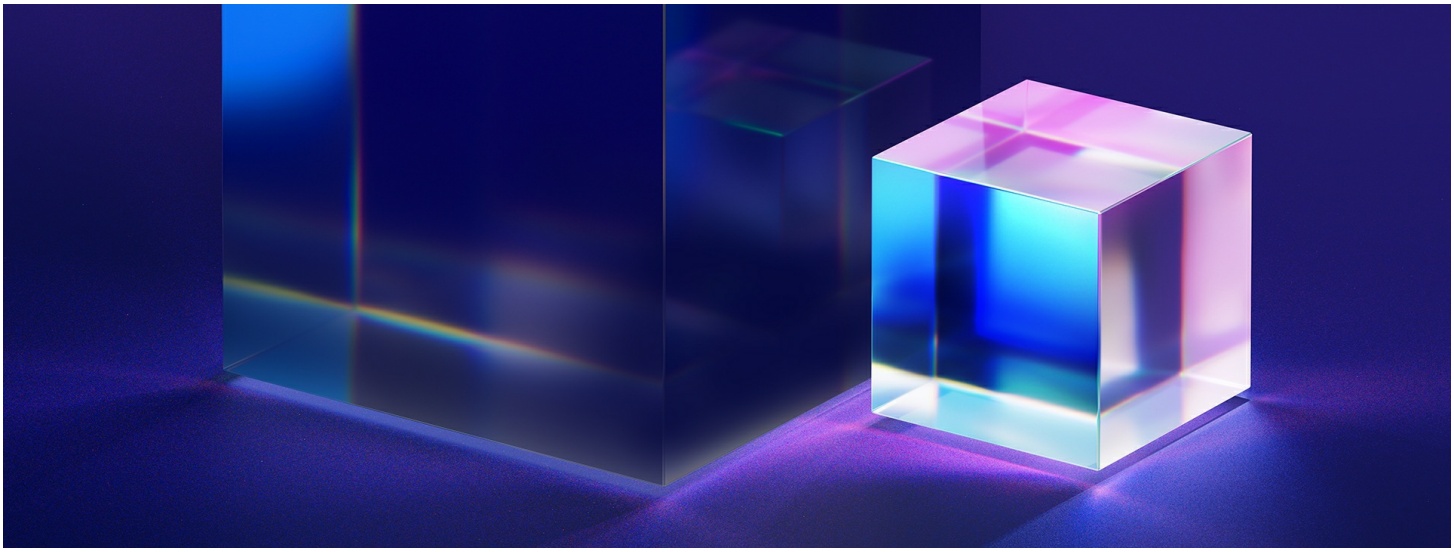
IBM DACH Newsroom

IBM Studie: Kosten von Datenlecks sinken in Deutschland erstmals seit fünf Jahren

• Durchschnittliche Schadenshöhe deutscher Unternehmen beträgt 3,87 Millionen Euro pro Fall

• KI-Sicherheitssoftware verkürzt Dauer von Angriffen

• Nur 52 %% der befragten deutschen Unternehmen verfügen über Richtlinien zur KI-Governance



Ehningen, 30. Juli 2025 - IBM (NYSE: IBM) veröffentlichte heute den jährlichen weltweiten Cost of a Data Breach Report. Die Ausgabe 2025 zeigt, dass die durchschnittlichen Kosten eines Datenlecks in Deutschland auf 3,87 Millionen Euro (ca. 4,03 Millionen US-Dollar) pro Vorfall gesunken sind – im Vorjahr lagen sie noch bei 4,9 Millionen Euro (ca. 5,31 Millionen US-Dollar). Weltweit sank der Durchschnittswert auf 4,44 Millionen US-Dollar pro Vorfall. Die geringeren Kosten sind teilweise auf eine schnellere Erkennung zurückzuführen, die durch den Einsatz von künstlicher Intelligenz (KI) in Security Operations Centern (SOC) ermöglicht wird.

Im Gegensatz dazu stiegen die Kosten pro Datenleck in den USA deutlich an: Dort meldeten Unternehmen einen Rekordwert von durchschnittlich 10 Millionen US-Dollar pro Vorfall (2024: 9,36 Millionen US-Dollar). Ursache sind höhere Aufwendungen für Erkennung und Eskalation sowie höhere Bußgelder der Regulierungsbehörden. Leichte Kostensteigerungen verzeichneten auch die Benelux-Länder, Kanada und Indien.

KI-Risiken werden noch unterschätzt

Die weltweit geringere Schadenshöhe ist zum Teil auf den Einsatz von KI-gestützter Sicherheitssoftware zurückzuführen. Gleichzeitig meldeten jedoch 13 % der befragten Unternehmen Sicherheitsvorfälle, bei denen KI-Modelle oder -Anwendungen kompromittiert wurden; weitere 8 % wussten nicht, ob sie in dieser Form betroffen waren. 97 % der Betroffenen verfügten nicht über angemessene KI-Zugriffskontrollen. Die meisten dieser Vorfälle (29 %) betrafen SaaS-basierte KI-Services von Drittanbietern, gefolgt von intern trainierten Lösungen (26 %) und Open-Source-Modellen (26 %).

Bei Datenlecks zählt jeder Tag

Die Zeitspanne zur Identifizierung und Eindämmung eines Vorfalls bleibt ein entscheidender Kostentreiber. Deutsche Unternehmen benötigten 2025 durchschnittlich 170 Tage, um Sicherheitsvorfälle zu erkennen und einzudämmen – 15 Tage weniger als im Vorjahr und 71 Tage unter dem weltweiten Durchschnitt. Damit weist Deutschland die kürzeste Reaktionszeit aller untersuchten Länder und Regionen auf.

Weitere wichtige Erkenntnisse des Reports für Deutschland:

- **KI-Governance mit Luft nach oben**– 52 % der deutschen Unternehmen haben Richtlinien zur Regulierung des KI-Einsatzes und zur Eindämmung von „Schatten-KI“. Obwohl dieser Wert über dem globalen Durchschnitt von 37 % liegt, verfügen nur 39 % über explizite KI-Zugriffskontrollen. Fast jedes zweite Unternehmen (45 %) setzt strenge Freigabeprozesse für KI-Anwendungen ein, was das engmaschige deutsche Regulierungsumfeld unterstreicht.
- **KI-gestützte Sicherheitslösungen reduzieren Schadenshöhe** deutlich – 63 % der befragten Organisationen nutzen laut IBM Cost of a Data Breach Report 2025 KI-basierte Sicherheits- und Automatisierungstools umfassend oder teilweise (plus 5 %punkte gegenüber 2024). Firmen mit umfangreichem KI-Einsatz verkürzten den Lebenszyklus von Datenlecks um 15 Tage (155 vs. 170) und senkten die durchschnittlichen Kosten um 1,35 Millionen Euro im Vergleich zu Unternehmen ohne diese Technologien.
- **Industrieunternehmen nach wie vor stark betroffen**– Wie 2024 verzeichneten Industrieunternehmen die höchsten Durchschnittskosten pro Vorfall (2025: 6,67 Millionen Euro; 2024: 9,34 Millionen Euro), gefolgt von Pharmaunternehmen (4,62 Millionen Euro) und Finanzdienstleistern (4,46 Millionen Euro).
- **Wichtigstes Einfallstor: Lieferkette und Dritte**– In 16 % der deutschen Fälle erfolgte der Erstzugriff über die Lieferkette oder Drittanbieter-Systeme, was im Schnitt 4,52 Millionen Euro kostete. Phishing lag mit 14 % und 4,15 Millionen Euro Schaden an zweiter Stelle. Denial-of-Service-Attacken (ebenfalls 14 %) verursachten durchschnittlich 3,14 Millionen Euro. Gestohlene oder kompromittierte Anmeldedaten fielen von 20 % (Platz 1 im Vorjahr) auf 8 % (Platz 5), verursachten aber immer noch 4,2 Millionen Euro Schaden (2024: 5,11 Millionen Euro).

„Der erste Rückgang der Schadenshöhe von Datenlecks seit fünf Jahren ist eine gute Nachricht für die deutschen Unternehmen“, sagte Christine Barbara Müller, Partner & Head of Security Services DACH bei IBM Deutschland. „Das zeigt, dass das Rennen gegen immer versiertere Angreifer noch lange nicht verloren ist. Die Investitionen der letzten Jahre in ausgereifte KI-basierte Sicherheitssysteme zahlen sich aus, und IT-Teams setzen diese effektiv gegen immer ausgefeiltere Attacken ein. Positiv ist auch, dass deutsche Unternehmen Cyberangriffe vergleichsweise schnell erkennen und eindämmen. Trotzdem dürfen wir uns nicht ausruhen: KI-Anwendungen und die darunterliegende Infrastruktur haben in vielen Unternehmen eine starke strategische Bedeutung gewonnen und müssen auf Daten-, Modell und Zugriffsebene noch besser abgesichert werden. Zusätzlich muss der Einsatz von Schatten-KI durch Mitarbeitende eingedämmt werden, um dieses Einfallstor für Cyberkriminelle zu schließen. In diesen Bereichen sehe ich in Deutschland trotz steigenden Kostendrucks auf die Unternehmen weiterhin Luft nach oben“, schließt Müller.

Zusätzliche Erkenntnisse für weitere Länder

Der Cost of a Data Breach Report 2025 liefert auch Daten aus Frankreich, Italien, dem Vereinigten Königreich und den Benelux-Staaten. Hier einige zusätzliche Informationen über diese Länder:

- **Durchschnittliche Dauer von Datenlecks in Tagen:**
  - Vereinigtes Königreich – 210 (2024: 230)
  - Italien – 186 (2024: 218)
  - Frankreich – 284 (2024: 294)

    - Benelux – 253 (2024: 265)
- **Häufigster initialer Angriffsvektor:**
    - Vereinigtes Königreich – Kompromittierung von Lieferketten und Drittanbietern (18 %)
    - Italien – Phishing 17 % (unverändert zu letztem Jahr)
    - Frankreich – DoS Angriffe, physischer Diebstahl bzw. Probleme mit der physischen Sicherheit, menschliches Versagen durch Insider über Lieferketten/Drittanbietern – jeweils 13 %
    - Benelux – Gestohlene oder kompromittierende Zugangsdaten sowie menschliches Versagen durch Insider – jeweils 15 %
- **Nutzung von KI-basierten Sicherheits- und Automatisierungslösungen**(Anteil der Unternehmen, die diese laut Report umfangreich oder im begrenzten Umfang nutzen):
    - Vereinigtes Königreich – 76 % (2024: 71 %)
    - Italien – 76 % (2024: 69 %)
    - Frankreich – 65 % (2024: 70 %)
    - Benelux – 71 % (2024: 66 %)

Weltweite Beobachtungen im Cost of a Data Breach Report 2025:

- **Hohen Kosten durch Schatten-KI –** Organisationen mit hohem Einsatz von Schatten-KI (unregulierte, nicht autorisierte Nutzung von KI) verzeichneten durchschnittlich 670.000 US-Dollar höhere Kosten pro Datenleck als Unternehmen mit geringer oder keiner Schatten-KI – einer der größten Kostentreiber 2025.
- **Datenlecks haben langfristige Auswirkungen** – Nahezu 90 % der betroffenen Unternehmen meldeten Betriebsunterbrechungen, und lediglich ein Drittel hatte seine Systeme zum Zeitpunkt der Studie vollständig wiederhergestellt; die meisten benötigten dafür mehr als 100 Tage.
- **Sinkende Bereitschaft zu Lösegeldzahlungen** – Laut der aktuellen Studie lehnten 63 % der befragten Organisationen Erpressungsforderungen ab (2024: 59 %). Dennoch bleiben die durchschnittlichen Kosten von Erpressungs- oder Ransomware-Angriffen hoch – insbesondere, wenn der Angriff vom Täter offengelegt wird, bevor das Unternehmen ihn erkennt (5,08 Millionen US-Dollar).
- **Sicherheitsinvestitionen stagnieren trotz steigender KI-Risiken.** Nur 49 % der teilnehmenden Unternehmen und Organisationen planen nach einem Vorfall zusätzliche Sicherheitsinvestitionen (2024: 63 %). Weniger als die Hälfte davon will explizit KI-gestützte Lösungen priorisieren.

Über den Cost of a Data Breach Report

Der Cost of a Data Breach Report basiert auf einer eingehenden Analyse von mehr als 3.470 Interviews zu realen Schadensereignissen in 600 Unternehmen weltweit. Der Untersuchungszeitraum erstreckte sich von März 2024 bis Februar 2025. Der Report wird vom Ponemon Institute erstellt und von IBM gesponsert und analysiert und gilt seit zwei Jahrzehnten als Branchenbenchmark. In Deutschland erscheint er seit 17 Jahren. Im Laufe der Zeit hat der Report Vorfälle in insgesamt 6.784 Unternehmen und Organisationen weltweit untersucht.

Mit der rasanten Verbreitung von KI im Unternehmensumfeld hat die Studie 2025 erstmals Sicherheit und Governance im Zusammenhang mit KI untersucht: Welche Daten werden bei KI-bezogenen Vorfällen ins Visier genommen? Welche Kosten entstehen durch KI-gesteuerte Angriffe? Wie verbreitet und risikobehaftet ist Schatten-KI?

Erkenntnisse aus den Reports von 2025 bis 2025:

- **2005:** Fast die Hälfte (45 %) aller Datenlecks wurden durch verlorene oder gestohlene Geräte wie Laptops oder USB-Sticks verursacht. Nur 10 % der Vorfälle waren auf gehackte elektronische Systeme zurückzuführen.
- **2015:** Sicherheitsvorfälle aufgrund von Fehlkonfigurationen in der Cloud wurden damals noch nicht einmal als Gefahrenkategorie eingestuft. Heute gehören sie zu den wichtigsten Bedrohungen.
- **2020:** Ransomware begann sich stark auszubreiten. Bis 2021 verursachten diese Vorfälle durchschnittliche Kosten von 4,62 Millionen Dollar pro Datenleck. Im aktuellen Report für 2025 stieg dieser Wert, wenn der Angriff von den Angreifern selbst offengelegt wurde, auf durchschnittlich 5,08 Millionen Dollar.
- **2025:** KI-Sicherheit wurde erstmals untersucht und erweist sich gleichzeitig als neue, hochrelevante Angriffsfläche und als Treiber für schnellere Erkennung und geringere Gesamtkosten auf Unternehmensseite.

Zusätzliche Informationen

- Laden Sie eine Kopie des aktuellen Cost of a Data Breach Report herunter.
- Melden Sie sich für das IBM Webinar „Cost of a Data Breach“ am Mittwoch, 13. August 2025, um 17:00 Uhr MESZ an.

Über IBM

IBM ist ein führendes Unternehmen im Bereich Hybrid Cloud, KI und Beratung. Wir helfen Kunden in über 175 Ländern, Erkenntnisse aus ihren Daten zu kommerzialisieren, Geschäftsprozesse zu optimieren, Kosten zu senken und an der Spitze ihrer Branche zu bleiben. Tausende von Regierungsbehörden und Unternehmen in kritischen Infrastruktursektoren wie Finanzdienstleistungen, Telekommunikation und Gesundheitswesen verlassen sich für eine schnelle, effiziente und sichere digitale Transformation auf die Hybrid-Cloud-Plattform von IBM und Red Hat OpenShift. IBMs bahnbrechende Innovationen in den Bereichen KI, Quantencomputing, branchenspezifische Cloud-Lösungen und Beratung eröffnen unseren Kunden offene und flexible Optionen. Gestützt wird das Ganze durch das langjährige Engagement von IBM für Vertrauen, Transparenz, Verantwortung, Inklusion und Service. Weitere Informationen finden sich unter www.ibm.com.

Dicsclaimer: Diese Pressemitteilung enthält Informationen aus dem IBM Cost of a Data Breach Report 2025. Alle Angaben erfolgen nach bestem Wissen, jedoch ohne Gewähr auf Vollständigkeit oder rechtliche Verbindlichkeit.

Kontakt für Journalisten:

Barbara Jax

IBM Unternehmenskommunikation

barbara.jax@at.ibm.com

https://de.newsroom.ibm.com/2025-07-30-IBM-Studie-Kosten-von-Datenlecks-sinken-in-Deutschland-erstmals-seit-funf-Jahren