Kiteworks

2024 Analyse für die Kommunikation sensibler Inhalte in der Fertigung: Sicherheit und Compliance-Trends

HIGHLIGHTS

Verwendete Kommunikations-tools	**17 %**	7+
	8 %	6
	27 %	5
	20 %	4
	17 %	3
	11 %	2
	2 %	1
Austausch sensibler Inhalte mit externen Parteien	**11 %**	über 5.000
	23 %	2.500 bis 4.999
	32 %	1.000 bis 2.499
	20 %	500 bis 999
	15 %	weniger als 499
Datentypen, die am meisten Sorgen bereiten (Top 3)	**79 %**	Finanzunterlagen
	46 %	Geistiges Eigentum
	46 %	Juristischer Schriftwechsel
	44 %	GenKI LLMs
	35 %	Persönliche Daten
	23 %	M&A
	15 %	CUI und FCI
	13 %	Patienteninformationen
Größter Fokus auf Datenschutz und Compliance (Top 2)	**52 %**	Datenschutzgesetze der U.S.-Staaten
	36 %	DSGVO
	33 %	SEC-Anforderungen
	29 %	CMMC
	21 %	HIPAA
	18 %	Länderspezifische Datenschutzgesetze
	11 %	PCI DSS
Wichtigste Sicherheits-validierungen (Top 2)	**58 %**	ISO 27001, 27017, 27018
	37 %	IRAP (Australien)
	33 %	SOC 2 Type II
	29 %	NIST 800-171/CMMC 2.0
	29 %	FedRAMP Moderate
	9 %	NIS 2-Richtlinie
Anzahl der Hacks bei der Kommunikation sensibler Inhalte	**14 %**	10+
	12 %	7 bis 9
	23 %	4 bis 6
	29 %	2 bis 3
	23 %	1
	0 %	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 der Fertigung. Dieser Kurzbericht konzentriert sich auf die wichtigsten Ergebnisse für die Fertigungsindustrie 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 Hersteller verwenden fünf oder mehr Kommunikationstools, um sensible Inhalte zu versenden und auszutauschen. Dies ist etwas weniger als die 53 % der Befragten weltweit, die dies tun. Hinsichtlich der Nachverfolgung und Kontrolle sensibler Inhalte gaben 52 % der Hersteller an, dass sie in der Lage sind, intern versandte und ausgetauschte sensible Inhalte nachzuverfolgen und zu kontrollieren, während nur 39 % angaben, dass sie in der Lage sind, extern ausgetauschte sensible Inhalte nachzuverfolgen und zu kontrollieren.

Wenn es um den Datenschutz bei der Kommunikation sensibler Inhalte und die Einhaltung gesetzlicher Vorschriften geht, stehen für die Hersteller die Verhinderung der Preisgabe vertraulichen geistigen Eigentums und von Geschäftsgeheimnissen (61 %) sowie die Vermeidung von Betriebsunterbrechungen und Umsatzeinbußen (44 %) an erster Stelle. Dagegen gaben die Befragten branchenübergreifend an, den Abfluss von vertraulichem geistigem Eigentum und Geschäftsgeheimnissen verhindern (56 %) und langwierige und kostspielige Rechtsstreitigkeiten vermeiden (51%) zu wollen. Die geringste Priorität wurde von den Befragten aus der Fertigungsindustrie der Vermeidung negativer Auswirkungen auf die Marke eingeräumt (15 %).

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

Das Management der mit externen Parteien verbundenen Risiken ist eine große Herausforderung für Unternehmen in der Fertigungsindustrie. 34 % der Befragten gaben an, dass sie sensible Inhalte mit mehr als 2.500 externen Parteien austauschen. Zwei Drittel der Hersteller tauschen sensible Inhalte mit mehr als 1.000 externen Parteien aus. Gute Nachrichten gab es in Bezug auf die Verfolgung und Kontrolle der Kommunikation sensibler Inhalte in der Fertigungsindustrie. Ein höherer Prozentsatz (79 %) als in jeder anderen Branche gab an, dass sie mehr als drei Viertel der sensiblen Inhalte nachverfolgen und kontrollieren können, sobald diese eine Anwendung verlassen.

Bewertung des aktuellen Compliance-Status bezüglich sensibler Inhalte

94 % der Hersteller gaben an, dass die Messung und das Management der Compliance bei der Kommunikation sensibler Inhalte einiger bis erheblicher Verbesserungen bedarf. Dies ist deutlich mehr als die Gesamtzahl der Befragten (88 %). Die einzige Branche, die eine größere Lücke als die Fertigungsindustrie meldete, waren Dienstleistungsunternehmen (96 %).

Die Hersteller nannten die Datenschutzgesetze der US-Bundesstaaten als ihre wichtigste Sorge vor anderen Datenschutz- und Compliance-Vorschriften (52 % nannten sie an erster oder zweiter Stelle). Dies ist keine große Überraschung, da mittlerweile 18 nationale Gesetze in den Vereinigten Staaten verabschiedet wurden. 36 % der Unternehmen nannten die DSGVO als eines der beiden wichtigsten Themen. PCI DSS wurde von 11 % der Unternehmen an erster oder zweiter Stelle genannt.

Bei der Prüfung und Auswahl von Sicherheitsvalidierungen oder -zertifizierungen nannten 58 % der Hersteller ISO27001, 27017 und 27018 als eine der beiden wichtigsten Zertifizierungen. Überraschenderweise wurde das Information Security Registered Assessors Program (IRAP), das von der australischen Regierung beaufsichtigt wird, um die Cybersicherheit unabhängig zu bewerten, Risiken zu identifizieren und Abhilfemaßnahmen vorzuschlagen, von 37 % der Hersteller am häufigsten genannt - häufiger als SOC 2Type II (33 %).

Bewertung des Sicherheitsrisikos für sensible Inhalte

98 % der Hersteller gaben an, dass die Messung und das Management von Sicherheitsrisiken im Zusammenhang mit der Kommunikation sensibler Inhalte in hohem oder gewissem Maße verbesserungsbedürftig sind (im Vergleich zu 88 % aller Befragten). Dies ist ein signifikanter Unterschied und eine Sicherheitslücke.

Erweiterte Sicherheitsfunktionen und -verfahren wie Verschlüsselung, Multi-Faktor-Authentifizierung sowie Überwachung und Kontrolle werden von den Herstellern nur in 42 % der Fälle für bestimmte sensible Inhalte eingesetzt (gegenüber 39 % in allen anderen Branchen). Dies weist auf ein Sicherheitsrisiko hin, das behoben werden muss.

Bewertung der Kosten für Sicherheit und Compliance

Wie in den meisten anderen Branchen zeigen die Umfragedaten, dass Unternehmen der Fertigungsindustrie einem ernsthaften Risiko von Datenschutzverletzungen ausgesetzt sind, wenngleich sie besser abschneiden

als die Branche insgesamt. Konkret gaben 49 % der Hersteller an, dass ihre sensiblen Inhalte fünf oder mehr Mal angegriffen wurden (24 % gaben sieben oder mehr Mal an). Dies ist besser als bei allen Umfrageteilnehmern: Bei 32 % waren es sieben oder mehr und bei 55 % vier oder mehr.

Hinsichtlich der Kosten für Rechtsstreitigkeiten stehen die Hersteller der Umfrage zufolge besser da als die meisten anderen Wirtschaftszweige: 18 % der Befragten gaben an, jährlich mehr als 5 Mio. USD für Rechtsstreitigkeiten auszugeben. Im Vergleich dazu gaben 25 % aller Befragten an, dass ihre Prozesskosten über 5 Mio. USD liegen.

Kenntnis und Kategorisierung der Datentypen

Fast die Hälfte (49 %) der Hersteller gab an, mehr als drei Viertel ihrer unstrukturierten Daten zu taggen und zu klassifizieren, weitere 30 % gaben an, mehr als die Hälfte zu taggen und zu klassifizieren. Diese Prozentsätze entsprechen in etwa den globalen Zahlen, wo 48 % angaben, drei Viertel oder mehr ihrer unstrukturierten Daten zu taggen und zu klassifizieren.

Aber nicht alle unstrukturierten Daten müssen klassifiziert werden, so zumindest die Meinung der Befragten. 18 % der Befragten aus dem produzierenden Gewerbe gaben an, dass 80 % oder mehr der unstrukturierten Daten klassifiziert werden sollten. 58 % gaben an, dass weniger als 60 % der unstrukturierten Daten gekennzeichnet und klassifiziert werden sollten.

Robustes Management sensibler Inhalte ist in der Fertigungsindustrie unerlässlich

Der “2024 Sensitive Content Communications Report” von Kiteworks unterstreicht die dringende Notwendigkeit eines robusten Risiko- und Compliance-Managements für die Kommunikation sensibler Inhalte in der Fertigungsindustrie. Finanzdokumente wurden von den Befragten aus der Fertigungsindustrie mit Abstand als die Datenart genannt, die das größte Risiko darstellt (79 %) - der höchste Wert aller Branchen.

Die Hersteller 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. Die Hälfte der Befragten muss mehr als 11 Protokolle abgleichen. Dies führt zu einem enormen Berichtsstau. 11 % verbringen 2.500 Stunden oder mehr pro Jahr damit und weitere 21 % mehr als 2.000 Stunden.

Lesen Sie den vollständigen Bericht