Kiteworks

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

HIGHLIGHTS

Verwendete Kommunikations-Tools	**8 %**	7+
	14 %	6
	25 %	5
	22 %	4
	17 %	3
	6 %	2
	2 %	1
Austausch sensibler Inhalte mit externen Parteien	**7 %**	über 5.000
	31 %	2.500 bis 4.999
	39 %	1.000 bis 2.499
	14 %	500 bis 999
	10 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	**61 %**	Juristischer Schriftwechsel
	48 %	Finanzunterlagen
	39 %	Persönliche Daten
	37 %	CUI und FCI
	36 %	Geistiges Eigentum
	34 %	Patienteninformationen
	31 %	GenKI LLMs
	15 %	M&A
Größter Fokus auf Datenschutz und Compliance (Top 2)	**43 %**	HIPAA
	42 %	SEC-Anforderungen
	32 %	CMMC
	31 %	Datenschutzgesetze der U.S.-Staaten
	25 %	DSGVO
	18 %	Länderspezifische Datenschutzgesetze
	11 %	PCI DSS
Wichtigste Sicherheits-validierungen (Top 2)	**48 %**	ISO 27001, 27017, 27018
	47 %	NIST 800-171/CMMC 2.0
	45 %	IRAP (Australien)
	38 %	FedRAMP Moderate
	20 %	SOC 2 Type II
	4 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	**3 %**	10+
	40 %	7 bis 9
	29 %	4 bis 6
	17 %	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 bei der Verwaltung sensibler Inhalte in verschiedenen Regionen, einschließlich APAC (Asien-Pazifik). Der Bericht präsentiert die wichtigsten Ergebnisse in Bezug auf die APAC-Region 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

52 % der Unternehmen in der APAC-Region nutzen fünf oder mehr Kommunikations-Tools, um sensible Inhalte zu versenden und auszutauschen, was nur geringfügig unter dem weltweiten Durchschnitt von 53 % liegt. Bei der Nachverfolgung und Kontrolle sensibler Inhalte liegen die Unternehmen in der APAC-Region gleichauf mit dem weltweiten Durchschnitt: 61 % gaben an, dass sie mehr als drei Viertel der Inhalte nachverfolgen und kontrollieren. Die APAC-Region liegt genau im weltweiten Durchschnitt, aber deutlich hinter Amerika (70%).

Es überrascht nicht, dass die Vereinheitlichung und der Schutz der Kommunikation sensibler Inhalte für viele Unternehmen ein zunehmend wichtiges Ziel darstellt. Allerdings unterscheiden sich die Gründe in APAC von denen in Amerika und EMEA. 79 % nannten die Vermeidung negativer Auswirkungen auf die Marke als ersten oder zweiten Grund - verglichen mit der Verhinderung des Abflusses von vertraulichem geistigem Eigentum und Geschäftsgeheimnissen als Hauptgrund in EMEA (61 %) und der Vermeidung von Betriebsunterbrechungen und Umsatzeinbußen in Amerika (57 %). Die Vermeidung langwieriger und kostspieliger Rechtsstreitigkeiten (z. B. Sammelklagen aufgrund von Datenverlusten) wurde von Unternehmen in APAC am zweithäufigsten genannt (61 %).

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

Der Umgang mit den Risiken, die von externen Parteien ausgehen, ist ein wichtiges Anliegen für Unternehmen in den APAC-Ländern, die ein höheres Datenvolumen pro Unternehmen austauschen als Unternehmen in EMEA und Amerika: 77 % teilen, senden oder tauschen Daten mit mehr als 1.000 externen Parteien aus (verglichen mit 63 % in Amerika und EMEA). Dies ist besorgniserregend, da 39 % der Unternehmen in APAC angaben, dass sie sensible Daten in weniger als der Hälfte der Fälle nachverfolgen und kontrollieren können, sobald diese eine Anwendung verlassen.

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

83 % der Unternehmen in der Region APAC gaben an, dass die Messung und das Management der Compliance bei der Kommunikation mit sensiblen Inhalten einer gewissen bis deutlichen Verbesserung bedarf. Dies ist etwas weniger als der weltweite Durchschnitt von 88 %. Allerdings gaben 32 % der Befragten an, dass erhebliche Verbesserungen erforderlich sind - genauso viel wie in Nord- und Südamerika und mehr als in EMEA (25 %).

Wenn es um die Prüfung und Auswahl von Sicherheitsvalidierungen und -zertifizierungen geht, nannten die Unternehmen in der APAC-Region ISO27001, 27017 und 27018 als die wichtigsten (53 % nannten sie entweder an erster oder zweiter Stelle). NIST 800-171/CMMC 2.0 wurde von den Befragten aus APAC am zweithäufigsten genannt, gefolgt von IRAP (33 %). Letzteres ist nicht überraschend, wenn man bedenkt, dass viele der APAC-Befragten aus Australien stammen.

Bewertung des Sicherheitsrisikos für sensible Inhalte

82 % der Unternehmen in der APAC-Region gaben an, dass die Messung und das Management von Sicherheitsrisiken im Zusammenhang mit der Kommunikation sensibler Inhalte erheblich oder in gewissem Maße verbesserungsbedürftig sind. Dies ergibt Sinn, wenn man sich die Daten zu Sicherheitsverletzungen ansieht: 72 % der Unternehmen in APAC gaben an, dass ihre sensiblen Inhalte viermal oder öfter verletzt wurden (43 % gaben siebenmal oder öfter an). Das sind deutlich mehr als in EMEA und Amerika (48 % bzw. 53 %). Wie in EMEA und Amerika weiß eine erschreckend hohe Anzahl von Unternehmen in APAC nicht einmal, wie oft ihre sensiblen Inhalte angegriffen wurden (5 %).

Erweiterte Sicherheitsfunktionen und -verfahren wie Verschlüsselung, Multi-Faktor-Authentifizierung und Governance Tracking und -Kontrolle werden von Unternehmen in der APAC-Region nur in 43 % der Fälle für einige sensible Inhalte eingesetzt (57 % setzen sie immer ein, was deutlich unter den 67 % in Amerika liegt).

Bewertung der Risikos für Sicherheit und Compliance

Die Umfragedaten zeigen, dass in APAC ein hohes Risiko für Datenschutzverletzungen besteht. 42 % der Befragten gaben an, dass ihr Unternehmen im letzten Jahr mehr als sieben Datenschutzverletzungen zu verzeichnen hatte. Dies liegt deutlich über dem weltweiten Durchschnitt von 32 %, die von mehr als sieben Datenschutzverletzungen berichteten. Weitere 28 % berichteten von vier bis sechs Datenschutzverletzungen. 6 % gaben an, dies nicht zu wissen.

Hinsichtlich der Kosten für Rechtsstreitigkeiten ergab die Umfrage, dass 22 % der Unternehmen in der APAC-Region im vergangenen Jahr mehr als 5 Mio. USD für Rechtsstreitigkeiten ausgegeben haben. Dies ist weniger als der weltweite Durchschnitt von 25 %, die Prozesskosten von mehr als 5 Mio. USD angaben. Weitere 26 % der befragten APAC-Unternehmen gaben an, dass ihre Prozesskosten zwischen 3 und 5 Mio. USD lagen.

Kenntnis und Kategorisierung der Datentypen

24 % der Unternehmen in APAC gaben an, dass sie weniger als 50 % ihrer unstrukturierten Daten taggen und klassifizieren. Das ist etwas mehr als der weltweite Durchschnitt; 22 % taggen und klassifizieren weniger als ein Viertel; weitere 30 % gaben an, dass sie weniger als 50 % taggen und klassifizieren.

Diese Zahlen gewinnen an Bedeutung, wenn man die Antworten der Befragten aus APAC auf die Frage nach dem Prozentsatz der unstrukturierten Daten, die klassifiziert werden müssen, betrachtet. 20% gaben an, dass sie 25% oder weniger ihrer unstrukturierten Daten identifizieren und klassifizieren (und weitere 45% gaben zwischen 40% und 60% an). Im Vergleich zum weltweiten Durchschnitt liegen die Befragten in APAC zurück: 40 % weltweit identifizieren und klassifizieren 60 % oder mehr ihrer sensiblen Daten gegenüber 33 % in APAC.

Robustes Management sensibler Inhalte in APAC ist unerlässlich

Der “2024 Sensitive Content Communications Report” von Kiteworks zeigt die besonderen Herausforderungen auf, denen sich Unternehmen in APAC bei der Verwaltung der Kommunikation sensibler Inhalte gegenübersehen. Die Tatsache, dass 52 % der Unternehmen in der APAC-Region fünf oder mehr Kommunikationstools einsetzen, verdeutlicht die Komplexität der Nachverfolgung und Kontrolle sensibler Inhalte. Interessanterweise ist die Hauptmotivation für die Vereinheitlichung und den Schutz der Kommunikation sensibler Inhalte in der APAC-Region die Vermeidung schädlicher Auswirkungen auf die Marke, gefolgt von der Reduzierung kostspieliger Prozessrisiken.

Eine überwältigende Mehrheit der Unternehmen in APAC erkennt die Notwendigkeit, die Messung und das Management von Compliance- und Sicherheitsrisiken im Zusammenhang mit der Kommunikation sensibler Inhalte zu verbessern. Die Häufigkeit von Datenschutzverletzungen bei Unternehmen in der APAC-Region in Verbindung mit der geringen Verbreitung fortschrittlicher Sicherheitsmaßnahmen unterstreicht die Dringlichkeit, diese Schwachstellen zu beseitigen. Die Verbesserung von Datenklassifizierungs- und Kennzeichnungsverfahren sowie die Implementierung robuster Sicherheitsmaßnahmen sind für Unternehmen in APAC entscheidend, um ihre sensiblen Inhalte zu schützen und die Compliance in einer zunehmend komplexen digitalen Landschaft zu gewährleisten.

Lesen Sie den vollständigen Bericht