mimecast

THE STATE OF HUMAN RISK 2025

Sicherheitsverantwortliche haben sich weiterentwickelt

Im Jahr 2024 war die größte Herausforderung im Bereich der Cybersicherheit nicht mehr Technologielücken, sondern menschliche Risiken. Obwohl Unternehmen Milliarden an Euros in den Schutz ihrer Tech-Stacks stecken, können sie Sicherheitsverletzungen nicht vermeiden. Das liegt daran, dass die Abwehr von Angriffen nicht nur ein technologisches, sondern auch ein menschliches Problem ist. Tatsächlich sind heute die meisten Sicherheitsvorfälle auf Insider-Bedrohungen, Zugangsdatenmissbrauch und benutzerbedingte Fehler zurückzuführen. Angreifer hacken sich 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.

Dass heutige Bedrohungen so komplex geworden sind, ist darauf zurückzuführen, dass externe Bedrohungen und Angriffe immer besser erkannt, vereitelt und abgewehrt werden. Dieser Fokus auf den Schutz gegen externe Bedrohungsfaktoren hat allerdings zur Konsequenz, dass Unternehmen ihre internen Risiken nicht ausreichend im Blick haben.

Mitarbeiter, Verkäufer, Berater, Auftragnehmer … alle diese Menschen sind über ihre Geräte Angriffen ausgesetzt. Trotz exzellenter Abwehrmaßnahmen im gesamten Tech-Stack treten daher immer wieder Hacks auf.

Zwei Drittel der für diesen Bericht befragten Sicherheitsverantwortlichen gaben an, dass es unvermeidlich oder wahrscheinlich ist, dass ihr Unternehmen 2025 negative geschäftliche Auswirkungen durch einen Angriff erleiden wird, der über E-Mail oder Collaboration-Tools (Tools für die Zusammenarbeit) gestartet wurde. Tatsächlich war der Cyberangriff auf Change Healthcare – einer der bedeutendsten Sicherheitsverstöße des Jahres 2024 – größtenteils auf menschliches Versagen zurückzuführen. Angreifer entwendeten die Anmeldedaten eines Mitarbeiters anhand einer Phishing-E-Mail, sodass sie ohne Multi-Faktor-Authentifizierung auf das Netzwerk zugreifen konnten, um anschließend sensible Daten abzugreifen und Ransomware einzusetzen. Bei United Healthcare schätzt man die Kosten für die Reaktion auf diese Sicherheitsverletzung auf 2,3 bis 2,45 Milliarden US-Dollar.

Um Gefahren wie diese abzuwehren, benötigen Unternehmen eine Strategie für den effektiven Umgang mit menschlichen Sicherheitsrisiken (Human Risk Management, HRM). In vorliegendem Bericht erklären wir, welche menschlichen Sicherheitsrisiken es aktuell gibt, welche Auswirkungen sie für Unternehmen haben und wie Unternehmen diese Gefahren handhaben und mindern können. Diese Erkenntnisse gehen aus einer umfassenden globalen Umfrage zum aktuellen Stand der Cybersicherheit und des menschlichen Sicherheitsrisikos hervor, mit der Mimecast das Forschungsunternehmen Vanson Bourne im November und Dezember 2024 beauftragt hatte. Bei den Teilnehmern dieser Befragung handelte es sich um 1.100 IT-Sicherheitsmitarbeiter und IT-Entscheidungsträger aus den Vereinigten Staaten, dem Vereinigten Königreich, Frankreich, Deutschland, Südafrika und Australien. Diese arbeiten in einer Vielzahl von Unternehmen (mit mindestens 250 Mitarbeitern) in privaten und öffentlichen Sektoren, darunter im Gesundheitswesen, im Einzelhandel, im Finanzwesen, in der Fertigung und in Versorgungsunternehmen.

Mit dieser Umfrage wollten wir herausfinden:

Wie Unternehmen das Thema Cybersicherheit handhaben, insbesondere in Bezug auf menschliche Sicherheitsrisiken

Wie sie Collaboration-Tools nutzen und wie sich das auf ihre Cybersicherheit auswirkt

Wie sich ihre Budgets auf die Cybersicherheit und den Umgang mit menschlichen Risiken auswirken

Wie sich KI auf die Cybersicherheit auswirkt, sowohl als Bedrohung als auch als Lösung

DIE WICHTIGSTEN ERGEBNISSE DES BERICHTS „THE STATE OF HUMAN RISK 2025“

85% gaben an, dass ihr Unternehmensbudget für Cybersicherheit in den letzten 12 Monaten gestiegen ist.

57% gaben an, dass ein zusätzliches Budget für Cybersicherheitspersonal und -drittanbieterdienste erforderlich ist. **52%** gaben an, dass ein zusätzliches Budget für die Absicherung ihrer Collaboration-Tools (nicht-E-Mail-basierte Tools wie Teams oder Slack) erforderlich ist. **47%** gaben an, dass für den Schutz ihres E-Mail-Verkehrs ein noch größeres Budget benötigt wird

95% gaben an, dass ihr Unternehmen KI zur Abwehr von Cyberangriffen und/oder Insider-Bedrohungen einsetzt, aber **81%** sind besorgt darüber, dass sensible Daten über GenAI-Tools freigegeben werden könnten.

55% sind NICHT vollständig mit spezifischen Strategien auf KI-gestützte Bedrohungen vorbereitet.

94% der Befragten sind der Meinung, dass es nicht einfach ist, Mitarbeiter zur Einhaltung von Compliance-Standards und Sicherheitsprotokollen zu bewegen

Tools für die Zusammenarbeit stellen nach wie vor eine wachsende Angriffsfläche dar, wobei im Jahr 2024 **37%** der Befragten von einer Zunahme in diesem Bereich und im Jahr 2025 **44%** von einer Zunahme berichteten.

95% erwarteten auch im Jahr 2025 noch Herausforderungen im Bereich der E-Mail-Sicherheit.

61% gaben an, dass es unvermeidlich oder wahrscheinlich ist, dass ihr Unternehmen im Jahr 2025 negative geschäftliche Auswirkungen durch einen Angriff im Zusammenhang mit einem Collaboration-Tool erleiden wird.

HUMAN RISK MANAGEMENT ALS NEUER IMPERATIV

Sicherheitsverantwortliche kennen das menschliche Risiko

HRM ist ein vernetzter Cybersicherheitsansatz und er berücksichtigt, dass der Schutz eines Unternehmens ein kontinuierlicher Prozess ist. Sicherheitsverantwortliche müssen die schwierige Entscheidung treffen, auf welche Tools sie sich verlassen sollen und wie sie ihr Budget am besten einsetzen, um Risiken zu minimieren. Doch trotz der großen Auswahl an Sicherheitstools auf dem Markt berichten viele CISOs immer noch, dass es ihnen schwerfällt, sich ein klares Bild von den Risiken in ihrem Unternehmen zu machen.

Tatsächlich zeigt eine Gartner-Studie, dass über 90 % der Mitarbeiter, die zugaben, während der Arbeit unsichere Verhaltensweisen an den Tag zu legen, sich darüber bewusst waren, dass ihre Handlungen das Risikoniveau des Unternehmens erhöhen würden, dies aber trotzdem taten. Bei einem menschenzentrierten Sicherheitsdesign ist es der Mensch, der im Mittelpunkt der Kontrollmaßnahmen, des Designs und der Implementierung steht – nicht die Technologie, die Bedrohung oder der Standort. Laut Gartner werden bis 2027 50 % der CISOs menschenzentrierte Designpraktiken für ihre Cybersicherheitsprogramme anwenden, um operative Hindernisse zu minimieren und die Akzeptanz von Kontrollmaßnahmen zu maximieren.

Entsprechend hob ein CIO aus der Versicherungsbranche hervor: „Technische Sicherheitsvorkehrungen wie Firewalls und die Angriffserkennung sind unverzichtbar, aber ihre Wirksamkeit ist letztendlich auch vom menschlichen Verhalten abhängig.“ Diese Aussage unterstreicht den wachsenden Konsens darüber, dass HRM nicht nur eine unterstützende Maßnahme ist: Es ist für moderne Cybersicherheitsstrategien schlichtweg unverzichtbar.

Zusammenfassung

Die Verwendung von Collaboration-Tools ebenso wie die Petabytes an Daten, die Mitarbeiter erstellen, abrufen, ändern und verschieben, haben dazu geführt, dass die Cybersicherheit ein neues Niveau an Komplexität erreicht hat.

In diesem Bericht werden Sie mehr über die folgenden Themen erfahren:

- Unternehmen erlangen ein größeres Bewusstsein für Insider-Risiken, da Insider Zugang zu gefährdetem geistigem Eigentum haben.
- Während immer mehr Unternehmen KI-Tools einsetzen, um ihre Unternehmenssicherheit und Teameffizienz zu erhöhen, nutzen Cyberkriminelle generative KI, um realistischere Phishing-E-Mails, Nachrichten in Collaboration-Tools, schädliche Webseiten und sogar Deepfakes zu erstellen.
- Während der E-Mail-Verkehr und die Zusammenarbeit früher vor allem vor externen Angreifern geschützt wurden, sind Unternehmen heute durch große Veränderungen in ihrer Arbeitsweise dazu gezwungen, sich mit den Risiken externer und interner Bedrohungen auseinanderzusetzen.
- Trotz aufgestockter Cybersicherheitsbudgets, mit denen menschliche Sicherheitsrisiken ebenso wie die Sicherheit des E-Mail-Verkehrs und der Collaboration-Tools von Unternehmen gewährleistet werden sollen, kämpfen Sicherheitsverantwortliche weiterhin mit den Kosten für einen kontinuierlichen Schutz.

MARKTAKZEPTANZ DES HUMAN RISK MANAGEMENTS

Cybersicherheit im Wandel

Menschliches Versagen trägt zu 95 % der Datenschutzverletzungen bei. Um die Herausforderung des menschlichen Sicherheitsrisikos zu lösen, benötigen Unternehmen einen speziellen Ansatz zur Identifizierung, Bewertung und Minderung dieser Risiken, der auf jeden Benutzer individuell zugeschnitten ist.

Jeden Tag unterliegen Unternehmen Sicherheitsrisiken wie versehentlichen Datenlecks, ungesicherten Kommunikationskanälen und schlechter Passworthygiene. Daten von Mimecast zeigen, dass ein kleiner Teil der Belegschaft unverhältnismäßig oft zu Sicherheitsvorfällen beiträgt – nur 8 % der Mitarbeiter sind für 80 % der Vorfälle verantwortlich. HRM-Lösungen helfen Unternehmen dabei, bessere Präventionsstrategien umzusetzen, anstatt sich nur auf die Vorfallreaktion zu konzentrieren, und das ohne ihre Produktivität oder ihr Innovationspotenzial zu beeinträchtigen.

Dieser Wandel trägt der Erkenntnis Rechnung, dass ein gutes Sicherheitsbewusstsein allein nicht ausreicht. Während fast 87 % der befragten Unternehmen ihre Mitarbeiter vierteljährlich darin schulen, Bedrohungen zu erkennen und zu melden, nennen 33 % der Teilnehmer immer noch Mitarbeiterfehler als ihre größte Sorge. 27 % befürchten, dass Müdigkeit die Wachsamkeit von Mitarbeitern beeinträchtigt. Um diese einzelnen Herausforderungen zu lösen, benötigen Unternehmen zielgerichtete Ansätze.

.

87% der Befragten gaben an, dass ihr Unternehmen seine Mitarbeiter mindestens einmal im Quartal darin schult, Cyberangriffe zu erkennen..

33% befürchten Fehler und menschliches Versagen bei der Handhabung von E-Mail-Bedrohungen durch Mitarbeiter.

27% befürchten, dass erschöpfte Mitarbeiter nachlässiger agieren.

6% gaben an, dass die Sicherheitsrichtlinien ihres Unternehmens kontinuierlich als Reaktion auf neue Trends aktualisiert werden.

Obwohl die Sicherheit des E-Mail-Verkehrs nach wie vor entscheidend für den Unternehmensschutz ist, ist dieser Sicherheitsaspekt heute nur noch ein Teil des Puzzles. Beim Umgang mit menschlichen Sicherheitsrisiken müssen Gefahren gestoppt werden, bevor sie zu Sicherheitsvorfällen werden – die Devise lautet also Prävention statt Reaktion. Angesichts der zuvor erwähnten Erkenntnis (8 % der Mitarbeiter sind für 80 % der Sicherheitsvorfälle verantwortlich) müssen CISOs Produktivität und Innovation auf der einen Seite und menschliche Risiken auf der anderen Seite gut abwägen. Eine effektive KI wird sie dabei unterstützen.

Gefragt nach dem Schutz ihres E-Mail-Verkehrs und ihrer Collaboration-Tools geben nur 10 % der Befragten an, dass ihr Unternehmen entsprechende Cybersicherheitssysteme implementiert hat. Noch erschreckender ist, dass laut unserer Befragten nur 6 % der Unternehmen ihre Sicherheitsrichtlinien kontinuierlich auf der Grundlage neuer Cybersicherheitstrends anpassen. Darüber hinaus meinten die Befragten, dass ihre Unternehmen mehr Einsicht darin benötigen, wenn Daten auf USB-Geräten aus dem Unternehmen getragen werden (82 %) oder in Dateien an private E-Mail-Adressen gesendet werden (85 %).

Unsere Umfrageteilnehmer wurden gebeten, sich dazu zu äußern, wie ihr Unternehmen die Effektivität seiner Strategien zum Umgang mit menschlichen Sicherheitsrisiken misst:

44% gaben an, dass sie eine verstärkte Meldung von Vorfällen durch Mitarbeiter erwarten.

44% gaben an, dass sie die Erfolgsquoten von Phishing-Simulationen überwachen.

43% gaben an, dass sie Mitarbeiterfeedback in Umfragen erfassen.

41% gaben an, dass sie die Häufigkeit und Schwere von Sicherheitsvorfällen beobachten.

39% gaben an, dass sie im Anschluss von Schulungen Tests oder Quiz durchführen.

34% gaben an, dass sie sich ansehen, wie viele Mitarbeiter zusätzliche Sicherheitsschulungen benötigen.

Sicherheitsexperten warnen vor einem hohen Fehlerrisiko in folgenden Bereichen:

Versehentliche Freigabe von Daten	**84%**
Übermäßige Weitergabe von Unternehmensinformationen auf Social Media	**82%**
Schlechte Passworthygiene	**81%**
Verwendung nicht genehmigter Cloud-Speicher oder anderer Angebote	**80%**
Zugriff auf Dateien/Apps über ungesicherte Netzwerke	**80%**
Verwendung persönlicher E-Mail-Konten	**79%**
Nutzung von Tools für die Zusammenarbeit	**76%**
Verwendung eines Smartphones für arbeitsbezogene Aufgaben	**76%**
Surfen im Internet/Online-Shopping	**76%**

Menschliches Versagen

Cybersicherheitsprobleme, die durch menschliches Versagen entstehen, können erhebliche finanzielle und reputationsbezogene Folgen haben. Zu den kostspieligen Konsequenzen gehören Produktausfallzeiten, aufwändige Behebungsmaßnahmen für Sicherheitsverletzungen und möglicherweise auch irreparable Imageschäden. Fehler wie das Versenden sensibler Informationen an falsche Empfänger oder die unsachgemäße Entsorgung von Daten treten überraschend häufig auf und haben oft katastrophale Folgen.

Ein CIO aus der Versicherungsbranche erklärte die Risiken: „Unbeabsichtigte Datenschutzverletzungen treten dann auf, wenn Mitarbeiter durch falsch adressierte E-Mails oder die Nichteinhaltung von Datenvernichtungsprotokollen versehentlich sensible Systeme gefährden. Diese Fehler sind zwar unbeabsichtigt, haben aber trotzdem schwerwiegende Folgen."

Um diesen Herausforderungen zu begegnen, setzen Unternehmen zunehmend auf vernetzte HRM-Plattformen. Im Gegensatz zu isolierten Lösungen bieten diese Plattformen eine durchgängige Transparenz über externe und interne Risiken. Mithilfe dieser Systeme können Unternehmen ihre Collaboration-Tools überwachen, gefährdete Mitarbeiter identifizieren und potenziell schädliche Handlungen wie etwa eine unbefugte Datenfreigabe verhindern, bevor es zu Datenschutzverletzungen kommt.

HRM-Plattformen

Heute ist es wichtiger denn je, dass sich Unternehmen vor internen oder Insider-Risiken schützen können. Aus diesem Grund verlangen Unternehmen – insbesondere Kleinunternehmen – von ihren Mitarbeitern, dass sie nicht nur Bedrohungen im E-Mail-Verkehr und in Collaboration-Tools identifizieren, sondern dass sie auch auf den ordnungsgemäßen Umgang mit Unternehmensdaten achten. Früher setzten Unternehmen unzusammenhängende Lösungen ein, um dieses Problem des menschlichen Sicherheitsrisikos anzusprechen, aber heute ist das nicht mehr zeitgemäß.

HRM-Plattformen nehmen eine umfassende Analyse des Risikoprofils individueller Nutzer vor und liefern dabei Einblicke in Verhaltensmuster, Angriffsfaktoren sowie Gesamtrisikobewertungen. Der Angriffsfaktor ist eine wichtige Kennzahl: Sie quantifiziert das Risiko, dem eine Person ausgesetzt ist, basierend etwa auf der Anzahl der erhaltenen Phishing-E-Mails. Während Endbenutzer ihren Angriffsfaktor nicht kontrollieren können, ist er für Sicherheitsexperten von unschätzbarem Wert, da er einen direkten Einfluss auf das Gesamtrisiko des Unternehmens hat.

BUDGETS UND DAS GESCHÄFT DER SICHERHEIT

Die Cybersicherheitsausgaben in der Geschäftswelt steigen: 85 % der befragten Unternehmen berichteten von entsprechenden Budgeterhöhungen im letzten Jahr. Dennoch reichen diese Erhöhungen nicht aus, um steigenden Anforderungen gerecht zu werden. Nur 3 % der Sicherheitsverantwortlichen waren zuversichtlich, dass ihre Budgets ausreichen, während die Mehrheit angab, dass zusätzliche Investitionen im Personalbereich und für den Schutz ihrer Collaboration-Tools und ihres E-Mail-Verkehrs erforderlich sind.

Doch das Problem beschränkt sich nicht nur auf die Finanzierung. Viele CISOs müssen auch immer wieder darum kämpfen, ihre Vorstände von neuen Initiativen zu überzeugen. Da ist eine effektive Kommunikation mit Führungskräften entscheidend, damit weitere Investitionen in die Cybersicherheit nicht als Luxus, sondern als eine Notwendigkeit verstanden werden. Vorstände verlangen zunehmend klare Nachweise für den ROI dieser Tools und möchten messbare Auswirkungen auf die Geschäftskontinuität und die Sicherheitslage sehen. Insbesondere in Großunternehmen müssen Sicherheitsverantwortliche und IT-Leitung eng zusammenarbeiten, um den Vorstand darüber in Kenntnis zu setzen, welchen Sicherheitsbedrohungen das Unternehmen aktuell ausgesetzt ist, wie das Unternehmen diese Bedrohungen handhabt, was eine mangelnde Vorfallreaktion für das Unternehmen bedeuten könnte und welche zusätzlichen Werkzeuge und Ressourcen benötigt werden, um das Unternehmen abzusichern.

Gleichzeitig müssen Sicherheitsverantwortliche der Effizienz Priorität einräumen. Wenn sie ihre Teams mit unzusammenhängenden Tools überladen, schaffen sie nur zusätzliche Komplexität, die es ihnen erschwert, in einem Meer von Daten handfeste Erkenntnisse zu finden. Mit einem zentralisierten und integrierten HRM-Ansatz können Sicherheitsverantwortliche nicht nur ihre Abläufe rationalisieren, sondern auch die Zweckmäßigkeit ihres Budgets anhand klarer Ergebnisse belegen.

85% gaben an, dass ihr Unternehmensbudget für Cybersicherheit in den letzten 12 Monaten gestiegen ist.

3% meinten, dass in keinem Bereich ihrer Cybersicherheit zusätzliches Budget erforderlich sei.

57% gaben an, dass zusätzliches Budget für Personal sowie Dienstleistungen von Drittanbietern im Bereich der Cybersicherheit benötigt wird.

52% sagten, dass zusätzliches Budget für den Schutz ihrer Collaboration-Tools (nicht-E-Mail-basierte Tools wie Teams oder Slack) erforderlich ist.

47% gaben an, dass ein zusätzliches Budget für die E-Mail-Sicherheit erforderlich ist.

CISOs und ihr Sicherheitsbudget

Sicherheitsverantwortliche werden stets mit Budgetbeschränkungen leben müssen, und es macht ohnehin keinen Sinn, die eigenen Ausgaben ständig zu erhöhen, um immer wieder neue Sicherheitstools zu implementieren. Je mehr Tools Unternehmen haben, desto höher wird auch die Komplexität ihres Tech-Stacks – mehr Konsolen, mehr Protokolle, mehr von allem.

Sicherheitsteams haben die Aufgabe, aus einem schier endlosen Strom von Datenpunkten, Warnungen und Vorfällen sinnvolle Schlussfolgerungen zu ziehen. Je mehr Tools sie dafür nutzen, je größer wird die Herausforderung, die wirklich wichtigen Informationen aus diesem riesigen Meer von Daten zu fischen. Noch komplizierter wird es, wenn sie für jedes dieser Tools ein separates Dashboard haben. Außerdem erzählen Daten isoliert betrachtet eine ganz andere Geschichte als in aggregierter Form. Zum Beispiel sollte man auf jeden Fall untersuchen, wenn ein Nutzer auf einen verdächtigen Link klickt, wenn ein verdächtiger Anmeldeversuch von einem neuen Standort registriert wird oder wenn Quellcode aus dem Unternehmen getragen wird. Wenn jedoch alle diese Ereignisse nacheinander bei einem einzelnen Benutzer auftreten, sollten alle Alarmglocken läuten.

Gespräche über Budget- und Sicherheits-ROIs sind weitaus einfacher zu bestreiten, wenn Sicherheitsteams ihre Daten schnell und präzise genug korrelieren können, um Vorfälle zu identifizieren, bevor diese sich ausweiten. Dann können sie ihre Positionen gegenüber der eigenen Führung oder dem Vorstand leichter verteidigen.

Aber nur

3%

meinten, dass in keinem Bereich ihrer Cybersicherheit zusätzliches Budget erforderlich sei.

BEDROHUNGSSCHUTZ FÜR E-MAIL UND ZUSAMMENARBEIT

Schutz des E-Mail-Verkehrs und der Zusammenarbeit

Plattformen für die Zusammenarbeit wie Slack, Zoom und Microsoft Teams, ebenso wie E-Mail-Tools sind zu Eckpfeilern des Geschäftslebens geworden. Leider zielen Cyberkriminelle auf diese alltäglichen Interaktionen ab, um sich Zugang zu Unternehmenssystemen zu verschaffen. Dabei machen sie oft Mitarbeiter zu unwissenden Teilnehmern ihrer Machenschaften. Tatsächlich stellen Tools für die Zusammenarbeit nach wie vor eine wachsende Angriffsfläche dar, mit einem Anstieg der Angriffe um 7 % gegenüber 2024. Trotz der Verfügbarkeit fortschrittlicher Sicherheitstools bleibt E-Mail der häufigste Einstiegspunkt für Angreifer.

Daher ist es für Unternehmen wichtig, KI-gestützte Sicherheitslösungen einzuführen. KI-Tools sichern nicht nur den E-Mail-Verkehr und Plattformen für die Zusammenarbeit ab, sondern verbessern auch die Mitarbeiterproduktivität, indem sie ausgeklügelte Bedrohungen abfangen, bevor sie in Ihr System eindringen. Diese Technologien sind so konzipiert, dass sie sich an immer neue Angreifertaktiken anpassen, um selbst die vorsichtigsten Mitarbeiter davor zu schützen, zum Opfer zu werden.

Die wachsende Bedrohung gegenüber Collaboration-Plattformen sollte Sicherheitsverantwortliche aufhorchen lassen. Viele Unternehmen haben tatsächlich bereits entsprechend reagiert, wobei einige von ihnen drastische Maßnahmen ergreifen. Marriott zum Beispiel implementierte nach einem Slack-basierten Angriff strengere Sicherheitsvorkehrungen, während Disney seine Verwendung von Slack sogar komplett einstellte, um die damit verbundenen Risiken zu beseitigen. Allerdings ist das Verbot von Tools für die Zusammenarbeit nicht wirklich nachhaltig für die betriebliche Effizienz. Sicherheitsteams sollten stattdessen ihrer Verpflichtung nachkommen, integrierte Richtlinien zu entwickeln, die Benutzer auf all ihren Arbeitsflächen schützen.

44% der Befragten haben in den letzten 12 Monaten eine Zunahme der Bedrohungen über Collaboration-Tools festgestellt.

60% gaben an, dass ihr Unternehmen über eine formelle Cybersicherheitsstrategie verfügt, die alle wichtigen Geschäftsbereiche abdeckt – im Vergleich zu 48 % im Vorjahr.

96% gaben an, dass die Einführung einer formellen Cybersicherheitsstrategie das Cybersicherheitsrisiko ihres Unternehmens reduziert hat.

95% erwarteten im Jahr 2025 Herausforderungen im Bereich der E-Mail-Sicherheit.

61% gaben an, dass es unvermeidlich oder wahrscheinlich ist, dass ihr Unternehmen im Jahr 2025 negative geschäftliche Auswirkungen durch einen Angriff im Zusammenhang mit einem Collaboration-Tool erleiden wird.

79% stimmten zu, dass der Einsatz von Collaboration-Tools in ihrem Unternehmen neue Bedrohungen und Sicherheitslücken mit sich bringt, die dringend behoben werden müssen.

67% stimmten zu, dass die meisten nativen Sicherheitsmaßnahmen von Collaboration-Tools ihren Anforderungen nicht gerecht werden.

Eine Plattform für den Umgang mit menschlichen Sicherheitsrisiken (Human Risk Management, HRM) könnte hier die passende Lösung sein. Sie wäre beispielsweise in der Lage, den Schutz eines Collaboration-Tools wie Slack anhand einer Integration mit der Slack-API zu unterstützen. Dadurch könnte ein Unternehmen alle seine Slack-Nachrichten aufzeichnen – einschließlich Bearbeitungen und Löschungen. Dies wiederum ermöglicht eine umfassende Überwachung, Datenverlustprävention und E-Discovery, da das Unternehmen durch eine KI-gestützte Analyse in einem durchsuchbaren Archiv sensible Informationen und potenzielle Compliance-Verstöße in Slack-Gesprächen identifizieren kann. Eine HRM-Plattform würde damit als zentraler Kontrollpunkt zur Durchsetzung von Datensicherheitsrichtlinien auf der Collaboration-Plattform dienen.

Ausgeklügelte Business-Email-Compromise-Angriffe

Die Geschäftswelt registriert immer mehr Business-Email-Compromise(BEC)-Angriffe. Forschungen zeigen einen signifikanten Anstieg in der Häufigkeit und Raffinesse dieser Angriffe, was hauptsächlich auf die zunehmende Verfügbarkeit von KI-Tools zurückzuführen ist, die überzeugendere Phishing-Kampagnen mit einem höheren Grad der Personalisierung ermöglichen. Dadurch sind ausgefeilte BEC-Angriffe heute schädlicher denn je und noch schwerer zu erkennen.

Gleichzeitig ist KI aber auch für die Bekämpfung von BEC unerlässlich, da sie sich an immer raffiniertere Bedrohungen anpassen kann. Allerdings müssen Sicherheitsteams ihre KI dafür auch unter Beachtung bewährter Methoden anwenden. Die Herausforderung für Sicherheitsteams besteht darin, riesige Datenmengen effektiv zu handhaben, während Bedrohungsakteure ihre Techniken ständig ändern. Heute brauchen Unternehmen daher Erkennungsmethoden, die sich nicht auf Signaturen oder heuristische Analysen stützen.

Der IT-Leiter eines Einzelhandelsunternehmens fasste die Notwendigkeit des Einsatzes von KI wie folgt zusammen: „Man sollte nicht versuchen, Probleme mit KI punktuell zu lösen. Man muss sich dem Konzept voll und ganz verschreiben.“

Der IT-Leiter eines Versorgungsunternehmens spiegelte diese Aussage und erklärte, dass nicht nur der Einsatz von KI-Tools in Unternehmen wichtig sei, sondern dass auch Sicherheitsanbieter dazu bereit sein sollten, bei der Implementierung zu helfen. „Ich denke, die KI wird sich schnell weiterentwickeln und wir werden uns ihr auch schnell ganz verschreiben müssen“, sagte er. „Besonders im Cyberspace muss man den Entwicklungen immer einen Schritt voraus sein. Also suchen wir nach Anbietern, die uns dabei helfen können.“

> “Ich denke, [BEC] wird sich schnell weiterentwickeln, und wir werden [KI] ebenfalls zügig integrieren müssen.”
>
> – Head of IT, Retail

Umfrageergebnisse

95 % unserer Befragten erwarteten sich für das Jahr 2025 Herausforderungen im Bereich der E-Mail-Sicherheit und 44 % berichteten von einem Anstieg der Bedrohungen über Collaboration-Tools in den vorangegangenen 12 Monaten. Diese Statistiken untermauern noch einmal die Ergebnisse aus Mimecasts jüngsten Bedrohungsdaten, aus denen eine Zunahme von Spam, Angriffen mit Identitätsmissbrauch und bekannter Malware sowie eine allgemeine Zunahme der Bedrohungen pro Benutzer für alle Unternehmensgrößen im Nahen Osten und in Südafrika hervorgingen.

79 % der Befragten stimmten zu, dass die Verwendung von Collaboration-Tools in ihrem Unternehmen neue Bedrohungen und Sicherheitslücken mit sich bringt, die dringend gehandhabt werden müssen. Darüber hinaus gaben 61 % an, dass es unvermeidlich oder wahrscheinlich ist, dass ihr Unternehmen im Jahr 2025 durch einen Angriff im Zusammenhang mit einem Collaboration-Tool negative Geschäftsauswirkungen erleiden wird. 67 % stimmten zu, dass die nativen Sicherheitsmaßnahmen der meisten Collaboration-Tools ihren Anforderungen nicht gerecht werden.

Es gibt jedoch auch gute Nachrichten: 60 % der Umfrageteilnehmer sagten, dass ihr Unternehmen über eine formelle Cybersicherheitsstrategie verfügt, die alle wichtigen Geschäftsfunktionen abdeckt – im Vergleich zu nur 48 % im Jahr 2024. 96 % waren der Meinung, dass die Einführung einer formellen Cybersicherheitsstrategie das Risikoniveau ihres Unternehmens verbessert hat.

Darüber hinaus gaben 38 % der Unternehmen an, dass ihre Cybersicherheitspraktiken beim Schutz ihrer Mitarbeiter und ihrer Lieferkette vollständig wirksam sind, und 37 % sagten dasselbe über den Schutz ihrer Kunden. 48 % waren der Meinung, dass ihre Cybersicherheitspraktiken überwiegend wirksam zum Schutz von Mitarbeitern und Kunden waren, und 46 % sagten dasselbe für ihre Lieferkette. Eine Minderheit ist demnach der Meinung, dass sie ihre Mitarbeiter (14 %), Kunden (15 %) und Lieferketten (16 %) nicht oder nur unzureichend schützen kann.

Die Mehrheit der befragten Unternehmen hat bereits Sicherheitsmaßnahmen für ihren E-Mail-Verkehr und ihre Collaboration-Tools implementiert oder ist dabei, diese umzusetzen:

53% überwachen und schützen derzeit ihren ausgehenden E-Mail-Verkehr vor Datenlecks oder -abschöpfung, und 33 % sind aktuell dabei, solche Schutzmaßnahmen zu implementieren

54% suchen aktiv nach und schützen sich vor E-Mail-Angriffen wie Malware und schädlichen Links in eingehenden E-Mails, und 34 % sind aktuell dabei, solche Schutzmaßnahmen zu implementieren.

53% suchen aktiv nach und schützen sich vor E-Mail-Angriffen oder Datenlecks in internen E-Mails, und 35 % sind aktuell dabei, solche Schutzmaßnahmen zu implementieren.

52% überwachen ihre Collaboration-Tools auf Angriffe, und 34 % sind aktuell dabei, solche Schutzmaßnahmen zu implementieren.

53% identifizieren E-Mails, die ihre E-Mail-Domains fälschen, und 29 % sind aktuell dabei, solche Schutzmaßnahmen zu implementieren.

48% erkennen und entfernen schädliche oder unerwünschte E-Mails, die sich bereits in den Posteingängen ihrer Mitarbeiter befinden, und 40 % sind aktuell dabei, solche Schutzmaßnahmen zu implementieren.

66% suchen aktiv nach und schützen sich vor E-Mail-Angriffen, bevor diese die Posteingänge ihrer Mitarbeiter erreichen, und 28 % sind aktuell dabei, solche Schutzmaßnahmen zu implementieren.

DATENVERLUST UND INSIDER-RISIKO

Externe Risiken bleiben zwar eine Priorität für Sicherheitsteams, doch sie müssen künftig genauso wachsam sein, um Risiken aus dem Unternehmensinneren zu handhaben – sowohl absichtliche als auch unabsichtliche.

Insider-Bedrohungen nehmen die unterschiedlichsten Formen an: ein unzufriedener Mitarbeiter, der geistiges Eigentum stiehlt oder externen Bedrohungsakteuren Zugang zu kritischen Systemen gewährt; ein komplett überlasteter und erschöpfter Benutzer, der nachlässig wird; ein Benutzer, der seine Anmeldedaten versehentlich an einen Bedrohungsakteur weitergegeben hat; oder ein gezielt anvisierter Benutzer, der einem Social-Engineering-Angriff von Cyberkriminellen zum Opfer gefallen ist und ihnen dadurch Zugang zu Systemen gewährt hat. Tatsache ist, dass Unternehmen sich darauf vorbereiten müssen, durch interne Benutzer kompromittiert zu werden.

43% der Befragten stellten in den letzten 12 Monaten eine Zunahme interner Bedrohungen oder Datenlecks fest, die durch kompromittierte, unvorsichtige oder nachlässige Mitarbeiter verursacht wurden.

66% waren besorgt, dass der Datenverlust durch Insider in ihrem Unternehmen in den folgenden 12 Monaten zunehmen würde.

Datenlecks, Datenverluste, Datendiebstähle oder Datenpreisgaben, die von Insidern verursacht werden, würden die Unternehmen der Befragten durchschnittlich **$13.9 Millionen** US-Dollar kosten.

Umfrageergebnisse

Auf die Frage nach fahrlässigen, kompromittierten und gezielt anvisierten Benutzern berichteten 43 % der Befragten in den letzten 12 Monaten von einer Zunahme interner Bedrohungen oder Datenlecks, und 66 % erwarteten in den folgenden 12 Monaten einen Anstieg der Datenverluste in ihrem Unternehmen. Entscheidungsträger im Sicherheitsbereich gaben an, dass sie ein Insider-Datenleck und -Diebstahl durchschnittlich 13,9 Millionen US-Dollar kosten würde.

Künstliche Intelligenz

Im Bereich der Cybersicherheit kommt künstliche Intelligenz immer öfter zum Einsatz. Viele Unternehmen entscheiden sich zunehmend für KI-gestützte Lösungen, um immer ausgeklügeltere Cyberbedrohungen zu bekämpfen, Anomalien zu erkennen und ihre allgemeine Sicherheitslage zu verbessern. Dieser Trend ist darauf zurückzuführen, dass KI große Datenmengen schnell analysieren und Muster erkennen kann, die mit traditionellen Methoden möglicherweise unbemerkt bleiben würden. Doch leider wird KI auch zunehmend von Cyberkriminellen als Waffe eingesetzt. KI-gestützte Cyberangriffe nutzen Algorithmen und Techniken zur Automatisierung, Beschleunigung und Verbesserung verschiedener Phasen von Cyberangriffen.

Mimecast's Threat Intelligence Hub stellt eine kürzlich erfolgreich durchgeführte Phishing-Kampagne vor, bei dem ein legitimes CMS missbraucht wurde, um betrügerische E-Mails mit Stellenangeboten von bekannten Marken zu versenden.

Weitere bekannte Cyberangriffe in der Branche, die durch Insider unterstützt wurden: eine Datenfreilegung bei Pegasus Airlines aufgrund von Mitarbeiterfahrlässigkeit; die dreifache Datenpanne bei Mailchimp, verursacht durch Social Engineering; der Diebstahl von Slacks Code-Repositories durch einen kompromittierten Anbieter; der Diebstahl geistigen Eigentums durch einen böswilligen Insider bei Yahoo; und eine riesige Datenpanne durch ehemalige Tesla-Mitarbeiter.

KI zu Verteidigungszwecken

Unternehmen verwenden KI im Rahmen ihrer Cybersicherheitsbemühungen hauptsächlich dafür, Bedrohungen besser zu erkennen. Mit einer KI können sie große Datenmengen analysieren, um Muster und Anomalien zu identifizieren, die auf schädliche Aktivitäten hinweisen können. Dies wiederum führt zu kürzeren Reaktionszeiten und einer proaktiven Bedrohungsabwehr. Letztere umfasst Funktionen wie die automatisierte Reaktion auf Vorfälle, die Verhaltensanalyse von Benutzeraktivitäten, den Schwachstellenscan und prädiktive Analysen zur Vorhersage potenzieller Angriffe. Gleichzeitig wird das menschliche Eingreifen in Routineaufgaben wie Protokollanalysen und Systemüberwachung auf ein Minimum reduziert.

95%

der Befragten gaben an, dass ihr Unternehmen KI einsetzt, um sich gegen Cyberangriffe und/oder interne Bedrohungen zu verteidigen.

81%

waren besorgt über die Möglichkeit, dass sensible Daten über GenAI-Tools freigegeben werden könnten.

55%

sind NICHT vollständig mit spezifischen Strategien auf KI-gestützte Bedrohungen vorbereitet.

KI zu Angriffszwecken

Cyberkriminelle nutzen ebenfalls generative KI. Sie erstellen damit realistischere Phishing-E-Mails und Webseiten mit schädlichen Inhalten, wodurch Mitarbeiter leichter dazu verleitet werden, auf Links zu klicken, schädliche Anhänge herunterzuladen und schädliche Webseiten zu besuchen. Cyberkriminelle nutzen KI aber auch, um bestimmte Aufgaben zu automatisieren, realistischere Deepfakes zu erzeugen, ausgewählte Opfer mit personalisierten Kampagnen anzugreifen und sogar raffiniertere Malware zu entwickeln, die schwerer zu erkennen ist. Des Weiteren nutzen Bedrohungsakteure KI, um den Code potenzieller Opfer zu scannen, sodass sie weniger Zeit benötigen, um Schwachstellen zu finden.

Die meisten Organisationen verwenden KI-Tools, um Insider-Risiken zu minimieren:

46%
Bedrohungserkennung und Echtzeitüberwachung

46%
Analyse von und Reaktion auf Phishing-Angriffe(n)

43%
Schutz von Endpunkten und Anti-Malware-Tools

43%
Verhaltens- oder Stimmungsanalyse und Erkennung von Insider-Bedrohungen

43%
Automatisierte Systeme zur Reaktion auf Vorfälle

Governance und Compliance

Durch Governance und Compliance schaffen Unternehmensverantwortliche einen starken Rahmen zur Identifizierung und Handhabung von Cyberrisiken, mit dem sie einen rechtlich einwandfreien Unternehmensbetrieb sowie die Ausrichtung an Branchenstandards und internen Richtlinien gewährleisten. Governance und Compliance richten den Fokus auf die Absicherung sensibler Daten, die Gewährleistung der Geschäftskontinuität und die Vermeidung negativer rechtlicher Konsequenzen aus Datenschutzverletzungen oder Sicherheitsvorfällen. Somit stellen sie die proaktive Verteidigung eines Unternehmens gegen einen unsichtbaren Feind dar.

Mit KI können Unternehmen jedoch noch einen Schritt weiter gehen. Wenn sie KI geschickt einsetzen, können sie damit ihre Compliance-Bemühungen erheblich verstärken: KI arbeitet unermüdlich daran, überwältigende Datenmengen zu analysieren, potenzielle Bedrohungen zu erkennen, Anomalien in Echtzeit zu identifizieren, langwierige Sicherheitsarbeiten zu automatisieren, eingehende Angriffe vorherzusagen und Reaktionen zu priorisieren. KI ermöglicht ihnen eine vorausschauende Bedrohungsabwehr, unterstützt sie bei der Einhaltung relevanter Sicherheitsstandards und -vorschriften und maximiert ihre Effizienz bei der E-Discovery.

Mit KI können Unternehmen jeder Größe, Branche und an jedem Standort weltweit nicht nur ihr Compliance- und Sicherheitsniveau verbessern, sondern auch die Effizienz ihrer Mitarbeiter. Die Zukunft der Cybersicherheit besteht somit aus Sicherheitstools, die KI auf strategisch wertvolle Weise nutzen. Außerdem ist KI wohl die einzige Möglichkeit, der Welt der Cyberkriminalität mit ihren immer ausgeklügelteren Angriffen einen Schritt voraus zu bleiben.

Umfrageergebnisse

Zum Thema künstliche Intelligenz gaben 95 % der Befragten an, dass ihr Unternehmen KI einsetzt, um sich gegen Cyberangriffe und/oder Insider-Bedrohungen zu verteidigen. 81 % waren besorgt über das Potenzial für Lecks sensibler Daten durch GenAI-Tools und 55 % waren nicht vollständig mit spezifischen Strategien auf KI-gestützte Bedrohungen vorbereitet.

Wie reagieren Unternehmen auf das Potenzial von KI, menschliche Verhaltensweisen und Fehler in der Cybersicherheit auszunutzen?

44% Implementierung von KI-gestützten Überwachungs- und Schutztools

44% Entwicklung interner KI-Tools zum Schutz vor KI-gesteuerten Angriffen

42% Schulungen zur Nutzung von KI, damit keine Schwachstellen ausgenutzt werden

40% Erstellung von Richtlinien zur Nutzung von KI

38% Aktualisierung oder Einführung eines Verhaltenskodex für KI-gesteuerte Risiken

36% Zusammenarbeit/Austausch relevanter Informationen mit Partnern

35% Durchführung simulierter KI-gesteuerter Phishing-Angriffe

DAS SICHERHEITSBEWUSSTSEIN IN UNTERNEHMEN ENTWICKELT SICH WEITER

Dass die Belegschaft eines Unternehmens ein gutes Sicherheitsbewusstsein hat, ist eine unabdingbare Voraussetzung der modernen Cybersicherheit. Mitarbeiter werden dadurch dazu befähigt, Cyberbedrohungen zu erkennen und effektiv darauf zu reagieren, während gleichzeitig Risiken wie Datenschutzverletzungen minimiert werden. Der Mensch ist die bedeutendste Schwachstelle in Unternehmenssystemen, doch ein gutes Sicherheitsbewusstsein verleitet Mitarbeiter dazu, sich mit ihren Sicherheitsprotokollen auseinanderzusetzen, sodass sie schädliche Aktivitäten erkennen und die digitalen Vermögenswerte ihres Unternehmens besser schützen können.

Unbedingt vermeiden sollte man es jedoch, allen Mitarbeitern identische Schulungen anzubieten, ohne Nutzern mit erhöhtem Risiko besondere Beachtung zu schenken. Um Einzelpersonen gezielt zu unterstützen, braucht es einen innovativen Ansatz. Wichtige Grundlage dafür sind interaktive und ansprechende Module, die kritische Themen wie die Phishing-Erkennung, die Passworthygiene und den Datenschutz abdecken. Um die Effektivität und Relevanz von Schulungen zu erhöhen, sollten auf der Basis von personalisierten Risikoprofilen gezielte Maßnahmen ergriffen werden, wie etwa die Anpassung von Inhalten für Personen, die aufgrund von datengestützten Tests als hochriskant identifiziert wurden.

HRM-Plattformen stellen die nächste Entwicklungsstufe im Bereich des Sicherheitsbewusstseins dar. Diese Plattformen bieten Echtzeiteinblicke in das Verhalten von Mitarbeitern und ihre jeweiligen Risikostufen, sodass Unternehmen Schulungen gezielt bei Hochrisikonutzern durchführen können. HRM-Tools können die Effektivität dieser Maßnahmen quantifizieren, indem sie messbare Verbesserungen im Verhalten aufzeigen und Bereiche identifizieren, in denen noch Lücken bestehen. Dadurch kann wiederum die Wirksamkeit der Maßnahmen gewährleistet werden.

Es ist wichtig zu verstehen, dass eine Einheitslösung zur Stärkung des Sicherheitsbewusstseins nicht funktioniert. Adaptive Lernlösungen sind von entscheidender Bedeutung, da sie Ressourcen auf Mitarbeiter fokussieren, deren Verhalten das höchste Risiko aufweist. Ebenso müssen HRM-Plattformen über kontinuierliche Feedbackschleifen die Fortschritte und Schwächen der einzelnen Nutzer aufzeigen können, um im Laufe der Zeit eine Kultur der proaktiven Cybersicherheit aufzubauen.

Umfrageergebnisse

Zum aktuellen Stand der Sicherheitsbewusstseinsschulungen zeigt unsere Studie, dass 87 % der Unternehmen ihre Mitarbeiter mindestens einmal im Quartal darin schulen, Cyberangriffe zu erkennen. Das ist zwar gut für die Stärkung des Sicherheitsbewusstseins, doch trotzdem befürchteten 33 % der Befragten Fehler und menschliches Versagen im Umgang mit E-Mail-Bedrohungen durch Mitarbeiter, 27 % befürchteten, dass die Wachsamkeit der Mitarbeiter durch Müdigkeit nachlässt, und 43 % stellten in den letzten 12 Monaten eine Zunahme interner Bedrohungen oder Datenlecks fest, die durch kompromittierte, unvorsichtige oder fahrlässige Mitarbeiter initiiert wurden. Darüber hinaus befürchteten zwei Drittel, dass der Datenverlust durch Insider in ihrem Unternehmen in den folgenden 12 Monaten zunehmen würde.

Der Frust über ein mangelndes Sicherheitsbewusstsein spiegelt sich in der Aussage eines IT-Leiters aus der Versorgungsbranche wider, als er sagte: „Ich wünschte, alle wären auf dem gleichen Level, was das Sicherheitsbewusstsein angeht. Wir versuchen es in unserer Unternehmenskultur zu verankern. Wir verbringen viel Zeit damit, Wissen zu vermitteln – im Intranet, durch Schulungen, anhand von Materialien oder über unsere Kommunikation. Wir versuchen, das Thema in den Vordergrund zu rücken.“ Kontinuierliche Sensibilisierungsschulungen, unterstützt durch eine HRM-Plattform zur Identifizierung der risikoreichsten Nutzer, können Unternehmen dabei helfen, dieses Ziel zu erreichen.

87% der Befragten gaben an, dass ihr Unternehmen seine Mitarbeiter mindestens einmal im Quartal darin schult, Cyberangriffe zu erkennen.

33% befürchteten Fehler und menschliches Versagen bei der Handhabung von E-Mail-Bedrohungen durch Mitarbeiter.

27% befürchteten, dass erschöpfte Mitarbeiter nachlässiger agieren.

43% stellten in den vorangegangenen 12 Monaten eine Zunahme interner Bedrohungen oder Datenlecks fest, die durch kompromittierte, unvorsichtige oder nachlässige Mitarbeiter verursacht wurden.

66% waren besorgt, dass der Datenverlust durch Insider in ihrem Unternehmen in den folgenden 12 Monaten zunehmen würde.

> „Wir versuchen, es als festen Bestandteil der Unternehmenskultur zu etablieren..“
>
> – IT Director, Utilities

WICHTIGE ERKENNTNISSE UND EMPFEHLUNGEN

In den letzten neun Jahren hat Mimecast jedes Jahr eine Umfrage durchgeführt, um den jeweils aktuellen Stand der Cybersicherheit zu ermitteln. Bisher mussten wir den Schwerpunkt auf den Schutz des E-Mail-Verkehrs und der Zusammenarbeit legen. Dieses Jahr hat sich unser Fokus allerdings aufgrund einer Veränderung in der Sicherheitslandschaft auf das menschliche Risiko verlagert. Die im diesjährigen Bericht enthaltenen Informationen sollen unseren Lesern Einblick einerseits in die Methoden geben, mit denen andere Cybersicherheitsexperten ihre Unternehmen schützen, andererseits aber auch in ihre Herausforderungen.

Wir hoffen, dass Sie diesen Bericht und die darin enthaltenen Daten für sich nutzen, um einen entsprechenden Plan zu erstellen, mit dem Sie Ihr Unternehmen im kommenden Jahr schützen werden.

1. Bewerten Sie die menschlichen Sicherheitsrisiken Ihres Unternehmens und implementieren Sie entsprechende HRM-Tools

Bewerten Sie den Reifegrad Ihrer Strategie zum Umgang mit menschlichen Sicherheitsrisiken (Human Risk Management, HRM). Identifizieren Sie Faktoren, die zum menschlichen Risiko beitragen, wie komplexe Prozesse, Arbeitsbelastung und Stressniveaus. Entwickeln Sie eine Strategie, welche die individuelle Risikotoleranz Ihres Unternehmens berücksichtigt. Erkunden Sie umfassende HRM-Plattformen, die zu Ihrem Budget und Ihren Ressourcen passen. Nutzen Sie diese Werkzeuge, um menschliche Risiken effektiv zu überwachen, zu verwalten und zu reduzieren.

2. Erhöhen Sie die Sichtbarkeit von Insider-Bedrohungen

Führen Sie Bewertungen durch, um das absichtliche und unabsichtliche Insider-Risikopotenzial Ihres Unternehmens zu verstehen. Achten Sie besonders auf Mitarbeiter, die das Unternehmen verlassen oder die am ehesten von Cyberkriminellen ins Visier genommen werden könnten. Setzen Sie entsprechende Tools ein – idealerweise innerhalb einer HRM-Plattform –, um das Verhalten von Mitarbeitern zu überwachen, verdächtige Aktivitäten zu erkennen und das Risiko von Datenverlusten oder Kompromittierungen durch Insider-Bedrohungen zu mindern.

3. Holen Sie sich möglichst viel Unterstützung durch künstliche Intelligenz

Überprüfen Sie regelmäßig die KI-Tools, die Ihr Team verwendet. Stellen Sie sicher, dass sie vollständig im Unternehmen integriert und auf dessen Bedürfnisse abgestimmt sind. Informieren Sie sich kontinuierlich über neue KI-Tools und die Taktiken, die Cyberkriminelle anwenden.

4. Stärken Sie die Sicherheit Ihres E-Mail-Verkehrs und Ihrer Collaboration-Tools

Bewerten und aktualisieren Sie Ihre E-Mail-Sicherheitstools. Ziehen Sie die Einführung umfassender Plattformen für den Schutz Ihres E-Mail-Verkehrs und Ihrer Collaboration-Tools in Betracht. Schulen Sie Ihre Benutzer darin, raffinierte Phishing- und BEC-Angriffe zu erkennen, und unterstützen Sie sie mit fortschrittlichen KI-basierten Sicherheitstechnologien.

5. Mindern Sie die Risiken Ihrer Collaboration-Tools

Sie sollten sich darüber im Klaren sein, dass Tools für die Zusammenarbeit zunehmend zur Angriffsfläche werden. Schützen Sie Ihre Mitarbeiter bei der Verwendung dieser Tools, indem Sie ähnliche Sicherheitsmaßnahmen wie für Ihren E-Mail-Verkehr implementieren, um die Bedrohungen auf ein Minimum zu reduzieren.

6. Optimieren Sie Ihre Sicherheitsbudgets für HRM-Plattformen

Arbeiten Sie daran, die Zustimmung der Geschäftsleitung für die Implementierung einer umfassenden HRM-Plattform zu gewinnen. Evaluieren Sie sorgfältig, ob potenzielle Lösungen intern verwaltet werden oder ob eine externe Unterstützung durch den Anbieter erforderlich ist. Weisen Sie Ihre Mittel möglichst effektiv zu, um die kritischsten Sicherheitsaspekte abzudecken.

7. Identifizieren Sie Hochrisikobenutzer; überwachen und messen Sie die Effektivität Ihrer Schulungen

Verwenden Sie HRM-Plattformen, um diejenigen Mitarbeiter zu identifizieren, die am anfälligsten für Cyberangriffe sind. Richten Sie dann zusätzliche Schulungen und Sicherheitsmaßnahmen auf diese Personen aus, um Ihr Gesamtrisiko zu minimieren. Verfolgen Sie kontinuierlich den Erfolg Ihrer Initiativen zur Stärkung des Sicherheitsbewusstseins.

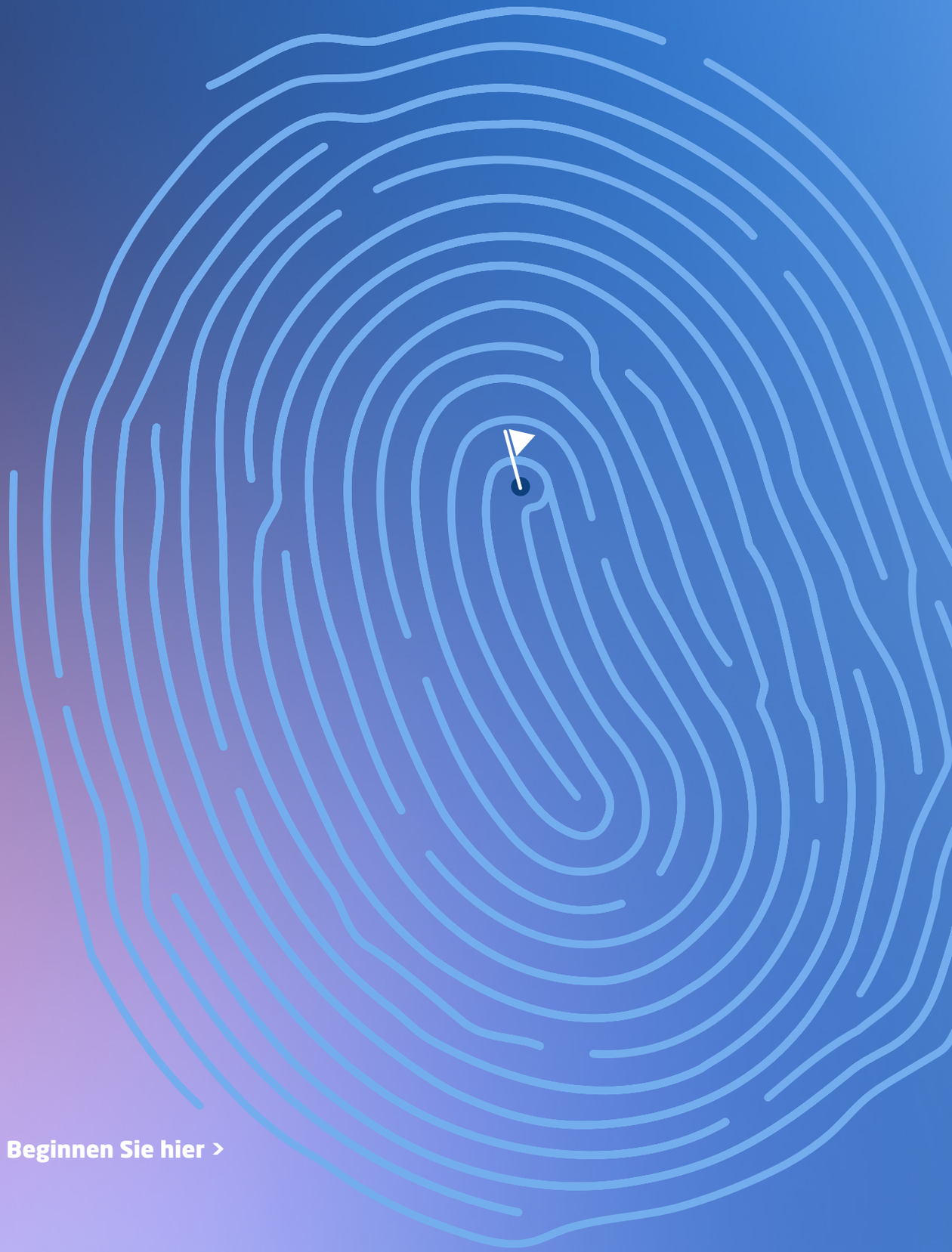
8. Entwickeln Sie Ihre Schutzmaßnahmen gegen Business Email Compromise weiter

Evaluieren Sie Ihr Risiko, Opfer von BEC-Angriffen zu werden, und stellen Sie sicher, dass alle Mitarbeiter gut darauf geschult sind, diese Bedrohungen zu erkennen. Kombinieren Sie Ihre Schulungen mit effektiver Technologie, um sich gegen ausgeklügelte E-Mail-basierte Betrugsmaschen zu verteidigen.

METHODIK

Dies ist das neunte Jahr in Folge, dass Mimecast eine eingehende globale Umfrage zum jeweils aktuellen Stand der Cybersicherheit durchgeführt hat. Für unseren Bericht für das Jahr 2025 beauftragten wir das Forschungsunternehmen Vanson Bourne im Zeitraum von November bis Dezember 2024 mit der Befragung von 1.100 IT-Sicherheitsmitarbeitern und IT-Entscheidungsträgern aus den Vereinigten Staaten, dem Vereinigten Königreich, Frankreich, Deutschland, Südafrika und Australien. Unsere Teilnehmer arbeiteten in einer Reihe von privaten und öffentlichen Sektoren, darunter im Gesundheitswesen, im Einzelhandel, im Finanzwesen, in der verarbeitenden Industrie und in Versorgungsunternehmen. Die Befragten mussten aus Unternehmen mit mindestens 250 Beschäftigten stammen. Vanson Bourne führte ebenfalls qualitative Interviews mit Sicherheitsverantwortlichen aus dem Vereinigten Königreich durch.

Die Teilnehmer der Umfrage arbeiteten in Unternehmen mit einer Größe zwischen 250 und 500 Mitarbeitern (5 % der Gesamtzahl) und mehr als 10.000 Mitarbeitern (20 % der Gesamtzahl). Diese Unternehmen verteilten sich auf 11 Industriesektoren, darunter Finanzdienstleistungen (12 %), Technologie und Telekommunikation (13 %), Einzelhandel (15 %), Gesundheitswesen (10 %), verarbeitendes Gewerbe (11 %) und öffentlicher Sektor (5 %).



Beginnen Sie hier >

mimecast®

Über Mimecast

Mimecast ist eine KI-gestützte, API-fähige und vernetzte Human Risk Management-Plattform. Sie wurde entwickelt, um Unternehmen vor dem gesamten Spektrum von Cyberbedrohungen zu schützen. Dafür integriert sie moderne, benutzerfreundliche Technologie mit Strategien für das Erkennen von Risiken und den Aufbau von Sicherheitskompetenz, die immer den Nutzer im Fokus behalten. Darauf ausgelegt, unsichtbare Risiken sichtbar zu machen und Dateneinblicke so aufzubereiten, dass sie als Entscheidungsgrundlage dienen können, eröffnet sie Unternehmen proaktive Handlungsmöglichkeiten. Sie hilft, Kommunikations- und Kollaborationslandschaften zu schützen, kritische Daten zu sichern, Mitarbeiter aktiv in das Risikomanagement einzubeziehen und eine Sicherheitskultur zu fördern, die mit Unternehmenszielen wie Geschäftskontinuität und Steigerung der Produktivität in Einklang steht. Über 42.000 Unternehmen weltweit vertrauen Mimecast, um der sich dynamisch entwickelnden Bedrohungslandschaft einen Schritt voraus zu sein. Von internen Risiken bis hin zu externen Gefahren – Mimecast bietet Kunden mehr. Mehr Sichtbarkeit. Mehr Einblicke. Mehr Agilität. Mehr Sicherheit.