Microsoft Security

Data Security Index

Trends, Insights und Strategien für den Schutz Ihrer Daten und den Umgang mit generativer KI

Bericht 2024

Vorwort

Im zweiten Jahr unserer Untersuchung zu der sich ständig verändernden Datensicherheitslandschaft sind die Herausforderungen und Chancen, die vor uns liegen, komplexer denn je. Im vergangenen Jahr hat der Schweregrad von Datensicherheitsvorfällen zugenommen. In diesem datenzentrierten Zeitalter entwickeln sich die Strategien und Tools, die zum Schutz von Daten verwendet werden, rasant weiter.

In diesem Jahr erforschen wir neue Grenzen: die Rolle und die Auswirkungen von generativer KI (KI) auf Datensicherheitsstrategien.

KI sorgt mit beispiellosen Möglichkeiten weltweit für mehr Innovation und Effizienz. Trotz dieses enormen Potenzials beschäftigen Unternehmen sich jedoch auch mit Datensicherheitsrisiken und deren möglichen Auswirkungen auf die Verantwortlichkeiten für Datensicherheitsteams. KI ist ein Katalysator für Unternehmen zur Stärkung ihrer grundlegenden Datensicherheitspraktiken, sodass sie sich darauf vorbereiten können, die Auswirkungen von übermäßiger Datenfreigabe und Datenlecks zu minimieren und Prozesse für eine sichere KI-Einführung zu schaffen. Andererseits kann KI Unternehmen auch bei der Verbesserung ihrer Datensicherheitspraktiken unterstützen, indem sie versteckte Risiken und Lücken im Schutz identifiziert, Schutzrichtlinien empfiehlt und dazu beiträgt, Sicherheitsvorfälle schneller zu untersuchen und zu beheben.

Das Ziel unserer Untersuchung ist es, Datensicherheitsverantwortlichen praktische Insights und Tipps zu liefern, damit sie ihre Teams dabei unterstützen können, ihre Datensicherheitsstrategie auf sichere Weise anzupassen, um die KI-Nutzung effektiv zu schützen, und KI in ihre Datensicherheitsstrategien zu integrieren. Die Reichweite und das Potenzial von KI sind beeindruckend, und doch steht sie lediglich für die jüngste transformative Welle in Unternehmen. Denn ähnlich wie hybrides Arbeiten, die Cloud und die zunehmende Mobilität, die die letzten Jahre geprägt haben, zeigt sich durch KI eine zeitlose Notwendigkeit: Die Umsetzung dieser Initiativen muss mit hoher Transparenz erfolgen, um Risiken zu minimieren und einen maximalen Nutzen zu erzielen. Auf der Basis dieser Erkenntnisse sorgt eine ordnungsgemäße Absicherung der in KI verwendeten Daten sowie der Einsatz von KI zur Verbesserung von Datensicherheitsmaßnahmen für eine höhere Produktivität, Resilienz und Agilität, wenn Teams zukünftige Herausforderungen bewältigen.

Wir laden Sie ein, sich die neuesten Ergebnisse anzusehen, und hoffen, dass die Insights Ihnen bei der Verbesserung Ihres Datensicherheitsstatus helfen und Sie dazu inspirieren, KI zu nutzen und eine umfassende Datensicherheitsstrategie zu gestalten, die für mehr Innovationen sorgt und eine sicherere Zukunft für uns alle gewährleistet.

Rudra Mitra
Corporate Vice President
Microsoft Data Security and Compliance

Einführung

Unternehmen erleben im Durchschnitt 156 Datensicherheitsvorfälle pro Jahr. Die Auswirkungen dieser Vorfälle bedeuten für Entscheidungstragende im Bereich Datensicherheit eine ständige Sorge. Dafür gibt es einen guten Grund: Ein einziger Vorfall kann massive finanzielle Folgen sowie Reputationsschäden verursachen, insbesondere in einer sich ständig weiterentwickelnden Bedrohungslandschaft, in der Angreifende alle möglichen Schwachstellen ausnutzen. Dies wird durch die schnelle Einführung von KI noch verstärkt, da Benutzende ohne angemessene Schutz- und Sicherheitsmaßnahmen versehentlich oder in böswilliger Absicht sensible geschäftskritische Daten (darunter Mitarbeiter- und Kundeninformationen, geistiges Eigentum, Finanzprognosen und Betriebsdaten) gefährden können. Auf der Suche nach neuen Möglichkeiten, diese Vielzahl von sensiblen Daten zu schützen, haben viele Entscheidungstragende ihre Aufmerksamkeit auf den immensen Vormarsch von KI gerichtet.

KI stellt eine doppelte Herausforderung dar. Zwei Drittel der Unternehmen geben zu, dass ihre Mitarbeitenden nicht autorisierte KI-Tools verwenden. Deshalb müssen sie sicherstellen, dass die Mitarbeitenden KI-Tools auf sichere Weise verwenden. Gleichzeitig besteht die Möglichkeit, in einer anspruchsvollen Datensicherheitsstrategie KI auch als effektives Tool einzusetzen.

KI-gestützte Datensicherheitslösungen spielen bereits eine entscheidende Rolle bei der Erkennung und Reaktion auf Bedrohungen in Echtzeit, der Verbesserung der Gesamtgeschwindigkeit und Genauigkeit von Datensicherheitsprogrammen und der Bereitstellung von Insights, die Datenschutzvorfälle verhindern, bevor sie auftreten. Unternehmen müssen die Risiken bewältigen, die KI mit sich bringt. Sie müssen ihr Potenzial nutzen, Muster zu erkennen, deren Verarbeitung und Analyse mit Maschinengeschwindigkeit für Menschen eine Herausforderung darstellen kann. Und sie müssen immer komplexere Cyberangriffe abwehren.

Im Jahr 2023 beauftragte Microsoft das unabhängige Forschungsinstitut Hypothesis mit der Durchführung einer internationalen Umfrage unter mehr als 800 Datensicherheitsfachkräften und startete eine Data Security Index-Initiative, um unsere Zusammenarbeit mit Partner- und Kundenunternehmen zu verbessern und Führungskräfte bei der Entwicklung ihrer eigenen Datensicherheitsstrategien zu unterstützen.

Der Bericht des Jahres 2024 baut auf der vorherigen Untersuchung auf und liefert neue Insights aus einer erweiterten internationalen Umfrage unter mehr als 1.300 Datensicherheitsfachkräften. Während die Daten konsistente Insights liefern und Trends in den von uns befragten Märkten aufzeigen, decken wir neue Erkenntnisse rund um die aktuellen weltweiten Datensicherheits- und KI-Praktiken und -Trends auf.

hypothesis Microsoft Security

Die wichtigsten Erkenntnisse

1

Die Datensicherheitslandschaft ist nach wie vor fragmentiert, was die Notwendigkeit kohärenter Datensicherheitsstrategien für herkömmliche und neue Risiken im Zusammenhang mit der KI-Nutzung erhöht.

Unternehmen berichten von einem hohen Maß an Zufriedenheit und Vertrauen in ihre Datensicherheitsmaßnahmen. Der Schweregrad von Datensicherheitsvorfällen nimmt jedoch weiter zu, insbesondere aufgrund von Lücken, die Unternehmen zwischen ihren aktuellen Datensicherheitsrichtlinien und der zunehmenden Nutzung/Einführung von KI-Anwendungen feststellen. Angesichts dieser Herausforderungen und Notwendigkeiten verlassen sich viele Unternehmen immer noch auf mehrere Datensicherheitstools, was ihre Anfälligkeit und ihr Risiko insgesamt erhöhen kann.

2

Da Endbenutzende zunehmend KI-Apps verwenden, ist die Integrität der sensibelsten Daten von Unternehmen immer stärker gefährdet, sodass mehr Transparenz und neue Schutzkontrollen erforderlich sind.

KI-Tools sind bei der täglichen Arbeit unverzichtbar geworden, was Unternehmen Sorgen in Bezug auf Datensicherheitsrisiken bereitet. Sie wissen, dass sie ihre Abwehrmaßnahmen verstärken müssen, und sind bestrebt, durch KI verursachte Datensicherheitsvorfälle zu verhindern. Die unbefugte Nutzung dieser Tools unterstreicht jedoch die Notwendigkeit, die Transparenz zu maximieren.

3

Entscheidungstragende sind optimistisch bezüglich des Potenzials von KI, ihre Datensicherheitsmaßnahmen zu unterstützen

Unternehmen investieren aktiv in Datensicherheitstools, die KI integrieren, um die Erkennungs- und Reaktionsfunktionen zu verbessern. KI kann helfen, ungeschützte Daten zu erkennen, Schutzrichtlinien zu empfehlen und Datensicherheitsvorfälle schneller zu untersuchen und zu beheben, sodass Datensicherheitsteams wertvolle Arbeitszeit einsparen und sich so besser auf strategische Aufgaben konzentrieren können. Der Einsatz von KI stärkt zudem das Vertrauen in und die Zufriedenheit mit der allgemeinen Datensicherheitsstrategie von Unternehmen – insbesondere ihre Fähigkeit, schnell und präzise auf Vorfälle zu reagieren.

1

Die Datensicherheitslandschaft ist nach wie vor fragmentiert, was die Notwendigkeit kohärenter Datensicherheitsstrategien für herkömmliche und neue Risiken im Zusammenhang mit der KI-Nutzung erhöht.

Es besteht eine Diskrepanz zwischen dem Vertrauen der Entscheidungstragenden in ihre Datensicherheitspraktiken und dem tatsächlichen Schutzniveau für ihre Daten

Laut dem Bericht von 2023 ist die überwiegende Mehrheit der Entscheidungstragenden von ihren Datensicherheitsstrategien überzeugt, und 2024 gaben 74 % an, dass sie mit ihren aktuellen Lösungen zufrieden sind. Sie fühlen sich sicher, wenn es darum geht, sensible Daten nachzuverfolgen und zu verwalten: 88 % glauben, dass sie wissen, wo sich die meisten ihrer kritischen Informationen befinden, und 85 % sagen, dass ihre Daten ordnungsgemäß klassifiziert und gekennzeichnet wurden. Die meisten vertrauen ihren Sicherheitskontrollen, wobei 79 % überzeugt sind, dass sie die Exfiltration von Daten verhindern können. 76 % beschreiben ihren Ansatz als proaktiv statt reaktiv.

Ihre Zuversicht wird jedoch auf die Probe gestellt, da der Schweregrad von Vorfällen stetig zunimmt. **Die durchschnittliche Anzahl der jährlichen Datensicherheitsvorfälle ist mit 166 im Jahr 2023 und 156 im Jahr 2024 hoch geblieben, und der Schweregrad dieser Vorfälle ist ebenfalls gestiegen, von 20 % auf 27 %.**

156

Datensicherheitsvorfälle

27 %

der Vorfälle wurden als schwerwiegend eingestuft
(Steigerung von 20 % gegenüber 2023)

63 %

der Warnungen werden pro Tag überprüft

„Der Ort, an dem eine Softwareplattform bereitgestellt wurde, wo die Daten gespeichert werden und wer auf diese Daten zugreift, hat die Datensicherheit und die Verwaltung unserer KI-Tools und Anbieter erheblich verkompliziert. Wir verfügen über Daten aus mehr als 100 Jahren, die wir schützen und entsprechend den gesetzlichen Anforderungen in jedem Land, in dem wir tätig sind, verwalten müssen“, so der Senior Manager für Information Governance bei einem Schwermaschinenhersteller.

Die Zunahme des Schweregrads von Datensicherheitsvorfällen hat zu einem Anstieg der Anzahl von Warnungen geführt. **Unternehmen sind mit durchschnittlich 66 Warnmeldungen pro Tag konfrontiert, gegenüber 52 im Jahr 2023.** Diese Zahl variiert je nach Unternehmensgröße erheblich, wobei mittelgroße Unternehmen (500–999 Mitarbeitende) und große Unternehmen (1.000–4.999 Mitarbeitende) durchschnittlich 56 Warnungen und sehr große Unternehmen (über 5.000 Mitarbeitende) durchschnittlich 80 Warnungen pro Tag erhalten.

Angesichts der schieren Menge an Datensicherheitswarnungen überrascht es nicht, dass die meisten Unternehmen einfach nicht Schritt halten können. Im Durchschnitt überprüfen Datensicherheitsteams 63 % ihrer täglichen Warnungen. 35 % dieser Warnungen erweisen sich als falsch positiv. Dieses Missverhältnis zwischen vermeintlicher Kontrolle und operativer Realität überfordert Datensicherheitsteams. Sie versuchen zu beurteilen, ob sie über die richtigen Schutzmaßnahmen verfügen oder wie sie diese verfeinern können, und befürchten gleichzeitig, dass potenziell schwerwiegende Vorfälle übersehen werden könnten.

Um herkömmliche und neu aufkommende Datenrisiken im Zusammenhang mit der Nutzung von KI-Tools zu bewältigen, besteht ein wachsender Bedarf an robusteren und kohärenteren Datensicherheitsstrategien

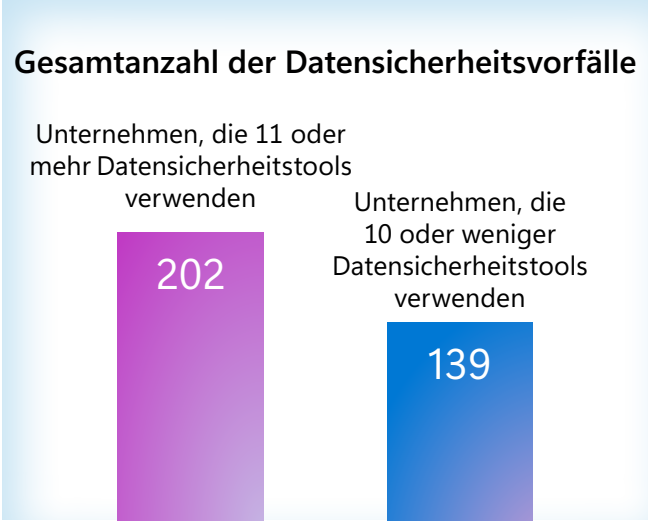
Trotz der wachsenden Anzahl von Tools, die ihnen zur Verfügung stehen, geben viele Entscheidungstragende weiterhin offen zu, dass mehr nicht immer besser ist. So nennen 21 % den Mangel an konsolidierter und umfassender Transparenz (und den Mangel an einem gemeinsamen Verständnis der Risiken), der durch unterschiedliche Tools verursacht wird, als ihre größte Herausforderung/ihr größtes Risiko.[1]

Die meisten Entscheidungstragenden (82 %) sind sich einig, dass eine umfassende, vollständig integrierte Plattform der Verwaltung mehrerer isolierter Tools vorzuziehen ist. **Im Durchschnitt müssen sie mit 12 verschiedenen Datensicherheitslösungen jonglieren. Dies führt zu Komplexität, die ihre Anfälligkeit erhöht.** Dies gilt insbesondere für die größten Unternehmen: Im Durchschnitt verwenden mittelgroße Unternehmen 9 Tools, große Unternehmen 11 und sehr große Unternehmen 14.

Die Daten zeigen eine starke Korrelation zwischen der Anzahl der verwendeten Datensicherheitstools und der Häufigkeit von Datensicherheitsvorfällen. Mittelgroße und große Unternehmen melden durchschnittlich 89 Vorfälle pro Jahr, während sehr große Unternehmen sogar mit 248 Vorfällen pro Jahr konfrontiert sind. Dieser enorme Unterschied verdeutlicht das hohe Risiko, dem größere Unternehmen ausgesetzt sind, auch wenn sie ein beträchtliches Vertrauen in ihre Datensicherheitsmaßnahmen äußern.

Im Jahr 2024 verzeichneten Unternehmen, die mehr Datensicherheitstools einsetzen (11 oder mehr), durchschnittlich 202 Daten-sicherheitsvorfälle, verglichen mit 139 Vorfällen bei Unternehmen mit 10 oder weniger Tools.

1. Umfrage zur Datensicherheit vom September 2024, Entscheidungstragende aus den Bereichen Governance, Compliance und Datenschutz, von Microsoft bei der Agentur MDC Research in Auftrag gegeben



Fragmentierte Lösungen erschweren das Verständnis des Datensicherheitsstatus, da Daten isoliert sind und verteilte Workflows den umfassenden Einblick in potenzielle Risiken einschränken können. Wenn Tools nicht integriert sind, müssen Datensicherheitsteams Prozesse entwickeln, um Daten zu korrelieren und eine zusammenhängende Übersicht über Risiken zu erstellen. Dies kann zu blinden Flecken führen und es schwierig machen, Risiken effektiv zu erkennen und zu minimieren.

Zunehmend Anlass zur Sorge gibt der Anstieg von Datensicherheitsvorfällen durch die Nutzung von KI-Anwendungen, die sich von 27 % im Jahr 2023 auf 40 % im Jahr 2024 fast verdoppelt haben. Dieser Anstieg der Vorfälle wird durch die Zunahme der Malware- und Ransomware-Angriffe von 50 % im Jahr 2023 auf 59 % verstärkt. Angriffe durch die Nutzung von KI-Apps legen nicht nur sensible Daten offen, sondern gefährden auch die Funktionalität der KI-Systeme selbst, was die ohnehin schon fragmentierte Datensicherheitslandschaft noch komplizierter macht. Kurz gesagt, es besteht ein immer dringenderer Bedarf an robusteren, kohärenteren Datensicherheitsstrategien, die sowohl herkömmliche als auch neu auftretende Risiken im Zusammenhang mit der Nutzung von KI-Tools bewältigen können.

Der Weg in die Zukunft

Der zunehmende Schweregrad von Datensicherheitsvorfällen zeigt eine Chance auf, wie KI helfen kann. Unternehmen, die auf dem neuesten Stand sind, implementieren KI-gestützte Datensicherheit, um die Priorisierung von Vorfällen zu unterstützen, die Datenklassifizierung zu automatisieren und Möglichkeiten zur Feinabstimmung aktueller Schutzrichtlinien zu ermitteln. KI kann automatisch den potenziellen Schweregrad von Vorfallwarnungen synthetisieren und Datensicherheitsteams verwertbare Insights für eine schnelle Reaktion liefern, um den Zeitaufwand bei Fehlalarmen zu reduzieren. Dies optimiert Workflows und ermöglicht es Datensicherheitsteams, sich stärker auf strategische Verbesserungen der Datensicherheit und proaktive Maßnahmen zu konzentrieren.

2

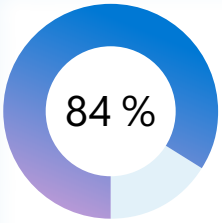
Da Endbenutzende zunehmend KI-Apps verwenden, ist die Integrität der sensibelsten Daten von Unternehmen immer stärker gefährdet, sodass mehr Transparenz und neue Schutzkontrollen erforderlich sind.

KI gewinnt bei der täglichen Arbeit eine immer größere Bedeutung – und Unternehmen müssen diese neue Realität akzeptieren und sich aktiv daran anpassen

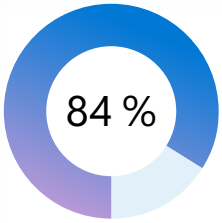
Die schnelle Einführung von KI-Tools durch die Mitarbeitenden hat zu erheblichen Veränderungen in der Herangehensweise von Unternehmen an die Datensicherheit geführt. Während KI Produktivität und Workflows transformiert, kann sie – wie jede neue Technologie – auch bestehende Risiken verstärken oder neue mit sich bringen, die einen anderen Ansatz zum Schutz sensibler Informationen erfordern. Daher haben Unternehmen immer noch damit zu kämpfen, in einer sich schnell verändernden Landschaft ihren Platz zu finden. Eine Fachkraft im Bereich Engineering und Analytics im Transportwesen sagt: „Wir überwachen Daten auf der KI-Ebene sorgfältiger. Es besteht ein Spannungsverhältnis zwischen Produktivität und Sicherheit, Präzision und Datenschutz."

Das Vertrauen in die Absicherung der KI-Nutzung durch die Mitarbeitenden ist nach wie vor durchwachsen. Die Mehrheit (84 %) wünscht sich mehr Sicherheit bei der Verwaltung und Ermittlung von Dateneingaben. Während 22 % der Unternehmen äußerst zuversichtlich sind, dass sie ihre Daten schützen können, sind die meisten (59 %) nur „sehr zuversichtlich", was darauf hindeutet, dass hier Verbesserungspotenzial besteht. Die meisten Unternehmen (86 %) geben an, dass sie bezüglich der Verwaltung und Ermittlung von Daten, die von KI-Tools generiert wurden, gerne optimistischer wären.

Während KI für die tägliche Produktivität immer wichtiger wird, hat die Nutzung von KI-Apps auch die Besorgnis in Bezug auf Datensicherheitsvorfälle verstärkt. **Fast ein Drittel (31 %) der Unternehmen rechnet mit einer Zunahme von Datensicherheitsvorfällen aufgrund der KI-Nutzung durch Mitarbeitende. 84 % räumen ein, dass sie mehr tun müssen, um sich vor diesen Risiken zu schützen.** Diese Ängste sind bei den größten Unternehmen besonders groß: Während 26 % der mittelgroßen Unternehmen eine Zunahme von KI-bezogenen Datensicherheitsvorfällen erwarten und 29 % der großen Unternehmen, rechnen 36 % der sehr großen Unternehmen, also eine deutlich größere Gruppe, mit einem Anstieg.



wünschen mehr Sicherheit bei der Verwaltung und Ermittlung von Dateneingaben in KI-Apps und -Tools



stimmen zu, dass sie mehr tun müssen, um sich vor riskanter Nutzung von KI-Apps und -Tools durch Mitarbeitende zu schützen

Die unbefugte Nutzung von KI ist weit verbreitet

40 % geben an, dass ihre KI-Apps bereits bei einem Datensicherheitsvorfall angegriffen oder kompromittiert wurden. Bei größeren Unternehmen ist diese Zahl erneut höher: Mittelgroße Unternehmen berichten von einer Vorfallrate von 36 %, große Unternehmen berichten von 38 % und sehr große Unternehmen verzeichneten mit 44 % die meisten Vorfälle.

Eine nicht autorisierte Nutzung von KI tritt häufig auf, wenn sich Mitarbeitende mit persönlichen Zugangsdaten anmelden oder private Geräte für arbeitsbezogene Aufgaben verwenden. **Im Durchschnitt geben 65 % der Unternehmen zu, dass ihre Mitarbeitenden nicht autorisierte KI-Tools nutzen.** Wie Mitarbeitende nicht autorisierte KI-Tools verwenden:

- 53 % melden sich mit ihren persönlichen Zugangsdaten für berufliche Zwecke an.
- 48 % verwenden ihr privates Gerät, wenn sie KI für die Arbeit nutzen.
- 47 % verwenden ihre geschäftlichen Zugangsdaten, um KI für persönliche Zwecke zu nutzen.

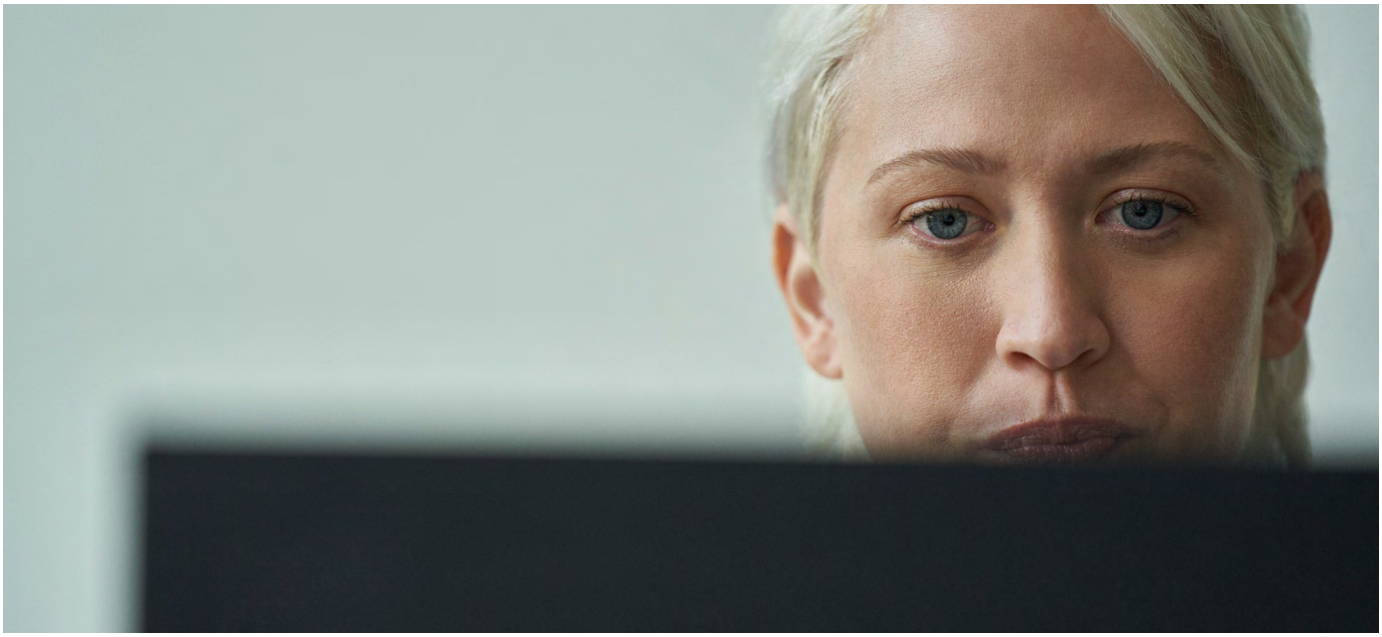
Die Hälfte aller Unternehmen gibt an, dass sie besorgt sind über fehlende Kontrollen zur Erkennung und Minimierung von Risiken, wenn Mitarbeitende KI-Apps auf eine nicht sichere Weise verwenden. Diese Zahl variiert je nach Unternehmensgröße, wobei 43 % der mittelgroßen, 50 % der großen und 54 % der sehr großen Unternehmen Bedenken hinsichtlich ihrer Fähigkeit äußern, diese Risiken zu bewältigen.

Angesichts des zunehmenden Einsatzes von KI sind mehr Datensicherheitskontrollen erforderlich

KI wird immer stärker in die täglichen Betriebsabläufe integriert, und Unternehmen erkennen die Notwendigkeit für einen besseren Schutz. **Während 96 % der Unternehmen Bedenken hinsichtlich der Nutzung dieser Tools durch ihre Mitarbeitenden haben, sind fast ebenso viele bereit, in Lösungen zu investieren, um ihre Bedenken auszuräumen.**

„Besonderes Gewicht hat die Frage: Wie können Sie KI einen Schritt voraus sein? Der Sicherheitsfokus liegt auf der Reduzierung der Datengröße und einer sorgfältigeren Überwachung der Daten. Auf KI-Ebene benötigen Sie mehr Daten, um Ihre Modelle repräsentativer zu machen und Verzerrungen zu identifizieren. Wie bringen Sie das alles in Einklang?“, so eine leitende Fachkraft im Bereich Engineering, Architecture und Analytics im Transportwesen. Die überwiegende Mehrheit der Entscheidungstragenden (87 %) ist bereit, sowohl Zeit als auch Geld in das Training von Mitarbeitenden zu sicheren Praktiken für die Nutzung von KI-Tools zu investieren. **Denn 85 % sagen, dass die Verwendung dieser Tools durch Mitarbeitende von entscheidender Bedeutung ist, um wettbewerbsfähig zu bleiben.**

Fast alle Unternehmen (93 %) haben bereits mit der Entwicklung oder Implementierung von Kontrollen für die KI-Nutzung begonnen, aber viele befinden sich noch in einer frühen Phase. Nur 39 % haben die Implementierung von Datensicherheitskontrollen für KI vollständig abgeschlossen, während 24 % Richtlinien ausgearbeitet, diese aber noch nicht umgesetzt haben. Ein VP für Datensicherheit im Gastgewerbe erklärt: „Wir müssen uns über Kontrollen für KI abstimmen, beginnen aber in der Zwischenzeit mit der Nutzung von KI. Sie erleichtert den Alltag und hilft uns, effizienter zu arbeiten.“



Während Unternehmen Maßnahmen ergreifen, um sensible Daten vor Missbrauch in KI-Apps zu schützen, besteht ein eindeutiger Bedarf an umfassenderen Kontrollen. Derzeit konzentrieren sich 43 % der Unternehmen darauf, das Hochladen sensibler Daten in KI-Apps zu verhindern, während weitere 42 % alle Aktivitäten und Inhalte innerhalb dieser Apps für potenzielle Untersuchungen oder Reaktionen auf Vorfälle protokollieren. Ebenso blockieren 42 % den Benutzerzugriff auf nicht autorisierte Tools, und der gleiche Prozentsatz investiert in Mitarbeitertrainings zum sicheren Umgang mit KI.

Unternehmen mit Mitarbeitenden, die KI auf nicht autorisierte Weise nutzen, haben einen höheren Bedarf an bestimmten Arten von Kontrollen. **Von denjenigen mit nicht autorisierter KI-Nutzung benötigen 42 % Kontrollen, um riskante Benutzende basierend auf KI-Abfragen zu identifizieren, verglichen mit 30 % bei denjenigen ohne unbefugte Nutzung. Darüber hinaus benötigen 40 % der Unternehmen, die mit einer nicht autorisierten KI-Nutzung zu kämpfen haben, Kontrollen, um den Lebenszyklus von Daten zu verwalten (z. B. Aufbewahrungs- und Löschprotokolle), verglichen mit 27 % der Unternehmen, die dieses Problem nicht haben.**

Die 5 wichtigsten erforderlichen KI-Kontrollen

Hochladen sensibler Daten in die KI verhindern	43 %
Alle Aktivitäten und Inhalte für potenzielle Untersuchungen oder Reaktionen auf Vorfälle in KI-Tools protokollieren	42 %
Benutzerzugriff auf nicht autorisierte KI-Tools blockieren	42 %
Mitarbeitende im sicheren Umgang mit KI-Tools trainieren	42 %
Riskante Benutzende basierend auf KI-Abfragen identifizieren	41 %

Der Weg in die Zukunft

Um ein hohes Datensicherheitsniveau aufrechtzuerhalten, benötigen Teams einen umfassenden Satz an Kontrollen, um ihre Daten in KI-Apps zu ermitteln, zu schützen und zu verwalten. Hier sind drei wichtige Strategien, die Teams anwenden können:

Erhöhen der Transparenz der Nutzung von KI-Apps und der Daten, die diese Apps verwenden: Nutzen Sie Datensicherheitstools, die KI-Apps erkennen und verwenden können. Diese Tools bieten Einblick in eine umfassende Liste der verwendeten KI-Apps zusammen mit ihren Risikoprofilen, einschließlich Details wie unterstützte Datensicherheits-kontrollen und die Einhaltung von Vorschriften. Verwenden Sie Tools, die eine konsistente Klassifizierung sensibler Daten in KI-Interaktionen ermöglichen, und zeigen Sie Trends rund um den Datenfluss durch KI-Apps auf.

Entwickeln und Durchsetzen von Richtlinien: Erstellen Sie Richtlinien basierend auf den aus der Analyse gewonnenen Insights. Diese Richtlinien können Richtlinien für genehmigte KI-Apps und Verfahren zum Blockieren oder Einschränken der Nutzung nicht genehmigter Apps durch Mitarbeitende umfassen. Selbst in genehmigten KI-Apps können Sie granulare Richtlinien erstellen, die den Fluss nicht sensibler Daten zulassen und gleichzeitig die Verwendung sensibler und geschäftskritischer Daten einschränken. Dies kann das Blockieren bestimmter Aktionen umfassen, z. B. das Einfügen sensibler Daten in browserbasierte KI-Tools, um Datensicherheit zu gewährleisten.

Regelmäßiges Bewerten von Risiken und Anpassen von Richtlinien: Erstellen Sie regelmäßig Berichte, die die Risikostufen der verwendeten KI-Apps, Trends bei der Nutzung sensibler Daten durch diese Apps sowie Benutzeraktivitäten rund um die Apps zeigen. Dies hilft Ihnen dabei, die allgemeine Risikolandschaft einzuschätzen und fundierte Entscheidungen über die relevantesten Datensicherheitsrichtlinien zu treffen.

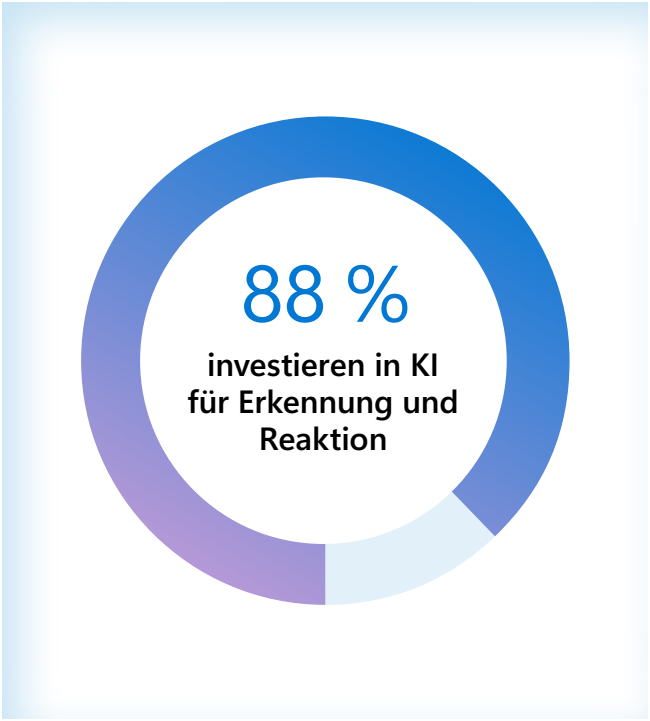
3

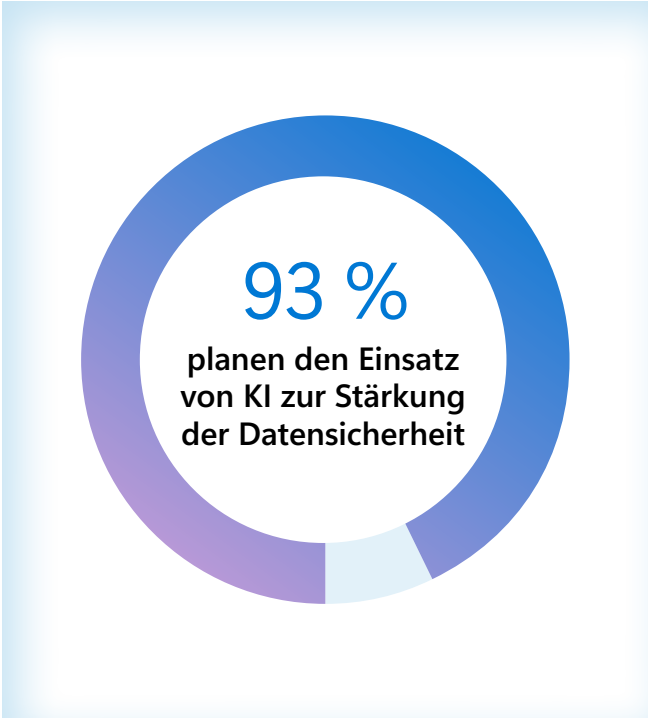
Entscheidungstragende sind optimistisch bezüglich des Potenzials von KI, ihre Datensicherheitsmaßnahmen zu unterstützen

Untersuchungen zur Daten-sicherheit stützen sich in hohem Maße auf KI

Die überwiegende Mehrheit (88 %) der Unternehmen investiert bereits in KI, um ihre Erkennungs- und Reaktionsmaßnahmen zu verbessern – die Ermittlung sensibler Daten, die Erkennung anomaler Aktivitäten und der automatische Schutz gefährdeter Daten. **77 % der Unternehmen glauben, dass KI diese Prozesse beschleunigen wird, und 76 % denken, dass sie die Genauigkeit ihrer Erkennungs- und Reaktionsstrategien verbessern wird.**

Während 73 % der Entscheidungstragenden Bedenken hinsichtlich des Einsatzes von KI zur Stärkung der Datensicherheit äußern, geben 50 % an, dass dies ihre Nutzung von KI zur Stärkung der Datensicherheit nicht beeinträchtigt hat, und nur 23 % sagen, dass dies sie zurückgehalten hat. Insgesamt planen überwältigende 93 % zumindest, KI zur Stärkung der Datensicherheit einzusetzen, auch wenn sie Bedenken haben.



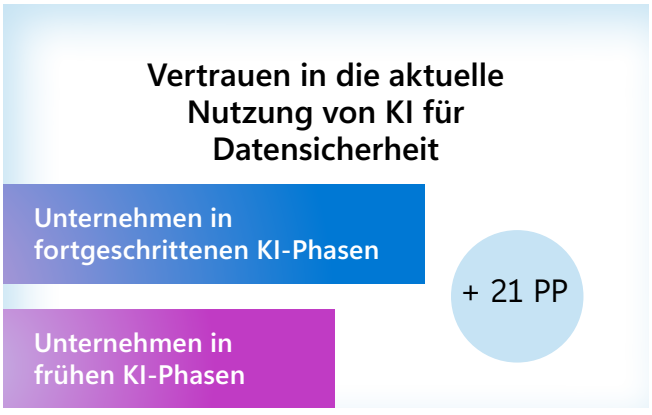


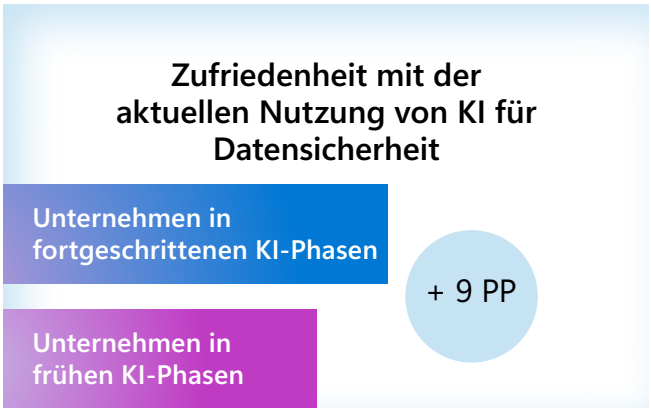
Die Nutzung von KI zur Stärkung der Datensicherheit steigert die Transparenz, das Vertrauen und die Zufriedenheit

Einer der Hauptvorteile der Nutzung von KI zur Stärkung der Datensicherheit ist ihre Fähigkeit, die Transparenz für alle Systeme zu erhöhen. Damit wird die Sorge von Entscheidungstragenden in Bezug auf den Speicherort und die Klassifizierung von Daten (20 %) abgemildert.[1] 88 % der Entscheidungstragenden im Bereich Datensicherheit glauben, dass die Integration von KI in Datensicherheitslösungen ihren Teams mehr Transparenz verschafft, sodass Unternehmen weitaus mehr Daten verarbeiten und analysieren können, als es sonst möglich wäre. Mittelgroße Unternehmen konzentrieren sich in erster Linie auf die Reduzierung kurzfristiger Risiken, beispielsweise die Minimierung menschlicher Fehler in ihren Datensicherheitsprozessen. Tatsächlich räumen 43 % der mittelgroßen Unternehmen der Reduzierung von Risiken, die durch menschliche Fehler entstehen, Priorität ein, verglichen mit nur 37 % der sehr großen Unternehmen.

Im Gegensatz dazu sind größere Unternehmen in ihrem Ansatz fortschrittlicher und legen den Schwerpunkt auf langfristige Risiken und die Notwendigkeit von Anpassungsfähigkeit. Dieser höhere Grad an Ausgereiftheit ermöglicht es Datensicherheitsteams, sich besser an neue Risiken anzupassen. Dies hat für 49 % der sehr großen Unternehmen oberste Priorität, verglichen mit 43 % der mittelgroßen Unternehmen.

Insgesamt berichten Unternehmen, die in ihrer Nutzung von KI zur Stärkung der Datensicherheit bereits weiter fortgeschritten sind, von einem wesentlich höheren Maß an Vertrauen und Zufriedenheit mit ihren Datensicherheitsstrategien. **90 % der Befragten, die sich in fortgeschrittenen Phasen der KI-Implementierung befinden, sind äußerst oder sehr zuversichtlich bezüglich ihrer Nutzung von KI zur Stärkung der Datensicherheit, verglichen mit 69 % in früheren Phasen. In ähnlicher Weise zeigen sich 76 % der Unternehmen mit fortgeschrittener KI-Nutzung zufrieden mit ihren Datensicherheitslösungen, während nur 67 % der Unternehmen in früheren Phasen dies ebenfalls berichten.**





1. Umfrage vom September 2024 unter Entscheidungstragenden in den Bereichen Datensicherheit, Governance, Compliance und Datenschutz, die im Auftrag von Microsoft von der Agentur MDC Research durchgeführt wurde

Unternehmen reduzieren die Anzahl von Datensicherheitsvorfällen und verbessern die Verwaltung von Warnungen mit KI

Unternehmen, die KI zur Stärkung ihrer Datensicherheitsprozesse einsetzen, melden deutlich weniger Warnungen. **Im Durchschnitt erhalten diejenigen, die KI-gesteuerte Datensicherheitstools implementiert haben, 47 Warnungen pro Tag, verglichen mit 79 Warnungen bei denjenigen, die keine derartigen Tools implementiert haben. Und diejenigen, die KI verwenden, können 66 % ihrer täglichen Warnungen überprüfen, während Unternehmen, die KI nicht verwenden, nur 60 % überprüfen können.**

Darüber hinaus nutzen Unternehmen, die KI zur Stärkung der Datensicherheit einsetzen, KI mit größerer Wahrscheinlichkeit auch zur Risikominimierung (56 % gegenüber 26 %). Die Verringerung der Anzahl von Warnungen und die bessere Möglichkeit, diese mithilfe von KI zu minimieren, scheint einen erheblichen Einfluss auf die Gesamtzahl der Datensicherheitsvorfälle gehabt zu haben. Unternehmen, die KI zur Stärkung der Datensicherheit implementiert haben, verzeichnen einen Rückgang bei Datensicherheitsvorfällen um 65 % im Vergleich zu Unternehmen, die KI nicht zur Stärkung der Datensicherheit einsetzen.

Die größten Auswirkungen hat KI voraussichtlich auf die Reaktion

Was die Erkennung angeht, erwarten 33 % der Entscheidungstragenden, dass mithilfe von KI anomale Aktivitäten erkannt werden, während 23 % glauben, dass KI die Untersuchung potenzieller Datensicherheitsvorfälle unterstützt. Weitere 22 % sehen das Potenzial, dass KI Empfehlungen zur besseren Absicherung ihrer Datenumgebungen geben kann.

Die Reaktion ist jedoch der Bereich, in der KI nach Meinung der Entscheidungstragenden die weitreichendsten Auswirkungen haben wird. 34 % glauben, dass KI die unbefugte Weitergabe sensibler Daten automatisch blockieren kann, und 32 % sagen, dass sie gefährdete Daten schützt. Weitere 26 % sind der Meinung, dass KI dazu beiträgt, Datensicherheitsrisiken zu minimieren und entsprechende Kontrollen anzuwenden, während ebenso viele erwarten, dass KI riskantes Nutzerverhalten automatisch kennzeichnet.

Der Weg in die Zukunft

Die Integration von KI in Datensicherheitslösungen kann hilfreich sein, da sie Teams Echtzeitinformationen, Zusammenfassungsfunktionen und Unterstützung natürlicher Sprache bietet, um Bereiche hervorzuheben, die sonst vielleicht übersehen worden wären. Dies kann auch Untersuchungen beschleunigen und das Know-how von Datensicherheitsteams erweitern. So können sich diese Funktionen auswirken:

Warnungszusammenfassung: Untersuchungen können aufgrund der Menge der zu analysierenden Quellen und der unterschiedlichen Richtlinienregeln eine sehr komplexe Aufgabe sein. Durch die Einbettung von KI in Data Loss Prevention (DLP) und Insider Risk Management (IRM) können Teams schnell eine Zusammenfassung der Warnungen erhalten, einschließlich der Quelle, der Richtlinienregeln und der Insights zum Benutzerrisiko, um zu verstehen, welche sensiblen Daten kompromittiert wurden und welches Benutzerrisiko damit verbunden ist.

Kontextbezogene Kommunikation: Unternehmen müssen gesetzliche Anforderungen rund um die Unternehmenskommunikation einhalten, was oft eine umfassende Überprüfung von Verstößen erforderlich macht. KI kann Datensicherheitsteams dabei unterstützen, Inhalte anhand von Vorschriften und Unternehmensrichtlinien zu bewerten, um hochriskante Kommunikation hervorzuheben, die zu einem Datensicherheitsvorfall führen könnte.

Umwandlung natürlicher Sprache in Keyword-Abfrage: Die Suche kann ein komplexer und zeitaufwändiger Workflow während Untersuchungen sein, der in der Regel die Verwendung einer Keyword-Abfragesprache erfordert. Mit KI können Datensicherheitsteams Such-Prompts in natürlicher Sprache eingeben, um den Beginn der Suche zu optimieren und umfassendere Untersuchungen zu ermöglichen.

Abschließende Empfehlungen

1 Schützen Sie sich vor Datensicherheitsvorfällen durch die Einführung einer integrierten Plattform

Die Einführung einer vollständig integrierten Datensicherheitsplattform bietet eine sicherere und schlankere Strategie in einer sich zunehmend weiterentwickelnden Landschaft, reduziert die Komplexität, erhöht die Transparenz und verbessert gleichzeitig den Schutz. Ein integrierter Ansatz kann Unternehmen dabei unterstützen, die Verwaltung des Datensicherheitsstatus zu verbessern, indem er Datensicherheitskontrollen zentralisiert und durchgängige Transparenz für Daten, Benutzende und Aktivitäten hinweg bietet, wodurch die Erkennung von Datenrisiken und der Schutz davor gestärkt und optimiert werden. 82 % der Unternehmen sind der Meinung, dass eine integrierte Plattform überlegen ist. Der Schritt hin zu Konsolidierung ist daher nicht nur nützlich, sondern unerlässlich.

2 Erhöhen Sie die Transparenz bei der internen Verwendung von KI, um die notwendigen Kontrollen für die KI-Nutzung durch die Mitarbeitenden zu bewerten, die sich nicht auf die Produktivität auswirken

Der zunehmende Einsatz von KI am Arbeitsplatz kann bestehende Risiken verstärken und neue Risiken mit sich bringen. Unternehmen räumen ein, dass sie mehr tun müssen, um sich vor einer nicht sicheren KI-Nutzung zu schützen. Die Nutzung von integrierten Kontrollen und Einblicken in KI-Apps ist entscheidend, um Datensicherheit ohne Unterbrechung der Produktivität zu gewährleisten. Das Training der Mitarbeitenden im sicheren Umgang mit KI kann Unternehmen dabei helfen, riskantes Verhalten zu minimieren und gleichzeitig sicherzustellen, dass Teams weiterhin von diesen leistungsstarken Tools profitieren.

3 Verbessern Sie Ihre Datensicherheitsstrategie mithilfe von KI

KI ermöglicht es Datensicherheitsteams, sich auf strategischere Initiativen zu konzentrieren, anstatt auf ständige Bedrohungen und eine hohe Anzahl von Warnungen zu reagieren. Unternehmen, die sich in fortgeschrittenen Phasen der KI-Implementierung befinden, sind selbstbewusster und zufriedener mit ihren Datensicherheitslösungen als diejenigen, die gerade erst einsteigen. Durch die Bereitstellung von KI als Teil einer umfassenden Datensicherheitsstrategie können Unternehmen ihre Transparenz verbessern. Dies stärkt ihre Fähigkeit, Risiken zu erkennen und darauf zu reagieren, und verbessert letztlich ihre allgemeine Datensicherheit.

Ziele der Untersuchung

Die Zielsetzungen der Untersuchung lauteten wie folgt:

1. Verständnis der Datensicherheits-landschaft, einschließlich Prioritäten, Denkweisen und Herausforderungen sowie der Ursache und Auswirkungen von Datensicherheitsvorfällen
2. Untersuchung der Zukunft der Datensicherheit, einschließlich neuer Strategien und Innovationen und der Investitionspläne von Unternehmen für die Zukunft
3. Ermittlung der Rolle von KI bei der Verbesserung der Datensicherheit und der Rolle von KI beim Schutz von Daten

Methodik

Vom 5. bis zum 23. August 2024 wurde eine 20-minütige internationale Online-Umfrage unter 1.376 Entscheidungstragenden aus dem Bereich Datensicherheit durchgeführt.

Bei den Fragen ging es um die Datensicherheitslandschaft und die Datensicherheitsvorfälle im Vergleich zu 2023. Darüber hinaus umfasste die Umfrage in diesem Jahr Fragen zur Absicherung der KI-Nutzung durch Mitarbeitende und zum Einsatz von KI zur Stärkung der Datensicherheit.

Rekrutierung der Teilnehmenden

Um die Auswahlkriterien zu erfüllen, mussten die Entscheidungstragenden aus dem Bereich Datensicherheit folgenden Vorgaben entsprechen:

- CISO und ähnliche Entscheidungstragende (C-2 und höher) mit Zuständigkeit für Datensicherheit
- Beschäftigung in Enterprise-Organisationen (mehr als 500 Mitarbeitende, verschiedene Größen)
- Mischung aus regulierten und nicht regulierten Branchen (keine Bildungs-, Regierungs- oder Non-Profit-Organisation)

Nachfolgend wird angegeben, wie sich die 1.376 Entscheidungstragenden aus dem Bereich Datensicherheit, die für die Untersuchung befragt wurden, auf die jeweiligen Länder verteilen:

- USA: 302
- Großbritannien: 305
- Indien: 301
- Brasilien: 158
- Frankreich: 156
- Australien: 154

hypothesis Microsoft Security