Kiteworks

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

HIGHLIGHTS

Verwendete Kommunikations-Tools	**5 %**	7+
	7 %	6
	37 %	5
	21 %	4
	12 %	3
	9 %	2
	5 %	1
Austausch sensibler Inhalte mit externen Parteien	**7 %**	über 5.000
	40 %	2.500 bis 4.999
	19 %	1.000 bis 2.499
	16 %	500 bis 999
	19 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	**58 %**	Persönliche Daten
	50 %	Geistiges Eigentum
	46 %	Finanzunterlagen
	42 %	Juristischer Schriftwechsel
	35 %	GenKI LLMs
	23 %	Patienteninformationen
	23 %	CUI und FCI
	23 %	M&A
Größter Fokus auf Datenschutz und Compliance (Top 2)	**49 %**	CMMC
	44 %	Datenschutzgesetze der U.S.-Staaten
	37 %	HIPAA
	35 %	SEC-Anforderungen
	23 %	DSGVO
	12 %	Länderspezifische Datenschutzgesetze
	0 %	PCI DSS
Wichtigste Sicherheits-validierungen (Top 2)	**36 %**	NIST 800-171/CMMC 2.0
	60 %	ISO 27001, 27017, 27018
	33 %	FedRAMP Moderate
	19 %	SOC 2 Type II
	16 %	IRAP (Australien)
	7 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	**5 %**	10+
	51 %	7 bis 9
	14 %	4 bis 6
	14 %	2 bis 3
	2 %	1
	14 %	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 Hochschulwesens. Dieser Kurzbericht konzentriert sich auf die wichtigsten Ergebnisse für den Hochschulbereich 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

Fast die Hälfte (49 %) der Hochschulen verwendet fünf oder mehr Kommunikationstools, um sensible Inhalte zu versenden und auszutauschen. Dies ist etwas weniger als der Durchschnitt der gesamten Kohorte (53 %). In Bezug auf die Nachverfolgung und Kontrolle sensibler Inhalte gaben nur 19 % der befragten Hochschulen an, dass sie in der Lage sind, sensible Daten nachzuverfolgen und zu kontrollieren, die intern versendet und ausgetauscht werden; ein noch geringerer Anteil der befragten Hochschulen gab an, dass sie in der Lage sind, sensible Daten nachzuverfolgen und zu kontrollieren, die extern ausgetauscht werden (14%). Dies ist deutlich schlechter als die Durchschnittswerte für die gesamte Kohorte - 51 % für den internen Datenaustausch und 43 % für den externen Datenaustausch.

Das Hochschulwesen ist in Bezug auf den Umgang mit sensiblen Daten weitaus anfälliger als andere Sektoren. Abgesehen von personenbezogenen Daten und Patienteninformationen, die an sich schon ein Risiko darstellen, werden im Hochschulbereich auch hochvertrauliche Daten wie nationales geistiges Eigentum und Staatsgeheimnisse, einschließlich Forschungsdaten für das US-Verteidigungsministerium, übermittelt und weitergegeben. Aufgrund der schlechten Governance des Sektors sind die Risiken greifbar.

Wenn es um den Schutz der Kommunikation sensibler Inhalte und die Einhaltung von Vorschriften geht, wird die Vermeidung langwieriger und kostspieliger Rechtsstreitigkeiten von 63 %

der Befragten als erste oder zweite Priorität genannt. An zweiter Stelle folgt die Verhinderung der Offenlegung von vertraulichem geistigem Eigentum und Geschäftsgeheimnissen (56 %). Diese beiden Top-Prioritäten spiegeln die Zunahme von Datenschutzbestimmungen und deren Durchsetzung sowie die Notwendigkeit des Schutzes vertraulicher Daten, einschließlich der zwischen Hochschuleinrichtungen ausgetauschten Daten, wider.

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

Der Umgang mit Risiken, die von externen Parteien ausgehen, stellt eine große Lücke im Hochschulbereich dar. 47 % der Befragten gaben an, dass sie sensible Inhalte mit mehr als 2.500 externen Parteien austauschen (etwas mehr als die globale Kohorte mit 44 %) und 66 % tun dies mit mehr als 1.000 externen Parteien (was dem Durchschnitt aller Befragten von 66 % entspricht). Wenn es darum geht, sensible Inhalte zu verfolgen und zu kontrollieren, sobald sie eine Anwendung verlassen, ist der Hochschulsektor einer der etwas fortgeschritteneren Sektoren: 31 % gaben 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

84 % der befragten Hochschulen gaben an, dass die Messung und das Management der Compliance bei der Kommunikation sensibler Inhalte einiger bis erheblicher Verbesserungen bedarf. Dies ist etwas weniger als die Gesamtzahl der Befragten (88 %).

Das Engagement vieler Hochschulen in Angelegenheiten der Verteidigungsindustrie (DIB) zeigte sich bei der Frage, welcher Compliance-Standard für sie am wichtigsten sei. Die Befragten aus dem Hochschulbereich nannten CMMC 2.0 als ihre erste oder zweite Priorität (49 %). An zweiter Stelle standen die Datenschutzgesetze der US-Bundesstaaten (44 %), was auf die Notwendigkeit des Schutzes personenbezogener Daten hinweist.

Von den verschiedenen Sicherheitsstandards und -validierungen wurde NIST 800-171 von den Befragten aus dem Hochschulbereich am häufigsten gewählt (63 %), was wahrscheinlich auf den Umfang des Datenaustauschs mit der Bundesregierung zurückzuführen ist. Dicht gefolgt von ISO 27001, 27017 und 27018 (60 %).

Bewertung des Sicherheitsrisikos für sensible Inhalte

86 % der befragten Hochschulen gaben an, dass die Messung und das Management von Sicherheitsrisiken im Zusammenhang mit der Kommunikation sensibler Inhalte erheblich oder in gewissem Maße verbesserungsbedürftig sind; weitere 2 % gaben an, dass sie derzeit keine Maßnahmen ergriffen haben. Beide Werte liegen weitgehend innerhalb der Fehlermarge für die gesamte Kohorte.

56 % der Befragten aus dem Hochschulbereich gaben an, dass ihre sensiblen Inhalte sieben oder mehr Mal verletzt wurden. Dies ist insofern besorgniserregend, als die Zahl der Verstöße deutlich höher ist als in der Gesamtkohorte (32 % gaben an, sieben oder mehr Verstöße erlebt zu haben). Dies ist eine gravierende Lücke, die geschlossen werden muss. Das Hochschulwesen steht zweifellos im Fadenkreuz böswilliger Angreifer. Die DBIR-Studie von Verizon ergab, dass das Hochschulwesen häufiger als die meisten anderen Sektoren ins Visier genommen wurde und mehr Sicherheitsverletzungen zu verzeichnen hatte als jeder andere Sektor.[1]

Die Befragten aus dem Hochschulsektor gaben an, dass sie in höherem Maße als andere Sektoren fortschrittliche Sicherheitsfunktionen und -verfahren wie Verschlüsselung, Multi-Faktor-Authentifizierung und Nachverfolgung und Kontrolle der Übertragung sensibler Inhalte einsetzen (65 % aller Befragten). Dies ist mehr als in der gesamten Kohorte (59 %).

Bewertung der Kosten für Sicherheit und Compliance

Alle Datenschutzverletzungen im Hochschulbereich führen zu einem erhöhten Prozessrisiko. Fast die Hälfte der Befragten gab an, jährlich mehr als 5 Mio. USD für Rechtsstreitigkeiten auszugeben. Dies ist der höchste Wert aller Branchen und zeigt, dass die Hochschulen sowohl die Sicherheit als auch das Management der Kommunikation sensibler Inhalte verdoppeln oder verdreifachen müssen. Die Tatsache, dass 19 % der befragten Hochschulen angaben, die Kosten von Rechtsstreitigkeiten aufgrund von Datenschutzverletzungen nicht zu kennen, verschärft das Risiko.

Kenntnis und Kategorisierung der Datentypen

Viele Befragte aus dem Hochschulbereich gaben an, dass sie mehr als 50 % ihrer unstrukturierten Daten taggen und klassifizieren (79 %). Im Vergleich zu vielen anderen Wirtschaftszweigen sind die Hochschulen nicht der Ansicht, dass unstrukturierte Daten in großem Umfang gekennzeichnet und klassifiziert werden müssen (nur 14 % gaben an, dass mehr als 60 % gekennzeichnet und klassifiziert werden müssen).

Robustes Management sensibler Inhalte ist im Hochschulwesen 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 Bereich des Hochschulwesens. Überraschenderweise wurde geistiges Eigentum - im Gegensatz zu geschützten Patienteninformationen (58 %) - von den Befragten als die Datenkategorie mit dem größten Risiko (74 %) genannt.

Der Schutz personenbezogener Daten von Studierenden, Dozenten und Mitarbeitern ist zweifellos ein wichtiger Teil der Aufgaben von Hochschuleinrichtungen. Daher überrascht es nicht, dass die Befragten aus dem Hochschulbereich personenbezogene Daten häufiger als andere Datenarten nannten (58 % nannten sie an erster oder zweiter Stelle). Gleichzeitig ist der Schutz sensibler Daten im Zusammenhang mit geistigem Eigentum und Geschäftsgeheimnissen sogar noch wichtiger. 50 % der Befragten aus dem Hochschulbereich nannten diese Art von Daten als das höchste oder zweithöchste Risiko.

Hochschuleinrichtungen 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. 58 % der Befragten müssen mehr als 11 Protokolle abgleichen (10 Prozentpunkte mehr als der Durchschnitt aller Befragten). 9 % der Befragten aus dem Hochschulwesen wussten nicht, wie viele Protokolle sie abgleichen müssen. Im Vergleich zu anderen Branchen verbringen die Hochschulen mehr Zeit mit dem Abgleich von Protokollen zur Erstellung von Compliance-Berichten - 49 % wenden 2.000 Stunden pro Jahr für diese Berichte auf.

[1] “2024 Data Breach Investigations Report”, Verizon, Mai 2024.

Lesen Sie den vollständigen Bericht