LastPass •••|

DATENBLATT: LASTPASS BUSINESS

Sichere Passwort-verwaltung im gesamten Unternehmen

Ein Passwort-Manager sollte alle Mitarbeiter abdecken – nicht nur bestimmte Abteilungen oder Personen.

Wenn Sie einen Passwort-Manager nur in einzelnen Abteilungen einführen, räumt das Risiken und Schwachstellen nicht aus dem Weg – im Gegenteil. Arbeitskräfte verbringen heutzutage mehr als 70 Prozent ihrer Zeit online; ihre digitale Präsenz ist größer denn je. Dazu kommt, dass Passwörter immer öfter wiederverwendet werden: 92 Prozent der Internetnutzer wissen, dass es riskant ist, dasselbe oder ein ähnliches Passwort mehrmals zu verwenden, aber 65 Prozent tun es trotzdem.* Wenn Sie Mitarbeiter nicht mit den richtigen Tools ausstatten, lässt sich schlechtes Passwortverhalten den besten Sicherheitsmaßnahmen zum Trotz nicht ausmerzen.

Betrachten Sie Passwörter als eine Art Generalschlüssel, der jede Tür zu Ihrem Unternehmen öffnet – egal, ob diese Tür jeden Tag oder nur einmal im Jahr in Gebrauch ist. Und während Arbeitskräfte immer mobiler werden, kommen neue Türen hinzu. Laut einer Studie eröffneten Internetnutzer im Jahresvergleich beispielsweise um 50 Prozent mehr Online-Konten, aber nur 32 Prozent der beruflich genutzten Konten waren mit einem starken Passwort geschützt.

Wenn Mitarbeiter schwache oder wiederverwendete Passwörter erstellen, verwalten oder untereinander austauschen, ist der Schlüssel zu Ihrem Unternehmen in Gefahr. Die Lösung? Eine LastPass-Standortlizenz für Ihre gesamte Belegschaft, damit Passwörter kein leidiges Thema mehr sind und die allgemeine IT-Sicherheit erhöht wird.

Sichere und effiziente Zusammenarbeit

Bei LastPass können Ihre Mitarbeiter anderen Personen in Echtzeit sicheren Zugriff auf einzelne Konten oder freigegebene Ordner gewähren, um Konten sowohl intern als auch extern gemeinsam zu nutzen. Natürlich lässt sich der Zugriff jederzeit wieder aufheben. Wird das freigegebene Konto vom LastPass-Vault aus aufgerufen, kann das Passwort selbst sogar verborgen bleiben. Eine effiziente Zusammenarbeit war noch nie einfacher – und sicherer.

Adieu, Sicherheitslücken: LastPass ist in vorhandene Technologien integrierbar

Oft wird angenommen, dass eine einzelne Security-Lösung das gesamte Unternehmen schützt, aber eine SSO-Lösung deckt beispielsweise nur einen Teil der Apps ab. Häufig wird Single Sign-On zum Schutz von Business-Apps wie Workday oder Slack eingesetzt. Aber was ist, wenn Ihre Mitarbeiter ihre Firmengeräte auch privat verwenden oder umgekehrt? Ein Passwort-Manager lässt sich in Ihre vorhandenen Lösungen integrieren oder kann sie ergänzen, sodass jeder Zugriffspunkt optimal geschützt ist.

*LastPass-Bericht 2021 zur Psychologie der Passwörter

Unternehmensweite Implementierung: große Ersparnisse und mehr Unterstützung

Bei einer LastPass-Standortlizenz erhält jeder Mitarbeiter ein LastPass-Business-Konto, wobei eine Pauschalgebühr und kein benutzerbasierter Tarif verrechnet wird. So kann LastPass flexibel mit Ihrem Unternehmen mitwachsen, ohne dass zusätzliche Kosten anfallen. Auf Wunsch steht Ihnen auch ein Customer Success Manager (CSM) bei der Implementierung zur Seite. Jeder LastPass-Business-Kontoinhaber hat außerdem Anspruch auf ein kostenloses Families-Konto: ein privates Konto, das mit fünf weiteren Konten für Verwandte oder Freunde verknüpft ist.

Sichere Passwortverwaltung für alle: einige häufige Anwendungsbereiche im Überblick

IT	Zum Schutz der Technologien und Sicherheitsinfrastruktur des Unternehmens sowie zur Aufrechterhaltung des Betriebs müssen IT-Teams eine große Anzahl von Passwörtern verwalten. Ob Serverwartung oder administrative Aufgaben, sie benötigen eine einfache Lösung zur Absicherung und gemeinsamen Nutzung von Zugangsdaten. Nur so können sie den Schutz wichtiger Firmendaten gewährleisten, das Onboarding neuer Mitarbeiter beschleunigen und technische Probleme verhindern.
Vertrieb und Business Development	Die von diesen Teams eingesetzten Tools umfassen Kundenmanagementservices, Demo-Logins und Automatisierungssoftware, um die Beziehungen zu Kunden und Lieferanten besser zu verwalten. Da Vertriebsmitarbeiter tendenziell viel unterwegs sind und auf Mobilgeräten in den verschiedensten WLANs arbeiten, sind sie außerdem online größeren Gefahren ausgesetzt.
Marketing	Marketingteams verwenden Websites und Tools für PR-Arbeit, Kampagnen und die Datenanalyse, und arbeiten häufig mit externen Anbietern von Marketingdienstleistungen zusammen. Eine kürzlich von Gartner durchgeführte Studie ergab, dass Marketingabteilungen mehr für Technologie ausgeben als IT-Abteilungen. Häufig teilen sich die Teammitglieder eine einzige Lizenz für ihre Tools.
Social Media	Social-Media-Teams betreuen oft Dutzende (oder gar Hunderte) Social-Media-Konten und verwenden Tools für die Inhaltserstellung und -verbreitung sowie die Datenanalyse. Viele dieser Dienste unterstützen Single Sign-On mit SAML oder die Verbundanmeldung nicht; vor allem, wenn Logins von mehreren Personen gemeinsam genutzt werden.
Technik/ Entwicklung	Als Lebensader vieler Produkte müssen Mitglieder des Technik-/Entwicklungsteams vertrauliche Unterlagen untereinander austauschen und mit internen und externen Tools und Teams arbeiten, um Produktupdates oder neue Versionen fristgerecht bereitzustellen.
Personal-verwaltung	HR-Teams benötigen in der Regel Softwaretools, um die Einstellung neuer Arbeitskräfte, die Gehaltsabrechnung, Mitarbeitervergünstigungen oder die Leistung und Anwesenheit der Belegschaft zu managen. Wenn neue Teammitglieder dazustoßen oder bestehende das Unternehmen verlassen, müssen sie umgehend in das Benutzerverzeichnis aufgenommen bzw. daraus entfernt werden.
Finanzen/ Buchhaltung/ Rechtswesen	Finanz-, Buchhaltungs- und Rechtsabteilungen nutzen Softwaretools, um Budgets, Einnahmen, Ausgaben, Kredit- und andere Zahlungskarten, elektronische Signaturen und die strategische Entscheidungsfindung zu verwalten – einige der vertraulichsten Daten von Unternehmen.
Support/ Kundenservice	Diese Teams verwenden in der Regel Tools zur Verwaltung von Helpdesk-Tickets, Fehlerberichten und der Fehlerüberwachung sowie zur Produktprüfung und Problemlösung. Mitarbeiter benötigen oft von jedem Ort aus sofort Zugriff. Ein Passwort-Manager verfügt über die passenden Richtlinien dafür.
Alle anderen	Consultants, Praktikanten, Büroleiter, Operations Manager – die Liste ist lang. Ob Einzelpersonen oder ganze Abteilungen, ob große oder kleine Teams, alle müssen sicher mit anderen zusammenarbeiten können. Das heißt: Alle benötigen einen Passwort-Manager.

LastPass kontaktieren

Lassen Sie nicht zu, dass ein einziges wiederverwendetes Passwort Ihr gesamtes Unternehmen gefährdet.