Kiteworks

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

HIGHLIGHTS

Verwendete Kommunikations-Tools	**13 %**	7+
	12 %	6
	25 %	5
	21 %	4
	18 %	3
	8 %	2
	3 %	1
Austausch sensibler Inhalte mit externen Parteien	**13 %**	über 5.000
	27 %	2.500 bis 4.999
	23 %	1.000 bis 2.499
	14 %	500 bis 999
	23 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	**53 %**	Finanzunterlagen
	50 %	Geistiges Eigentum
	46 %	Persönliche Daten
	38 %	GenKI LLMs
	38 %	Juristischer Schriftwechsel
	32 %	Patienteninformationen
	28 %	CUI und FCI
	15 %	M&A
Größter Fokus auf Datenschutz und Compliance (Top 2)	**57 %**	DSGVO
	29 %	Datenschutzgesetze der U.S.-Staaten
	28 %	CMMC
	27 %	Länderspezifische Datenschutzgesetze
	23 %	HIPAA
	22 %	SEC-Anforderungen
	14 %	PCI DSS
Wichtigste Sicherheits-validierungen (Top 2)	**59 %**	ISO 27001, 27017, 27018
	42 %	NIST 800-171/CMMC 2.0
	27 %	SOC 2 Type II
	27 %	IRAP (Australien)
	20 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	**10 %**	10+
	17 %	7 bis 9
	21 %	4 bis 6
	26 %	2 bis 3
	17 %	1
	9 %	weiß nicht

Der “2024 Kiteworks Sensitive Content Communications Privacy and Compliance Report” bietet eine detaillierte Analyse der Herausforderungen und Trends bei der Verwaltung sensibler Inhalte in verschiedenen Regionen, einschließlich EMEA (Europa, Naher Osten und Afrika). Der Bericht präsentiert die wichtigsten Ergebnisse in Bezug auf die EMEA-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

Die Hälfte der Unternehmen in der EMEA-Region nutzt fünf oder mehr Kommunikations-Tools, um sensible Inhalte zu versenden und auszutauschen. Dies entspricht einem geringeren Anteil als den 53 %, die weltweit diese Vorgehensweise nutzen. Im Vergleich zu den globalen Ergebnissen, bei denen 39 % der Unternehmen mehr als die Hälfte ihrer Kommunikation mit sensiblen Inhalten nicht nachverfolgen und kontrollieren können, sobald diese versendet, geteilt oder übertragen werden, haben die Unternehmen in der EMEA-Region ein größeres Problem: 45 % sind dazu nicht in der Lage.

Die Vereinheitlichung und der Schutz der Kommunikation mit sensiblen Inhalten ist für viele Unternehmen ein zunehmend wichtiges Ziel. Die Verhinderung von unerwünschtem Datenabfluss, von vertraulichem geistigen Eigentum und Geschäftsgeheimnissen (62 % nannten dies als erste oder zweite Priorität) sowie die Vermeidung langwieriger/teurer Rechtsstreitigkeiten (51 %, z. B. Sammelklagen aufgrund von Datenverlusten) haben für die Unternehmen in der EMEA-Region oberste Priorität. Die Ergebnisse zeigen, dass Unternehmen die Notwendigkeit erkennen, die Kommunikation mit sensiblen Inhalten zu konsolidieren, um Risiken zu minimieren und die betriebliche Effizienz zu verbessern.

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

Der Umgang mit Risiken, die von externen Parteien ausgehen, ist für Unternehmen in der EMEA-Region ein wichtiges Anliegen. 63 % der Unternehmen in der EMEA-Region tauschen vertrauliche Inhalte mit mehr als 1.000 externen Parteien aus, was etwas unter dem weltweiten Wert (66 %) liegt. Dies ist besorgniserregend, da nur 45 % der Unternehmen in der EMEA-Region angaben, dass sie in etwa der Hälfte der Fälle in der Lage sind, sensible Daten zu verfolgen und zu kontrollieren, sobald diese eine Anwendung verlassen.

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

86 % der Unternehmen in der EMEA-Region gaben an, dass die Messung und das Management der Compliance bei der Kommunikation sensibler Inhalte etwas bis deutlich verbessert werden muss. Dieser Wert liegt leicht unter dem weltweiten Durchschnitt von 88 %.

Es überrascht nicht, dass die Unternehmen in der EMEA-Region die DSGVO vor anderen Datenschutz- und Compliance-Vorschriften ganz oben auf ihre Prioritätenliste gesetzt haben (57 % an erster oder zweiter Stelle). Danach folgten die Datenschutzgesetze der US-Bundesstaaten (29 %) und CMMC 2.0 (28 %). Im Falle von CMMC 2.0 ist für EMEA-Unternehmen, die in den USA tätig sind, die Einhaltung der Gesetze der einzelnen US-Bundesstaaten und der Bundesgesetze wichtig. Bei der Prüfung und Auswahl von Sicherheitsvalidierungen und -zertifizierungen nannten die Befragten aus der EMEA-Region ISO 27001, 27017 und 27018 häufiger (59 %) als die Befragten aus der APAC-Region (48 %) und Amerika (46 %). Überraschenderweise wurde die NIS 2-Richtlinie nur in 20 % der Fälle genannt.

Bewertung des Sicherheitsrisikos für sensible Inhalte

88 % der Unternehmen in der EMEA-Region geben an, dass ihre Messung und ihr Management von Sicherheitsrisiken im Zusammenhang mit der Kommunikation sensibler Inhalte stark oder etwas verbesserungsbedürftig sind. 48 % der Unternehmen in der EMEA-Region gaben an, dass ihre sensiblen Inhalte viermal oder öfter angegriffen wurden (27 % gaben an, dass ihre sensiblen Inhalte siebenmal oder öfter angegriffen wurden). Noch beunruhigender ist die Tatsache, dass 9 % der Unternehmen in der EMEA-Region zugaben, dass sie darüber nicht Bescheid wüssten.

Erweiterte Sicherheitsfunktionen und -verfahren wie Verschlüsselung, Multi-Faktor-Authentifizierung sowie Governance-Tracking und -Kontrolle werden von 43 % der Unternehmen in der EMEA-Region nur für einige sensible Inhalte eingesetzt. Weitere 4 % gaben an, dass erweiterte Sicherheitsfunktionen überhaupt nicht genutzt werden. 53 % der Unternehmen in der EMEA-Region gaben an, dass sie ständig erweiterte Sicherheitsmaßnahmen nutzen. Im Vergleich zum weltweiten Durchschnitt (59 %) liegt EMEA hier zurück.

Bewertung der Kosten für Sicherheit und Compliance

27 % der Befragten in der EMEA-Region gaben an, im vergangenen Jahr mehr als sieben Datenschutzverletzungen bei der Kommunikation sensibler Inhalte erlebt zu haben. Weitere 21 % berichteten von vier bis sechs Verstößen. Dies ist etwas weniger als der weltweite Durchschnitt von 32 % mit mehr als sieben Datenschutzverletzungen. Ebenso besorgniserregend ist die Tatsache, dass 9 % der Befragten nicht sicher waren, wie viele Datenschutzverletzungen in ihrem Unternehmen aufgetreten sind.

Was die finanziellen Auswirkungen von Datenschutzverletzungen betrifft, so gaben 25 % der Unternehmen in der EMEA-Region an, dass sie mehr als 5 Mio. USD an Rechtskosten zu tragen hatten, was dem weltweiten Durchschnitt entspricht. Weitere 16 % gaben an, dass sie zwischen 3 und 5 Mio. USD verloren haben - beziehungsweise gaben 41 % an, dass sie im vergangenen Jahr mehr als 3 Mio. USD verloren haben. Diese Zahlen sind zwar nicht so hoch wie in Nord- und Südamerika, aber immer noch beachtlich.

Kenntnis und Kategorisierung der Datentypen

21 % der Unternehmen in der EMEA-Region gaben an, dass sie weniger als 25 % ihrer unstrukturierten Daten taggen und klassifizieren, weitere 33 % gaben an, dass sie weniger als die Hälfte taggen und klassifizieren. Diese Prozentsätze stimmen mit dem weltweiten Durchschnitt überein: 21 % taggen und klassifizieren weniger als ein Viertel, während weitere 29 % angaben, die Hälfte oder weniger zu taggen und zu klassifizieren.

Diese Zahlen gewinnen an Bedeutung, wenn man die Antworten der EMEA-Befragten auf die Frage nach dem Prozentsatz der unstrukturierten Daten, die klassifiziert werden müssen, betrachtet. 24 % gaben an, dass sie 40 % oder weniger ihrer unstrukturierten Daten identifizieren und klassifizieren müssen (und weitere 37 % gaben an, dass sie zwischen 40 % und 60 % klassifizieren müssen). Dies weist auf eine Lücke hin: unstrukturierte Daten, die nicht gekennzeichnet und klassifiziert sind, jedoch klassifiziert werden müssen.

Robustes Management sensibler Inhalte in EMEA ist unerlässlich

Der “2024 Kiteworks Sensitive Content Communications Report” unterstreicht die Bedeutung von Risikomanagement und Compliance bei der Kommunikation sensibler Inhalte. Für Unternehmen in der EMEA-Region sind der Einsatz fortschrittlicher Kommunikations-Tools, die Eindämmung von Risiken seitens externer Parteien, die Einhaltung strenger Compliance-Standards und das Verständnis der Art von Daten, mit denen sie umgehen, wesentliche Bestandteile einer robusten Cybersicherheitsstrategie. Darüber hinaus werden Unternehmen in der EMEA-Region von der nächsten Generation des Digital Rights Management (DRM) profitieren, das eine erweiterte Verwaltung sensibler Inhalte ermöglicht.

Da sich die Bedrohungslandschaft ständig weiterentwickelt, ist ein proaktiver und umfassender Ansatz für das Management sensibler Inhalte unerlässlich, um die Datenintegrität zu wahren und Unternehmenswerte zu schützen. Unternehmen in der EMEA-Region, die sich im Vergleich zu den globalen Trends etwas stärker auf bestimmte Aspekte konzentrieren, sind gut aufgestellt, um diese Herausforderungen effektiv zu meistern.

Lesen Sie den vollständigen Bericht