Kiteworks

Nordamerika-Analyse 2024 für die Kommunikation sensibler Inhalte: Sicherheit und Compliance-Trends

HIGHLIGHTS

Verwendete Kommunikations-Tools	**16 %**	7+
	21 %	6
	29 %	5
	16 %	4
	13 %	3
	3 %	2
	0 %	1
Austausch sensibler Inhalte mit externen Parteien	**13 %**	über 5.000
	30 %	2.500 bis 4.999
	27 %	1.000 bis 2.499
	10 %	500 bis 999
	20 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	**50 %**	Finanzunterlagen
	46 %	Patienteninformationen
	44 %	Persönliche Daten
	43 %	GenKI LLMs
	39 %	Geistiges Eigentum
	37 %	Juristischer Schriftwechsel
	23 %	CUI und FCI
	17 %	M&A
Größter Fokus auf Datenschutz und Compliance (Top 2)	**53 %**	Datenschutzgesetze der U.S.-Staaten
	44 %	DSGVO
	31 %	HIPAA
	29 %	SEC-Anforderungen
	19 %	Länderspezifische Datenschutzgesetze
	16 %	CMMC
	9 %	PCI DSS
Wichtigste Sicherheits-validierungen (Top 2)	**50 %**	ISO 27001, 27017, 27018
	53 %	NIST 800-171/CMMC 2.0
	36 %	SOC 2 Type II
	37 %	IRAP (Australien)
	21 %	FedRAMP Moderate
	20 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	**10 %**	10+
	20 %	7 bis 9
	37 %	4 bis 6
	16 %	2 bis 3
	9 %	1
	9 %	weiß nicht

Der “2024 Kiteworks Sensitive Content Communications Privacy and Compliance Report” bietet eine detaillierte Analyse der Herausforderungen und Trends bei der Verwaltung sensibler Inhalte in verschiedenen Branchen, einschließlich Finanzdienstleistungen. Dieser Kurzbericht konzentriert sich auf die wichtigsten Ergebnisse in Bezug auf Finanzdienstleistungen und beleuchtet die für die Kommunikation sensibler Inhalte verwendeten Tools, Bedenken hinsichtlich der Cybersicherheit, Risiken bei der Kommunikation mit externen Parteien, spezifische Cyberbedrohungen und Auswirkungen auf die Compliance.

Verwaltung aller Kommunikations-Tools für sensible Inhalte

66 % der Finanzdienstleister nutzen fünf oder mehr Kommunikationstools, um vertrauliche Inhalte zu versenden und auszutauschen, was über dem weltweiten Durchschnitt von 53 % liegt. In Bezug auf die Nachverfolgung und Kontrolle sensibler Inhalte gaben 57 % der Finanzdienstleister an, dass sie in der Lage sind, intern versandte und ausgetauschte sensible Daten nachzuverfolgen und zu kontrollieren, während 49 % angaben, dass sie in der Lage sind, extern ausgetauschte sensible Daten nachzuverfolgen und zu kontrollieren.

Bei den Prioritäten für die Kommunikation sensibler Inhalte in Bezug auf Datenschutz und Compliance waren die beiden wichtigsten Prioritäten für Finanzdienstleister (57 %) die Verhinderung des Abflusses vertraulichen geistigen Eigentums und von Geschäftsgeheimnissen sowie die Eindämmung langwieriger und kostspieliger Rechtsstreitigkeiten. Weltweit, über alle Branchen hinweg, standen diese beiden Prioritäten an erster und zweiter Stelle, wenn auch in geringerem Maße (56 % bzw. 51 %). Die geringste Priorität wurde von den Befragten aus dem Finanzdienstleistungssektor der Vermeidung negativer Auswirkungen auf die Marke eingeräumt (15 %).

Bewertung des mit externen Parteien verbundenen Risikos in Bezug auf sensible Inhalte

Das Risikomanagement in Bezug auf externe Parteien stellt für Finanzdienstleister eine große Herausforderung dar. 43 % der Unternehmen geben an, dass sie sensible Inhalte mit mehr als 2.500 externen Parteien austauschen. Erstaunliche 70 % haben mehr als 1.000 externe Parteien in ihrer Content-Lieferkette (mehr als der Durchschnitt von 66 % in allen Branchen).

Dieses Bild ist besorgniserregend, da 44 % der befragten Finanzdienstleister angaben, dass sie sensible Inhalte in etwa der Hälfte der Fälle verfolgen und kontrollieren können, sobald sie eine Anwendung verlassen.

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

82 % der Unternehmen aus dem Finanzdienstleistungssektor gaben an, dass die Messung und das Management der Einhaltung der Vorschriften für die Kommunikation sensibler Inhalte etwas bis erheblich verbessert werden muss. Dies ist weniger als die Gesamtzahl der Befragten (88 %) angaben.

Die Finanzunternehmen nannten die Datenschutzgesetze der US-Bundesstaaten als wichtigste Priorität vor anderen Datenschutz- und Compliance-Vorschriften (53 % an erster oder zweiter Stelle). Dies ist keine große Überraschung, wenn man bedenkt, dass mittlerweile 18 Gesetze in den einzelnen Bundesstaaten verabschiedet wurden. 44 % der Unternehmen nannten die DSGVO als eine der beiden wichtigsten Vorschriften. PCI DSS wurde von 9 % der Finanzdienstleister an erster oder zweiter Stelle genannt.

Bei der Prüfung und Auswahl von Sicherheitsvalidierungen bzw. -zertifizierungen sind die Finanzdienstleister im Vergleich zu allen Umfrageteilnehmern näher zusammengerückt. So nannten 53 % der Befragten NIST 800-171/ CMMC 2.0 als eine der beiden wichtigsten Zertifizierungen. ISO 27001, 27017 und 27018 folgten mit 50 %, während die NIS 2-Richtlinie, die später in diesem Jahr in Kraft tritt, mit 9 % am seltensten genannt wurde. Dass NIST 800-171 die Liste anführt, ist eine kleine Überraschung, da diese Norm vor allem für Unternehmen gilt, die mit der US-Regierung und dem US-Verteidigungsministerium zusammenarbeiten.

Bewertung des Sicherheitsrisikos für sensible Inhalte

88 % der Unternehmen im Finanzdienstleistungssektor geben an, dass die Messung und das Management von Sicherheitsrisiken im Zusammenhang mit der Kommunikation sensibler Inhalte erheblich oder in gewissem Maße verbesserungsbedürftig sind (dasselbe Ergebnis wie im weltweiten Vergleich).

57 % der Finanzdienstleister gaben an, dass ihre sensiblen Inhalte fünfmal oder öfter verletzt wurden (30 % sagten, siebzigmal oder öfter). Fast 1 von 10 Befragten aus dem Finanzsektor gab an, dass sie sich nicht sicher sind, wie viele Datenschutzverstöße ihr Unternehmen erlebt hat.

Erweiterte Sicherheitsfunktionen und -verfahren wie Verschlüsselung, Multi-Faktor-Authentifizierung und Governance-Tracking und -Kontrolle werden von Finanzdienstleistern nur in 36 % der Fälle für einige sensible Inhalte eingesetzt (4 % setzen sie überhaupt nicht ein; 60 % setzen sie ständig ein). Diese Ergebnisse liegen unter den Ergebnissen der weltweiten Umfragen in den verschiedenen Branchen und zeigen ein potenzielles Problem für Finanzdienstleister auf.

Bewertung der Kosten für Sicherheit und Compliance

Wie in den meisten Wirtschaftszweigen zeigen die Umfrageergebnisse, dass die Finanzdienstleistungsbranche ein hohes Risiko für Datenschutzverletzungen darstellt. 30 % der Befragten gaben an, im vergangenen Jahr sieben oder mehr Datenschutzverletzungen erlebt zu haben. Dies ist etwas besser als der weltweite Durchschnitt, wo 32 % von mehr als sieben Datenschutzverletzungen berichteten. Weitere 37 % berichteten von vier bis sechs Datenschutzverletzungen.

Hinsichtlich der Kosten für Rechtsstreitigkeiten gaben 36 % der befragten Finanzunternehmen an, dass sie mehr als 5 Mio. USD pro Jahr ausgeben. Dies liegt über dem weltweiten Durchschnitt, bei dem 25 % angaben, dass ihre Kosten für Rechtsstreitigkeiten 5 Mio. USD übersteigen. Darüber hinaus gaben 55 % der befragten Finanzdienstleister an, dass sie mehr als 3 Mio. USD ausgeben, verglichen mit nur 45 % weltweit.

Kenntnis und Kategorisierung der Datentypen

19 % der Unternehmen im Finanzdienstleistungssektor gaben an, dass sie weniger als 25 % ihrer unstrukturierten Daten kennzeichnen und klassifizieren; weitere 23 % gaben an, dass sie weniger als die Hälfte kennzeichnen und klassifizieren. Diese Prozentsätze stimmen mit dem weltweiten Durchschnitt überein; 20 % taggen und klassifizieren weniger als ein Viertel.

Aber nicht alle unstrukturierten Daten müssen klassifiziert werden, zumindest gaben dies die meisten Befragten an. 20 % der Finanzunternehmen gaben an, dass mehr als 80 % klassifiziert werden müssen und weitere 23 % gaben an, dass mehr als 60 % klassifiziert werden müssen - oder anders ausgedrückt: 43 % gaben an, dass mehr als 60 % klassifiziert werden müssen. Dies zeigt eine Diskrepanz, insbesondere im Vergleich zum weltweiten Durchschnitt, wo 22 % weniger als ein Viertel und 35 % zwischen 40 % und 60 % taggen und klassifizieren.

Robustes Management sensibler Inhalte in EMEA ist unerlässlich

Der “Kiteworks 2024 Sensitive Content Communications Report” unterstreicht die dringende Notwendigkeit eines robusten Risiko- und Compliance-Managements bei der Kommunikation sensibler Inhalte in Finanzdienstleistungsunternehmen. Finanzdokumente wurden von den Befragten als die Datenart genannt, die das größte Risiko darstellt (50 %), obwohl auch andere häufig genannt wurden. Finanzunternehmen sind sicherlich ein Ziel krimineller Akteure; zwei Drittel hatten im letzten Jahr mehr als fünf Datenschutzverstöße zu verzeichnen.

Unternehmen im Finanzsektor verbringen viel Zeit mit der Verwaltung der Protokolle, die von den zahlreichen Kommunikationstools erzeugt werden, die sie für den Austausch und Versand sensibler Inhalte verwenden. Fast die Hälfte (48 %) der Befragten muss mehr als 11 Protokolle abgleichen, und 8 % der Befragten wissen nicht einmal, wie viele Protokolle sie abgleichen müssen. Dies führt zu einem enormen Stau in den Berichtsprotokollen. 11 % verbringen 2.500 Stunden oder mehr pro Jahr damit und weitere 20 % mehr als 2.000 Stunden.

Lesen Sie den vollständigen Bericht