LastPass •••|

Die wichtigsten Fakten über die Sicherheit von LastPass

Bei LastPass hat die Sicherheit oberste Priorität. Unser Passwort-Manager wurde speziell für den Schutz Ihrer Passwörter und anderer wichtiger Informationen entwickelt. Sie können daher beruhigt sein, dass Ihre vertraulichen Daten bei LastPass sicher sind. Wir setzen unter anderem folgende Sicherheitsmaßnahmen ein:

- **Ein bewährtes Sicherheitsmodell,** das in puncto Transparenz und Best Practices den Ton angibt.
- **Lokale Verschlüsselung,** die sensible Informationen vor der Synchronisation mit LastPass unkenntlich macht.
- **Leistungsfähige Sicherheitsmerkmale,** die Sie vor Bedrohungen und Angriffen schützen.

Im Folgenden finden Sie grundlegende Informationen dazu, wie LastPass Daten verschlüsselt, unseren Dienst noch robuster macht und Ihre Sicherheit maximiert.

Bewährtes Sicherheitsmodell

Wir schützen unsere Infrastruktur, indem wir Best Practices nutzen und regelmäßige Systemupgrades vornehmen. Darüber hinaus sind unsere Rechenzentren vollkommen redundant aufgebaut, was die Gefahr von Ausfällen oder eines Single Point of Failure minimiert. In der Praxis hat sich LastPass mittlerweile bei mehr als 32.000 Firmenkunden etabliert – von Fortune-500-Unternehmen bis hin zu führenden Technologieanbietern. Unsere Kunden verlassen sich nicht zuletzt wegen unseres bewährten Sicherheitsmodells auf LastPass:

- **Die SOC-2-Compliance nach Typ II, die sogenannte Service Organization Control 2 (SOC 2) Type II compliance:** Nur wenige Passwortmanager verfügen über die SOC-2-Compliance nach Typ II, die eine detaillierte Überprüfung und Validierung unserer Kontrollen und Prozesse darstellt und bestätigt, dass unsere Produkte und Systeme auf Sicherheit und Zuverlässigkeit ausgerichtet sind. SOC 2 gilt weitgehend als „Goldstandard" für Softwareanbieter, und das regelmäßige Durchlaufen des SOC-2-Verfahrens ist einer der vielen Beweise für unser Engagement in Sachen Sicherheit und Verfügbarkeit der Dienste.
- **Regelmäßige Audits und Penetrationstests:** Wir beauftragen vertrauenswürdige, unabhängige Sicherheitsfirmen der Spitzenklasse damit, den LastPass-Dienst und unsere Infrastruktur routinemäßigen Prüfungen und Tests zu unterziehen. Alle LastPass-Server werden täglich auf Schwachstellen untersucht, detaillierte interne Penetrationstests erfolgen vierteljährlich.
- **TLS für die sichere Datenübertragung:** Obwohl sensible Daten bereits mit AES-256 verschlüsselt sind, sichert dieses TLS-Protokoll die Verbindung mit LastPass und schützt so die Benutzerdaten zusätzlich vor Man-in-the-Middle-Angriffen, bei denen der Datenverkehr im Netzwerk von anderen Personen abgefangen wird.
- **Bug-Bounty-Programm:** LastPass hat gute Kontakte zu Experten im Bereich der Sicherheitsforschung aufgebaut. Wir wissen ihre Arbeit sehr zu schätzen, da sowohl unser Produkt als auch unsere Kunden von ihrer Aufmerksamkeit profitieren. Unser Bug-Bounty-Programm gibt Sicherheitsforschern Anreize, gefundene Mängel und Schwachstellen auf verantwortungsbewusste Weise zu melden, sodass wir die nötigen Verbesserungsmaßnahmen ergreifen können: https://bugcrowd.com/lastpass
- **Zuverlässige Dienste:** Um für Redundanz zu sorgen, operiert LastPass auf mehreren, geografisch verteilten Einrichtungen, wovon jede den Datenverkehr der Kunden bewältigen kann.
- **Transparente Reaktion auf Vorfälle:** Wenn uns Fehler oder Schwachstellen gemeldet werden, reagiert unser Team sofort, um diese gemäß unserem Incident-Response-Plan zu untersuchen, zu überprüfen und zu beheben. Wir bitten unsere Community, unsere Technologien auf den Prüfstand zu stellen, wir reagieren schnell und wir verfolgen eine transparente Kommunikation – damit haben wir uns das Vertrauen der Community erarbeitet.

Sichere Produktarchitektur

Die Sicherheit Ihres Kontos muss vom ersten Moment an gewährleistet sein. Wenn Sie Ihr Master-Passwort für LastPass anlegen, generieren wir daraus einen eindeutigen Verschlüsselungsschlüssel, der nur für Sie gilt. Das Master-Passwort und der Schlüssel verlassen Ihr Gerät nie und werden unter keinen Umständen an LastPass gesendet oder weitergegeben. Ohne diesen Schlüssel sind die verschlüsselten Daten bedeutungslos. LastPass wurde dafür entwickelt, um Ihre sensiblen Daten zu schützen, und zwar mit Hilfe dieser Best Practices:

- **Endpunktverschlüsselung:** Bei LastPass kann nur der User seinen Vault entschlüsseln und darauf zugreifen. Die Verschlüsselung erfolgt ausschließlich auf Geräteebene; nicht auf den Servern von LastPass. Das heißt, Ihre vertraulichen Daten werden bereits verschlüsselt mit LastPass synchronisiert, bevor sie dort sicher gespeichert werden.
- **256-Bit-AES-Verschlüsselung:** Dieser Algorithmus gilt allgemein als nicht zu brechen und wird von Banken und dem US-Militär zur Verschlüsselung eingesetzt.
- **PBKDF2-SHA256 gegen Brute-Force-Angriffe:** PBKDF2 sorgt dafür, dass Ihr Master-Passwort und der Schlüssel zusätzlich vor groß angelegten Brute-Force-Angriffen geschützt werden, indem die benötigte Zeit für einen einzigen Versuch, das Passwort zu erraten, um ein Wesentliches verlängert wird. LastPass verwendet SHA-256, einen langsameren Hash-Algorithmus, und verarbeitet die Eingabe bei der Schlüsselerstellung in 5000 Runden PBKDF2, bevor der Login-Hash des Users generiert wird. Durch die Verlangsamung von Brute-Force-Angriffen macht PBKDF2 den Versuch, nur ein einziges Master-Passwort zu knacken, sehr schwierig.
- **Persönliches Master-Passwort:** Unsere beste Sicherheitsmaßnahme ist die, dass wir schlicht und einfach keinen Zugriff auf vertrauliche Daten in Ihrem Vault haben. LastPass überträgt oder speichert Ihr Master-Passwort nie. Unsere Logik ist: Wenn LastPass nicht auf Ihre Daten zugreifen kann, dann können das Hacker auch nicht.

Leistungsfähige Sicherheitsmerkmale

Wir gehen nicht nur in Sachen Datenschutz weit über das Notwendige hinaus. Wir bieten unseren Kunden auch die Möglichkeit, selbst Einfluss auf ihre Sicherheit zu nehmen, indem wir sowohl die Sicherheit ihres Kontos als auch die Sicherheit im Allgemeinen anhand von dafür vorgesehenen Funktionen verbessern. Diese umfassen:

- **Multifaktor-Authentifizierung:** Ein verpflichtender zweiter Anmeldeschritt, bevor Sie Zugriff erhalten, erhöht die Sicherheit. LastPass Authenticator ermöglicht eine Verifizierung per Push-Benachrichtigung und erzeugt so ein sicheres und optimiertes Nutzungserlebnis. Wir arbeiten darüber hinaus mit führenden Anbietern für Authentifizierungslösungen zusammen.
- **Steuerungsmöglichkeiten für Unternehmen:** Mehr als 100 konfigurierbare Richtlinien helfen Ihnen beim Aufbau einer Sicherheitsumgebung, die sowohl auf globaler als auch individueller Ebene ganz an Ihre Wünsche und Bedürfnisse angepasst ist, beispielsweise indem Zugriffe nur aus vertrauenswürdigen Umgebungen zugelassen werden. Das Dashboard für Administratoren gibt Einblick in die Passwortsicherheit im gesamten Unternehmen.
- **Automatische Sperre:** Wenn Sie Ihren Schreibtisch verlassen oder eines Ihrer Geräte gar verloren geht, kann LastPass Sie automatisch abmelden, um Ihre Daten vor fremden Blicken zu schützen.
- **Passwortprüfung:** Sie können die Passwörter in Ihrem Vault einer Prüfung unterziehen, um schwache, mehrmals verwendete, kompromittierte und alte Passwörter zu identifizieren und zu ersetzen.
- **Schutz vor Phishing-Angriffen:** LastPass gibt Ihre Passwörter nur auf den von Ihnen gespeicherten und als vertrauenswürdig gekennzeichneten Websites ein.

Nähere technische Details und weitere Informationen zu unserem Sicherheitsmodell finden Sie im technischen Whitepaper von LastPass.