Kiteworks

2024 Analyse der Kommunikation sensibler Inhalte im Finanzsektor: 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)	**53 %**	NIST 800-171/CMMC 2.0
	50 %	ISO 27001, 27017, 27018
	36 %	SOC 2 Type II
	37 %	IRAP (Australien)
	21 %	FedRAMP Moderate
	11 %	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 im Umgang mit sensiblen Inhalten in verschiedenen Branchen, einschließlich Finanzdienstleistungen. Dieser Kurzbericht konzentriert sich auf die wichtigsten Erkenntnisse in Bezug auf Finanzdienstleistungen und beleuchtet die für die Kommunikation sensibler Inhalte verwendeten Tools, Bedenken hinsichtlich der Cybersicherheit, Risiken bei der Kommunikation mit Dritten, spezifische Cyberbedrohungen und die Auswirkungen auf die Compliance.

Verwaltung aller Kommunikationstools für sensible Inhalte

66 % der Finanzdienstleister nutzen fünf oder mehr Kommunikationstools, um sensible 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, sensible Daten nachzuverfolgen und zu kontrollieren, die intern versendet und ausgetauscht werden, während 49 % angaben, dass sie in der Lage sind, sensible Daten nachzuverfolgen und zu kontrollieren, die extern ausgetauscht werden.

Wenn es um die Kommunikation sensibler Inhalte geht, sind die beiden wichtigsten Prioritäten für Finanzdienstleister (57 %), den Abfluss von vertraulichem geistigem Eigentum und Geschäftsgeheimnissen zu verhindern und langwierige und kostspielige Rechtsstreitigkeiten zu vermeiden. Über alle Branchen hinweg stehen 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 schädlicher Auswirkungen auf die Marke eingeräumt (15 %).

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

Das Management von Risiken, die von externen Parteien ausgehen, stellt für Finanzdienstleister eine große Herausforderung dar. 43 % gaben an, dass sie sensible Inhalte mit mehr als 2.500 externen Parteien austauschen. Erstaunliche 70 % haben mehr als 1.000 externe Parteien in ihrer Inhaltslieferkette (über dem Durchschnitt von 66 % in allen Branchen).

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

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

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

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

Wenn es um die Prüfung und Auswahl von Sicherheitsvalidierungen oder -zertifizierungen geht, 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. Es folgen 50 % für ISO 27001, 27017 und 27018. Die NIS 2-Richtlinie, die später in diesem Jahr in Kraft tritt, wurde mit 9 % am seltensten genannt. Dass NIST 800-171 an der Spitze der Liste steht, ist eine kleine Überraschung, da dieser Standard in erster Linie für Unternehmen gilt, die mit der US-Regierung und dem US-Verteidigungsministerium (DoD) Geschäfte machen.

Bewertung des Sicherheitsrisikos für sensible Inhalte

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

57 % der Finanzdienstleister gaben an, dass ihre sensiblen Inhalte fünfmal oder öfter angegriffen wurden (30 % gaben siebenmal oder öfter an). Fast jeder zehnte Befragte aus dem Finanzsektor gab an, nicht sicher zu sein, wie viele Datenschutzverletzungen es in seinem Unternehmen gegeben 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 denen weltweiter Umfragen in verschiedenen Branchen und weisen auf ein potenzielles Problem für Finanzdienstleister hin.

Bewertung der Kosten für Sicherheit und Compliance

Wie in den meisten Branchen zeigen die Daten der Umfrage, dass Finanzdienstleistungen ein hohes Risiko für Datenschutzverletzungen darstellen. 30 % der Befragten gaben an, im vergangenen Jahr sieben oder mehr Datenschutzverletzungen erlebt zu haben. Dies ist etwas besser als der weltweite Durchschnitt, der 32 % mit mehr als sieben Datenschutzverletzungen ausweist. Weitere 37 % gaben an, dass sie zwischen vier und sechs Datenschutzverletzungen hatten.

36 % der befragten Finanzunternehmen gaben an, jährlich mehr als 5 Mio. USD für Rechtsstreitigkeiten auszugeben. Dies ist mehr als der weltweite Durchschnitt, wonach 25 % der Befragten angaben, dass ihre Kosten für Rechtsstreitigkeiten 5 Mio. USD übersteigen. Darüber hinaus gaben 55 % der befragten Finanzdienstleister an, mehr als 3 Mio. USD für Rechtsstreitigkeiten auszugeben, 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 taggen und klassifizieren; weitere 23 % gaben an, dass sie weniger als die Hälfte taggen und klassifizieren. Diese Prozentsätze entsprechen dem weltweiten Durchschnitt, wonach 20 % weniger als ein Viertel kennzeichnen und klassifizieren.

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, weitere 23 %, also insgesamt 43 %, gaben an, dass mehr als 60 % klassifiziert werden müssen. Dies zeigt eine Diskrepanz, insbesondere im Vergleich zum weltweiten Durchschnitt, wonach 22 % weniger als ein Viertel und 35 % zwischen 40 % und 60 % taggen und klassifizieren.

Robustes Management sensibler Inhalte in EMEA ist unerlässlich

Der “2024 Kiteworks Sensitive Content Communications Privacy and Compliance Report” unterstreicht die dringende Notwendigkeit eines robusten Risiko- und Compliance-Managements für die Kommunikation sensibler Inhalte im Finanzsektor. Finanzdokumente wurden von den Befragten als der Datentyp mit dem höchsten Risiko (50 %) genannt, obwohl auch andere Datentypen häufig genannt wurden.Finanzunternehmen sind zweifellos ein Ziel für böswillige Akteure; zwei Drittel hatten mehr als fünf Datenschutzverletzungen im letzten Jahr.

Finanzunternehmen verbringen viel Zeit mit der Verwaltung der Protokolle, die von den zahlreichen Kommunikationstools erzeugt werden, die sie für den Austausch und die Übertragung 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 Protokollstau. 11 % verbringen 2.500 Stunden oder mehr pro Jahr damit und weitere 20 % mehr als 2.000 Stunden.

Lesen Sie den vollständigen Bericht