Sicherheitsbewusstsein fälschlicherweise für eine Verteidigungsstrategie hielten. Die Frage, vor der jeder Sicherheitsverantwortliche jetzt steht, ist einfach: Handeln Sie schon vor dem nächsten Vorfall oder erst danach?

mimecast

Mimecast ist ein führendes Cybersicherheitsunternehmen, das die Art und Weise verändert, wie Unternehmen menschliche Risiken verwalten und mindern. Die KI-gestützte, API-fähige, vernetzte Human-Risk-Management-Plattform wurde speziell entwickelt, um Unternehmen vor dem gesamten Spektrum an Cyberbedrohungen zu schützen. Durch die Integration modernster Technologie mit menschenzentrierten Ansätzen verbessert unsere Plattform die Sichtbarkeit und liefert strategische Erkenntnisse, die entschlossenes Handeln ermöglichen und Unternehmen dabei unterstützen, ihre kollaborativen Umgebungen zu schützen, ihre kritischen Daten zu sichern und Mitarbeiter aktiv in die Risikominderung und Produktivitätssteigerung einzubeziehen. Mehr als 42.000 Unternehmen weltweit vertrauen auf Mimecast, um der sich ständig weiterentwickelnden Bedrohungslandschaft immer einen Schritt voraus zu bleiben. Von Insiderrisiken bis hin zu externen Bedrohungen – mit Mimecast erhalten Kunden mehr. Mehr Sichtbarkeit. Mehr Einblick. Mehr Agilität. Mehr Sicherheit.

mimecast.com