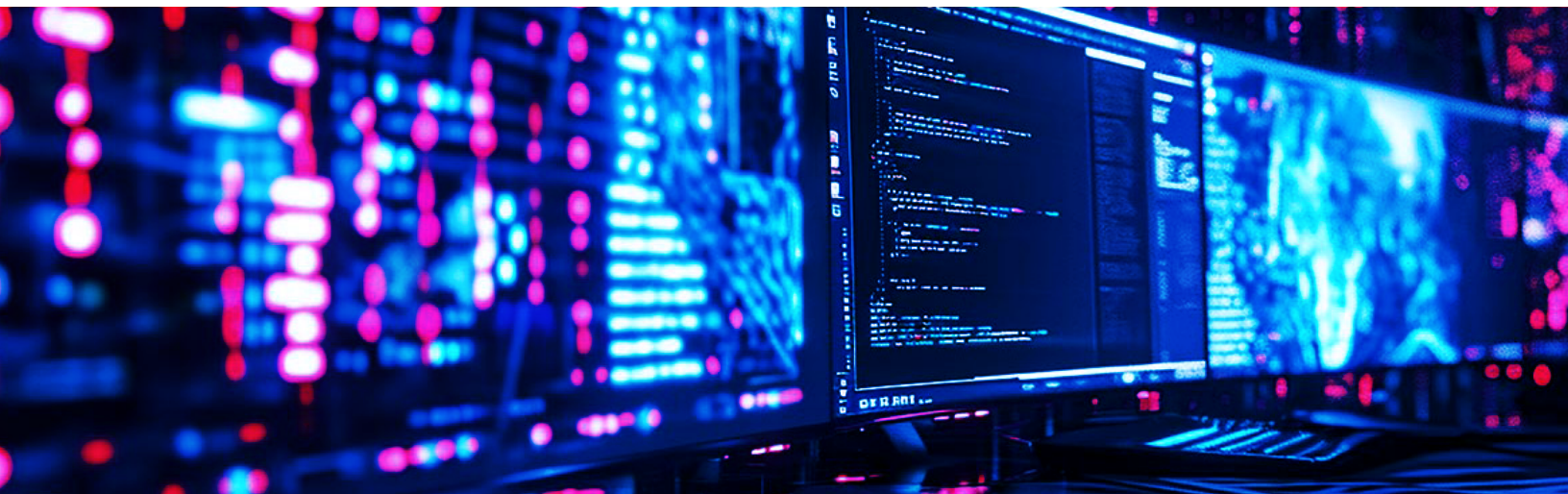




2024 Bericht über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte

Schutz der Kommunikation sensibler Inhalte

KURZBERICHT



Der “2024 Sensitive Content Communications Privacy and Compliance Report” von Kiteworks bietet eine detaillierte Analyse der aktuellen Datensicherheits- und Datenschutzverfahren weltweit. Mit Beiträgen von 572 Fachleuten aus den Bereichen IT, Cybersicherheit und Compliance unterstreicht der Bericht die Bedeutung des Schutzes sensibler Daten, einschließlich personenbezogener Daten, geschützter Patienteninformationen, Finanzdaten und geistigen Eigentums. Der Bericht unterstreicht die verheerenden Auswirkungen von Datenschutzverletzungen, die zu finanziellen Verlusten, Reputationsschäden, behördlichen Sanktionen und Betriebsunterbrechungen führen können.

Methodik des Berichts

Der Bericht basiert auf einer umfassenden Umfrage, die von Centiment zwischen Februar und März 2024 durchgeführt wurde und 33 Fragen zu Datensicherheit, Datenschutz und Compliance enthielt. Die Antworten wurden von Fachleuten aus acht Ländern in Nordamerika, Europa, dem Nahen Osten, Afrika (EMEA) und dem asiatisch-pazifischen Raum gesammelt, die verschiedene Branchen wie Sicherheit und Verteidigung, Fertigung, Gesundheitswesen, Finanzdienstleistungen, öffentliche Verwaltung und Bildungswesen vertraten. Die Vielfalt der Befragten gewährleistet eine breite Perspektive auf die Herausforderungen und Prioritäten beim Schutz sensibler Inhalte.



Die wichtigsten Ergebnisse des Kiteworks-Berichts

1. Sicherheitsrisiken im Zusammenhang mit sensiblen Inhalten

Sensible Inhalte geraten zunehmend ins Visier von Cyberkriminellen. Der Bericht zeigt, dass fast ein Drittel der Befragten im letzten Jahr sieben oder mehr kriminelle externe Hackerangriffe erlebt hat. Einige der wichtigsten Ergebnisse:

32%

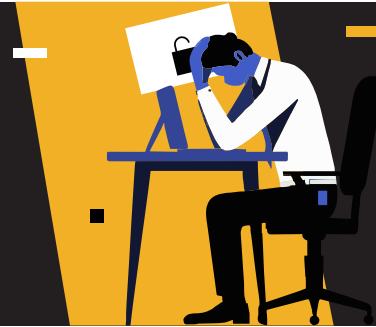
der Befragten meldeten **sieben oder mehr Datenschutzverletzungen**

68%

Über 68 % der Befragten aus den Bereichen **Hochschulen, Sicherheit und Verteidigung sowie Öl und Gas** meldeten mehrere Datenschutzverletzungen

28%

Im Bereich **Pharma und Life Sciences** meldeten nur 28 % der Befragten vier oder mehr Datenschutzverletzungen



2. KI-Cyber-Risiken und die Kommunikation sensibler Inhalte

KI-Technologien, insbesondere generative KI (GenKI) und große Sprachmodelle (Large Language Models, LLM), stellen erhebliche Sicherheits Herausforderungen dar. Nahezu die Hälfte der Cybersicherheitsbeauftragten ist besorgt über den Zugriff externer Parteien auf sensible Daten durch KI-Tools und befürchtet Datenlecks und Fehlentscheidungen durch KI-Systeme. Weitere relevante Ergebnisse:

48%

der Befragten finden es **schwierig, Zero-Trust-Prinzipien** sowohl in On-Premises- als auch in Cloud-Umgebungen **anzuwenden**

45%

Der Unternehmen haben bei der Sicherheit sensibler Inhalte **noch kein Zero Trust erreicht**

Nur

35%

der Befragten in Großbritannien

39%

& aus dem Mittleren Osten und dem asiatisch-pazifischen Raum

haben **Zero-Trust-Maßnahmen eingeführt**



3. Compliance-Risiken und Kommunikation sensibler Inhalte

Der Umgang mit Datenschutzbestimmungen wird immer komplexer, da Gesetze wie die DSGVO und der CCPA ständige Anpassungen erfordern. Der Bericht zeigt, dass 93 % der Unternehmen ihre Cybersicherheitsstrategien als Reaktion auf die sich ändernden Vorschriften überdenken mussten.¹ Einige der wichtigsten Ergebnisse:

93%

der Unternehmen mussten ihre **Cybersicherheitsstrategien** aufgrund neuer Vorschriften überdenken¹

Nur

11%

der Befragten gaben an, dass beim Management des Compliance-Risikos **keine Verbesserungen erforderlich** seien

43%

der Unternehmen gaben an, **nicht in der Lage zu sein**, den gesamten Austausch externer Inhalte **zu verfolgen, zu kontrollieren und zu dokumentieren**



4. Die Rolle menschlichen Versagens bei Datenschutzverletzungen

Menschliches Versagen ist ein erheblicher Risikofaktor, der für 68 % aller Datenschutzverletzungen verantwortlich ist. Um dieses Risiko zu verringern, sollten Unternehmen regelmäßige Schulungen, Multi-Faktor-Authentifizierung (MFA), strenge Zugangskontrollen, umfassende Datenverschlüsselung und wirksame Pläne zur Reaktion auf Vorfälle einführen. Die wichtigsten Ergebnisse:

68 % der Fehler, die zu Datenschutzverletzungen führen, sind nutzerbedingt



Branchen wie das Gesundheitswesen und der Finanzsektor sind besonders anfällig für nutzerbedingte Datenschutzverletzungen



5. Datenschutz, Compliance und die Kommunikation sensibler Inhalte

Der Bericht hebt die hohen Kosten von Datenschutzverstößen hervor, wobei die Prozesskosten oft 2 Mio. USD jährlich und unter Umständen sogar 7 Mio. USD übersteigen. Eine ordnungsgemäße Datenklassifizierung ist unerlässlich, doch viele Unternehmen tun sich damit schwer. Einige der Ergebnisse:

60%

der Befragten gaben an, jährlich mehr als 2 Mio. USD für Rechtsstreitigkeiten im Zusammenhang mit Datenschutzverletzungen auszugeben

49%

der Unternehmen gaben an, dass 75 % oder mehr ihrer unstrukturierten Daten gekennzeichnet oder klassifiziert sind

41%

der Befragten gaben an, dass die DSGVO und die Datenschutzgesetze der US-Bundesstaaten die beiden wichtigsten Bereiche sind, auf die sie sich in Bezug auf Datenschutz und Compliance konzentrieren



6. Compliance, Risikomanagement und die Kommunikation sensibler Inhalte

Compliance-Berichte stellen nach wie vor eine Herausforderung dar, da viele Unternehmen nicht in der Lage sind, den gesamten externen Austausch von Inhalten zu verfolgen und zu dokumentieren. Der Bericht empfiehlt, in fortschrittliche Tools und Prozesse zu investieren, um den Aufwand für die Compliance-Berichterstattung zu verringern und die Sicherheitsverfahren zu verbessern. Einige der Ergebnisse:

53%

der Befragten priorisieren ISO-Standards

42%

legen den Schwerpunkt auf NIST 800-171

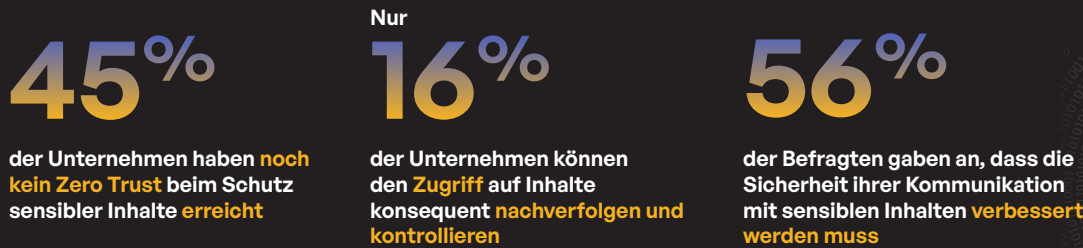
62%

der Unternehmen wenden jährlich mehr als 1.500 Arbeitsstunden für Compliance-Berichte auf



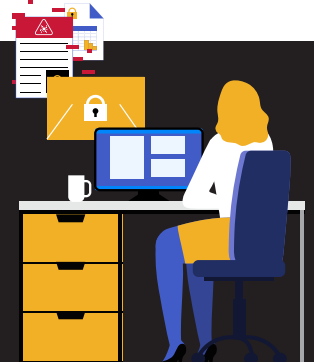
7. Cybersicherheit, Risikomanagement und die Kommunikation sensibler Inhalte

Das Erreichen von Zero Trust ist entscheidend für die Sicherheit von Inhalten, aber auch eine Herausforderung. Der Bericht unterstreicht die Bedeutung erweiterter Sicherheitsmaßnahmen, einschließlich Verschlüsselung, Bedrohungserkennung und Schulung des Sicherheitsbewusstseins. Eine effektive Nachverfolgung und Kontrolle des Zugriffs auf sensible Inhalte ist ebenfalls von entscheidender Bedeutung.









8. Operative Prozesse und die Kommunikation sensibler Inhalte

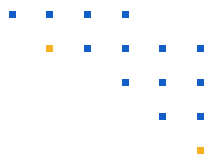
Das Management von Risiken, die von externen Parteien ausgehen, die Konsolidierung von Kommunikationstools und die Bewältigung der Herausforderungen im Zusammenhang mit dem Abgleich von Protokollen sind von entscheidender Bedeutung für den Schutz sensibler Inhalte. Der Bericht empfiehlt, die Anzahl der Tools zu reduzieren, verlässliche Nachverfolgungsmechanismen zu implementieren und die Einhaltung der Datenschutzbestimmungen zu gewährleisten. Die wichtigsten Ergebnisse:



Effektive Strategien zum Schutz der Kommunikation sensibler Inhalte

Vor dem Hintergrund der acht oben genannten Erkenntnisse sollten die Unternehmen Prioritäten setzen:

- | | | | | | |
|--|---|---|--|--|--|
|  <p>1. Konsolidierung von Kommunikationstools:</p> <p>Die Reduzierung der Anzahl von Tools kann das Risiko von Datenschutzverletzungen senken und die Effizienz verbessern</p> |  <p>2. Implementierung von inhaltsdefiniertem Zero Trust:</p> <p>Strenge Zugangskontrollen und eine kontinuierliche Überwachung nach dem Zero-Trust-Prinzip sind unerlässlich</p> |  <p>3. Aufbau von Private Content Networks:</p> <p>Die Isolierung sensibler Kommunikation erhöht die Sicherheit</p> |  <p>4. Verbesserung der Sicherheitsmaßnahmen:</p> <p>Investitionen in Verschlüsselung, MFA und Bedrohungserkennung</p> |  <p>5. Verbesserung der Compliance-Berichterstattung:</p> <p>Automatisierte Prozesse sorgen für eine zuverlässige Nachverfolgung</p> |  <p>6. Priorisierung der Datenklassifikation:</p> <p>Implementieren von Systemen, die Daten mit hohem Risiko kategorisieren und schützen</p> |
|--|---|---|--|--|--|



Fazit

Der Kiteworks-Bericht 2024 unterstreicht die dringende Notwendigkeit robuster Strategien für Datensicherheit und Compliance. Durch die Bewältigung der identifizierten Herausforderungen und die Umsetzung der empfohlenen Strategien können Unternehmen ihre sensiblen Inhalte besser schützen, die Einhaltung von Vorschriften gewährleisten und Risiken in der komplexen digitalen Landschaft von heute minimieren.

Weitere Informationen finden Sie auf der [Website des Berichts](#) mit regionalen und branchenspezifischen Kurzberichten, Infografiken und einer Kitecast-Podcast-Episode.

¹“Despite increased budgets, organizations struggle with compliance,” Help Net Security, 24. Mai 2024.