Kiteworks

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

HIGHLIGHTS

Verwendete Kommunikations-tools	19 %	7+
	21 %	6
	19 %	5
	21 %	4
	16 %	3
	3 %	2
	1 %	1
Austausch sensibler Inhalte mit externen Parteien	22 %	über 5.000
	29 %	2.500 bis 4.999
	21 %	1.000 bis 2.499
	16 %	500 bis 999
	12 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	49 %	Juristischer Schriftwechsel
	44 %	Finanzunterlagen
	43 %	Patienteninformationen
	42 %	Persönliche Daten
	41 %	Geistiges Eigentum
	38 %	GenKI LLMs
	31 %	CUI und FCI
	12 %	M&A
Größter Fokus auf Datenschutz und Compliance (Top 2)	41 %	Datenschutzgesetze der U.S.-Staaten
	40 %	HIPAA
	34 %	DSGVO
	33 %	SEC-Anforderungen
	21 %	CMMC
	19 %	Länderspezifische Datenschutzgesetze
	12 %	PCI DSS
Wichtigste Sicherheits-validierungen (Top 2)	47 %	SOC 2 Type II
	45 %	NIST 800-171/CMMC 2.0
	43 %	ISO 27001, 27017, 27018
	36 %	IRAP (Australien)
	21 %	FedRAMP Moderate
	8 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	12 %	10+
	22 %	7 bis 9
	26 %	4 bis 6
	17 %	2 bis 3
	14 %	1
	9 %	weiß nicht

Der “2024 Sensitive Content Communications Privacy and Compliance Report” von Kiteworks bietet eine detaillierte Analyse der Herausforderungen und Trends im Umgang mit sensiblen Inhalten in verschiedenen Branchen, einschließlich des Dienstleistungssektors. Der Bericht konzentriert sich auf die wichtigsten Ergebnisse für den Dienstleistungssektor und beleuchtet die für die Kommunikation sensibler Inhalte verwendeten Tools, Bedenken hinsichtlich der Cybersicherheit, Risiken bei der Kommunikation mit externen Parteien, spezifische Cyberbedrohungen und die Auswirkungen auf die Compliance.

Verwaltung aller Kommunikationstools für sensible Inhalte

59 % der professionellen Dienstleister verfügen über mehr als fünf Kommunikationstools für den Versand und Austausch sensibler Inhalte, was über dem Durchschnitt der gesamten Kohorte (53 %) liegt; 40 % verwenden sechs oder mehr Kommunikationstools. Hinsichtlich der Nachverfolgung und Kontrolle sensibler Inhalte gehören die professionellen Dienstleister zu den fortschrittlichsten: 71 % gaben an, dass sie sensible Inhalte nach dem Verlassen einer Anwendung nachverfolgen und kontrollieren können.

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

Aufgrund der großen Zahl externer Parteien, mit denen die professionellen Dienstleister sensible Inhalte übermitteln und austauschen, ist das Risiko einer Datenschutzverletzung durch externe Parteien bei den professionellen Dienstleistern höher als in den meisten anderen Branchen. 47 % gaben an, sensible Daten mit 2.500 oder mehr Dritten auszutauschen (68 % tauschen mit mehr als 1.000 externen Parteien aus). Diese Zahlen sind deutlich höher als in der Gesamtkohorte: 27 % gaben an, sensible Daten mit 2.500 externen Parteien auszutauschen und 54 % gaben an, dies mit 1.000 externen Parteien zu tun.

Die Tatsache, dass die Nachverfolgung und Kontrolle sensibler Daten innerhalb und außerhalb des Unternehmens für viele Unternehmen problematisch ist, erschwert deren Handhabung zusätzlich.

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

96 % der befragten Dienstleistungsunternehmen gaben an, dass bei der Messung und dem Management der Compliance für die Kommunikation sensibler Inhalte ein gewisser bis erheblicher Verbesserungsbedarf besteht. Dies ist deutlich mehr als alle anderen Befragten (88%).

Aufgrund der zahlreichen branchenübergreifenden Interaktionen, die von professionellen Dienstleistungsunternehmen durchgeführt werden, hat das regulatorische Umfeld zweifellos einen erheblichen Einfluss auf sie. Mehrere Compliance- und Datenschutzbestimmungen standen ganz oben auf der Liste der regulatorischen Prioritäten der Dienstleistungsunternehmen. 41 % nannten die neuen Datenschutzgesetze der US-Bundesstaaten, 40 % HIPAA, 34 % die DSGVO und 33 % die SEC-Vorschriften.

Die gleiche enge Gruppierung der Antworten ergab sich bei den Fragen zu Sicherheitsstandards und -validierungen: 47 % nannten SOC 2 Type II, 45 % NIST 800-171/CMMC 2.0 und 43 % ISO 27001, 27017 und 27018 als eine der beiden wichtigsten Prioritäten bei der Sicherheitsvalidierung und -zertifizierung.

Bewertung des Sicherheitsrisikos für sensible Inhalte

94 % der Befragten aus dem Dienstleistungssektor gaben an, dass die Messung und das Management von Sicherheitsrisiken im Zusammenhang mit der Kommunikation sensibler Inhalte in hohem oder gewissem Maße verbesserungsbedürftig sind, ein deutlich höherer Prozentsatz als der Durchschnitt der gesamten Kohorte (88 %).

34 % der Befragten aus dem Dienstleistungssektor gaben an, dass ihre sensiblen Inhalte sieben oder mehr Mal kompromittiert wurden. Dies ist etwas mehr als der Durchschnitt der gesamten Kohorte von 32 %.

Der Einsatz erweiterter Sicherheitsfunktionen zur Nachverfolgung, Kontrolle und Sicherheit ist bei Dienstleistungsunternehmen weit verbreitet. 71 % gaben an, dass sie sensible Inhalte nachverfolgen und kontrollieren können, wenn sie intern übermittelt werden, während 60 % angaben, dass sie dies auch können, wenn sie extern übermittelt oder weitergeleitet werden. Diese Reife spiegelt möglicherweise ein deutlich höheres Vertrauen in ihre Fähigkeit wider, Sicherheitsrisiken zu minimieren (siehe oben).

Ähnliches gilt für die Umfrageergebnisse zu den Kosten, die für die Eindämmung von Datenschutzverletzungen aufgewendet werden. Nur 10 % der Befragten gaben an, mehr als 7 Mio. USD pro Jahr auszugeben, 27 % mehr als 5 Mio. USD. Im Gegensatz dazu gaben 25 % aller Befragten an, 5 Mio. USD oder mehr auszugeben.

Kenntnis und Kategorisierung der Datentypen

Die Datenart, die den Befragten im Dienstleistungsbereich am meisten Sorgen bereitet, ist die juristische Kommunikation (49 %), gefolgt von Finanzdokumenten (44 %) und Patienteninformationen (43 %). 52 % der Befragten gaben an, dass sie etwa drei Viertel ihrer unstrukturierten Daten taggen und klassifizieren. Nicht alle unstrukturierten Daten müssen gekennzeichnet und klassifiziert werden. 24 % der Befragten gaben jedoch an, dass mehr als 80 % ihrer unstrukturierten Daten gekennzeichnet und klassifiziert werden sollten; 53 % gaben an, dass es 60 % oder mehr sind. Diese Zahlen sind deutlich höher als die der gesamten Kohorte, die 18 % für alle unstrukturierten Daten und 40 % für drei Viertel angab, was wahrscheinlich auf einen höheren Reifegrad im Dienstleistungssektor hinweist.

Robustes Management sensibler Inhalte ist im Dienstleistungsbereich unerlässlich

Der “2024 Sensitive Content Communications Report” von Kiteworks unterstreicht die dringende Notwendigkeit eines robusten Risiko- und Compliance-Managements für die Kommunikation sensibler Inhalte im Dienstleistungssektor.

Dienstleistungsunternehmen 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. 43 % der Befragten müssen mehr als 11 Protokolle abgleichen, das ist weniger als in der Gesamtkohorte (48 %). Darüber hinaus wussten 9 % der Befragten aus dem Bereich Professional Services nicht, wie viele Protokolle sie abgleichen müssen. Schließlich ist die Zahl der Arbeitsstunden, die für die Erstellung von Compliance-Berichten aus Protokollen aufgewendet werden, im Vergleich zu den meisten anderen Wirtschaftszweigen beträchtlich, was wahrscheinlich auf die Besonderheiten der Dienstleistungsbranche zurückzuführen ist. 38 % der Befragten wenden mehr als 2.000 Arbeitsstunden pro Jahr auf und 78 % mehr als 1.500 Stunden.

Lesen Sie den vollständigen Bericht