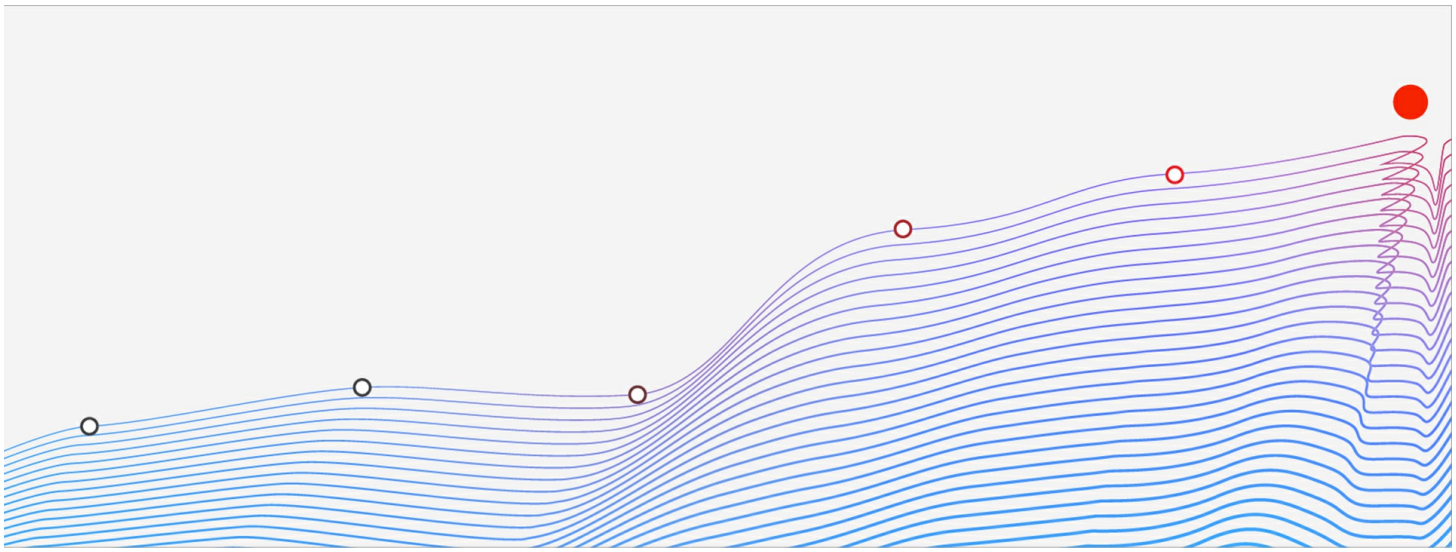
IBM DACH Newsroom

IBM-Bericht: Ein Datenleck kostet deutsche Unternehmen durchschnittlich 4,3 Millionen Euro

Deutsche Unternehmen, die stark auf KI und Automatisierung setzen, verkürzen Lebenszyklen von Datenlecks um 81 Tage und senken die Folgekosten pro Vorfall um 1,76 Millionen Euro



CAMBRIDGE, Massachusetts, Ehningen, 24. Juli 2023 -- IBM (NYSE: IBM) Security hat heute seinen jährlichen **Cost of a Data Breach Report** [1] veröffentlicht, aus dem hervorgeht, dass die durchschnittlichen Kosten eines Datenlecks (also Verletzungen der Sicherheit, der Integrität oder auch der Verfügbarkeit von Daten) im Jahr 2023 sich in Deutschland auf 4,3 Mio. EUR beliefen. Dies ist ein leichter Rückgang gegenüber den 4,41 Mio. EUR des letzten Jahres. Der Report stellte weiter fest, dass die analysierten deutschen Unternehmen im Schnitt 182 Tage benötigten, um Datenlecks aufzudecken und einzudämmen. Das sind 95 Tage weniger als im globalen Durchschnitt, der 277 Tage betrug.

Laut dem IBM-Bericht von 2023 sind die Unternehmen geteilter Meinung darüber, wie sie mit den zunehmenden Kosten und der Häufigkeit von Datenlecks umgehen wollen. Die Studie ergab, dass obwohl 95 % der untersuchten Unternehmen mehr als einen solchen Vorfall verzeichnet haben, wobei die betroffenen Unternehmen die Kosten hierfür eher an die Verbraucher weitergeben (57 %) als ihre Sicherheitsinvestitionen zu erhöhen (51 %).

Der 2023 Cost of a Data Breach Report basiert auf einer eingehenden Analyse realer Datenlecks, die 553 Unternehmen weltweit zwischen März 2022 und März 2023 erlitten haben. Die von IBM Security in Auftrag gegebene und analysierte Studie wurde vom Ponemon Institute durchgeführt und wird seit 18 Jahren veröffentlicht. Zu den wichtigsten Ergebnissen des IBM-Berichts 2023 gehören:

- **KI nimmt Fahrt auf -** KI und Automatisierung hatten den größten Einfluss auf die Geschwindigkeit, mit der die untersuchten Unternehmen Datenlecks erkennen und eindämmen konnten. Deutsche Unternehmen, die stark auf beide Technologien setzen, verzeichneten einen 81 Tage kürzeren Lebenszyklus von Datenlecks als Unternehmen, die diese Technologien nicht einsetzten (160 Tage versus 241 Tage).

- **Schweigen kostet -** Ransomware-Opfer in der Studie, die die Strafverfolgungsbehörden einschalteten, sparten im Vergleich zu denjenigen, die die Strafverfolgungsbehörden nicht einschalteten, weltweit durchschnittlich 470.000 US-Dollar (ca. 418.000 EUR) an Kosten pro Vorfall. Trotz dieser potenziellen Einsparungen haben 37 % der untersuchten Ransomware-Opfer bei einem Ransomware-Angriff die Strafverfolgungsbehörden nicht eingeschaltet.

- **Lücken bei der Erkennung** - Nur ein Drittel der weltweit untersuchten Vorfälle wurde von eigenen Cyber-Security-Teams der Unternehmen entdeckt, während 27 % durch die Angreifer aufgedeckt wurden. Datenlecks, die erst durch den Angriff offenbart wurden, kosteten im globalen Durchschnitt fast 1 Mio. Dollar (ca. 890.000 EUR) mehr als jene bei den Organisationen, welche die Angriffe selbst erkannten.

„Zeit ist die neue Währung in der Cybersecurity, sowohl für die Verteidiger als auch für die Angreifer. Wie der Bericht zeigt, können eine frühzeitige Erkennung und eine schnelle Reaktion die Auswirkungen eines Angriffs erheblich reduzieren", so Chris McCurdy, General Manager, Worldwide IBM Security Services. „Sicherheitsteams müssen sich darauf konzentrieren, wo die Angreifer am ehesten effektiv sein könnten, und ihre Bemühungen darauf konzentrieren, sie zu stoppen, bevor sie ihre Ziele erreichen. Investitionen in Erkennungs- und Reaktionsmaßnahmen gegen Bedrohungen, die die Geschwindigkeit und Effizienz von Verteidigern erhöhen – beispielsweise mit KI und Automatisierung - sind entscheidend, um dieses Gleichgewicht auszubalancieren.“

Jede Sekunde kostet

Laut dem Bericht von 2023 haben die weltweit analysierten Unternehmen, die KI und Automatisierung im Sicherheitsbereich vollständig einsetzen einen durchschnittlich 108 Tage kürzeren Zeitraum von Datenlecks im Vergleich zu Unternehmen, die diese Technologien nicht einsetzen. Zudem meldeten sie deutlich geringere Kosten für solche Vorfälle. Die analysierten Unternehmen, die umfassend auf KI und Automatisierung im Sicherheitsbereich gesetzt haben, verzeichneten im globalen Durchschnitt auch um fast 1,8 Mio. US-Dollar (ca. 1,6 Mio. EUR) niedrigere Kosten im Falle von Datenlecks als Unternehmen, die diese Technologien nicht eingesetzt haben - die größte Kostenersparnis, die in dem Bericht ermittelt wurde.

Dieser Trend zeigte sich auch bei deutschen Unternehmen. Diejenigen, die im Cyber-Security-Bereich bereits KI und Automatisierung ausgiebig nutzen, meldeten durchschnittliche Kosten von „nur“ 3,51 Mio. EUR pro Schadensereignis. Unternehmen, die keine derartigen Technologien einsetzen, mussten mit durchschnittlichen Kosten von 5,27 Mio. EUR pro Datenleck rechnen. Das entspricht 1,76 Mio. EUR mehr. Trotzdem setzen 47 % der analysierten Unternehmen in Deutschland bisher keine KI- oder Automatisierungslösungen im Cyber-Security Bereich ein. Es gibt hier also bedeutendes Potenzial, die Zeiten für Erkennung und Behebung deutlich zu verkürzen und auch die Kosten von Datenlecks zu senken.

Ransomware-Angriffe sollten nicht verschwiegen werden

Einige untersuchte Unternehmen scheuen sich nach wie vor, bei einem Ransomware-Angriff die Strafverfolgungsbehörden einzuschalten, weil sie glauben, dass dies die Situation nur verkomplizieren würde. In diesem Jahr hat sich der IBM-Bericht zum ersten Mal näher mit diesem Thema befasst und das Gegenteil bewiesen. Bei den analysierten Unternehmen, die die Strafverfolgungsbehörden nicht einschalteten, war weltweit der Zeitraum der Datenlecks im Durchschnitt 33 Tage länger als bei denen, die die

Strafverfolgungsbehörden einschalteten - und dieses Schweigen hatte seinen Preis. Die untersuchten Ransomware-Opfer, die die Strafverfolgungsbehörden nicht einschalteten, zahlten im Durchschnitt 470.000 US-Dollar (ca. 418.000 EUR) mehr, als diejenigen, die dies taten.

Trotz der laufenden Bemühungen der Strafverfolgungsbehörden, mit Ransomware-Opfern zusammenzuarbeiten, entschieden sich global 37 % der analysierten Unternehmen dafür, sie nicht einzuschalten. Hinzu kommt, dass fast die Hälfte (47 %) aller untersuchten Ransomware-Opfer Berichten zufolge das Lösegeld bezahlt hat. Es ist klar, dass Unternehmen mit diesen falschen Vorstellungen über Ransomware aufräumen sollten. Die Zahlung von Lösegeld und die Tatsache, dass die Strafverfolgungsbehörden nicht eingeschaltet werden, treiben nur die Schadenskosten in die Höhe und verzögern die Reaktion.

Cybersecurity-Teams entdecken Verstöße nur selten selbst

Bei der Erkennung und Abwehr von Bedrohungen sind einige Fortschritte zu verzeichnen. Laut dem IBM Threat Intelligence Index 2023 konnten die Cyber-Security-Teams im vergangenen Jahr einen größeren Anteil der Ransomware-Angriffe abwehren. Dennoch finden die Angreifer immer noch Wege, um durch die Lücken der Verteidigungsmaßnahmen zu schlüpfen. Der Bericht ergab, dass weltweit nur einer von drei untersuchten Vorfällen von den eigenen Sicherheitsteams oder -tools des Unternehmens entdeckt wurde, während 27 % der Datenlecks erst durch den Angreifer und 40 % von einer neutralen dritten Partei wie etwa den Strafverfolgungsbehörden aufgedeckt wurden.

Bei Unternehmen, die die Datenlecks selbst entdeckten, fielen die Kosten pro Vorfall um fast 1 Million US-Dollar (ca. 890.000 EUR) geringer aus als bei Unternehmen, die durch einen Angreifer entdeckt wurden (5,23 Millionen US-Dollar gegenüber 4,3 Millionen US-Dollar bzw. ca. 4,65 Mio EUR gegenüber ca. 3,82 Mio. EUR). Durch den Angreifer aufgedeckte Datenlecks hatten außerdem eine um fast 80 Tage längere Laufzeit (320 gegenüber 241 Tage) im Vergleich zu Unternehmen, die den Vorfall intern aufdeckten. Die beträchtlichen Kosten- und Zeiteinsparungen, die sich aus der Früherkennung ergeben, zeigen, dass sich die Investition in diese Strategien langfristig auszahlen würde.

Weitere Erkenntnisse aus dem IBM-Bericht 2023 sind:

- **Verschiedene Umgebungen betroffen** – In Deutschland führten 41 % der analysierten Vorfälle zu einem Datenverlust in mehreren Platftormen, darunter Public Cloud, Private Cloud und On-Premise. Dies resultierte dann auch in höheren Kosten von durchschnittlich 4,56 Mio. EUR. Das bewegt sich auch im Rahmen der globalen Ergebnisse.

- **Der DevSecOps-Vorteil** - In Deutschland konnten Unternehmen, die einen DevSecOps-Ansatz anwenden, die Kosten von Datenlecks um durchschnittlich 300.780 EUR senken.

Zusätzliche Quellen

- Den vollständigen Report für das Jahr 2023 können Sie hier

herunterladen: https://www.ibm.com/security/data-breach

- Lesen Sie mehr über die wichtigsten Ergebnisse des Berichts in diesem IBM Security Intelligence Blog.
- Melden Sie sich für das IBM Security Cost of a Data Breach Webinar 2023 am Dienstag, den 1. August 2023, um 17:00 Uhr MESZ hier an.
- Setzen Sie sich mit dem IBM Security X-Force-Team in Verbindung, um einen persönlichen Überblick über die Ergebnisse zu erhalten: https://ibm.biz/book-a-consult.
- Mehr Informationen zu den Empfehlungen des Berichts finden Sie hier: Cost of a Data breach Action Guide.

Über IBM Sicherheit

IBM Security unterstützt die größten Unternehmen und Regierungen der Welt mit einem integrierten Portfolio von Sicherheitsprodukten und -dienstleistungen, die mit dynamischer KI und Automatisierungsfunktionen ausgestattet sind. Das Portfolio, das von der weltweit anerkannten IBM Security X-Force®-Forschung unterstützt wird, ermöglicht es Unternehmen, Bedrohungen vorherzusehen, Daten zu schützen, während sie sich bewegen, und schnell und präzise zu reagieren, ohne geschäftliche Innovationen zu behindern. Tausende von Unternehmen vertrauen IBM als ihrem Partner bei der Bewertung, Strategieentwicklung, Implementierung und Verwaltung von Sicherheitstransformationen. IBM betreibt eine der weltweit umfangreichsten Organisationen für Sicherheitsforschung, -entwicklung und -bereitstellung, überwacht täglich mehr als 150 Milliarden Sicherheitsereignisse in mehr als 130 Ländern und hat weltweit mehr als 10.000 Sicherheitspatente erteilt bekommen.

Pressekontakt:

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

---

[1] The 2023 Cost of a Data Breach Report ,conducted by Ponemon Insitute, is sponsored and analyzed by IBM Security.
