LastPass

Haben Sie eine lückenlose Cybersicherheitsstrategie?

Der digitale Fußabdruck von Unternehmen wächst. Ihre Mitarbeiter müssen immer mehr Zugangsdaten verwalten …

70 % der Nutzer verbrachten mehr Zeit online als im Jahr davor und erstellten um 50 % mehr Konten.[1]

„Zu viele Passwörter" sind für 36 % der großen Unternehmen ein Problem.[2]

… doch unsichere Passwortgewohnheiten verhindern Fortschritte bei der Cybersicherheit und unterminieren die diesbezügliche Strategie von Unternehmen.

85 % der Datenschutzverletzungen basieren auf gedankenlosem und fehlerhaftem Handeln, das Phishing und den Diebstahl von Zugangsdaten begünstigt.[3]

65 % der Nutzer verwenden (fast) immer dasselbe Passwort oder Varianten davon.[4]

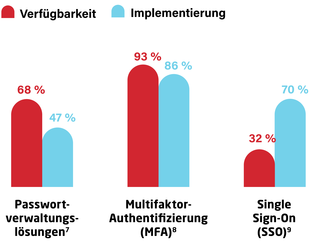
Sind Sie bereit für Ihre ersten Schritte mit LastPass Business? **Mehr erfahren**

IT-Verantwortliche wissen: Passwörter sind vor dem Hintergrund zunehmender Datenschutzverletzungen eine ernstzunehmende Gefahr für das Unternehmen.

89 % der IT-Verantwortlichen geben der Eindämmung passwortbedingter Risiken einen sehr hohen bis hohen Stellenwert.[5]

Die durchschnittlichen globalen Gesamtkosten eines Datenlecks beliefen sich 2021 auf 4,24 Millionen US-Dollar. Am **stärksten stieg der Wert in den letzten sieben Jahren (10 %).**[6]

Große Unternehmen implementieren verfügbare Lösungen für das Identitäts- und Zugriffsmanagement nicht konsistent. Das schafft Sicherheitslücken und begünstigt Datendiebstahl.



MFA an jedem Zugriffspunkt ist zu umständlich.
Sich bei jeder App authentifizieren zu müssen, ist für Mitarbeiter stressig und hinderlich. Es untergräbt die Akzeptanz der Lösung.

Ein reines SSO-Konzept deckt nicht jeden Login ab.
Nicht all Apps und Webservices sind mit SAML (Security Assertion Markup Language) kompatibel – der Technik, auf der SSO basiert.

Wie schließen Sie diese Lücken und verhindern das Eindringen von Datendieben in Ihr Unternehmen?

PASSWORT-MANAGEMENT AUF ENTERPRISE-NIVEAU

MFA für zentrale Apps und sichtbare Zugriffspunkte

SSO für häufig genutzte Konten

Ein Passwort-Manager für den Rest

LastPass Business bietet Arbeitskräften ein reibungsloses Nutzungserlebnis und erhöht die Kontrolle und Transparenz für die IT-Abteilung – mit einem speziell für Unternehmen entwickelten Passwort-Manager, der einfach zu verwalten und zu bedienen ist.

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

Mehr erfahren

Quellen:
1 LastPass-Bericht zur Psychologie der Passwörter 2021
2 IDC-Infobrief im Auftrag von LastPass: „Die Zukunft der Arbeit mit EPM, Identitätsverwaltung und Zugriffssteuerung" #EUR148370521, 23. Februar 2022
3 2021 Verizon DBIR
4 LastPass-Bericht zur Psychologie der Passwörter 2021
5 IDG-Umfrage bei Unternehmen 2022
6 Bericht „Kosten einer Datenschutzverletzung", IBM und Ponemon Institute, 2021
7 IDG-Umfrage bei Unternehmen 2022
8 Ibid
9 Ibid.

04.28.2022/PDF/GOTO0251