Kiteworks

Top 11 Datenpannen

Sinnvolle Erkenntnisse und Empfehlungen mit dem Kiteworks Risikoexpositionsindex

1H 2024 BERICHT

Inhaltsverzeichnis

Einleitung

Sehr geehrte Leserinnen und Leser,

während wir uns durch die komplexe Landschaft der Cybersicherheit im Jahr 2024 navigieren, sind die zunehmende Häufigkeit und Schwere von Datenschutzverstößen unbestreitbar. Allein in der ersten Hälfte dieses Jahres haben Cyberkriminelle über eine Milliarde Datensätze kompromittiert, was mehrere Sektoren betrifft, einschließlich Telekommunikation, Gesundheitswesen, Finanzen und Regierung. Diese Vorfälle haben nicht nur die Schwachstellen innerhalb unserer digitalen Infrastrukturen aufgedeckt, sondern auch die dringende Notwendigkeit robuster Cybersicherheitsstrategien zur Schutz sensibler Daten unterstrichen.

Der Bericht „Top 11 Datenschutzverstöße im 1. Halbjahr 2024“ nutzt den Kiteworks Risk Exposure Index, um eine detaillierte Analyse der bedeutendsten Verstöße zu bieten, die in der ersten Jahreshälfte aufgetreten sind. Unsere Erkenntnisse offenbaren mehrere alarmierende Trends, von der steigenden Prävalenz von Ransomware-Angriffen bis hin zu den Schwachstellen, die mit Interaktionen Dritter und internen Fehlern verbunden sind. Dieser Bericht hebt die kritische Bedeutung des Managements von sensiblen Inhaltskommunikationen in allen Sektoren hervor, besonders da Organisationen zunehmend auf mehrere Kommunikationstools und Dienste Dritter angewiesen sind, was zahlreiche Eintrittspunkte für Cyberbedrohungen schaffen kann.

Bei Kiteworks sind wir dazu verpflichtet, Organisationen bei der Minderung dieser Risiken zu unterstützen, indem wir handlungsorientierte Einblicke und Empfehlungen bereitstellen. Der in diesem Bericht vorgestellte Risk Exposure Index ist ein strategisches Werkzeug, das Organisationen dabei helfen soll, Datenschutzverstöße basierend auf ihrer Schwere und potenziellen Auswirkung zu bewerten und zu priorisieren. Durch die Anwendung dieses umfassenden Rahmens können Organisationen Ressourcen besser zuweisen, ihre Sicherheitspositionen stärken und ihre Gesamtresilienz gegenüber zukünftigen Verstößen verbessern.

Wir hoffen, dass dieser Bericht wertvolle Orientierung bietet, während Sie weiterhin Ihre sensiblen Informationen schützen. Gemeinsam können wir eine sicherere digitale Zukunft aufbauen.

Mit freundlichen Grüßen,

Patrick Spencer

Patrick E. Spencer, Ph.D.
Vizepräsident für Unternehmensmarketing und Forschung
Kiteworks

Überblick über Datenpannen im 1H 2024

Die erste Hälfte des Jahres 2024 verzeichnete einen signifikanten Anstieg sowohl in der Anzahl als auch im Umfang von Datenpannen, was die wachsende Raffinesse und Entschlossenheit von Cyberkriminellen weltweit widerspiegelt. Laut Daten des Identity Theft Resource Center (ITRC)[1] kompromittierten die zehn größten Datenpannen in diesem Zeitraum über eine Milliarde Datensätze in verschiedenen Sektoren, einschließlich Telekommunikation, Gesundheitswesen, Finanzen, Technologie und Regierungsbehörden. Diese Vorfälle reichen von Ransomware-Angriffen und Schwachstellen in der Lieferkette bis hin zu unbeabsichtigten Datenlecks und unterstreichen die vielfältigen Taktiken, die von Cyberkriminellen eingesetzt werden, sowie die weit verbreiteten Schwachstellen in verschiedenen Branchen. Die Top-10-Liste des ITRC schloss den National Public Data-Breach nicht ein, der bis zu 2,9 Milliarden Datensätze von 1,3 Millionen Personen offenlegte. Daher haben wir den National Public Data in unseren Bericht aufgenommen.

Erkenntnisse im Kiteworks 2024 Sensitive Content Communications Privacy and Compliance Report betonen weiterhin die kritische Natur des Managements sensibler Daten in allen Sektoren.[2] Der Bericht hebt die Herausforderungen hervor, denen Organisationen beim Schutz sensibler Inhalte gegenüberstehen, da sie zunehmend auf mehrere Kommunikationstools und Interaktionen mit Drittanbietern angewiesen sind, was zahlreiche Schwachstellen schaffen kann. Zum Beispiel stellte der Bericht fest, dass diejenigen mit 10 oder mehr Kommunikationstools 3,55-mal mehr Datenpannen erlebten als der durchschnittlich von der gesamten Befragtengruppe gemeldete Wert.

Schlüsseltrends bei Datenschutzverstößen

Wenn man unter die Haube der Top 11 Datenpannen im 1. Halbjahr 2024 schaut, kommen verschiedene wichtige Erkenntnisse zum Vorschein:

1. **Ransomware-Angriffe:** Ransomware bleibt eine vorherrschende Angriffsmethode, die Organisationen in verschiedenen Sektoren ins Visier nimmt. Hochkarätige Sicherheitsverletzungen, wie die bei Change Healthcare und MediSecure, zeigen die verheerenden Auswirkungen, die Ransomware nicht nur durch die Störung von Betriebsabläufen, sondern auch durch den Kompromiss sensibler Daten haben kann. Diese Angriffe haben zu erheblichen finanziellen Verlusten und Betriebsunterbrechungen geführt und betonen die Notwendigkeit robuster Verteidigungsstrategien gegen Ransomware.

2. **Das enorme Ausmaß der Datenexposition:** Das Volumen der in Datenschutzverletzungen exponierten Daten hat sich eskaliert, wobei Vorfälle, die Millionen von Datensätzen betreffen, immer häufiger werden. Zum Beispiel erlitt AT&T zwei große Brüche, die zusammen über 180 Millionen Kundenakten kompromittierten, einschließlich persönlicher Informationen und Anruflisten. Ähnlich betraf der Bruch bei Snowflake mehrere Unternehmen und legte Hunderte Millionen von Datensätzen offen, was die weitreichende Bedrohung durch Lieferkettenangriffe in der heutigen vernetzten digitalen Landschaft veranschaulicht (bestätigt durch die Erkenntnisse im Verizon Data Breach Investigations Report 2024, wo 15% aller Angriffe im letzten Jahr mit der Lieferkette verbunden waren).[3]

3. **Schwachstellen in verschiedenen Sektoren:** Datenschutzverletzungen beschränken sich nicht auf einen einzelnen Sektor; stattdessen betreffen sie eine breite Palette von Branchen, die jeweils einzigartige Schwachstellen aufweisen. Sektoren wie das Gesundheitswesen, die Finanzbranche und die Technologiebranche sind aufgrund der sensiblen Natur der von ihnen verarbeiteten Daten besonders gefährdet und im Top-10-Bericht über Datenschutzverletzungen des ITRC für das erste Halbjahr 2024 gut vertreten. Das Fehlen von Governance-Tracking und -Kontrollen sowie fortgeschrittene Sicherheitsfähigkeiten sind die Hauptgründe. Der Kiteworks-Bericht hebt beispielsweise hervor, dass 57 % der Organisationen externe Inhalte, die gesendet und geteilt werden, nicht nachverfolgen, kontrollieren und darüber berichten können.

4. **Aufkommende Bedrohungen durch Drittparteienrisiken und interne Fehler:** Jenseits externer Angriffe haben sich auch Risiken durch Drittparteien und interne Fehler als signifikante Bedrohungen herausgestellt. Die Datenschutzverstöße bei Kaiser und USPS, bei denen sensible Informationen versehentlich mit Werbetreibenden geteilt wurden, unterstreichen die wachsende Besorgnis über die interne Datenverwaltung und die Risiken, die mit Interaktionen mit Drittparteien verbunden sind. Die Nachverfolgung und Kontrolle des Datenflusses zu und von all den Drittparteien, mit denen Organisationen Daten austauschen, ist schwierig, wobei zwei Drittel der Organisationen berichten, dass sie sensible Inhalte mit über 1.000 Drittparteien austauschen.[4]

Datenschutzverstoß-Details

Datenverstoß	Risiko expositi-onsindex	Anzahl der betroffenen Datensätze	Geschätzte gesamtwirtschaftliche Auswirkungen (USD)	Art der konvertierten Daten	Verstöße gegen gesetzliche Vorgaben	Ransomware Nachfrage
Change Healthcare	**9.46**	100,000,000	$17,900,000,000	Persönliche, medizinische,	HIPAA, HITECH Act, California CMIA, Texas Medical Records Privacy Act, HIPAA-Sicherheitsregel, HIPAA-Datenschutzregel	Ja, unbekannter Betrag bezahlt
National Public Data	**9.46**	2,900,000,000	$501,700,000,000	Persönliche Sozialversiche-rungsnummern	FTC Act, DSGVO, verschiedene US-amerikanische Datenschutzgesetze der Bundesstaaten wie CCPA	Nein
AT&T (two breaches)	**9.37**	110,000,000	$19,690,000,000	Telefonnummern, Anrufprotokolle, persönliche Informationen	FCC-Vorschriften (CPNI), FTC Act, CCPA, NY SHIELD Act, DSGVO, Telekommunikationsgesetz	Ja, ungenannte Summe
Synnovis	**9.11**	300,000,000	$53,700,000,000	Patienteninteraktion-sdaten	UK Data Protection Act 2018, DSGVO, NIS-Verordnungen, UK NHS Data Security and Protection Toolkit	Ja, 50 Millionen Dollar gefordert
Ticketmaster	**8.79**	560,000,000	$100,240,000,000	Vollständige Namen, Adressen, E-Mail-Adressen, Telefonnummern, Zahlungskartendaten	PCI DSS, FTC Act, CCPA, Massachusetts Data Breach Notification Law, DSGVO	Nein
Kaiser	**7.60**	13,400,000	$2,398,600,000	Website-Suchbegriffe, Gesundheits-informationen	HIPAA, HITECH Act, California CMIA, FTC Act, DSGVO (wenn EU-Bürger betroffen sind)	Nein
MediSecure	**7.56**	13,000,000	$2,327,000,000	Persönliche und Gesundheitsdaten	Australisches Datenschutzgesetz, Healthcare Identifiers Act, landesspezifische Gesundheitsdaten-Regulierungen	Ja, unbekannte Menge
USPS	**7.31**	62,000,000	$11,098,000,000	Postanschriften, Tracking-Daten	CCPA, FTC Act, verschiedene staatliche Datenschutzgesetze, DSGVO (falls zutreffend)	Nein
Evolve Bank	**6.83**	7,600,000	$1,360,400,000	Persönliche Informationen	CCPA, GLBA (Gramm-Leach-Bliley Act), FTC Safeguards Rule, staatliche Datenschutzgesetze für Finanzdaten	Ja, unbekannte Menge
Cencora	**6.23**	1,000,000	$179,000,000	Gesundheitsdaten	HIPAA, FDA-Vorschriften, landesspezifische Datenschutzgesetze im Gesundheitswesen (z.B. Kalifornien CMIA, Texas Medical Records Privacy Act)	Nein
Infosys McCamish Systems	**6.23**	6,078,263	$1,074,000,000	Sozialversicherungs-nummern, medizinische Informationen, Finanzdaten	CCPA, GLBA, FTC Act, staatliche Datenschutzgesetze für Versicherungen, HIPAA (falls zutreffend)	Ja, unbekannte Menge

Tabelle 1: Details zu Datenschutzverstößen.

Kosten von Datenpannen

TDie zunehmende Häufigkeit und Schwere von Datenschutzverstößen unterstreicht die dringende Notwendigkeit für Unternehmen, fortschrittliche Cybersicherheitsmaßnahmen zu ergreifen. Der IBM-Bericht über die Kosten eines Datenschutzverstoßes 2024 enthüllt, dass die globalen Durchschnittskosten eines Datenschutzverstoßes im vergangenen Jahr um 10 % gestiegen sind und nun 4,88 Millionen Dollar betragen.[5]

Die finanziellen Auswirkungen von Datenschutzverstößen auf Unternehmen gehen über die unmittelbaren Kosten hinaus, die mit der Erkennung, Eskalation und Benachrichtigung verbunden sind. Es gibt erhebliche direkte Kosten,

wie regulatorische Bußgelder, rechtliche Vergleiche, forensische Untersuchungen und die Benachrichtigung von Kunden. Organisationen, die Datenschutzvorschriften wie die Datenschutz-Grundverordnung (DSGVO) oder den Health Insurance Portability and Accountability Act (HIPAA) nicht einhalten, können erhebliche Bußgelder erhalten. Zum Beispiel belief sich die Gesamtsumme der DSGVO-Bußgelder am 1. März 2024 auf etwa 4,48 Milliarden Euro (4,96 Milliarden USD), ein Anstieg von 1,71 Milliarden Euro gegenüber dem Vorjahr.[6] Gleichzeitig stiegen die durchschnittlichen Kosten eines DSGVO-Verstoßes von etwa 500.000 Euro im Jahr 2019 auf 4,4 Millionen Euro (4,4 Millionen USD) im Jahr 2023.

Zusätzlich zu diesen globalen oder nationalen Vorschriften fügen regionale oder staatliche Datenschutzvorschriften wie der California Consumer Protection Act (CCPA) eine größere Komplexität und Herausforderungen für Unternehmen mit Geschäftstätigkeiten in diesen Standorten hinzu.

Risikofaktoren bei Datenpannen

Volumen und Art der offengelegten Daten

Die Risikofaktoren, die mit Datenschutzverstößen verbunden sind, werden erheblich durch das Volumen und die Art der exponierten Daten beeinflusst. In der ersten Hälfte des Jahres 2024 variierten die Verstöße stark hinsichtlich der Arten der kompromittierten Datensätze. Persönliche Daten sind definitiv ein Hauptziel, wobei Verizon berichtet, dass fast 60% der Datenschutzverstöße personenbezogene Daten (personenbezogene Informationen, PII) betrafen, einschließlich Namen, Adressen, Sozialversicherungsnummern und finanzieller Informationen wie Kreditkartendetails.[7] Gesundheitsakten, einschließlich sensibler Patienteninformationen, waren ebenfalls stark im Visier, insbesondere bei Verstößen, die Gesundheitsorganisationen betrafen, wo die Offenlegung von geschützten Gesundheitsinformationen (PHI) aufgrund von regulatorischen Anforderungen wie HIPAA ein weiteres Risiko darstellte.

Anzahl der Opfer

Das Ausmaß der Auswirkungen eines Datenschutzverstoßes wird oft durch die Anzahl der betroffenen Personen und Einrichtungen bestimmt. In der ersten Hälfte des Jahres 2024 waren mehrere Verstöße zu verzeichnen, die Millionen von Personen in verschiedenen Sektoren betrafen. So hatten beispielsweise Verstöße im Telekommunikations- und Gesundheitssektor weitreichende Folgen und betrafen Zehnmillionen von Kunden und Patienten.

Sensibilität der offengelegten Daten

Das Sensibilitätsniveau der exponierten Daten ist ein kritischer Faktor bei der Bestimmung der Schwere und Auswirkung eines Datenschutzverstoßes. Daten mit hoher Sensibilität, wie Sozialversicherungsnummern, Gesundheitsakten und Finanzinformationen, bergen ein größeres Risiko als Daten mit geringer Sensibilität wie E-Mail-Adressen oder allgemeine Geschäftsinformationen. Verstöße, die Daten mit hoher Sensibilität betreffen, führen wahrscheinlicher zu schwerwiegenden Konsequenzen, wie Identitätsdiebstahl, Finanzbetrug und anderen bösartigen Aktivitäten. In Fällen, in denen sensible Finanzinformationen oder Gesundheitsakten betroffen sind, ist aufgrund der strengen Anforderungen an den Datenschutz für diese Arten von Daten sowohl die resultierende regulatorische Maßnahme als auch die höheren Behebungskosten deutlich größer.

Methoden des Datenlecks

Methoden, die bei Datenschutzverstößen verwendet werden, haben sich weiterentwickelt und spiegeln die zunehmende Raffinesse der Taktiken von Cyberkriminellen wider. Zu den gängigen Methoden gehören Ransomware-

Angriffe, Phishing-Kampagnen, Insider-Bedrohungen und das Ausnutzen von Schwachstellen in Diensten oder Software von Drittanbietern. Ransomware bleibt ein vorherrschender Angriffsvektor, bei dem Angreifer Daten verschlüsseln und ein Lösegeld für deren Freigabe fordern, was oft zu erheblichen betrieblichen Unterbrechungen und finanziellen Verlusten führt.

Phishing-Angriffe sind ebenfalls weiterhin eine führende Ursache für Verstöße und nutzen Techniken des Social Engineering, um Mitarbeiter dazu zu verleiten, sensible Informationen preiszugeben oder unbefugten Zugriff zu gewähren. Das Ausnutzen von Schwachstellen in Diensten von Drittanbietern oder Angriffe auf die Lieferkette ist ein wachsender Trend. Insbesondere können Verstöße, die von Schwachstellen bei Drittanbietern ausgehen, weitreichende Auswirkungen haben, da sie oft mehrere Organisationen betreffen und ganze Netzwerke von Geschäftspartnern und Kunden beeinflussen. Dieser Trend unterstreicht die Notwendigkeit robuster Praktiken für das Risikomanagement von Drittanbietern und regelmäßiger Schwachstellenbewertungen.

Entwicklung des Risikoexpositionsindex

Einführung des Risikoexpositionsindex

Der Risikoexpositionsindex ist ein strategisches Werkzeug, das entwickelt wurde, um Datenpannen basierend auf ihrer Schwere und potenziellen Auswirkung zu bewerten und zu priorisieren. In einer Ära, in der Datenpannen zunehmend häufiger und komplexer werden, stehen Unternehmen vor erheblichen Herausforderungen bei der Bewertung des Risikos, das jede Panne für ihre Operationen, ihren Ruf und die Einhaltung von Vorschriften darstellt. Der Risikoexpositionsindex zielt darauf ab, einen standardisierten Rahmen für die Quantifizierung und den Vergleich der Risiken, die mit verschiedenen Datenpannen verbunden sind, bereitzustellen. Durch die Nutzung dieses Index können Organisationen ihre Cybersicherheitsmaßnahmen priorisieren, Ressourcen effektiver zuweisen und ihre gesamte Sicherheitslage verbessern, indem sie sich auf die kritischsten Bedrohungen konzentrieren.

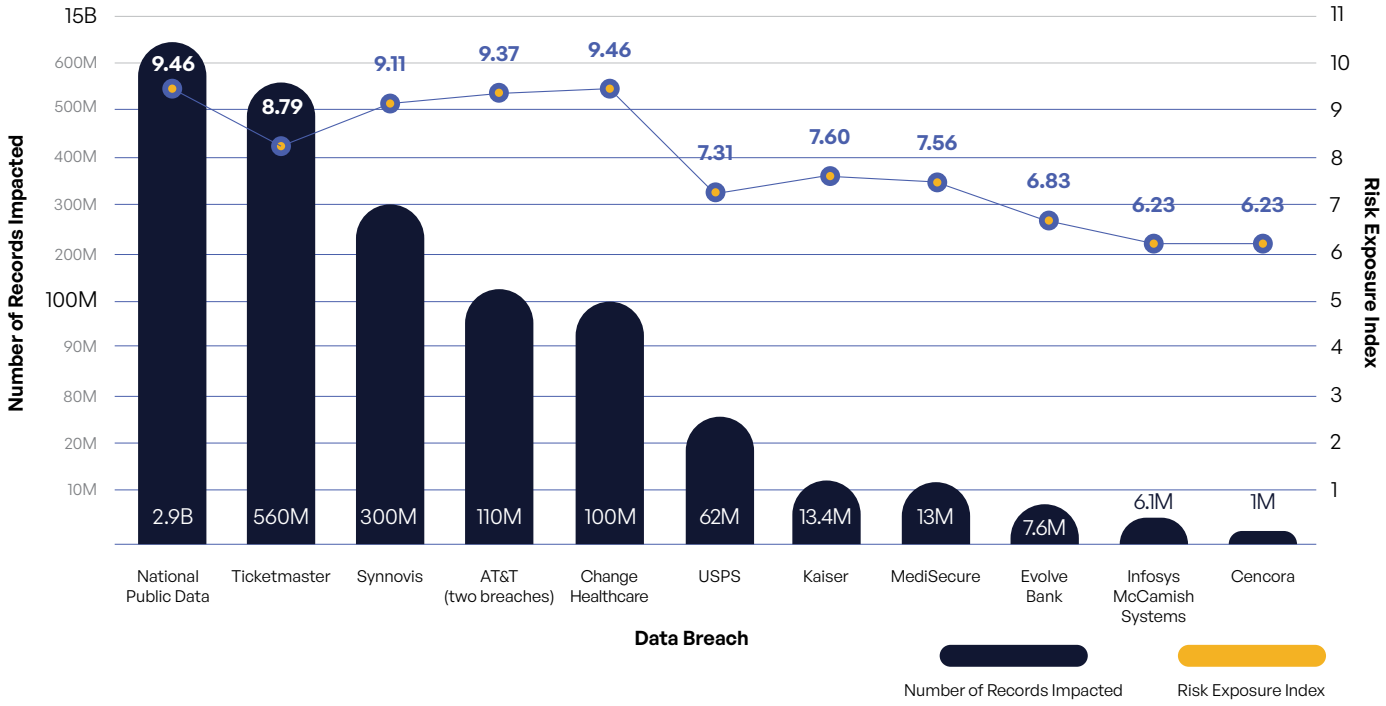

Abbildung 1: Anzahl der durch Datenschutzverstoß betroffenen Datensätze.

Wie der Risikoexpositionsindex funktioniert

Der Risikoexpositionsindex geht über traditionelle Kennzahlen wie die Anzahl der offengelegten Datensätze oder die entstandenen finanziellen Kosten hinaus. Stattdessen berücksichtigt er eine Reihe von Faktoren, um ein nuancierteres Verständnis der Schwere eines Datenschutzvorfalls zu bieten. Diese Faktoren können den Typ der kompromittierten Daten, das Ausmaß der Exposition, das Potenzial für regulatorische Strafen und die langfristigen Auswirkungen auf den Markenruf umfassen. Indem diese Elemente zu einer einzigen, umfassenden Punktzahl aggregiert werden, ermöglicht der Index Organisationen, die Schwere jedes Vorfalls objektiv zu bewerten und fundierte Entscheidungen darüber zu treffen, wo sie ihre Minderungsanstrengungen konzentrieren sollten.

Methodik des Risikoexpositionsindex

Die Methodik zur Berechnung des Risikoexpositionsindex umfasst mehrere Kriterien, die jeweils zur Gesamtrisikobewertung eines Verstoßes beitragen. Diese Kriterien wurden sorgfältig ausgewählt, um einen ganzheitlichen Blick auf die mit einem Verstoß verbundenen Risiken zu bieten und umfassen Folgendes:

1. **Anzahl der offengelegten Datensätze:** Dieses Kriterium bewertet das Volumen der Daten, die während eines Verstoßes kompromittiert wurden. Je größer die Anzahl der offengelegten Datensätze, desto höher die Risikobewertung, da größere Verstöße in der Regel schwerwiegendere Folgen haben, einschließlich eines erhöhten Potenzials für Identitätsdiebstahl, Betrug und Reputationsschäden.

2. **Geschätzte finanzielle Auswirkungen:** Dieses Kriterium bewertet die potenziellen finanziellen Verluste, die durch einen Verstoß entstehen, einschließlich direkter Kosten wie Bußgelder, Anwaltskosten und Sanierungsaufwendungen sowie indirekter Kosten wie Geschäftsverluste und Reputationsschäden. Verstöße mit höheren geschätzten finanziellen Auswirkungen erhalten eine höhere Punktzahl, was die erhebliche wirtschaftliche Belastung widerspiegelt, die sie für Organisationen darstellen.

3. **Ransomware-Beteiligung:** Angesichts der zunehmenden Bedrohung durch Ransomware-Angriffe berücksichtigt dieses Kriterium speziell Verstöße, die Ransomware involvieren. Ransomware-Angriffe sind besonders störend, verursachen oft erhebliche Betriebsausfälle und erfordern umfangreiche Wiederherstellungsbemühungen. Verstöße, die Ransomware beinhalten, erhalten aufgrund der Komplexität und Schwere der erforderlichen Reaktion eine höhere Bewertung.

4. **Datensensibilität:** Die Sensibilität der Daten, die bei einem Verstoß offengelegt werden, ist ein entscheidender Faktor bei der Bestimmung ihres Risikolevels. Verstöße, die hochsensible Daten betreffen, wie geschützte Gesundheitsinformationen (PHI) oder Finanzunterlagen, erhalten höhere Bewertungen. Dies spiegelt das erhöhte Risiko von regulatorischen Strafen, rechtlichen Maßnahmen und die Notwendigkeit umfassender Sanierungsbemühungen wider, um betroffene Personen zu schützen.

5. **Schwere des Verstoßes:** Dieses Kriterium berücksichtigt die Gesamtauswirkungen des Verstoßes auf die betroffene Organisation, einschließlich Betriebsunterbrechungen, Kundenvertrauen und langfristigen Reputationsschäden. Die Schwere wird basierend auf dem Umfang des Verstoßes, den beteiligten Daten und der Wirksamkeit der Reaktion der Organisation bewertet. Schwerwiegendere Verstöße erhalten höhere Punktzahlen, um ihre breiteren Auswirkungen widerzuspiegeln.

6. **Anzahl der betroffenen Vorschriften:** Dieses Kriterium bewertet die regulatorische Landschaft, die durch den Verstoß beeinflusst wird. Verstöße, die mehrere Vorschriften wie die DSGVO, HIPAA oder CCPA verletzen, erhalten höhere Punktzahlen. Dies spiegelt die Komplexität des Managements der Compliance über verschiedene Rechtsgebiete hinweg und das Potenzial für mehrere Bußgelder und rechtliche Schritte wider.

Normalisierungsprozess und Punkteanpassung

Um sicherzustellen, dass der Risikoexpositionsindex eine faire und konsistente Messung der Schwere von Datenschutzverstößen bietet, wird ein **Normalisierungsprozess** angewendet, um die Punktzahlen auf eine standardisierte Skala von 1-10 anzupassen. Dieser Prozess umfasst mehrere Schritte:

1. **Datenerfassung und Erstbewertung:** Jeder Datenschutzverstoß wird anhand der oben genannten sechs Kriterien bewertet, und jedem Kriterium wird basierend auf vordefinierten Bereichen eine Anfangspunktzahl zugewiesen. Beispielsweise können Verstöße, die mehr als 10 Millionen Datensätze offenlegen, die Höchstpunktzahl für das Kriterium „Anzahl der offengelegten Datensätze“ erhalten.
2. **Weight Assignment:** Each criterion is assigned a weight based on its relative importance in determining the overall risk level. For instance, “Data Sensitivity” and “Estimated Financial Impact” may be weighted more heavily than “Number of Records Exposed” to reflect their critical impact on the organization’s security posture and compliance requirements.
3. **Gewichtungszuweisung:** Jedes Kriterium wird basierend auf seiner relativen Bedeutung bei der Bestimmung des gesamten Risikoniveaus gewichtet. Beispielsweise können „Datensensibilität“ und „Geschätzte finanzielle Auswirkungen“ stärker gewichtet werden als „Anzahl der offengelegten Datensätze“, um deren kritischen Einfluss auf die Sicherheitslage und die Compliance-Anforderungen der Organisation widerzuspiegeln.
4. **Punkteaggregation:** Die gewichteten Punkte für jedes Kriterium werden aggregiert, um eine Gesamtrisikopunktzahl für jeden Datenschutzverstoß zu berechnen. Diese Gesamtpunktzahl repräsentiert die Gesamtschwere des Verstoßes basierend auf der Kombination aller Risikofaktoren.
5. **Endgültige Bewertung der Zuweisung:** Die normalisierten Bewertungen werden überprüft und validiert, um Genauigkeit und Konsistenz zu gewährleisten. Jeder Verstoß wird dann einem endgültigen Risikoexpositionsindex auf der Skala von 1-10 zugewiesen, wobei höhere Werte schwerwiegendere Verstöße anzeigen, die sofortige Aufmerksamkeit und Maßnahmen erfordern.

Durch die Anwendung dieser strengen Methodik bietet der Risikoexpositionsindex einen zuverlässigen und umsetzbaren Rahmen zur Bewertung und Verwaltung von Risiken bei Datenschutzverletzungen. Dies ermöglicht Organisationen, ihre Cybersicherheitsstrategien zu verbessern und ihre sensiblen Daten besser vor sich entwickelnden Bedrohungen zu schützen.

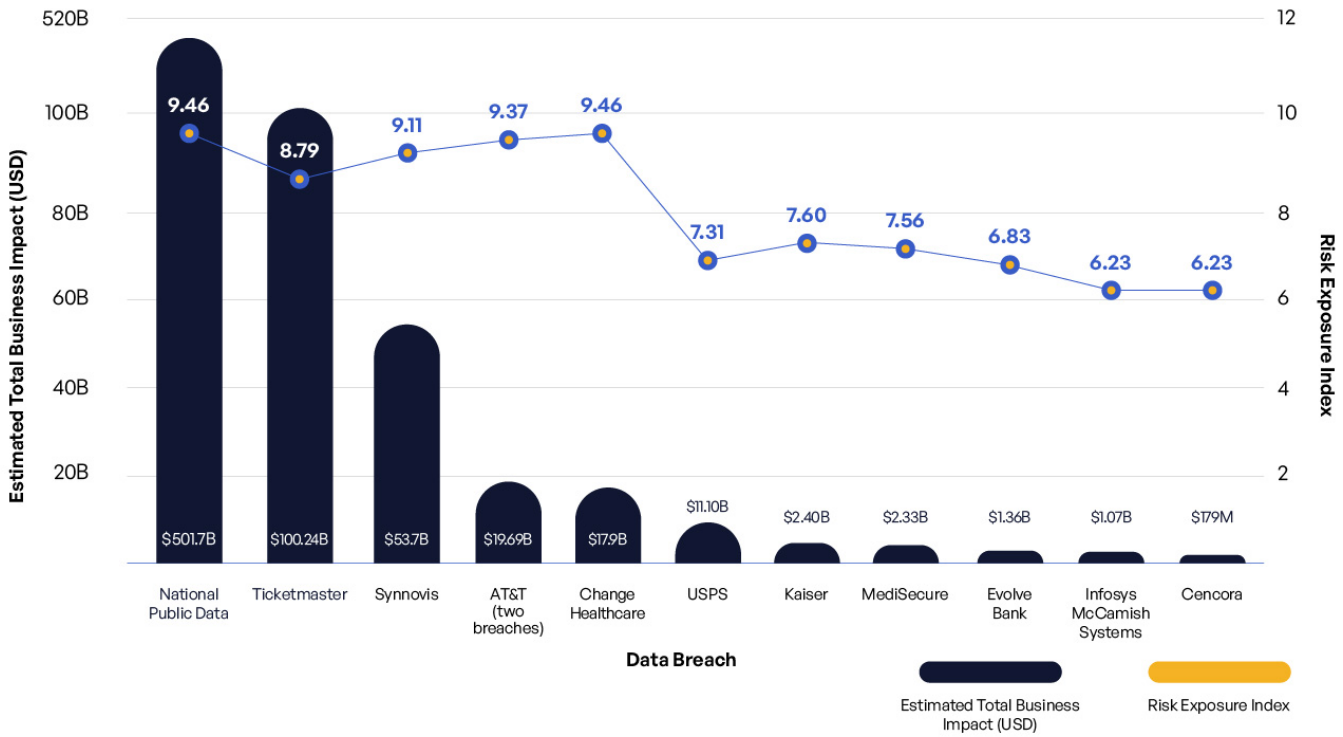

Abbildung 2: Geschätzte gesamtwirtschaftliche Auswirkungen durch Datenpannen.

Analyse der Top 11 Datenschutzverstöße basierend auf dem Risikoexpositionsindex

Im Folgenden finden Sie die korrigierte Rangliste der Top 11 Datenpannen in der ersten Hälfte des Jahres 2024, basierend auf ihrem Risikoexpositionsindex.

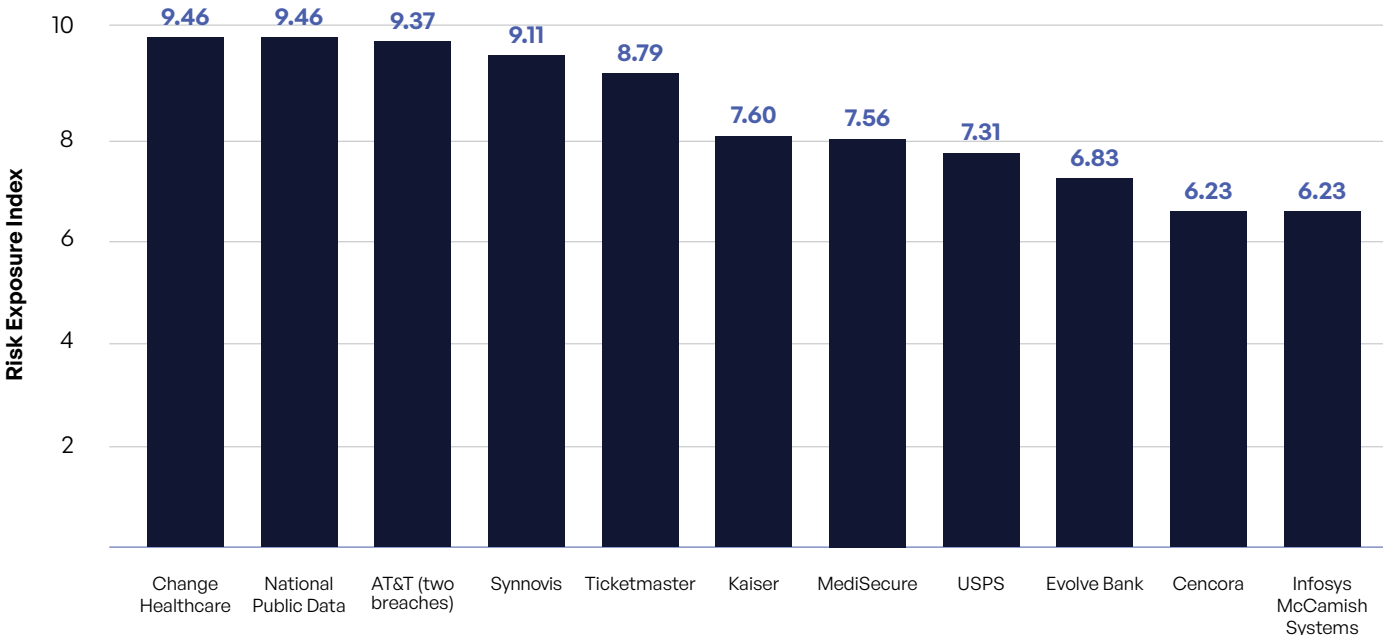

Abbildung 3: Risikoexpositionswert der Top 11 1H 2024 Data Breaches.

1. Change Healthcare (Risikoexposition: 9.46)

Beschreibung des Vorfalls: Change Healthcare erlebte einen Ransomware-Angriff, der zum Diebstahl sensibler Gesundheitsdaten führte, einschließlich persönlicher, medizinischer und Abrechnungsinformationen, die 100 Millionen Datensätze betrafen.

Auswirkungsanalyse: Der Bruch hatte erhebliche finanzielle Auswirkungen, mit Kosten, die mit Lösegeldzahlungen, Systemwiederherstellung und Rechtsgebühren verbunden waren. Die betrieblichen Störungen waren erheblich und beeinträchtigten die Patientenversorgung in verschiedenen Gesundheitseinrichtungen. Der Reputationsschaden war umfangreich und führte zu einem Vertrauensverlust unter Patienten und Partnern.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze:

100.000.000

Geschätzte finanzielle Auswirkungen: 17.900.000.000 $

Datensensibilität (1-5): 5

Finanzielle Auswirkungen (1-5): 4

Regulatorische Compliance (1-5): 5

2. National Public Data (Risikoexposition: 9.46)

Beschreibung des Vorfalls: Der Vorfall ereignete sich am 23. Dezember 2023. National Public Data, ein Datenmakler, der auf Hintergrundüberprüfungen und Betrugspräventionsdienste spezialisiert ist, gab an, dass 2,9 Billionen Datensätze von 1,3 Millionen Personen betroffen waren.

Auswirkungsanalyse: Zu den durch den Vorfall offengelegten Informationen gehörten Sozialversicherungsnummern, Namen, E-Mail-Adressen, Telefonnummern und Postadressen.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze:

2.900.000.000

Geschätzte finanzielle Auswirkungen: 501.700.000.000 $

Datensensibilität (1-5): 5

Finanzielle Auswirkungen (1-5): 5

Regulatorische Compliance (1-5): 4

3. AT&T (Risikoexposition: 9.37)

Beschreibung des Vorfalls: Dieser Vorfall betraf den Diebstahl von 110 Millionen Kundendatensätzen, einschließlich Telefonnummern, Anrufprotokollen und persönlichen Informationen, aufgrund von unbefugtem Zugriff.

Auswirkungsanalyse: Bedeutende finanzielle Kosten entstanden durch regulatorische Strafen und die Ausgaben für die Benachrichtigung der Kunden. Der Vorfall hatte betriebliche Auswirkungen, einschließlich Dienstunterbrechungen und verstärkter Überprüfung der Datenverarbeitungspraktiken von AT&T. Der Reputationsschaden führte zu einem Rückgang des Kundenvertrauens und einer erhöhten Abwanderungsrate.

Beim zweiten Datendiebstahl bei AT&T, obwohl die genaue Anzahl der Datensätze nicht explizit angegeben ist, ist es vernünftig zu schätzen, dass die Gesamtzahl der kompromittierten Datensätze über beide Diebstähle hinweg deutlich höher als 110 Millionen ist, möglicherweise im Milliardenbereich, angesichts der Natur von Anruf- und Textaufzeichnungen über einen Zeitraum von sechs Monaten für eine so große Kundenbasis.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze:

110,000,000

Geschätzte finanzielle Auswirkungen: $19,690,000,000

Datensensibilität (1-5): 3

Finanzielle Auswirkungen (1-5): 5

Regulatorische Compliance (1-5): 5

4. Synnovis (Risikoexposition: 9.11)

Beschreibung des Vorfalls: Synnovis, ein britisches Pathologielabor, wurde Ziel eines Ransomware-Angriffs, bei dem Daten zu 300 Millionen Patienteninteraktionen kompromittiert und medizinische Dienstleistungen gestört wurden.

Auswirkungsanalyse: Zu den finanziellen Auswirkungen gehörten Kosten für die Wiederherstellung des Dienstes und potenzielle regulatorische Strafen. Der operative Einfluss war erheblich, da viele medizinische Eingriffe verschoben wurden, was zu einem kritischen Vorfall im Gesundheitssektor führte. Der Reputationsschaden beeinträchtigte das Vertrauen innerhalb der Gesundheitsgemeinschaft.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze:

300.000.000

Geschätzte finanzielle Auswirkungen: 53.700.000.000 $

Datensensibilität (1-5): 1

Finanzielle Auswirkungen (1-5): 5

Regulatorische Compliance (1-5): 4

5. Ticketmaster (Risikoexposition: 8.79)

Beschreibung des Vorfalls: Der Vorfall bei Snowflake, der Ticketmaster betraf, legte 560 Millionen Kundenakten offen, einschließlich vollständiger Namen, Adressen, E-Mail-Adressen, Telefonnummern und Zahlungskartendaten.

Auswirkungsanalyse: Zu den finanziellen Auswirkungen gehörten Kosten für die Behebung und potenzielle Rechtsstreitigkeiten. Betriebliche Auswirkungen umfassten Störungen der Kundendienste und verstärktes Sicherheitsmonitoring. Reputationsschäden betrafen Snowflake und seine Kunden und warfen Bedenken hinsichtlich der Cloud-Sicherheit auf.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze: 560,000,000

Geschätzte finanzielle Auswirkungen: $100,240,000,000

Datensensibilität (1-5): 2

Finanzielle Auswirkungen (1-5): 5

Regulatorische Compliance (1-5): 5

6. Kaiser (Risikoexposition: 7.60)

Beschreibung des Vorfalls: Kaiser teilte versehentlich vertrauliche Gesundheitsinformationen von 13,4 Millionen Patientenakten mit Werbetreibenden aufgrund von Tracking-Codes, die auf seiner Website verwendet wurden.

Auswirkungsanalyse: Zu den finanziellen Auswirkungen gehörten regulatorische Bußgelder und rechtliche Einigungen. Die betrieblichen Auswirkungen umfassten die Überarbeitung der Daten-Governance und der Datenschutzpraktiken. Der Vorfall verursachte erheblichen Reputationsschaden und löste Bedenken hinsichtlich des Datenschutzes aus.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze:

13.400.000

Geschätzte finanzielle Auswirkungen: 2.398.600.000 $

Datensensibilität (1-5): 5

Finanzielle Auswirkungen (1-5): 4

Regulatorische Compliance (1-5): 5

7. MediSecure (Risikoexposition: 7.56)

Beschreibung des Vorfalls: MediSecure, ein australischer Anbieter von Rezepten, erlitt einen Ransomware-Angriff, bei dem die persönlichen und gesundheitlichen Daten von fast 13 Millionen Australiern kompromittiert wurden.

Auswirkungsanalyse: Zu den finanziellen Kosten gehörten Lösegeldzahlungen und Rechtskosten. Die betrieblichen Auswirkungen waren erheblich, störten die Gesundheitsdienste und führten zur Insolvenz. Reputationsschäden untergruben das Vertrauen von Kunden und Partnern.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze:

13,000,000

Geschätzte finanzielle Auswirkungen: $2,327,000,000

Datensensibilität (1-5): 5

Finanzielle Auswirkungen (1-5): 4

Regulatorische Compliance (1-5): 3

8. USPS (Risikoexposition: 7.31)

Beschreibung des Vorfalls: USPS teilte postalische Adressen von eingeloggten Nutzern mit Werbetreibenden wie Meta, LinkedIn und Snap durch Tracking-Codes.

Auswirkungsanalyse: Der Vorfall führte zu finanziellen Kosten durch Bußgelder und Vergleiche. Betriebliche Auswirkungen umfassten Änderungen der Daten-Governance-Praktiken. Reputationsschäden führten zu verstärkter Überprüfung und Bedenken hinsichtlich der Datenschutzpraktiken.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze:

62.000.000

Geschätzte finanzielle Auswirkungen: 11.098.000.000 $

Datensensibilität (1-5): 1

Finanzielle Auswirkungen (1-5): 4

Regulatorische Compliance (1-5): 5

9. Evolve Bank (Risikoexposition: 6.83)

Beschreibung des Vorfalls: Evolve Bank, ein Anbieter von Banking-as-a-Service, erlebte einen Ransomware-Angriff, bei dem die persönlichen Informationen von über 7,6 Millionen Menschen kompromittiert wurden.

Auswirkungsanalyse: Finanzielle Auswirkungen umfassten Lösegeldzahlungen und regulatorische Strafen. Betriebliche Störungen waren erheblich, beeinträchtigten den Kundenservice und führten zu verstärkten Sicherheitsmaßnahmen. Der Reputationsschaden war bedeutend und beeinträchtigte das Kundenvertrauen.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze:

7,600,000

Geschätzte finanzielle Auswirkungen: $1,360,400,000

Datensensibilität (1-5): 3

Finanzielle Auswirkungen (1-5): 3

Regulatorische Compliance (1-5): 3

10. Infosys McCamish Systems (Risikoexposition: 6.23)

Beschreibung des Vorfalls: Der Vorfall führte zur Offenlegung von Sozialversicherungsnummern, medizinischen Informationen und Finanzdaten und betraf 6.1 Millionen Datensätze.

Auswirkungsanalyse: Finanzielle Auswirkungen umfassten regulatorische Bußgelder und Kosten, die mit der Benachrichtigung über Datenschutzverstöße verbunden waren. Betriebliche Auswirkungen betrafen verbesserte Sicherheitsmaßnahmen und bessere Praktiken zum Datenschutz. Reputationsverluste beeinträchtigten das Kundenvertrauen und die Beziehungen zu Partnern.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze: 6,078,263

Geschätzte finanzielle Auswirkungen: $1,074,000,000

Datensensibilität (1-5): 5

Finanzielle Auswirkungen (1-5): 2

Regulatorische Compliance (1-5): 5

11. Cencora (Risikoexposition: 6.23)

Beschreibung des Vorfalls: Der Datenschutzverstoß führte zur Offenlegung sensibler Gesundheitsdaten, einschließlich Patientenakten und anderer vertraulicher medizinischer Daten, und betraf etwa 1 Million Datensätze. Dieser Angriff auf die Lieferkette betraf Datensätze von mindestens 27 Pharma- und Biotechnologieunternehmen.

Auswirkungsanalyse: Finanzielle Auswirkungen umfassten regulatorische Bußgelder und Kosten, die mit der Benachrichtigung über Datenschutzverstöße verbunden waren. Betriebliche Auswirkungen betrafen verbesserte Sicherheitsmaßnahmen und bessere Praktiken zum Datenschutz. Reputationsverluste beeinträchtigten das Kundenvertrauen und die Beziehungen zu Partnern.

Risikoexposition-sübersicht:

Aufgedeckte Datensätze:

1.000.000

Geschätzte finanzielle Auswirkungen: 179.000.000 $

Datensensibilität (1-5): 5

Finanzielle Auswirkungen (1-5): 2

Regulatorische Compliance (1-5): 5

Mit dem Risikoexpositionsindex

Unser Risikoexpositionsindex berücksichtigt mehr als nur die Anzahl der offengelegten Datensätze oder die Anzahl der betroffenen Opfer. Dieser umfassende Ansatz bietet ein klareres Verständnis der wahren Schwere und des potenziellen Einflusses jedes Datenverstoßes. Während eine größere Anzahl von offengelegten Datensätzen auf einen bedeutenden Verstoß hindeuten kann, bedeutet dies nicht notwendigerweise, dass die Risikoexposition höher ist. Mehrere Faktoren tragen zur Risikobewertung eines Verstoßes bei, was manchmal dazu führen kann, dass ein Verstoß mit weniger Datensätzen eine höhere Risikobewertung erhält als einer mit mehr Datensätzen.

1. Natur und Sensibilität der betroffenen Daten

Die Art der kompromittierten Daten ist ein kritischer Faktor, der den Risikoexpositionsindex beeinflusst. Zum Beispiel hatte der Vorfall bei Change Healthcare, der 100 Millionen Datensätze betraf, hauptsächlich persönliche, medizinische und Abrechnungsinformationen zur Folge. Diese Art von Daten ist hochsensibel,

was zu schwerwiegenden Folgen führt, wie dem unwiederbringlichen Verlust von Gesundheitsdaten, was das Risikoexpositionslevel erhöht, trotz einer kleineren Anzahl von Datensätzen im Vergleich zu anderen Vorfällen. Ähnlich erzielte der Vorfall bei Cencora, mit nur 1 Million offengelegten Datensätzen, ebenfalls eine hohe Bewertung auf der Risikoskala aufgrund der Sensibilität der betroffenen Gesundheitsdaten, was zeigt, dass die Art der Daten oft entscheidender ist als das Volumen der Daten.

2. Regulatorische und Compliance-Implikationen

Regulatorische Auswirkungen können das Gesamtrisiko eines Datenschutzvorfalls erheblich beeinflussen. Zum Beispiel hatte der Vorfall bei AT&T, der 110 Millionen Datensätze betraf, ein erhebliches Risiko nicht nur aufgrund der Anzahl der Datensätze, sondern auch wegen der potenziellen Verstöße gegen mehrere Vorschriften, einschließlich der FCC-Vorschriften, des FTC Act und des CCPA. Diese regulatorischen Verstöße können zu erheblichen Bußgeldern und Strafen führen, was das Gesamtrisiko des Vorfalls erhöht. Im Gegensatz dazu könnte ein Vorfall, der eine größere Anzahl von Datensätzen betrifft, wie bei Ticketmaster mit 560 Millionen Datensätzen, ein geringeres Risiko darstellen, wenn die kompromittierten Daten nicht so schwerwiegende regulatorische Konsequenzen nach sich ziehen.

3. Potenzielle Auswirkungen über unmittelbare Verluste hinaus

Die langfristigen Konsequenzen eines Datenschutzverstoßes, wie Identitätsdiebstahl, finanzieller Betrug oder Reputationsschaden, werden ebenfalls im Risikoexpositionsindex berücksichtigt. Der Synnovis-Vorfall, bei dem 300 Millionen Datensätze von Patienteninteraktionen betroffen waren, ist ein Beispiel, bei dem die langanhaltende Auswirkung auf Patientendienste und das Vertrauen zu einem hohen Risikowert führte. Obwohl die Anzahl der Datensätze geringer war als beim Ticketmaster-Vorfall, erhöhte das Potenzial für anhaltenden Schaden an Patienten und Gesundheitsdiensten das Risikoexpositionsmaß erheblich. Dieses Beispiel zeigt, dass der Index die breiteren Implikationen eines Verstoßes über den unmittelbaren Datenverlust hinaus berücksichtigt.

4. Ransomware und Erpressungsfaktoren

Die Präsenz von Lösegeldforderungen durch Ransomware kann ebenfalls das Risikoscore eines Vorfalls erhöhen, unabhängig von der Anzahl der betroffenen Datensätze. Der Vorfall bei Synnovis beispielsweise sah sich mit einer Lösegeldforderung von 50 Millionen Dollar konfrontiert, was zu seinem hohen Risikoscore beitrug. Selbst mit weniger betroffenen Datensätzen als beim Ticketmaster-Vorfall erhöhen die zusätzlichen Kosten und Risiken, die mit Lösegeldforderungen verbunden sind, einschließlich potenzieller doppelter Erpressung und Wiederherstellungskosten, das gesamte Risiko des Vorfalls.

5. Die Auswirkungen von Datensensibilität und das Potenzial für Identitätsdiebstahl

Die Auswirkungen von Datensensibilität werden bei Datenschutzverstößen deutlich, wie sie Unternehmen wie Change Healthcare und Synnovis erfahren mussten, bei denen es um hochsensible medizinische und persönliche Informationen ging. Das Potenzial für Missbrauch, wie Identitätsdiebstahl und Finanzbetrug, trägt erheblich zum höheren Risiko dieser Datenschutzverstöße bei, selbst im Vergleich zu Vorfällen, die eine größere Menge weniger sensibler Daten betreffen, wie den, den Ticketmaster erlebte.

Abschließende Gedanken

Unsere Analyse der elf größten Datenpannen in der ersten Hälfte des Jahres 2024 offenbart mehrere entscheidende Erkenntnisse über die sich wandelnde Landschaft der Cyberbedrohungen:

1. **Vielfältige Angriffsvektoren und zunehmende Raffinesse:** Cyberkriminelle setzen weiterhin eine Vielzahl von Angriffsmethoden ein, von Ransomware und unbefugtem Zugriff bis hin zu unbeabsichtigtem Datenaustausch, jede mit einzigartigen Auswirkungen auf Sicherheitsstrategien. Diese Vielfalt an Angriffsvektoren unterstreicht die Bedeutung für Organisationen, einen mehrschichtigen Sicherheitsansatz zu verfolgen, der eine breite Palette potenzieller Bedrohungen anspricht.
2. **Bedeutende Auswirkungen von Ransomware:** Ransomware-Angriffe, insbesondere solche, die auf hochwertige Sektoren wie das Gesundheitswesen und die Finanzbranche abzielen, haben sich als sowohl störend als auch kostspielig erwiesen. Verstöße wie die, die Change Healthcare und Synnovis betrafen, haben die schwerwiegenden operativen, finanziellen und reputationsbedingten Schäden gezeigt, die daraus resultieren können. Organisationen müssen robuste Ransomware-Abwehrmaßnahmen priorisieren, einschließlich fortschrittlicher Bedrohungserkennung, schneller Reaktionsfähigkeiten und umfassender Daten-Backup-Strategien.
3. **Hohe Sensibilität und Volumen exponierter Daten:** Datenschutzverletzungen, die große Mengen sensibler Informationen betreffen, insbesondere persönliche und finanzielle Daten, haben aufgrund ihres Potenzials für Identitätsdiebstahl, Finanzbetrug und regulatorische Strafen konsequent zu höheren Risikobewertungen geführt. Dies unterstreicht die Notwendigkeit verstärkter Datenschutzmaßnahmen, insbesondere für Organisationen wie National Public Data, die sensible Daten über mehrere Kommunikationstools und -plattformen hinweg verarbeiten.
4. **Drittparteien- und Lieferketten-Schwachstellen:** Mehrere Sicherheitsverletzungen, wie die bei AT&T und Ticketmaster, haben die Schwachstellen hervorgehoben, die mit Drittanbietern und Partnern in der Lieferkette verbunden sind. Dies unterstreicht die kritische Notwendigkeit einer kontinuierlichen Überwachung und robusten Verwaltung von Beziehungen zu Drittanbietern, um Risiken, die mit erweiterten Netzwerken verbunden sind, zu mindern.
5. **Regulatorische Compliance und rechtliche Konsequenzen:** Die Analyse zeigt, dass Datenpannen oft zu Verstößen gegen mehrere Vorschriften führen, was erhebliche Bußgelder und rechtliche Konsequenzen nach sich zieht. Unternehmen müssen ihre Compliance-Frameworks und Daten-Governance-Praktiken stärken, um regulatorische Verstöße und damit verbundene finanzielle Strafen zu vermeiden.
6. **Ganzheitliche Risikobewertung:** Die Ergebnisse des Berichts unterstreichen die Bedeutung der Berücksichtigung mehrerer Faktoren bei der Bewertung des Risikoexposures eines Datenschutzverstoßes. Es geht nicht allein um die Anzahl der betroffenen Datensätze oder die unmittelbaren finanziellen Kosten; das wahre Risiko wird oft durch eine Kombination von Elementen geformt, einschließlich der Sensibilität der kompromittierten Daten, des Potenzials für regulatorische Verstöße und der breiteren Implikationen für langfristigen Reputationsschaden.
7. **Kontextuelle Auswirkungen von Verstoßtyp und Datensensibilität:** Die Ergebnisse zeigen, dass die Art des Verstoßes und die Sensibilität der betroffenen Daten entscheidende Faktoren sind, die das gesamte Risikoexposure beeinflussen. Ein Verstoß, der eine kleine Anzahl hochsensibler Datensätze betrifft, wie zum Beispiel Sozialversicherungsnummern oder medizinische Unterlagen, kann schwerwiegendere Folgen haben als ein Verstoß, der eine große Menge weniger sensibler Daten umfasst. Dies zeigt, dass Organisationen den Kontext und Inhalt der verletzten Daten bewerten müssen, nicht nur die Menge, um die potenziellen Auswirkungen vollständig zu verstehen.

Umsetzbare Empfehlungen

1. **Verfolgen Sie gehärtete Sicherheitskonzepte:** Organisationen sollten ihre Cybersicherheitsrahmen mit gehärteten Sicherheitsmaßnahmen erweitern, die speziell darauf ausgerichtet sind, die Kommunikation sensibler Inhalte zu schützen. Dies umfasst die Bereitstellung fortschrittlicher Sicherheitsfunktionen wie Intrusion Detection und Prevention Systeme, sichere Kommunikationskanäle und kontinuierliches Bedrohungsmonitoring, um unbefugten Zugriff zu verhindern und potenzielle Sicherheitsverletzungen zu mindern.
2. **Implementieren Sie fortschrittliche Verschlüsselungstechniken:** Um die Privatsphäre und Sicherheit sensibler Daten zu gewährleisten, sollten Unternehmen fortschrittliche Verschlüsselungsmethoden für Daten im ruhenden Zustand, während der Übertragung und bei der Nutzung einsetzen. Die Verschlüsselung der Kommunikation sensibler Inhalte hilft, unbefugten Zugriff und Datenpannen zu verhindern, gewährleistet die Einhaltung gesetzlicher Vorgaben und schützt sensible Informationen.
3. **Implementierung von Next-Gen Digital Rights Management (DRM):** Unternehmen sollten robuste Strategien für das digitale Rechtemanagement implementieren, um den Zugriff auf sensible Inhalte zu kontrollieren und zu überwachen. Dies umfasst die Definition von Zugriffsrechten, die Nachverfolgung der Dokumentennutzung und die Anwendung von Kontrollen, um die unautorisierte Weitergabe oder den Missbrauch sensibler Informationen zu verhindern, wodurch das Risiko von Datenschutzverstößen reduziert und die Einhaltung von Datenschutzvorschriften sichergestellt wird.
4. **Verbessern Sie die Praktiken des Risikomanagements bei Drittanbietern:** Überwachen und bewerten Sie regelmäßig die Sicherheitspraktiken von Drittanbietern und Partnern, um Risiken, die mit erweiterten Netzwerken verbunden sind, zu minimieren. Dies umfasst die Durchsetzung strenger Sicherheitsanforderungen für Interaktionen mit Dritten und die Implementierung sicherer Kommunikationsprotokolle zum Schutz sensibler Daten, die mit externen Entitäten geteilt werden.
5. **Fokus auf Datensensibilität und Compliance:** Stärken Sie die Praktiken des Datenschutzes, indem Sie die Sicherheit von hochsensiblen Informationen durch Zugriffskontrollen, Verschlüsselung und umfassendes Monitoring priorisieren. Stellen Sie die Einhaltung von Datenschutzvorschriften sicher, indem Sie regelmäßig die Praktiken der Datenverarbeitung prüfen und robuste Governance-Rahmenwerke aufrechterhalten, um die Kommunikation sensibler Inhalte zu schützen.

Zukunftsausblick

Da Cyberbedrohungen in ihrer Komplexität und Reichweite weiter zunehmen, müssen Unternehmen wachsam und proaktiv in ihren Bemühungen um Cybersicherheit bleiben. Die wachsende Abhängigkeit von digitalen Plattformen und Dienstleistungen Dritter wird wahrscheinlich die Angriffsfläche vergrößern, was ein umfassendes Risikomanagement wichtiger denn je macht. Durch die Nutzung von Tools wie dem Risk Exposure Index und die Annahme einer zukunftsorientierten Herangehensweise an die Cybersicherheit können Organisationen sich besser gegen zukünftige Verstöße schützen und potenzielle Auswirkungen minimieren.

Anhang

Risikoexpositionsindex-Algorithmus

Bewertungskriterien

1. **Anzahl der freigegebenen Datensätze:**
   - Über 100,000,000: 6 punkte
   - 10,000,001-100,000,000: 5 punkte
   - 1,000,001-10,000,000: 4 punkte
   - 100,001-1,000,000: 3 punkte
   - 10,001-100,000: 2 punkte
   - 1-10,000: 1 punkt
2. **Geschätzte finanzielle Auswirkungen:**
   - Über $10,000,000,000: 6 punkte
   - $1,000,000,001-$10,000,000,000: 5 punkte
   - $100,000,001-$1,000,000,000: 4 punkte
   - $10,000,001-$100,000,000: 3 punkte
   - $1,000,001-$10,000,000: 2 punkte
   - $1-$1,000,000: 1 punkt
3. **Beteiligung an Ransomware:**
   - Ja: 1 punkt
   - Nein: 0 punkte
4. **Datensensibilität:**
   - **5 punkte (Äußerst sensible Daten):** Verstöße, die hochvertrauliche Informationen wie Sozialversicherungsnummern, medizinische Unterlagen, biometrische Daten oder streng vertrauliche Unternehmensdaten betreffen, die bei einer Offenlegung schweren Schaden oder irreparable Schäden verursachen könnten.
   - **4 punkte (Hochsensible Daten):** Verstöße, die sensiblere Informationen wie Finanzdaten (Kreditkartennummern, Bankkontodetails), Gesundheitsinformationen oder Daten, die zu Identitätsdiebstahl oder Betrug führen könnten, betreffen.
   - **3 punkte (Sensible Daten):** Verstöße, die personenbezogene Daten (PII) wie E-Mail-Adressen, Telefonnummern oder andere persönliche Details betreffen, die potenziell für Phishing oder Spam verwendet werden könnten.
   - **2 punkte (Mäßige Sensibilität):** Daten, die nicht-öffentliche, weniger sensible Informationen wie Namen, Adressen oder Kontaktinformationen enthalten, die leicht beschafft werden können, aber kein signifikantes Risiko darstellen, wenn sie offengelegt werden.
   - **1 punkt (Geringe Sensibilität):** Verstöße, die Daten betreffen, die nicht sensibel oder öffentlich zugänglich sind, wie generische oder anonymisierte Datensätze, die keine personenbezogenen Daten oder sensiblen persönlichen Daten enthalten.

5. **Schweregrad:**
   - **5 punkte (Kritische Auswirkungen):** Katastrophale Auswirkungen mit schwerwiegenden finanziellen Folgen, erheblichen Risiken für die öffentliche Gesundheit, weit verbreitetem Identitätsdiebstahl oder einem schweren Ansehensverlust, der zu einem dauerhaften Vertrauensverlust führt.
   - **4 punkte (Hohe Auswirkungen):** Erhebliche Konsequenzen, einschließlich umfangreichem Identitätsdiebstahl, Betrugsfällen, erheblichen finanziellen Verlusten oder regulatorischen Bußgeldern.
   - **3 punkte (Mäßige Auswirkungen):** Mäßiger Schaden, wie begrenzte finanzielle Verluste oder Reputationsschäden, einige Fälle von Identitätsdiebstahl oder mäßige regulatorische Prüfungen.
   - **2 punkte (Geringe Auswirkungen):** Geringfügige Störungen, minimaler finanzieller Einfluss oder begrenzte Exposition ohne nennenswerten Schaden für Einzelpersonen oder betriebliche Abläufe.
   - **1 punkt (Minimaler Einfluss):** Verstöße mit wenig bis gar keinen Auswirkungen auf das Unternehmen oder Einzelpersonen, möglicherweise aufgrund einer zeitnahen Eindämmung oder des Fehlens einer wertvollen Datenexposition.

6. **Anzahl der betroffenen vorschriften:**
   - 5 oder mehrere vorschriften: 5 punkte
   - 4 vorschriften: 4 punkte
   - 3 vorschriften: 3 punkte
   - 2 vorschriften: 2 punkte
   - 1 vorschriften: 1 punkt

Algorithmen-Details

1. Fassen Sie die Punkte aus allen sechs Kriterien zusammen.
2. Teilen Sie die Summe durch 2,8, um die Punktzahl auf eine Skala von 1-10 zu normalisieren.
3. Runden Sie das Ergebnis auf zwei Dezimalstellen ab.

Endpunktzahl = (Punkte für Aufzeichnungen + Punkte für finanzielle Auswirkungen + Ransomware-Punkt + Datensensibilität + Schweregrad + Punkte für Vorschriften)

2.8 *(HINWEIS: Maximale mögliche Rohpunktzahl: 28 Punkte; minimale mögliche Rohpunktzahl: 5 Punkte)*

1. "2023 Data Breach Report," Identity Theft Resource Center, January 2024.
2. "Cost of a Data Breach Report 2024," IBM, July 2024.
3. "2024 Data Breach Investigations Report," Verizon, April 2024.
4. "Privacy in Practice 2024," ISACA, January 2024.
5. "Cost of a Data Breach Report 2024," IBM, July 2024.
6. "Enforcement Tracker Database," CMS, accessed September 2, 2024.
7. "2024 Data Breach Investigations Report," Verizon, May 2024.