Kiteworks

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

HIGHLIGHTS

Verwendete Kommunikations-Tools	**17 %**	7+
	16 %	6
	20 %	5
	24 %	4
	11 %	3
	7 %	2
	1 %	1
Austausch sensibler Inhalte mit externen Parteien	**14 %**	über 5.000
	24 %	2.500 bis 4.999
	31 %	1.000 bis 2.499
	11 %	500 bis 999
	19 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	**74 %**	Geistiges Eigentum
	58 %	Patienteninformationen
	37 %	Persönliche Daten
	37 %	Finanzunterlagen
	35 %	CUI und FCI
	21 %	GenKI LLMs
	21 %	Juristischer Schriftwechsel
	16 %	M&A
Größter Fokus auf Datenschutz und Compliance (Top 2)	**46 %**	DSGVO
	41 %	HIPAA
	37 %	Datenschutzgesetze der U.S.-Staaten
	26 %	Länderspezifische Datenschutzgesetze
	24 %	SEC-Anforderungen
	17 %	CMMC
	9 %	PCI DSS
Wichtigste Sicherheits-validierungen (Top 2)	**49 %**	ISO 27001, 27017, 27018
	39 %	IRAP (Australien)
	36 %	NIST 800-171/CMMC 2.0
	33 %	SOC 2 Type II
	27 %	FedRAMP Moderate
	16 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	**13 %**	10+
	14 %	7 bis 9
	14 %	4 bis 6
	36 %	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 Gesundheitswesens. Dieser Kurzbericht konzentriert sich auf die wichtigsten Ergebnisse für das Gesundheitswesen 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

53 % der Unternehmen des Gesundheitswesens nutzen fünf oder mehr Kommunikationstools, um sensible Inhalte zu versenden und auszutauschen, was dem Durchschnitt der gesamten Kohorte entspricht. In Bezug auf die Nachverfolgung und Kontrolle sensibler Inhalte gaben 53 % der Unternehmen des Gesundheitswesens an, dass sie sensible Inhalte nachverfolgen und kontrollieren können, die intern versendet und ausgetauscht werden, während 44 % angaben, dass sie sensible Inhalte nachverfolgen und kontrollieren können, die extern ausgetauscht werden. Beide Werte liegen leicht über dem Durchschnitt aller Befragten von 51 % bzw. 43 %.

Wenn es um die Kommunikation sensibler Inhalte, den Datenschutz und die Einhaltung gesetzlicher Vorschriften geht, haben für die Unternehmen des Gesundheitswesens die Verhinderung des Abflusses vertraulicher Daten und Betriebsgeheimnisse sowie die Vermeidung von Verstößen gegen gesetzliche Vorschriften (Bußgelder und Strafen) oberste Priorität - 61 % bzw. 56 %. Diese Werte liegen deutlich über dem Durchschnitt aller Befragten - 56 % bzw. 48 %. Die verstärkte Durchsetzung von Datenschutzbestimmungen wie HIPAA dürfte der Grund für diese höhere Priorität im Gesundheitswesen sein. Wie in den meisten anderen Branchensegmenten gaben die Befragten im Gesundheitswesen am seltensten an, negative Auswirkungen auf die Marke vermeiden zu wollen (19 %).

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

Das Management der mit externen Parteien verbundenen Risiken ist eine große Herausforderung für Unternehmen im Gesundheitswesen. 38 % der Befragten gaben an, dass sie sensible Inhalte mit mehr als 2.500 externen Parteien austauschen (unter dem weltweiten Durchschnitt von 44 %). Erstaunliche 69 % haben mehr als 1.000 externe Parteien in ihrer Lieferkette für Inhalte (mehr als der branchenübergreifende Durchschnitt von 66 %). Wenn es darum geht, sensible Inhalte zu verfolgen und zu kontrollieren, sobald sie eine Anwendung verlassen, ist das Gesundheitswesen einer der ausgereiftesten Sektoren: 74 % geben an, dass sie mehr als drei Viertel der sensiblen Inhalte verfolgen und kontrollieren können, sobald sie eine Anwendung verlassen (knapp hinter 79 % der Hersteller).

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

90 % der Unternehmen des Gesundheitswesens gaben an, dass die Messung und das Management der Compliance bei der Kommunikation sensibler Inhalte einiger bis erheblicher Verbesserungen bedarf. Dies ist etwas mehr als die Gesamtzahl der Befragten (88 %).

Die Unternehmen des Gesundheitswesens nannten die DSGVO als wichtigste Vorschrift vor anderen Datenschutz- und Compliance-Vorgaben (46 % an erster oder zweiter Stelle). Die am zweithäufigsten genannte Vorschrift war HIPAA (41 %). Dieser Doppelsieg macht Sinn, wenn man bedenkt, wie genau die Behörden vertrauliche Patienteninformationen unter die Lupe nehmen.

Bei der Prüfung und Auswahl von Sicherheitsvalidierungen oder -zertifizierungen lagen die Unternehmen des Gesundheitswesens relativ dicht beieinander, wobei ISO 27001, 27017 und 27018 in 49 % der Fälle als erste oder zweite Validierung oder Zertifizierung genannt wurden. Die am zweithäufigsten genannte Sicherheitsvalidierung lag mit 39 % (IRAP) 10 Prozentpunkte dahinter. Diese Werte entsprechen denen der gesamten Kohorte, in der ISO 27001, 27017 und 27018 von 53 % und IRAP von 33 % genannt wurden.

Bewertung des Sicherheitsrisikos für sensible Inhalte

91 % der Unternehmen im Gesundheitswesen geben 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 im weltweiten branchenübergreifenden Durchschnitt).

41 % der Unternehmen im Gesundheitswesen gaben an, dass ihre sensiblen Inhalte vier oder mehr Mal angegriffen wurden (27 % gaben an, sieben oder mehr Mal angegriffen worden zu sein). Dies ist weniger als in der branchenübergreifenden Kohorte, in der 32 % sieben oder mehr Datenschutzverletzungen angaben und 55 % vier oder mehr. Darüber hinaus gab fast jeder zehnte Befragte (9 %) im Gesundheitswesen an, nicht sicher zu sein, wie viele Datenpannen in seinem Unternehmen aufgetreten sind.

Fortgeschrittene Sicherheitsfunktionen und -verfahren wie Verschlüsselung, Multi-Faktor-Authentifizierung und Governance-Tracking und -Kontrolle werden von den Unternehmen im Gesundheitswesen nur in 44 % der Fälle für einige sensible Inhalte eingesetzt (einige Prozentpunkte weniger als die 41 % aller Befragten - 39 % gaben an, einige davon zu verwenden, und 2 % gaben an, keine davon zu verwenden).

Bewertung der Kosten für Sicherheit und Compliance

Hinsichtlich der Kosten für Rechtsstreitigkeiten gaben 38 % der Befragten aus dem Gesundheitswesen an, dass sie mehr als 3 Mio. USD pro Jahr ausgeben. Dies liegt unter dem weltweiten Durchschnitt, wo 45 % der Befragten angaben, dass ihre Prozesskosten über 3 Mio. USD liegen. Eine große Anzahl (13 %) der Befragten aus dem Gesundheitswesen gab an, nicht zu wissen, wie viel ihr Unternehmen jährlich für Rechtsstreitigkeiten ausgibt, was über dem Wert von 9 % in der gesamten Kohorte liegt.

Kenntnis und Kategorisierung der Datentypen

65 % der Unternehmen im Gesundheitswesen gaben an, dass sie mehr als drei Viertel ihrer unstrukturierten Daten taggen und klassifizieren, was deutlich besser ist als bei der Gesamtzahl der Befragten, von denen 58 % dies angaben. Diese höhere Kennzeichnungs- und Klassifizierungsrate könnte das Ergebnis einer größeren Sensibilität für sensible Daten im Gesundheitswesen sein. Ironischerweise gaben nur 26 % der Befragten aus dem Gesundheitswesen an, dass 80 % oder mehr der unstrukturierten Daten gekennzeichnet und klassifiziert werden müssen (oder 54 %, die angaben, dass 60 % oder mehr gekennzeichnet und klassifiziert werden müssen).

Robustes Management sensibler Inhalte ist im Gesundheitswesen unerlässlich

Der “2024 Sensitive Content Communications Report” von Kiteworks unterstreicht die dringende Notwendigkeit eines robusten Risiko- und Compliance-Managements für die Kommunikation sensibler Inhalte in Unternehmen des Gesundheitswesens. Überraschenderweise wurde geistiges Eigentum - im Gegensatz zu geschützten Patienteninformationen (58 %) - von den Befragten als die Datenkategorie mit dem größten Risiko (74 %) genannt.

Unternehmen des Gesundheitswesens verbringen viel Zeit mit der Verwaltung der Protokolle, die von den zahlreichen Kommunikationstools erzeugt werden, die sie für den Austausch und die Übermittlung sensibler Inhalte verwenden. 58 % der Befragten müssen mehr als 11 Protokolle abgleichen (gegenüber einem Durchschnitt von 48 % aller Befragten), und 6 % der Befragten wissen nicht einmal, wie viele Protokolle sie abgleichen müssen. Dies führt zu einem enormen Berichtsstau. 11 % verbringen 2.500 Stunden oder mehr pro Jahr damit und weitere 19 % mehr als 2.000 Stunden. 64 % verbringen mehr als 1.500 Stunden pro Jahr damit.

Lesen Sie den vollständigen Bericht

Copyright © 2024 Kiteworks. Kiteworks hat es sich zur Aufgabe gemacht, Unternehmen in die Lage zu versetzen, die Risiken beim Senden, Teilen, Empfangen und Speichern sensibler Inhalte effektiv zu managen. Die Kiteworks-Plattform stellt Kunden ein Private Content Network zur Verfügung, das Content Governance, Compliance und Schutz bietet. Die Plattform vereinheitlicht, verfolgt, kontrolliert und schützt sensible Inhalte, die innerhalb des Unternehmens und über die Unternehmensgrenzen hinaus ausgetauscht werden. Dadurch wird das Risikomanagement erheblich verbessert und die Einhaltung gesetzlicher Vorgaben für die gesamte Kommunikation mit sensiblen Inhalten sichergestellt.