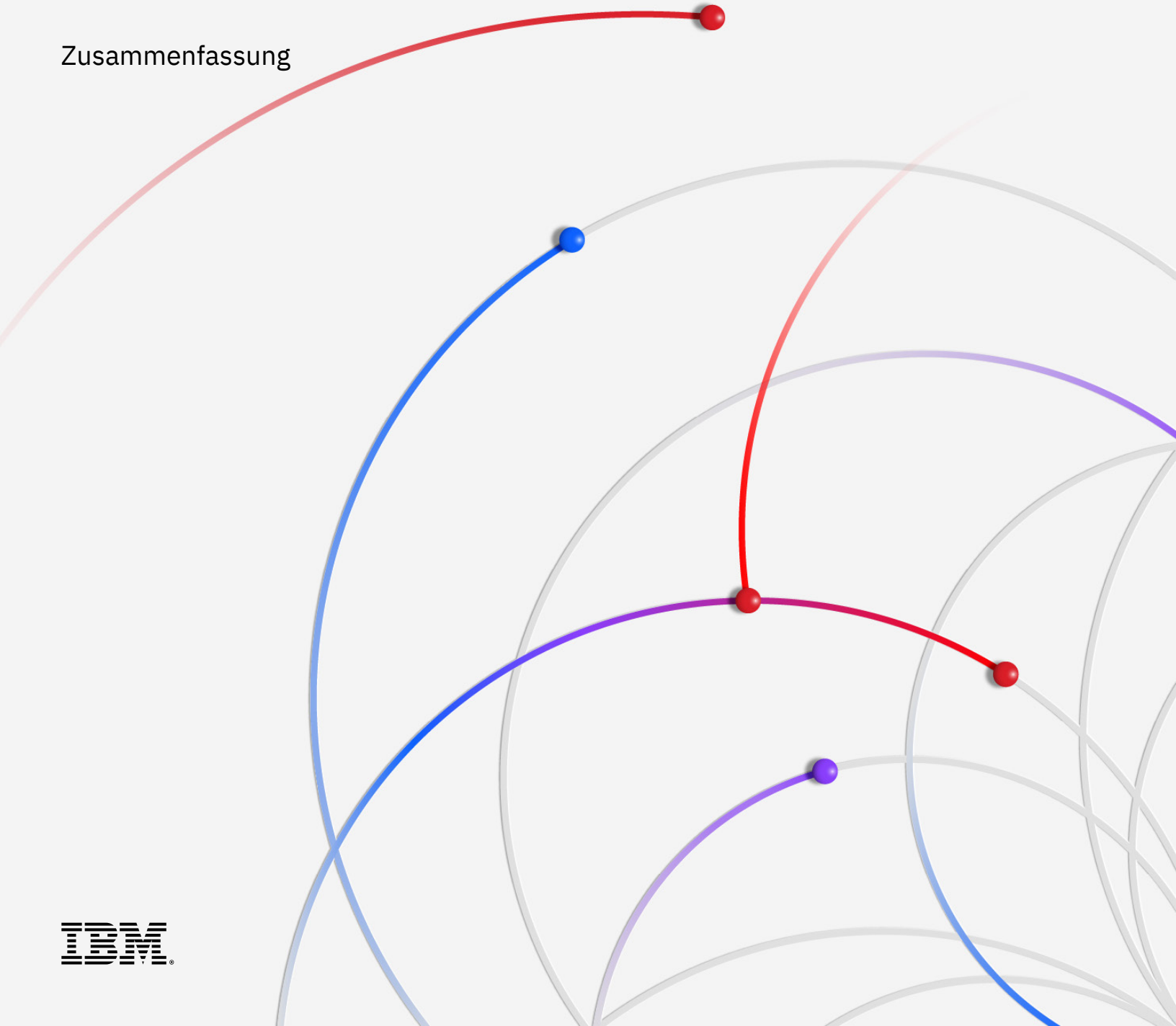
Cost of a Data Breach Report

2024

Bericht über die Kosten eines Datenlec s

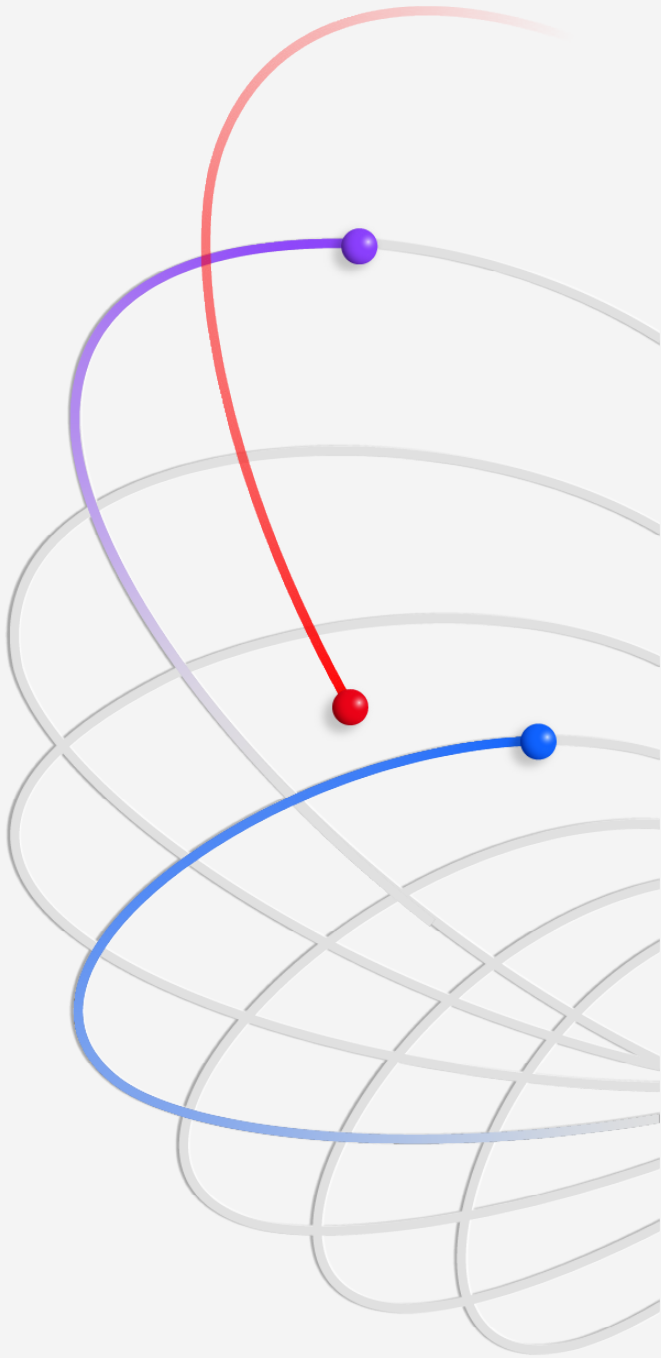
Zusammenfassung



IBM

Inhaltsverzeichnis

Zusammenfassung



Der jährliche Cost of a Data Breach Report von IBM vermittelt Führungskräften in den Bereichen IT, Risikomanagement und Sicherheit zeitnahe, quantifizierbare Daten für strategische Entscheidungsprozesse. Darüber unterstützt er sie bei der Verwaltung ihrer Risikoprofile und Sicherheitsinvestitionen. Der diesjährige Bericht – der 19. der Reihe – spiegelt die durch den technologischen Wandel bedingten Veränderungen wider, wie etwa die Zunahme von Schattendaten (also Daten, die in nicht verwalteten Datenquellen gespeichert sind) sowie das Ausmaß und die Kosten von Geschäftsunterbrechungen aufgrund von Data Breaches.

Die diesjährige Studie, die unabhängig vom Ponemon Institute durchgeführt und von IBM gesponsert, analysiert und veröffentlicht wurde, untersuchte 604 Unternehmen, die zwischen März 2023 und Februar 2024 von Data Breaches betroffen waren. Die Forscher untersuchten Unternehmen aus 17 Branchen in 16 Ländern und Regionen und Data Breaches, bei denen zwischen 2.100 und 113.000 Datensätze kompromittiert wurden. Um belastbare Erkenntnisse zu gewinnen, befragten die Forscher des Ponemon Institute 3.556 Führungskräfte und Sicherheitsfachleute und Unternehmensführung, die aus erster Hand über die Data Breaches in ihren Unternehmen berichten konnten.

Das Ergebnis ist ein Benchmark-Bericht, den Führungskräfte und Sicherheitsfachleute nutzen können, um ihre Sicherheitsvorkehrungen zu verbessern und Innovationen voranzutreiben, insbesondere im Hinblick auf die Einführung von KI in der Sicherheit und die Sicherheit ihrer Initiativen im Bereich der generativen KI.

Wir beginnen den diesjährigen Bericht mit zwei wesentlichen Entwicklungen. Zum einen sind die weltweiten Durchschnittskosten eines Data Breach im Vergleich zum Vorjahr um 10 % gestiegen und erreichten 4,88 Mio. USD – der größte Anstieg seit der Pandemie. Dieser Kostenanstieg ist auf Betriebsunterbrechungen sowie den Kundensupport und die Behebung nach einem Data Breach zurückzuführen. Auf die Frage, wie man mit diesen Kosten umgehe, antworteten mehr als die Hälfte der Unternehmen, sie würden sie an die Kunden weitergeben. In einem wettbewerbsintensiven Markt, der aufgrund der Inflation bereits unter Preisdruck steht, kann es gefährlich sein, diese Kosten den Kunden aufzubürden.

Zweitens stellten die Forscher fest, dass sich der Einsatz von KI und Automatisierung im Sicherheitsbereich auszahlt und die Kosten von Sicherheitsverletzungen in einigen Fällen um durchschnittlich 2,2 Mio. US-Dollar gesenkt werden konnten. KI- und Automatisierungslösungen verkürzen die Zeit, die erforderlich ist, um ein Data Breach zu identifizieren und einzudämmen und den daraus resultierenden Schaden zu begrenzen. Mit anderen Worten: Unternehmen ohne Unterstützung durch KI und Automatisierung müssen damit rechnen, dass die Erkennung und Eindämmung eines Data Breach im Vergleich zu Unternehmen, die diese Lösungen einsetzen, länger dauert und höhere Kosten verursacht.

Wie wir branchenübergreifend beobachten konnten, sind Cybersicherheitsteams notorisch unterbesetzt. Die diesjährige Studie ergab, dass mehr als die Hälfte der betroffenen Unternehmen mit einem gravierenden Mangel an Sicherheitsfachkräften zu kämpfen hatte – ein Qualifikationsdefizit, das im Vergleich zum Vorjahr um einen zweistelligen Prozentsatz gestiegen ist. Dieser Fachkräftemangel verschärft sich, da die Bedrohungslage in der Geschäftswelt zunimmt. Der anhaltende Wettlauf um die Einführung generativer KI in nahezu allen Unternehmensbereichen wird voraussichtlich bisher unbekannte Risiken mit sich bringen und den Druck auf die Cybersicherheitsteams weiter erhöhen.

Dieser Bericht bietet Erkenntnisse und Empfehlungen aus der Forschung, die dazu beitragen können, die potenziellen finanziellen Schäden und Reputationsschäden durch Data Breaches zu verringern.

Neuerungen im Bericht 2024

Um neuen Technologien, neuen Taktiken und aktuellen Ereignissen gerecht zu werden, entwickeln wir den Data Breach Kostenreport jedes Jahr weiter. In der diesjährigen Studie wird zum ersten Mal untersucht:

- ob Unternehmen langfristige Betriebsstörungen erlitten haben, z. B. die Unfähigkeit, Verkaufsaufträge zu bearbeiten, die vollständige Stilllegung von Produktionsanlagen oder einen ineffektiven Kundenservice.
- ob der Data Breach gespeicherte Daten in nicht verwalteten Datenquellen, auch bekannt als Schattendaten, umfasste
- in welchem Umfang Unternehmen in den vier Phasen ihrer Sicherheitsabläufe (Prävention, Erkennung, Untersuchung und Reaktion) KI und Automatisierung nutzen
- die Art der Erpressungsangriffe, z. B. Erpressung und Ransomware-Angriffe oder nur Erpressung und Datenexfiltration
- wie viel Zeit benötigt wurde, um Daten, Systeme oder Dienste wieder in den Zustand vor dem Angriff zu versetzen
- wie lange es dauerte, bis Unternehmen den Data Breach meldeten, wenn sie dazu verpflichtet waren
- ob Unternehmen, die nach einem Ransomware-Angriff Strafverfolgungsbehörden einschalteten, das Lösegeld bezahlten

Wesentliche Feststellungen

Die im Folgenden dargestellten Ergebnisse basieren auf der Analyse von Forschungsdaten des Ponemon Institute durch IBM.

4,88 Mio. USD

Durchschnittliche Gesamtkosten einer Verletzung
Die durchschnittlichen Kosten eines Data Breach stiegen von 4,45 Mio. USD im Jahr 2023 auf 4,88 Mio. USD. Das ist ein Anstieg von 10 % und der höchste seit der Pandemie. Gründe für diesen Anstieg liegen in gestiegenen Kosten durch entgangene Geschäfte – darunter Betriebsausfälle und Kundenverluste – sowie den Kosten für die Reaktion nach einem Data Breach, beispielsweise der Besetzung des Kundenservice-Helpdesks und der Zahlung höherer Bußgelder. Zusammengerechnet beliefen sich diese Kosten auf 2,8 Mio. USD. Das ist der höchste Gesamtbetrag für entgangene Geschäfte und Maßnahmen nach Data Breaches in den letzten sechs Jahren.

2,2 Mio. USD

Kosteneinsparungen durch umfassenden KI-Einsatz in der Prävention
Zwei von drei untersuchten Unternehmen gaben an, dass sie in ihren Sicherheitsabteilungen KI und Automatisierung für die Sicherheit einsetzen. Dies entspricht einem Anstieg von 10 % im Vergleich zum Vorjahr. Bei einem umfassenden Einsatz von KI im Präventionsworkflow – Angriffsflächenmanagement (ASM), Red-Teaming und Posture Management – fielen für Unternehmen die Kosten für Data Breaches im Durchschnitt um 2,2 Mio. US-Dollar niedriger aus als für Unternehmen, die KI im Präventionsworkflow nicht nutzten. Dies ist die größte Kosteneinsparung, die im Bericht 2024 festgestellt wurde.

26,2 %

Zunehmender Mangel an Fachkräften für Cybersicherheit
Mehr als die Hälfte der betroffenen Unternehmen haben mit einem erheblichen Mangel an Sicherheitsfachkräften zu kämpfen. Dieses Problem stellt im Vergleich zum Vorjahr eine Steigerung um 26,2 % dar und entspricht durchschnittlichen Data Breach-Mehrkosten in Höhe von 1,76 Mio. USD. Obwohl jedes fünfte Unternehmen angibt, in irgendeiner Form generative KI-Sicherheitstools zu nutzen, um die Lücke durch Produktivitäts- und Effizienzsteigerungen zu schließen, bleibt der Fachkräftemangel eine Herausforderung.

1 von 3

Data Breaches betraf auch Schattendaten
35 % der Data Breaches betrafen auch Schattendaten. Dies zeigt, dass die Verbreitung der Daten deren Nachverfolgung und Sicherung erschwert. Der Diebstahl von Schattendaten verursachte um 16 % höhere Kosten. Die Forscher fanden heraus, dass die Speicherung von Daten in verschiedenen Umgebungen eine verbreitete Speicherstrategie ist, die für 40 % der Data Breaches verantwortlich ist. Außerdem dauerte es länger, diese Breaches zu erkennen und einzudämmen. Im Gegensatz dazu wurden Daten, die in nur einem Umgebungstyp gespeichert waren, seltener gestohlen, unabhängig davon, ob es sich bei dieser Umgebung um eine Public Cloud (25 %), lokale Umgebung (20 %) oder Private Cloud (15 %) handelte.

4,99 Mio. USD

durchschnittliche Kosten bei einem böswilligen Insider-Angriff
Im Vergleich zu anderen Vektoren verursachen Angriffe durch böswillige Insider mit durchschnittlich 4,99 Mio. US-Dollar die höchsten Kosten. Zu den weiteren kostspieligen Angriffsmethoden gehörten der Angriff auf geschäftliche E-Mails, Phishing, Social Engineering und gestohlene oder kompromittierte Zugangsdaten. Generative KI könnte bei der Entstehung einiger dieser Phishing-Angriffe eine Rolle spielen. Beispielsweise ist es dank generativer KI selbst für nicht-englischsprachige Personen einfacher denn je, grammatikalisch korrekte und plausible Phishing-Nachrichten zu erstellen.

46 %

der Data Breaches betrafen personenbezogene Daten von Kunden
Bei fast der Hälfte aller Data Breaches ging es um personenbezogene Kundendaten (PII), darunter beispielsweise Steueridentifikationsnummern, E-Mail-Adressen, Telefonnummern und Privatadressen. Knapp dahinter folgten Datensätze zu geistigem Eigentum (IP) (43 % der Data Breaches). Die Kosten für IP-Datensätze sind im Vergleich zum Vorjahr erheblich gestiegen – von 156 USD pro Datensatz im Vorjahresbericht auf 173 USD pro Datensatz in der diesjährigen Studie.

1 Mio. USD

Kosteneinsparungen, wenn Strafverfolgungsbehörden bei Ransomware-Angriffen eingeschaltet werden
Zwei Drittel der Unternehmen, die Opfer von Ransomware-Angriffen wurden und Strafverfolgungsbehörden einschalteten, zahlten das Lösegeld nicht. Darüber hinaus konnten diese Unternehmen die Kosten des Angriffs im Durchschnitt um fast eine Million US-Dollar senken, wenn man ein eventuell gezahltes Lösegeld ausschließt. Durch den Einbezug von Strafverfolgungsbehörden konnte außerdem die für die Erkennung und Eindämmung von Data Breaches erforderliche Zeit von 297 Tagen auf 281 Tage verkürzt werden.

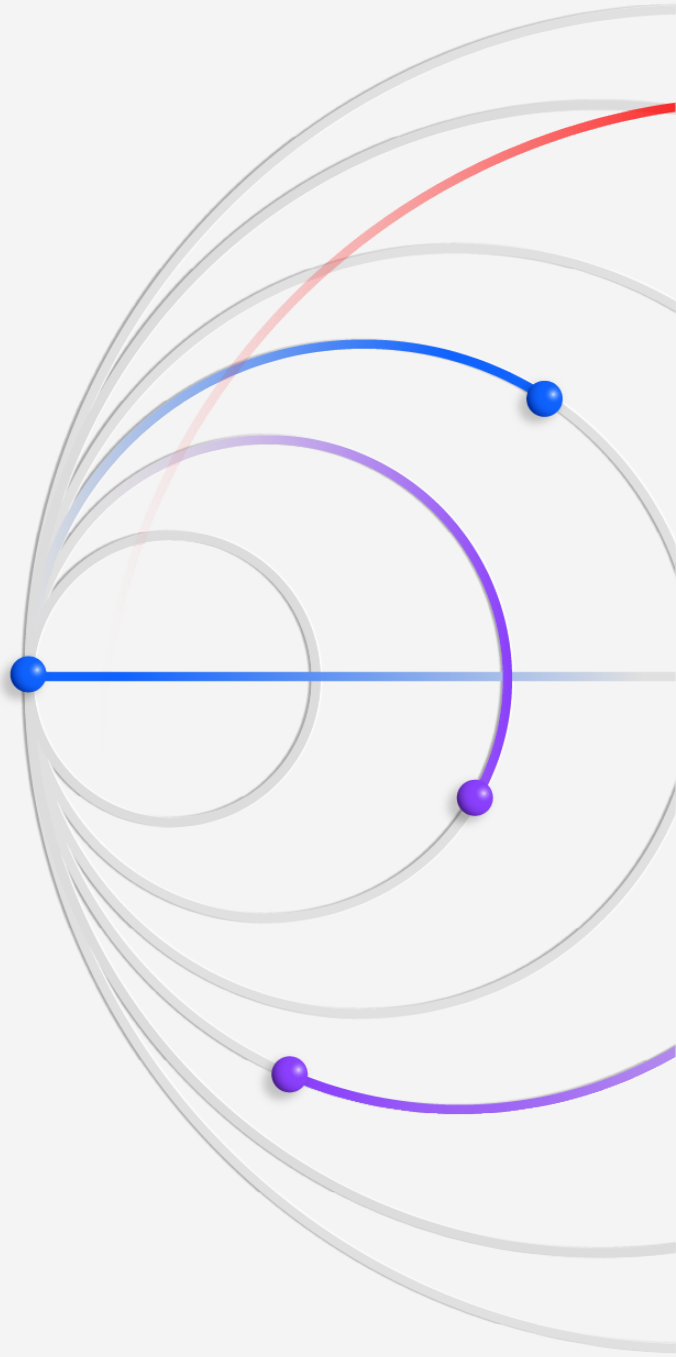
292

Tage zur Identifizierung und Eindämmung von Data Breaches im Zusammenhang mit gestohlenen Zugangsdaten
Bei Data Breaches, bei denen gestohlene oder kompromittierte Zugangsdaten im Spiel waren, dauerte die Identifizierung und Eindämmung aller Angriffsvektoren am längsten (292 Tage). Auch die Bearbeitung ähnlicher Angriffe, bei denen Mitarbeiter und Mitarbeiterzugangsdaten ausgenutzt wurden, dauerte lange. Beispielsweise beanspruchten Phishing-Angriffe durchschnittlich 261 Tage, während Social-Engineering-Angriffe durchschnittlich 257 Tage benötigten.

830.000 USD

betrug der höchste durchschnittliche Kostenanstieg aller Branchen
Der Industriesektor erlebte den höchsten Kostenanstieg aller Branchen; im Vergleich zum letzten Jahr stiegen die Schäden pro Data Breach um durchschnittlich 830.000 USD. Dieser Kostenanstieg könnte für Industrieunternehmen die Notwendigkeit schnellerer Reaktionen bedeuten, da Unternehmen in diesem Sektor für betriebliche Ausfallzeiten sehr empfindlich sind. Dennoch lag die Zeit zur Erkennung und Eindämmung eines Data Breach bei Industrieunternehmen über dem Branchendurchschnitt: Sie betrug 199 Tage zur Erkennung und 73 Tage zur Eindämmung.

Empfehlungen zur Reduzierung der Kosten eines Data Breach



Unsere Empfehlungen umfassen erfolgreiche Sicherheitsansätze, die mit geringeren Kosten und kürzeren Zeiten für die Erkennung und Eindämmung von Sicherheitsverletzungen verbunden sind.

Behalten Sie den Überblick über Ihre Daten

Die meisten Unternehmen verteilen Daten auf mehrere Umgebungen, z. B. lokale Datenspeicher, Private Clouds und Public Clouds. Allerdings verfügen viele Unternehmen über unvollständige oder veraltete Datenbestände, was die Bemühungen, herauszufinden, welche Daten gestohlen wurden und wie sensibel oder vertraulich diese sind, verzögert. Solche Verzögerungen können die Reaktion erschweren und die Kosten eines Data Breach erhöhen.

Sicherheitsteams sollten sicherstellen, dass sie einen umfassenden Einblick in all diese Umgebungen haben, um Daten unabhängig von ihrem Speicherort kontinuierlich überwachen und schützen zu können. Möglich wären zum Beispiel ein Data Security Posture Management (DSPM) und andere Lösungen wie ein Identity Access Management und ASM in all diesen Umgebungen, um konsistenten und umfassenden Schutz zu erreichen.

Sicherheitsteams müssen Hybridumgebungen und der Public Cloud besondere Aufmerksamkeit schenken. 40 % der Data Breaches betrafen Daten, die in mehreren Umgebungen gespeichert waren. Wenn diese Daten in der Public Cloud gespeichert waren, verursachte dies mit 5,17 Mio. US-Dollar die höchsten durchschnittlichen Kosten. Es ist zwingend erforderlich, dass Sicherheitsteams ein tieferes Verständnis für die spezifischen Risiken und Kontrollen jedes von ihnen eingesetzten Cloud-Services erlangen.

Die umgebungsübergreifende Datenverwaltung wird durch die Auswirkungen nicht verwalteter Daten noch komplizierter. Mehr als ein Drittel der Data Breaches betreffen Schattendaten. Sicherheitsteams müssen mittlerweile davon ausgehen, dass ihre Unternehmen über nicht verwaltete Datenquellen verfügen. Unverschlüsselte Daten, auch Daten in KI-Workloads, erhöhen das Risiko noch weiter. Eine Datenverschlüsselungsstrategie muss die Art der Daten, ihre Verwendung und ihren Speicherort berücksichtigen, um das Risiko im Falle einer Sicherheitsverletzung zu verringern.

Präventionsstrategien mit KI und Automatisierung stärken

Die Einführung generativer KI-Modelle und Drittanbieter-Anwendungen im gesamten Unternehmen sowie die fortschreitende Nutzung von IoT-Geräten (IoT: Internet der Dinge) und SaaS-Anwendungen erweitern die Angriffsfläche und setzen Sicherheitsteams unter Druck.

Der Einsatz von KI und Automatisierung zur Unterstützung von sicherheitsbezogenen Präventionsstrategien – auch in den Bereichen ASM, Red-Teaming und Posture Management – kann häufig durch verwaltete Sicherheitsservices abgedeckt werden. Unternehmen, die KI und Automatisierung zur Sicherheitsprävention einsetzten, erzielten in der diesjährigen Studie die größte Wirkung ihrer KI-Investitionen im Vergleich zu drei anderen Sicherheitsbereichen: Erkennung, Untersuchung und Reaktion. Sie sparten durchschnittlich 2,22 Mio. USD gegenüber Unternehmen, die keine KI in der Präventionstechnologie einsetzten.

Setzen Sie bei der Einführung generativer KI auf Sicherheit

Obwohl Unternehmen mit generativer KI schnell vorankommen,sind nur 24 % der Initiativen im Bereich der generativen KI abgesichert. Mangelnde Sicherheit birgt das Risiko, dass Daten und Datenmodelle Sicherheitsverletzungen ausgesetzt sind, die den Nutzen und die Vorteile, die generative KI-Projekte bringen sollen, untergraben können.

Da die Einführung generativer KI in großem Maßstab voranschreitet, benötigen Unternehmen ein Framework zur Sicherung generativer KI-Daten, -Modelle und -Nutzung sowie zur Einrichtung von KI-Governance-Kontrollen. Sie müssen die Trainingsdaten sichern, indem sie diese vor Diebstahl und Manipulation schützen. Unternehmen können Datenerkennung und -klassifizierung nutzen, um sensible Daten zu erkennen, die beim Training oder bei der Feinabstimmung verwendet werden. Zudem können sie Datensicherheitskontrollen für Verschlüsselung, Zugriffsverwaltung und Compliance-Überwachung implementieren.

Bei generativer KI sind Unternehmen nicht nur mit dem Risiko und der Zunahme von Schattendaten konfrontiert, sondern auch mit Schattenmodellen. Sie müssen das Posture Management auf die KI-Modelle selbst ausdehnen, um sensible KI-Trainingsdaten zu schützen und die Verwendung unautorisierter oder *Schatten-KI*-Modelle sowie KI-Missbrauch oder Datenlecks zu erkennen.

Die Sicherung der Entwicklung von KI-Modellen erfordert die Suche nach Schwachstellen in der Pipeline, die Abschottung von Integrationen und die Durchsetzung von Richtlinien und Zugriffsbeschränkungen. Um die Nutzung generativer KI-Modelle abzusichern, müssen Sicherheitsteams auf böswillige Eingaben, wie etwa Prompt-Eingaben, sowie auf Outputs mit sensiblen Daten achten. Sie müssen KI-Sicherheitslösungen einsetzen, die in der Lage sind, KI-spezifische Angriffe wie Datenvergiftung, Modellumgehung und Modellextraktion zu erkennen und darauf zu reagieren. Außerdem ist es wichtig, ein Reaktions-Playbook zu entwickeln, um Zugriffe zu verweigern und kompromittierte Modelle unter Quarantäne zu stellen und zu isolieren.

Angesichts der wachsenden Bedrohungslage durch generative KI und andere IT-Initiativen müssen Sicherheitsschulungen auch für Nicht-Sicherheitsfachleute angeboten werden, zum Beispiel für Data Scientists und Datentechniker, die in KI-Teams arbeiten.

Verbessern Sie Ihr Cyber-Reaktionstraining

Es ist wichtiger denn je, wie ein Unternehmen während und nach einem Data Breach reagiert und kommuniziert – mit der Unternehmensleitung, Aufsichtsbehörden und Kunden. In der diesjährigen Studie wurden 75 % des durchschnittlichen Kostenanstiegs aufgrund von Data Breaches auf die Kosten für entgangene Geschäfte zurückgeführt, einschließlich Ausfallzeiten, Kunden- und Auftragsverluste sowie Kosten für die Gewinnung neuer Kunden. Dazu gehörten auch Reaktionsmaßnahmen nach einem Data Breach, etwa die Einrichtung eines Help Desks für Kunden, die Bereitstellung einer Kreditüberwachung für betroffene Kunden und die Zahlung von Bußgeldern. Fazit: Investitionen in die Vorbereitung von Reaktionen auf einen Data Breach können dazu beitragen, die entstehenden Kosten zu reduzieren.

Technische Reaktionsfähigkeiten müssen durch strategische Planung ergänzt werden, um die geschäftlichen Auswirkungen abzudecken, Kunden zu schützen und die Geschäftskontinuität aufrechtzuerhalten. Durch den Aufbau einer Governance und frühzeitige Entscheidungsfindung können Führungskräfte den Umgang mit größeren Geschäftsunterbrechungen planen und Maßnahmen optimieren, die im Falle eines Angriffs dem Unternehmen zugute kommen.

Unternehmen können ihre Fähigkeit zur Bewältigung und Reaktion auf Angriffe mit großen Auswirkungen durch die Teilnahme an Cyber-Krisenübungen verbessern. An diesen Übungen können sowohl die Sicherheitsteams als auch die Unternehmensleitung teilnehmen, so dass das gesamte Unternehmen seine Fähigkeit zur Erkennung, Eindämmung und Reaktion auf Sicherheitsverletzungen verbessern kann. Sicherheitsleiter sollten im Vorfeld mit ihren Geschäftsfunktionen und Kommunikationsteams im gesamten Unternehmen zusammenarbeiten, um Reaktionspläne zu entwickeln und zu testen. Da die Bedrohungslage durch generative KI und andere IT-Initiativen zunimmt, müssen Sicherheitsschulungen auch für Nicht-Sicherheitsexperten angeboten werden. Zu diesen Fachkräften gehören Data Scientists und Datentechniker, die in Teams für maschinelles Lernen und KI arbeiten, sowie diejenigen, die für die Gewährleistung von KI-Workloads auf lokalen und Cloud-Ressourcen verantwortlich sind.

Investitionen in die Reaktionsbereitschaft tragen dazu bei, die kostspieligen und störenden Auswirkungen von Data Breaches zu verringern, die Geschäftskontinuität zu wahren und die Beziehungen zu Kunden, Partnern und anderen wichtigen Stakeholdern aufrechtzuerhalten. Darüber hinaus beruhigt eine gut vorbereitete Reaktion die Mitarbeiter und reduziert Stress, Kummer und interne Reibungsverluste, da die akuten Phasen eines Angriffs von einem gut vorbereiteten Führungsteam gemanagt, kontrolliert und kommuniziert werden.

Über IBM und das Ponemon Institute

Ponemon Institute

Das 2002 gegründete Ponemon Institute widmet sich der unabhängigen Forschung und Aufklärung zur Förderung verantwortungsvoller Praktiken im Umgang mit Daten und Datenschutz in Unternehmen und Behörden. Unsere Aufgabe ist es, hochwertige empirische Studien zu wesentlichen Themen durchzuführen, die die Verwaltung und Sicherheit sensibler Daten zu Personen und Unternehmen betreffen.

Das Ponemon Institute hält im Hinblick auf Vertraulichkeit, Datenschutz und Forschungsethik strenge Standards ein und sammelt im Rahmen seiner geschäftlichen Forschung keinerlei personenbezogene Daten von Einzelpersonen oder identifizierbare Unternehmensdaten. Darüber hinaus stellen strenge Qualitätsstandards sicher, dass Befragten keine sachfremden, irrelevanten oder unangemessenen Fragen vorgelegt werden.

Bei Fragen oder Anmerkungen zu diesem Forschungsbericht, inklusive Anfragen zur Genehmigung einer Zitierung oder Vervielfältigung des Berichts, wenden Sie sich bitte per Post, Telefon oder E-Mail an:

Ponemon Institute LLC
Forschungsabteilung
1-800-887-3118
research@ponemon.org

IBM

IBM ist ein weltweit führender Anbieter von Hybrid-Cloud-, KI- und Business-Services und hilft Kunden in über 175 Ländern dabei, Erkenntnisse aus ihren Daten zu gewinnen, Geschäftsprozesse zu rationalisieren, Kosten zu senken und sich Wettbewerbsvorteile in ihren Branchen zu verschaffen. All dies wird durch das legendäre IBM Engagement für Vertrauen, Transparenz, Verantwortung, Inklusivität und Service unterstützt. Weitere Informationen finden Sie unter www.ibm.com/de-de.

Möchten Sie mehr über die Verbesserung Ihres Sicherheitsstatus erfahren? Besuchen Sie ibm.com/de-de/security Diskutieren Sie mit in der IBM Security Community

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de
IBM Corporation
New Orchard Road
Armonk, NY 10504, USA

Hergestellt in den Vereinigten Staaten von Amerika
Juli 2024