Kiteworks

2024 Analyse für die Kommunikation sensibler Inhalte in der öffentlichen Verwaltung: Sicherheit und Compliance

HIGHLIGHTS

Verwendete Kommunikations-tools	**28 %**	7+
	3 %	6
	28 %	5
	7 %	4
	24 %	3
	10 %	2
	0 %	1
Austausch sensibler Inhalte mit externen Parteien	**28 %**	über 5.000
	10 %	2.500 bis 4.999
	24 %	1.000 bis 2.499
	7 %	500 bis 999
	31 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	**61 %**	Juristischer Schriftwechsel
	50 %	Geistiges Eigentum
	44 %	GenKI LLMs
	33 %	Persönliche Daten
	33 %	Patienteninformationen
	33 %	Finanzunterlagen
	28 %	M&A
	17 %	CUI und FCI
Größter Fokus auf Datenschutz und Compliance (Top 2)	**55 %**	Länderspezifische Datenschutzgesetze
	45 %	DSGVO
	28 %	Datenschutzgesetze der U.S.-Staaten
	24 %	SEC-Anforderungen
	21 %	CMMC
	14 %	HIPAA
	14 %	PCI DSS
Wichtigste Sicherheits-validierungen (Top 2)	**48 %**	ISO 27001, 27017, 27018
	45 %	NIST 800-171/CMMC 2.0
	34 %	FedRAMP Moderate
	31 %	SOC 2 Type II
	24 %	IRAP (Australien)
	17 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	**17 %**	10+
	10 %	7 bis 9
	17 %	4 bis 6
	34 %	2 bis 3
	17 %	1
	3 %	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 staatlichen Behörden. Dieser Bericht konzentriert sich auf die wichtigsten Ergebnisse für die öffentliche Verwaltung 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

59 % der staatlichen Behörden nutzen fünf oder mehr Kommunikationstools für den Versand und Austausch sensibler Inhalte, das ist mehr als der Durchschnitt der gesamten Kohorte (53 %). Hinsichtlich der Nachverfolgung und Kontrolle sensibler Inhalte gaben 59 % der befragten Behörden an, dass sie sensible Daten, die intern versandt und ausgetauscht werden, nachverfolgen und kontrollieren können; der gleiche Prozentsatz gab an, dass sie dies auch beim externen Austausch können. Beide Werte liegen leicht über dem Durchschnitt aller Befragten von 51 % bzw. 43 %. Dies könnte auf die unterschiedlichen Sicherheitskontrollen und -standards auf staatlicher Ebene zurückzuführen sein.

In Bezug auf den Datenschutz bei der Kommunikation sensibler Inhalte und die Einhaltung gesetzlicher Vorschriften war die Verhinderung des Abflusses vertraulicher Daten und Geschäftsgeheimnisse für die Befragten aus Bundesbehörden mit Abstand die höchste Priorität (69 % nannten dies entweder als höchste oder als zweithöchste Priorität). Abgesehen von den Unternehmen im Rechtswesen war dies die höchste Antwortrate für diese Priorität. Der Prozentsatz liegt deutlich über dem der Gesamtkohorte (56%). Die zweithäufigste Priorität war die Vermeidung von Gesetzesverstößen und den damit verbundenen Bußgeldern und Strafen sowie die

Schadensbegrenzung - wahrscheinlich im Zusammenhang mit den verschiedenen Standards, die staatliche Behörden nun einhalten müssen (z. B. CMMC 2.0, Executive Order 14028, etc.).

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

Das Management von Risiken im Zusammenhang mit externen Parteien ist eine wichtige Priorität für staatliche Behörden. 38 % der Befragten gaben 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 die öffentliche Verwaltung eine der am weitesten entwickelten Branchen. 62 % der Befragten gaben an, dass sie mehr als drei Viertel der sensiblen Inhalte nachverfolgen und kontrollieren können, wenn sie eine Anwendung verlassen.

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

86 % der Befragten aus Regierungsstellen gaben an, dass die Messung und das Management der Einhaltung der Vorschriften für die Kommunikation sensibler Inhalte einiger bis erheblicher Verbesserungen bedarf. Dies ist etwas weniger als die 88 % aller Befragten.

Der öffentliche Sektor ist im Allgemeinen sehr auf den Datenschutz der einzelnen Bürger und Einwohner bedacht. In unserer Umfrage wurden die länderspezifischen Datenschutzgesetze von den Befragten aus Behörden in 55 % der Fälle an erster oder zweiter Stelle genannt - deutlich mehr als im Durchschnitt aller Befragten (21 %). Die DSGVO lag mit 45 % an zweiter Stelle.

Bei der Prüfung und Auswahl von Sicherheitsvalidierungen oder -zertifizierungen nannten die Befragten aus Behörden ISO 27001, 27017 und 27018 als höchste Priorität (48 %), gefolgt von NIST 800-171/CMMC 2.0 (45 %). Staatliche Sicherheitsstandards gelten nicht nur für den privaten, sondern auch für den öffentlichen Sektor, so dass ein weiterer Anstieg dieser Zahlen zu erwarten ist.

Bewertung des Sicherheitsrisikos für sensible Inhalte

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

44 % der Befragten aus dem Bereich der öffentlichen Verwaltung gaben an, dass ihre sensiblen Inhalte viermal oder öfter kompromittiert wurden (27 % sagten, siebenmal oder öfter). Dies sind weniger als in der branchenübergreifenden Kohorte, in der 32 % sieben oder mehr Datenschutzverletzungen zugaben und 55 % sagten, sie hätten vier oder mehr gehabt. Möglicherweise deutet dies darauf hin, dass Behörden ein besseres Risikomanagement betreiben als ihre Kollegen in der Privatwirtschaft. Staatliche Behörden stehen zweifellos im Fadenkreuz böswilliger Akteure, so dass dies eine potenziell gute Nachricht sein könnte (ein Datenpunkt, den Sie bei der Umfrage im nächsten Jahr im Auge behalten sollten).

Erweiterte Sicherheitsfunktionen und -verfahren wie Verschlüsselung, Multi-Faktor-Authentifizierung und Governance-Tracking und -Kontrolle werden von Behörden nur in etwas mehr als der Hälfte der Fälle (52 %) für einige sensible Inhalte eingesetzt. Das ist messbar besser als in der globalen Kohorte mit 41 % - 39 % gaben an, dies für einige zu nutzen, und 2 % gaben an, dies nicht zu tun. Dies zeigt erneut, dass der öffentliche Sektor im Vergleich zu allen Befragten ein höheres Sicherheitsniveau aufweist.

Bewertung der Kosten für Sicherheit und Compliance

Die Kosten für Rechtsstreitigkeiten im Zusammenhang mit Datenschutzverletzungen werden häufig mit dem privaten Sektor in Verbindung gebracht, sind jedoch auch für den öffentlichen Sektor relevant. 35 % der befragten Behörden gaben an, dass sie jährlich mehr als 3 Mio. USD für Rechtsstreitigkeiten im Zusammenhang mit Datenschutzverletzungen ausgeben. Hinsichtlich der Kosten für Rechtsstreitigkeiten gaben 45 % der befragten Behörden an, dass sie jährlich mehr als 3 Mio. USD ausgeben. 7 % der befragten Behörden gaben an, dass sie ihre jährlichen Kosten für Rechtsstreitigkeiten aufgrund von Datenschutzverletzungen nicht kennen.

Kenntnis und Kategorisierung der Datentypen

45 % der befragten Behörden gaben an, mehr als drei Viertel der unstrukturierten Daten zu kennzeichnen und zu klassifizieren. Dies ist etwas weniger als die Gesamtzahl der Befragten, von denen 48 % dies angaben. Bei der Frage, wie viele ihrer unstrukturierten Daten mit Tags versehen oder klassifiziert werden müssen, zeigt sich eine Diskrepanz: 41 % gaben an, dass 80 % oder mehr ihrer unstrukturierten Daten gekennzeichnet oder klassifiziert werden müssen.

Robustes Management sensibler Inhalte ist in der öffentlichen Verwaltung unerlässlich

Der “2024 Sensitive Content Communications Report” von Kiteworks unterstreicht die Notwendigkeit eines robusten Risiko- und Compliance-Managements für die Kommunikation sensibler Inhalte im Bereich der öffentlichen Verwaltung. Die Befragten nannten die juristische Kommunikation als ihr größtes Datenproblem (61 %). An zweiter Stelle folgt das geistige Eigentum (50 %). Angesichts der anhaltenden Welle von Angriffen auf vertrauliche Daten durch Schurkenstaaten macht diese Antwort Sinn. Diese Prioritäten auf nationaler Ebene stehen im Gegensatz zu den Antworten der Gesamtkohorte, wo Finanzdokumente in 55 % der Fälle und juristischer Schriftwechsel in 44 % der Fälle genannt wurden.

Die Behörden 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. 48 % der Befragten müssen mehr als 11 Protokolle abgleichen (dies entspricht dem Durchschnitt aller Befragten). 10 % der Befragten der staatlichen Stellen wussten nicht, wie viele Protokolle abgeglichen werden müssen. Daraus ergibt sich ein enormer Protokollstau in den öffentlichen Verwaltungen, wenn auch in geringerem Umfang als in der Privatwirtschaft: 21 % verbringen 2.000 Stunden oder mehr pro Jahr damit, während 56 % mehr als 1.500 Stunden aufwenden.

Lesen Sie den vollständigen Bericht