IBM „Cost of a Data Breach“-Studie 2021: Kosten für Sicherheitsvorfälle steigen auf 17-Jahres-Hoch

KI, Sicherheitsanalysen und Verschlüsselung senken die Kosten stark, Automatisierung von Sicherheitslösungen steigt um 13 Prozent

CAMBRIDGE, MA, Ehningen, 28. Juli 2021: Die COVID-19-Pandemie treibt die Kosten für Sicherheitsvorfälle auf ein nie gemessenes Niveau – international wie in Deutschland. 4,11 Millionen Euro kostet ein Datenvorfall ein deutsches Unternehmen im Durchschnitt. Deutschland bleibt damit auf Platz vier der teuersten Märkte für Datenpannen: Mit umgerechnet 4,84 Mio. US-Dollar liegen die Kosten bei den untersuchten Unternehmen hierzulande über dem weltweiten Durchschnitt von 4,24 Millionen US-Dollar pro Vorfall. Zu diesen Ergebnissen kommt die neueste „Cost of a Data Breach“-Studie des Ponemon-Instituts, die von IBM Security gesponsert und ausgewertet wird. Dabei handelt es sich um den höchsten gemessenen Wert seit Beginn der Erhebung vor 17 Jahren.

Weltweit haben Unternehmen im Report des letzten Jahres pandemiebedingt bereits höhere Security-Ausgaben erwartet, nun zeigt sich, dass sie damit richtiglagen. Die schnelle Umstellung auf Home Office und andere Formen der Distanzarbeit scheint zu teureren Datenvorfällen geführt zu haben. In Deutschland erhöhten sich die Kosten pro kompromittiertem Datensatz (z.B. persönlich identifizierbare Informationen, wie etwa Kreditkartendaten) um 8 Euro auf 170 Euro, die Gesamtkosten pro Datenvorfall erhöhten sich um 0,6 Mio. Euro (Vorjahr: 4,05 Mio. Euro).

Die Ergebnisse der Studie zeigen, wie sehr das Thema IT-Security weltweit durch die Turbo-Digitalisierung ins Hintertreffen geraten ist: 60 Prozent der Unternehmen migrierten während der Pandemie in die Cloud. Das Thema Sicherheit spielte dabei eine zweitrangige Rolle. Cloud-Security ist aber auch schon während der Migration wichtig: Datenvorfälle, die sich während eines Cloud-Migrationsprojekts zutrugen, kosteten fast 19 Prozent mehr. Weniger Kosten hatten diejenigen der untersuchten Unternehmen, die einen hybriden Cloud-Ansatz verfolgen: Sie zahlten 3,61 Mio. US-Dollar pro Vorfall – im Gegensatz zu 4,80 Mio. US-Dollar bei primär öffentlichem Cloud-Ansatz und 4,55 Mio. US-Dollar bei einem primären Private-Cloud-Ansatz.

Es gibt jedoch auch positive Nachrichten. 2020 dauerte die Identifizierung und Eindämmung einer Datenschutzverletzung in Deutschland im Durchschnitt 151 Tage (dabei entfallen 123 Tage auf die Erkennung und 28 auf die Eindämmung) und damit neun Tage weniger als im Vorjahr. Damit steht Deutschland im internationalen Durchschnitt gut da, denn der liegt bei 287 Tagen (212 Tage zur Erkennung, 75 zur Eindämmung). Zur Verdeutlichung: Bei diesem Tempo ist eine Datenschutzverletzung, die sich am 1. Januar ereignet, erst am 14. Oktober abgeschlossen – deutsche Unternehmen hingegen hätten den Vorgang bereits am 1. Juni abgeschlossen. Das ist auch deshalb wichtig, weil die Kosten mit zunehmender Dauer des Vorfalls stark steigen.

„Höhere Kosten für Datenverstöße sind eine weitere zusätzliche Ausgabe für Unternehmen im Zuge des schnellen technologischen Wandels während der Pandemie“, sagt Chris McCurdy, Vice President and General Manager, IBM Security. „Während die Kosten für Datenpannen im vergangenen Jahr ein Rekordhoch erreicht haben, zeigt der Bericht auch positive Anzeichen für die Auswirkungen moderner Sicherheitstaktiken wie KI, Automatisierung und die Einführung eines ‚Zero-Trust‘-Ansatzes – was sich in Zukunft bei der Reduzierung der Kosten für diese Vorfälle auszahlen könnte.“ 85 Prozent der befragten deutschen Unternehmen gaben an, einen ‚Zero-Trust‘-Ansatz ganz (46 Prozent) oder teilweise (39 Prozent) implementiert zu haben.

Eine Auswahl weiterer Studienergebnisse:

- **Betriebliche Veränderungen als Kostentreiber: Untersuchte Unternehmen in** Branchen, die pandemiebedingt mit großen betrieblichen Veränderungen konfrontiert waren (Gesundheitswesen, Einzelhandel, Gastgewerbe und Herstellung/Vertrieb von Konsumgütern) verzeichneten einen erheblichen Anstieg der Kosten für Sicherheitsvorfälle. Beispiel Gesundheitswesen: Hier steigen die Kosten für Datenverletzungen auf 9,23 Mio. US-Dollar pro Vorfall, wodurch die Branche im internationalen Durchschnitt zur teuersten überhaupt wird. In Deutschland verzeichneten dagegen die Sektoren Finanzen, Industrie und Technologie die höchsten Kosten für Sicherheitsvorfälle.
- **Das Geschäft leidet am meisten:** Mit 38 Prozent machen Geschäftsausfälle im internationalen Vergleich den größten Teil der Kosten eines Datenvorfalls aus. Das sind durchschnittlich 1,59 Mio. US-Dollar an entgangenem Geschäft. Darunter fallen erhöhte Kundenfluktuation, entgangene Umsätze aufgrund von Systemausfällen und die steigenden Kosten für die Akquise. In Deutschland stellen diese Kosten mit 1,29 Mio. Euro jedoch „nur“ den zweitgrößten Posten, während „Erkennung und Eskalation“ mit 1,41 Mio. Euro zu Buche schlagen.
- **Meiste Angriffe durch gestohlene Anmeldeinformationen:** 20 Prozent der untersuchten Sicherheitsverletzungen waren auf kompromittierte Anmeldeinformationen zurückzuführen. Hier dauerte auch die Erkennung mit durchschnittlich 250 Tagen am längsten (im Vergleich zu 212 Tagen bei einer durchschnittlichen Sicherheitsverletzung). In Deutschland liegt dieser Wert mit 21 Prozent leicht über dem Durchschnitt, die höchsten Kosten werden allerdings durch kompromittierte

Geschäfts-E-Mails verursacht.

- **Sicherheitsautomatisierung in Unternehmen steigt**: Die teilweise oder vollständige Automatisierung von Sicherheitslösungen stieg um 13 Prozent im Vergleich zum Vorjahr (65 Prozent vs. 52 Prozent im Vorjahr) – für die untersuchten Unternehmen sanken auch die Kosten pro Vorfall auf 2,90 Mio. US-Dollar. KI, Sicherheitsanalysen und Verschlüsselung sparten zwischen 1,25 und 1,49 Mio. US-Dollar im Vergleich zu Datenpannen, bei denen diese Technologien nicht in nennenswertem Umfang eingesetzt wurden. 66 Prozent der befragten deutschen Unternehmen hatten Sicherheitsautomatisierungen ganz oder teilweise umgesetzt, 26 Prozent bezeichneten die Einführung als abgeschlossen.

Die siebzehnte „Cost of a Data Breach"-Studie von IBM Security und dem Ponemon-Institut basiert auf einer detaillierten Analyse realer Datenschutzverletzungen, die zwischen Mai 2020 und März 2021 bei über 500 Unternehmen weltweit aufgetreten sind. Aus Deutschland haben 35 Unternehmen an der Studie teilgenommen.

Mehr Informationen und Studienergebnisse finden Sie in der ausführlichen US-Originalmeldung: https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

Die komplette **„Cost of a Data Breach"-Studie 2021** können Sie hier herunterladen: ibm.com/databreach.

Bei Interesse können Sie sich auch für das kostenlose Webinar zur Studie anmelden. Es findet am 18. August 2021 um 17:00 Uhr CEST statt. Zur Anmeldung geht es unter ibm.biz/CODBwebinar.

Über IBM Security

IBM Security bietet eines der fortschrittlichsten und integriertesten Portfolios an Produkten und Dienstleistungen für die Unternehmenssicherheit. Das Portfolio, das von der weltweit agierenden IBM X-Force®-Forschung unterstützt wird, ermöglicht es Unternehmen, Risiken effektiv zu managen und sich gegen neue Bedrohungen zu schützen. IBM betreibt eine der weltweit größten Forschungs-, Entwicklungs- und Serviceorganisationen für Sicherheit, überwacht 150 Milliarden Sicherheitsereignisse pro Tag in mehr als 130 Ländern und hält weltweit mehr als 10.000 Sicherheitspatente. Weitere Informationen finden Sie unter www.ibm.com/security, folgen Sie @IBMSecurity auf Twitter oder besuchen Sie den IBM Security Intelligence Blog.

For further information: Dagmar Domke, IBM Unternehmenskommunikation, Telefon: +49-170-480-8228, dagmar.domke@de.ibm.com