VansonBourne

Deutscher Bericht

Vertrauen in die Cloud aufbauen

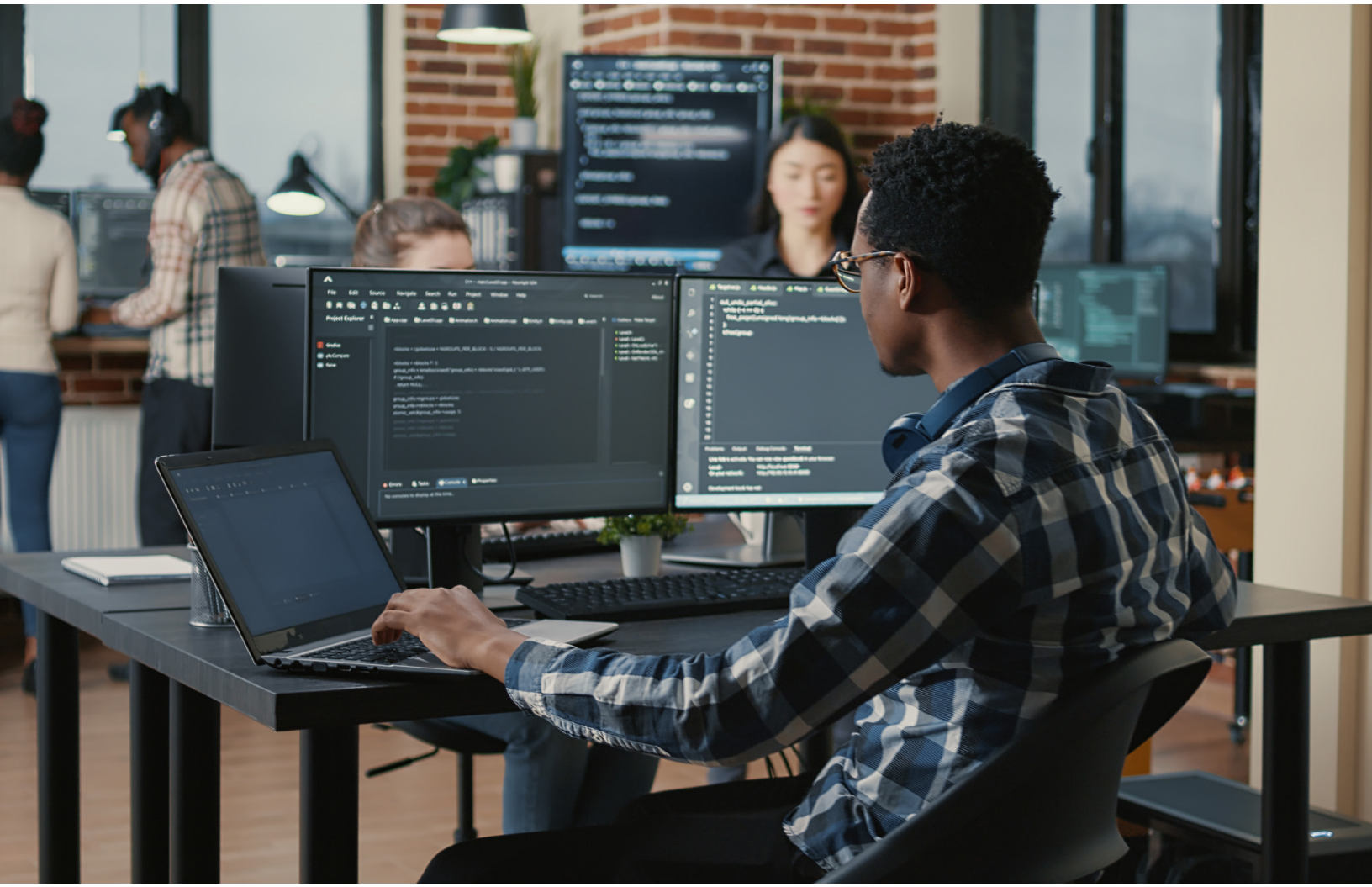
Wie Vertrauen und Sicherheit die nächste Phase des Cloud-Wachstums prägen

Einführung

Die Cloud ist heute die Grundlage jeder Unternehmensmodernisierung. Sie prägt die Art und Weise, wie deutsche Unternehmen digitale Dienste aufbauen, skalieren und absichern. Und die Cloudnutzung nimmt immer weiter zu – die Frage ist heute nicht mehr, ob die Cloud überhaupt vertrauenswürdig ist, sondern wie dieses Vertrauen angesichts zunehmender Komplexität und steigender Cyberrisiken gestärkt werden kann.

Diese Zusammenfassung liefert als Teil einer globalen Forschungsstudie zu Vertrauen in die Cloud und Resilienz einen fokussierten Einblick in den deutschen Markt. Sie untersucht, wie Unternehmen die Cloud in den Mittelpunkt ihrer Geschäftsstrategie stellen, wo operative und sicherheitsbezogene Herausforderungen einen schnelleren Fortschritt behindern und wie Investitionen und Erfahrungen dazu beitragen, diese zu überwinden.

Unternehmen, die auf die Cloud zum Ausbau ihrer Geschäftstätigkeit setzen, reizen möglicherweise auch die betrieblichen Vorteile, die das Modell der geteilten Verantwortung mit sich bringt, bei dem Cloud-Anbieter für die Infrastrukturkapazität, Verfügbarkeit und Sicherheit zuständig sind. Die Umfrageergebnisse widerlegen auch die Mythen über eine höhere Unsicherheit beim Einsatz der Cloud und zeigen stattdessen, dass Cloud-Kunden noch stärker in die Cloud als ihre primäre Plattform für die Entwicklung innovativer Anwendungen investieren werden. Gleichzeitig definiert KI neu, wie effektiver Schutz und Widerstandsfähigkeit aussehen, und ermöglicht eine schnellere Erkennung, intelligentere Reaktionen und mehr Vertrauen in einem sich rasch wandelnden Umfeld.



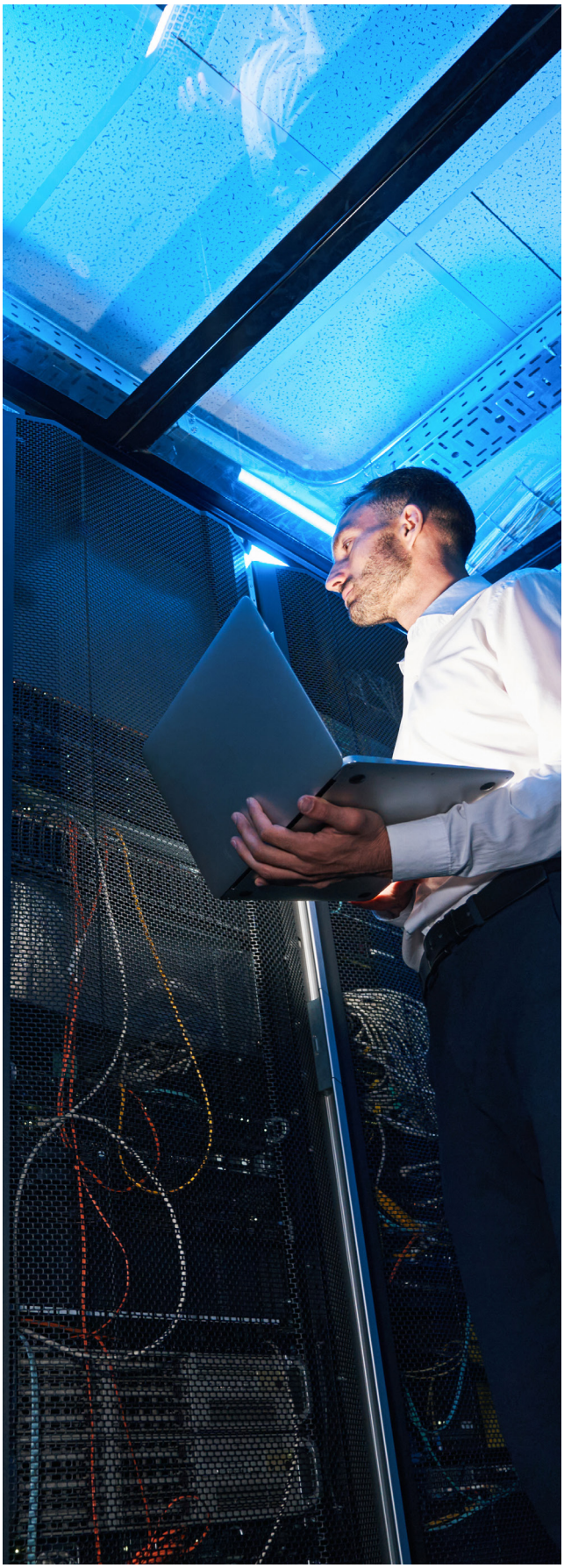
Abschnitt Eins: Die Grundlagen für Vertrauen in die Cloud

Die Public Cloud ist nicht mehr nur ein Ziel für ausgewählte Workloads. Sie ist zur Grundlage dafür geworden, wie Anwendungen aller Art konzipiert, entwickelt und skaliert werden. Im Durchschnitt laufen mittlerweile 61 % der Anwendungen Cloud-basiert, ein Anteil, der im nächsten Jahr voraussichtlich auf 72 % steigen wird, was eine deutliche Verlagerung hin zur Cloud darstellt.

Diese Beschleunigung wird durch Vertrauen und Investitionen gestützt. Bei der Entwicklung ihrer Cloud-Strategien liegt der Fokus der Unternehmen darauf, Flexibilität, Belastbarkeit und Sicherheit zu verbessern, um die Leistung in großem Maßstab zu steigern. Entscheidend ist, dass Veränderungen nicht nur geplant werden, sondern auch finanziert. Fast alle befragten Unternehmen erwarten, dass die Budgets für IT (97 %) und Cybersicherheit (93 %) in den nächsten 12 Monaten steigen werden.

Von allen befragten Ländern geben Unternehmen aus Deutschland am ehesten an, dass die IT-Budgets in den nächsten 12 Monaten insgesamt steigen werden. Allerdings liegt Deutschland nur an siebter Stelle der Länder, die dasselbe über ihre Cybersicherheitsbudgets sagen. Diese Diskrepanz könnte darauf hindeuten, dass deutsche Unternehmen zwar weiterhin daran interessiert sind, ihre IT-Kapazitäten auszubauen, viele jedoch bereits der Meinung sind, dass ihre Cybersicherheitsprogramme ausreichend ausgereift sind, und ihren Fokus daher auf die Optimierung bestehender Schutzmaßnahmen verlagern. Darüber hinaus beabsichtigen praktisch alle (99,5 %) der befragten Unternehmen in Deutschland , ihre Ausgaben für professionelle Dienstleistungen von Cloud-Anbietern zu erhöhen, was darauf hindeutet, dass Kunden Unterstützung durch die Fachkompetenz ihrer Anbieter erwarten.

Vertrauen in die Cloud geht Hand in Hand mit Zuversicht, und diese Zuversicht muss verdient werden. Unternehmen bewerten Anbieter nicht nur anhand ihrer Technologie, sondern auch anhand ihres Verhaltens. Die Einhaltung von Vorschriften (45 %) und Empfehlungen von vertrauenswürdigen Partnern, Kollegen oder Branchenanalysten (42 %) sind die beiden wichtigsten Faktoren, anhand derer Unternehmen aus Deutschland die Sicherheit eines Public-Cloud-Anbieters bewerten und ihm vertrauen. Doch Vertrauen bedeutet nicht für alle dasselbe. Beispielsweise lassen sich Fachleute eher von Empfehlungen von Kollegen und Partnern beeinflussen als ihre Kollegen in Entscheidungspositionen (Sicherheitsfachleute: 49 %, IT-Fachleute: 49 %, Sicherheits-DMs: 35 % und ITDMs: 34 %). Dies zeigt, dass Erfahrung und Reputation eine zentrale Rolle beim Aufbau von Vertrauen und für die Aufrechterhaltung des Vertrauens in die Cloud spielen.



Abschnitt Zwei: Wo Vertrauen auf die Probe gestellt wird: Auswirkungen von Sicherheit und Compliance

In gleicher Weise, wie Unternehmen zunehmend auf Cloud-Dienste setzen, bleibt auch das Vertrauen in die Public Cloud stark, insbesondere wenn man die in diese Dienste integrierten Sicherheitsvorkehrungen und ihre Konformität mit wichtigen Vorschriften, Zertifizierungen, Bescheinigungen und Branchen-Frameworks berücksichtigt. Unternehmen in Deutschland sind am drittstärksten davon überzeugt, dass ihre Cloud-Anbieter diese Standards erfüllen können (52 %), und am stärksten der Überzeugung, dass ihre Cloud-Anbieter über integrierte Sicherheitsfunktionen verfügen (53 %). Dies spiegelt das weit verbreitete Vertrauen in die Zuverlässigkeit und Leistungsfähigkeit der Cloud wider.

Public-Cloud-Anbieter arbeiten nach einem Modell der geteilten Verantwortung. Die Anbieter selbst sind für die Sicherheit der Cloud-Infrastruktur verantwortlich. Kunden müssen sich nur um die Sicherheit der Assets kümmern, die sie in die Cloud stellen, wodurch sich der Aufwand verringert. Für die Sicherheit ihrer Cloud implementieren Public-Cloud-Anbieter strengere Zugriffskontrollen als die meisten Unternehmen für ihre Büros. Zu den Sicherheitsvorkehrungen für den physischen Perimeter gehören hochsichere Zäune, Videoüberwachung, Einbruchmeldesysteme, Multi-Faktor-Zugangskontrolle und Wachpersonal – überwacht und kontrolliert von rund um die Uhr besetzten Sicherheitszentralen. Daten, die ein Rechenzentrum verlassen, werden auf Netzwerkebene verschlüsselt, während sie zwischen Infrastrukturstandorten übertragen werden.

Diese Investition in mehrschichtigen Schutz zahlt sich aus. Auf die Frage, welche Umgebung am besten geeignet ist, um wichtige Geschäfts- und IT-Anforderungen zu erfüllen, nannten die Befragten aus Deutschland in fast allen getesteten Bereichen durchweg die Public Cloud.

IT-Umgebung (lokal vs. Cloud-Anbieter), die am besten geeignet ist, um die folgenden Anforderungen zu erfüllen

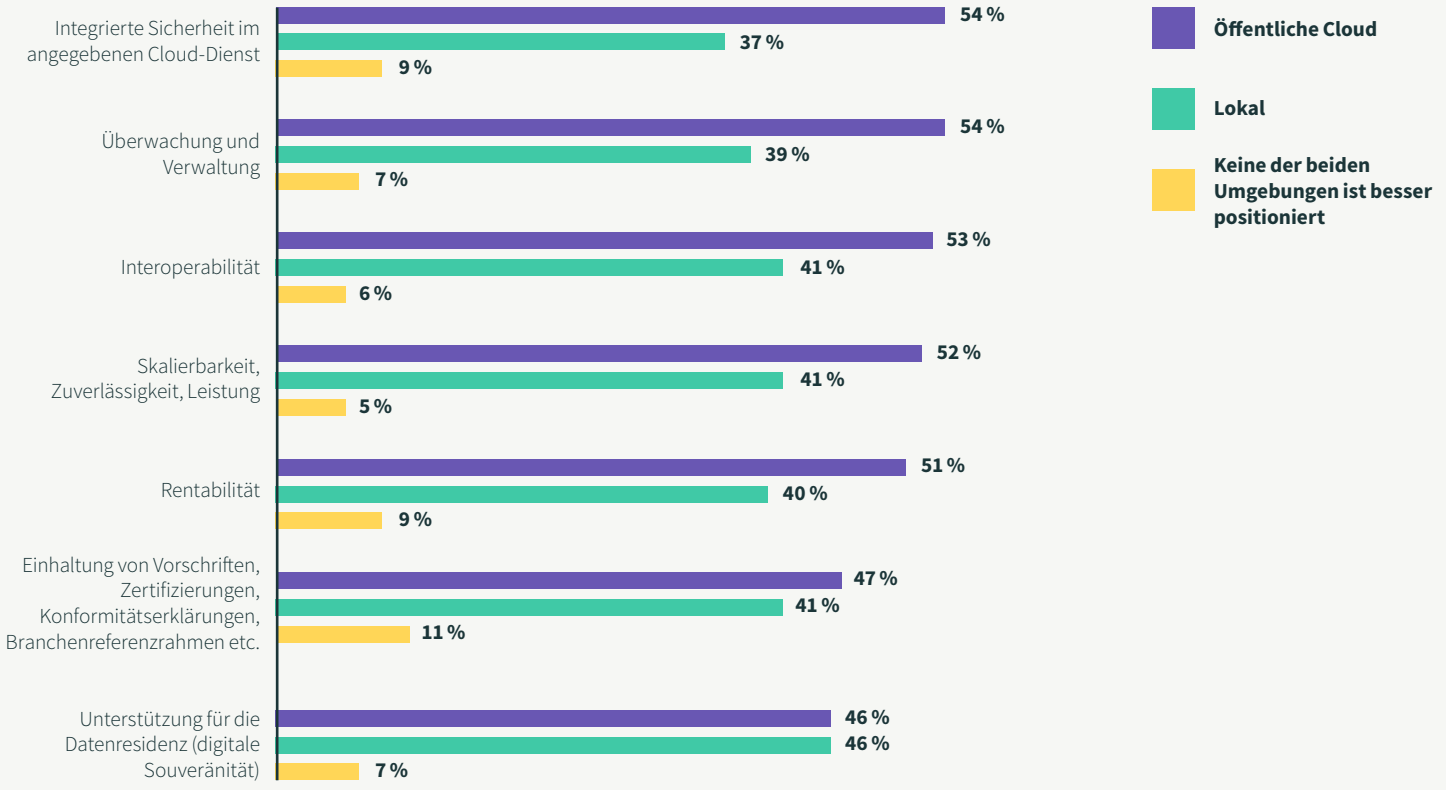


Abbildung 1. Welche IT-Umgebung (lokal oder Cloud-Anbieter) ist Ihrer Meinung nach am besten geeignet, um die folgenden Anforderungen zu erfüllen? [200]

Letztendlich basiert das Vertrauen in die Cloud auf Transparenz und Partnerschaft. Governance, disziplinierte Sicherheitspraktiken und gemeinsame Verantwortung sorgen zusammen für einen stärkeren Schutz und eine bessere Compliance, als die meisten Unternehmen alleine erreichen können.

Abschnitt Drei: Stärkung des Vertrauens in die Cloud durch KI

Da Cloud-Umgebungen immer komplexer werden, wird KI zunehmend zur nächsten unverzichtbaren Ebene dieser Verteidigung. Mit der zunehmenden Verbreitung von Cloud-Umgebungen entwickelt sich KI sowohl zu einem Katalysator für eine schnellere Erkennung als auch zu einem Eckpfeiler für zukünftige Resilienz.

Wichtigste Priorität zur Reduzierung von Cyberrisiken in den nächsten drei Jahren

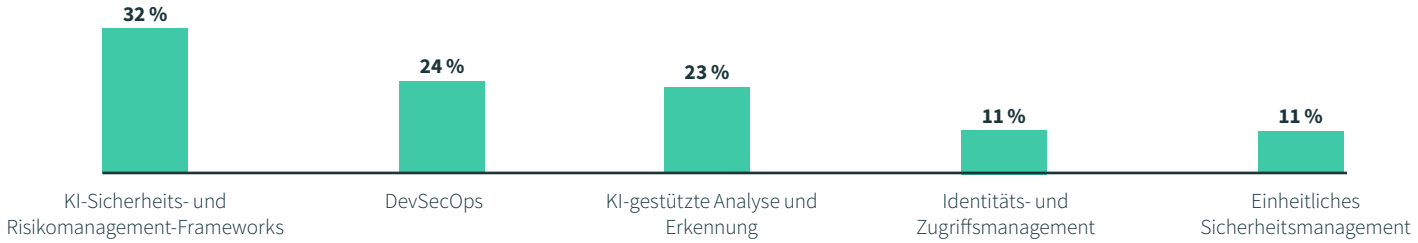


Abbildung 2. Welche der folgenden Maßnahmen werden Ihrer Meinung nach ggf. in den nächsten drei Jahren die wichtigste Priorität zur Reduzierung von Cyberrisiken darstellen? [200]

Knapp ein Drittel (32 %) der Befragten nannten KI-Sicherheits- und Risikomanagement-Frameworks als eine der wichtigsten Prioritäten für die Reduzierung von Cyberrisiken in den nächsten drei Jahren – ein vergleichsweise moderater Wert. Diese Positionierung lässt darauf schließen, dass viele deutsche Unternehmen die Anfangsphase der Einführung von KI-Sicherheits- und Risikomanagement-Frameworks hinter sich gelassen haben und sich nun auf deren Operationalisierung konzentrieren. Dabei nutzen sie die starke Dynamik der Standardisierung (z. B. ISO/IEC 42001) und nationale Leitlinien (über das BSI), um von der Konzeption zur Umsetzung von KI-Risikokontrollen überzugehen.

KI-Sicherheit und Risikomanagement-Frameworks sind die wichtigste Priorität für die Reduzierung von Cyberrisiken in den nächsten drei Jahren.

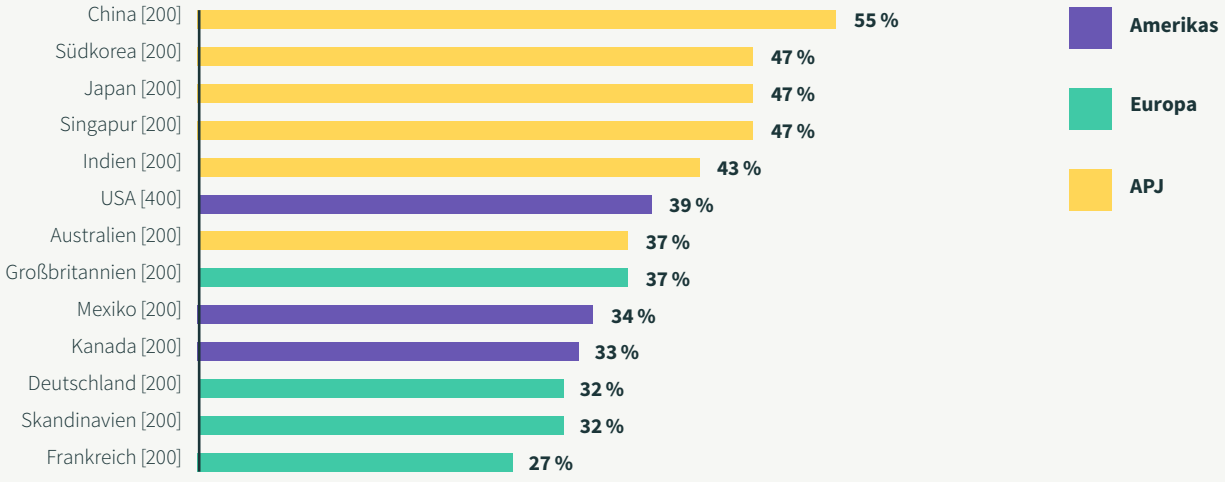


Abbildung 3. Welche der folgenden Maßnahmen wird Ihrer Meinung nach in den nächsten drei Jahren die wichtigste Priorität für die Reduzierung von Cyberrisiken sein? [Grundgesamtheitsgrößen im Diagramm] Nur diejenigen, die „KI-Sicherheit und Risikomanagement-Frameworks“ angegeben haben.

Dieser übergreifende Fokus auf Sicherheits- und Risikomanagement-Frameworks ist Beleg für die wachsende Erkenntnis, dass KI nicht nur die Art und Weise verändert, wie Unternehmen sich gegen Bedrohungen schützen, sondern auch, wie sie ihrer Rechenschaftspflicht nachkommen. Unternehmen betrachten KI als Verbündeten für die Automatisierung von Sicherheits- und Compliance-Kontrollen. Zwar haben sie die durch KI ermöglichten Innovationen willkommen geheißen, doch sie sind sich auch bewusst, dass KI-Sicherheits- und Risikokonzepte die nächste Herausforderung in den nächsten drei Jahren darstellen.

KI-Agenten werden auch eine größere Rolle bei der Automatisierung von Sicherheitszentren und der Überwachung von Risiken durch Dritte/Lieferketten spielen, wobei in den nächsten 12 Monaten mit einer verstärkten Anwendung dieser Agenten zu rechnen ist.

Aktuelle und geplante Nutzung von KI-Agenten für Sicherheitsaufgaben

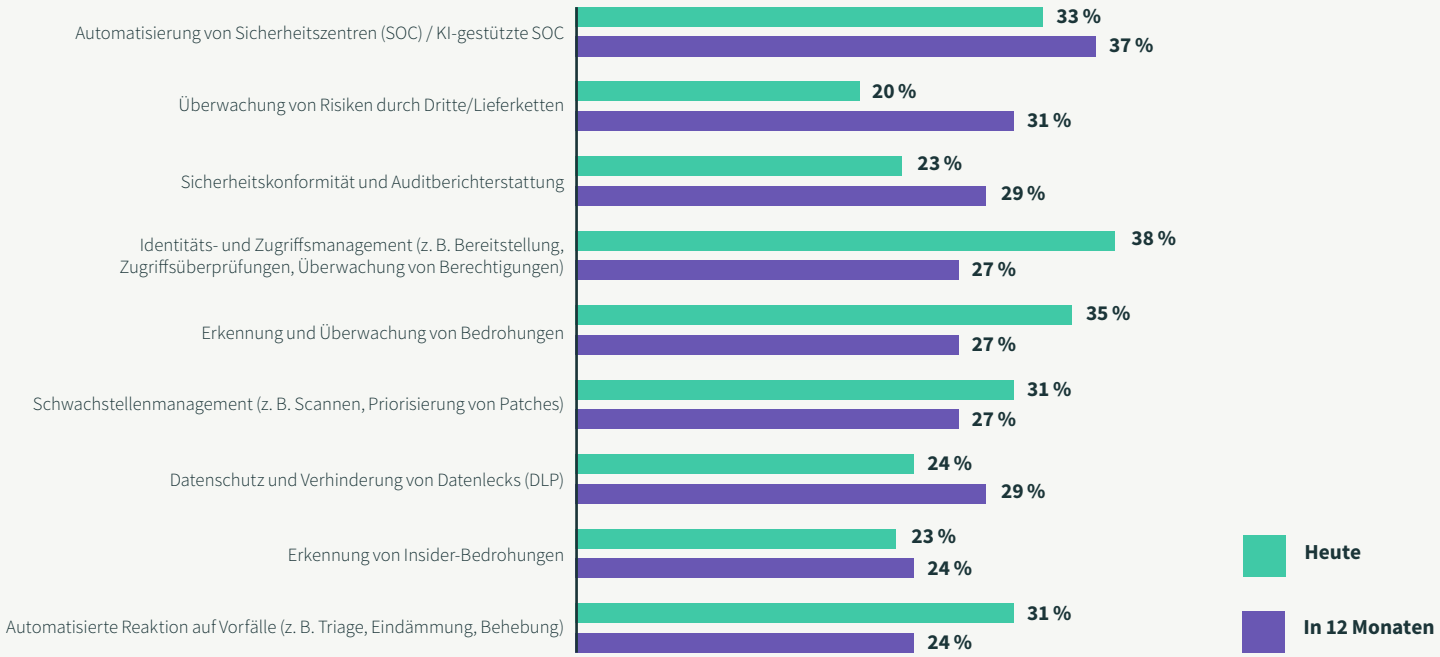


Abbildung 4. Welche der folgenden Sicherheitsaufgaben plant Ihr Unternehmen derzeit ggf. mit KI-Agenten zu lösen, und für welche Aufgaben ist deren Einsatz in den nächsten 12 Monaten vorgesehen? [200]

Über alle Befragten hinweg legen heute sicherheitsorientierte Fachleute eher Wert auf Identitäts- und Zugriffsmanagement (Sicherheitsfachleute: 51 %, IT-Fachleute: 45 %). Sicherheitsverantwortliche messen der Erkennung und Überwachung von Bedrohungen (37 %) und der Automatisierung von Security Operations Centern (SOC) bzw. KI-gestützten SOC (37 %) gleiche Priorität bei. ITDMs konzentrieren sich auf das Schwachstellenmanagement (38 %). Diese Unterschiede verdeutlichen, wie sehr die Sicherheitskultur in Deutschland von Präzision und klaren Rollen definiert ist. Anwendende Fachleute legen den Schwerpunkt auf Zugriffskontrolle, Entscheidungsträger setzen auf Automatisierung und Überwachung, um den Schutz zu skalieren, und IT-Führungskräfte konzentrieren sich auf die Beseitigung von Schwachstellen. In Kombination weist dies auf ein ausgereiftes Ökosystem hin, das den Schwerpunkt eher auf eine disziplinierte, mehrschichtige Verteidigung als auf reaktive Ausgaben legt.

Diese zunehmende Abhängigkeit von KI bringt jedoch auch neue Erwartungen hinsichtlich ihrer Sicherheit mit sich. Alle (100 %) Befragten aus Deutschland geben an, dass integrierte Sicherheitsfunktionen zu den wichtigsten Faktoren bei der Auswahl von KI-Lösungen von Drittanbietern gehören, was unterstreicht, dass Innovation allein nicht ausreicht. Vertrauen muss in jede Ebene des KI-Stacks integriert werden. 15 % der Befragten aus Deutschland stimmten nicht zu, dass Sicherheits- und Risikobedenken im Zusammenhang mit KI ein wesentliches Hindernis für die Verlagerung weiterer Workloads und/oder Daten in die Cloud darstellen, wobei Entscheidungsträger eher zu dieser Antwort neigten als anwendende Fachleute. Dies könnte auf Early Adopters hindeuten, die bereits Rahmenbedingungen geschaffen haben, um den Weg für die Einführung von KI zu ebnen. Viele KI-Sicherheitskonzepte und Frameworks zur Risikobewertung basieren auf grundlegenden Sicherheitsprinzipien, die in stark regulierten Branchen bereits angewendet werden.

Letztendlich hängt das anhaltende Vertrauen in die Cloud davon ab, wie effektiv Unternehmen die Schnittstelle zwischen Cloud und KI verwalten und sicherstellen, dass Innovationen durch eine starke Governance, Transparenz und ein sicheres Design auf jeder Ebene untermauert werden.

Fazit:

Für deutsche Unternehmen ist die Cloud zur Grundlage für Innovation, Skalierbarkeit und Sicherheit geworden. Dies erhöht allerdings die Komplexität. Integrationsherausforderungen, operative Komplexität und anhaltende Cybersicherheitsbedrohungen bleiben anhaltende Herausforderungen und erinnern daran, dass Modernisierung sowohl Disziplin als auch Ehrgeiz erfordert.

Als Reaktion darauf werden Investitionen in Governance, Transparenz und Automatisierung beschleunigt, wobei KI nun eine zentrale Rolle bei der Verbesserung der Erkennung, Reaktions- und Widerstandsfähigkeit spielt. Aber Technologie allein reicht nicht aus. Fortschritt hängt von starken Partnerschaften und von Anbietern ab, denen man vertraut, Transparenz, Zuverlässigkeit und Sicherheit in großem Maßstab zu bieten.

Der deutsche Markt treibt die Einführung der Cloud im Jahr 2025 voran und weiß um die damit verbundene Verantwortung. Der Erfolg dieser Strategie ist wesentlich damit verknüpft, dass die Grundlagen, in die investiert wurde, weiterverfolgt werden: Innovation, gestützt durch die Größe und operative Ausfallsicherheit der Cloud, geschützt durch die Sicherheit der Cloud – in der Cloud.

Über die Forschung:

AWS beauftragte den unabhängigen Marktforschungsspezialisten Vanson Bourne mit der Durchführung der Untersuchung, auf der dieser schriftliche Bericht basiert, im September und Oktober 2025. Die weltweite Studie befragte 2.800 Entscheidungsträger und Fachleute aus den Bereichen Technologie und Sicherheit, darunter 200 aus Unternehmen in Deutschland.

Alle Befragten hatten Verantwortung oder Einfluss auf Entscheidungen in Bezug auf Cloud-Umgebungen, Technologie oder Sicherheit innerhalb ihres Unternehmens, das eine Mischung aus lokalen Rechenzentren und Cloud-Umgebungen betreibt. Die Unternehmen mussten mindestens 500 Mitarbeiter beschäftigen (in den USA mindestens 1.000) und repräsentierten ein breites Spektrum von Branchen, darunter Gesundheitswesen und Biowissenschaften, Regierung/öffentlicher Sektor, Finanzdienstleistungen, Automobilindustrie und Fertigung, Einzelhandel und Konsumgüter, Telekommunikation, Informationstechnologie und Dienstleistungen, Medien, Freizeit und Unterhaltung, Bildung und gemeinnützige Organisationen sowie Energie, Öl und Gas und Versorgungsunternehmen.

Über Vanson Bourne:

Vanson Bourne ist ein unabhängiges Marktforschungsinstitut im Technologiebereich. Sein Ruf für solide und glaubwürdige forschungsbasierte Analysen beruht auf strengen Forschungsgrundsätzen und der Fähigkeit, die Meinungen von leitenden Entscheidungsträgern in allen technischen und geschäftlichen Funktionen sowie in allen Geschäftsbereichen und allen wichtigen Märkten einzuholen.

Weitere Informationen finden Sie unter www.vansonbourne.com

Der vollständige Bericht für mehrere Länder:

„Vertrauen in die Cloud aufbauen : Wie Vertrauen und Sicherheit die nächste Phase des Cloud-Wachstums prägen“