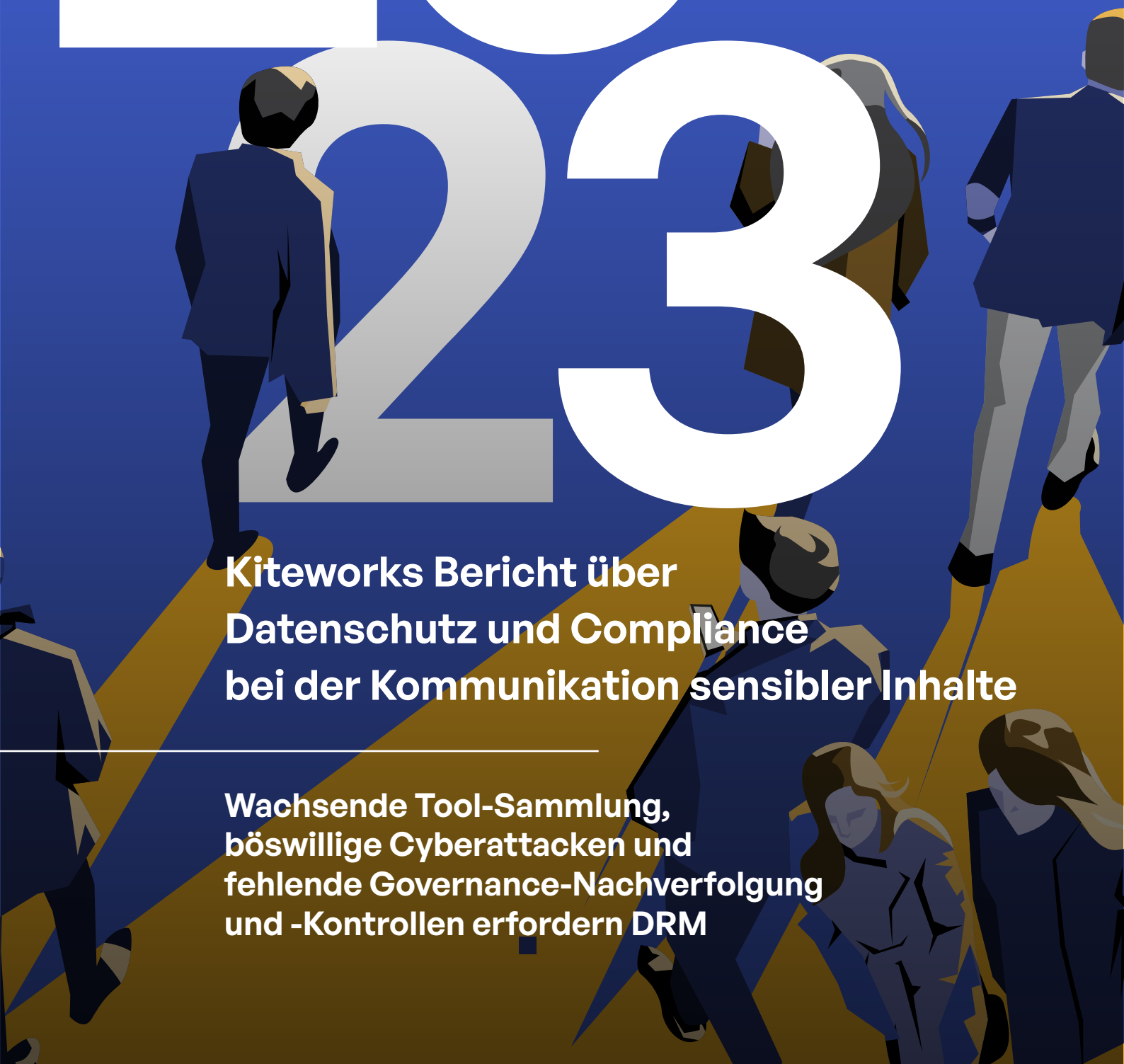
Kiteworks

2023



Kiteworks Bericht über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte

Wachsende Tool-Sammlung, böswillige Cyberattacken und fehlende Governance-Nachverfolgung und -Kontrollen erfordern DRM

Inhaltsverzeichnis

Vorwort

Vielen Dank für das Herunterladen des Kiteworks Reports 2023 über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte. Wir begrüßen diejenigen, die unseren ersten Bericht im Jahr 2022 gelesen haben, sowie die neuen Leser, die uns in diesem Jahr gefunden haben. Wir freuen uns, dass Sie uns bei dieser Untersuchung von häufig vernachlässigten Aspekten der Cybersicherheit und Compliance begleiten - dem Schutz von Inhalten, die nicht nur intern versendet und geteilt werden, sondern auch an unzählige externe Parteien, die ein Unternehmen nicht kontrollieren kann.

Der Schutz von Inhalten ist wichtig, da sie einen Großteil der Daten enthalten, die wir schützen müssen, um unsere Markenidentität zu wahren, Kunden zum Kauf zu bewegen, Wirtschaftsprüfer zufrieden zu stellen und unsere Marktposition zu schützen. Die Offenlegung von persönlich identifizierbaren Informationen, geschützten Gesundheitsdaten, Kreditkartentransaktionsdaten, Unternehmensfinanzen, geistigem Eigentum oder nicht öffentlichen Informationen über Fusionen und Übernahmen und andere rechtliche Angelegenheiten ist für jedes Unternehmen aus einer Vielzahl von Gründen katastrophal.

Damit das Unternehmen jedoch funktionieren kann, müssen diese Daten häufig mit bestimmten externen Parteien geteilt werden, die diese Informationen benötigen. In den meisten Unternehmen sind dies Tausende von Organisationen. Dieser Austausch von Inhalten zwischen den Beteiligten stellt für die Unternehmen ein enormes Sicherheits- und Compliance-Risiko dar. Die Umfrage, die dem diesjährigen Bericht zugrunde liegt, zeigt, dass diese Risiken in den meisten Fällen noch nicht entschärft wurden.

Der Zeitpunkt für diese Sicherheitslücken ist denkbar schlecht, denn die Risiken nehmen zu. Mehr Angriffe als in den letzten Jahren beinhalten heute Datendiebstahl. Die Exfiltration von Daten ist heute ein Standardbestandteil von Ransomware-Angriffen, die früher einfach nur Systeme blockierten. Gleichzeitig verschärfen Aufsichtsbehörden weltweit ihre Anforderungen und erhöhen die Strafen bei Nichteinhaltung. Und aus verschiedenen Gründen müssen sich Unternehmen an Rahmenwerke wie das National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) halten, das solche Sicherheitslücken schließen soll - und werden entsprechend geprüft. Aus all diesen Gründen glauben wir, dass das kommende Jahr für Unternehmen entscheidend sein wird, wenn es um den Schutz der Kommunikation mit sensiblen Inhalten geht.

Die wichtigste Erkenntnis aus den Daten der Studie ist die Bedeutung der digitalen Rechteverwaltung ("Digital Rights Management", DRM) für die Vereinheitlichung, Nachverfolgung, Kontrolle und den Schutz der Kommunikation sensibler Inhalte. Der Bericht zeigt zwar die oben erwähnten Lücken auf, stellt aber auch fest, dass die Unternehmen die Notwendigkeit von DRM-Funktionen erkennen und deren Implementierung auf der Roadmap haben. Wenn wir unseren Bericht für das Jahr 2024 vorlegen, wird es interessant sein zu sehen, ob sie auf ihrem Weg vorangekommen sind oder ob unsere Erkenntnisse nur eine Fata Morgana waren.

Mit freundlichen Grüßen

Patrick Spencer

Patrick Spencer, Ph.D.
VP of Corp. Marketing & Research, Kiteworks

Kurzübersicht

Wenn Sie im Rahmen Ihrer Arbeit jemals sensible Inhalte an externe Personen gesendet haben, ist dieser Bericht für Sie bestimmt. Wenn Sie auf "Senden" oder "Freigeben" geklickt haben, haben Sie wahrscheinlich nicht über die Auswirkungen Ihres Handelns auf Sicherheit und Compliance nachgedacht. Aber solche Handlungen stellen jedes Jahr ein größeres Risiko für Unternehmen dar. Der 2023 Kiteworks Bericht über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte untersucht das Verhalten von Unternehmen, die solche Inhalte mit Tausenden von anderen Unternehmen teilen.

Dieser Bericht basiert auf einer umfassenden weltweiten Befragung von IT-, Cybersicherheits- und Compliance-Experten in Unternehmen. Die Befragten repräsentieren ein breites Spektrum an Branchen, Regionen und Berufsgruppen. Die Antworten lieferten eine Reihe von Erkenntnissen über Sicherheit und Compliance bei der Kommunikation sensibler Inhalte.

Ein komplexes Netz von Empfängern, Kanälen und Tools

Die erste Erkenntnis ist, dass die Kommunikation sensibler Inhalte komplex ist. Die Zahl der externen Parteien, mit denen Unternehmen ihre sensiblen Inhalte austauschen müssen, ist überwältigend. 9 von 10 Unternehmen tauschen solche Inhalte mit mehr als 1.000 externen Organisationen aus, und 44 % geben an, dass diese Zahl 2.500 übersteigt.

Ebenso erstaunlich ist die Anzahl der Tools oder Systeme, die für den Austausch sensibler Inhalte verwendet werden: Die Hälfte der Befragten gibt an, Inhalte über sechs oder mehr Kanäle auszutauschen. Beide Prozentzahlen sind im Vergleich zu einer identischen Frage in der Umfrage für unseren Bericht 2022 deutlich angestiegen.

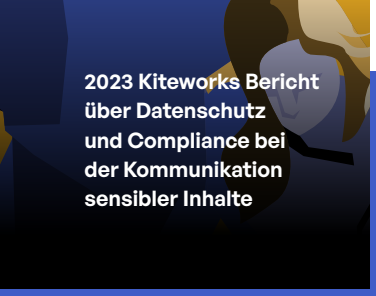
Ein weiteres Anzeichen für eine inakzeptable Komplexität: 85 % der Befragten verwenden vier oder mehr Tools, um die Verbreitung solcher Inhalte zu verfolgen, zu kontrollieren und zu schützen, und 46 % geben an, dass es sechs oder mehr sind.

90%

der Unternehmen teilen sensible Inhalte mit 1.000+ externen Parteien

100%

der Unternehmen nutzen 4+ Kanäle, um sensible Inhalte zu teilen



50%

nutzen 6+ Kommunikationstools zum Versenden und Teilen sensibler Inhalte

85%

der Unternehmen verwenden 4+ Systeme zur Überwachung, Kontrolle und zum Schutz der Kommunikation sensibler Inhalte

Bei der Sicherheitsreife bleibt noch viel zu tun

Eine weitere Erkenntnis ist, dass viele Unternehmen noch einen weiten Weg vor sich haben, um ihre Sicherheitsmaßnahmen für die Kommunikation sensibler Inhalte wirklich effektiv zu gestalten. Nur knapp ein Viertel der Befragten gibt an, dass ihre Verfahren zur Bewertung und Verwaltung der Sicherheit dort sind, wo sie sein sollten, und ein ähnlicher Prozentsatz berichtet, dass sie eine strategische Abstimmung zwischen der Bewertung und Verwaltung der Sicherheit sensibler Inhalte und ihrer Risikomanagementstrategie vorgenommen haben. Es ist offensichtlich, dass die große Mehrheit der Unternehmen noch viel zu tun hat.

Das Ergebnis dieser unvollständigen strategischen Arbeit ist, dass unsere Befragten viele Bedenken haben. E-Mail, Filesharing, Dateitransfer und Automatisierungssysteme stellen nach wie vor ein großes Risiko für Unternehmen dar, wenn sie zur Verbreitung sensibler Inhalte genutzt werden. Sie sind sich aber auch der Risiken bewusst, die von neu entstehenden Kanälen wie mobilen Anwendungen, Textnachrichten und APIs (Application Programming Interfaces) ausgehen. Die von uns befragten Experten sind auch besorgt über eine breite Palette von Angriffsmethoden auf alle Arten von sensiblen Daten, von persönlich identifizierbaren Informationen bis hin zu geistigem Eigentum.

Nur **27 %**

geben an, dass ihre *Sicherheitsmaßnahmen* für die Kommunikation sensibler Inhalte *nicht* verbessert werden müssen

Nur **26 %**

sagen, dass ihr *Sicherheitsmanagement* für die Kommunikation sensibler Inhalte *nicht* verbessert werden muss

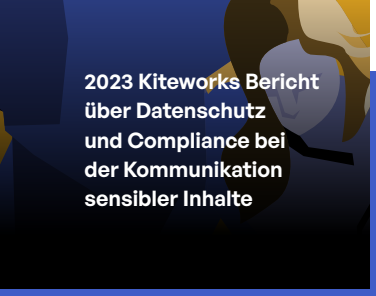
Nur **28 %**

geben an, dass ihre Bemühungen zum Schutz der Kommunikation mit sensiblen Inhalten bereits auf die Risikomanagementstrategie des Unternehmens *abgestimmt* sind

Mehr Compliance-Anforderungen ohne zusätzliche Ressourcen

Eine weitere Erkenntnis ist, dass die Einhaltung der Vorschriften für die in unserer Umfrage vertretenen Unternehmen nach wie vor schwierig ist. Die Europäer stehen besonders unter Druck, die EU-Datenschutzgrundverordnung (DSGVO) einzuhalten, die bei Nichteinhaltung hohe Geldstrafen vorsieht. Die meisten Befragten unterliegen jedoch den Datenschutzbestimmungen mindestens einer Gerichtsbarkeit und die meisten werden auch nach mindestens einem Branchenstandard geprüft. Darüber hinaus arbeiten 99 % der Befragten mit Behörden zusammen und müssen in diesem Zusammenhang besondere Anforderungen erfüllen.

Leider fordert diese Fülle an Compliance-Anforderungen einen hohen Tribut von den IT-, Sicherheits- und Compliance-Teams. Mehr als zwei Drittel der Unternehmen geben an, dass die Compliance allein für die Kommunikation sensibler Inhalte mindestens 300 Mitarbeiterstunden pro Jahr in Anspruch nimmt, mehr als ein Drittel beziffert diese Zahl auf über 500 Stunden. Nahezu jedes Unternehmen hat mindestens einen Mitarbeiter für diese Aufgabe abgestellt.



69 %

der Unternehmen verbringen 300+ Stunden pro Jahr mit der Überwachung und Dokumentation der Compliance bei der Kommunikation sensibler Inhalte

91 %

der Unternehmen stellen mindestens 1 Vollzeitkraft für Compliance im Bereich der Kommunikation sensibler Inhalte bereit

Nur 27 %

geben an, dass ihre Compliance-Maßnahmen bei der Kommunikation sensibler Inhalte bereits auf die Risikomanagementstrategie des Unternehmens abgestimmt sind

Best Practices - eine bunte Mischung

Eine weitere Erkenntnis ist, dass die Befragten zwar im Allgemeinen ein gutes Verständnis von Best Practices für die Kommunikation sensibler Inhalte haben, in der Praxis jedoch noch erhebliche Lücken bestehen. Wichtige Kontrollmechanismen wie das Prinzip der geringsten Zugriffsrechte, Multi-Faktor-Authentifizierung und Datenverschlüsselung sind zumindest für einen Teil des Austauschs sensibler Inhalte vorhanden. Bei der überwiegenden Mehrheit der Unternehmen ist der Schutz jedoch nicht vollständig.

Drei Viertel oder mehr der Unternehmen haben die Nachverfolgung, Protokollierung und Zugriffskontrolle für die Kommunikation mit sensiblen Inhalten noch nicht auf alle Abteilungen, alle Arten von Inhalten und alle Teile der Infrastruktur – ob vor Ort oder in der Cloud - ausgeweitet.

Nur

22 %

der Unternehmen verfolgen und erfassen die Zugriffe von externen Parteien in allen Abteilungen und für alle Arten von Inhalten

Nur

25 %

beschränken den Zugriff auf Ordner mit sensiblen Inhalten über alle Abteilungen und Inhaltstypen hinweg

Nur

22 %

verfolgen und kontrollieren den Zugriff auf sensible Inhalte auf administrativer Ebene, vor Ort und in der Cloud

Viel zu viele Exploits

Eine weitere, eher beunruhigende Erkenntnis ist, dass Unternehmen mit einer hohen Anzahl von Exploits konfrontiert sind, insbesondere im Zusammenhang mit der Kommunikation sensibler Inhalte. Mehr als 8 von 10 Unternehmen hatten im vergangenen Jahr vier oder mehr solcher Vorfälle, mehr als ein Drittel sogar mehr als sieben. Mehr als 6 von 10 Unternehmen hatten finanzielle Folgen eines Angriffs und mehr als 4 von 10 Unternehmen waren mit negativen Auswirkungen auf die Marke und die Compliance konfrontiert.

84 %

der Unternehmen hatten 4+ Exploits bei sensiblen Inhalten in der Kommunikation

62 %

erlitten einen finanziellen Schaden als Folge eines solchen Angriffs

Der langsame Weg zur digitalen Rechteverwaltung

Die beste Lösung für diese Probleme ist eine Methode, die als Digital Rights Management (DRM) bezeichnet wird. Dabei klassifizieren Unternehmen ihre Inhalte, teilen sie nach Risiko ein und kontrollieren den Zugriff auf Basis von Rollen - wobei bestimmte Aktionen auf bestimmte Arten von sensiblen Inhalten nur denjenigen zur Verfügung stehen, die sie für ihre Arbeit benötigen - und basierend auf dem geografischen Standort (z. B. Geofencing). Obwohl unsere Ergebnisse zeigen, dass die Unternehmen in Sachen DRM noch einen weiten Weg vor sich haben, gibt es auch gute Nachrichten. Die meisten Unternehmen geben an, dass sie viele Best Practices im Bereich DRM anwenden.

Mehr als 9 von 10 Unternehmen klassifizieren bereits vertrauliche Inhalte - eine Maßnahme, die durch Sicherheits- und Compliance-Bedenken in Bezug auf personenbezogene und andere sensible Daten motiviert ist. Die meisten dieser Unternehmen haben Benutzer, die offline auf sensible Inhalte zugreifen müssen - Führungskräfte, technische Außendienstmitarbeiter oder Vertriebsmitarbeiter. Viele haben ihre DRM-Anforderungen gründlich durchdacht. Allerdings verlangsamen Hindernisse wie die Notwendigkeit, unverschlüsselte Dateien mit externen Parteien zu bearbeiten, den Prozess. Ein weiterer Stolperstein ist die Notwendigkeit, die Kontrollen an verschiedene Benutzer, Rollen und Inhaltstypen anzupassen.

93 %

der Unternehmen klassifizieren sensible Inhalte

Jedoch,

55 %

der Befragten geben an, dass die Notwendigkeit einer Kontrolle nach Nutzer, Rolle und Inhaltsklasse ein Hindernis für den Einsatz von DRM darstellt

Vorsichtiger Optimismus für das kommende Jahr

Die Ergebnisse unserer Umfrage zeigen zwar, dass die Unternehmen viele Lücken beim Schutz der Kommunikation mit sensiblen Inhalten haben, aber das bedeutet auch, dass sie viele Möglichkeiten haben, im kommenden Jahr Verbesserungen vorzunehmen. Der Handlungsbedarf könnte nicht dringender sein, denn sensible Inhalte sind gefährdeter denn je. Wir hoffen, dass Unternehmen einen ganzheitlichen Ansatz verfolgen und die DRM-Prinzipien nutzen, um die Compliance zu verbessern, sich gegen interne Bedrohungen zu wappnen und sensible Inhalte zu schützen, unabhängig davon, woher sie stammen und wie sie übermittelt werden.

Einführung: Die Kommunikation mit sensiblen Inhalten ist nicht länger nur ein hehres Ziel

Willkommen zur zweiten Ausgabe des Kiteworks Reports über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte! Zum zweiten Mal in Folge haben wir fast 800 IT-, Sicherheits-, Risiko- und Managementexperten befragt, um herauszufinden, wie sie mit Datenschutz- und Compliance-Risiken bei der Kommunikation sensibler Inhalte umgehen. Es überrascht nicht, dass ihre Antworten unsere Aufmerksamkeit erregt haben. Sensible Inhalte sind das Herzstück des Geschäfts und der betrieblichen Abläufe eines jeden Unternehmens - und für viele ein lebenswichtiges Gut.

Unabhängig davon, ob diese Inhalte versehentlich an Personen oder Organisationen gesendet oder weitergegeben werden, die keinen Zugriff darauf haben sollten, oder ob sie absichtlich von böswilligen Cyberkriminellen gehackt werden, können die finanziellen, markenrechtlichen und aufsichtsrechtlichen Folgen verheerend sein.

Für Einzelpersonen, die mit einem Unternehmen interagieren, sind persönlich identifizierbare Informationen, geschützte Gesundheitsdaten und Kreditkartendaten gefährdet. Für Unternehmen sind geistiges Eigentum, finanzielle und rechtliche Details des Unternehmens und Informationen über Fusionen und Übernahmen anfällige Datenschätze für böswillige Akteure, die Profit machen oder Schaden anrichten wollen. Für Regierungsbehörden und damit verbundene Unternehmen könnte die Offenlegung von Informationen über die nationale Sicherheit, kritische Infrastrukturen und strafrechtliche Ermittlungen den Lauf der Weltgeschichte zum Schlechten verändern.

Wir warnen Sie davor, dass einige Inhalte dieses Berichts Stress auslösen könnten, insbesondere wenn Sie in den Bereichen Sicherheit, Compliance oder Risikomanagement tätig sind. Aber wir wollen die Dinge beim Namen nennen und Unternehmen dazu ermutigen, in den nächsten 12 Monaten wirksame Maßnahmen zum besseren Schutz ihrer Inhalte zu ergreifen. Wir hoffen, dass der Bericht für das kommende Jahr aufzeigen wird, wie Unternehmen ihre Sicherheits- und Compliance-Risiken im Zusammenhang mit der Kommunikation sensibler Inhalte besser managen. Mit einem Bewusstsein für die Probleme und strategischen Maßnahmen zu deren Lösung ist ein solches Ergebnis durchaus im Bereich des Möglichen.

Gnadenlose Angriffe, menschliche Schwächen, steigende Kosten

Es ist kein Geheimnis, dass die Cybersicherheit einen immer größeren Anteil am gesamten Risikoportfolio eines Unternehmens ausmacht. Es ist noch gar nicht so lange her, dass eine Firewall, ein VPN und ein Antivirusprogramm alles waren, was Unternehmen zum Schutz brauchten. Heute machen raffinierte Angreifer, die von großen Teams staatlich gesponserter Hacker oder Managed Services Providern auf dem Schwarzmarkt unterstützt werden, es unvermeidlich, dass ein Unternehmen Angriffe mit Ransomware, gestohlenen Zugangsdaten, URL-Manipulation oder Denial of Service - neben anderen Taktiken - erlebt.

Hinzu kommt der zunehmende Diebstahl von Inhalten als Teil dieser Angriffe. Untersuchungen von Mandiant haben ergeben, dass der Anteil des Datendiebstahls an den Vorfällen von 29 % auf 40 % gestiegen ist - ein Anstieg um 37 % innerhalb von 12 Monaten.[1] Die Entschlüsselung und Löschung von Dateien ist Teil von mehr als einem Viertel der Angriffe, die von mehr als 3.500 Tätergruppen durchgeführt werden, darunter 900 neue im Jahr 2022.

Der Verizon Data Breach Investigations Report[2] von 2023 zeigt, dass personenbezogene Daten (Personally Identifiable Information, PII) und geschützte Gesundheitsinformationen (Protected Health Information, PHI) bei mehr als 50 % der Sicherheitsverletzungen eine Rolle spielten - mehr als jede andere Art vertraulicher Daten. Im Hinblick auf die Angriffsvektoren stellt E-Mail weiterhin ein großes Sicherheitsproblem für Unternehmen dar. Sie rangiert als Systemziel gleich hinter Webanwendungen und Desktop-Sharing-Lösungen. Darüber hinaus werden fast 60 % der Social-Engineering-Angriffe unter dem Deckmantel der Kompromittierung von geschäftlichen E-Mails durchgeführt.

Neben böswilligen Handlungen ist auch menschliches Versagen ein wichtiger Faktor bei der Offenlegung sensibler Inhalte. Verizon stellt fest, dass 43 % der Datenschutzverletzungen auf eine fehlerhafte Verbreitung von Daten zurückzuführen sind, wenn Daten versehentlich an die falsche Partei weitergegeben werden. Weitere 23 % der Vorfälle sind Fehler bei der Veröffentlichung, bei denen Daten an die falsche Zielgruppe weitergegeben werden.[3]

Ein schwindelerregendes Arsenal an Datenschutzbestimmungen

Diese Kosten für Unternehmen, Einzelpersonen und die Gesellschaft stehen im Mittelpunkt der Bemühungen der Regulierungsbehörden weltweit. Um Standards zu setzen, die Unternehmen einhalten müssen, haben die Regulierungsbehörden eine schnell wachsende Liste von Vorschriften erlassen, die alles von Datenschutz bis hin zu Cybersicherheitsstandards abdecken. Vielerorts haben sie diese Anforderungen sogar noch verschärft. Unternehmen, die in einem großen geografischen Gebiet tätig sind, stehen vor zwei Herausforderungen: Sie müssen Prozesse und Kontrollen zum Schutz sensibler Daten implementieren und dies in einer Weise tun, die für die Aufsichtsbehörden in einem Flickenteppich von Rechtsordnungen leicht überprüfbar ist.

Die Datenschutzgrundverordnung (DSGVO) der Europäischen Union, die 2018 in Kraft getreten ist, ist wahrscheinlich die weltweit strengste Regelung für personenbezogene Daten. Sie gilt für Personen in den 27 EU-Mitgliedstaaten und sieht bei Nichteinhaltung empfindliche Geldbußen vor. Doch die DSGVO ist bei weitem nicht die einzige wichtige nationale Datenschutzverordnung. Nach der letzten Zählung sind es 157 Länder - nur 15 Monate zuvor waren es 145 Länder.[4] Darunter befinden sich unter anderem große Volkswirtschaften wie Australien, Brasilien, Kanada, China, Indien und Japan.

In den USA gibt es zwar keine nationale Regelung wie die DSGVO, aber der Health Insurance Portability and Accountability Act (HIPAA) enthält strenge Anforderungen an den Schutz von Gesundheitsdaten. Und seit der Verabschiedung des California Consumer Privacy Act (CCPA) im Jahr 2018 haben die einzelnen US-Bundesstaaten ihre eigenen Vorschriften erlassen, was die Situation für in Nordamerika tätige Unternehmen noch frustrierender macht. Derzeit haben insgesamt neun Bundesstaaten Gesetze zum Schutz von Verbraucherdaten verabschiedet.[5] Die Gesetze von Virginia, Colorado, Utah und Connecticut werden in der zweiten Jahreshälfte 2023 in Kraft treten, während Indiana, Iowa, Montana und Tennessee ihre Gesetze zwischen 2024 und 2026 umsetzen werden. Darüber hinaus gibt es in 10 weiteren Staaten aktive Gesetzesentwürfe, die sich irgendwo im Gesetzgebungsverfahren befinden.

Ein weiterer Auslöser für zusätzliche Regulierungen für Unternehmen, die in den USA tätig sind, sind Geschäfte mit der Bundesregierung. In den letzten zehn Jahren hat das Federal Risk and Authorization Management Program (FedRAMP) die Cybersicherheitsverfahren für Cloud-Dienste für alle US-Regierungsbehörden und ihre Auftragnehmer standardisiert und zahlreiche Privatunternehmen seinen Anforderungen unterworfen. Und nach einem holprigen Start verlangt die Version 2.0 der Cybersecurity Maturity Model Certification (CMMC) nun von den mehr als 300.000 Mitgliedern der Defense Industrial Base (DIB), dass sie einen von drei Reifegraden erfüllen, je nachdem, welche Art von Arbeit sie für das US-amerikanische Verteidigungsministerium (DoD) verrichten. Das Ziel ist es, sowohl kontrollierte, nicht klassifizierte Informationen (Controlled Unclassified Information, CUI) als auch Bundesvertragsinformationen (Federal Contract Information, FCI) zu schützen.

Und dann sind da noch diese lästigen Frameworks und Standards!

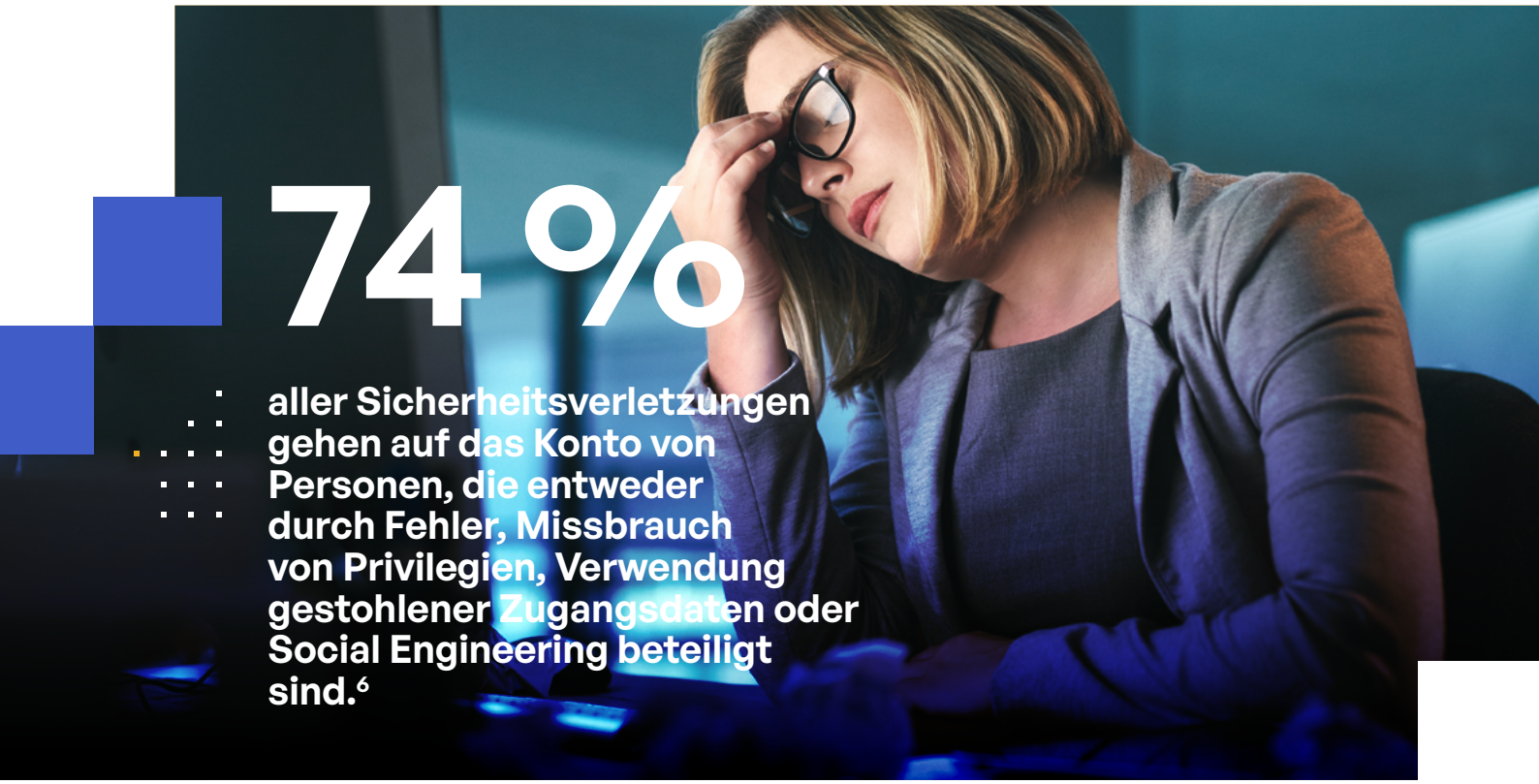
Neben den staatlichen Vorschriften werden die meisten Unternehmen heute anhand eines oder mehrerer Frameworks und Standards für Cybersicherheit geprüft. Die Einhaltung dieser Standards kann aufgrund der Art der Geschäftstätigkeit eines Unternehmens erforderlich sein, weil Anbieter von Cyber- und anderen Unternehmensversicherungen das Risikomanagement in ihre Zeichnungskriterien einbeziehen oder weil der Vorstand oder die Investoren auf der Einhaltung bestimmter bewährter Governance-Verfahren bestehen.

Unabhängig vom Grund kann die Nichteinhaltung des Payment Card Industry Data Security Standard (PCI DSS), des National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), der Standards der International Organization for Standardization (ISO) wie 27001, 27017 und 27018, der System and Organization Controls (SOC) des American Institute of Certified Public Accountants und anderer Standards für viele Unternehmen Konsequenzen haben.

Zahlreiche Schwierigkeiten bei der Bewertung und dem Management von Risiken bei der Kommunikation sensibler Inhalte

Wenngleich die Einhaltung einschlägiger Vorschriften und Rahmenbedingungen für den Geschäftserfolg von entscheidender Bedeutung ist, wissen Risikomanagementexperten, dass Strafen für die Nichteinhaltung von Vorschriften nur die Spitze des Eisbergs sind, wenn es um das mit sensiblen Inhalten verbundene Risiko für ein Unternehmen geht. Wie bei realen Eisbergen ist es sehr schwierig zu messen oder auch nur zu verstehen, was sich unter der Oberfläche dieser metaphorischen Eisberge befindet. Datenschutzverletzungen können den Ruf der Marke eines Unternehmens ernsthaft schädigen, sich negativ auf die Einnahmen auswirken und den Geschäftsbetrieb stören.

Ein Fazit lautet, dass Unternehmen die regulatorische Compliance als Untergrenze betrachten sollten, über der sie ihre Sicherheitsinfrastruktur und -verfahren für die Kommunikation sensibler Inhalte aufbauen - und nicht als Ziel an sich. Während Unternehmen in der Regel viel Energie und finanzielle Mittel in die Sicherheit von Netzwerken, Endgeräten, Anwendungen und Cloud-Infrastrukturen investieren, wird die Sicherheit von Inhalten, die zwischen Tausenden von Erst- und Drittparteien ausgetauscht werden, häufig vernachlässigt.



Methodik für diese Studie

Der Kiteworks Bericht über Datenschutz und Compliance für 2023 basiert auf einer umfassenden Befragung von 781 Fachleuten aus den Bereichen IT, Cybersicherheit sowie Risiko- und Compliance-Management. Wir geben das Feedback der Befragten für die gesamte Kohorte wieder, vergleichen es mit unseren Umfrageergebnissen von 2022 und analysieren es nach verschiedenen demografischen Details.

Ein sehr vielfältiger Pool von Befragten

Die Gruppe, die auf unsere Umfrage geantwortet hat, ist sehr vielfältig. Wir haben unsere Umfrage auf Mitarbeiter von Unternehmen mit mehr als 1.000 Mitarbeitern beschränkt (Abbildung 1). Tatsächlich vertritt fast die Hälfte der Befragten Unternehmen mit mehr als 15.000 Mitarbeitern, während 86 % mehr als 5.000 Mitarbeiter haben. Fast 3 von 10 Befragten kommen aus Europa, 14 % aus dem asiatisch-pazifischen Raum und 11 % aus dem Nahen Osten (Abbildung 2). Fast die Hälfte der Befragten kommt aus Nordamerika, davon 38 % aus den USA.

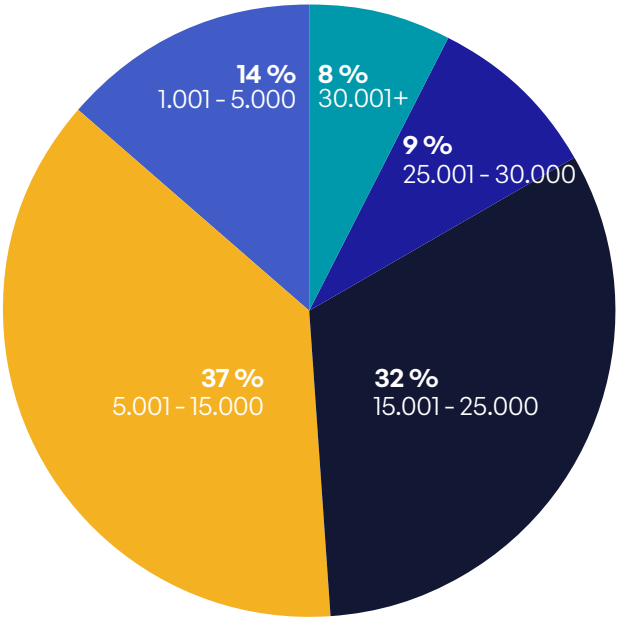


Abbildung 1: Größe des Unternehmens

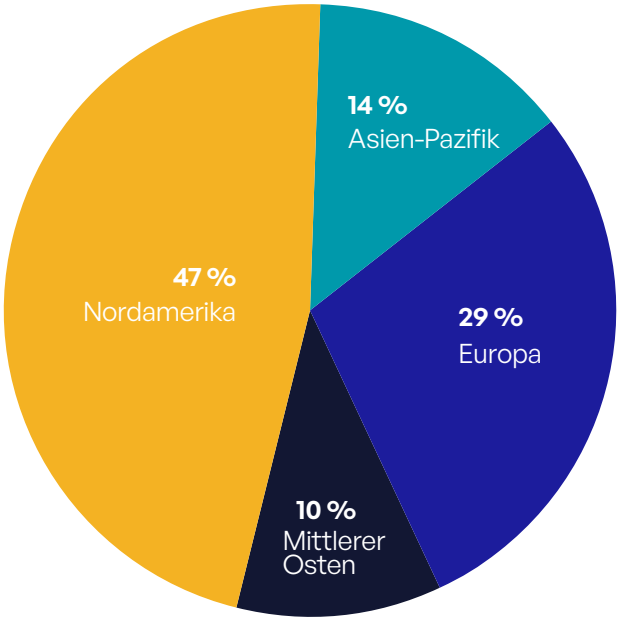


Abbildung 2: Hauptsitz des Unternehmens

Die Befragten kommen aus einer Vielzahl von Branchen (Abbildung 3), wobei Bundesbehörden, Sicherheits- und Verteidigungsunternehmen, Finanzdienstleister und Unternehmen aus dem Bereich Pharma/Biowissenschaften am stärksten vertreten sind. Unser Umfragepool umfasst ein ausgewogenes Verhältnis von Rollen und Ebenen innerhalb der Unternehmen (Abbildung 4). 45 % der Befragten sind im Bereich Risiko und Compliance tätig, der Rest ist im Bereich IT und Sicherheit angesiedelt. Die Kohorte ist auch ausgewogen zwischen der Führungsebene (47 %), dem mittleren Management (46 %) und den einzelnen Mitarbeitenden (7 %).

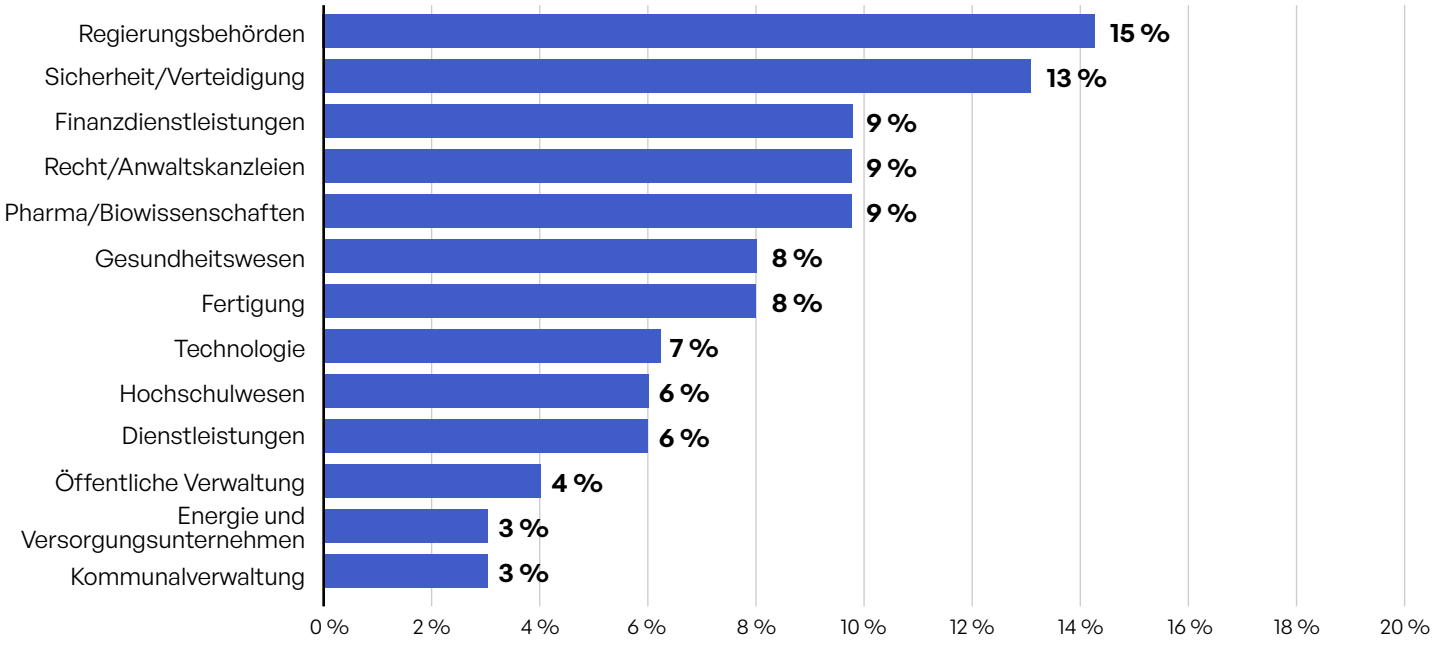


Abbildung 3: Branchen

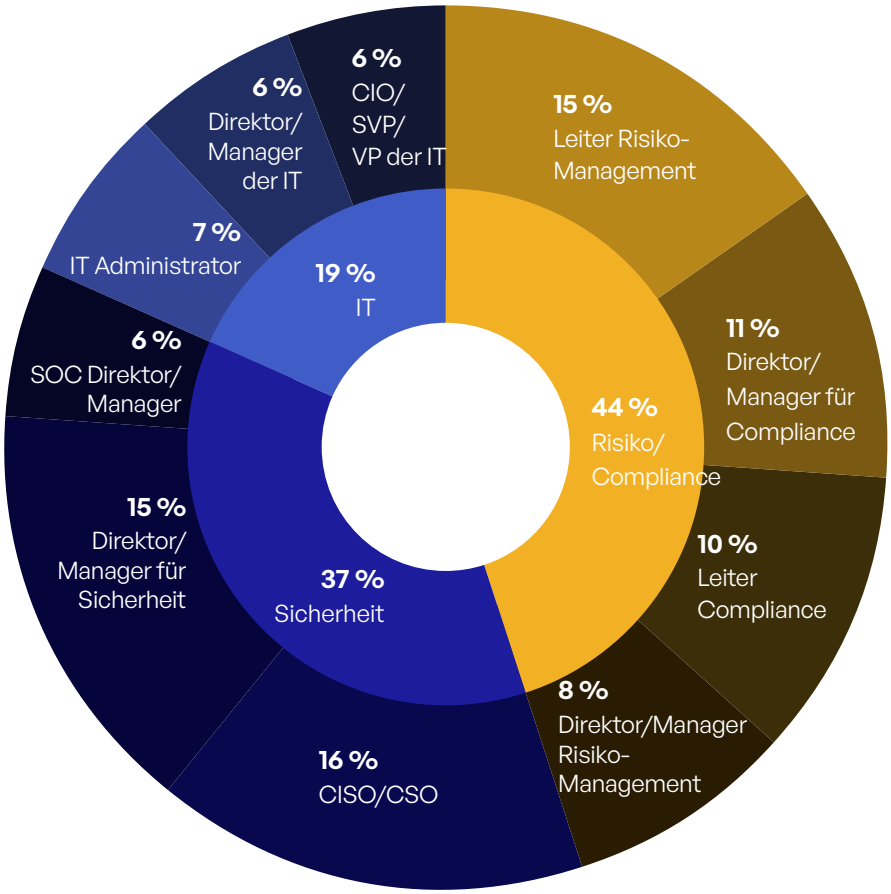


Abbildung 4: Berufsbezeichnung und Verantwortung des Befragten

Einblicke in den Datenschutz und die Compliance bei der Kommunikation sensibler Inhalte

Unsere Befragten beantworteten bereitwillig über 40 Fragen dazu, wie sie ihre Kommunikation mit sensiblen Inhalten verwalten und schützen. Das Ergebnis ist die Kombination aus jahrzehntelanger Erfahrung und unterschiedlichem Fachwissen. Bei der Auswertung der Umfrageergebnisse kristallisierten sich mehrere Bereiche mit klaren Erkenntnissen heraus:

Komplexität

Insight: Unternehmen tauschen Inhalte mit einer wachsenden Zahl von externen Parteien über verschiedene Kanäle aus, und das ist ein Problem

Wenn es eine Frage in unserer Umfrage gibt, die das Problem an der Wurzel packt, dann ist es die einfache Frage, mit wie vielen externen Parteien die Unternehmen Inhalte teilen. Ein Vergleich der Ergebnisse von 2022 und 2023 zeigt, dass sich das Problem verschärft. In diesem Jahr geben 90 % der Befragten an, dass sie Inhalte mit mehr als 1.000 externen Organisationen teilen, und 44 % geben an, dass diese Zahl über 2.500 liegt (Abbildung 5). Diese Zahlen sind deutlich höher als 2022, als 63 % mehr als 1.000 externe Parteien und ein Drittel mehr als 2.500 angaben.

Es überrascht nicht, dass größere Unternehmen insgesamt dazu tendieren, Inhalte mit mehr externen Parteien auszutauschen. 65 % der Unternehmen mit mehr als 30.000 Mitarbeitern tauschen Inhalte mit mehr als 5.000 externen Parteien aus. Aber selbst in kleineren Unternehmen (mit weniger als 5.000 Mitarbeitern) haben 93 % mehr als 1.000 externe Empfänger von Inhalten. Mehr als die Hälfte der Befragten in den Branchen Finanzdienstleistungen, Fertigung, Pharmazie/Biowissenschaften, Dienstleistungen sowie Sicherheit und Verteidigung gaben an, Inhalte mit mehr als 2.500 externen Parteien auszutauschen.

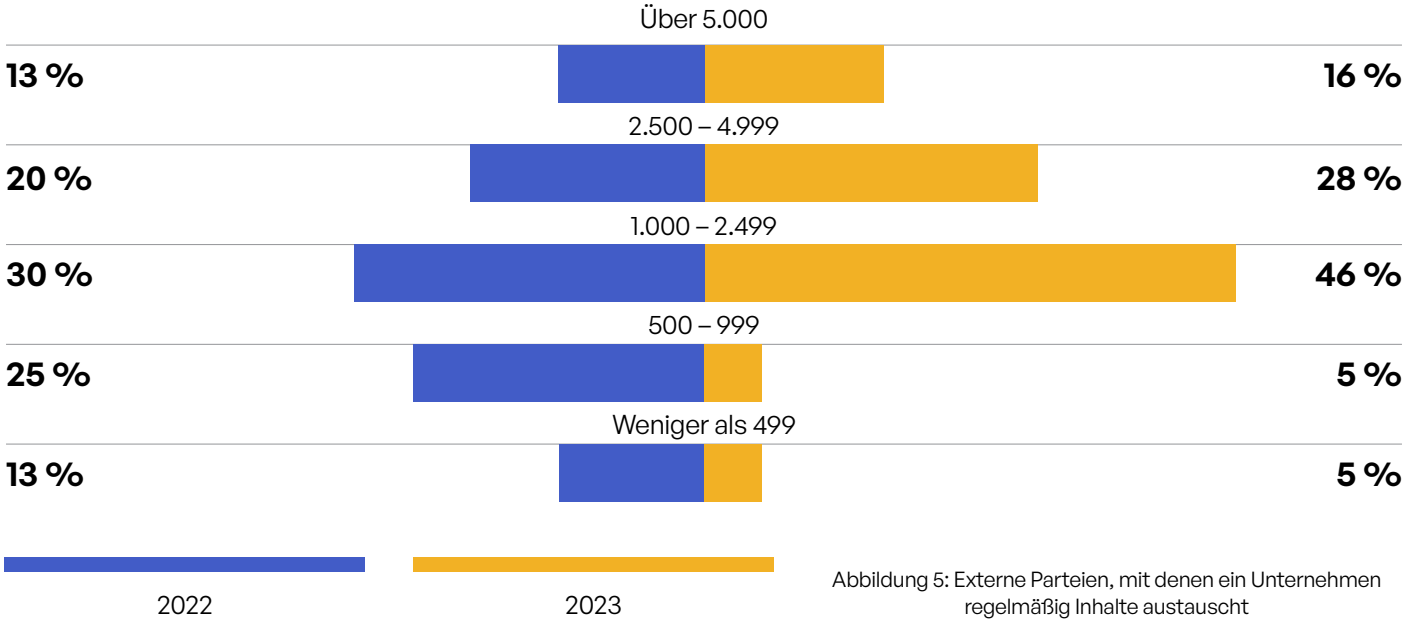


Abbildung 5: Externe Parteien, mit denen ein Unternehmen regelmäßig Inhalte austauscht

Ein umfangreiches Arsenal an Kommunikationskanälen

Das zweitwichtigste Element des Problems ist die Anzahl der Tools oder Kanäle, die für die Übertragung der Inhalte verwendet werden - eine Zahl, die in unserer Umfrage ebenfalls zunimmt. Im Jahr 2023 gibt die Hälfte der Befragten an, sechs oder mehr Tools für die Kommunikation sensibler Inhalte zu verwenden, und alle Befragten geben vier oder mehr Tools an (Abbildung 6). Im letzten Jahr nutzten "nur" zwei Drittel mehr als vier Tools und nur ein Viertel mehr als sechs! Das Spiel "Whac-A-Mole" ist also exponentiell schwieriger geworden.

Noch schlimmer ist die Situation bei den Finanzdienstleistern und im Gesundheitswesen, die über spezielle Anwendungen für die Übertragung von Inhalten verfügen. In diesen Branchen gaben weit mehr als zwei Drittel der Befragten an, mehr als sechs Tools für die Übertragung sensibler Inhalte zu verwenden. Auch die größten Unternehmen setzen überproportional viele Tools ein: 92 % der Unternehmen mit mehr als 30.000 Mitarbeitern nutzen sechs oder mehr Tools.

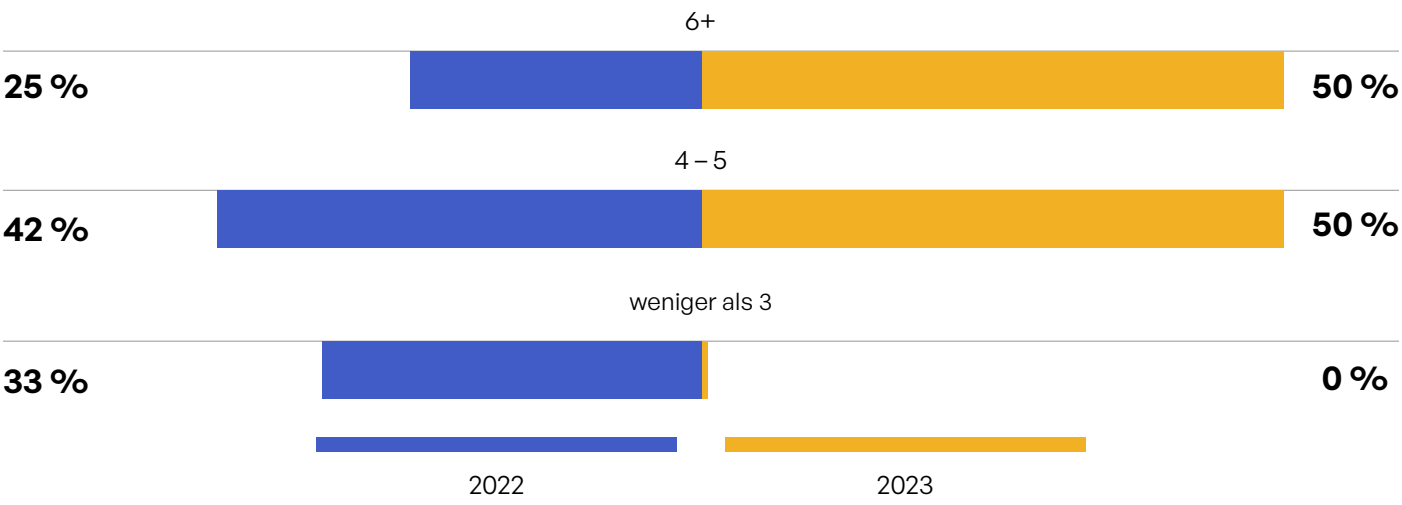


Abbildung 6: Tools / Systeme, die für die Kommunikation sensibler Inhalte verwendet werden

Enorme Komplikationen bei der Nachverfolgung und Kontrolle des Zugriffs auf Inhalte

Um auf die Metapher des Eisbergs zurückzukommen: Es ist keine Überraschung, dass es bei so vielen externen Partnern und so vielen Kanälen, über die Inhalte ausgetauscht werden, noch schwieriger ist, zu erkennen, was sich unter der Oberfläche befindet. Die Komplexität wird noch dadurch erhöht, dass Unternehmen mehrere Tools verwenden, um die Kommunikation mit Externen zu verfolgen, zu kontrollieren und zu schützen. Tatsächlich setzen 85 % vier oder mehr Systeme ein, 46 % sogar sechs oder mehr (Abbildung 7). Disaggregierte Datenquellen aus all diesen Tools erhöhen den Zeitaufwand der Mitarbeiter für die Erstellung von Sicherheitsberichten und Compliance-Nachweisen - und hinterlassen unweigerlich Lücken in der Transparenz.

Während sich viele der Maßnahmen zur Cybersicherheit nur indirekt auf das Endergebnis auswirken, sind die Kosten für diese Tool-Suppe ein separater Posten im Budget. Angesichts dieser Fülle an Lösungen überrascht es nicht, dass 69 % der Unternehmen mehr als 250.000 US-Dollar pro Jahr für Lizenzen ausgeben (Abbildung 8). Mehr als ein Viertel der Unternehmen aus den Bereichen Hochschulen und Pharma/Biowissenschaften geben mehr als 500.000 US-Dollar aus, während weit über die Hälfte (57 %) der Finanzdienstleister mehr als 350.000 US-Dollar aufwenden.

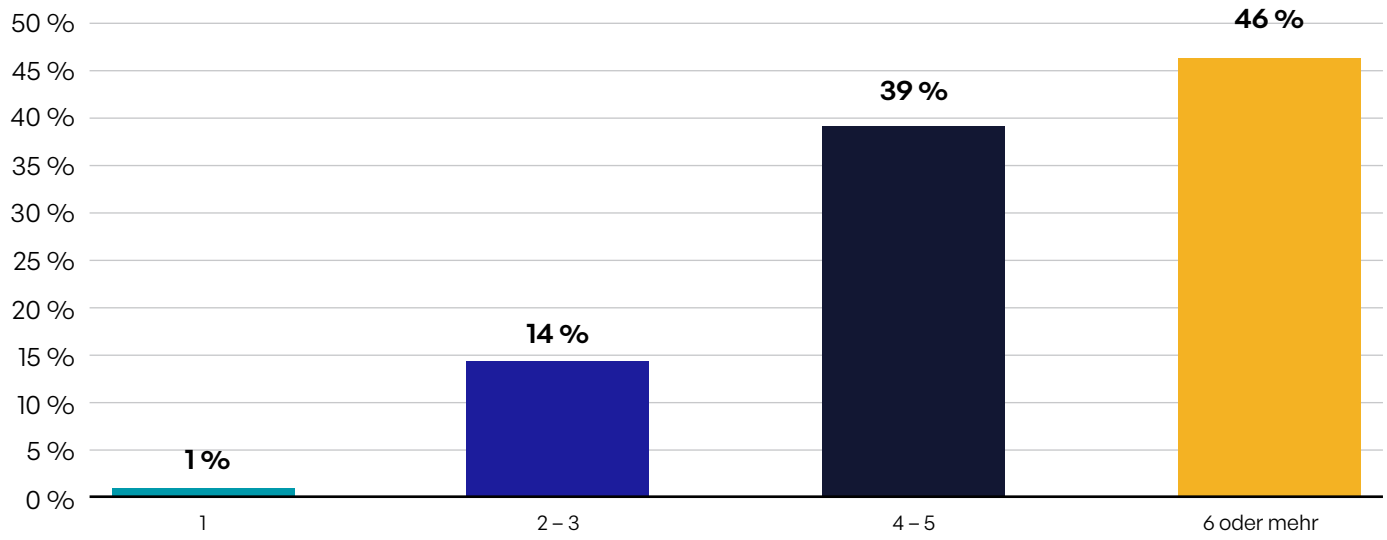


Abbildung 7: Systeme und Tools zur Nachverfolgung, Kontrolle und zum Schutz der Inhaltskommunikation mit externen Parteien

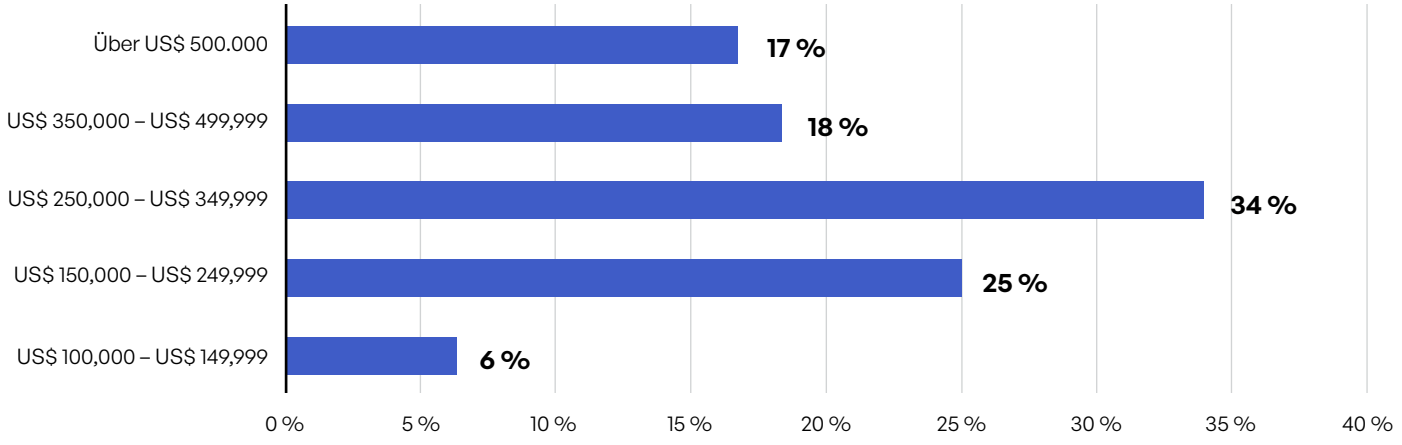


Abbildung 8: Jährliche Lizenzkosten für Tools und Systeme zur Kommunikation von Inhalten

So viele organisatorische Prioritäten!

Wenn man den Befragten acht wichtige Aspekte der sicheren Kommunikation von Inhalten vorlegt und sie bittet, die vier wichtigsten in eine Rangfolge zu bringen, fallen die Antworten sehr unterschiedlich aus. Das ist nicht unbedingt schlecht, denn alle acht sind wichtige Prioritäten, die jedes Unternehmen in einer anderen Reihenfolge erreichen kann.

Als wir die Antworten gewichteten, um den höheren Rängen mehr Punkte zuzuweisen[7], kristallisierten sich zwei Prioritäten heraus: Nachverfolgung von Inhaltsberechtigungen, Ablauf, Sperrung und Versionierung sowie Vereinheitlichung von Verwaltung, Nachverfolgung, Richtlinien und Berichterstattung (Abbildung 9). An dritter Stelle steht der Schutz von Inhalten, die sich in Bewegung befinden - eine wichtige Priorität, wenn sensible Inhalte intern und extern so weit verbreitet sind.

Es überrascht nicht, dass eDiscovery in Anwaltskanzleien (21 %) und im Gesundheitswesen (23 %) mehr Antworten erhielt. Die Nachverfolgung von Zugriffsrechten auf Inhalte war in Behörden (29 %) und bei professionellen Dienstleistern (20 %) ein wichtigeres Thema. Die Vereinheitlichung aller Systeme war eine Priorität in Sicherheits- und Verteidigungsunternehmen (29 %). Unabhängig von der unmittelbaren Priorität in den einzelnen Unternehmen sind alle acht Prioritäten sehr wichtig für die Kommunikation sensibler Inhalte.

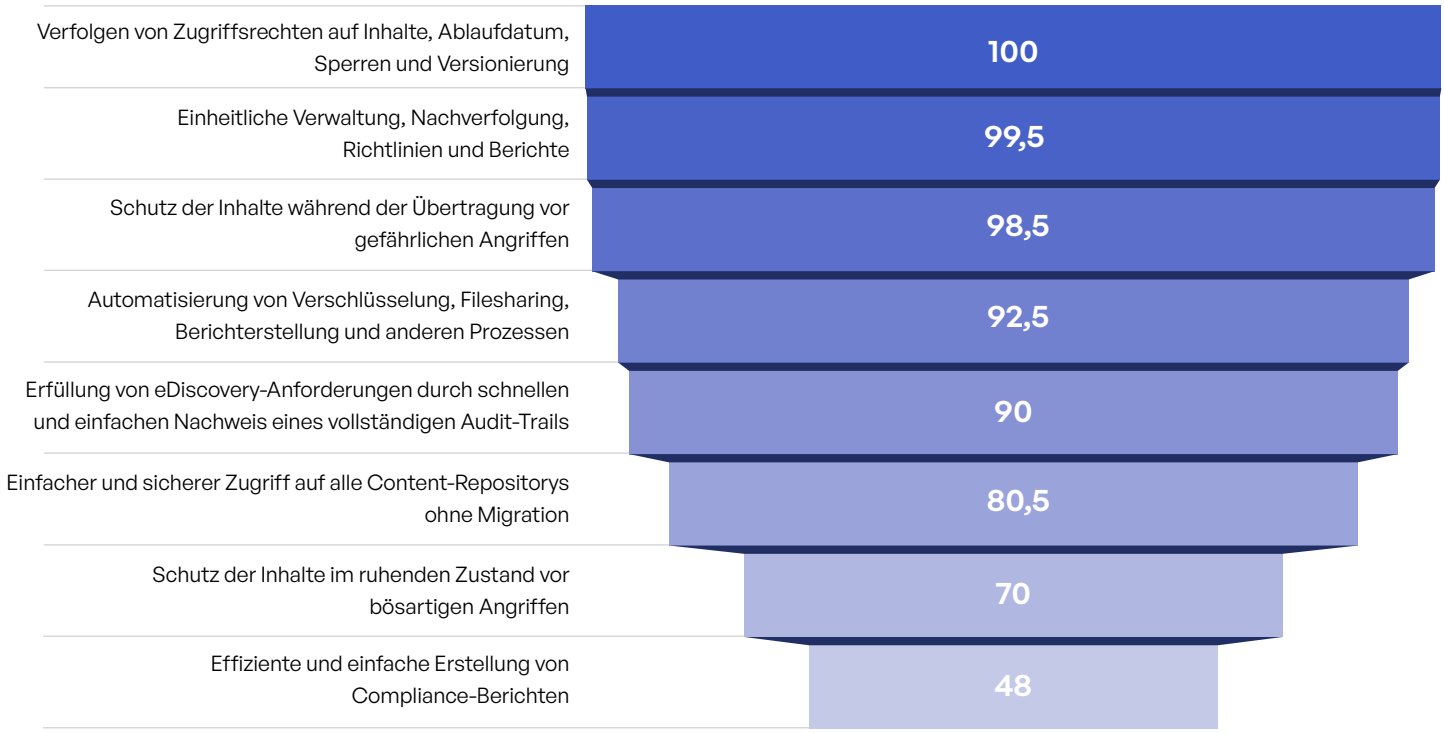


Abbildung 9: Gewichtete Punktzahl: Top-Prioritäten für die Kommunikation sensibler Inhalte (Reihenfolge der Top 4)

Gestohlene oder kompromittierte Zugangsdaten waren nicht nur der häufigste Grund für eine Datenschutzverletzung, sondern es dauerte mit 327 Tagen auch am längsten, sie zu identifizieren.[8]

Sicherheitsrisiko

Insight: Die Sicherheit der Kommunikation mit sensiblen Inhalten ist keine nachträglich zu lösende Aufgabe

Lassen Sie uns für einen Moment einen Blick auf das Risikomanagement werfen und Sie mitnehmen auf eine Tour durch zwei verschiedene Arten von Risiken, wenn es um die Kommunikation sensibler Inhalte geht - das Sicherheitsrisiko und das Compliance-Risiko. Wie bereits erwähnt, sollte Compliance als Mindestanforderung betrachtet werden, und Unternehmen sollten über die reine Erfüllung gesetzlicher Vorgaben hinausgehen, um das allgemeine Sicherheitsrisiko anzugehen.

Unabhängig von dieser Unterscheidung umfasst die Minderung beider Risikobereiche zwei Komponenten - die Bemessung des Risikos und dessen Management. Wie ein altes Sprichwort sagt: “Was gemessen wird, kann verbessert werden”. Leider ist es so, dass wenn es um die Bemessung und das Management von Sicherheit geht, ist sich unsere Kohorte im Großen und Ganzen bewusst, dass Verbesserungen notwendig sind. Nur knapp ein Viertel der Befragten gibt an, dass in ihrem Unternehmen in diesen beiden Bereichen kein Verbesserungsbedarf besteht (Abbildung 10). Interessanterweise ist ein höherer Prozentsatz (37 %) der Meinung, dass beim Sicherheitsmanagement noch größere Verbesserungen notwendig sind als bei der Sicherheitsbewertung (29 %).

Die Energie- und Versorgungsunternehmen sind wesentlich zuversichtlicher, was ihre Messverfahren betrifft: 52 % geben an, dass keine Verbesserungen erforderlich sind (Abbildung 11). Gleichzeitig sind 44 % der befragten Kommunalverwaltungen der Meinung, dass ihre Messmethoden erheblich verbessert werden müssen, während 46 % der Regierungsbehörden der Meinung sind, dass keine Verbesserungen erforderlich sind. In Bezug auf das Management sind die Kommunen bei weitem am zuversichtlichsten, da 52 % angeben, dass keine Verbesserungen erforderlich sind (Abbildung 12) - trotz ihres mangelnden Vertrauens in ihre Sicherheitsmessungen.

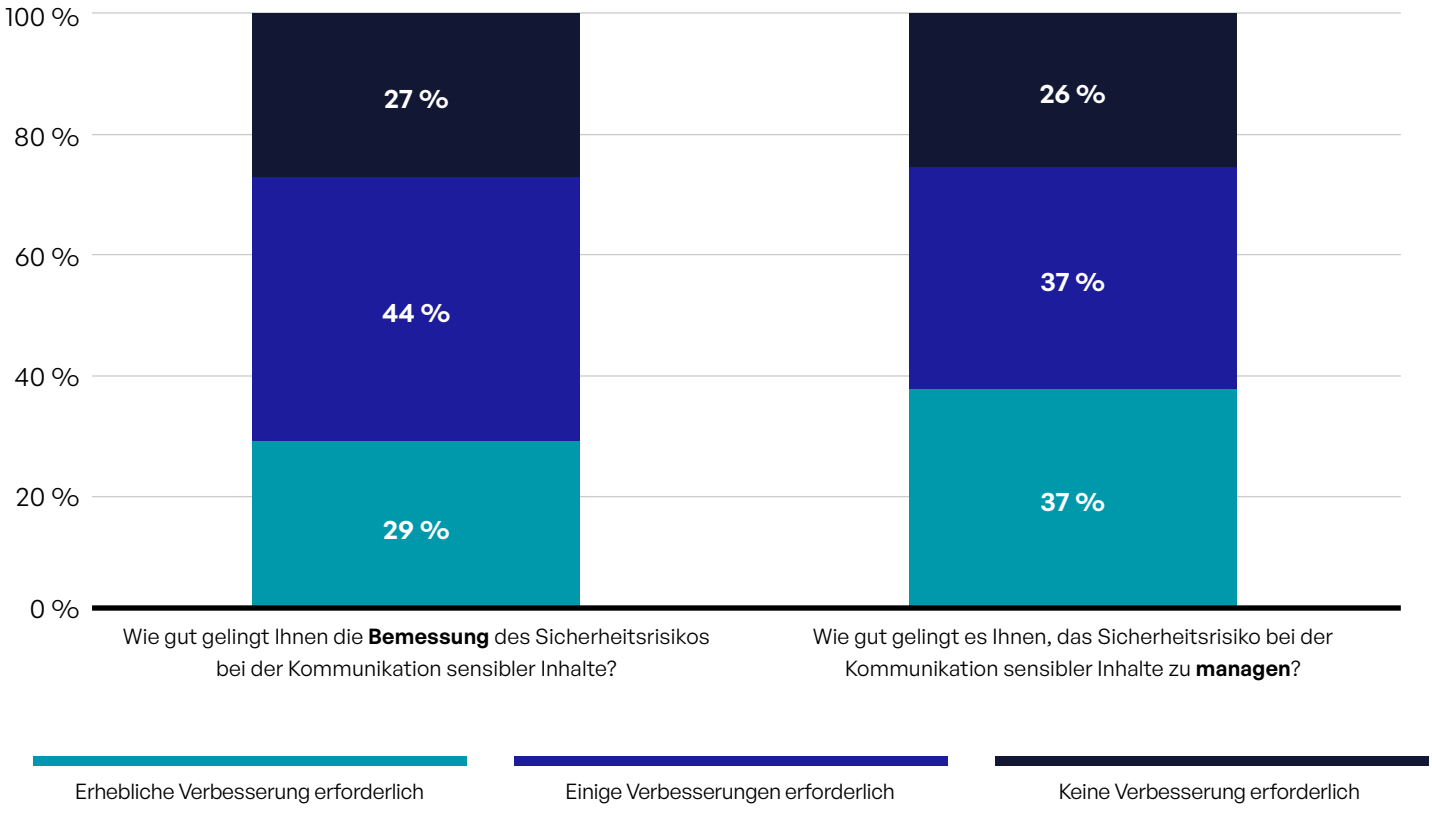


Abbildung 10: Reifegrad der Organisation bei der Bemessung und Verwaltung von Sicherheitsrisiken

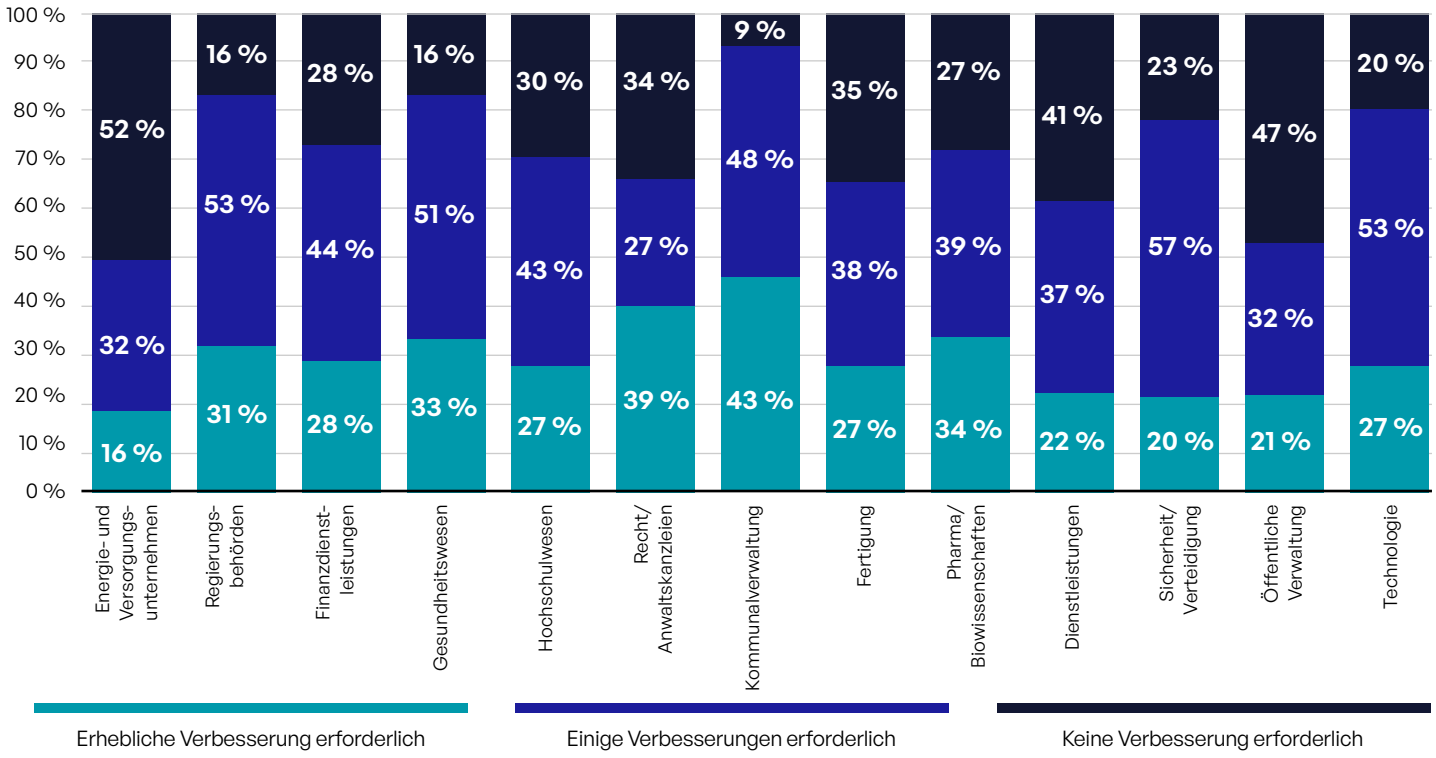


Abbildung 11: Bemessung des Sicherheitsrisikos für die Kommunikation sensibler Inhalte

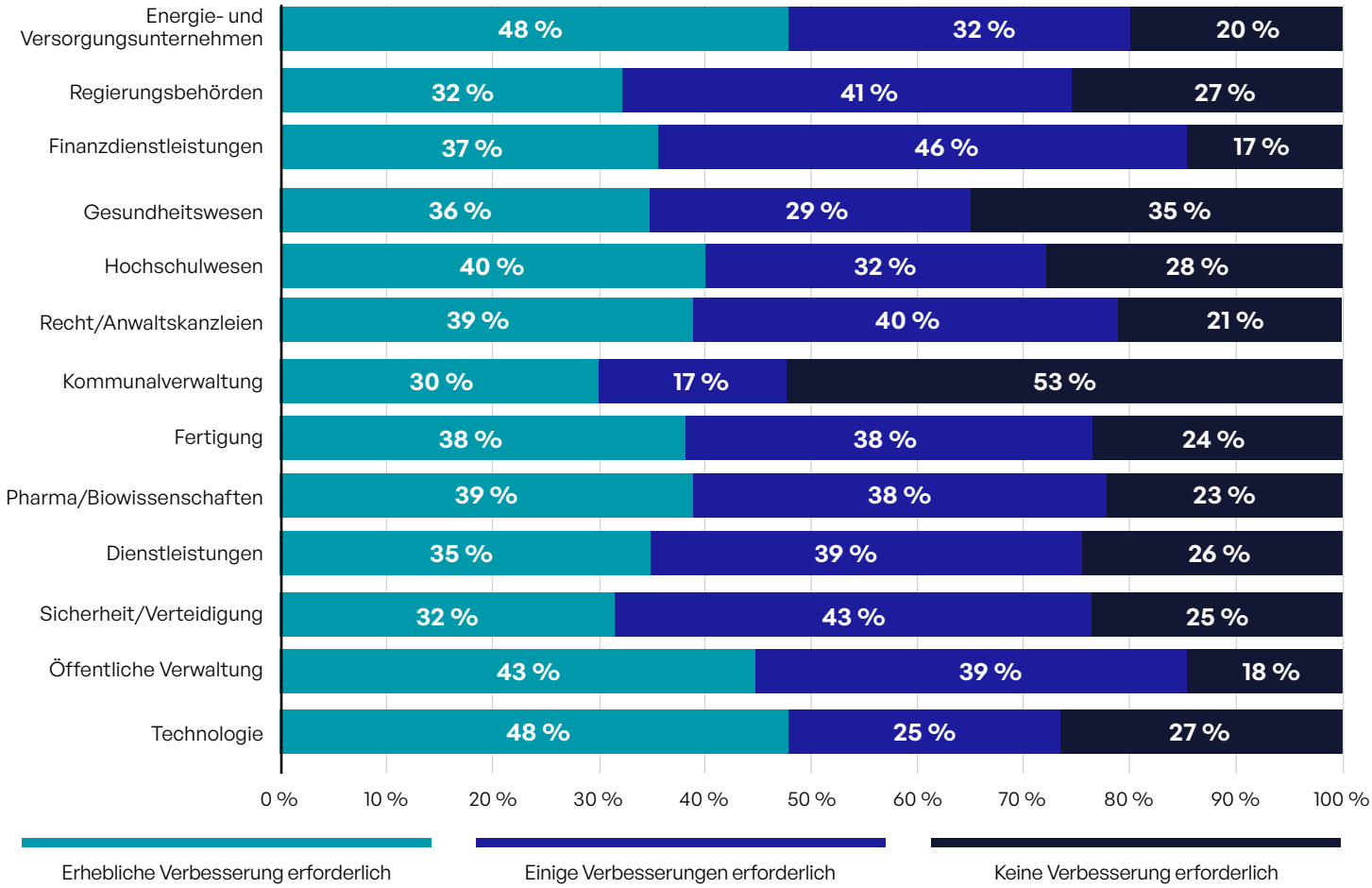


Abbildung 12: Management des Sicherheitsrisikos für die Kommunikation sensibler Inhalte

Mit jedem Kanal steigt das Risiko!

Wir sind sicher, dass jeder schockiert sein wird, wenn er erfährt, dass die E-Mail bei der Risikowahrnehmung im Vergleich zu anderen Kanälen für die Kommunikation von Inhalten klar führend ist: Jeder Fünfte stuft sie auf Platz 1 ein und zwei Drittel auf Platz 4 (Abbildung 13). Dennoch wird die E-Mail im Jahr 2023 als weniger riskant eingestuft als im Jahr 2022, als alle Befragten sie unter den ersten vier und 30 % sie auf Platz 1 einstuften. Filesharing-, File-Transfer- und Automatisierungs-Tools wurden im letzten Jahr ebenfalls als viel riskanter eingestuft. Mehr als 95 % der Befragten stuften sie 2022 unter den Top vier ein, verglichen mit 58 % bzw. 46 % im Jahr 2023.

Da es sich um eine Frage der Rangfolge handelt, ist der Grund für die etwas niedrigere Einstufung dieser bekannten Risiken zum Teil auf das gestiegene Risikoprofil neu aufkommender Kommunikationskanäle für Inhalte wie Programmierschnittstellen (APIs), Textnachrichten und mobile Anwendungen zurückzuführen, deren wahrgenommenes Risiko im Vergleich zum Vorjahr exponentiell gestiegen ist. Der Austausch von Inhalten über Chat wurde dieses Jahr neu in die Umfrage aufgenommen und zählt mit 37 % zu den vier größten Risiken.

Filesharing-Dienste werden vor allem in der Energie- und Versorgungswirtschaft als großes Risiko angesehen (mit 32 % auf Platz 1), während Webformulare (25 %) in der Finanzdienstleistungsbranche an erster Stelle stehen. E-Mails werden von Unternehmen in den Bereichen Technologie, Sicherheit und Verteidigung als noch größeres Risiko angesehen: mit 32 % in beiden Branchen nimmt dies den ersten Platz ein.

Unabhängig davon, welche Bedeutung die Befragten den einzelnen Kanälen beimessen, dürfen die Unternehmen nicht nachlässig sein. So wurde in jüngster Zeit eine Reihe von Hackerangriffen auf Managed File Transfer (MFT)-Tools bekannt, die zum Diebstahl sensibler Daten geführt haben.[9]

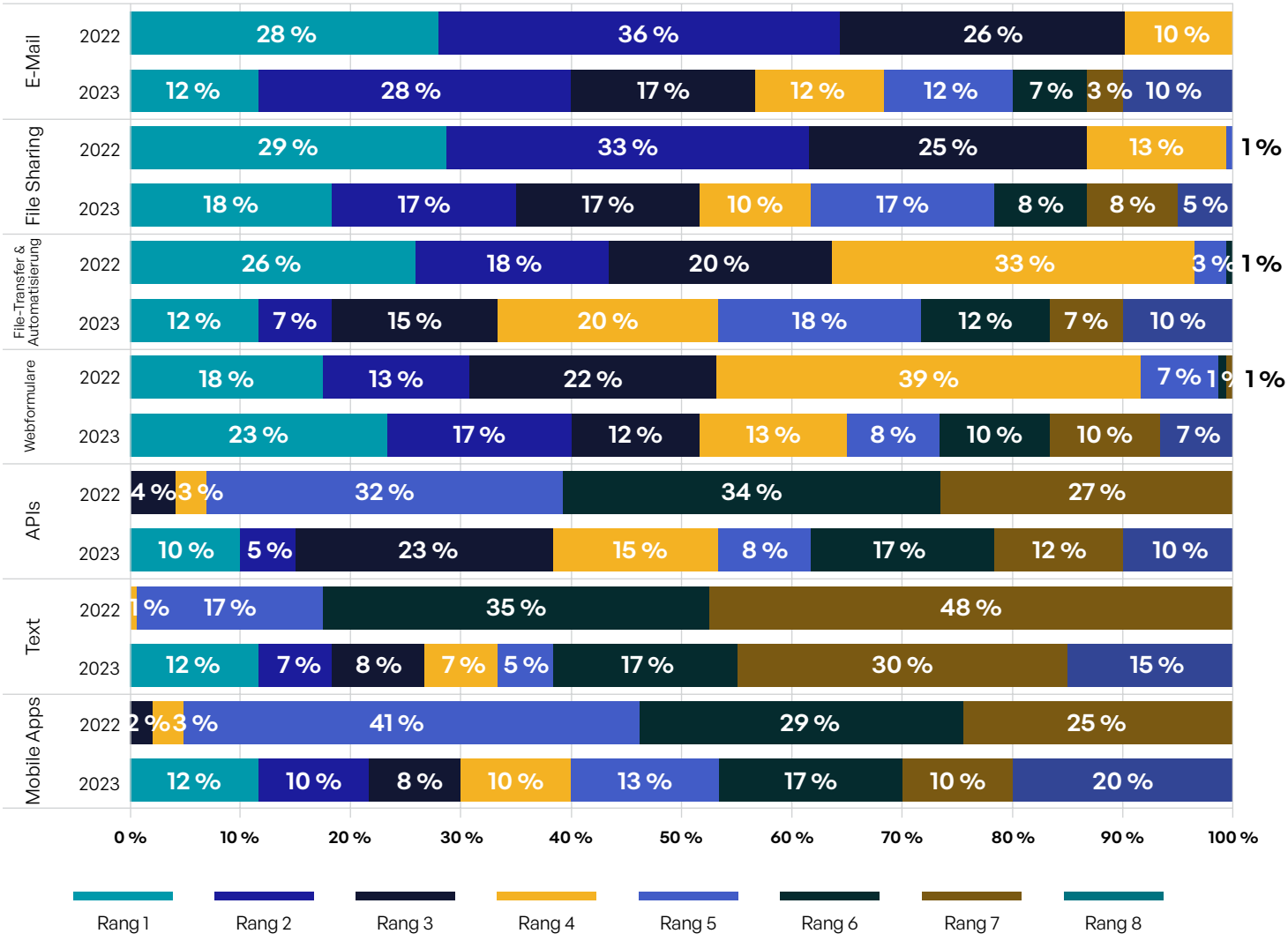


Abbildung 13: Kommunikationskanäle, die das höchste Risiko bergen

Zu viele Angriffsmethoden - zu wenig Schlaf

Bei der Frage nach den drei größten Bedrohungen aus einer Liste von 13 möglichen Angriffsvektoren und -taktiken fällt auf, dass jeder Punkt der Liste von mindestens 9 % der Befragten an erster, zweiter oder dritter Stelle genannt wird. Werden die Antworten jedoch gewichtet, um den höheren Rängen mehr Gewicht zu verleihen, so liegt der Diebstahl von Passwörtern oder Anmeldedaten weit vor den anderen Taktiken (Abbildung 14) und ist mit 34 % der Befragten die mit Abstand am häufigsten genannte Taktik unter den ersten drei. Rootkits und die Manipulation von URLs wurden jedoch am häufigsten genannt.

Bemerkenswert ist, dass sich die beiden größten Sicherheitsbedenken auf den Menschen beziehen. Unabhängig davon, ob die Befragten befürchten, dass Angreifer sich Zugang verschaffen, indem sie sich als interner Benutzer oder als Kundenkonto ausgeben, sind die Angriffsmethoden dieselben - und alle haben mit menschlichem Versagen zu tun.

Einige Methoden zur Erlangung von Nutzerdaten beinhalten die aktive Manipulation eines ahnungslosen Nutzers durch einen Social-Engineering-Angriff. Die häufigste Art dieser Angriffe ist die URL-Manipulation: Dem Benutzer wird vorgegaukelt, er befinde sich auf einer bestimmten legitimen Website, indem ihm eine URL präsentiert wird, die der tatsächlichen URL sehr ähnlich, aber nicht mit ihr identisch ist.

Andere Angriffsvektoren sind weniger direkt und beruhen eher auf menschlicher Berechenbarkeit. Benutzer neigen dazu, dieselben oder sehr ähnliche Passwörter für mehrere Systeme zu verwenden. Wenn ein Angreifer ein Passwort kennt, ist die Wahrscheinlichkeit hoch, dass er auch die anderen erraten kann. Aus diesem Grund ist die Durchsetzung einer angemessenen Passwortrichtlinie zusammen mit einer angemessenen und konsequenten Schulung der Benutzer eines der besten Mittel gegen die häufigsten Angriffe.

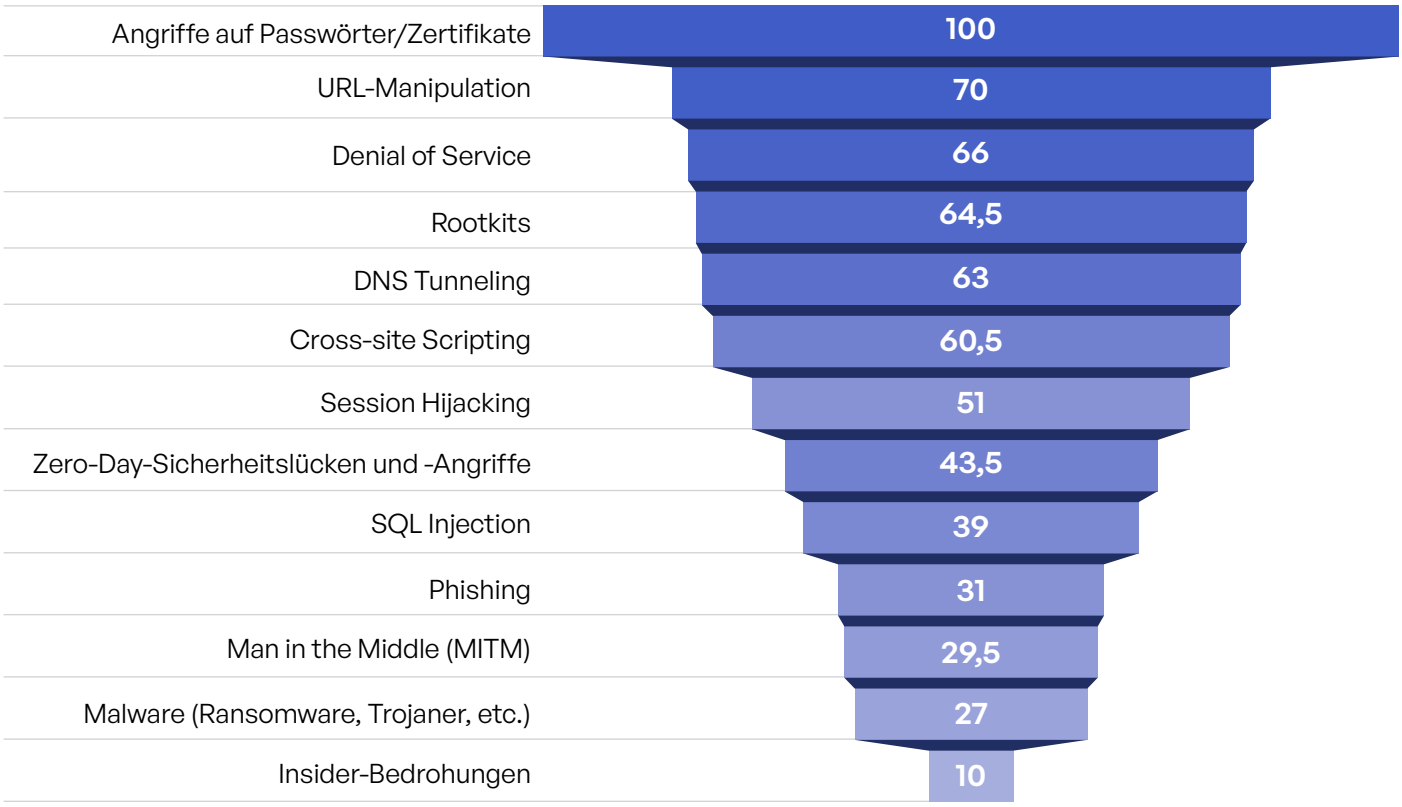


Abbildung 14: Gewichtete Bewertungen: Die wichtigsten Angriffsvektoren für die Kommunikation sensibler Inhalte

Mehr Datentypen, höheres Risiko

Bei der Einstufung von sechs verschiedenen Arten sensibler Inhalte nach dem Risiko, das sie für das Unternehmen darstellen, variieren die Antworten. Für mehr als die Hälfte der Befragten rangieren personenbezogene Daten, vertrauliche Patienteninformationen und juristische Dokumente auf den ersten drei Plätzen (Abbildung 15). Die regionalen Unterschiede sind nicht überraschend: In Europa und im asiatisch-pazifischen Raum, der Heimat der DSGVO und ähnlicher Gesetze in Asien / Pazifik, werden personenbezogene Daten höher bewertet. In Nordamerika wird mehr auf Patienteninformationen (PHI) geachtet, wo HIPAA eine wichtige Compliance-Anforderung ist. Interessanterweise wird geistiges Eigentum im Nahen Osten viel stärker als Risiko wahrgenommen. 60 % der Befragten zählen es zu den drei größten Risiken.

Die meisten Abweichungen nach Branchen sind ebenfalls nicht überraschend - oder zumindest verständlich:

- Größere Besorgnis über juristische Dokumente bei Finanzdienstleistungen, im Hochschulwesen und im Gesundheitswesen
- Mehr Gewicht auf Fusionen und Übernahmen in Anwaltskanzleien, freiberuflichen Dienstleistungen und Unternehmen im Bereich Pharma-/Biowissenschaften
- Mehr Nennungen von Finanzdokumenten in der Kommunalverwaltung
- Mehr Gewicht auf vertrauliche Patientendaten in Energie- und Versorgungsunternehmen sowie in Bundesbehörden - aber nicht im Gesundheitswesen, wo man den Schutz vermutlich besser im Griff hat

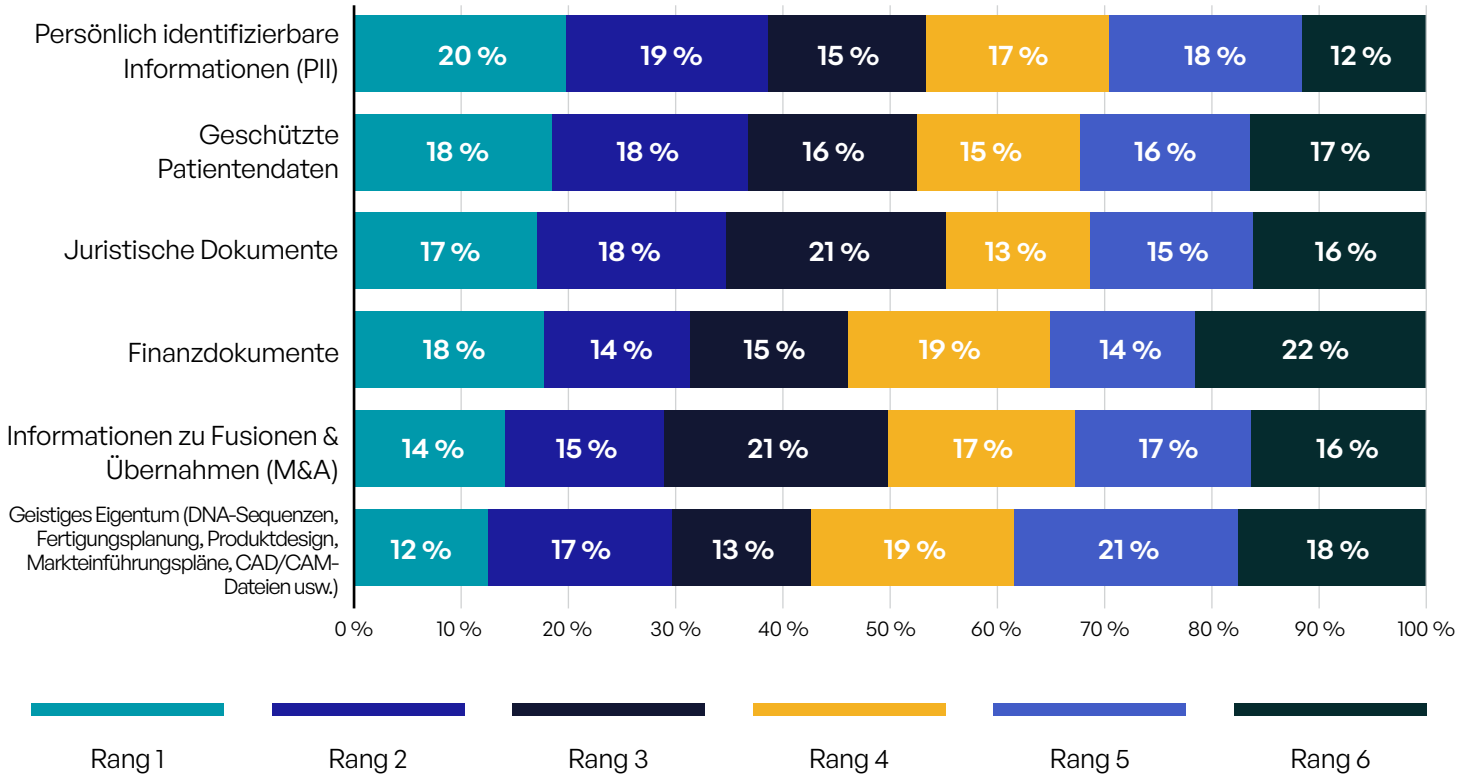


Abbildung 15: Sicherheits- und Compliance-Risiken nach Art der sensiblen Daten

Multitenant-Hosting-Infrastruktur macht es noch schwieriger

Multi-Tenant-Hosting-Lösungen sind eine kostengünstige Möglichkeit für den Zugang zu Cloud-basierten Diensten und erfreuen sich großer Beliebtheit. Bei diesem Modell teilen sich mehrere Organisationen dieselbe(n) virtuelle(n) Maschine(n), wenn sie auf eine bestimmte Anwendung oder Infrastruktur von einem Cloud Service Provider zugreifen. Natürlich bedeutet die Segmentierung theoretisch, dass die Unternehmen keinen Zugriff auf die Daten der anderen haben - aber es besteht das Risiko, dass etwas schief geht, wenn es zu einem Einbruch kommt. Dieses Risiko ist unseren sehr vorausschauenden Befragten nicht entgangen. 99 % von ihnen nennen das Risiko der Mandantenfähigkeit als Problem (Abbildung 16).

Eine beträchtliche Anzahl der Befragten nannte alle drei Gründe, aus denen Multi-Tenant-Hosting-Lösungen ein Risiko darstellen. Die am häufigsten genannte Sorge ist jedoch, dass sich ein Angreifer seitlich bewegen kann, sobald er in die Infrastruktur eines Mandanten eingedrungen ist. Die Befragten aus dem asiatisch-pazifischen Raum sind etwas besorgter darüber, dass ein Hacker eine Cloud-Instanz einer Anwendung übernehmen, eine Sandbox einrichten und Schwachstellen identifizieren könnte, die dann ausgenutzt werden könnten (36 % gegenüber 32 % in der gesamten Kohorte).

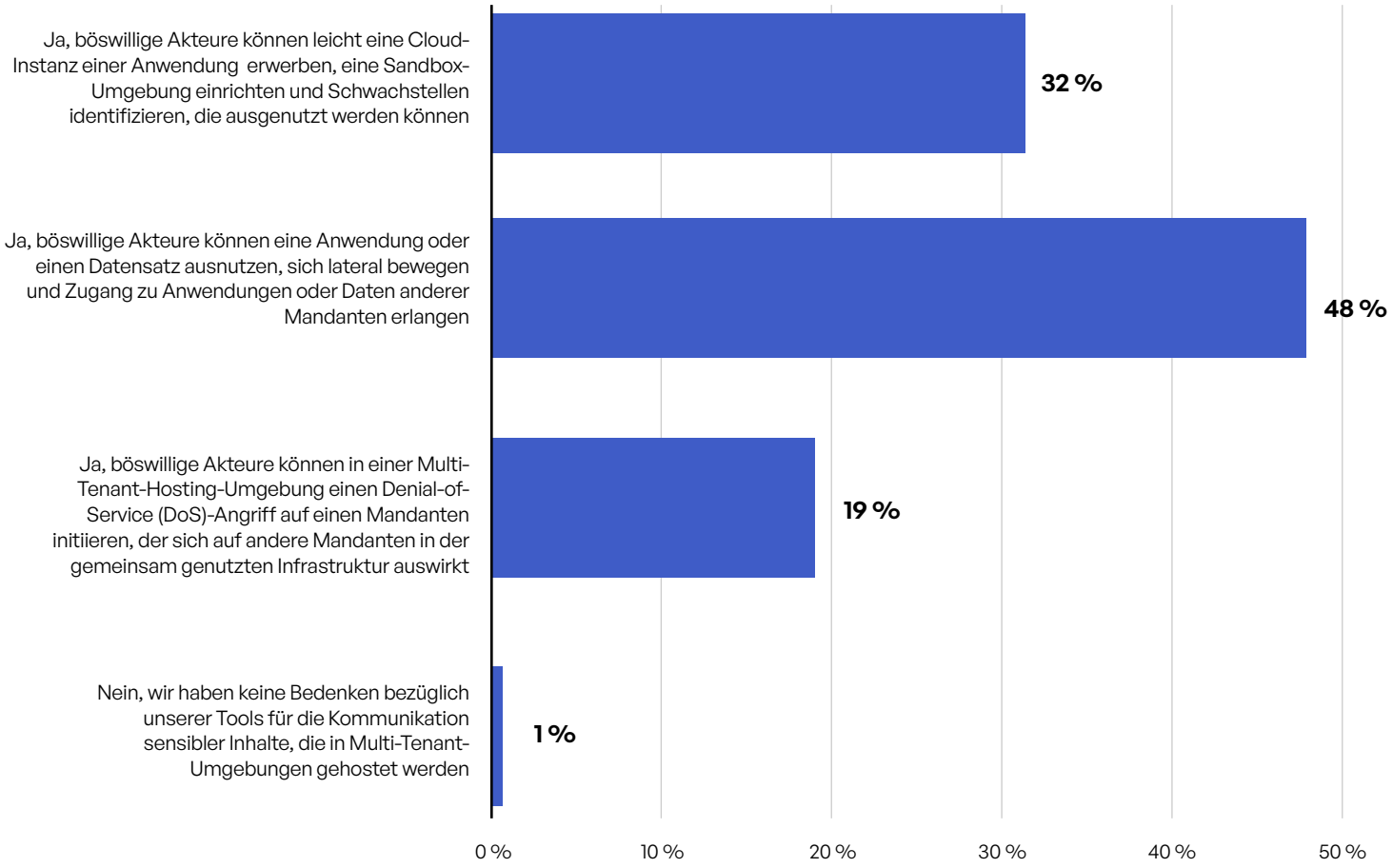


Abbildung 16: Sicherheitsbedenken in Bezug auf das Multi-Tenant-Hosting von Kommunikations-Tools

Raus aus dem “Hamsterrad”, um über Strategien zu sprechen

Nachdem eine Reihe spezifischer Fragen zum Thema Sicherheitsrisiko beantwortet wurden, möchten wir nun von der taktischen zur strategischen Ebene übergehen. Eine Priorität bei der Verbesserung der Sicherheitslage eines Unternehmens in einem bestimmten Bereich besteht darin, sicherzustellen, dass diese Bemühungen mit der allgemeinen Risikomanagementstrategie des Unternehmens übereinstimmen, einschließlich der Bemessung und des Managements. Auf die Frage nach dem Stand dieser Anpassung gaben 28 % der Befragten an, dass die Anpassung bereits abgeschlossen sei, während 47 % angaben, dass sie im Gange sei und voraussichtlich in den nächsten 12 Monaten abgeschlossen sein werde (Abbildung 17). Weitere 22 % sehen in der Anpassung eine Priorität für das kommende Jahr.

Einige Branchen sind weiter als andere. Regierungsbehörden (57 %), Anwaltskanzleien (52 %) und Energie- und Versorgungsunternehmen (44 %) geben eher an, dass die Anpassung abgeschlossen ist, während Pharma/Biowissenschaften (13 %), Finanzdienstleistungen (16 %) und Hochschulen (21 %) dies seltener bestätigen.

Auf die Frage, wie zufrieden sie insgesamt mit dem Risikomanagement ihres Unternehmens in Bezug auf die Kommunikation mit externen Parteien sind, geben 84 % der Befragten an, dass zumindest einige Verbesserungen erforderlich sind (Abbildung 18). Mehr als 4 von 10 Befragten sind der Meinung, dass erhebliche Verbesserungen notwendig sind - oder sogar, dass man das Kind mit dem Bade ausschütten und ganz von vorne anfangen sollte.

Es ist vielleicht ermutigend zu sehen, dass ein geringerer Prozentsatz der Befragten im Jahr 2023 einen völlig neuen Ansatz für notwendig hält als im Jahr 2022. Obwohl immer noch mehr Befragte der Meinung sind, dass erhebliche Verbesserungen erforderlich sind, könnte dies einen schrittweisen Fortschritt bedeuten. Leider sind in drei Sektoren - Hochschulwesen, Anwaltskanzleien und Technologie - mehr als die Hälfte der Befragten der Ansicht, dass erhebliche Verbesserungen erforderlich sind. Mehr als die Hälfte der europäischen Befragten teilt diese Ansicht.

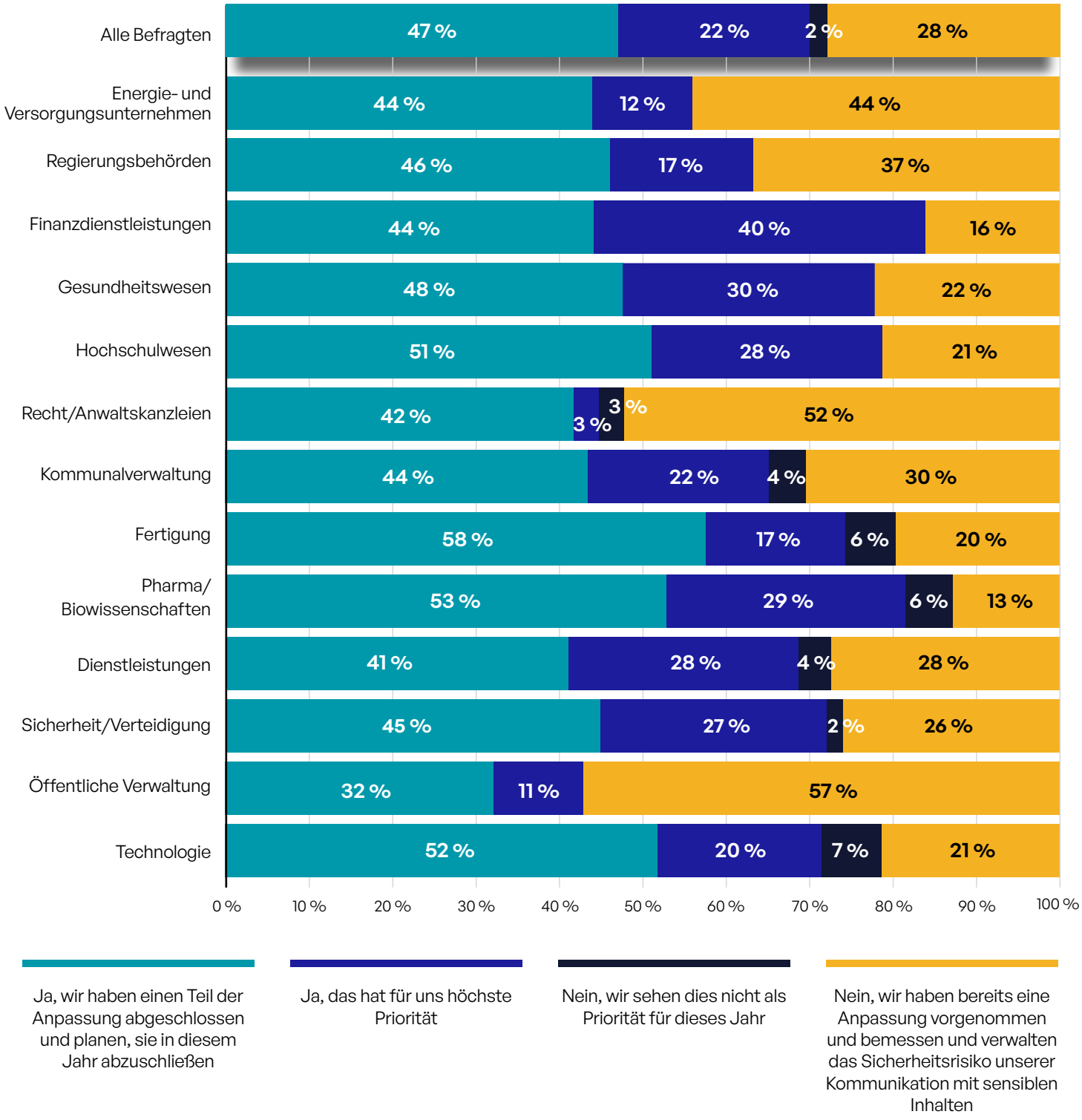


Abbildung 17: Die Anpassung der Risikomanagementstrategie im Hinblick auf die Bemessung und das Management der Risiken bei der Kommunikation sensibler Inhalte ist eine Priorität für das Jahr 2023

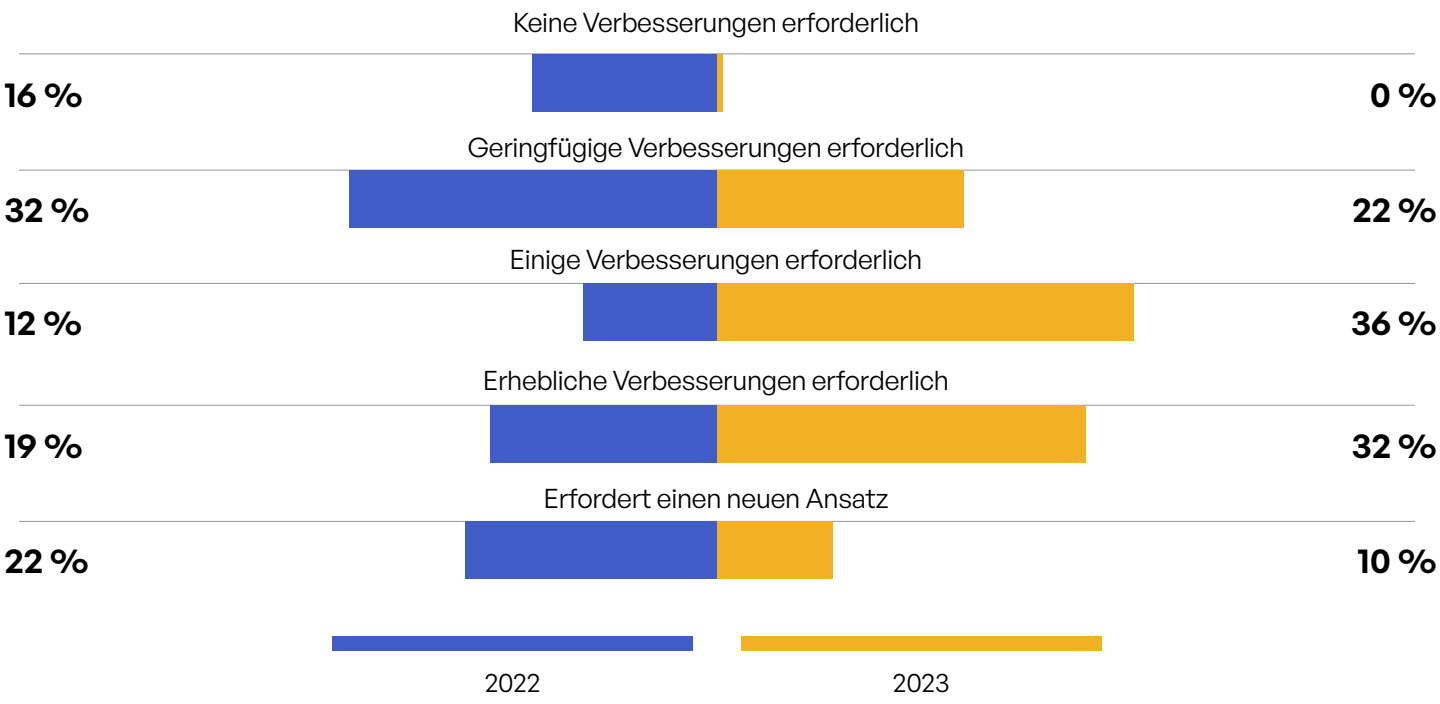


Abbildung 18: Grad der Zufriedenheit mit dem Risikomanagement in Bezug auf die Kommunikation mit externen Parteien

Compliance-Risiko

Insight: Zunehmende Compliance-Anforderungen zwingen Unternehmen zum Handeln

Der andere Risikobereich im Zusammenhang mit der Kommunikation sensibler Inhalte dreht sich um Compliance - ein Wort, das viele mit staatlichen Vorschriften in Verbindung bringen. Und davon gibt es sicherlich eine ganze Menge - vor allem für globale Unternehmen, die in vielen Ländern tätig sind.

Gesetze und Vorschriften sind jedoch nicht die einzigen Compliance-Anforderungen, die die meisten Unternehmen erfüllen müssen. Um nur das offensichtlichste Beispiel zu nennen: Jedes Unternehmen, das Zahlungskartentransaktionen abwickelt, muss den PCI DSS einhalten, ein Framework, das von der Branche selbst entwickelt und gepflegt wird. Standards wie das NIST CSF sind zwar freiwillig, helfen Unternehmen aber dabei, in bestimmten Branchen tätig zu sein, mit bestimmten Behörden Geschäfte zu machen oder eine Cyberversicherung zu erschwinglichen Konditionen abzuschließen.

Unabhängig von den Compliance-Anforderungen ist die Vorbereitung auf Audits wahrscheinlich ein Thema, mit dem sich die Risikomanagement- oder IT-Sicherheitsteams mindestens mehrmals im Jahr befassen. Audits können auch nach einem Cybervorfall durchgeführt werden. In jedem Fall können die Risiken eines fehlgeschlagenen Audits für das Unternehmen erheblich sein.

Compliance messen und managen

Unsere Umfrageteilnehmer beantworteten ähnliche Fragen zur Compliance wie im letzten Abschnitt zur Sicherheit - zum aktuellen Stand der Bemessung und des Managements (Abbildung 19). Wie bei der Sicherheit gibt knapp ein Viertel der Befragten an, dass weder bei der Bemessung noch beim Management von Compliance-Risiken Verbesserungen notwendig sind.

In Nordamerika ist das Ergebnis bei der Messung sogar noch schlechter: 79 % der Befragten sehen hier Verbesserungsbedarf. Im Nahen Osten hingegen geben 35 % der Befragten an, dass bei der Messung kein Verbesserungsbedarf besteht.

Betrachtet man diese Frage nach Branchen, so sind Energie- und Versorgungsunternehmen besonders pessimistisch, was die Bemessung der Compliance angeht. Nur 8 % geben an, dass kein Verbesserungsbedarf besteht. Ironischerweise sehen in der gleichen Branche 36 % keinen Verbesserungsbedarf beim Compliance-Management. Bei den Kommunen ist es genau umgekehrt: 39 % sehen keinen Verbesserungsbedarf bei der Bemessung, aber nur 21 % beim Management.

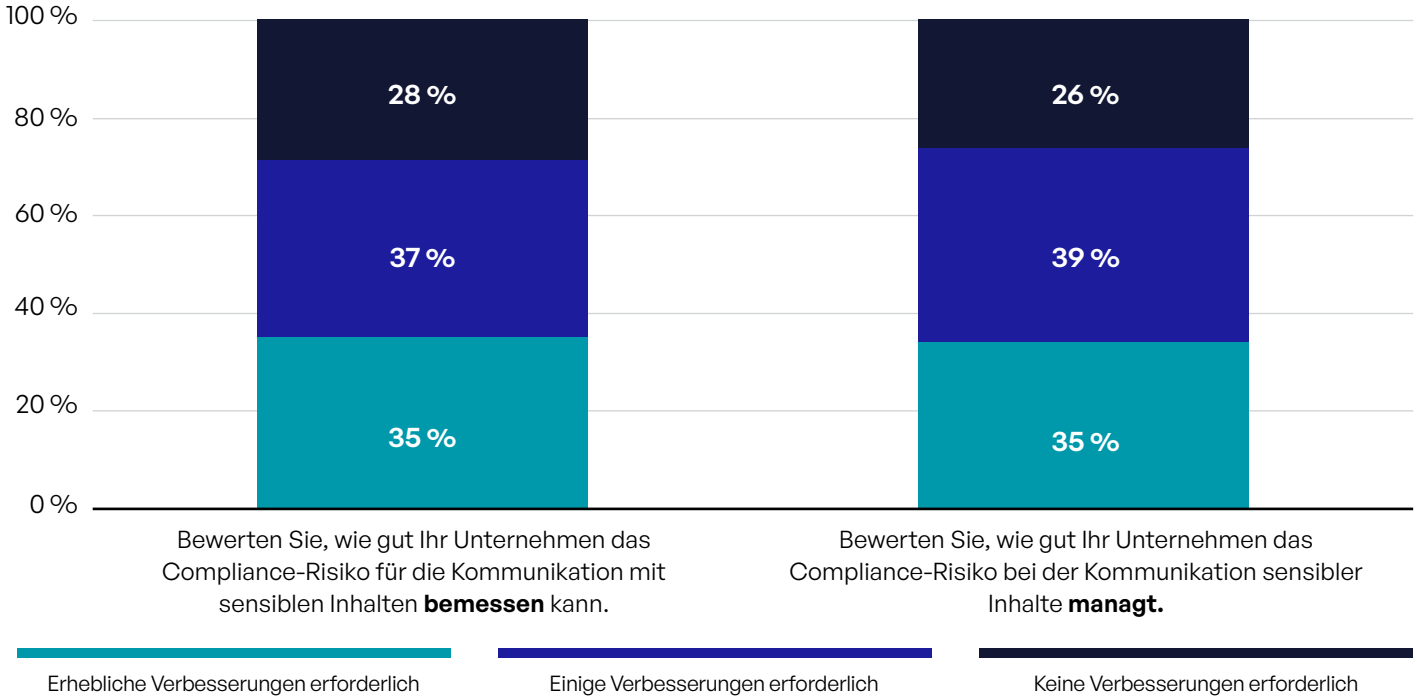


Abbildung 19: Reifegrad der Unternehmen bei der Bemessung und dem Management von Compliance-Risiken

Audits für eine Vielzahl von Vorschriften und Standards

Auf die Frage, welche Compliance-Vorschriften und -Standards sie einhalten müssen, ist PCI DSS (40 %) die häufigste Antwort - nicht überraschend, da es sich um einen globalen Standard handelt (Abbildung 20). An zweiter Stelle steht die GDPR/DSGVO mit 37 % aller Befragten, darunter 96 % der Europäer (Abbildung 20). Und HIPAA ist für 34 % der Befragten eine Voraussetzung, davon 92 % in den USA. Neben HIPAA unterliegen die nordamerikanischen Befragten einer Vielzahl von Vorschriften mit Akronymen wie HIPAA, GLBA, SOX, FINRA und FISMA - sowie den bereits erwähnten Vorschriften auf staatlicher Ebene. Befragte in anderen Ländern müssen oft länderspezifische Anforderungen erfüllen.

Zu den gängigen Security Frameworks gehören ISO 27001, 27017 und 27018, die von den Befragten am häufigsten genannt wurden (Abbildung 21). US-Unternehmen, die mit dem US-Verteidigungsministerium zusammenarbeiten, müssen jetzt CMMC 2.0 einhalten, und diejenigen, die mit anderen Behörden zusammenarbeiten, unterliegen FedRAMP. Auch verschiedene Standards des NIST werden, obwohl es sich um eine US-Behörde handelt, zunehmend weltweit eingesetzt.

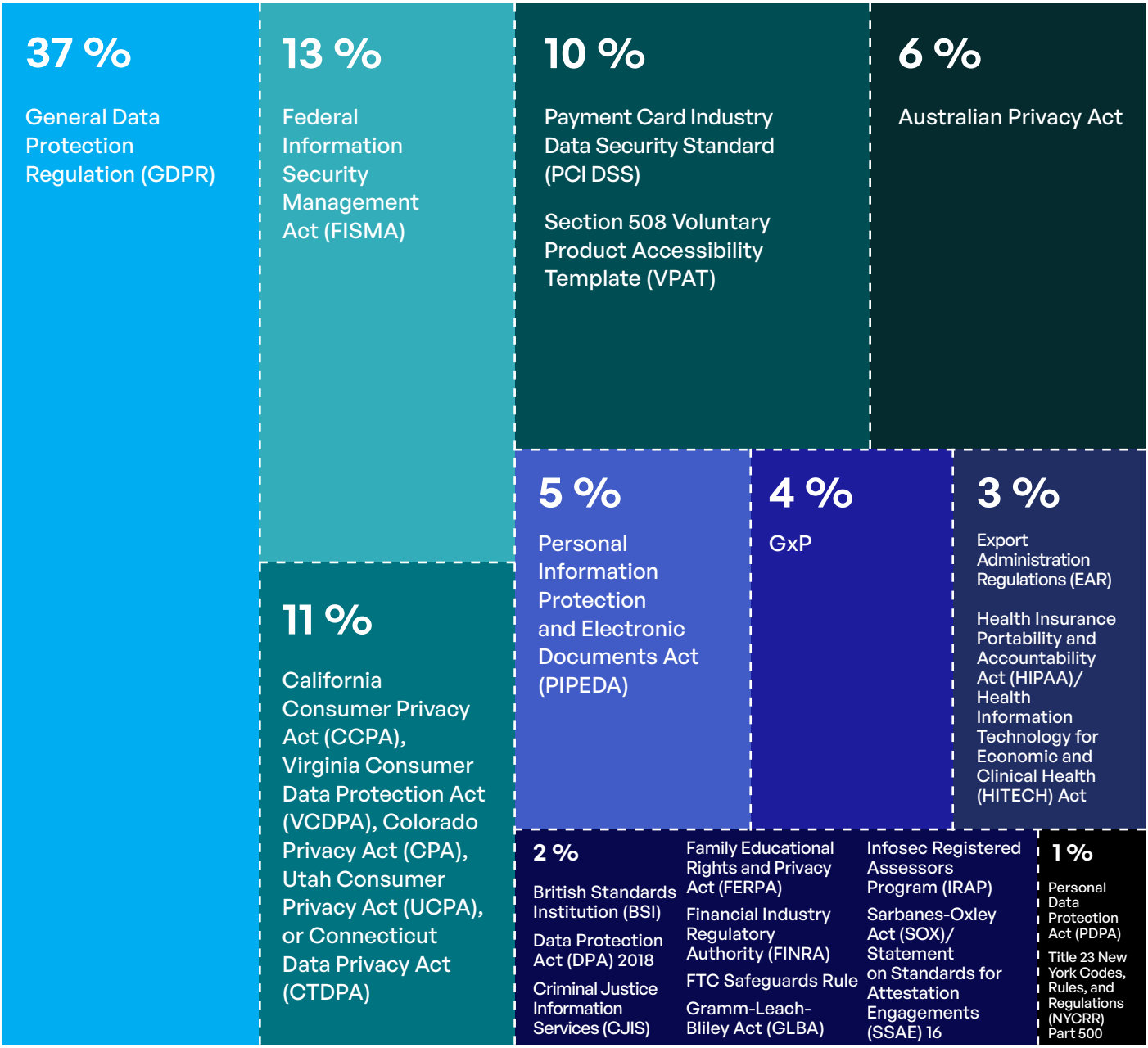


Abbildung 20: Geltende Datenschutzbestimmungen

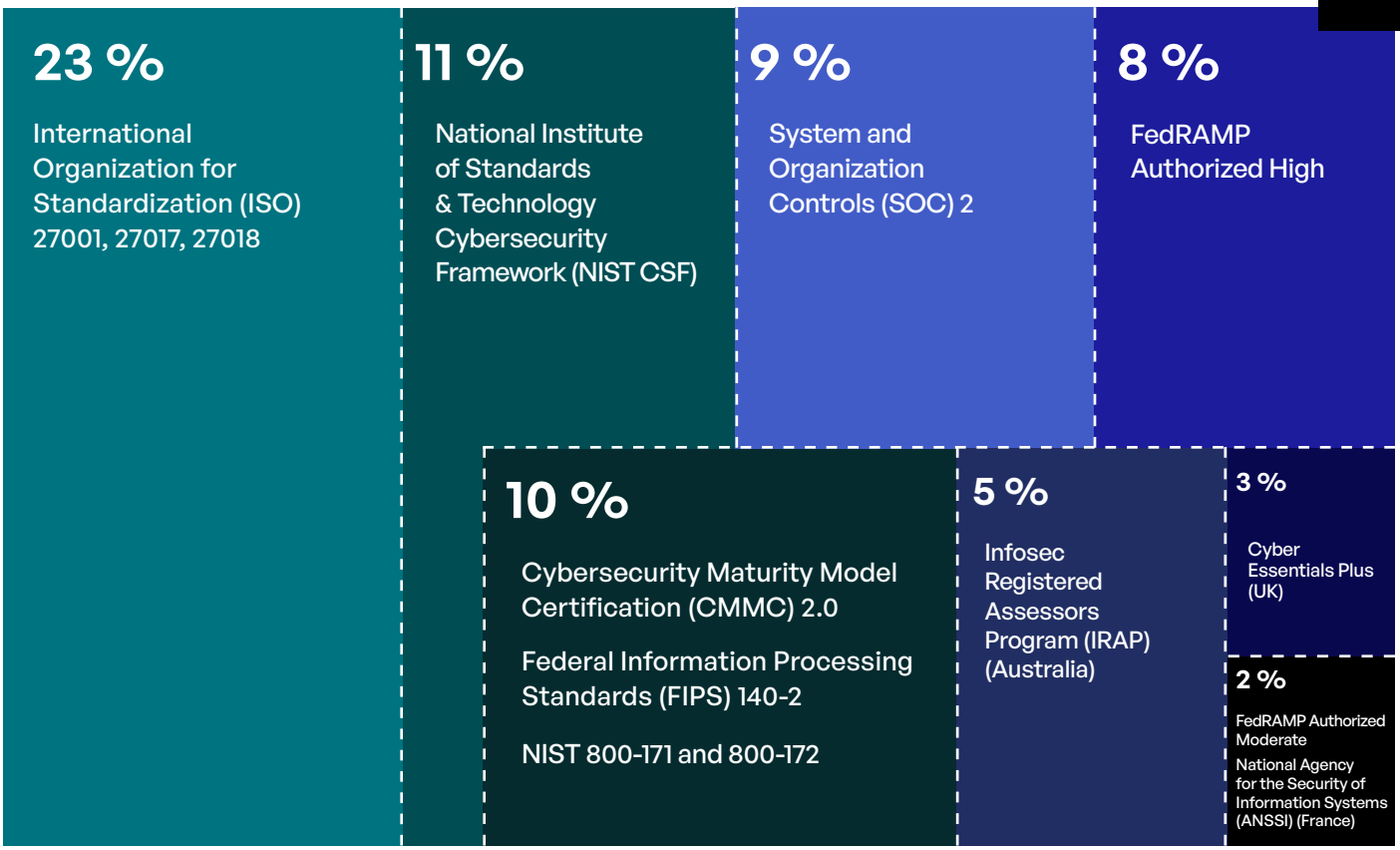
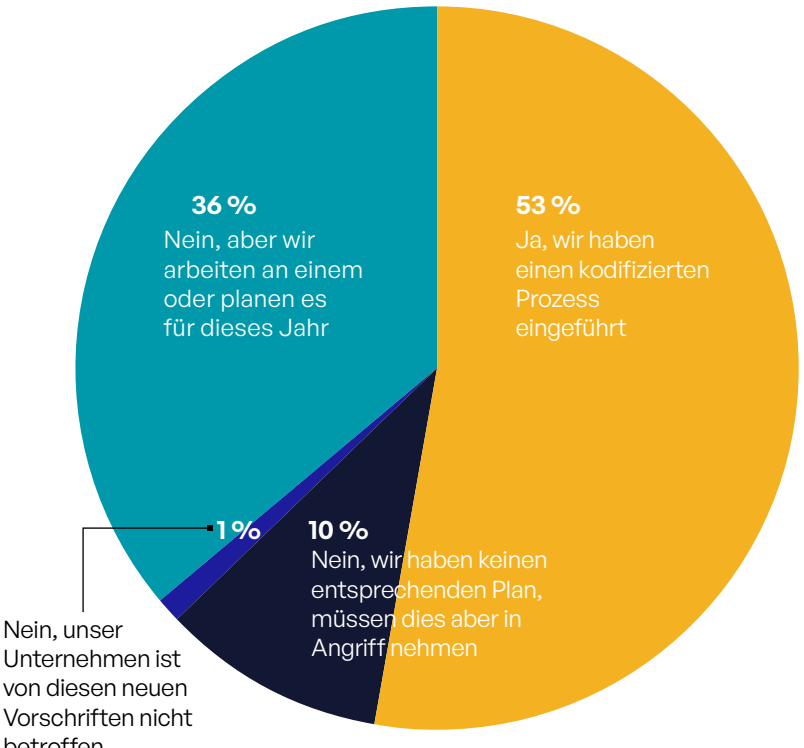


Abbildung 21: Geltende Datenschutzstandards

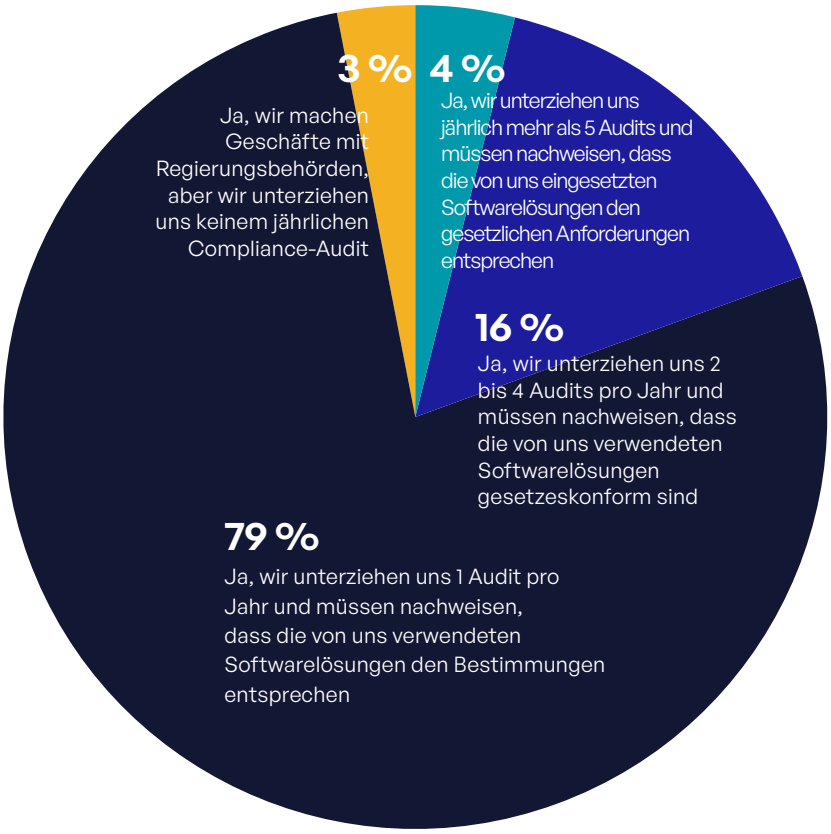
Während der California Consumer Privacy Act (CCPA) bei seiner Verabschiedung im Jahr 2018 großes Aufsehen erregte, wurden die im vergangenen Jahr verabschiedeten neuen US-Bundesvorschriften in Virginia, Colorado, Utah und Connecticut von den Medien weniger beachtet. Dennoch sind sich die meisten Befragten, die von diesen Regelungen betroffen sind, bewusst, dass sie sich in den nächsten Monaten an die neuen Regelungen halten müssen, wenn sie in diesen US-Bundesstaaten geschäftlich tätig sind (Abbildung 22). Von den Befragten in den USA gaben mehr als die Hälfte (53 %) an, bereits über ein kodifiziertes Verfahren zu verfügen, und 36 % erklärten, an einem solchen Verfahren zu arbeiten.

Während sich ein Großteil unserer bisherigen Diskussion über Regierungsverträge auf die US-Regierung bezog, geben fast alle Befragten weltweit an, Geschäfte mit Regierungsbehörden zu machen, und fast alle unterliegen Audits (Abbildung 23). Eine große Mehrheit in allen Regionen unterzieht sich einmal im Jahr einem Audit, wobei ein etwas höherer Prozentsatz in Asien (25 %) häufiger überprüft wird.

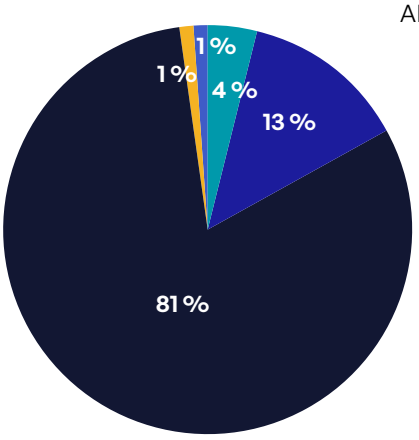


Nur Befragte aus den USA

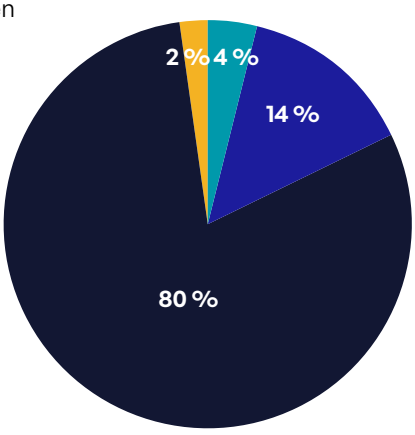
Abbildung 22: Hat Ihr Unternehmen eine Strategie für den Umgang mit den neuen Datenschutzgesetzen, die in vier Bundesstaaten (UT, VA, CT, CO) in diesem Jahr in Kraft treten werden?



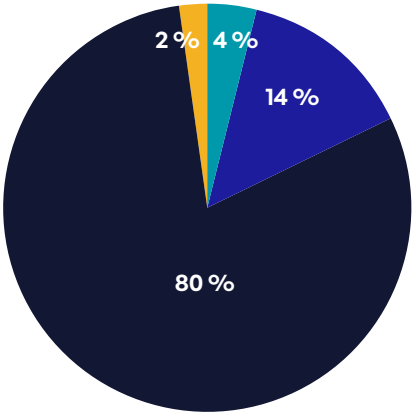
Alle Befragten



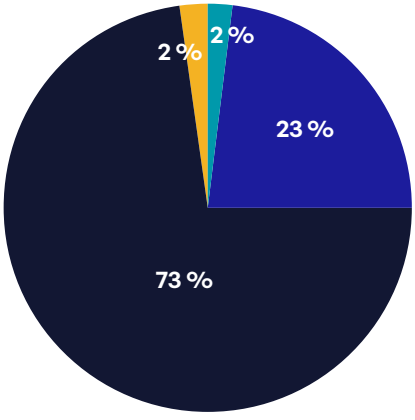
Nordamerika



Mittlerer Osten



Europa



Asien/Pazifik

Abbildung 23: Wir arbeiten mit Regierungsbehörden zusammen, die verlangen, dass die von uns verwendeten Software-Tools den Frameworks für Cybersicherheit entsprechen

Versicherungsschutz: Ein weiterer Anreiz für Compliance

Ein weiterer Grund für die Einhaltung gesetzlicher Vorgaben und Standards ist für die Unternehmen, bessere Konditionen für Cyber-Versicherungsschutz zu erhalten - oder überhaupt einen solchen Versicherungsschutz abschließen zu können. Insgesamt geben 88 % der Befragten an, dass ihre Versicherer Compliance-Risikomanagementverfahren im Zeichnungsprozess berücksichtigen (Abbildung 24). Noch höher ist dieser Anteil in Nordamerika, wo 93 % der Befragten einen Zusammenhang zwischen Compliance und Versicherungsschutz bestätigen.

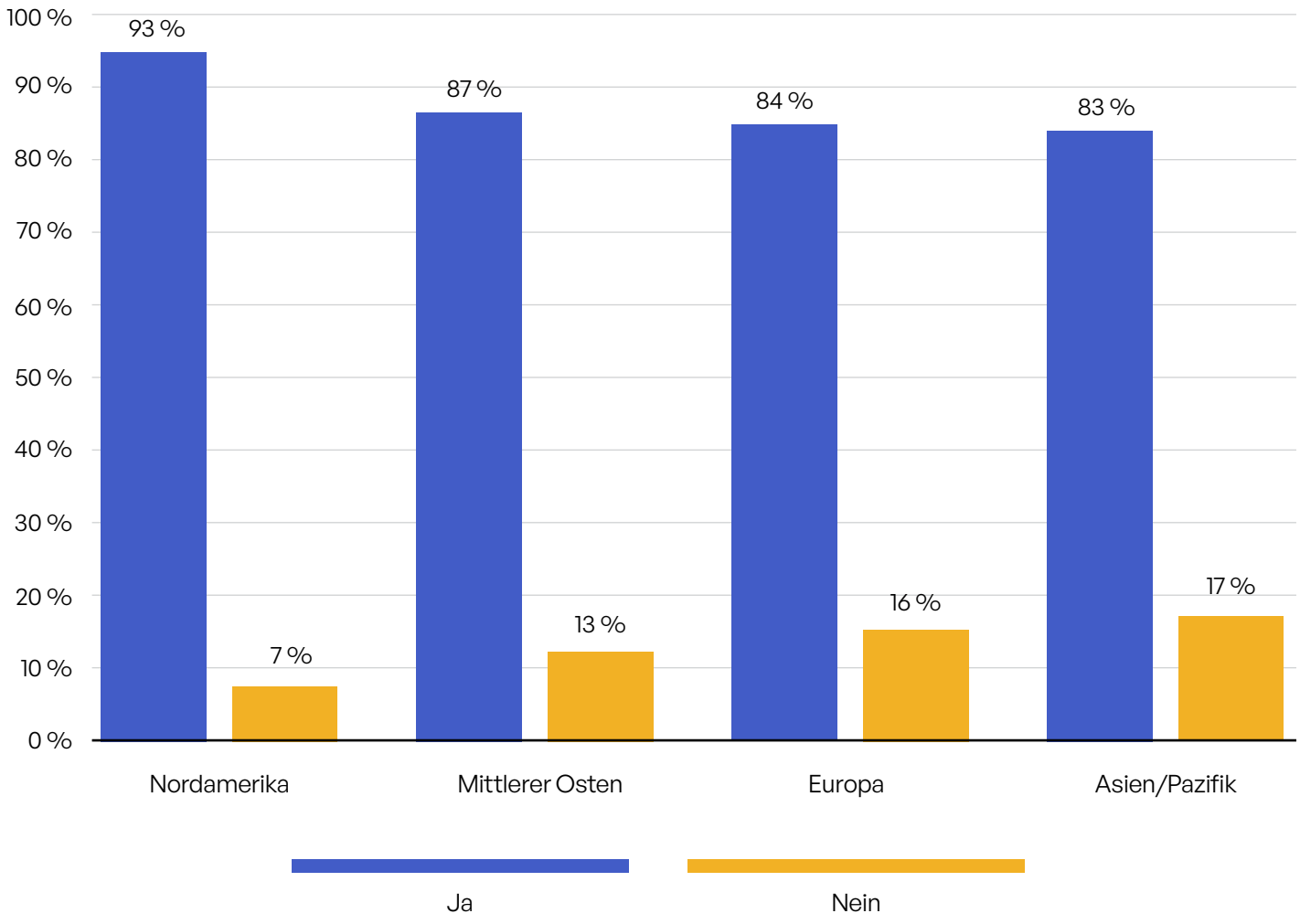


Abbildung 24: Anbieter von Cyber-Versicherungen berücksichtigen Datenschutz- und Compliance-Risikomanagement bei der Tarifgestaltung

Compliance strategisch angehen

Der Aufwand an Zeit, Geld und Energie, den die Unternehmen für die Einhaltung der Vorschriften aufbringen müssen, ist nicht unerheblich. Von allen Befragten geben 69 % an, dass ihre Bemühungen zur Einhaltung der Vorschriften für die Kommunikation sensibler Inhalte mehr als 300 Arbeitsstunden pro Jahr für die Überwachung und Berichterstattung erfordern. Deutlich mehr als ein Drittel (36 %) gibt an, dass diese Zahl bei über 500 Stunden liegt (Abbildung 25). In einigen Branchen - Finanzdienstleistungen, Gesundheitswesen, Hochschulen und Pharma/Biowissenschaften - geben mehr als 80 % der Befragten an, dass sie 300 oder mehr Stunden für die Compliance bei der Kommunikation sensibler Inhalte aufwenden.

Auf die Frage nach der Anzahl der Mitarbeiter, die sich mit der Einhaltung der Vorschriften für die Kommunikation sensibler Inhalte befassen, gab fast die Hälfte der Befragten (49 %) an, dass sie nur über eine Vollzeitstelle ("Full Time Equivalent", FTE) verfügen (Abbildung 26). 42 % der Befragten gaben jedoch an, dass sich zwei oder mehr FTEs mit Compliance befassen. In Branchen wie Finanzdienstleistungen, Gesundheitswesen, Hochschulen und Pharma/Biowissenschaften gab mehr als die Hälfte der Befragten an, dass mehr als eine Vollzeitstelle für Compliance erforderlich ist.

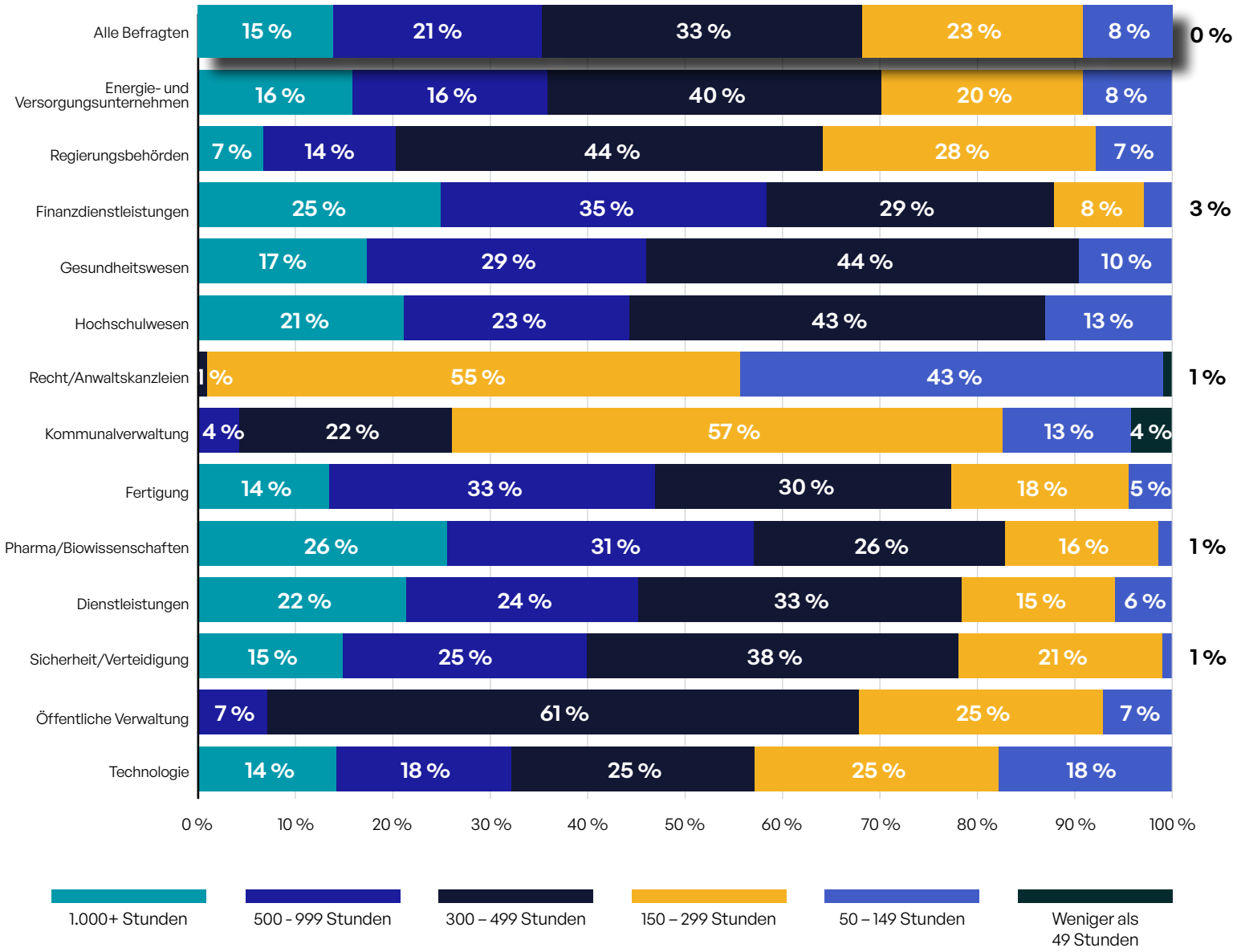


Abbildung 25: Jährlicher Zeitaufwand für die Nachverfolgung und Berichterstattung zur Compliance bei der Kommunikation sensibler Inhalte

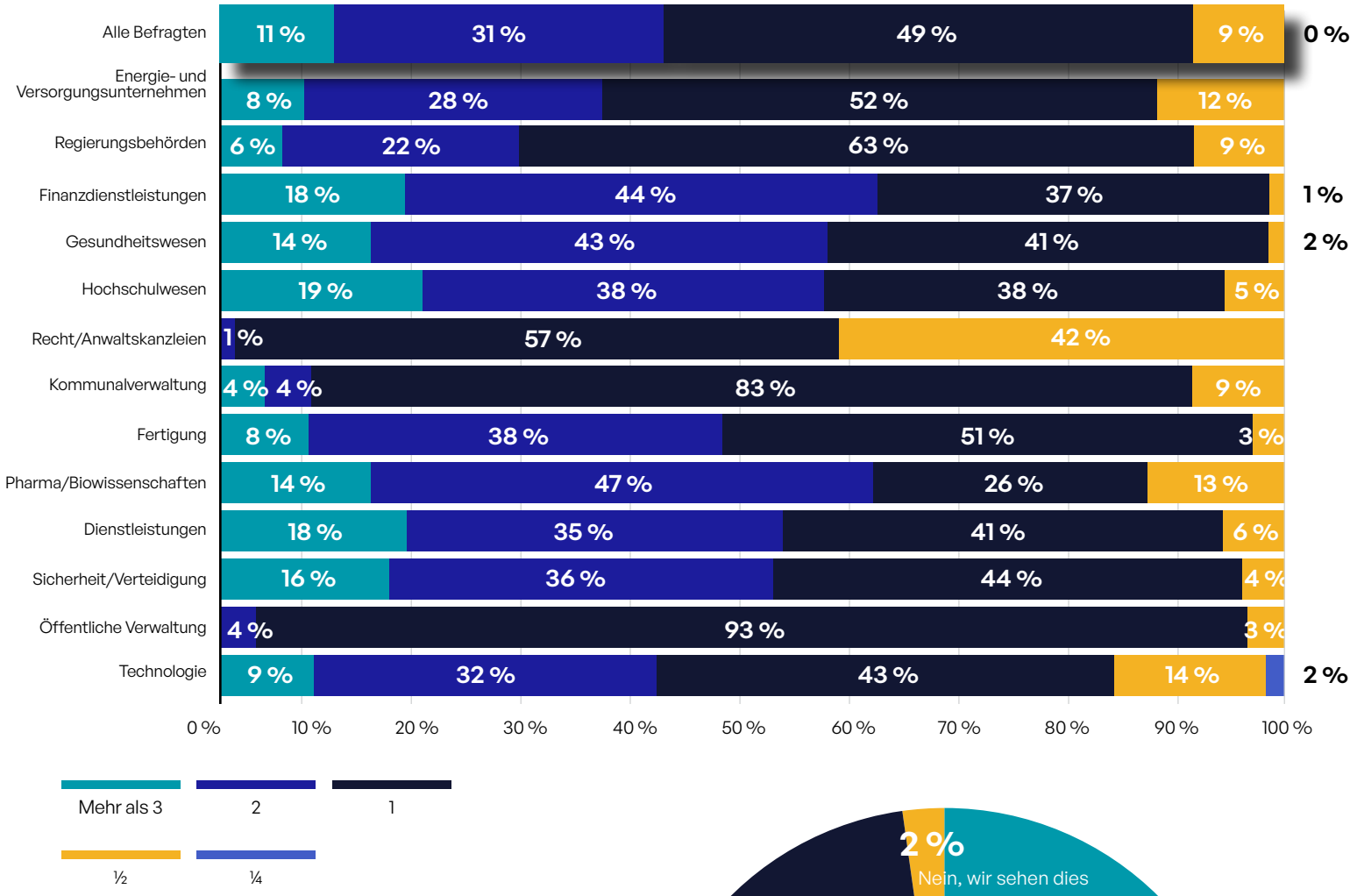


Abbildung 26: Zuweisung von Personal für die Nachverfolgung und Berichterstattung zur Compliance bei der Kommunikation sensibler Inhalte

Schließlich haben wir eine identische Frage zur Compliance gestellt, die wir am Ende des vorhergehenden Abschnitts zur Sicherheit diskutiert haben. In Bezug auf die Anpassung der Risikomanagementstrategie des Unternehmens an die Compliance-Strategie für die Kommunikation von Inhalten geben 27 % an, dass die beiden Strategien bereits aufeinander abgestimmt sind, 44 % geben an, dass die Anpassung im Gange ist und noch in diesem Jahr abgeschlossen werden soll, und 27 % geben an, dass dies für das kommende Jahr oberste Priorität hat (Abbildung 27).

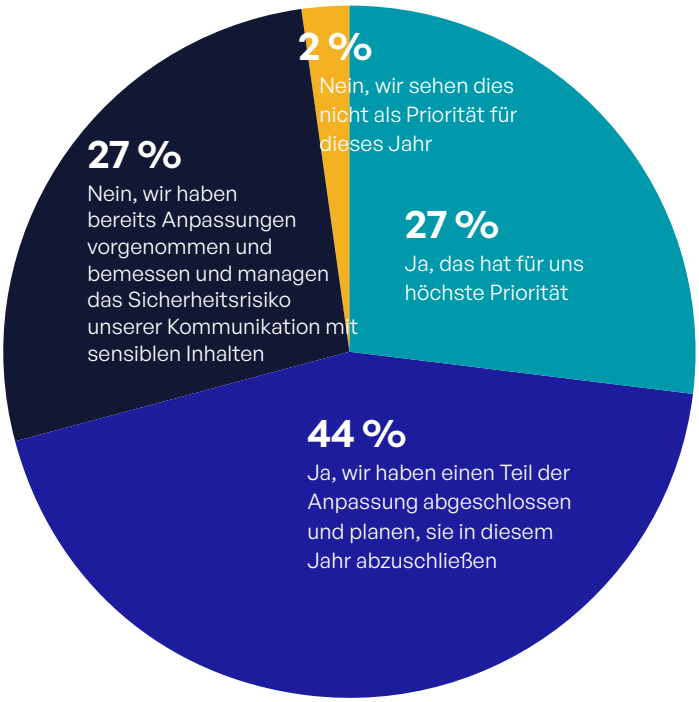


Abbildung 27: Anpassung der Risikomanagement-Strategie an die Bemessung und das Management des Compliance-Risikos bei der Kommunikation sensibler Inhalte

FedRAMP und CMMC: Die Schlüssel zu Geschäften mit der Regierung der Vereinigten Staaten

Die US-Regierung ist der weltweit größte Einkäufer von Waren und Dienstleistungen, und Hunderttausende von Unternehmen arbeiten mit mindestens einer Bundesbehörde zusammen. Es liegt auf der Hand, dass die US-Regierung ein großes Interesse daran hat, dass ihre umfangreiche Lieferkette die besten Sicherheitsverfahren einhält. Schließlich befinden sich einige der sensibelsten Daten der Welt in den Systemen der US-Regierung.

Deshalb hat die Regierung im Laufe der Jahre eine weltweite Führungsrolle bei der Entwicklung von Cybersicherheitsstandards übernommen, insbesondere durch Institutionen wie das NIST und die Cybersecurity and Infrastructure Security Agency (CISA). Ihre Arbeit hat zu Frameworks geführt, die auf dem besten Weg sind, globale Standards zu werden, wie z. B. das NIST CSF.

Für Auftragnehmer von Bundesbehörden und solche, die mit Bundesbehörden zusammenarbeiten wollen, stehen derzeit zwei spezifische Standards im Vordergrund - FedRAMP und CMMC.

FedRAMP: Standardisierte Anforderungen für Cloud-Services

Mit der zunehmenden Verbreitung von Cloud Computing im privaten Sektor hat das Office of Management and Budget (OMB) das Federal Risk and Authorization Management Program (FedRAMP) ins Leben gerufen, um einen standardisierten Ansatz für die Cloud-Sicherheit zu schaffen. Seit seiner Einführung im Jahr 2011 müssen alle Anbieter von Cloud-Diensten, die Dienstleistungen für Bundesbehörden erbringen, FedRAMP einhalten, unabhängig davon, ob sie Infrastructure-as-a-Service, Platform-as-a-Service oder Software-as-a-Service anbieten.

Unternehmen, die sich um Aufträge der US-Regierung bewerben, müssen sicherstellen, dass alle Cloud-Dienste, die sie für ihre Arbeit mit der Regierung nutzen, FedRAMP-zertifiziert sind. Dazu gehören auch Lösungen für die gemeinsame Nutzung sensibler Inhalte innerhalb einer Organisation und mit externen Parteien.

CMMC: Sicherheit für Auftragnehmer im Verteidigungsbereich

Verständlicherweise hat das US-Verteidigungsministerium (Department of Defense - DoD) Grund, noch strengere Anforderungen an seine Auftragnehmer zu stellen als andere Bundesbehörden. Die Cybersecurity Maturity Model Certification (CMMC) ist ein Versuch, genau das zu tun. CMMC 1.0 wurde im Jahr 2020 veröffentlicht und kam nur schwer in Gang, vor allem weil es an qualifizierten Prüfern für die erforderlichen Audits fehlte.

Um dieses Problem zu lösen, wurde im Mai 2013 die CMMC 2.0 veröffentlicht, mit einem vereinfachten Reifegradmodell und weniger häufigen Audits durch unabhängige Stellen, aber den gleichen strengen Anforderungen. Die CMMC-Zertifizierung soll den Schutz von nicht als Verschlusssache eingestuften Informationen (Classified Uncontrolled Information - CUI) und Vertragsinformationen des Bundes (Federal Contractual Information - FCI) verbessern und gilt für alle 300.000 Auftragnehmer des DoD.

CMMC 2.0 sieht drei Reifegrade vor, und jeder Auftragnehmer im Verteidigungsbereich muss nachweisen, dass er einen bestimmten Reifegrad erreicht, je nachdem, welche Art von Informationen er sendet, weiterleitet, empfängt und speichert. Auf jeder Stufe ist die Kontrolle der Weitergabe sensibler Inhalte eine der Anforderungen.

Mehr als die Hälfte der Zulieferer des Verteidigungsministeriums verlieren 40 % ihres Umsatzes, wenn sie Verträge mit dem Verteidigungsministerium aufgrund der Nichteinhaltung des CMMC verlieren.[11]

Prozess

Insight: Um es freundlich auszudrücken: Die Ergebnisse sind uneinheitlich, was die Einhaltung von Best Practices für die sichere Kommunikation von Inhalten betrifft

Unabhängig davon, welche Vorschriften und Rahmenwerke ein Unternehmen einhalten muss, ist die konsequente Befolgung etablierter Best Practices der beste Weg, um digitale Vermögenswerte zu schützen. Wie bereits erwähnt, ist dies bei sensiblen Inhalten schwierig, wenn man bedenkt, mit wie vielen externen Parteien sie geteilt werden, über wie viele verschiedene Kanäle sie übertragen werden und welche Tools Unternehmen zu ihrer Überwachung und Kontrolle einsetzen. Unsere Umfrage enthält eine Reihe von Fragen, mit denen wir herausfinden wollen, wie gut die Unternehmen die wichtigsten Kontrollen und Verfahren beherrschen.

Eine Frage trifft den Kern der Sache. Wir fragen nach der typischen Reaktion, wenn eine verschlüsselte E-Mail nicht entschlüsselt werden kann, und geben den Befragten drei weniger ideale Möglichkeiten: sich bei einem kostenlosen, aber nicht autorisierten E-Mail-Dienst anzumelden, um den Inhalt weiterzuleiten, den Absender zu bitten, einen unverschlüsselten, aber nicht veröffentlichten Link zu einem freigegebenen Laufwerk zu verwenden, oder den Absender zu bitten, eine passwortverschlüsselte Zip-Datei zu senden.

Man möchte meinen, dass dieses Problem selten auftritt, aber es kommt häufiger vor, als man denkt, da die verschiedenen Verschlüsselungsstandards nicht miteinander kompatibel sind. Unternehmen, die über keine automatische Entschlüsselung verfügen, haben daher nur wenige Möglichkeiten. Die Zip-Datei ist zumindest passwortgeschützt und wahrscheinlich die beste Wahl.

Von allen Befragten hat die Hälfte die beste Wahl getroffen, die andere Hälfte eine weniger gute (Abbildung 28). Ein höherer Prozentsatz der Befragten aus den Bereichen Finanzdienstleistungen, Hochschulen, Anwaltskanzleien, Kommunalverwaltung und Fertigung entschied sich für die Option ZIP-Datei.

Eine gute Nachricht: Als die Befragten in unserer Umfrage 2022 die gleiche Frage beantworteten, wählten nur 39 % die passwortverschlüsselte Zip-Datei, während 60 % den unverschlüsselten Link auf ein freigegebenes Laufwerk wählten. Vielleicht ist dies ein Zeichen dafür, dass sich die Befragten ihrer schlechten Gepflogenheiten bewusst geworden sind. Unabhängig davon zeigen die Antworten, dass die Befragten einen anderen Ansatz für die Ver- und Entschlüsselung von E-Mails benötigen, um sicherzustellen, dass sie keinen böswilligen Angriffen ausgesetzt sind. Ein Tipp an dieser Stelle: Werfen Sie einen Blick auf das E-Mail Protection Gateway von Kiteworks, das die Verschlüsselung von E-Mails automatisiert und die Entschlüsselung für den Benutzer unsichtbar macht, unabhängig davon, welches Verschlüsselungsprotokoll von Sender und Empfänger unterstützt wird.

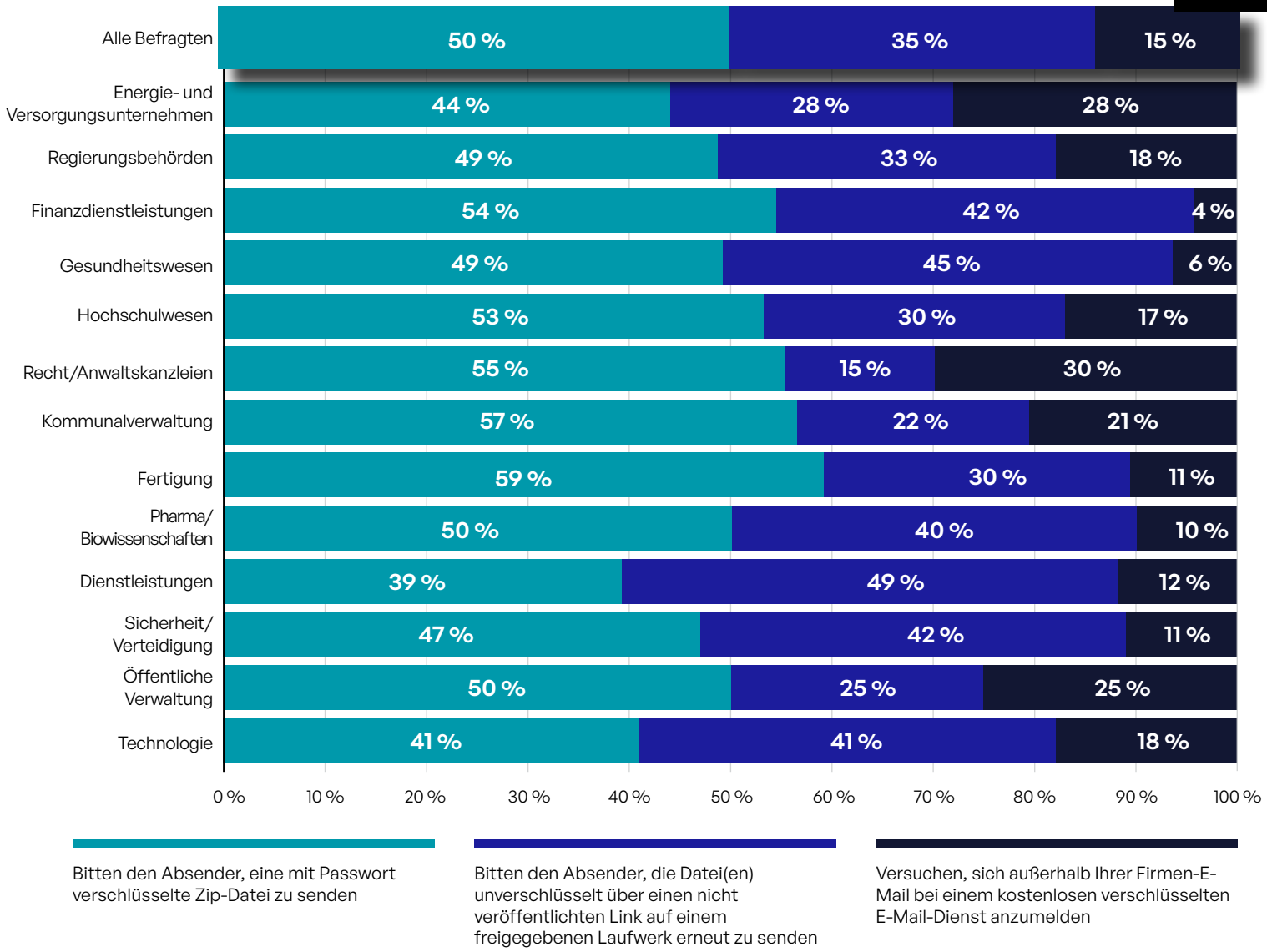


Abbildung 28: Wenn verschlüsselte E-Mails nicht entschlüsselt werden können

Zero Trust: Eine notwendige Priorität

In unserer Umfrage wurden mehrere Fragen dazu gestellt, wie gut die Befragten einen inhaltsdefinierten Zero-Trust-Ansatz zum Schutz sensibler Daten anwenden. Bei der Frage nach der Rangfolge der fünf besten Zero-Trust-Best-Practices wurden alle fünf als wichtig eingestuft. Gewichtet man die Antworten so, dass für höhere Ränge mehr Punkte vergeben werden, steht der Zugriff mit den geringsten Rechten an erster Stelle, gefolgt von der Nachverfolgung und Berichterstattung aus Compliance-Perspektive (Abbildung 29).

Eine weitere Frage bezieht sich auf Best Practices, um sicherzustellen, dass die Zusammenarbeit mit sensiblen Inhalten sicher ist und kein unbefugter Zugriff erfolgt. Auch hier gewichten die Befragten die sieben aufgelisteten Best Practices ähnlich (Abbildung 30). Etwas mehr Befragte bevorzugen die Multi-Faktor-Authentifizierung (33 % als erste oder zweite Priorität) und eine Firewall auf Anwendungsebene (31 %).

Die Prioritäten sind jedoch je nach Branche unterschiedlich. Digitales Rechtemanagement (DRM) wird in der Energie- und Versorgungswirtschaft bevorzugt, während Datenverschlüsselung in dieser Branche sowie im Hochschulsektor und in der Kommunal- und Landesverwaltung bevorzugt wird. Technologie-, Sicherheits- und Verteidigungsunternehmen legen großen Wert auf die Überwachung von Benutzerzugriffen und Dokumentenaktivitäten.

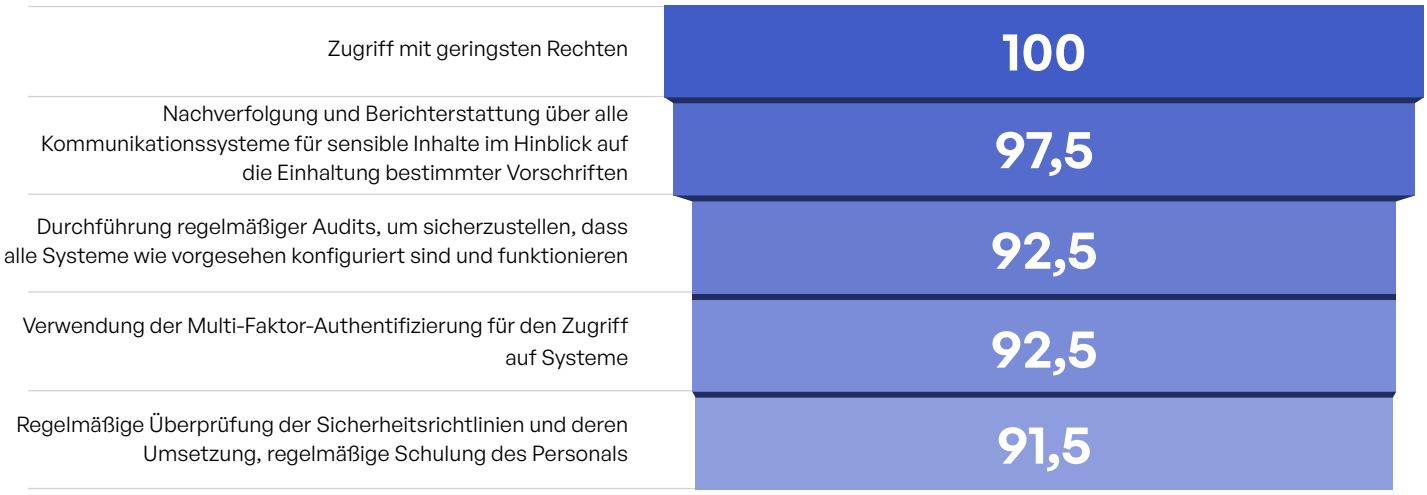


Abbildung 29: Gewichtete Punktzahl: Richtlinien und Verfahren zum Datenschutz und Compliance bei der Kommunikation sensibler Inhalte

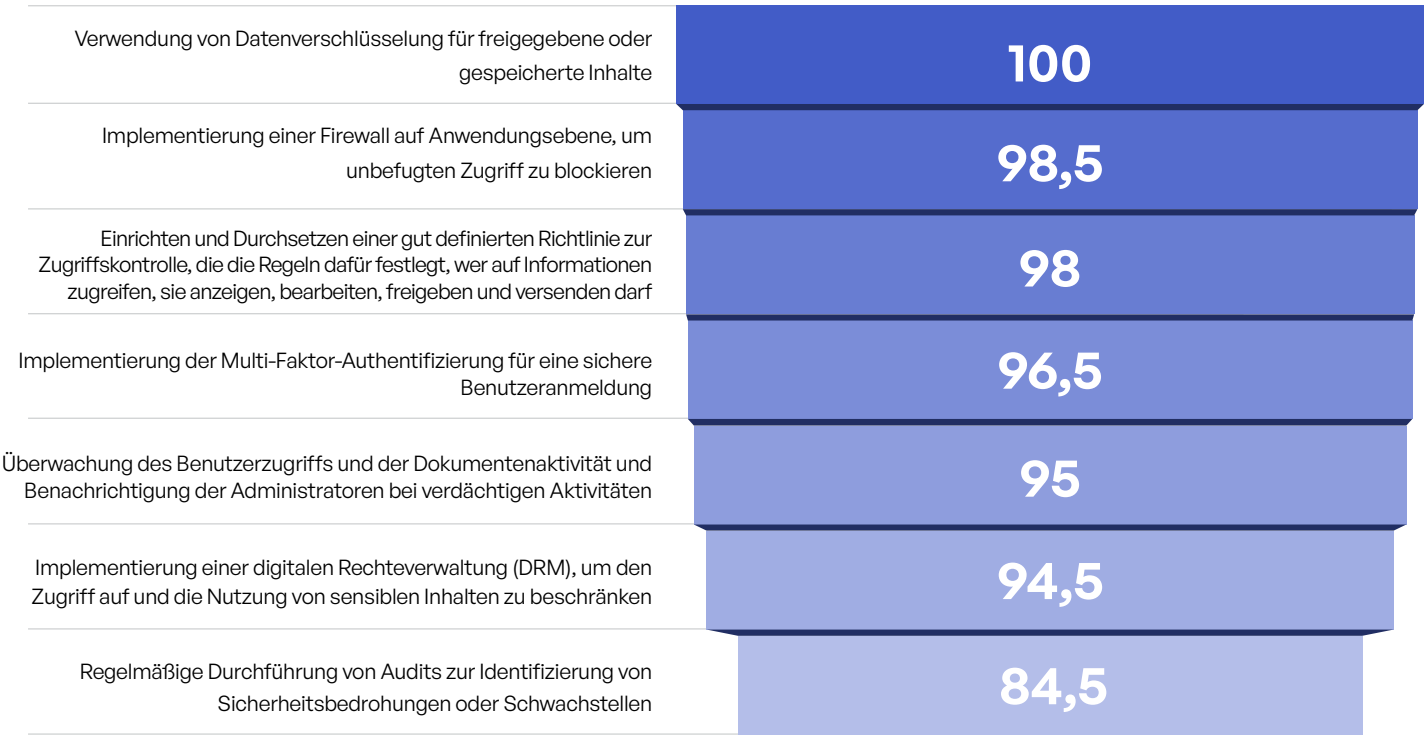


Abbildung 30: Richtlinien und Verfahren, die sicherstellen, dass die Zusammenarbeit mit sensiblen Inhalten sicher ist und kein unbefugter Zugriff auf Inhalte erfolgt

Nachverfolgung, Aufzeichnung und Berichterstattung im Zusammenhang mit Governance, Compliance und Sicherheit

Bei der Nachverfolgung und Protokollierung des Zugriffs externer Parteien auf sensible Dateien und Ordner haben sich die Umfrageergebnisse im Vergleich zu 2022 deutlich verschlechtert. In diesem Jahr geben nur 22 % der Unternehmen an, dass sie diese Nachverfolgung für alle Abteilungen durchführen (Abbildung 31). Und während 97 % der Unternehmen ein gewisses Maß an Nachverfolgung durchführen, tun dies drei Viertel nicht für alle Abteilungen oder Inhaltsarten - oder sind in ihrer allgemeinen Anwendung inkonsistent. Unsere Ergebnisse für 2022 zeigen, dass 49 % der Befragten ein vollständiges Tracking und Reporting eingeführt haben. Wir fragen uns, ob nicht einige aus der letztjährigen Kohorte unverdienten Ruhm für sich beanspruchen! Einige Branchen - Finanzdienstleistungen, Fertigung und Pharma/Biowissenschaften - haben etwas besser abgeschnitten, aber immer noch haben weniger als ein Drittel der Unternehmen diese Best Practice vollständig umgesetzt.

Eine weitere Ebene der Nachverfolgung und Berichterstattung ist die Kommunikation mit der Geschäftsführung und dem Vorstand. Die meisten Befragten (83 %) geben an, dass sie der Unternehmensleitung jährlich über Sicherheits- und Compliance-Risiken im Zusammenhang mit der Kommunikation sensibler Inhalte berichten (Abbildung 32). Im Gesundheitswesen, in der verarbeitenden Industrie und im Dienstleistungssektor geben mehr Befragte (zwischen 27 % und 30 %) an, dass sie solche Berichte vierteljährlich erstellen. (Anmerkung: Für den Bericht 2022 konnten die Befragten mehrere Antworten ankreuzen. 15 % kreuzten sowohl “ja, aber nur für bestimmte Abteilungen” als auch “ja, aber nur für bestimmte Inhaltsarten” an).

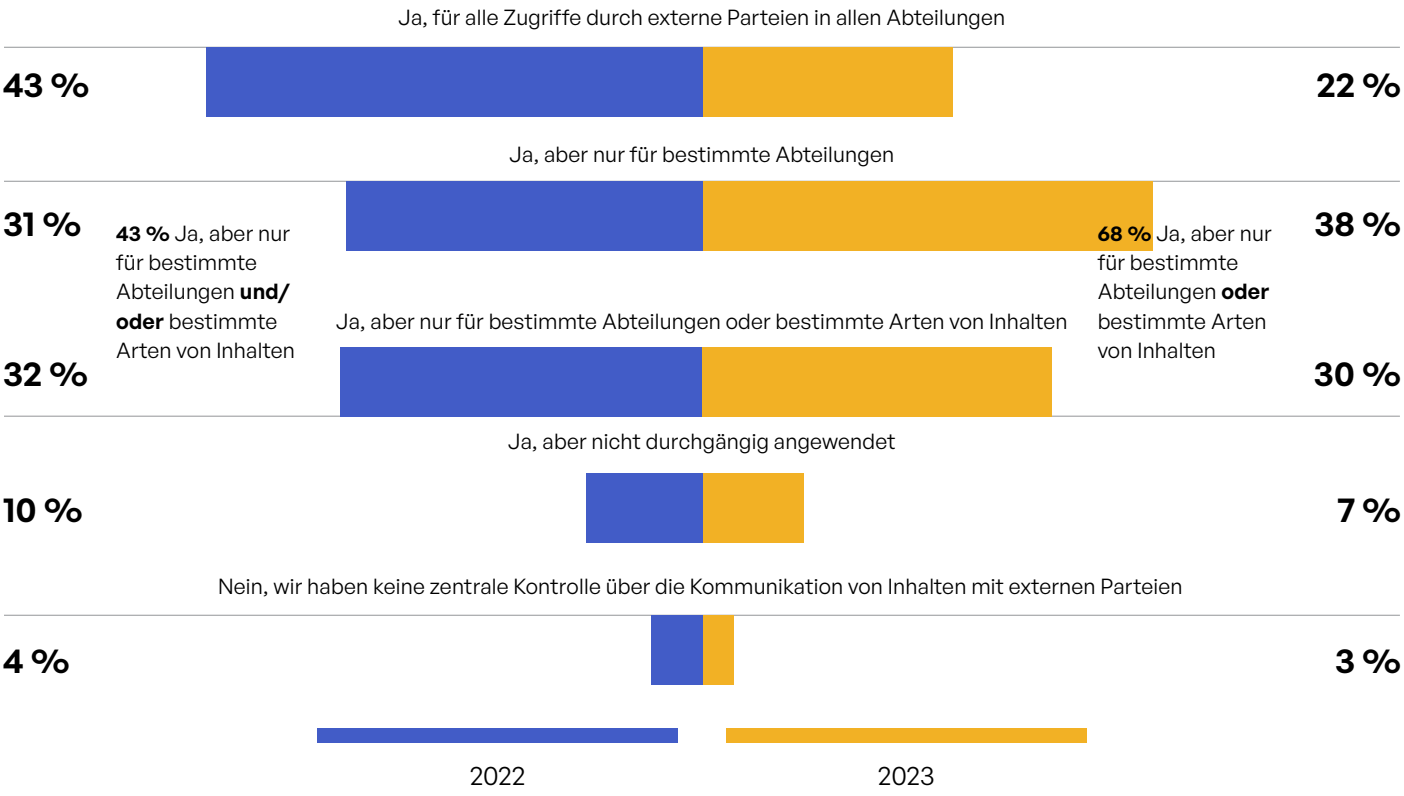


Abbildung 31: Nachverfolgung und Aufzeichnung des Zugriffs externer Parteien auf sensible Dateien und Ordner

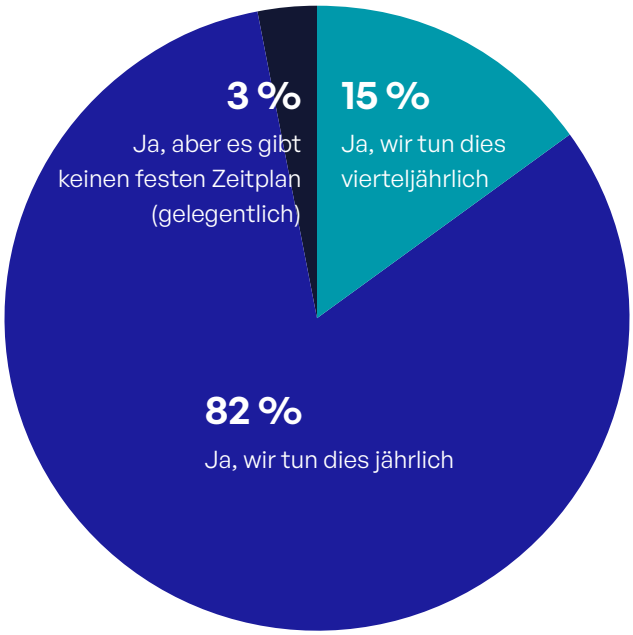


Abbildung 32: Nachverfolgung und Berichterstattung von Sicherheits- und Compliance-Risiken bei der Kommunikation sensibler Inhalte an das Management

Die Tür ist nicht vollständig geschlossen: Kontrollen, die den Zugang beschränken

Ähnlich wie bei der Nachverfolgung und Protokollierung des Zugriffs auf sensible Inhalte sind viele Unternehmen leider auch bei der Kontrolle dieses Zugriffs inkonsequent. Auf die Frage, ob ihr Unternehmen den Zugriff externer Parteien auf Ordner mit Funktionen wie Inhaltsberechtigungen, Ablaufdatum, Sperren und Versionierung verwaltet oder einschränkt, konnte nur ein Viertel der Befragten angeben, dies für alle Abteilungen und Inhaltstypen zu tun (Abbildung 33). Das bedeutet, dass drei Viertel der Unternehmen bei diesen Kontrollen Lücken oder gar keine Kontrollen haben. Die Tür zum Hühnerstall ist also offen!

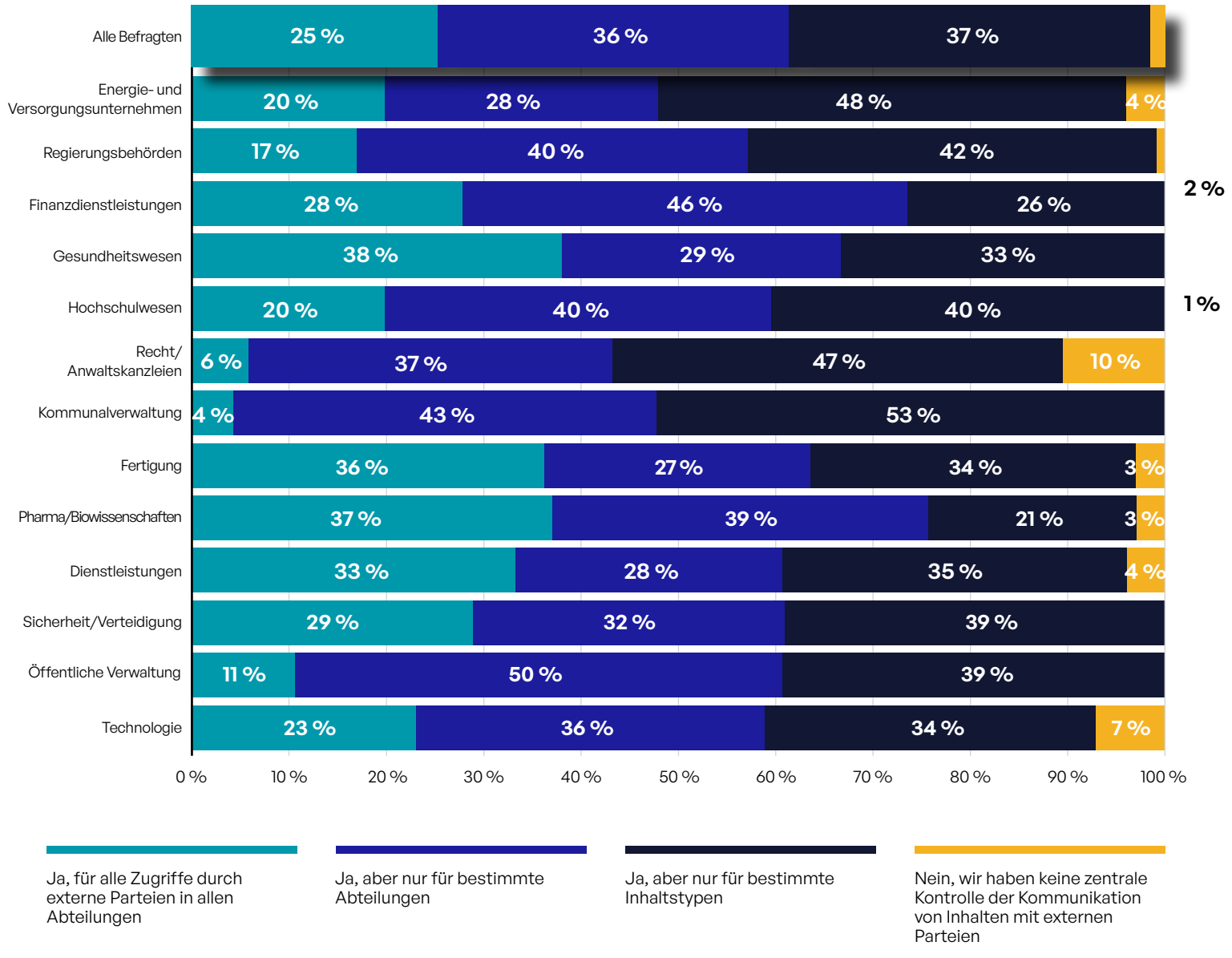
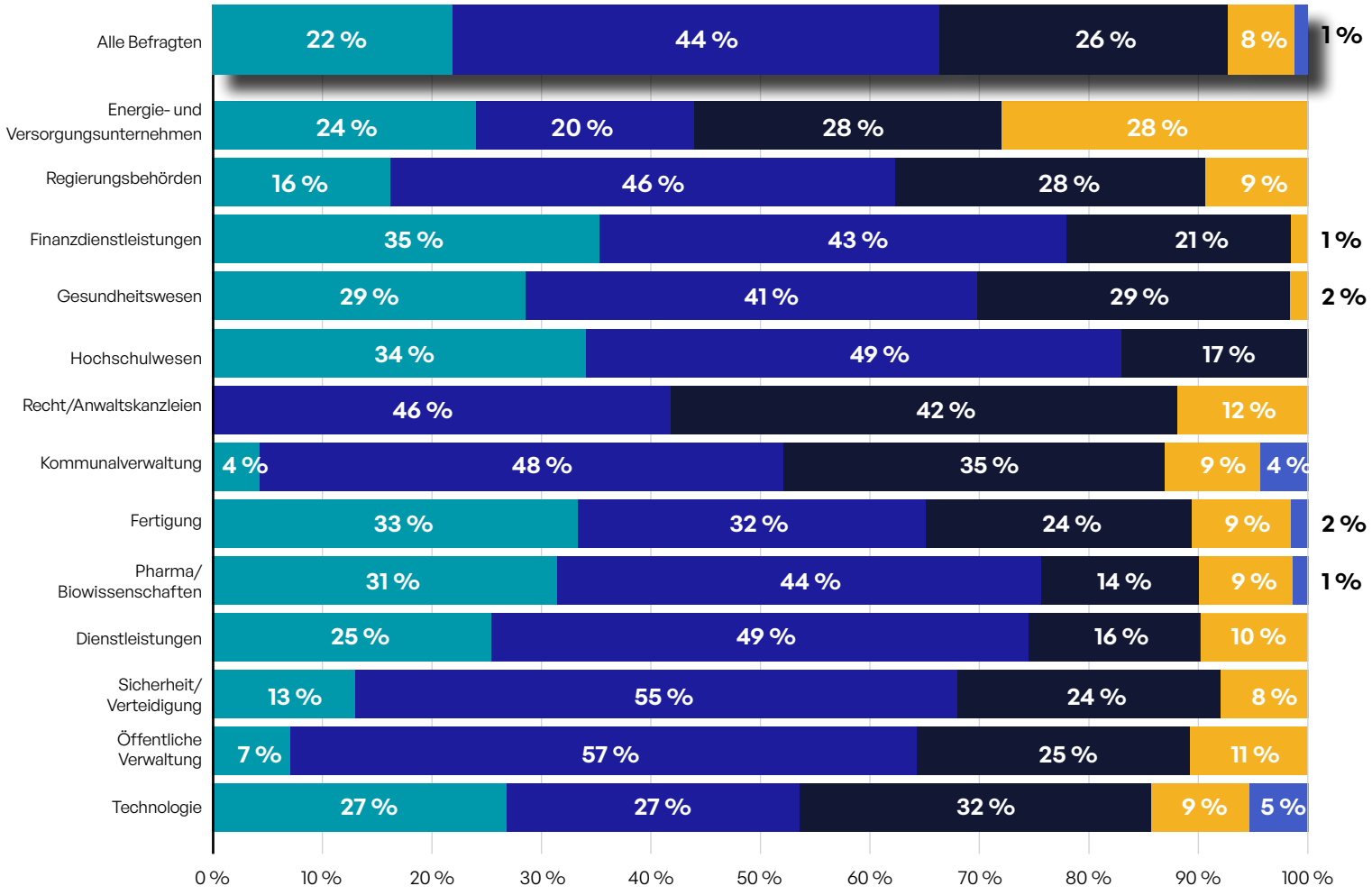


Abbildung 33: Verwalten oder beschränken des Zugriffs externer Parteien auf Ordner (mithilfe von Inhaltsberechtigungen, Ablaufdatum, Sperren und Versionierung usw.)

Ein weiterer Faktor, der von Jahr zu Jahr an Dringlichkeit gewinnt, ist die Sicherstellung, dass die Zugriffskontrollen für sensible Inhalte sowohl die lokale als auch die Cloud-Infrastruktur abdecken. In diesem Jahr geben nur 22 % der Befragten an, dass diese Schutzmaßnahmen sowohl lokal als auch in der Cloud vorhanden sind (Abbildung 34). In einigen Branchen sieht die Situation etwas besser aus: Ein Drittel oder mehr der Befragten aus den Bereichen Finanzdienstleistungen, Hochschulwesen und Fertigung geben an, die gesamte Infrastruktur zu kontrollieren. Auf der anderen Seite geben alle Behörden auf allen Ebenen sowie Sicherheits- und Verteidigungsunternehmen an, dass sie diese Best Practice zu 16 % oder weniger erfüllen, während keine der befragten Anwaltskanzleien dieses Schutzniveau erreicht.



Ja, wir haben Verwaltungsrichtlinien für die Nachverfolgung und Kontrolle für die Zusammenarbeit an und die Kommunikation mit sensiblen Inhalten vor Ort und in der Cloud

Ja, wir haben Verwaltungsrichtlinien für die Nachverfolgung und Kontrolle für die Zusammenarbeit an und die Kommunikation mit sensiblen Inhalten vor Ort, jedoch nicht in der Cloud

Ja, wir haben Verwaltungsrichtlinien für die Nachverfolgung und Kontrolle für die Zusammenarbeit an und die Kommunikation mit sensiblen Inhalten in der Cloud, jedoch nicht vor Ort

Ja, aber die Überwachung und Kontrolle der Richtlinien erfolgt auf der Ebene der einzelnen Inhaltseigentümer und nicht auf der Ebene der Administratoren

Nein, wir sind nicht in der Lage, Richtlinien zur Verfolgung und Kontrolle der Kommunikation mit sensiblen Inhalten anzuwenden

Abbildung 34: Richtlinien und Systeme zur Nachverfolgung und Kontrolle, wer Zugang zu sensiblen Inhalten hat und an wen sie gesendet und weitergegeben werden

Wird es jemals eine US-DSGVO geben ... oder gar einen globalen Standard?

Das Sammeln von Daten ist in den USA seit der Einführung des Internets ein lukratives - und legales - Geschäft. Persönlich identifizierbare Informationen (PII) aller Art sind Freiwild, und es ist für Einzelpersonen praktisch unmöglich, ihre persönlichen Daten aus all diesen Datenbanken entfernen zu lassen.

Eine langjährige Ausnahme von diesem "Wildwest"-Szenario bilden in den USA die geschützten Gesundheitsinformationen (PHI), die seit 1996 durch den Health Insurance Portability and Accountability Act (HIPAA) geregelt werden. Zum Zeitpunkt der Verabschiedung des Gesetzes hatte Präsident Clinton gehofft, eine umfassende Gesundheitsreform durchsetzen zu können, musste sich jedoch mit einem Gesetzentwurf begnügen, der die Übertragbarkeit von Krankenversicherungspolicen bei einem Arbeitsplatzwechsel erleichterte.[12] Weniger bekannt waren damals die "Accountability"-Bestimmungen des Gesetzes, die das Gesundheitsministerium verpflichten, Standards für die Nutzung und den Austausch von Gesundheitsdaten einzuführen und aufrechtzuerhalten.

Seitdem die Europäische Union die Allgemeine Datenschutzverordnung (DSGVO) im Jahr 2016 verabschiedet hat, haben Befürworter für eine ähnliche Regelung in den USA plädiert. Aber im heutigen politischen Klima kann man selten davon ausgehen, dass neue Gesetze verabschiedet werden, egal zu welchem Thema. Es gab bereits Bemühungen im Kongress, zumindest einige DSGVO-ähnliche Anforderungen zu erlassen, aber diese haben sich nicht durchsetzen können.[13]

Dies ist einer der Gründe, warum einzelne US-Bundesstaaten die Sache selbst in die Hand genommen haben. Neun Bundesstaaten haben in den letzten fünf Jahren Gesetze zum Schutz elektronischer Daten verabschiedet, und in zehn weiteren Bundesstaaten sind entsprechende Gesetze in Vorbereitung.[14] Dieser Flickenteppich an Anforderungen könnte ausreichen, um den Kongress und die Exekutive zum Handeln zu bewegen, um einen einheitlichen nationalen Standard zu schaffen.

In der Zwischenzeit haben weltweit tätige Unternehmen nach einem Regelwerk gesucht, das in allen Regionen für operative Konsistenz sorgt und gleichzeitig die Einhaltung der rechtlichen Anforderungen in allen Rechtsordnungen ermöglicht. Immer mehr Unternehmen entscheiden sich für das Cybersecurity Framework des National Institute of Standards and Technology (NIST CSF), das eine Reihe bewährter Verfahren enthält, die überall funktionieren.[15] Ironischerweise ist es der US-Regierung nicht gelungen, Rechtsvorschriften zum Schutz personenbezogener Daten zu erlassen, doch wird ein von einer US-Behörde entwickeltes Framework weltweit übernommen.

Die im Jahr 2023 unter der DSGVO verhängten Geldbußen werden die in den Jahren 2019, 2020 und 2021 insgesamt verhängten Geldbußen übersteigen.[16]

Cyber Exploits

Insight: Ein schlechter Tag im Büro - viele Sicherheitslücken bei der Kommunikation sensibler Inhalte

Das ultimative Ziel aller Cybersicherheitsbemühungen ist es, die Anzahl erfolgreicher Angriffe oder Exploits durch Angreifer jeglicher Art zu minimieren. Auf die Frage, wie viele Exploits die Umfrageteilnehmer in den letzten 12 Monaten speziell im Zusammenhang mit der Kommunikation sensibler Inhalte erlebt haben, sind die Ergebnisse nicht ermutigend. Insgesamt geben 84 % der Befragten an, im letzten Jahr vier oder mehr Exploits erlebt zu haben, 36 % berichten von mehr als sieben (Abbildung 35). Betrachtet man die Kosten eines erfolgreichen Angriffs, werden diese Zahlen noch alarmierender.

In einigen Branchen waren die Durchschnittswerte sogar noch höher: Im Gesundheitswesen, bei Finanzdienstleistern, in der Sicherheits- und Verteidigungsindustrie, in der Fertigung und im Dienstleistungssektor verzeichneten mehr als 90 % der Unternehmen vier oder mehr Sicherheitsvorfälle. Und mehr als die Hälfte der Unternehmen in den Bereichen Finanzdienstleistungen, Gesundheitswesen und Hochschulen verzeichneten mehr als sieben Sicherheitsvorfälle im Zusammenhang mit der Kommunikation sensibler Inhalte.

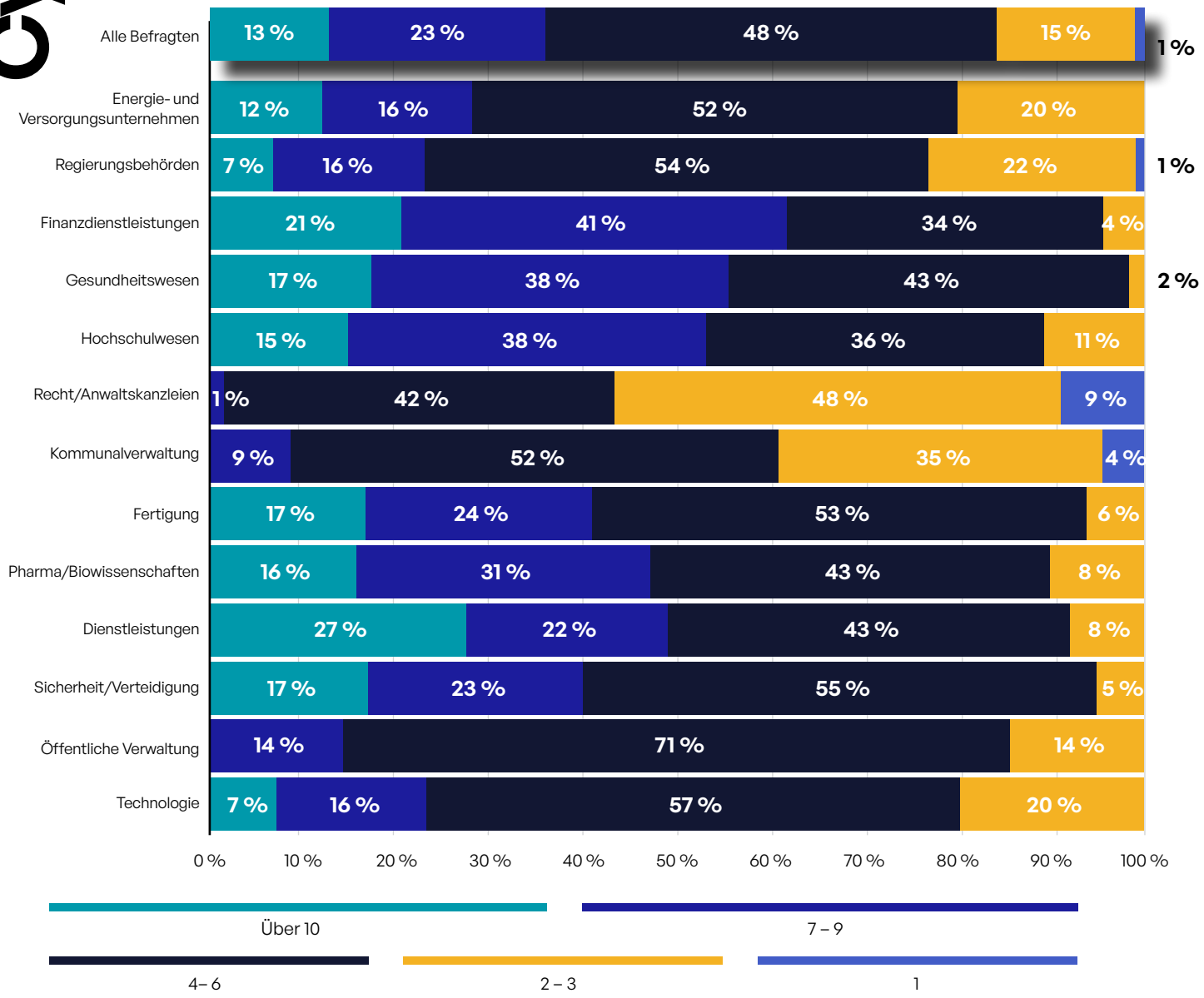


Abbildung 35: Exploits bei der Kommunikation mit sensiblen Inhalten im vergangenen Jahr nach Branchensegment

Auswirkungen von Exploits auf die Kommunikation sensibler Inhalte

Die Auswirkungen dieser Angriffe sind nicht unerheblich. Von allen Befragten berichteten 62 % von finanziellen Auswirkungen mindestens eines Exploits, 44 % von Auswirkungen auf die Marke und 42 % von Strafen und Bußgeldern (Abbildung 36).

Interessanterweise sahen mehr Befragte aus verschiedenen Branchen finanzielle Auswirkungen - Bundes- und Kommunalbehörden (jeweils 76 %), Anwaltskanzleien (72 %) und Technologieunternehmen (74 %). Auch die Auswirkungen auf die Marke wurden in der verarbeitenden Industrie (69 %), im Hochschulwesen (64 %), im Gesundheitswesen (59 %) und in Pharma-/Life-Sciences-Unternehmen (59 %) überdurchschnittlich stark wahrgenommen.

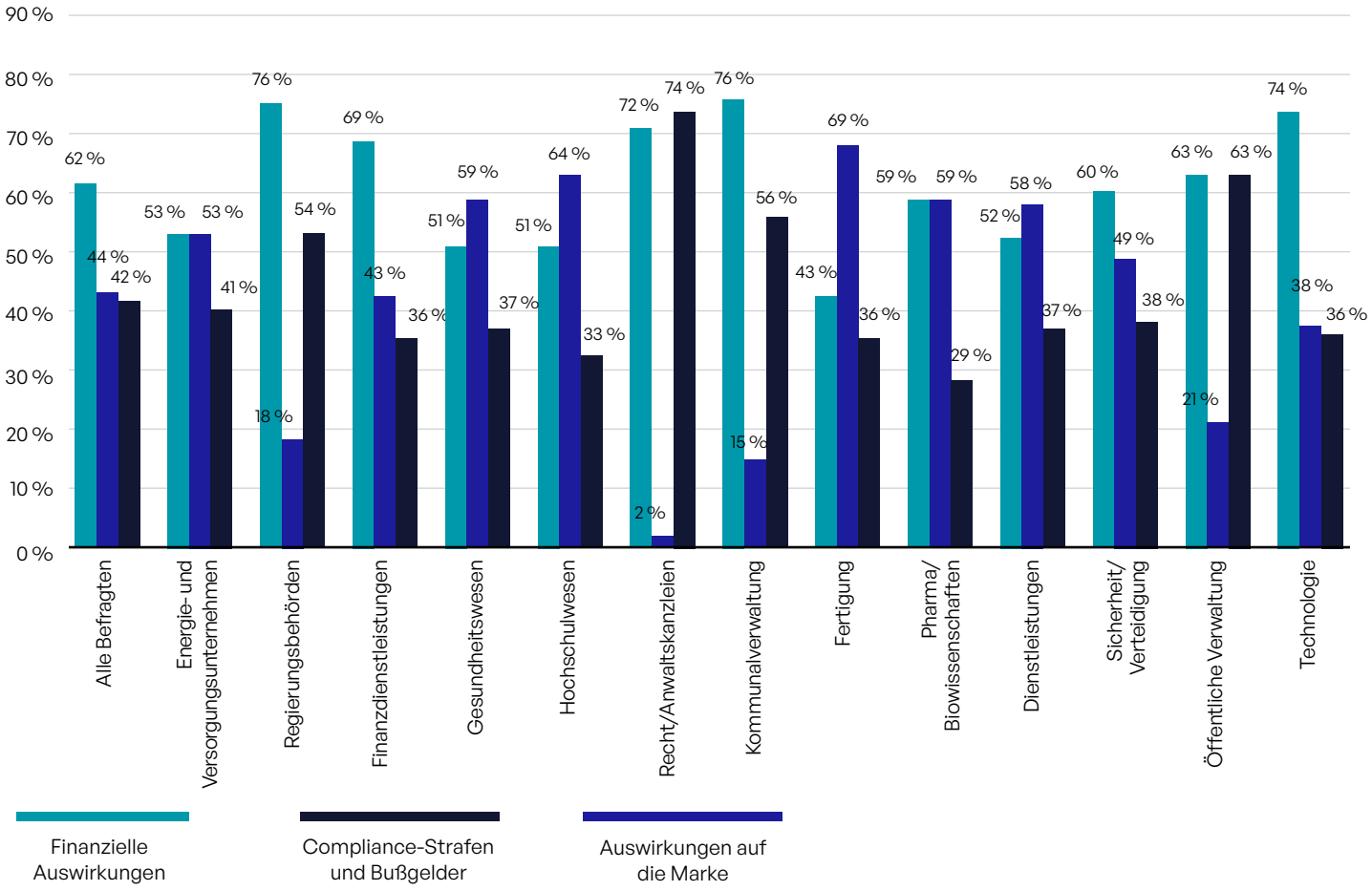
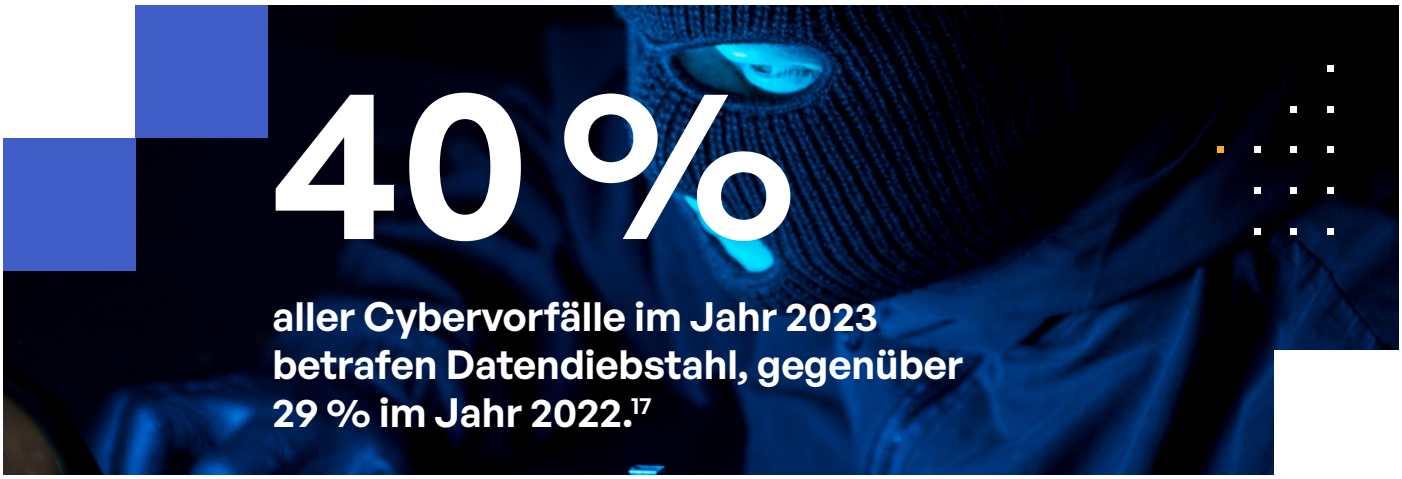


Abbildung 36: Von Datenschutzverletzungen betroffene Unternehmen nach Branchen



Digitale Rechteverwaltung

Insight: DRM ist notwendig, aber die Umsetzung steckt noch in den Kinderschuhen

Segmentierung ist der Schlüssel zum Schutz sensibler Daten aller Art. Wenn jeder in einem Unternehmen Zugriff auf alle Daten hat, steigt das Risiko einer versehentlichen oder absichtlichen Offenlegung sensibler Informationen. Wenn darüber hinaus externe Parteien Zugriff auf die Daten eines Unternehmens haben, vervielfacht sich das Risiko exponentiell. Werden digitale Assets jedoch so segmentiert, dass nur diejenigen, die die Daten benötigen, darauf zugreifen können, wird das Risiko erheblich reduziert und Unternehmen können die Einhaltung verschiedener Vorschriften und Standards erreichen. Dies ist eine zentrale Komponente des als digitale Rechteverwaltung (Digital Rights Management, DRM) bekannten Ansatzes.

Für den Erfolg von DRM ist eine umfassende und detaillierte Datenklassifizierung von entscheidender Bedeutung. Der Grund dafür ist, dass ein rollenbasierter Ansatz für den Zugriff eine Definition dessen erfordert, was jede Rolle in Bezug auf den Zugriff benötigt. Auf die einfache Frage, ob sie ihre Daten klassifizieren, antworteten 93 %, dass sie dies tun (Abbildung 37). Das ist also eine gute Nachricht.

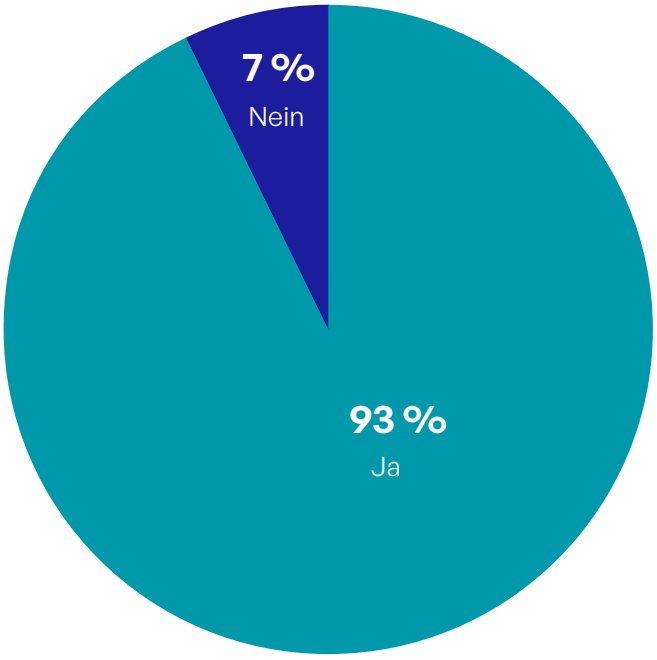


Abbildung 37: Organisationen, die sensible Inhalte klassifizieren

Viele Geschäftsfaktoren sprechen für die Klassifizierung

Die für die Datenklassifizierung angegebenen geschäftlichen Gründe sind vielfältig, wobei sieben der acht genannten Gründe von mindestens 10 % der Befragten an erster Stelle genannt wurden (Abbildung 38). Der Schutz personenbezogener Daten scheint die höchste Priorität zu haben, wobei die Einhaltung von Datenschutzbestimmungen (35 %), der Schutz personenbezogener Daten von Mitarbeitern (27 %) und die Einhaltung von Datenschutzbestimmungen für Kunden und Partner (26 %) am häufigsten als die beiden wichtigsten Prioritäten genannt wurden. Aber auch der Schutz von persönlichen Gesundheitsdaten und geistigem Eigentum sowie die Einhaltung einer Vielzahl von Branchenvorschriften und -standards sind häufig genannte Prioritäten.

Eine weitere Triebfeder für die Datenklassifizierung ist die Frage, welche Mitarbeiter Offline-Zugriff auf sensible Inhalte benötigen. 98 % der Befragten müssen Führungskräften, Vorstandsmitgliedern und Außendienstmitarbeitern Offline-Zugriff gewähren, während 92 % dies auch für ihre Vertriebs- und Kundenbetreuungsteams benötigen. Die höchste Priorität haben Führungskräfte auf Reisen. 41 % der Befragten insgesamt (Abbildung 39) und eine große Mehrheit aller Unternehmen unabhängig von ihrer Größe und den meisten Branchen gaben dies an.

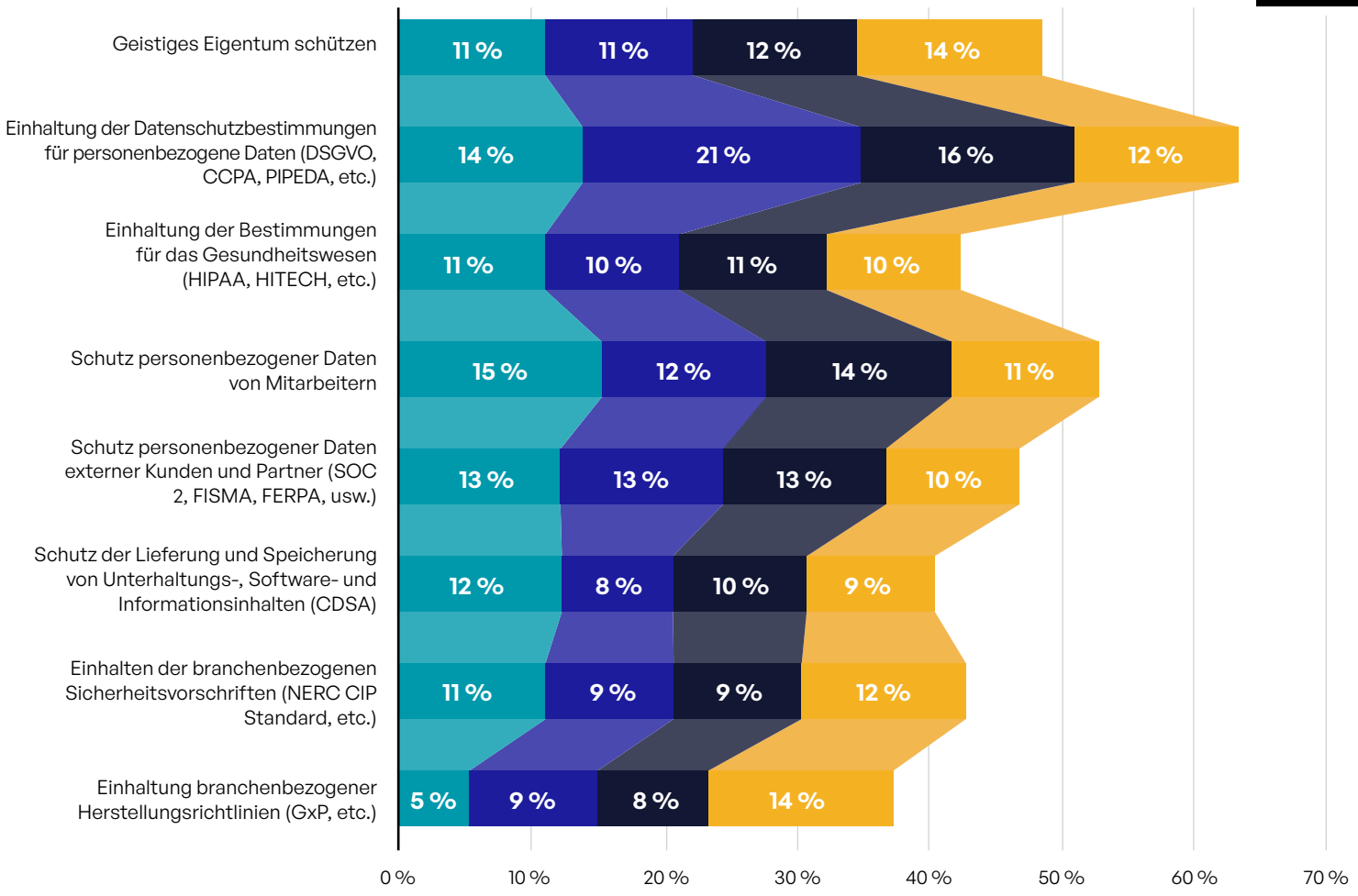


Abbildung 38: Treiber für die Datenklassifizierung

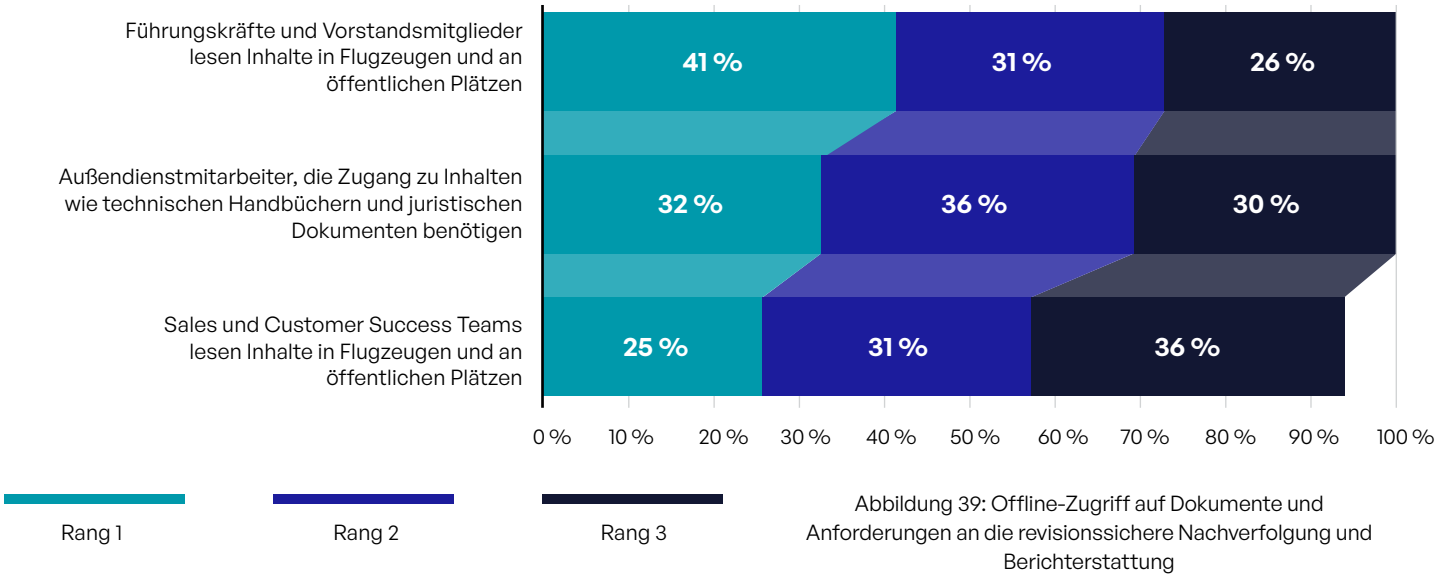


Abbildung 39: Offline-Zugriff auf Dokumente und Anforderungen an die revisionssichere Nachverfolgung und Berichterstattung

Anforderungen an - und Hindernisse für - die Einführung von DRM

Die Anforderungen von Frameworks wie NIST CSF und die Notwendigkeit, sensible Inhalte besser zu schützen, bedeuten, dass viele Unternehmen die Notwendigkeit erkennen, über eine einfache Datenklassifizierung und -kontrolle hinauszugehen. Um die nächste Stufe zu erreichen, beginnen sie mit der Einführung von DRM. DRM-Tools können zum Schutz sensibler Inhalte eingesetzt werden, wenn diese an externe Parteien weitergegeben werden. DRM ist nicht neu, es existiert schon seit Jahrzehnten. Leider halten die meisten DRM-Bemühungen und -Projekte nicht, was sie versprechen. Es fehlt an der notwendigen Kontrolle und Sicherheit, und der Schutz der digitalen Werte vor internen und externen Bedrohungen ist unzureichend.

Wir haben die Umfrageteilnehmer nach ihren wichtigsten Anforderungen an eine DRM-Lösung gefragt und sie gebeten, sechs mögliche Antworten in eine Rangfolge zu bringen. Wie bei vielen unserer Ranking-Fragen waren die Antworten sehr unterschiedlich. Wenn man sie gewichtet, gewinnt in einem Fotofinish die Benutzerfreundlichkeit, gefolgt vom Schutz der “Kronjuwelen” des Unternehmens und einer vollständigen und umfassenden Protokollierung (Abbildung 40).

Auf die Frage nach den Stolpersteinen bei der Einführung von DRM nannten 55 % der Befragten als zweitwichtigstes Problem die Suche nach einem Tool, das in der Lage ist, Compliance-Standards zu erfüllen, wobei der Zugriff an Benutzer, Rollen und Inhaltsklassen gebunden ist (Abbildung 41). Ebenfalls häufig genannt wurden die Notwendigkeit, auf den Clients externer Partner unverschlüsselte Inhalte öffnen zu können (53 % der Nennungen) und die Notwendigkeit, alle Arten von Inhalten anzeigen und bearbeiten zu können (50 %).

Ganzheitliche Compliance-Funktionen sind ein noch größeres Hindernis für Unternehmen aus den Bereichen Energie und Versorgung (72 % in den Top 2), Recht (62 %), öffentliche Verwaltung (61 %), Technologie (61 %) und Dienstleistungen (60 %). Der Bedarf ist besonders belastend für Vertreter der Bereiche Dienstleistungen (70 %), Kommunalverwaltung (69 %) und Technologie (61 %).

Abbildung 40: Gewichtete Bewertung: Größte DRM-Herausforderungen für die Kommunikation sensibler Inhalte

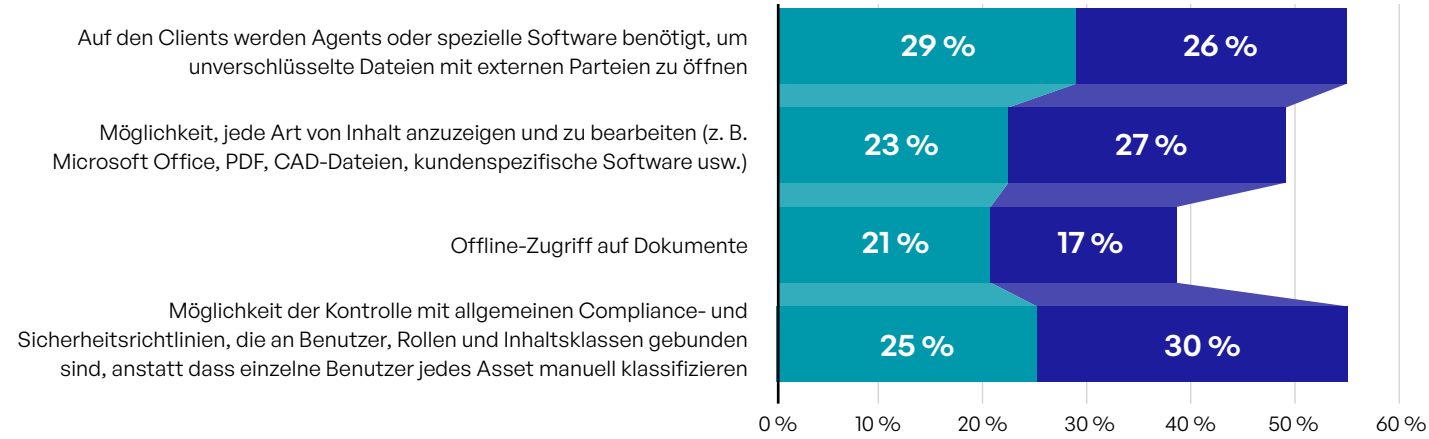


Abbildung 41: Die größten Stolpersteine bei DRM/eDRM

NIST CSF und DRM: Best Practices für die Kommunikation sensibler Inhalte

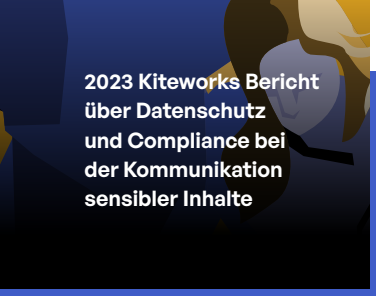
Wie bereits erwähnt, entwickelt sich das NIST CSF de facto zu einem globalen Standard, obwohl es von der US-Regierung für die Cybersicherheit von US-Organisationen entwickelt wurde. Wie ein Marktbeobachter bemerkte, ist das NIST CSF zur "gemeinsamen Sprache der internationalen Cybersicherheit" geworden.[18]

Das Vorhandensein eines gemeinsamen Frameworks eröffnet eine faszinierende Möglichkeit - die Möglichkeit, die gesamte sensible Datei- und E-Mail-Kommunikation auf einer einzigen Plattform mit auf diesem Framework basierenden Richtlinien zu verfolgen und zu kontrollieren. Dies kann einen inhaltsdefinierten Zero-Trust-Ansatz ermöglichen, der es Administratoren erlaubt, den Zugriff auf bestimmte Inhaltsklassen nach Rolle - oder sogar nach individuellem Benutzer - zu verfolgen und zu kontrollieren, und zwar in einer Weise, die dem NIST CSF und einer Vielzahl anderer Anforderungen entspricht.

Eine solche Plattform kann die nächste Generation des Digital Rights Management (DRM) einleiten. Laut Gartner besteht DRM aus drei Elementen:[19]

- **Es hat ein kryptografisches Element:** Informationen werden verschlüsselt, so dass der Schutz mit den Daten mitreist, unabhängig davon, wo sie sich bewegen oder ruhen.
- **Es hat ein Identitätselement:** Benutzer müssen authentifiziert werden und den Richtlinien für bestimmte Benutzerrollen und -gruppen entsprechen, bevor sie auf geschützte Daten auf einem beliebigen System zugreifen können.
- **Es verfügt über ein Element der granularen Nutzungskontrolle:** Benutzer erhalten bestimmte Rechte innerhalb von Anwendungen (z. B. die Möglichkeit, sensible Informationen nur anzuzeigen, zu bearbeiten, zu drucken, zu kopieren/einzufügen oder Screenshots zu erstellen).

Dies könnte Unternehmen in die Lage versetzen, die Kontrolle über die Informationslieferkette von externen Parteien zu übernehmen, die unseren Daten zufolge in den meisten Unternehmen aus Tausenden von Verbindungen besteht. Sie können die Kontrolle über die Sicherheit sensibler Inhalte übernehmen, die über alle Kanäle ausgetauscht werden, einschließlich E-Mail, Filesharing, Managed File Transfer und Webformulare.



Alle Teile Zusammenfügen

Wir sind optimistisch und gehen davon aus, dass wir jedes Jahr, wenn wir unseren Bericht über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte veröffentlichen, schrittweise Verbesserungen bei den Risiken für Datenschutz und Compliance bei der Kommunikation sensibler Inhalte feststellen werden. Auch wenn wir in diesem Jahr in einigen Bereichen Verbesserungen feststellen konnten, gibt es immer noch zu viele Bereiche, in denen sich die Situation nicht verbessert oder sogar verschlechtert hat (autsch!). Beispielsweise geben fast drei Viertel der Unternehmen an, dass sie bei der Bemessung und dem Management von Sicherheits- und Compliance-Risiken noch Verbesserungsbedarf haben. Ein noch höherer Prozentsatz der Befragten - 78 % - verfolgt und kontrolliert noch nicht die Kommunikation mit sensiblen Inhalten, weder vor Ort noch in der Cloud, und auch nicht für alle Arten von Inhalten in allen Abteilungen.

Dies geschieht zu einer Zeit, in der dringender Handlungsbedarf besteht. Kriminelle Akteure richten ihre Angriffe zunehmend auf sensible Inhalte, und ihre Taktiken werden immer raffinierter.

Gleichzeitig stellen Menschen allzu oft ihre Menschlichkeit unter Beweis, indem sie versehentlich sensible Inhalte öffentlich oder an eine Gruppe von Personen weitergeben, die nichts davon wissen müssen. Als Reaktion auf diese sich schnell entwickelnde Bedrohungslandschaft entwickeln die Aufsichtsbehörden strengere Anforderungen und führen uns alle - ob wir wollen oder nicht - in ein Zeitalter der Compliance.

Leider bedeuten Finanzknappheit und Fachkräftemangel im Bereich der Cybersicherheit, dass es unmöglich ist, das Problem mit Personal zu lösen - wenn es denn überhaupt funktionieren würde. Die Unternehmen haben keine andere Wahl, als mit den gleichen Mitarbeitern wie bisher gegen eine wachsende Zahl von Bedrohungen anzukämpfen und immer höhere Compliance-Ziele zu erreichen. Das ist für jede Organisation eine entmutigende Aufgabe.

Es gibt einige ermutigende Anzeichen. Bei der Analyse unserer Umfrageergebnisse haben wir Anzeichen dafür gefunden, dass Führungskräfte und Experten die Sicherheits- und Compliance-Probleme bei der Kommunikation mit sensiblen Inhalten erkannt haben und der Lösung dieser Probleme Priorität einräumen. Wir sind zuversichtlich, dass der Bericht des nächsten Jahres zeigen wird, dass die Unternehmen dieses Problem besser im Griff haben und es sowohl effizient als auch effektiv angehen.

Da die Sicherheit der Kommunikation mit sensiblen Inhalten in der Vergangenheit bei vielen Unternehmen zu kurz gekommen ist, haben diejenigen, die dieses Thema ernst nehmen, im kommenden Jahr die Chance, einen großen Beitrag zur Verbesserung ihres Gesamtrisikoprofils zu leisten. Die wichtigsten Prioritäten für 2023 sollten sein:

- **Ein ganzheitlicher Compliance-Ansatz:** Ein Flickenteppich von Vorschriften in verschiedenen Rechtsordnungen - in den USA sogar von Bundesstaat zu Bundesstaat - zwingt Unternehmen, ihren Fokus zu verlagern. In der neuen Ära der Compliance müssen Unternehmen aufhören, sich auf die Kästchen jeder einzelnen Vorschrift zu konzentrieren, und sich stattdessen an universelle Best Practices halten, die die Einhaltung aller Vorschriften ermöglichen. Wir glauben, dass der beste Ansatz darin besteht, ein universelles Framework wie das NIST CSF zu übernehmen und auf die vollständige Einhaltung aller Elemente hinzuarbeiten. Dies führt zu DRM.
- **Verfolgen eines DRM-Ansatzes:** Es ist von entscheidender Bedeutung, dass Unternehmen einen ganzheitlichen Ansatz verfolgen, um Daten granular zu kategorisieren und jede Kategorie denjenigen leicht zugänglich zu machen, die sie zur Erfüllung ihrer Aufgaben benötigen - und für alle anderen unzugänglich zu machen.
- **Schutz vor internen Bedrohungen:** Mitarbeiter und andere Personen mit Zugang zu internen Systemen sind für fast jede fünfte Datenschutzverletzung verantwortlich.[21] Durch die Klassifizierung und Segmentierung von Daten und die Beschränkung des Zugriffs auf bestimmte Datentypen je nach Rolle können sich Unternehmen vor böswilliger, gut gemeinter oder versehentlicher Datenweitergabe durch Insider schützen.
- **Umfassende Sicherheitsfunktionen:** Cyberkriminelle und Schurkenstaaten erkennen den Wert sensibler Inhalte und zielen auf Schwachstellen und Lücken in den Sicherheitsmechanismen der Kommunikationstools ab, mit denen diese Informationen übermittelt und verbreitet werden. Es ist wichtig, die Sicherheitsfunktionen Ihrer Kommunikationstools zu verstehen und zu überprüfen. Eine Überprüfung anhand der in diesem Bericht genannten Prioritäten ist ein guter Ausgangspunkt.

Damit Unternehmen arbeiten können, müssen sie häufig sensible Inhalte mit Hunderten oder Tausenden von externen Parteien austauschen - ganz zu schweigen davon, dass sie es internen Parteien ermöglichen, diese Informationen zu senden, auszutauschen, zusammenzuarbeiten und zu speichern. Die Bewegung dieser Daten stellt ein enormes Risiko dar, und der Schutz dieser Datenbewegungen sollte im Zeitalter der Compliance eine Priorität für jedes Unternehmen sein. Der Schutz der Kommunikation sensibler Inhalte sollte neben der Sicherheit von Netzwerken, Endgeräten und Anwendungen sowie der Sicherheit von Datenspeichern, die sensible Inhalte enthalten, Priorität haben.

Für viele Unternehmen ist dies nach wie vor eine der größten Sicherheitslücken. Das Kiteworks Private Content Network (PCN) ermöglicht fortschrittliches DRM, indem es Unternehmen hilft, die gesamte Kommunikation sensibler Datei- und E-Mail-Daten auf einer einzigen NIST CSF-konformen Plattform nachzuverfolgen und zu kontrollieren.

Literaturhinweise

[1] "M-Trends 2023," Mandiant, Mai 2023.

[2] "2023 Data Breach Investigations Report," Verizon, Juni 2023.

[3] ebd.

[4] Graham Greenleaf, "Now 157 Countries Have Data Privacy Laws," UNSW Law Research, 15. März 2022.

[5] "US State Privacy Legislation Tracker," International Association of Privacy Professionals, updated 9. Juni 2023.

[6] "2023 Data Breach Investigations Report," Verizon, Juni 2023.

[7] Bei unseren "gewichteten Bewertungen" der verschiedenen Ranking-Fragen in diesem Bericht haben wir den Rang 1 im Vergleich zum Rang 4 8-mal so stark gewichtet. Die Ränge 2 und 3 wurden 4- bzw. 2-mal so stark gewichtet wie der jeweilige Rang 4. Die Rankings wurden auf einer 100-Punkte-Skala berechnet.

[8] "2023 Data Breach Investigations Report," Verizon, Juni 2023.

[9] Carly Page, "Hackers Launch Another Wave of Mass-hacks Targeting Company File Transfer Tools," TechCrunch, 2. Juni 2023; "GoAnywhere MFT Hack Impacts Up to 1 Million Community Health Systems Patients and Growing Gootloader Attacks," Defensorum, 18. Februar 2023.

[10] "The State of Cloud-Native Security Report 2023," PrismaCloud und Palo Alto Networks, Zugriff am 15. Juni 2023.

[11] "Defenseless: A Statistical Report on the State of Cybersecurity Maturity Across the Defense Industrial Base (DIB)," Cybersheath Cybersecurity Report 2022, Dezember 2022.

[12] "The History of HIPAA," Accountable, 7. April 2021.

[13] Elizabeth Schultze, "The U.S. Wants to Copy Europe's Strict Data Privacy Law—But Only Some of It," CNBC, 23. Mai 2019.

[14] "US State Privacy Legislation Tracker," International Association of Privacy Professionals, aktualisiert am 9. Juni 2023.

[15] Willem Hendrickx, "NIST's Cybersecurity Framework Has Become the Common Language for International Cybersecurity," SC Media, 19. Mai 2022.

[16] Martin Armstrong, "Data Protection Fines Reach Record High in 2023," Statista, Mai 2023.

[17] "M-Trends 2023," Mandiant, Mai 2023.

[18] Willem Hendrickx, "NIST's Cybersecurity Framework Has Become the Common Language for International Cybersecurity," SC Media, 19. Mai 2022.

[19] John Girard and Marc-Antoine Meunier, "Succeed With Digital Rights Management, Five Steps at a Time," Gartner, 21. November 2018.

[20] "Global Cybersecurity Outlook 2023," World Economic Forum and Accenture, Januar 2023.

[21] "2023 Data Breach Investigations Report," Verizon, Juni 2023.

Kiteworks