Kiteworks

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

HIGHLIGHTS

Verwendete Kommunikations-tools	**20 %**	7+
	15 %	6
	25 %	5
	20 %	4
	15 %	3
	0 %	2
	5 %	1
Austausch sensibler Inhalte mit externen Parteien	**5 %**	über 5.000
	35 %	2.500 bis 4.999
	20 %	1.000 bis 2.499
	15 %	500 bis 999
	25 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	**71 %**	Finanzunterlagen
	58 %	Juristischer Schriftwechsel
	42 %	GenKI LLMs
	33 %	Geistiges Eigentum
	29 %	M&A
	25 %	Patienteninformationen
	25 %	CUI und FCI
	17 %	Persönliche Daten
Größter Fokus auf Datenschutz und Compliance (Top 2)	**40 %**	DSGVO
	40 %	Datenschutzgesetze der U.S.-Staaten
	30 %	HIPAA
	30 %	SEC-Anforderungen
	30 %	Länderspezifische Datenschutzgesetze
	20 %	CMMC
	10 %	PCI DSS
Wichtigste Sicherheits-validierungen (Top 2)	**55 %**	NIST 800-171/CMMC 2.0
	50 %	IRAP (Australien)
	35 %	ISO 27001, 27017, 27018
	30 %	FedRAMP Moderate
	25 %	SOC 2 Type II
	5 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	**20 %**	7 bis 9
	20 %	4 bis 6
	40 %	2 bis 3
	15 %	1
	5 %	weiß nicht

Der “2024 Sensitive Content Communications Privacy and Compliance Report” von Kiteworks bietet eine eingehende Analyse der Herausforderungen und Trends im Umgang mit sensiblen Inhalten in verschiedenen Branchen, einschließlich der Rechtsbranche. Dieser Bericht konzentriert sich auf die wichtigsten Ergebnisse für den juristischen Sektor 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 Kommunikations-tools für sensible Inhalte

60 % der Anwaltskanzleien nutzen fünf oder mehr Kommunikationstools, um sensible Inhalte zu versenden und auszutauschen, und damit mehr als der Durchschnitt der gesamten Kohorte (53 %). Wenn es um die Verfolgung und Kontrolle sensibler Inhalte geht, gaben 60 % der Kanzleien an, dass sie vertrauliche Daten, die intern versandt und weitergegeben werden, verfolgen und kontrollieren können, während 45 % angaben, dass sie dies tun können, wenn sie extern ausgetauscht werden. Beide Werte sind etwas besser als die Durchschnittswerte aller Befragten von 51 % bzw. 43 %.

Hinsichtlich der Prioritäten bei der Kommunikation sensibler Inhalte im Hinblick auf Datenschutz und Compliance war die Verhinderung des Abflusses vertraulichen geistigen Eigentums und von Geschäftsgeheimnissen für die Befragten aus dem Rechtsbereich bei weitem die höchste Priorität (75 % nannten dies als oberste oder zweithöchste Priorität). Dies war der höchste Wert aller Branchen und lag deutlich über dem Anteil der gesamten Kohorte (56 %). Die Vermeidung von Gesetzesverstößen und damit verbundenen Bußgeldern und Strafen sowie die Vermeidung von langwierigen und kostspieligen Rechtsstreitigkeiten hatten die zweithöchste Priorität (45 %).

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

Das Risikomanagement in Bezug auf externe Parteien ist eine wichtige Priorität für Anwaltskanzleien. 40% geben an, dass sie sensible Inhalte mit mehr als 2.500 externen Parteien austauschen (weniger als die globale Kohorte mit 44 %) und 60 % tun dies mit mehr als 1.000 externen Parteien (etwas weniger als der Durchschnitt aller Befragten von 66 %). Wenn es darum geht, sensible Inhalte zu verfolgen und zu kontrollieren, sobald sie eine Anwendung verlassen, ist der Rechtssektor einer der am weitesten entwickelten Sektoren: 60 % geben an, dass sie mehr als drei Viertel der sensiblen Inhalte verfolgen und kontrollieren können, sobald sie eine Anwendung verlassen.

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

75% der Anwaltskanzleien gaben an, dass die Messung und das Management der Compliance bei der Kommunikation sensibler Inhalte einiger bis erheblicher Verbesserungen bedarf. Dies ist weniger als die Gesamtzahl der Befragten (88%).

Die DSGVO und die neuen Datenschutzgesetze der US-Bundesstaaten wurden von 40 % der Befragten an erster oder zweiter Stelle genannt. HIPAA, SEC-Anforderungen und länderspezifische Datenschutzgesetze lagen mit 30 % gleichauf. Das Aufkommen unterschiedlicher Gesetze in den einzelnen US-Bundesstaaten macht es zunehmend schwieriger, Geschäfte zwischen verschiedenen Bundesstaaten zu tätigen, insbesondere aufgrund der Unterschiede zwischen diesen neuen Gesetzen. Da Anwaltskanzleien mit einem globalen Kundenstamm und Niederlassungen in der ganzen Welt zu tun haben, ist der hohe Prozentsatz der Befragten, die länderspezifische Datenschutzgesetze nannten, verständlich.

Bei der Prüfung und Auswahl von Sicherheitsvalidierungen oder -zertifizierungen nannten 55 % der befragten Kanzleien NIST 800-171 als erste oder zweite Priorität. Danach folgt IRAP mit 50 % als erste oder zweite Priorität. Da die meisten Anwaltskanzleien direkt mit Bundesbehörden zusammenarbeiten oder ihre Mandanten dies tun, ist dieses Ergebnis keine große Überraschung (in beiden Fällen liegen die Werte deutlich höher als in der gesamten globalen Kohorte).

Bewertung des Sicherheitsrisikos für sensible Inhalte

80 % der Anwaltskanzleien gaben an, dass die Messung und das Management von Sicherheitsrisiken im Zusammenhang mit der Kommunikation sensibler Inhalte erheblich oder in gewissem Maße verbesserungsbedürftig sind; 20 % gaben an, dass keine Verbesserungen erforderlich sind. Dieser Wert ist höher als in den meisten anderen Branchen. Wie die Daten über Datenschutzverletzungen zeigen, ist ein höheres Maß an Vertrauen jedoch nicht gleichbedeutend mit einem geringeren Risiko.

40 % der Anwaltskanzleien gaben an, dass ihre sensiblen Inhalte viermal oder öfter verletzt wurden (20 % gaben siebenmal oder öfter an). Diese Zahlen sind niedriger als in der branchenübergreifenden Kohorte, in der 32 % sieben oder mehr Datenschutzverstöße und 55 % vier oder mehr Datenschutzverstöße angaben. Darüber hinaus gaben 5 % der Befragten aus dem Rechtswesen an, dass sie sich nicht sicher seien, wie viele Datenschutzverletzungen in ihrem Unternehmen aufgetreten seien.

Erweiterte Sicherheitsfunktionen und -verfahren wie Verschlüsselung, Multi-Faktor-Authentifizierung und Governance Tracking und -Kontrolle werden nur bei einigen sensiblen Inhalten eingesetzt, die zu 50 % intern

und zu 45 % extern versendet werden. Dies ist zwar besser als in der Gesamtkohorte (39 % bzw. 38 %), aber es besteht noch erheblicher Verbesserungsbedarf.

Bewertung der Kosten für Sicherheit und Compliance

Hinsichtlich der Kosten für Rechtsstreitigkeiten gaben 45% der befragten Anwälte an, dass sie mehr als 3 Mio. USD pro Jahr ausgeben. Dies entspricht dem weltweiten Durchschnitt. 10% der Anwaltskanzleien gaben an, dass sie ihre jährlichen Kosten für Rechtsstreitigkeiten aufgrund von Datenschutzverletzungen nicht kennen.

Kenntnis und Kategorisierung der Datentypen

55 % der Kanzleien gaben an, mehr als drei Viertel der unstrukturierten Daten zu taggen und zu klassifizieren. Dies ist etwas weniger als die Gesamtzahl der Befragten, von denen 58% das Gleiche angaben. Auf die Frage, wie viele ihrer unstrukturierten Daten sie taggen oder klassifizieren müssen, gaben 60 % an, dass dies bei 40 % oder mehr der Fall sei, was erklären könnte, warum die Zahlen für die getaggten und klassifizierten Daten niedriger sind.

Robustes Management sensibler Inhalte ist im Rechtswesen 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 Rechtssektor. Die Befragten aus dem Rechtswesen nannten Finanzdokumente als ihr größtes Datenproblem (71 %), gefolgt von juristischer Korrespondenz (58 %). Dies ist eine kleine Überraschung, da man erwarten würde, dass die juristische Korrespondenz an erster Stelle steht. Beide Werte sind höher als in der Gesamtkohorte, in der Finanzdokumente in 55 % der Fälle und juristische Kommunikation in 44 % der Fälle genannt wurden.

Unternehmen der Rechtsbranche 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. 30 % der Befragten müssen mehr als 11 Protokolle abgleichen (allerdings weniger als der Durchschnitt von 48 % aller Befragten); 15 % der Befragten aus der Rechtsbranche wussten nicht, wie viele Protokolle sie abgleichen müssen. Dies führt zu einem enormen Stau bei der Berichterstellung. 45 % der Befragten verbringen 2.000 Stunden oder mehr pro Jahr damit, während 75 % mehr als 1.500 Stunden damit verbringen.

Lesen Sie den vollständigen Bericht