

Nichtstun bringt große Risiken mit sich: Ist Ihr Unternehmen geschützt?



Schauen wir genauer hin.

4,45 Millionen USD

Datenschutzverletzungen werden immer teurer.

In den letzten drei Jahren ist ein Anstieg um 15 % zu verzeichnen, sodass sich die weltweiten Durchschnittskosten einer Datenschutzverletzung im Jahr 2023 auf 4,45 Millionen US-Dollar belaufen.

Irren ist menschlich – und unter Umständen teuer für Ihr Unternehmen.

80%

dieser Datenschutzverletzungen haben als Ursache kompromittierte Zugangsdaten.¹

83%

der Unternehmen erlebten mehr als eine Datenschutzverletzung im Jahr 2022.²

4,76 Mio. USD

durchschnittliche Gesamtkosten einer Datenschutzverletzung aufgrund von Phishing.

4,62 Mio. USD

durchschnittliche Gesamtkosten einer Datenschutzverletzung aufgrund von kompromittierten Zugangsdaten.

183 USD pro Datensatz

Personenbezogene Daten sind ein begehrtes, da wertvolles Ziel.

Die am häufigsten betroffene Art von Daten sind personenbezogene Kundendaten – in 52 % der Datenschutzverletzungen.

Kosten eines Datensatzes: 183 US-Dollar.



Geschäftskonten sind tendenziell unsicherer, denn Angestellte tun sich mit Passwortverwaltung schwer.

Nur 33 % der Arbeitskräfte erstellen starke Passwörter für beruflich genutzte Konten.³

„Zu Viele Passwörter“

sind für mehr als ein Drittel der großen Unternehmen ein Problem.⁴



Die durchschnittlichen Gesamtkosten einer Datenschutzverletzung aufgrund kompromittierter geschäftlicher E-Mail-Konten belaufen sich auf 4,67 Mio. USD.

4,95 Millionen USD

Rasches Handeln ist das A und O.

Die durchschnittlichen Kosten eines Datenlecks, das mehr als 200 Tage andauert, belaufen sich auf 4,95 Millionen USD.

328 Tage

Die durchschnittliche Anzahl der Tage, um Datenschutzverletzungen aufgrund gestohlener oder kompromittierter Zugangsdaten zu erkennen und einzudämmen.

Ein Passwort-Manager der Enterprise-Klasse

kann Unternehmen dabei helfen, sich vor kostspieligen Datenschutzverletzungen zu schützen.



VERMEIDEN

Keine Wiederverwendung von Passwörtern mehr



STEUERN

Zentrale Passwortverwaltung



SCHÜTZEN

Schutz für sensible Daten der Angestellten



TEILEN

Einfache und sichere Passwortfreigabe

LastPass erhöht den Komfort für Mitarbeiter sowie die

Kontrolle und Transparenz



Mit mehr als einer Milliarde geschützter Websites, 33 Mio. Benutzern und 100.000 Geschäftskunden macht LastPass die Online-Sicherheit einfach.



Die Zukunft ist passwortlos

Schützen Sie jede Identität mit LastPass.

LastPass kontaktieren

Quellen:

(1) Data Breach Investigations Report von Verizon, 2021

(2) LastPass und OnePoll, 2021

(3) Psychologie der Passwörter, 2021

(4) IDC-InfoBrief im Auftrag von LastPass: Future of Work mit EPM, Identitäts- und Zugriffskontrollen ermöglichen, #EUR148370521, 23. Februar 2022

<https://www.ibm.com/reports/data-breach>