

---

Insight Leitfaden:  
Menschliche Faktoren  
im Bereich Security

---



## Einleitung

Wir bei Insight wissen um die Bedeutung eines ganzheitlichen Ansatzes für die Sicherheit. Angreifer suchen Ihren schwächsten Bereich, nicht Ihren stärksten. Wir verfügen über technisches Know-how in den fünf Technologiebereichen (Endpoints, Applikationen, Cloud, Netzwerk, Rechenzentrum und IOT sowie datenzentriert) - aber wir als führender Lösungsintegrator glauben, dass Sie auch genau auf die Interaktionen zwischen diesen Technologiebereichen (Governance, Risiko und Compliance, Identität und Zugriff, Bedrohungserkennung und -reaktion und menschliche Faktoren) achten sollten. Die Lücken, in denen sich die Technologiedomänen verbinden, sind häufig Bereiche, in denen ein zusätzlicher Wert erzielt werden kann, der dazu beiträgt, Ihre allgemeine Sicherheit auf kosteneffiziente Weise zu verbessern.

### Das ganzheitliche Sicherheitsmodell von Insight



## Was sind menschliche Faktoren und warum sind sie wichtig?

Obwohl die Sicherheitsinfrastruktur als auch Tools und Kontrollen kontinuierlich verbessert werden und in diese investiert wird, gibt es immer noch Verstöße, die nicht einfach zu erkennen und zu beheben sind. Es gibt viele spezialisierte Sicherheitskontrollen für verschiedene Arten von Bedrohungen und Angriffen auf Endgeräte bis hin zu Angriffen auf Lieferketten – aber wenn Sie untersuchen, wie diese Angriffe tatsächlich stattgefunden haben, sind die drei Hauptgründe:

- **Passwörter** – ein unsicheres Passwort wurde geknackt, ein Standardpasswort wurde unverändert gelassen oder dasselbe Passwort wurde an mehreren Standorten verwendet.
- **Phishing** – ein Benutzer wurde dazu getäuscht, entweder seine Anmeldedaten weiterzugeben, eine kompromittierte Website zu besuchen oder einen feindlichen Anhang zu öffnen.
- **Patching** – eine bekannte Schwachstelle wurde zu lange ungepatcht gelassen und von Malware ausgenutzt oder eine riskante Software wurde von einem Benutzer installiert, welcher kompromittiert wurde.

IT-Teams nutzen Technologie, um das Risiko von Sicherheitsverletzungen zu verringern, Endbenutzer spielen jedoch immer eine Rolle beim Sicherheitssupport eines Unternehmens. IT-Teams konzentrieren sich oft auf die Technologie und nur manchmal auf den Prozess und vergessen damit die menschliche Seite, obwohl der Mensch den Erfolg oder Misserfolg eines Projekts mitbestimmt.





**Prozess:** Die schriftlichen Richtlinien, in denen erklärt wird, was Benutzer tun sollten oder nicht, können viele Formen haben, wie z. B. Informationssicherheitsrichtlinien, Arbeitsverträge, Personalhandbücher, Richtlinien zur akzeptablen Nutzung oder Vorfallreaktionspläne.

**Technologie:** Die Tools, Systeme, Regeln und Kontrollen, die den Handlungsspielraum der Benutzer bestimmen, sollten robust genug sein, um gefährliche Aktivitäten zu begrenzen, aber gleichzeitig flexibel genug, um die Geschäftsabläufe nicht zu beeinträchtigen.

**Mitarbeiter:** wenn es keine dokumentierten Prozesse gibt oder die Mitarbeiter diese nicht kennen, müssen sie ihr eigenes Urteilsvermögen einsetzen. Versäumt Technologie es, eine neue Bedrohung zu verhindern, sind die Menschen oft die erste und letzte Verteidigungslinie und verlassen sich dabei allein auf ihre aktuellen Fähigkeiten und ihr Wissen aus Schulungen.

Bis 2027 werden 50 % der Chief Information Security Officers (CISOs) großer Unternehmen Praktiken für ein auf den Menschen ausgerichtetes Sicherheitsdesign eingeführt haben, um die Reibung, die durch Cybersicherheitsprozesse verursacht wird, zu minimieren und Kontrollanpassungen zu maximieren.

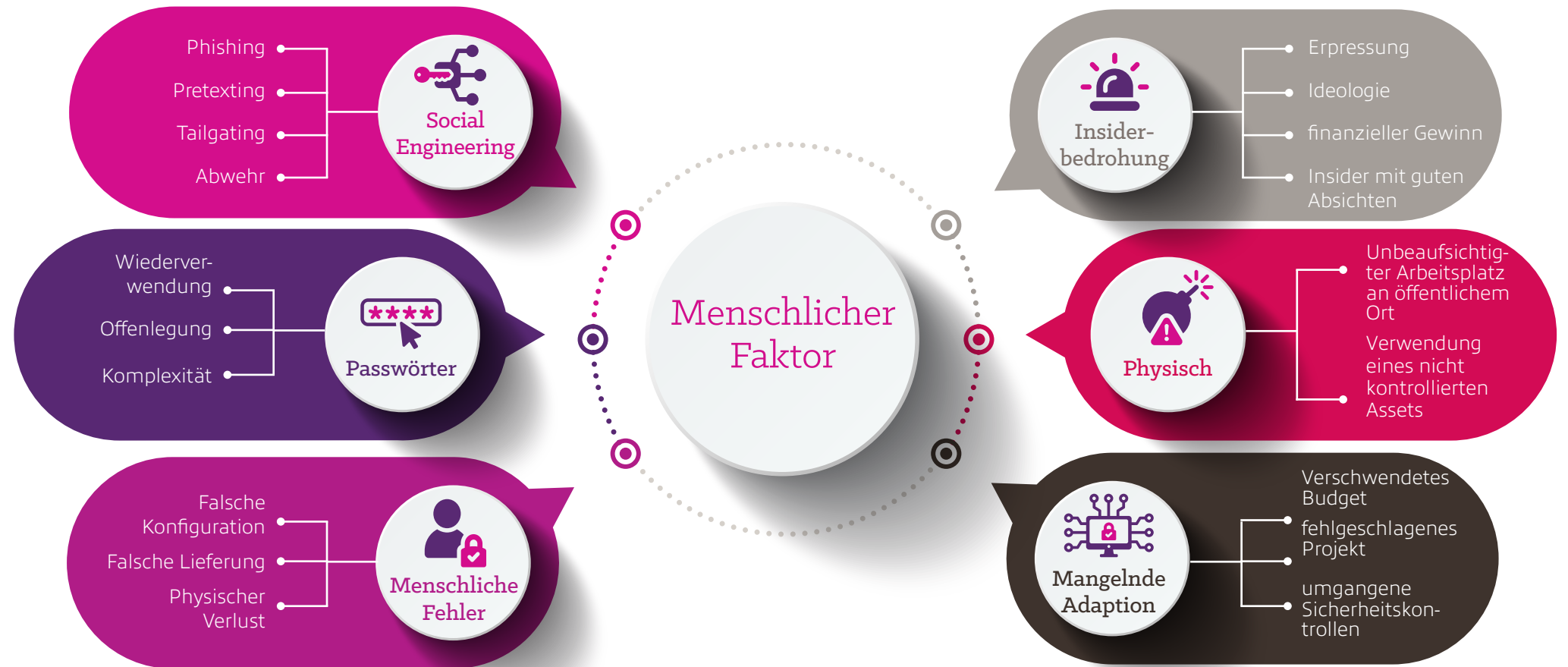
- Gartner identifiziert die wichtigsten Cybersicherheitstrends für 2023.

## Kompetenzlücke

Da die Cyberkompetenzlücke weiterhin ein Hindernis für Unternehmen darstellt, kann es erforderlich sein, Mitarbeiter aus anderen Teilen des Unternehmens in sicherheitsorientierte Rollen zu versetzen und sie mit den erforderlichen Fähigkeiten auszustatten. Schulungen und Begleitung am Arbeitsplatz haben ihre Grenzen, wenn die Fähigkeiten, die man vermitteln muss, in der Organisation kaum vorhanden sind. Für mehr qualifizierte Ressourcen wird die Schulung oft als unerlässlich angesehen, um technische Experten zu halten, die ihre Fähigkeiten auffrischen möchten.



Der menschliche Faktor kann sich auf fast jeden Aspekt Ihrer Sicherheitsstrategie auswirken



## Die Bedeutung von Personas

Sie sollten Ihre menschlichen Faktoren in der Sicherheitsstrategie auf die verschiedenen Arten von Benutzern oder Personas in Ihrem Unternehmen abstimmen. Ein generischer Ansatz ist nicht effektiv genug – die Mitarbeiter müssen in Bezug auf ihre aktuelle Rolle befähigt werden und verstehen, wie sie persönlich zur organisatorischen Sicherheit beitragen können.

Hier ein Beispiel für die Kategorisierung von Nutzertypen in einem Unternehmen. Dennoch gilt es zu berücksichtigen, dass jede Organisation individuell und anders ist.



### Endnutzer

- Unterschiedliche IT-Kenntnisse, einige mit lediglich Basis-Wissen
- Mehrsprachigkeit wird in globalen Organisationen eine Anforderung sein
- Themen können sich auf Phishing, DSGVO, physische Sicherheit usw. beziehen



### Entwickler

- Ist in der Regel technisch fortgeschritten, kennt aber möglicherweise keine sicheren Codiertechniken
- Es kann eine Nischenschulung erforderlich sein, wenn eine dem Entwickler bekannte Programmiersprache verwendet wird
- Gamification und praxisbezogenes Lernen wirken sich besser aus als nicht interaktives Lernen



### IT-Administrator

- Technisch fortgeschrittene Anwender wollen ihre bestehenden Fähigkeiten weiter entwickeln können und herausgefordert werden
- Gamification und Wettbewerb fördern die Akzeptanz
- Wie bei einem Piloten können praktische Fähigkeiten in einer sicheren, regelmäßig verwendeten Softwareumgebung helfen, auf reale Situationen mit hohem Sicherheitsstress zu reagieren



### Unternehmensleitung

- Fokus auf teambasierte Gruppenlernaktivitäten, um Entscheidungsfindungsprozesse, Rollen und Verantwortlichkeitsdefinitionen zu testen
- Geschäftszentriert
- Kann viele verschiedene Rollen einbeziehen, um die Teamdynamik zu testen



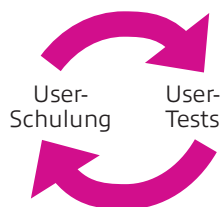
## Wie Insight helfen kann

### Managed Security Awareness für Endbenutzer

In der heutigen digitalen Softwareumgebung, in der die meisten Geschäftsvorgänge online durchgeführt werden, ist es von entscheidender Bedeutung, dass sich die Endbenutzer der Sicherheit bewusst sind. Unternehmen müssen sicherstellen, dass ihre Mitarbeiter die möglichen Gefahren von Cyberangriffen kennen und wissen, wie sie diese Gefahren reduzieren können. Dazu gehört, dass Mitarbeiter lernen, wie sie bewährte Verfahren für das Passwortmanagement befolgen, sichere Surfgegewohnheiten anwenden und verdächtige E-Mails erkennen und melden können.

Phishing-Angriffe sind eines der größten Risiken für die Cybersicherheit eines Unternehmens. Diese Angriffe versuchen, Personen dazu zu verleiten, persönliche Informationen wie Benutzernamen, Passwörter oder finanzielle Daten preiszugeben. Phishing-Simulationen sind eine nützliche Möglichkeit, Mitarbeitern beizubringen, wie sie sich vor diesen Angriffen schützen können. Indem sie gefälschte Phishing-E-Mails erstellen, die wie echte aussehen, können Mitarbeiter lernen, verdächtige E-Mails zu erkennen und zu melden.

Wir arbeiten mit KnowBe4 zusammen, einem Experten für Sicherheitsbewusstseinsschulungen für Endbenutzer, der eine vollständige Plattform mit Schulungsmodulen, Phishing-Simulationen und anderen Tools bereitstellt, die Mitarbeiter über die neuesten Bedrohungen und deren Vermeidung informieren. Die Plattform nutzt ansprechende Methoden wie Videos, Quiz und interaktive Spiele, um die Mitarbeiter einzubeziehen und das Schulungserlebnis angenehmer zu gestalten.



Deren Methodik basiert auf einem Trainings- und Testzyklus - nicht einmal im Jahr, sondern regelmäßig in kleinen Stücken, damit das Training verstärkt und Verbesserungen gemessen werden können. Schulungen können dann in der richtigen Menge und an den richtigen Personen durchgeführt werden.

Wir bieten eine komplette End-to-End-Lösung, die die KnowBe4-Plattform nutzt, um unseren Kunden effektive Schulungen zum Thema Sicherheitsbewusstsein zu bieten. Unser Managed Service umfasst eine kontinuierliche Überwachung und Berichterstattung, die es uns ermöglicht, Bereiche zu identifizieren, in denen zusätzliche Schulungen erforderlich sein könnten und unseren Kunden zeitnahes Feedback zu geben. Unternehmen können sich dann auf ihre Kerngeschäftsaktivitäten konzentrieren, während wir ihre Anforderungen an Schulungen zum Sicherheitsbewusstsein erfüllen und sie vor Cyberbedrohungen schützen.

## Plattform zur Resilienz der Cyber-Mitarbeiter

Eine SaaS-basierte Plattform, die entwickelt wurde, um die Cyber-Resilienz eines Unternehmens kontinuierlich zu trainieren, zu bewerten und zu verbessern sowie die Widerstandsfähigkeit der Cyber-Mitarbeiter einer Organisation nachzuweisen.

**Für Einzelpersonen:** Eine ansprechende, spielerische Softwareumgebung, die das gesamte Spektrum an praxisbezogenen technischen Schulungen für Unternehmen abdeckt.

- Offensive und defensive Cyber-Profis
- Entwickler und Application Security Experten
- Fachleute für Cloud- und Infrastruktursicherheit

**Für Teams:** Die Reaktion auf Sicherheitsbedrohungen erfordert Teamarbeit von Technikern bis hin zu Führungskräften. Wir beauftragen Teams aus Ihrem gesamten Unternehmen, ihre Fähigkeiten zur Krisenentscheidung und technischen Reaktion zu verbessern, um anpassungsfähig und effektiv auf Cyberrisiken zu reagieren.

- Führungsteams
- Krisenmanagement-Teams
- Technische Cyber-Teams

**Für die Organisation:** Übungen zur Kompetenzentwicklung, die transformative Verhaltensänderungen im gesamten Unternehmen vorantreiben.

- Führungskräfte
- Mitarbeiter/-innen
- Hochrisikoziele von Cyberangriffen

Alle diese Elemente sind von überall mit einem einfachen Webbrowser zugänglich und können daher auch von Personen außerhalb der Organisation verwendet werden, z. B. im Rahmen einer Einstellungsprüfung.

Als Unternehmen sind Sie in der Lage:

- Cyberfähigkeit kontinuierlich nachzuweisen.
- Reaktionsgeschwindigkeit und -qualität zu verbessern.
- Personalbeschaffung und Karriereentwicklung zu verbessern.
- Schwachstellen in Cloud und Applikationen zu reduzieren.
- Kosten für Cybersicherheit zu reduzieren.





## Adoption & Change Management

Adoption und Change Management spielen eine entscheidende Rolle bei der Unterstützung der menschlichen Faktoren der Cybersicherheit, indem sichergestellt wird, dass Sicherheitsmaßnahmen, -richtlinien und -technologien effektiv umgesetzt und in die Kultur und Praktiken eines Unternehmens integriert werden. Menschliche Faktoren wie Benutzerverhalten, Bewusstsein und Gewohnheiten sind häufig die schwächsten Glieder der Cybersicherheit, da sie von böswilligen Akteuren ausgenutzt werden können.

### So kann Insights Adoption und Change Management bei der Bewältigung dieser menschlichen Faktoren von Nutzen sein:

**Sensibilisierung und Schulung der Mitarbeiter:** Adoption und Change Management beinhaltet die Aufklärung der Benutzer über Cybersicherheitsbedrohungen, Best Practices und die Bedeutung von Sicherheit. Durch Schulungen und klare Kommunikation werden Benutzer sich potenzieller Risiken bewusster und können fundierte Entscheidungen treffen, die die Sicherheit verbessern.

**Verhaltensänderung:** Change Management zielt darauf ab, das Nutzerverhalten im Einklang mit den gewünschten Sicherheitspraktiken zu verändern. Durch die Einführung neuer Routinen und Gewohnheiten können Benutzer dazu ermutigt werden, sicheres Verhalten anzuwenden, wie z. B. die regelmäßige Aktualisierung von Passwörtern, Vorsicht bei Phishing-E-Mails und die Meldung verdächtiger Aktivitäten.

**Kulturwandel:** Erfolgreiche Einführungs- und Change Management-Initiativen fördern eine Kultur der Sicherheit innerhalb einer Organisation. Wenn Cybersicherheit in der Unternehmenskultur verankert ist, priorisieren Mitarbeiter eher die Sicherheit in ihren täglichen Aktivitäten, was zu einer sichereren Softwareumgebung führt.

**Widerstandsreduktion:** Menschen widerstehen häufig Veränderungen, insbesondere wenn sie ihre gewohnten Routinen stören. Effektive Change Management-Strategien antizipieren diesen Widerstand und gehen darauf ein. Sie tragen dazu bei, Rückschläge gegen Sicherheitsmaßnahmen zu mindern und die reibungslosere Einführung neuer Praktiken zu erleichtern.

**Benutzerorientiertes Design:** Adoption und Change Management-Prozesse beinhalten das Verständnis der Benutzeranforderungen und die Anpassung von Sicherheitslösungen an diese Anforderungen. Dieser benutzerzentrierte Ansatz erhöht die Wahrscheinlichkeit der Akzeptanz und reduziert die Reibung bei der Einführung von Sicherheitsmaßnahmen.

**Kontinuierliche Verbesserungen:** Adoption und Change Management sind fortlaufende Prozesse, bei denen Feedback eingeholt und Strategien auf der Grundlage realer Erfahrungen angepasst werden. Dies ermöglicht es Unternehmen, ihre Sicherheitspraktiken auf sich entwickelnde Bedrohungen und Benutzeranforderungen abzustimmen.

**Kommunikationskanäle:** Eine effektive Kommunikation ist der Schlüssel zur Förderung von Vertrauen und Transparenz bei Cybersicherheitsinitiativen. Adoption und Change Management bietet Wege für einen offenen Dialog zwischen Sicherheitsteams und Benutzern und stellt sicher, dass Bedenken und Missverständnisse angesprochen und geklärt werden.

**Abwehr von Insiderbedrohungen:** Durch die Förderung eines Zugehörigkeitsgefühls und der Loyalität unter den Mitarbeitern kann Adoption und Change Management dazu beitragen, die Wahrscheinlichkeit von Insiderbedrohungen zu verringern, bei denen Mitarbeiter absichtlich oder unabsichtlich die Sicherheit gefährden.

**Rechenschaftspflicht fördern:** Change Management-Prozesse betonen die individuelle und kollektive Verantwortung für die Sicherheit. Wenn Benutzer sich für ihre Handlungen verantwortlich fühlen, halten sie sich eher an Sicherheitsprotokolle und melden potenzielle Vorfälle zeitnah.

**Anpassung an neue Technologien:** Die Cybersicherheit entwickelt sich rasant weiter und es entstehen häufig neue Technologien. Adoption und Change Management helfen Benutzern, sich an diese Veränderungen anzupassen, indem sie Schulungen und Support anbieten und sicherstellen, dass neue Technologien von Anfang an sicher verwendet werden.

## Fazit

Menschen stellen das größte Sicherheitsrisiko für ein Unternehmen dar und müssen regelmäßig und effektiv geschult werden, um aktive Sicherheitshüter eines Unternehmens zu werden. Eine gut ausgebildete Person kann die letzte Verteidigungslinie gegen eine Sicherheitsverletzung sein, die Ihren technischen und prozessbasierten Kontrollen entgangen ist.

Die traditionelle jährliche Schulung zum Sicherheitsbewusstsein ist etwas, auf das sich kaum ein Mitarbeiter freut. Nicht verwunderlich in Anbetracht der geringen Mühe die Unternehmen in die Benutzerfreundlichkeit derartiger Schulungen investieren - ein trockenes Video und eine handvoll Quizfragen. So haben die meisten Mitarbeiter analog eine eher geringe Einstellung zum Thema Sicherheit. Unsere Empfehlung: Berücksichtigen Sie einige der bewährten Verfahren bei der Festlegung der menschlichen Faktoren in Ihrer Sicherheitsstrategie.



### Schulungsmethoden und -techniken:

- Nutzen Sie Gamification und Wettbewerb, um die Motivation des Einzelnen zur Teilnahme zu steigern.
- Schulungsmaßnahmen sollten regelmäßig und kurz sein – denken Sie an 10 Minuten pro Woche anstatt an eine Stunde pro Jahr für eine allgemeine Sicherheitsbewusstseinschulung.
- Verwenden Sie Tests, um auf organisatorischer Ebene sicherzustellen, dass Ihre Reifeziele erreicht werden und um den Teilnehmern ein sofortiges Feedback zu geben, dass sie den Inhalt verstanden haben.
- Erwägen Sie sowohl zielgerichtetes individuelles Enablement, das sich auf technische Fähigkeiten konzentriert, als auch teambasierte Übungen, um Prozesse und Teamarbeitsfähigkeiten zu testen.

### Kommunikation und Engagement:

- Genauso wichtig wie der Inhalt ist es, mit Menschen in ihrer Landessprache und im richtigen Tonfall zu sprechen.

### Störfallmanagement:

- Ein robuster, stressgetesteter Incident-Management-Prozess kann den Unterschied zwischen einem „run-of-the-mill“-Sicherheitsereignis und einem geschäftskritischen Incident ausmachen.

### Inklusivität im Sicherheitsbewusstsein:

- Ihre Strategie sollte alle Personas berücksichtigen, vom gelegentlichen IT-Benutzer bis hin zum technischsten Sicherheitsadministrator in Ihrem Unternehmen. Sie alle spielen eine Rolle bei der Aufrechterhaltung der Sicherheit

Der menschliche Aspekt der Sicherheitsstrategie eines Unternehmens ist nicht nur eine Formalität, sondern ein wesentlicher Faktor, der den Unterschied zwischen Sicherheit und Gefährdung ausmachen kann. Wie wir gezeigt haben, ist es von entscheidender Bedeutung, einen umfassenden Ansatz zu entwickeln, der die Bedeutung des menschlichen Elements anerkennt - vom Einsatz moderner Schulungsmethoden bis hin zur Gewährleistung von Vielfalt des menschlichen Elements. Indem wir uns auf kontinuierliches Lernen, effektive Kommunikation, ein starkes Vorfallsmanagement und die Einbeziehung aller Rollen innerhalb eines Unternehmens konzentrieren, schaffen wir die Grundlage für eine widerstandsfähige Sicherheitslage. Da sich Technologien ändern und Bedrohungen immer fortschrittlicher werden, ist es der gut ausgebildete, bewusste und engagierte Einzelne, der zuverlässig eine starke Barriere gegen mögliche Verstöße bilden wird. Adoption und Change Management stellen sicher, dass Sicherheitsmaßnahmen, Richtlinien und Technologien nahtlos in die Kultur und die täglichen Praktiken eines Unternehmens integriert werden. Es verändert die Perspektive von der einfachen Sensibilisierung zu einer praktischen Verhaltensänderung und schafft eine proaktive Sicherheitskultur. Dieser Wandel führt zu weniger Widerstand, fördert die kontinuierliche Verbesserung und stärkt das Verantwortungsbewusstsein der Mitarbeiter. Da sich die Cybersicherheitslandschaft verändert, ist es entscheidend, mit neuen Technologien Schritt zu halten. Change Management sorgt dafür, dass Unternehmen sich nicht nur anpassen, sondern inmitten dieser Veränderungen durch den sicheren und effektiven Einsatz neuer Tools florieren.

## Nächste Schritte

Durch das Verständnis Ihres Unternehmensrisikos, die Auswahl der richtigen Technologien und Plattformen für die Lernreise und deren Integration in Ihre Geschäftsprozesse kann Insight Ihnen helfen, eine konsistente Strategie für menschliche Faktoren in der Cybersicherheit zu entwickeln und umzusetzen. Wir können auch die Einführung verfolgen und verbessern, wenn diese voranschreitet.

Wenden Sie sich für weitere Informationen an unsere Sicherheitsberater oder Experten für Adoption und Change Management.