Kiteworks

2024

Prognose zum Umgang mit dem Risiko der Offenlegung vertraulicher Inhalte

12 Prognosen für die Kommunikation sensibler Inhalte in Bezug auf Cyberkriminalität, Cybersicherheit und Compliance-Trends

BERICHT

Einleitung: Das Risiko der Offenlegung vertraulicher Inhalte verstehen

Das Management Ihrer Datenschutz- und Compliance-Risiken wird von Jahr zu Jahr zunehmend schwieriger. Cyberkriminelle entwickeln ihre Strategien und Ansätze ständig weiter, was die Identifizierung, Eindämmung und Minderung der Schäden durch bösartige Angriffe erschwert.[1] In der Erkenntnis, dass sie mit einem erfolgreichen Angriff in Hunderte oder sogar Tausende von Unternehmen und Millionen von Datensätzen eindringen können, haben sich viele Schurkenstaaten und Cyberkriminelle der Lieferkette zugewandt, ein Trend, der sich unserer Meinung nach im Jahr 2024 noch verstärken wird. Auf Drittanbieter, einschließlich Technologieanbieter, entfielen im letzten Jahr 15 % aller erfolgreichen Datenschutzverletzungen.[2] Und da generative Künstliche Intelligenz (GenKI) und große Sprachmodelle (Large Language Models, LLMs) die digitale Landschaft im Sturm erobern, wurde das Nachverfolgen und Kontrollieren unserer sensiblen Inhalte noch schwieriger.

Als Reaktion darauf haben Aufsichtsbehörden ihre bestehenden Datenschutzbestimmungen weiterentwickelt und neue hinzugefügt. Sie haben auch die Bußgelder und Strafen für die Nichteinhaltung der Vorschriften verschärft. Diese “reaktionäre Bewegung” wird nicht nachlassen, sondern im kommenden Jahr an Fahrt aufnehmen. All dies bedeutet, dass Unternehmen den Zugriff auf Inhalte nachverfolgen und kontrollieren und mehr Audit-Logs erstellen müssen, um die Einhaltung der für sie relevanten Compliance-Anforderungen nachzuweisen.

Der vorliegende Prognosebericht 2024 von Kiteworks für die Kommunikation sensibler Inhalte untersucht die wichtigsten Trends des vergangenen Jahres und zeigt auf, was wir im kommenden Jahr erwarten. Zweifellos ist das Management des Datenschutzes und der Compliance der Kommunikation mit sensiblen Inhalten - E-Mail, Filesharing, Managed File Transfer (MFT), SFTP und Webformulare - eine schwierige Aufgabe, da viele der verwendeten Tools in Silos untergebracht sind. Darüber hinaus fehlen vielen dieser Tools, die vor einem Jahrzehnt oder noch früher entwickelt wurden, die fortschrittlichen Sicherheitsfunktionen, die notwendig sind, um sensible Inhalte vor bösartigen Cyberangriffen zu schützen. Infolgedessen Jahr kam es in diesem Jahr zu einigen schwerwiegenden Datenschutzverletzungen. Die Unternehmen sind alarmiert und viele überprüfen ihre aktuellen Tools für die Datei- und E-Mail-Datenkommunikation und evaluieren Alternativen. Anstatt diese Tools in getrennten Silos zu behalten, werden immer mehr Unternehmen im Jahr 2024 versuchen, sie auf einer Plattform zu zentralisieren (stellen Sie sich vor, Sie hätten nur ein Audit-Log und eine konsolidierte Richtlinienverwaltung an einem Ort).

12 Prognosen für Datenschutz und Compliance bei der Datenübertragung von Dateien und E-Mails für 2024

1. Datenschutz und Compliance-Risiko von KI LLMs

Trotz Verboten und Einschränkungen wird sich die Anzahl der Mitarbeiter und externer Parteien, die GenKI LLMs nutzen, voraussichtlich ab 2023 verdoppeln, da die Wettbewerbsvorteile zu bedeutend sind, um sie zu ignorieren. Beispielsweise posten 15 % der Mitarbeiter regelmäßig Unternehmensdaten in GenKI LLMs und ein Viertel dieser Daten gilt als sensibel.[3] Dies wird die Angriffsfläche erweitern und das Potenzial für eine versehentliche oder absichtliche Offenlegung von geistigem Eigentum (Intellectual Property, IP), personenbezogenen Daten, persönlichen Gesundheitsdaten, Finanzdokumenten, Kommunikation zu Fusionen und Übernahmen (M&A) und anderen sensiblen Inhalten, einschließlich AI-Anweisungen erhöhen und das Risiko von Datenlecks und die damit verbundenen Auswirkungen auf den Markenschaden, Geldbußen und Strafen sowie Rechtskosten steigern.

Selbst mit Fortschritten in der Sicherheitskontrolle werden Datenschutzverletzungen, die aus dem Missbrauch von GenKI LLMs resultieren, im Jahr 2024 zunehmen. Prominente Beispiele, die das Kundenvertrauen gefährden und die Aufsichtsbehörden auf den Plan rufen, sind wahrscheinlich zu erwarten. Dies wird die Datensicherheit zu einem zentralen Bestandteil der GenKI LLM-Strategien machen. Unternehmen, die sich nur langsam anpassen, müssen mit Reputationsverlusten, Umsatzeinbußen, potenziellen Bußgeldern und Strafen sowie laufenden Kosten für Rechtsstreitigkeiten rechnen.

Um Risiken zu minimieren, werden führende Unternehmen inhaltsbasierte Zero-Trust-Modelle implementieren, um den Zugriff und die Zusammenarbeit auf der Grundlage der Datensensibilität zu steuern, indem sie granulare Zugriffskontrollen und den Zugriff mit den geringstmöglichen Rechten (Least-Privilege-Zugriff) standardmäßig hinzuzufügen und den nicht authentifizierten Zugriff eliminieren. Dieser Übergang zu Zero Trust auf der Inhalts-Ebene beinhaltet auch die Integration von Echtzeit-Richtlinien zum Schutz vor Datenverlust (Data Loss Prevention, DLP) sowie die Protokollierung und Überwachung aller Zugriffe auf und Bewegungen von Inhalten.

Ausgereifte Funktionen zum Schutz vor Datenverlusten, die eine gründliche Prüfung der Inhalte und eine adaptive Risikobewertung nutzen, werden sich von Geräten und E-Mails auf die Echtzeit-Überwachung von GenKI LLM-Interaktionen ausdehnen. Der Einsatz von Digital Rights Management (DRM) für besonders risikoreiche Inhalte wird drastisch zunehmen um die Zusammenarbeit zu ermöglichen und gleichzeitig die Extraktion von Daten zu verhindern. Auch die Investitionen in Schulungen, die für das Thema Datensicherheit sensibilisieren sollen, werden steigen, um Mitarbeiter für den verantwortungsvollen Umgang mit GenKI LLMs zu schulen. Diejenigen, die jetzt handeln, um unstrukturierte Daten zu schützen und strenge Nachverfolgungs- und Kontrollmaßnahmen für Governance und Sicherheit einzuführen, werden ihre Sicherheits- und Compliance-Risiken reduzieren.

Fast zwei Drittel der Unternehmen experimentieren (29 %) mit GenKI oder bauen diese aus (33 %).[4]

Nur 20 % der Unternehmen haben Prozesse eingeführt, um die Verwendung personenbezogener Daten in GenKI LLMs zu reduzieren.[5]

2. Datenschutz und KI LLM Vorschriften und Standards

Wie bereits erwähnt, birgt das Aufkommen von GenKI LLMs erhebliche Datenschutz- und Compliance-Risiken für Unternehmen, und die Aufsichtsbehörden sind bemüht, Vorschriften und Standards für KI zu erlassen.

Im Zentrum dieser regulatorischen Aktivitäten steht die Executive Order (EO) des Weißen Hauses vom 30. Oktober, die darauf abzielt, die Risiken der KI zu überwachen und zu regulieren und gleichzeitig ihr Potenzial zu nutzen. Die EO ruft auch den Kongress zum Handeln auf und fordert insbesondere die Bundesbehörden auf, im Lauf des nächsten Jahres tätig zu werden. Die EO legt neue Standards für die Sicherheit und Sicherheit von KI fest, schützt die persönlichen Daten der US-Bürger und fördert ein faires, offenes und wettbewerbsfähiges Ökosystem und Marktplatz für KI und verwandte Technologien.[6] Die Verordnung stützt sich auf die Leitlinien des National Institute of Standards and Technology (NIST) und legt Anforderungen für die Nutzung, Bewertung und Beschaffung von KI-Software und -Systemen durch die US-Bundesregierung fest.[7] Die EO konzentriert sich nicht nur auf die Auswirkungen von KI auf den Arbeitsmarkt, sondern verpflichtet auch die Entwickler leistungsfähiger KI-Systeme dazu verpflichten, die Ergebnisse ihrer Sicherheitstests mit der Bundesregierung zu teilen, bevor sie der Öffentlichkeit zugänglich gemacht werden.

Die EO ist der erste Schritt im Plan der Bundesregierung, sich mit KI auseinanderzusetzen, und wir werden wahrscheinlich ab 2024 Gesetze auf US-Bundes- und einzelstaatlicher Ebene sehen. Derzeit ziehen mindestens 25 US-Bundesstaaten KI-bezogene Gesetzgebung in Betracht, und 15 haben Gesetze oder Resolutionen verabschiedet.[8]

Außerhalb der USA arbeitet die EU an einem KI-Gesetz, das bis 2026 schrittweise in Kraft treten wird.[9] Das Gesetz zielt darauf ab, denjenigen die KI entwickeln, bereitstellen und benutzen klare Anforderungen und Verpflichtungen hinsichtlich spezifischer KI-Anwendungen zu bieten und gleichzeitig den administrativen und finanziellen Aufwand für Unternehmen, insbesondere kleine und mittlere Unternehmen (KMU), zu reduzieren. Das Gesetz definiert vier Risikostufen für KI: inakzeptables Risiko, hohes Risiko, begrenztes Risiko und minimales oder kein Risiko. KI-Systeme mit hohem Risiko unterliegen strengen Auflagen, bevor sie auf den Markt gebracht werden dürfen.

Ein Bereich, in dem KI-Standards entstehen, ist das National Institute of Standards and Technology (NIST). Das NIST AI RMF Playbook legt besonderen Wert auf die Etablierung von Richtlinien, um den Risiken bei Drittsystemen zu begegnen, die Überprüfung der Sicherheit und Resilienz durch Red-Team-Übungen, die Implementierung von Data Governance und Datenschutzkontrollen, die Ermöglichung von Transparenz und Rechtsmitteln, die Dokumentation der Nachverfolgbarkeit von Systemen, die Stärkung der Aufsichtsfunktionen und die Integration des Risikomanagements in Richtlinien und Verfahren.[10] Im Jahr 2024 werden sich Unternehmen, die das NIST AI RMF nutzen, weiterhin darauf konzentrieren, die mit sensiblen Inhalten verbundenen Risiken durch robuste technische Kontrollen in Verbindung mit verantwortungsvollen KI-Verfahren wie Verständlichkeit, Rechenschaftspflicht und transparente Risikokommunikation zu managen.

Mit dem Inkrafttreten von Sicherheitsanforderungen und -standards müssen Unternehmen in der Lage sein, die Einhaltung gesetzlicher Standards einfach und schnell nachzuweisen, und die Nachvollziehbarkeit von Governance, beispielsweise mit detaillierten Audit-Logs, wird wichtig sein. Experten gehen davon aus, dass KI-Standards frühestens in der zweiten Hälfte des Jahres 2024 implementiert und durchgesetzt werden; die Governance-Strukturen dafür zu schaffen und funktionsfähig zu machen, wird einige Zeit in Anspruch nehmen.

Forrester prognostiziert, dass es mindestens drei Datenschutzverletzungen im Zusammenhang mit unsicherem von KI-generierten Code geben wird, und mindestens ein Unternehmen wird wegen seines Umgangs mit personenbezogenen Daten bestraft werden.[11]

3. Notwendigkeit eines modernen MFT-Ansatzes

Viele Lösungen für Managed File Transfer (MFT) basieren auf jahrzehntealter Technologie, die inhärente Sicherheitsmängel aufweist. Vor-Ort-Implementierungen, die von vielen Kunden bevorzugt werden, bestehen aus verschiedenen Funktionen, die in Silos untergebracht sind und keine vom Anbieter bereitgestellte Härtung (engl. Hardening) aufweisen. Die Kunden müssen eine Hardening-Strategie definieren und implementieren, wie Netzwerk- und Webanwendungs-Firewalls, Intrusion Detection, Entfernung von ungenutzten Diensten und Code sowie Antivirentechnologien. Aufgrund des isolierten Ansatzes liegt die Verantwortung für das Schwachstellenmanagement beim Kunden. Er muss feststellen, ob Code aktualisiert werden muss, kompatible Versionen aller Silo-Komponenten finden, die aktualisierten Komponenten Integrationstests unterziehen und sie dann in die Produktion migrieren. Darüber hinaus mangelt es vielen älteren MFT-Lösungen oft an fortschrittlicher Sicherheitstechnologie, wie Data Loss Prevention (DLP), Advanced Threat Prevention (ATP) und Content Disarm & Reconstruction (CDR).

Unternehmen werden im Jahr 2024 einen modernen Ansatz für virtuelle Appliances suchen, der es ihnen ermöglicht, mit nur einem Klick ein einheitliches Update vom MFT-Anbieter zu erhalten. Sie werden auch nach MFT-Lösungen suchen, die fortschrittliche Sicherheitsfunktionen integrieren, um der beispiellosen Komplexität und Menge von Cyberbedrohungen zu begegnen.

MFT-Tools werden für den automatisierten, zuverlässigen und sicheren digitalen Datenaustausch innerhalb des Unternehmens und mit externen Parteien eingesetzt, wobei die Einahltung der Vorschriften durch Governance-Tracking und -Kontrollen gewährleistet ist. Als Teil der Software-Lieferkette ist das Risiko veralteter MFT-Lösungen dramatisch. In den letzten Jahren haben wir eine spiralförmige Eskalation von Cyberangriffen auf die Software-Lieferkette durch Schurkenstaaten und Cyberkriminelle erlebt. Anfang dieses Jahres enthüllte IBM in seinem „Cost of a Data Breach Report“, dass 12 % der Datenschutzverletzungen die Software-Lieferkette betreffen. Gleichzeitig sind externe Parteien, die Teil der Software-Lieferkette sind, ein wichtiger Risikofaktor, da 15 % der Datenschutzverletzungen auf Dritte zurückzuführen sind.[12]

Zwei bedeutende MFT-Tools wurden 2023 durch Zero-Day-Exploits von Clop, einer russischen Cyber-Gang, angegriffen, die bereits in der Vergangenheit MFT-Tools ins Visier genommen hatte. In beiden Fällen wurden mehrere Zero-Day-Schwachstellen ausgenutzt - eine Remote-Code-Execution (RCE) bei Fortra GoAnywhere, von der mehr als 130 Organisationen betroffen waren[13] und eine SQL-Injection bei MOVEit, die über 2.000 Organisationen und 62 Millionen Einzelpersonen betraf.[14]

Wenn die beiden MFT-Angriffe im Jahr 2023 ein Indikator sind, werden Schurkenstaaten und Cyberkriminelle auch im Jahr 2024 Zero-Day-Schwachstellen in veralteten MFT-Lösungen ausnutzen. Wenn ein MFT-Tool gehackt wird, kann das Auswirkungen auf die Lieferkette haben und sensible Daten von Hunderten oder sogar Tausenden von Unternehmen, die Millionen von Einzelpersonen repräsentieren, offenlegen. Die Folgen können dramatisch sein und Bußgelder, Strafen, Rechtskosten, Sammelklagen und Markenschäden nach sich ziehen.

12 % der Datenschutzverletzungen im letzten Jahr betrafen die Software-Lieferkette.[15]

4. Die Notwendigkeit eines modernen E-Mail-Protection-Gateways

E-Mails sind nach wie vor der wichtigste Angriffsvektor für Malware und Phishing. Malware-Angriffe, die über E-Mails eingeleitet wurden, haben im vergangenen Jahr um 29 % zugenommen, während Phishing-Angriffe ebenfalls um 29 % und der BEC-Angriffe (Business E-Mail Compromise) um 66 % gestiegen sind.[16] Der Verizon Data Breach Investigations Report hat ergeben, dass sich die Zahl der BEC-Angriffe im Vergleich zum Vorjahr verdoppelt hat und der durchschnittliche Betrag, der pro Angriff gestohlen wurde, bei 50.000 Dollar lag.[17] Bei Phishing- und BEC-Angriffen erschweren das Fehlen robuster Filtern und der mangelnde Einblick in den Kontext von E-Mails die Erkennung und Abwehr ausgeklügelter Angriffe, die Social-Engineering-Taktiken nutzen. Mehr als 8 von 10 Datenschutzverletzungen zielen in erster Linie auf den Menschenals ersten Zugang ab, indem sie Social-Engineering-Strategien verwenden.[18] Darüber hinaus sind herkömmliche E-Mail-Sicherheitskonzepte gegen Zero-Day-Angriffe wirkungslos und verlassen sich auf das Bewusstsein der Nutzer, verdächtige E-Mails zu erkennen und zu melden; das Problem dabei ist, dass die Nutzer durch ausgeklügelte Angriffe leicht getäuscht werden können.

Wie bei veralteten MFT-Lösungen fehlen auch bei herkömmlichen E-Mail-Systemen moderne Sicherheitsfunktionen. Die gute Nachricht ist, dass wir eine signifikante Verbesserung bei der E-Mail-Verschlüsselung beobachtet haben. Eine Umfrage unter IT-Führungskräften ergab, dass 90 % den Schutz von Dokumenten und Informationen, die sie per E-Mail mit anderen Unternehmen austauschen, priorisieren.[19] Wenn diese intern geteilt werden, sind die Zahlen nicht so gut: 79 % der Unternehmen geben an, sensible Geschäftsdaten unverschlüsselt per E-Mail auszutauschen.[20] Und selbst wenn Unternehmen ihre E-Mails verschlüsseln, verwenden laut einer aktuellen Studie nur 35 % der Unternehmen eine umfassende Verschlüsselung.[21]

Es gibt mehrere Gründe, warum Unternehmen sich mit der E-Mail-Verschlüsselung schwer tun. Ein Grund ist, dass sie komplex und schwierig zu handhaben sein kann.[22] Es gibt verschiedene Arten und Ebenen der Verschlüsselung (z. B. PGP, S/MIME, DANE, STARTTLS), und der Austausch von öffentlichen Schlüsseln kann mühsam und oft riskant sein. Wenn verschlüsselte E-Mails nicht entschlüsselt werden können, müssen Unternehmen auf weniger als ideale (und weniger sichere) Optionen zurückgreifen, wie zum Beispiel die Anmeldung bei einem kostenlosen, aber nicht autorisierten E-Mail-Dienst, um den Inhalt zu übertragen, den Absender bitten, einen unverschlüsselten, aber nicht öffentlichen Link zu einem gemeinsamen Laufwerk zu verwenden, oder den Absender bitten, eine passwortgeschützte Zip-Datei zu senden.

Natürlich gibt es noch andere Sicherheitsmängel bei E-Mails, wie zum Beispiel das Fehlen von digitaler Rechteverwaltung (Digital Rights Management, DRM), Datenverlustprävention (Data Loss Prevention, DLP) und fortschrittlicher Bedrohungserkennung (Advanced Threat Detection), unsichere Cloud-Speicherung, die Verschlüsselung und Zugriffskontrollen fehlen, schlechtes Identitäts- und Zugriffsmanagement und veraltete oder falsch konfigurierte Mailserver vor Ort.

Aufgrund der oben genannten Fakten wird die E-Mail-Sicherheit für viele Unternehmen auch im Jahr 2024 eine Herausforderung bleiben. Solange Unternehmen kein E-Mail-Protection-Gateway einsetzen, welches das Versenden, Empfangen und Speichern von E-Mails über ein Zero-Trust-Richtlinienmanagement mit Single-Tenant-Hosting ermöglicht, wird die E-Mail-Sicherheit ein ernstzunehmendes Risiko bleiben - sowohl in Bezug auf den Datenschutz als auch auf die Einhaltung gesetzlicher Vorschriften.

Phishing-Angriffe stiegen im letzten Jahr um 47,2 % an, wobei vor allem der Bildungssektor und Finanzdienstleistungen ins Visier genommen wurden.[23]

5. Zunehmende Datenschutzbestimmungen und -standards

Im Jahr 2023 haben die Datenschutzbestimmungen und -standards weiter zugenommen. Gartner prognostiziert, dass bis Ende 2024 die personenbezogenen Daten von drei Vierteln der Weltbevölkerung unter Datenschutzbestimmungen fallen werden und das durchschnittliche jährliche Budget für Datenschutz in einem Unternehmen 2,5 Millionen US-Dollar überschreiten wird.[24] In den nächsten zwei Jahren werden die Bemühungen zur Regulierung des Datenschutzes auf Dutzende von Gerichtsbarkeiten ausgeweitet. So haben beispielsweise neben Kalifornien vier weitere US-Bundesstaaten im Jahr 2023 Datenschutzgesetze verabschiedet und zehn weitere haben bereits Datenschutzgesetze verabschiedet, deren Inkrafttreten in den Jahren 2024 und 2025 erfolgen wird. In zahlreichen anderen Staaten befinden sich Datenschutzgesetze in verschiedenen Stadien der legislativen Beratung.

Datenschutz ist nicht nur ein US-amerikanisches Phänomen. Es ist ein globales Anliegen, und im Jahr 2024 werden Datenschutzbestimmungen mit Sicherheit weiter an Bedeutung gewinnen. Neben der Datenschutz-Grundverordnung (DSGVO) sind beispielsweise mehrere EU-Gesetze in Vorbereitung, darunter der Digital Markets Act, der Digital Services Act und die KI-Verordnung.

Im Juli 2023 verabschiedete die EU ein neues Data Privacy Framework, das Datentransfers aus der EU, dem Vereinigten Königreich und der Schweiz in die USA erleichtert und den Selbstzertifizierungsprozess für Unternehmen beschreibt, die daran teilnehmen möchten. Um teilnehmen zu können, muss ein US-Unternehmen eine Selbstzertifizierung gegenüber dem US-Handelsministerium (Department of Commerce) abgeben und verpflichten, die Grundsätze der jeweiligen Rahmenvereinbarung(en) einzuhalten. Die Einhaltung ist verpflichtend, sobald ein Unternehmen sich selbst zertifiziert hat. Das US-Handelsministerium führt eine öffentliche Liste der teilnehmenden Unternehmen. Ein Unternehmen muss auf der Liste stehen, um die Teilnahme zu erwirken und personenbezogene Daten im Einklang mit den Rahmenvereinbarungen zu erhalten. Wenn ein Unternehmen von der Liste gestrichen wird, muss es die Behauptung der Teilnahme und Compliance einstellen. Es muss die Grundsätze jedoch weiterhin auf die zuvor erhaltenen Daten anwenden. Das EU-US Data Privacy Framework erleichtert den transatlantischen Datenfluss, der für Unternehmen von entscheidender Bedeutung ist, und gewährleistet gleichzeitig den Schutz personenbezogener Daten.

Das NIST Privacy Framework wurde 2020 veröffentlicht und hat sich als wertvoller Leitfaden erwiesen. Basierend auf den Entwürfen für Aktualisierungen des NIST Cybersecurity Framework (CSF) wird das Data Privacy Framework wahrscheinlich im Jahr 2024 erweitert, um das Risikomanagement von Unternehmen in den Bereichen Recht, Finanzen und Datenschutz zu verbessern. Dies wird Unternehmen besser positionieren, um Datenschutzrisiken ganzheitlich zu bewerten und zu mindern. Die Anpassung des Data Privacy Frameworks auf das geplante Bundesdatenschutzgesetz deutet darauf hin, dass es ein wichtiges Compliance-Instrument sein wird, da sich die Vorschriften weiterentwickeln. Aktualisierungen, die wir wahrscheinlich im Jahr 2024 sehen werden, umfassen eine verbesserte Integration mit dem NIST Cybersecurity Framework, um Datenschutz als Unternehmensrisiko neben anderen Bereichen wie Finanzen und Recht besser zu adressieren, eine erweiterte Anleitung für das Management von Datenschutzrisiken im gesamten Unternehmen, nicht nur in IT-Systemen,[25] und die Anpassung an neue Datenschutzbestimmungen zur Unterstützung der Compliance.[26]

Erwähnenswert sind auch die erwarteten Änderungen am Cybersecurity Framework (CSF) des NIST. Das NIST hat im August 2023 einen Entwurf zur Aktualisierung des CSF veröffentlicht und plant, die endgültige Version CSF 2.0 Anfang 2024 zu veröffentlichen.[27] Das aktualisierte Framework zielt darauf ab, ein breiteres Spektrum von Unternehmen anzusprechen und gleichzeitig das Risikomanagement zu verbessern. Zu den wichtigsten Änderungen gehören die Betonung kontinuierlicher Risikobewertungen, die Priorisierung kontinuierlicher Verbesserungen, die Stärkung des Risikomanagements in der Lieferkette und die Bereitstellung weiterer Implementierungsbeispiele. Der Nachweis der Einhaltung der sich ständig weiterentwickelnden und neuen Datenschutzbestimmungen bleibt für viele Unternehmen eine Herausforderung. Es ist zu erwarten, dass im Jahr 2024 mehr Unternehmen die Governance zentralisieren und Audit-Logs für die Nachverfolgung und Berichterstattung nutzen werden. Da jedoch viele Unternehmen immer noch von isolierten Kommunikationsansätzen für sensible Inhalte berichten, kann dies ein schwieriges Unterfangen sein.

6. Zunehmende Bedeutung der Datenhoheit

Die Lokalisierung von Daten ist ein wachsender Trend, der die Datensouveränität für Unternehmen im Jahr 2024 zu einer Herausforderung macht.[28] Die Konferenz der Vereinten Nationen für Handel und Entwicklung berichtet, dass 70 % der Länder regeln, wie Unternehmen Daten über ihre Bürger erfassen, speichern und verwenden.[29] Viele neue Datenschutzgesetze verlangen von Unternehmen, die Kontrolle darüber zu behalten, in welchem Land Daten gespeichert werden. Dies kann eine erhebliche Herausforderung für multinationale Unternehmen darstellen. Gleichzeitig ist die Demokratisierung von Daten, also die Praxis, Daten für jeden in einem Unternehmen unabhängig von technischen Fähigkeiten zugänglich und nutzbar zu machen, ein Trend, der sich auf die Datenhoheit auswirken wird. Dieser Trend wird Unternehmen dazu veranlassen, sicherzustellen, dass Daten für alle Beteiligten zugänglich sind, während die Datenhoheit gewahrt bleibt. Die Datenhoheit bezieht sich auf alle Arten von Daten, einschließlich personenbezogener Daten, sowie andere Daten, im Zusammenhang mit den Aktivitäten und dem Betrieb eines Unternehmens.

Unternehmen in allen Wirtschaftssektoren, einschließlich Behörden, Technologie, Gesundheitswesen und Finanzdienstleistungen, priorisieren zunehmend Initiativen zur Datenhoheit aufgrund der zahlreichen damit verbundenen Vorteile. Die Datenhoheit ermöglicht es Unternehmen, die Einhaltung lokaler und internationaler Datenschutzvorschriften zu gewährleisten, was rechtliche Risiken minimiert, einen Ruf für verantwortungsvollen Umgang mit Daten schafft und Unternehmen vor hohen Bußgeldern schützt. Durch die Priorisierung der Datenhoheit können Unternehmen das Vertrauen von Kunden und Stakeholdern stärken, den Ruf ihrer Marke verbessern und kostspielige rechtliche Probleme vermeiden.

Entscheidungen über die Bereitstellung von Anwendungen werden stark von den Anforderungen der Datenhoheit beeinflusst, insbesondere in Ländern mit strengen Gesetzen, wie Deutschland und China. Der United States CLOUD Act, der US-Unternehmen dazu verpflichtet, Daten auf Anordnung oder Vorladung herauszugeben, unabhängig davon, wo sie gespeichert sind, erschwert den internationalen Betrieb und kann möglicherweise gegen Vorschriften wie die DSGVO verstoßen. Multi-Tenant-Hosting-Optionen können die Einhaltung der Datenhoheit erschweren und es für Unternehmen schwieriger machen, die Einhaltung von Gesetzen zur Datenlokalisierung nachzuweisen.

Kunden, die Datenhoheit fordern, ziehen es oft vor, mit Anbietern zusammenzuarbeiten, die Dienstleistungen im eigenen Land hosten. Für Cloud-basierte Dienste könnten Hosting-Zonen im Inland ausreichen, es sei denn, sie sind von Gesetzen wie dem US CLOUD Act betroffen. In komplexeren Szenarien entscheiden sich Unternehmen zunehmend für das Hosting im eigenen Land oder nutzen Funktionen zur Datenhoheit in ihren Anwendungen, um länderübergreifende Implementierungen zu verwalten, obwohl dies bei Compliance-Audits zu Problemen führen kann.[30]

Wenn sich Anwendungscluster über mehrere Länder erstrecken, ist die Funktionalität von Datenhoheitszonen eine wertvolle Fähigkeit. Um die oben genannten Herausforderungen im Jahr 2024 zu meistern, sollten Unternehmen auf Single-Tenant-Hosting zurückgreifen, das die Datenhoheit und die Fähigkeit der Unternehmen, diese nachzuweisen, vereinfacht.

Unternehmen werden sich zunehmend für das Hosting im eigenen Land entscheiden oder Funktionen zur Datenhoheit in ihren Anwendungen nutzen, um länderübergreifende Implementierungen zu verwalten, auch wenn dies bei Compliance-Audits zu Problemen führen kann.

7. Erhöhte Bußgelder für Datenschutzverstöße

Strafen und Bußgelder im Zusammenhang mit Datenschutzverstößen haben in den letzten zwei Jahren zugenommen, einschließlich der rekordverdächtigen Bußgelder für Verstöße gegen die DSGVO, und werden voraussichtlich auch im Jahr 2024 weiter steigen. Einige bemerkenswerte Fälle aus dem Jahr 2023 beinhalten eine Strafe von 1,3 Milliarden US-Dollar gegen Meta (Facebook) durch die irische Datenschutzkommission, 391,5 Millionen US-Dollar gegen Google in einem Vergleich mit 40 US-Bundesstaaten, 61,7 Millionen US-Dollar gegen Amazon durch die FTC und 2,1 Millionen US-Dollar gegen Uber, ebenfalls durch die FTC.

Die Aufsichtsbehörden konzentrieren sich auf die Durchsetzung von Datenschutzgesetzen und verhängen Strafen bei Verstößen. Laxe Corporate Governance und Sicherheit machen Unternehmen zu einem leichteren Ziel für Aufsichtsbehörden, die mit harten Strafen ein Exempel statuieren können. Die in jüngster Zeit verhängten hohen Geldstrafen, wie die gegen Marriott und British Airways im Rahmen der DSGVO, waren zum großen Teil auf Mängel im Bereich der Datensicherheit zurückzuführen. Dieser Präzedenzfall deutet darauf hin, dass Aufsichtsbehörden hart gegen Unternehmen vorgehen werden, die fahrlässig personenbezogene Daten preisgeben. Mit der Verabschiedung zusätzlicher Datenschutzgesetze, sowohl von einzelnen US-Bundesstaaten als auch weltweit, werden die strafrechtlichen Folgen weiter verschärfen.

Die Durchsetzung von Datenschutzbestimmungen wird auch im Jahr 2024 nicht nachlassen, da der größte Teil der Weltbevölkerung inzwischen von Datenschutzbestimmungen erfasst wird. Mit dem wachsenden Fokus auf Datenschutz werden immer mehr Unternehmen spezielle Datenschutzverfahren einführen. Für Unternehmen, die in mehreren Ländern tätig sind, erfordert dies einen neuen Ansatz bei der Gestaltung und Beschaffung von Cloud-Service-Modellen, um unterschiedlichen Lokalisierungsstrategien im Jahr 2024 gerecht zu werden.

Im ersten Halbjahr 2023 wurden mehr DSGVO-Strafen verhängt als in den Jahren 2019, 2020 und 2021 zusammen - sie erreichten über 1,8 Milliarden US-Dollar.[31]

75 % der weltweiten Bevölkerung werden bis Ende 2024 mit ihren personenbezogenen Daten unter Datenschutz-bestimmungen fallen.[32]

8. Einführung von FedRAMP-autorisierten Lösungen für die Kommunikation sensibler Inhalte

Der von Präsident Joe Biden unterzeichnete James M. Inhofe National Defense Authorization Act (NDAA) für das Haushaltsjahr 2023 verankert das FedRAMP-Programm innerhalb der General Services Administration und implementiert wichtige Änderungen im FedRAMP-Programm, um die Prozesse für die Einführung und Nutzung von Cloud-Diensten durch die Regierung weiter zu optimieren. Das Office of Management and Budget (OMB) hat außerdem einen Entwurf für einen Leitfaden zur Modernisierung von FedRAMP veröffentlicht, um den heutigen Herausforderungen der Cloud zu begegnen. Dieser Entwurf enthält einen Plan zur Skalierung von FedRAMP, zur Stärkung seines Ansatzes zur Sicherheitsüberprüfung und zur Beschleunigung der sicheren Einführung von Cloud-Produkten und -Diensten in der US-Bundesregierung.[33]

Bis 2024 wird die FedRAMP-Autorisierung, die durch einen strengen jährlichen Auditprozess erreicht wird, voraussichtlich eine Grundvoraussetzung für jeden Cloud-Service-Anbieter sein, der mit der US-Bundesregierung zusammenarbeiten möchte. Für Auftragnehmer der Defense Insdustrial Base (DIB) beinhaltet die Cybersecurity Maturity Model Certification (CMMC) 2.0 die FedRAMP-Anforderungen, und mit einer FedRAMP-autorisierten Datei- und E-Mail-Datenkommunikationen ist der Nachweis der Compliance für DIB-Auftragnehmer wesentlich einfacher. Da immer mehr DIB-Vertragspartner die CMMC Level 2 Zertifizierung im Jahr 2024 anstreben, werden DIB-Auftragnehmer Technologielösungen suchen, die auch für die Datei- und E-Mail-Datenkommunikation verwendet werden können.

9. Aufkommen des Digital Rights Managements zum Schutz sensibler Inhalte

Die Einführung der digitalen Rechteverwaltung (Digital Rights Management, DRM) wird sich beschleunigen, da Unternehmen bestrebt sind, sensible Inhalte zu schützen und die zunehmenden Vorschriften einzuhalten.[34] Marktforscher prognostizieren ein starkes Wachstum des DRM-Marktes, der bis 2024 möglicherweise über 5 Milliarden US-Dollar erreichen könnte.[35] Gartner weist darauf hin, dass die Einbindung von DRM in weiterreichende Technologie-Trends einen starken Einfluss haben und 2024 für Unternehmen einen immer höheren Stellenwert einnehmen wird.[36] Für das Management von inhaltsdefinierten Richtlinien werden sich Unternehmen an Sicherheitsstandards wie dem NIST Cybersecurity Framework (CSF) und NIST 800-53 orientieren.

Zu den wichtigsten Antriebsfaktoren zählen zunehmende Cyberbedrohungen, Datenschutzgesetze und die Notwendigkeit, den internen und externen Austausch von Inhalten zu kontrollieren. DRM der nächsten Generation ist für den Datenschutz von entscheidender Bedeutung, da es einen anhaltenden Schutz sensibler Daten auch außerhalb der Unternehmensgrenzen bietet. Um mit DRM erfolgreich zu sein, benötigen Unternehmen einheitliche Nachverfolgung, Kontrolle und Transparenz in ihren digitalen Ökosystemen. Dies erfordert die Einhaltung von Best Practices in Bezug auf Governance, Workflows und Zugriffskontrollen.

Im Jahr 2024 werden Datenklassifizierung und DRM-Richtlinienmanagement die Unternehmen dazu veranlassen, einen Datenschutz zu implementieren, der für Daten mit geringem Risiko den Zugriff mit den geringsten Rechten und Wasserzeichen vorsieht, für Daten mit mittlerem Risiko ein „view only“ DRM und für Daten mit hohem Risiko ein sicheres Video-Stream-Management, das Downloads und Copy & Paste blockiert. Stark regulierte Branchen werden die größten Nutzer von DRM der nächsten Generation sein. Das Gesundheitswesen beispielsweise, das zu den am stärksten von Cyberangriffen betroffenen Branchen gehört, muss immense Mengen an personenbezogenen Daten und persönlichen Gesundheitsinformationen schützen, die innerhalb ihrer Organisationen und mit unzähligen Dritten ausgetauscht, gesendet, empfangen und gespeichert werden. Finanzdienstleister, Hersteller, Anwaltskanzleien, Regierungsbehörden und Bildungseinrichtungen gehören ebenfalls zu den Branchen, in denen der Austausch von Dateien und E-Mails mit hohen Risiken und drastischen Konsequenzen verbunden ist. Sie werden sich daher zunehmend mit DRM der nächsten Generation befassen, um ihre Datenschutz- und Compliance-Risiken zu managen.

Nur 22 % der Unternehmen verfügen über Richtlinien und Systeme zur Nachverfolgung und Kontrolle des Zugriffs auf sensible Inhalte und an wen diese gesendet und mit wem sie geteilt werden.[37]

10. Integration moderner Sicherheit in die Kommunikation mit sensiblen Inhalten

Fortschrittliche Cybersicherheits-Tools wie Cloud Data Loss Prevention (DLP), Advanced Threat Prevention (ATP) für die nächste Generation von Antivirenprogrammen sowie Sandbox-Detonation und Content-Disarmament & Rekonstruktion (CDR) können in Lösungen für das Senden, Teilen und Speichern sensibler Inhalte integriert werden. Im Jahr 2024 werden Unternehmen fortschrittliche Cybersicherheitstechnologien einsetzen, die die Anwendung von Richtlinien, Scans und Bereinigungen auf Daten während der Übertragung und im ruhenden Zustand ermöglichen. Mit DLP können Unternehmen ausgehende E-Mails und Anhänge scannen, um zu verhindern, dass sensibler Daten versehentlich weitergegeben werden. CDR kann eingehende Dokumente bereinigen, indem aktive Inhalte aus Sicherheitsgründen entfernt werden. MFT-Plattformen unterstützen häufig standardmäßig DLP, Virenschutz, Sandboxing und erweiterte Schutzfunktionen. Die Integration dieser Funktionen in den Inhaltsübertragungsprozess erhöht die Sicherheit. Datenlecks und -verluste werden verhindert, indem Übertragungen, die gegen Richtlinien verstoßen, blockiert werden. Malware wird durch Antiviren-Scans und Sandbox-Detonation am Eindringen in die Umgebung gehindert. Eingehende Inhalte werden durch CDR auf ihre Sicherheit überprüft.

Im Jahr 2024 werden Unternehmen einen besseren Einblick in den Informationsfluss haben wollen, um die Überwachung zu verbessern und detaillierte Audit-Logs zu erhalten. Die Durchsetzung von Sicherheitsrichtlinien wird durch die Konsolidierung in zentralisierten Plattformen wie MFT vereinfacht. Tools für die Kommunikation mit sensiblen Inhalten wie E-Mail, Filesharing, MFT und Webformulare werden alle von einer engen Integration mit ATP profitieren.

Der Markt für Content Disarm & Reconstruction (CDR) wird bis 2026 voraussichtlich mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von 15,7 % wachsen. Grund dafür sind die Kosten für Datenschutzverletzungen und die strengere Regulierung und Einhaltung von Vorschriften für die Sicherheit von Inhalten.[38]

Es wird erwartet, dass der Markt für Data Loss Prevention (DLP) mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von 22,3 % wachsen wird, wobei der Schwerpunkt auf Datenerkennung, Durchsetzung von Richtlinien, Datenklassifizierung und Reaktion auf Vorfälle liegen wird.[39]

11. Zentralisierung der Kommunikation mit sensiblen Inhalten und das PCN

Traditionelle Zero-Trust-Architekturen konzentrieren sich auf den Schutz des Netzwerkperimeters und die Überprüfung von Benutzern und Geräten, die eine Verbindung herstellen möchten. Inhalte jedoch existieren über den Perimeter hinaus und Netzwerke verstehen die Sensibilität von Inhalten nicht. Hier kommt das Paradigma der Private Content Networks (PCNs) ins Spiel, das die Bedeutung der Inhaltsensibilität über die Netzwerktopologie stellt. Ein PCN nutzt inhaltsdefinierte Vertrauensprinzipien, weist Inhalten Sensibilitätskennzeichen zu und setzt entsprechende Schutzmaßnahmen wie Verschlüsselung und Zugriffskontrolle auf Basis dieser Kennzeichen durch. Dies stellt sicher, dass die Sicherheitsmaßnahmen dem Grad der Sensibilität des Inhalts entsprechen und nicht nur seinem Standort innerhalb der Netzwerkinfrastruktur.

Die PCN-Architektur geht über traditionelle Zero-Trust-Modelle hinaus, indem sie ein umfassendes Richtlinienmanagement integriert, das sich dynamisch an die Sensibilitätsklassifikation des Inhalts anpasst. Dieses System setzt automatisch Risikorichtlinien durch, die die Rolle des Benutzers, die Klassifikation des Inhalts und die beabsichtigten Aktionen berücksichtigen und somit die Legitimität und den Umfang der Zugriffs- oder Übertragungsberechtigungen bestimmen. Eine solche Granularität in der Durchsetzung von Richtlinien ist entscheidend für die Aufrechterhaltung strenger Sicherheitsvorkehrungen, insbesondere bei der Verarbeitung sensibler Daten, die zusätzliche Überprüfungsschritte wie Begründungsformulare oder Unterschriften von Vorgesetzten erfordern.

Das PCN bietet auch einen robusten Logging-Mechanismus, der alle Interaktionen mit Inhalten akribisch aufzeichnet und so ein umfangreiches Audit-Log für die Einhaltung gesetzlicher Vorschriften und interne Reviews bereitstellt. Dieser Einblick in den Fluss und die Verwendung sensibler Daten ist ein Grundpfeiler des Zero-Trust-Ansatzes, der auf dem Prinzip “Nie vertrauen, immer überprüfen” beruht.

Die Ausweitung von Sicherheit und Compliance auf die Inhaltsebene wird 2024 weiter Dynamik gewinnen. Die Unternehmen werden einen besseren Schutz und eine effizientere Verwaltung der Kommunikationskanäle für sensible Inhalte in einer einheitlichen PCN-Plattform mit Zero-Trust-Sicherheits- und Compliance-Richtlinien anstreben.

Fast 75 % der Unternehmen geben an, dass ihre Messung und ihr Management der Kommunikation mit sensiblen Inhalten in hohem oder gewissem Maße verbesserungsbedürftig sind.[40]

12. Zunahme der Kommunikation von sehr großen Dateien mit sensiblen Inhalten

Die Herausforderungen im Umgang mit großen Dateien, die sensible Inhalte enthalten, werden für Unternehmen immer dringlicher. Die Ausweitung bestehender Anwendungsfälle für große Dateien ist in mehreren sich schnell entwickelnden Bereichen bemerkenswert. So erlebt beispielsweise die Biotechnologiebranche eine explosionsartige Zunahme der Größe von DNA-Sequenzdateien, da die Genforschung und die personalisierte Medizin an Bedeutung gewinnen. Ebenso führen Fortschritte in Design und Technik zu immer größeren und komplexeren CAD-Dateien. In der Strafverfolgung wird zunehmend auf Videobeweise zurückgegriffen, die sichere und effiziente Speicher- und Übertragungslösungen erfordern. Marketingabteilungen nutzen hochauflösende Videos und Grafiken, um Aufmerksamkeit zu erregen, und in den Bereichen Wirtschaft, Finanzhandel, Wissenschaft und medizinische Forschung werden Analysedateien immer größer und sensibler. Diese wachsenden Dateigrößen erfordern robuste Lösungen für den sicheren Umgang und die Speicherung.

Wie bereits erwähnt, ist ein weiterer Bereich, den es zu überwachen gilt, der Bereich der Trainingsdatensätze für private LLMs, ein noch junges, aber sich schnell entwickelndes Feld. Da diese Modelle immer ausgefeilter werden und auf spezifische Bedürfnisse von Unternehmen zugeschnitten sind, werden die Datensätze, auf denen sie trainieren, immer größer und sensibler. Dieser Trend deutet auf eine Zukunft hin, in der das Management von großen, sensiblen Trainingsdatensätzen zu einem wichtigen betrieblichen Anliegen wird.

Der Aspekt des Kunden-Supports bei Produkten, die Software enthalten, hat die Bedeutung des Umgangs mit großen Log- und HTTP-Archivdateien (HAR) hervorgehoben, die eine Fülle von sensiblen Informationen enthalten. Die Sicherheitslücke bei Okta ist eine deutliche Erinnerung an die Schwachstellen, die diese Dateien aufweisen können.[41] Diese Herausforderung wird dadurch verschärft, dass Mitarbeiter möglicherweise nicht genehmigte und unsichere Methoden zur Übertragung dieser großen Dateien verwenden, wodurch sich die Risiken für den Datenschutz erhöhen. Zwar haben auf Unternehmen ausgerichtete Cloud-Speicherlösungen wie Microsoft 365 und Box die Dateigrößenbeschränkungen auf bis zu 250 GB erhöht, doch dies ist immer noch unzureichend im Vergleich zu den Anforderungen der genannten Anwendungsfälle. Diese und andere Plattformen werden weiterhin unter Druck stehen, die sichere Übertragung und Speicherung immer größerer Dateien zu unterstützen, da die traditionellen Produktgrenzen hinter den Bedürfnissen moderner datenintensiver Geschäftsprozesse zurückbleiben.

Viele Unternehmen stoßen beim Austausch und der Übertragung sensibler Daten auf operative Herausforderungen, da viele Filesharing- und File-Transfer-Lösungen auf 250 GB oder weniger beschränkt sind.

Schlussfolgerung: Erkenntnisse aus unseren 12 Prognosen

Die Landschaft der Kommunikation mit sensiblen Inhalten verändert sich rasant aufgrund technologischer Innovationen und zunehmender regulatorischer Maßnahmen. Unternehmen stehen unter wachsendem Druck, vertrauliche Daten vor zunehmenden Cyberbedrohungen zu schützen und die Einhaltung immer strengerer internationaler Vorschriften und Standards zu gewährleisten.

Unser Prognosebericht 2024 zeigt die wichtigsten Trends auf, die die Sicherheit und Compliance von sensiblen Inhalten im Jahr 2024 beeinflussen werden. Zu den wichtigsten Erkenntnissen des Berichts gehören:

- Fortschrittliche KI-Technologien, einschließlich LLMs, stellen neue Herausforderungen für Datenschutz und Compliance dar, die eine strenge Governance, umfassende Sicherheitsmaßnahmen und die ethische Nutzung von KI erfordern.
- Künftige Vorschriften, wie die KI-Gesetzgebung der EU und die erwartete US-Bundesgesetzgebung, werden neue Standards für den Umgang mit personenbezogenen Daten setzen, die Unternehmen effektiv umsetzen müssen.
- Die Ausbreitung der Datenlokalisierung erfordert die Neugestaltung von Apps und Cloud-Konfigurationen, um den Anforderungen an die Datenhoheit gerecht zu werden.
- Zunehmende Bußgelder und Strafen für Datenschutzverletzungen erfordern verbesserte Governance- und Sicherheitsrahmen, um Verstöße zu verhindern.
- Die Weiterentwicklung des DRM ist für den fortlaufenden Schutz vertraulicher Informationen unerlässlich.
- Die Integration von fortschrittlicher Sicherheitstechnologien, einschließlich Cloud-basierter Data Loss Prevention (DLP), Advanced Threat Protection (ATP) und Content Disarm & Reconstruction (CDR), in Infrastrukturen für sensible Inhalte hilft, Sicherheitslücken zu schließen.
- Die Konsolidierung von Lösungen für Kommunikationskanäle wie E-Mail, Filesharing, Managed File Transfer und Webformulare in einem zusammenhängenden PCN verbessert die Sicherheit und die Einhaltung gesetzlicher Vorgaben.
- Neue Anwendungen in verschiedenen Bereichen erzeugen außergewöhnlich große Dateien, die die Kapazität traditioneller Systeme übersteigen.

Veraltete, isolierte Tools für die Kommunikation mit sensiblen Inhalten sind unzureichend, da sie die notwendigen fortschrittlichen Funktionen, integrierten Abwehrmaßnahmen und umfassende Governance vermissen lassen, um der sich verändernden Bedrohungslage zu begegnen. Durch die Einführung von Zero-Trust-Architekturen, detaillierten inhaltsbasierten Sicherheitsmodellen, einer starkem Zugriffsverwaltung und integriertem DRM, Data Loss Prevention und anderer modernster Sicherheitsmaßnahmen können Unternehmen Risiken mindern und die Einhaltung von Vorschriften in einem Umfeld zunehmender Regulierung gewährleisten. Wenn Sie Ihre Pläne für 2024 machen, sollten Sie Ihre Strategien zur Kommunikation sensibler Inhalte überdenken und sicherstellen, dass Sie die richtigen Technologien im Einsatz haben, um Ihre Datei- und E-Mail-Kommunikation zu schützen.

References

[1] "Cybersecurity Forecast 2024: Insights for future planning," Google Cloud, November 2023.

[2] "Sensitive Content Communications Privacy and Compliance 2023 Report," Kiteworks, August 2023.

[3] Stephanie Schappert, "Workers regularly post sensitive data into ChatGPT," cybernews, 16. Juni 2023.

[4] Matthew Guarini, "Predictions 2024: Tech Leaders Boost Ops To Grow With AI," Forrester Blog, 24. Oktober 2023.

[5] "The state of AI in 2023: Generative AI's breakout year," McKinsey, 1. August 2023.

[6] "FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence," The White House, 30. Oktober 2023.

[7] Shiva Aminian, et al., "President Biden Issues Long-Awaited Artificial Intelligence Executive Order," Akin, 30. Oktober 2023.

[8] "Artificial Intelligence 2023 Legislation," National Conference of State Legislatures, September 27, 2023.

[9] "Regulatory framework proposal on artificial intelligence," European Commission, abgerufen November 8, 2023.

[10] "NIST AI RMF Playbook," NIST, accessed November 8, 2023.

[11] Phil Muncaster, "Forrester: GenAI Will Lead to Breaches and Fines in 2024," Forrester, 2. November 2023.

[12] "Cost of a Data Breach Report 2023," IBM, Mai 2023.

[13] Becky Bracken, "Clop Keeps Racking Up Ransomware Victims With GoAnywhere Flaw," DARKREADING, 27. März 2023.

[14] Wes Davis, "MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023," The Verge, 10. November 2023.

[15] "Cost of a Data Breach Report 2023," IBM, Mai 2023.

[16] "Worldwide 2022 Email Phishing Statistics and Examples," Trend Micro, 31. Mai 2023.

[17] "Data Breach Investigations Report 2023," Verizon, März 2023.

[18] "Worldwide 2022 Email Phishing Statistics and Examples," Trend Micro, 31. Mai 2023.

[19] "90% of Organizations Prioritizing Email Encryption," Echoworx Blog, 4. Mai 2021.

[20] "Survey: 83 Percent of U.S. Organizations Have Accidentally Exposed Sensitive Data," Egress Press Release, 21. Februar 2019.

[21] "How to Protect Your Sensitive Information With Email Encryption," Pulse Technology, 18. September 2023.

[22] "Why Is Email Encryption Not Widely Used," Trustifi, 8. Februar 2021.

[23] Deepen Desai, et al., "2023 Phishing Report Reveals 47.2% Surge in Phishing Attacks Last Year," Zscaler Blog, 18. April 2023.

[24] "Gartner Identifies Top Five Trends in Privacy Through 2024," Gartner, 31. Mai 2022.

[25] "NIST Drafts Major Update to Its Widely Used Cybersecurity Framework," NIST, 8. August 2023.

[26] Valdez Ladd, "NIST's Privacy Framework for Proposed US Federal Privacy Law," ISACA, 15. Februar 2023.

[27] "NIST Drafts Major Update to Its Widely Used Cybersecurity Framework," NIST, 8. August 2023.

[28] "How to Achieve Data Compliance in 2024," Exadel, 16. Oktober 2023.

[29] "Data Sovereignty: Definition, Requirements, and How To Ensure It," Spanning, abgerufen 8. November 2023.

[30] "Understanding the Implications of Data Sovereignty and Why Data Residency may be a Better Choice for Your Business," Trustwave, 27. Oktober 2023.

[31] Alexis Porter, "Lessons Learned From GDPR Fines in 2023," CPO Magazine, 2. August 2023.

[32] "Gartner Identifies Top Five Trends in Privacy Through 2024," Gartner Press Release, 31. Mai 2022.

[33] Billy Mitchell, "With draft guidance, OMB kickstarts effort to modernize FedRAMP for today's cloud challenges," FEDSCOOP, 27. Oktober 2023.

[34] Katie Walsh, "13 Key Digital Asset Management Best Practices for 2024," Brandfolder, 26. Oktober 2023.

[35] "Digital Rights Management Market Research Report 2024-2030 | 98 Pages Report," Market Reports World, 3. November 2023.

[36] Rick Dagley, "Gartner Predicts Top 10 Strategic Technology Trends for 2024," ITProToday, 16. Oktober 2023.

[37] "Sensitive Content Communications Privacy and Compliance Report 2023," Kiteworks, Juli 2023.

[38] "Content Disarm and Reconstruction Market by Component (Solutions and Services), Application Area (Email, Web, FTP, and Removable Devices), Deployment Mode, Organization Size, Vertical, and Region—Global Forecast to 2026," MarketsandMarkets, Februar 2022.

[39] "Data Loss Prevention Market to be Worth $9.33 Billion by 2030," Grand View Research, 17. Juli, 2023.

[40] "Sensitive Content Communications Privacy and Compliance Report 2023," Kiteworks, Juli 2023.

[41] Bob Ertl, "How the Okta Customer Support Hack Exposed Sensitive Data and Access Credentials," Kiteworks Blog, 28. Oktober 2023.