Kiteworks

2024 Analyse für die Kommunikation sensibler Inhalte im Bereich Sicherheit und Verteidigung: Sicherheit und Compliance

HIGHLIGHTS

Verwendete Kommunikations-tools	**16 %**	7+
	27 %	6
	14 %	5
	15 %	4
	20 %	3
	6 %	2
	1 %	1
	1 %	weiß nicht
Austausch sensibler Inhalte mit externen Parteien	**7 %**	über 5.000
	26 %	2.500 bis 4.999
	39 %	1.000 bis 2.499
	18 %	500 bis 999
	10 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	**53 %**	Finanzunterlagen
	50 %	GenKI LLMs
	50 %	Geistiges Eigentum
	41 %	Juristischer Schriftwechsel
	36 %	Persönliche Daten
	34 %	Patienteninformationen
	26 %	CUI und FCI
	12 %	M&A
Größter Fokus auf Datenschutz und Compliance (Top 2)	**41 %**	HIPAA
	38 %	Datenschutzgesetze der U.S.-Staaten
	38 %	CMMC
	32 %	DSGVO
	28 %	SEC-Anforderungen
	18 %	PCI DSS
	6 %	Länderspezifische Datenschutzgesetze
Wichtigste Sicherheits-validierungen (Top 2)	**50 %**	ISO 27001, 27017, 27018
	44 %	NIST 800-171/CMMC 2.0
	38 %	FedRAMP Moderate
	35 %	IRAP (Australien)
	22 %	SOC 2 Type II
	11 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	**3 %**	10+
	39 %	7 bis 9
	26 %	4 bis 6
	20 %	2 bis 3
	7 %	1
	5 %	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 Sicherheits- und Verteidigungssektors. Dieser Kurzbericht konzentriert sich auf die wichtigsten Ergebnisse im Bereich Sicherheit und Verteidigung 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

57 % der Unternehmen im Bereich Sicherheit und Verteidigung nutzen fünf oder mehr Kommunikationstools, um sensible Inhalte zu versenden und auszutauschen, etwas weniger als die 53 % der Befragten weltweit. In Bezug auf die Nachverfolgung und Kontrolle sensibler Inhalte gaben 41 % der Unternehmen im Bereich Sicherheit und Verteidigung an, dass sie in der Lage sind, intern versandte und ausgetauschte sensible Daten nachzuverfolgen und zu kontrollieren, während nur 39 % angaben, dass sie in der Lage sind, extern ausgetauschte sensible Daten nachzuverfolgen und zu kontrollieren. Dies ist messbar schlechter als in der globalen branchenübergreifenden Kohorte, die 51 % bzw. 43 % angab (und ein Grund zur Sorge für die Behörden der Verteidigungsministerien).

In Bezug auf die Prioritäten bei der Kommunikation sensibler Inhalte, Datenschutz und Compliance haben für die Unternehmen des Sektors Sicherheit und Verteidigung die Vermeidung langwieriger/kostenintensiver Rechtsstreitigkeiten aufgrund von Datenschutzverletzungen (57 %) und die Verhinderung der Offenlegung vertraulichen geistigen Eigentums und von Geschäftsgeheimnissen (50 %) die höchste Priorität. Ersteres ist etwas höher als in der branchenübergreifenden Kohorte (51 %), während letzteres niedriger ist (im Vergleich zu 56 %).

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

Der Umgang mit Risiken, die von externen Parteien ausgehen, stellt für fast alle Unternehmen eine große Herausforderung dar. Im Vergleich zu anderen Branchen haben Sicherheits- und Verteidigungsunternehmen etwa genauso viele externe Parteien, mit denen sie sensible Daten austauschen (33 % tun dies mit mehr als 2.500). Wie die meisten anderen Branchensegmente haben sie Schwierigkeiten, sensible Daten zu verfolgen und zu kontrollieren, wenn sie eine Anwendung verlassen. Nur 10 % geben an, dass ihnen dies in 100 % der Fälle gelingt, während 37 % sagen, dass es ihnen in 50 % oder weniger der Fälle gelingt.

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

83 % der Unternehmen im Bereich Sicherheit und Verteidigung gaben an, dass erhebliche (22 %) oder einige (60 %) Verbesserungen bei der Einhaltung der Vorschriften für die Kommunikation sensibler Inhalte erforderlich seien. Dies ist etwas besser als in der branchenübergreifenden Gesamtgruppe, in der nur 11 % angaben, keinen Verbesserungsbedarf zu haben.

Überraschenderweise nannten Sicherheits- und Verteidigungsunternehmen HIPAA als das Datenschutzgesetz, das ihnen die größten Sorgen bereitet (41 %). Die Einhaltung der CMMC 2.0 stand mit 38 % an zweiter Stelle (zusammen mit den Datenschutzgesetzen der US-Bundesstaaten). Die Einhaltung länderspezifischer Datenschutzgesetze wurde am seltensten genannt (6 %). Angesichts der Tatsache, dass die vollständige Umsetzung der CMMC nicht mehr lange auf sich warten lässt, ist dieser Prozentsatz niedrig und möglicherweise besorgniserregend. Basierend auf den Daten aus anderen Studien sind die meisten Sicherheits- und Verteidigungsunternehmen nicht auf CMMC vorbereitet, daher ist die Tatsache, dass die Einhaltung von CMMC nicht häufiger genannt wurde, ein Warnsignal.

Wenn es um die Prüfung und Auswahl von Sicherheitsvalidierungen oder -zertifizierungen geht, nannten 50 % der Sicherheits- und Verteidigungsunternehmen ISO 27001, 27017 und 27018 als eine der beiden wichtigsten Normen. 44 % gaben an, dass NIST 800-171/CMMC ihr wichtigster Standard für die Sicherheitszertifizierung/-validierung ist. FedRAMP Moderate wurde an dritter Stelle genannt (38 %). Die NIS 2-Richtlinie wurde am seltensten genannt (11 %).

Bewertung des Sicherheitsrisikos für sensible Inhalte

Wie bei der Frage nach der Compliance gaben etwas mehr Sicherheits- und Verteidigungsunternehmen an, dass die Sicherheit ihrer Kommunikation mit sensiblen Inhalten erheblich oder etwas verbessert werden muss. Erweiterte Sicherheitsfunktionen und -verfahren wie Verschlüsselung, Multi-Faktor-Authentifizierung und Governance-Tracking und -Kontrolle für die interne Kommunikation von Inhalten werden nur von 55 % der Sicherheits- und Verteidigungsunternehmen eingesetzt (im Vergleich zu 59 % aller Befragten). Das Gleiche gilt für die externe Kommunikation von Inhalten; nur 51 % tun dies im Vergleich zu 59 % aller Befragten. Diese beiden Daten deuten auf ein Sicherheitsrisiko hin, das es zu beseitigen gilt.

Bewertung der Kosten für Sicherheit und Compliance

Angesichts der Tatsache, dass Cyberkriminelle und Schurkenstaaten Sicherheits- und Verteidigungsunternehmen ins Visier nehmen, weil diese sensible und geheime Inhalte versenden und weitergeben, ist die Zahl der gemeldeten Datenschutzverletzungen im vergangenen Jahr besorgniserregend: 42 % der Befragten gaben an, sieben oder mehr Datenschutzverletzungen erlebt zu haben (im Vergleich zu 32 % aller Befragten).

Im Hinblick auf die Kosten von Rechtsstreitigkeiten ergab die Umfrage, dass die Unternehmen im Bereich Sicherheit und Verteidigung einem hohen Risiko ausgesetzt sind. Mehr als die Hälfte (53 %) gab an, dass die

jährlichen Kosten für Rechtsstreitigkeiten aufgrund von Datenschutzverletzungen 3 Mio. USD oder mehr betragen (im Vergleich zu 45 % aller Befragten).

Kenntnis und Kategorisierung der Datentypen

Nahezu die Hälfte (48 %) der Unternehmen im Bereich Sicherheit und Verteidigung gaben an, mehr als drei Viertel ihrer unstrukturierten Daten zu kennzeichnen und zu klassifizieren, weitere 28 % gaben an, mehr als die Hälfte zu kennzeichnen und zu klassifizieren. Diese Prozentsätze entsprechen in etwa den globalen Zahlen, bei denen 48 % angaben, drei Viertel oder mehr ihrer unstrukturierten Daten zu kennzeichnen und zu klassifizieren.

Aber nicht alle unstrukturierten Daten müssen klassifiziert werden, so zumindest die Meinung der Befragten. 27 % der Befragten aus dem Bereich Sicherheit und Verteidigung gaben an, dass 60 % oder mehr der unstrukturierten Daten klassifiziert werden müssen. Weitere 47 % der Sicherheits- und Verteidigungsunternehmen sind der Meinung, dass nur 40 % bis 60 % gekennzeichnet und klassifiziert werden müssen.

Robustes Management sensibler Inhalte ist im Bereich Sicherheit und Verteidigung 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 Sicherheit und Verteidung. Finanzdokumente wurden als der Datentyp mit dem höchsten Risiko genannt (53 %), gefolgt von generativen KI-LLMs und geistigem Eigentum (beide 50 %). Bei GenKI-LLMs hatte der Bereich Sicherheit und Verteidigung zusammen mit dem Energie- und Versorgungssektor den höchsten Anteil.

Unternehmen im Bereich Sicherheit und Verteidigung verbringen viel Zeit mit der Verwaltung der Protokolle, die von den zahlreichen Kommunikationstools erzeugt werden, die sie für den Austausch und den Versand sensibler Inhalte verwenden. Fast drei von zehn Unternehmen geben an, dass sie 2.000 Stunden oder mehr für diese Aufgabe aufwenden. Weitere 38 % verbringen zwischen 1.500 und 1.999 Stunden damit.

Lesen Sie den vollständigen Bericht