IBM DACH Newsroom

IBM „Cost of a Data Breach“- Studie 2022: Verbraucher zahlen den Preis, da die Kosten für Datenschutzverletzungen ein Allzeithoch erreichen

• 60% der Unternehmen, bei denen eine Datenschutzverletzung eintrat, hoben danach die Preise an • Der Großteil der Unternehmen der kritischen Infrastruktur hinkt bei der Einführung von Zero Trust hinterher • 550.000 US-Dollar an zusätzlichen Kosten für Unternehmen mit zu wenig Personal

CAMBRIDGE, Mass., 27. Juli 2022 – IBM Security veröffentlicht heute die alljährliche„Cost of a Data Breach“-Studie 2022[1] Daraus geht hervor, dass Datenschutzverletzungen kostspieliger und folgenschwerer sind als je zuvor, wobei die durchschnittlichen Kosten einer Datenschutzverletzung für die befragten Unternehmen mit 4,35 Millionen US-Dollar einen neuen Höchststand erreicht haben.

Da die Kosten für Datenschutzverletzungen in den letzten beiden Jahren laut Bericht um fast 13% anstiegen, könnten diese Vorfälle auch zu steigenden Kosten für Waren und Dienstleistungen beitragen. Tatsächlich hoben 60% der untersuchten Unternehmen ihre Preise für Produkte oder Services aufgrund der Datenschutzverletzung an, und das zu einer Zeit, in der die Herstellungskosten inflations- und lieferkettenbedingt bereits weltweit in die Höhe schnellen.

Die stetige Zunahme von Cyberattacken zeigt auch, welche „tiefgreifenden Auswirkungen“ Datenschutzverletzungen auf Unternehmen haben. Aus der IBM Studie geht hervor, dass 83% der untersuchten Unternehmen während ihres Bestehens bereits mehr als eine Datenschutzverletzung erlebt haben. Ein weiterer Faktor, der sich erst im Laufe der Zeit zeigt, sind die Nachwirkungen von Datenschutzverletzungen auf diese Unternehmen, noch lange nach ihrem Auftreten. So fallen fast 50% der Kosten für Datenschutzverletzungen mehr als ein Jahr danach an.

Die „Cost of a Data Breach“-Studie 2022 basiert auf einer**umfassenden Analyse zwischen März 2021 und März 2022 von realen Datenschutzverletzungen bei 550 Unternehmen weltweit**. Die von IBM Security finanzierte und analysierte Untersuchung wurde vom Ponemon Institute durchgeführt.

Zu den wichtigsten Ergebnissen der IBM Studie 2022 gehören:

- **Rückstände bei Zero Trust in kritischer Infrastruktur –** Fast 80% der untersuchten Unternehmen mit kritischer Infrastruktur setzen keine Zero-Trust-Strategien ein, wodurch die durchschnittlichen Kosten einer Datenschutzverletzung auf 5,4 Millionen US-Dollar steigen – 1,17 Millionen US-Dollar mehr im Vergleich zu denen, die auf Zero Trust setzen. Wobei es sich bei 28% der Datenschutzverletzungen bei diesen Unternehmen um Ransomware- oder zerstörerische Angriffe handelte.

- **Bezahlen, zahlt sich nicht aus –** Ransomware-Opfer aus der Studie, die den Lösegeldforderungen von Erpressern

nachkamen, hatten durchschnittlich nur 610.000 US-Dollar niedrigere Kosten für eine Datenschutzverletzung im Vergleich zu denen, die nicht zahlten – ohne dass der bezahlte Lösegeldbetrag berücksichtigt wird. Unter Berücksichtigung der hohen Kosten von Lösegeldzahlungen kann die finanzielle Last sogar noch höher werden, was nahelegt, dass die Zahlung des Lösegeldes allein möglicherweise keine effektive Strategie ist.

- **Sicherheitslücken in Clouds –** 43% der untersuchten Unternehmen befinden sich in einem frühen Stadium der Umsetzung von Sicherheitsmaßnahmen in ihren Cloudumgebungen oder haben noch gar nicht damit begonnen. Dies resultiert in durchschnittlich mehr als 660.000 US-Dollar höheren Kosten einer Datenschutzverletzung als bei untersuchten Unternehmen mit ausgereifter Sicherheit in ihren Cloudumgebungen.

- **KI und Automatisierung bei Security bringen Kosteneinsparungen von mehreren Millionen US-Dollar**– Untersuchte Unternehmen, die KI und Automatisierung für Security nutzen, verzeichneten durchschnittlich 3,05 Millionen US-Dollar weniger Kosten bei Datenschutzverletzungen im Vergleich zu Unternehmen, die die Technologie nicht einsetzen – dies ist die größte Kosteneinsparung, die in der Studie beobachtet wurde.

„Unternehmen müssen in Security-Fragen Angreifern zuvorkommen. Es ist an der Zeit, Angreifer daran zu hindern, ihre Ziele zu erreichen und die Auswirkungen von Angriffen zu minimieren. Je mehr Unternehmen versuchen, ihren IT-Perimeter zu perfektionieren, anstatt in Früherkennung und Reaktionsfähigkeit zu investieren, desto einfacher können Sicherheitsvorfälle die Lebenshaltungskosten in die Höhe treiben“ so Charles Henderson, Global Head of IBM Security X-Force. „Dieser Bericht zeigt, dass die richtigen Strategien in Verbindung mit den richtigen Technologien den Unterschied machen, wenn Unternehmen angegriffen werden.“

Übermäßiges Vertrauen in Unternehmen der Kritischen Infrastrukturen

Im vergangenen Jahr scheinen Bedenken bezüglich kritischer Infrastruktur als Angriffsziel weltweit zugenommen zu haben, während viele staatliche Cybersicherheitsbehörden zu Wachsamkeit bei störenden Angriffen mahnen. Tatsächlich zeigt der Bericht von IBM, dass Ransomware- und zerstörerische Angriffe 28% der Datenschutzverletzungen bei den untersuchten Unternehmen der kritischer Infrastruktur ausmachten, und hebt hervor, wie Bedrohungsakteure versuchen, die globalen Lieferketten, die von diesen Unternehmen abhängig sind, zu unterbrechen. Dazu gehören unter anderem Unternehmen aus dem Finanzdienstleistungs-, Industrie-, Transport- und Gesundheitssektor.

Trotz der Forderung nach Vorsicht, und ein Jahr, nachdem die Biden-Administration eineDurchführungsverordnung für Cybersicherheit mit Schwerpunkt auf Nutzung einer Zero-Trust-Strategie zur Stärkung der nationalen Cybersicherheit veranlasste, nutzen laut Bericht nur 21% der untersuchten Unternehmen mit kritischer Infrastruktur ein Zero-Trust-Sicherheitsmodell. Hinzu kommt, dass 17% der Datenschutzverletzungen bei Unternehmen der kritischer Infrastruktur darauf zurückzuführen sind, dass zunächst ein Geschäftspartner angegriffen wurde, was die Sicherheitsrisiken verdeutlicht, die eine zu vertrauensvolle Umgebung mit sich bringt.

Unternehmen, die Lösegeld zahlen, haben nichts davon

Laut IBM Studie von 2022 hatten Unternehmen, die den Lösegeldforderungen von Erpressern nachkamen nur 610.000 US-Dollar niedrigere durchschnittliche Kosten bedingt durch eine Datenschutzverletzung im Vergleich zu denen, die nicht zahlten – ohne Berücksichtigung des gezahlten Lösegelds. Bei der Abrechnung der durchschnittlichen Lösegeldzahlung, die laut Sophos im Jahr 2021 812.000 US-Dollar erreichte, konnten Unternehmen, die sich für die Zahlung des Lösegeldes entschieden haben, höhere Gesamtkosten auffangen. Sie finanzieren damit ungewollt künftige Ransomware-Attacken mit Kapital, das für Korrektur- und Wiederherstellungsmaßnahmen verwendet werden könnte. Gleichzeitig riskierten Sie regulatorische Strafen.

Die Dauerhaftigkeit von Ransomware wird trotz erheblicher globaler Bemühungen, diese aufzuhalten, durch die Industrialisierung der Cyberkriminalität verstärkt. Der IBM Security X-Force fand heraus, dass die Dauer von Ransomware-Attacken bei den untersuchten Unternehmen in den letzten drei Jahren um 94% zurückging – und zwar von über zwei Monate auf knapp vier Tage. Diese exponentiell kürzeren Angriffslebenszyklen können zu Angriffen mit größeren Auswirkungen führen, da Verantwortliche für Cybersicherheitsvorfälle nur sehr kurze Zeitfenster zur Erkennung und Eindämmung von Angriffen bleiben. Da die „Zeit bis zur Lösegeldzahlung“ auf wenige Stunden reduziert wird, ist es wichtig, dass Unternehmen strikte Tests von Incident-Response-Playbooks (IR) im Voraus priorisieren. Im Bericht heißt es jedoch, dass bis zu37 % der untersuchten Unternehmen, die über Incident-Response-Pläne verfügen, diese nicht regelmäßig testen.

Hybrid-Cloud-Vorteil

Die Studie zeigte zudem, dass Hybrid-Cloud-Umgebungen die am weitesten verbreitete (45%) Infrastruktur bei den untersuchten Unternehmen sind. Mit durchschnittlich 3,8 Millionen US-Dollar Kosten einer Datenschutzverletzung verzeichneten Unternehmen mit einem Hybrid-Cloud-Modell niedrigere Kosten verglichen mit Unternehmen mit einem reinen Public- oder Private-Cloud-Modell, die durchschnittlich 5,02 Millionen US-Dollar bzw. 4,24 Millionen US-Dollar verzeichneten. Tatsächlich waren die untersuchten Hybrid-Cloud-Anwender in der Lage, Datenschutzverletzungen durchschnittlich 15 Tage früher zu erkennen und einzudämmen als der globale Durchschnitt von 277 Tagen pro Teilnehmer.

Der Bericht hebt hervor, dass 45% der untersuchten Datenschutzverletzungen in der Cloud auftraten, und unterstreicht damit die Bedeutung der Cloud-Sicherheit. Allerdings gaben 43% der berichtenden Unternehmen an, dass sie sich erst in einem frühen Stadium der Sicherheitsmaßnahmen zum Schutz ihrer Cloudumgebungen befinden oder noch gar nicht damit begonnen haben. Dies resultiert in höheren Kosten einer Datenschutzverletzung[2]. Untersuchte Unternehmen, die keine Sicherheitsverfahren in ihren Cloudumgebungen implementiert haben, benötigten durchschnittlich 108 Tage mehr, um eine Datenschutzverletzung zu erkennen und einzudämmen, als Unternehmen, die Sicherheitsmassnahmen in allen Bereichen konsistent anwenden.

Weitere Ergebnisse der IBM Studie 2022:

- **Phishing wird zur teuersten Ursache von Datenschutzverletzungen –** Während kompromittierte Zugangsdaten weiterhin die häufigste Ursache einer Datenschutzverletzung sind (19%), reiht sich nun Phishing auf Platz zwei (16%) und als teuerste Ursache ein, mit durchschnittlichen Kosten von 4,91 Millionen US-Dollar einer Datenschutzverletzung für die befragten Unternehmen.

- **Kosten für Datenschutzverletzungen im Gesundheitswesen erreichen erstmals zweistellige Zahlen** – Im 12. Jahr in Folge verzeichneten Teilnehmer aus dem Gesundheitswesen die teuersten Datenschutzverletzungen aller Branchen mit ansteigenden durchschnittlichen Kosten einer Datenschutzverletzung im Gesundheitswesen um fast 1 Million US-Dollar auf ein Rekordhoch von 10,1 Millionen US-Dollar.

- **Unzureichendes Sicherheitspersonal** – 62% der untersuchten Unternehmen gaben an, dass sie nicht über ausreichend Personal verfügen, um ihre Sicherheitsstrategie umzusetzen. Das sind durchschnittlich 550.000 US-Dollar mehr Kosten bei Datenschutzverletzungen als bei Unternehmen, die angeben, dass sie über ausreichend Personal verfügen.

Zusätzliche Quellen

- Eine Kopie des Berichts „Cost of a Data Breach"- Studie 2022 können Sie unter folgender Adresse herunterladen: https://www.ibm.com/security/data-Breach.
- Melden Sie sich für das IBM Security Cost of a Data Breach-Webseminar 2022 am Mittwoch, 3. August 2022, um 11:00 Uhr ET, hier an.
- Nehmen Sie Kontakt mit dem IBM Security X-Force-Team auf, um eine persönliches Review der Ergebnisse zu erhalten: https://ibm.biz/book-a-consult.

Informationen zu IBM Security

IBM Security bietet eines der fortschrittlichsten und integrierten Portfolios von Sicherheitsprodukten und -services für Unternehmen. Mit dem Portfolio, das von der weltweit bekannten IBM Security X-Force®-Forschung unterstützt wird, können Unternehmen Risiken effektiv verwalten und sich vor neuen Bedrohungen schützen.IBM verfügt über eine der weltweit größten Organisationen für Sicherheitsforschung, -entwicklung und -bereitstellung, überwacht über 150 Milliarden Sicherheitsereignisse pro Tag in mehr als 130 Ländern und hat weltweit mehr als 10.000 Sicherheitspatente. Weitere Informationen finden Sie unter www.ibm.com/security, folgen Sie @IBMSecurity auf Twitter oder besuchen Sie denIBM Security Intelligence-Blog.

Pressekontakt IBM DACH:
IBM
Kerstin Pehl
Unternehmenskommunikation IBM DACH
Tel: +49-176-10185348
E-Mail: kerstin.pehl@de.ibm.com

[1] „Cost of a Data Breach“- Studie 2022, durchgeführt vom Ponemon Institute, finanziert und analysiert von IBM

[2] Durchschnittliche Kosten von 4,53 Millionen US-Dollar im Vergleich zu durchschnittlichen Kosten von 3,87 Millionen US-Dollar bei teilnehmenden Unternehmen mit ausgereiften Cloud-Sicherheitsverfahren

---

Additional assets available online: Photos

https://de.newsroom.ibm.com/2022-07-27-Cost-of-a-Data-Breach-Studie-2022