TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN FÜR LASTPASS

Betriebliche Datenschutz- und Datensicherheitskontrollen

Datum der Veröffentlichung: Februar 2022

1 Produkte und Services

In diesem Dokument werden die technischen und organisatorischen Maßnahmen (TOMs) für LastPass beschrieben. LastPass ist eine Passwortverwaltungs- und SSO-Lösung (Single Sign-On), die es Anwendern ermöglicht, ihre Benutzerkennungen und Zugangsdaten für Online-Anwendungen und Websites sicher zu speichern, zu erstellen und abzurufen.

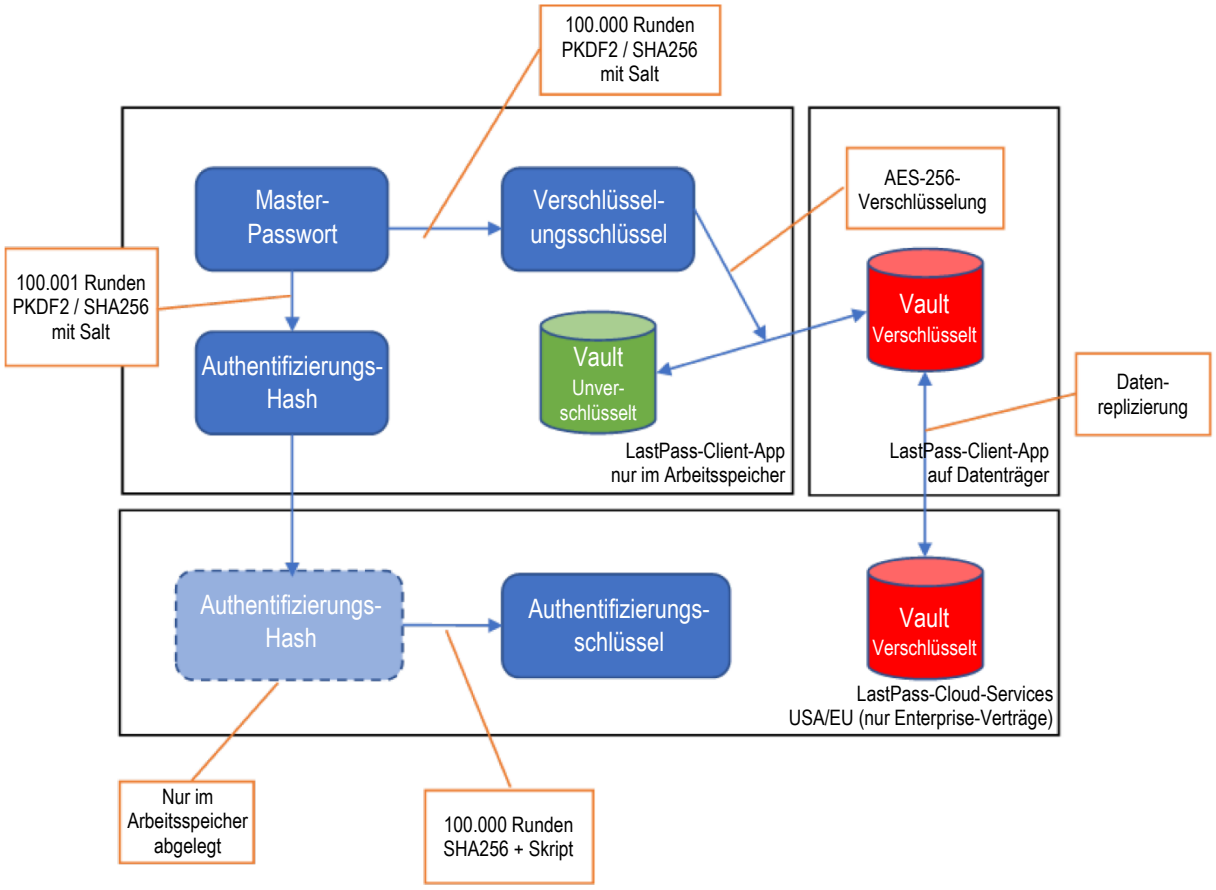
LastPass Enterprise: Zusätzlich zu den bereits vorhandenen branchenführenden Passwortverwaltungsfunktionen verfügt LastPass Enterprise jetzt über eine Single Sign-On-Technologie (SSO) mit über 1.200 vorinstallierten Apps. Somit können Sie mit LastPass Enterprise jeden Eintrittspunkt mit einer einzigen Lösung verwalten.

LastPass Multi-Factor Authentication (MFA): Diese Lösung geht über eine standardmäßige Zwei-Faktor-Authentifizierung (2FA) hinaus. LastPass MFA stellt sicher, dass ausschließlich die richtigen Benutzer zur richtigen Zeit auf die richtigen Daten zugreifen – ohne unnötige zusätzliche Komplexität. Durch die Kombination von biometrischen Faktoren wie Gesicht und Fingerabdruck mit kontextbezogenen Faktoren wie Standort und IP-Adresse bietet LastPass MFA eine intuitive und für Mitarbeiter unkomplizierte Authentifizierung, die von Administratoren schnell und einfach für Cloud-Apps, ältere und lokal installierte Apps sowie VPN zur Verfügung gestellt werden kann.

LastPass Identity: LastPass Identity ist eine Kombination aus LastPass Enterprise und LastPass MFA. Über ein zentrales Dashboard werden Passwörter, Authentifizierungen und alle derzeit genutzten Anwendungen erfasst, sodass ein unternehmensweiter Überblick über alle Endbenutzeraktivitäten möglich wird.

2 Produktarchitektur

Der LastPass-Service umfasst einen Vault, in dem vertrauliche Benutzerdaten gespeichert werden. Zudem macht er sich ein Zero-Knowledge-Framework zunutze. Der Zugriff darauf ist nur durch Eingabe des Master-Passworts des Benutzers möglich, das nicht in unverschlüsselter Form von LastPass aufbewahrt wird. LastPass kann dieses Master-Passwort weder speichern noch abrufen. Benutzereingaben über die LastPass-Web- oder Mobilgeräte-App sind auf dem Benutzergerät mit dem eindeutigen Schlüssel des Benutzers verschlüsselt, und die mit AES-256 verschlüsselten Daten werden zur sicheren Speicherung mit LastPass synchronisiert. Der Benutzer kann die eigenen Daten bei Bedarf mithilfe des Master-Passworts abrufen und entschlüsseln. Dies erfolgt vollständig auf Benutzer- und Geräteebene.



Die LastPass-Infrastruktur ist darauf ausgelegt, die Service-Verfügbarkeit zu erhöhen und das Risiko von Ausfällen aufgrund eines Single Point of Failure zu reduzieren. Je nach der gewählten Datenspeicherort-Einstellung (diese wird bei der Kontoerstellung festgelegt) kommt dabei Folgendes zum Einsatz: (a) redundante Aktiv/Passiv-Rechenzentren in den USA oder Europa oder (b) erstklassige, von Cloud-Hosting-Anbietern bereitgestellte Rechenzentren in Australien, Singapur, Indien oder Kanada. Alle Rechenzentren befinden sich an Cloud- oder Co-Location-Einrichtungen, in denen die Umweltbedingungen überwacht werden und rund um die Uhr physische Sicherheit geboten wird.

Zudem ist mit LastPass der Offline-Zugriff möglich. Das bedeutet, dass ein Benutzer, der nicht mit dem Internet verbunden ist, über die LastPass-Browsererweiterung oder -Mobilgeräte-App noch auf eine Version seines verschlüsselten Vaults zugreifen kann (diese Version wurde nach der letzten Anmeldung des Benutzers auf seinem Gerät zwischengespeichert). Weitere Informationen zur LastPass-Architektur finden Sie im technischen Whitepaper zu LastPass.

3 LastPass – technische Kontrollen

LastPass nutzt technische Sicherheitskontrollen nach Branchenstandard gemäß der Art und Weise und des Umfangs der Services (gemäß Definition des Begriffs in den Nutzungsbedingungen). Diese Kontrollen wurden zum Schutz der Service-Infrastruktur und der darin enthaltenen Daten entwickelt. Sie finden die Nutzungsbedingungen unter https://www.goto.com/company/legal/terms-and-conditions.

3.1 Logische Zugriffskontrolle

Es werden logische Zugriffskontrollverfahren eingesetzt, um die durch nicht autorisierten Anwendungszugriff entstehenden Bedrohungen sowie Datenverlust in Unternehmens- und Produktionsumgebungen zu verhindern oder zu minimieren. Mitarbeiter erhalten bei Bedarf minimalen Zugriff (oder „Least Privilege“-Zugriff) auf angegebene LastPass-Systeme, -Anwendungen, -Netzwerke und -Geräte. Zudem sind Benutzerrechte basierend auf der funktionalen Rolle und Umgebung voneinander getrennt.

3.2 Perimeterverteidigung und Erkennung von Eindringversuchen

LastPass setzt branchenübliche Tools, Techniken und Services für den Perimeterschutz ein. Diese sollen verhindern, dass nicht autorisierter Netzwerkdatenverkehr in die Produktinfrastruktur gelangt. Dazu gehören unter anderem folgende Tools:

- Systeme zur Erkennung von Eindringversuchen, mit denen Systeme, Dienste, Netzwerke und Anwendungen auf unbefugte Zugriffe überwacht werden
- Überwachung wichtiger System- und Konfigurationsdateien, um die Wahrscheinlichkeit unbefugter Änderungen zu verhindern bzw. zu reduzieren
- Eine gehostete und/oder cloudbasierte Application-Firewall und ein DDoS-Angriffsschutz auf Anwendungsebene, bei dem der LastPass-Datenverkehr über einen Proxy geleitet wird, um schädlichen Serververkehr abzuwehren
- Eine lokale Firewall auf Anwendungsebene, die zusätzlichen Schutz vor den Top-Ten-OWASP-Bedrohungen sowie vor anderen Schwachstellen von Webanwendungen und vor schädlichem Verkehr bietet
- Host-basierte Firewalls auf LastPass-Webservern, die ein- und ausgehende Verbindungen filtern, einschließlich interner Verbindungen zwischen LastPass-Systemen.

3.3 Datentrennung

LastPass nutzt eine mehrinstanzenfähige Architektur, die basierend auf dem LastPass-Konto eines Benutzers oder einer Organisation logisch auf Datenbankebene getrennt ist. Nur authentifizierten Parteien wird Zugriff auf die relevanten Konten gewährt.

3.4 Physische Sicherheit

LastPass arbeitet mit Rechenzentren zusammen, um physische Sicherheit und umgebungsbezogene Sicherheitskontrollen für Serverräume mit Produktionsservern zu bieten. Zu diesen Kontrollen gehören:

- Videoüberwachung und Aufzeichnung
- Multifaktor-Authentifizierung für hochsensible Bereiche
- Temperaturregelung von Heizung, Lüftung und Klimaanlage
- Sprinkleranlage und Rauchmelder
- Unterbrechungsfreie Stromversorgung (USV)
- Zwischenböden oder umfassendes Kabelmanagement
- Kontinuierliche Überwachung und Warnmeldungen
- Schutz vor häufigen Naturkatastrophen und vom Menschen verursachten Katastrophen entsprechend der Geografie und des Standorts des jeweiligen Rechenzentrums
- Geplante Wartung und Validierung aller wichtigen Sicherheits- und Umgebungskontrollen

LastPass beschränkt den physischen Zugang zu Produktionsrechenzentren auf autorisierte Einzelpersonen. Für den Zugang zu einer Hosting-Einrichtung in einem Serverraum vor Ort oder eines Drittanbieters ist die Einreichung eines Antrags über das entsprechende Ticketing-System und die Genehmigung des jeweiligen Managers sowie eine Überprüfung und Genehmigung der Technikabteilung erforderlich. Die LastPass-Verwaltung überprüft die Protokolle für den physischen Zugang zu Rechenzentren und Serverräumen mindestens auf vierteljährlicher Basis. Darüber hinaus wird der physische Zugang zu Rechenzentren nach Beendigung der Tätigkeit des zuvor autorisierten Personals aufgehoben.

3.5 Datensicherung, Notfallwiederherstellung und Verfügbarkeit

LastPass wird basierend auf der gewählten Datenspeicherort-Einstellung (diese wird bei der Kontoerstellung festgelegt): (a) in vollständig redundanten, Aktiv/Passiv-Rechenzentren in den USA oder Europa oder (b) in erstklassigen, von Cloud-Hosting-Anbietern bereitgestellten Rechenzentren in Australien oder Singapur betrieben. Die LastPass-Passwort-Manager- und LastPass-SSO-Funktionen sind auf separate Rechenzentren verteilt. Jedes Rechenzentrum kann den gesamten LastPass-Datenverkehr aller Benutzer handhaben.

Alle Benutzerdaten werden unter Verwendung mehrerer Rechenzentren redundant und mit automatischer Notfallwiederherstellung sowie automatischem Failover gespeichert.

LastPass sichert Kundeninhalt innerhalb desselben Rechenzentrums in 24-Stunden- und 7-Tage-Intervallen. Darüber hinaus erfolgt alle sieben Tage eine entsprechende Sicherung in einem geografisch entfernten Rechenzentrum, die vier Wochen lang aufbewahrt wird.

Um die Sicherheit Ihrer Daten zu gewährleisten, nutzt die LastPass-SSO-Datenbank die sogenannte 7-Tage-Point-in-Time-Wiederherstellung (PITR, Point-in-Time Restore). Zusätzlich wird im Rahmen einer Langzeitsicherung (LTR, Long-Term Retention) die erste Sicherungskopie eines 7-Tage-Intervalls vier Wochen lang aufbewahrt und die erste Sicherungskopie jedes vierwöchigen Zeitraums drei Monate lang.

Bei Aktivierung der entsprechenden Funktion wird automatisch eine sichere, verschlüsselte, lokale Kopie des Vaults eines Benutzers gespeichert, wenn der Benutzer über eine Browser-erweiterung oder eine Mobilgeräte-App auf LastPass zugreift. Diese zwischengespeicherte Version ermöglicht es dem Benutzer, offline auf seine Daten zuzugreifen, wenn keine Internetverbindung verfügbar ist.

3.6 Malware-Schutz

Malware-Schutzsoftware mit Überwachungsprotokollen wird auf allen LastPass-Servern eingesetzt. Warnmeldungen, die auf mögliche böswillige Aktivitäten hinweisen, werden an ein entsprechendes Reaktionsteam gesendet.

3.7 Verschlüsselung

LastPass verfügt über einen kryptographischen Standard, der den Empfehlungen von Branchengruppen, staatlichen Veröffentlichungen und anderen für Standards relevanten Gruppen entspricht. Dieser Standard wird regelmäßig überprüft und die ausgewählten Technologien und Verschlüsselungen werden aktualisiert, wenn dies als notwendig erachtet wird.

LastPass nutzt kryptographische Mechanismen zur Abwehr von Brute-Force-Passwortangriffen. Die im LastPass-Vault eines Benutzers gespeicherten vertraulichen Daten werden mit einem eindeutigen Verschlüsselungsschlüssel verschlüsselt, der sich nicht im Besitz von LastPass befindet. Dieser Schlüssel wird aus dem Master-Passwort des Benutzers abgeleitet.

Benutzerauthentifizierung

Zur Authentifizierung des Benutzers beim LastPass-Server generiert LastPass ein Authentifizierungstoken, und zwar durch Hashen des Master-Passworts und der E-Mail-Adresse eines Benutzers. Dieses Hash-Verfahren umfasst jetzt standardmäßig 100.000 Runden PBKDF2 mit SHA-256 auf der Client-Seite, bevor das Token an den Server weitergegeben wird. Der Server führt weitere 100.000 Runden SHA-256 und Skript durch, bevor das Ergebnis mit einem in der LastPass-Datenbank gespeicherten Wert verglichen wird, um zu ermitteln, ob die Authentifizierung erfolgreich war.

Vault-Verschlüsselung im Ruhezustand

Die LastPass-Browsererweiterung oder -Mobilgeräte-App setzt PBKDF2 mit SHA-256 ein, um einen eindeutigen Verschlüsselungsschlüssel aus dem Master-Passwort des Benutzers abzuleiten. Dieser Verschlüsselungsschlüssel verbleibt auf dem Gerät des Benutzers (und wird nie an LastPass übertragen) und wird zur Verschlüsselung der Vault-Daten mit dem AES-256-Algorithmus verwendet. Auf Windows-Geräten kommen Krypto-APIs von Microsoft zum Einsatz, die als zusätzliche Schutzschicht dienen. Der verschlüsselte Vault wird über TLS an LastPass übertragen und serverseitig in diesem verschlüsselten Zustand gespeichert. Darüber hinaus wird der lokal verschlüsselte Vault auf dem Benutzergerät (nach der Anmeldung) zwischengespeichert, sodass bei Bedarf offline darauf zugegriffen werden kann.

SSO-Verschlüsselung im Ruhezustand

LastPass-SSO nutzt transparente Datenverschlüsselung. Dabei wird der Speicher der gesamten Datenbank mit einem symmetrischen Schlüssel, der als Datenbank-Verschlüsselungsschlüssel bezeichnet wird, verschlüsselt. Dieser Datenbank-Verschlüsselungsschlüssel wird durch einen transparenten Datenverschlüsselungsschutz geschützt – ein dienstseitig verwaltetes Zertifikat.

Beim Start der Datenbank wird der verschlüsselte Datenbank-Verschlüsselungsschlüssel entschlüsselt und zur Entschlüsselung und erneuten Verschlüsselung der Datenbankdateien im SQL Server Database Engine-Prozess eingesetzt. Bei der transparenten Datenverschlüsselung erfolgen die Echtzeit-E/A-Verschlüsselung und -Entschlüsselung auf Seitenebene. Jede Seite wird beim Einlesen in den Speicher entschlüsselt und dann vor dem Schreiben auf dem Datenträger verschlüsselt.

Das integrierte Serverzertifikat unterscheidet sich von Server zu Server, und als Verschlüsselungsalgorithmus wird AES 256 verwendet. Da sich die Datenbanken in einer Georeplikationsbeziehung befinden, sind sowohl die Primärdatenbank als auch die Geo-Sekundärdatenbank durch den übergeordneten Serverschlüssel der Primärdatenbank geschützt. LastPass SSO speichert die SAML-Zertifikate zur Verarbeitung vorübergehend auf Speicher, der mit 256-Bit-AES-Verschlüsselung verschlüsselt ist.

Die Zertifikate werden gemäß der internen Sicherheitsrichtlinie automatisch geändert, und der Stammschlüssel wird durch einen geheimen internen Speicher geschützt.

Verschlüsselung während der Übertragung

Um den Kundeninhalt während der Übertragung zu schützen, wird er zunächst mit dem AES-256-CBC-Modus verschlüsselt und dann beim Senden über HTTPS mit TLS-Protokollen (Transport Layer Security) geschützt. Darüber hinaus nutzt LastPass die neueste Version von Secure Shell (SSH) mit starken Verschlüsselungssammlungen für angegebene Administrationsfunktionen.

Generell wird die Konnektivität zu sensiblen Systemen und Diensten, einschließlich des Zugriffs auf die internen LastPass-Netzwerke, durch angemessene Transport-Verschlüsselungstechnologien geschützt.

3.8 LastPass-Enterprise-Funktionen

Zurücksetzen von Master-Passwörtern

LastPass Enterprise bietet Superadministrator-Funktionen, mit denen Unternehmen ausgewählten Administratoren (sogenannten Superadministratoren) Rechte zum Zurücksetzen der Master-Passwörter von Benutzern zuweisen können.

Sofern ein Superadministrator zugewiesen wurde, wird beim Erstellen eines neuen Benutzers oder beim Ändern eines Master-Passworts eine Kopie des lokalen Benutzerschlüssels, der zum Verschlüsseln und Entschlüsseln des Benutzer-Vaults verwendet wird, im Superadministratorkonto verschlüsselt. Nur das Superadministrator-Konto kann diesen lokalen Schlüssel entschlüsseln, um eine Rücksetzung des Master-Passworts zu veranlassen. LastPass erlaubt es Superadministratoren nicht, über diese Funktion auf den Inhalt des Benutzer-Vaults zuzugreifen – es kann ausschließlich eine Rücksetzung des Master-Passworts vorgenommen werden.

3.9 Schwachstellen-Management

Die internen und externen Systeme und Netzwerke werden monatlich auf Schwachstellen überprüft. Es werden auch regelmäßig Schwachstellenprüfungen dynamischer und statischer Anwendungen vorgenommen und Penetrationstestaktivitäten für bestimmte Umgebungen ausgeführt. Für die Ergebnisse dieser Überprüfungen und Tests werden in Netzwerküberwachungstools Berichte erstellt und wo dies basierend auf der Wichtigkeit der identifizierten Schwachstellen erforderlich ist, werden Abhilfemaßnahmen ergriffen.

Schwachstellen werden auch in monatlichen und vierteljährlichen Berichten kommuniziert und verwaltet, die den relevanten Entwicklungsteams sowie dem Management zur Verfügung gestellt werden.

3.10 Protokollierung und Warnmeldungen

LastPass erfasst identifizierten anomalen oder verdächtigen Datenverkehr in entsprechenden Sicherheitsprotokollen in den jeweiligen Produktionssystemen.

4 Organisatorische Kontrollen

LastPass bietet einen umfassenden Satz an organisatorischen und administrativen Kontrollen zum Schutz des Sicherheits- und Datenschutzstatus von LastPass.

4.1 Sicherheitsrichtlinien und -verfahren

LastPass pflegt umfangreiche Sicherheitsrichtlinien und -verfahren, die an Geschäftszielen, Compliance-Programmen und der allgemeinen Unternehmensführung ausgerichtet sind. Diese Richtlinien und Verfahren werden regelmäßig überprüft und bei Bedarf aktualisiert, um die Einhaltung von Vorschriften stets sicherzustellen.

4.2 Einhaltung der Standards

LastPass hält geltende rechtliche, finanzielle, datenschutzrechtliche und regulatorische Anforderungen ein und erfüllt die folgenden Zertifizierungen und externen Audit-Berichte:

- TRUSTe Enterprise Privacy & Data Governance Practices Zertifizierung, um operative Datenschutz- und Data Protection-Kontrollen zu berücksichtigen, die sich an den wichtigsten Datenschutzgesetzen und anerkannten Datenschutzabkommen orientieren. Weitere Informationen finden Sie in unserem Blog-Beitrag.
- Service Organization Control (SOC) 2 Type 2-Bericht des American Institute of Certified Public Accountants (AICPA). BSI Cloud Computing Catalogue (C5).
- Service Organization Control (SOC) 3 Type II-Bericht des American Institute of Certified Public Accountants (AICPA).
- Einhaltung des Payment Card Industry Data Security Standard (PCI DSS) bei den E-Commerce- und Zahlungsumgebungen von LastPass.
- Interne Kontrollenbewertung wie im Rahmen der Jahresrechnungsprüfung durch das Public Company Accounting Oversight Board (PCAOB) erforderlich.

4.3 Sicherheitsvorgänge und Incident-Management

Das Security Operations Center (SOC) von LastPass ist mit dem Security Operations-Team besetzt und ist für das Erkennen von und Reagieren auf Sicherheitsereignisse verantwortlich. Das SOC verwendet Sicherheitssensoren und Analysesysteme, um mögliche Probleme zu identifizieren und hat einen Vorfallsreaktionsplan entwickelt, der die entsprechenden Reaktionen vorgibt.

Der Vorfallsreaktionsplan ist auf die wichtigen LastPass-Kommunikationsprozesse, die Incident-Management-Richtlinie für Informationssicherheit sowie standardmäßige Betriebsvorgänge ausgerichtet. Er wurde entwickelt, um vermutete oder identifizierte Sicherheitsereignisse in den Systemen und Services – einschließlich LastPass – zu verwalten, zu identifizieren und zu beheben. Laut Vorfallsreaktionsplan gibt es Techniker, die Ereignisse und Schwachstellen hinsichtlich der Sicherheit von Informationen identifizieren und alle vermuteten oder bestätigten Ereignisse gegebenenfalls mit dem Management eskalieren. Mitarbeiter können Sicherheitsvorfälle gemäß dem auf der Intranet-Seite von LastPass dokumentierten Prozess per E-Mail, Telefon und/oder Ticket melden. Alle identifizierten oder vermuteten Ereignisse werden über standardisierte Ereignistickets dokumentiert, eskaliert und je nach Wichtigkeit selektiert.

4.4 Anwendungssicherheit

Das Anwendungssicherheitsprogramm von LastPass basiert auf dem Microsoft Security Development Lifecycle (SDL) für einen sicheren Produktcode. Zu den Hauptelementen dieses Programms gehören manuelle Codeüberprüfungen, Bedrohungsmodellierung, statische Codeanalysen, dynamische Analysen und Systemhärtung. Darüber hinaus nimmt LastPass an einem von BugCrowd gehosteten Bug-Bounty-Programm

(https://bugcrowd.com/lastpass) teil, das externe Sicherheitsexperten anspornt, potenzielle Sicherheitsschwachstellen verantwortungsbewusst offenzulegen.

4.5 Personalsicherheit

Überprüfungen der Mitarbeiter – soweit dies nach geltendem Recht zulässig und für die Position angemessen ist – werden weltweit bei neuen Mitarbeitern vor dem Datum ihrer Einstellung vorgenommen. Die Ergebnisse werden im Personalstammblatt des Mitarbeiters hinterlegt. Die Kriterien der Mitarbeiterüberprüfung variieren in Abhängigkeit der Gesetze, der Arbeitsverantwortung und dem Führungsniveau des potenziellen Mitarbeiters und unterliegen den üblichen und zulässigen Praktiken des jeweiligen Lands.

4.6 Sicherheitsbewusstsein und Schulungsprogramme

Neueingestellte Mitarbeiter werden zur Orientierung über die Sicherheitsrichtlinien und den Verhaltenskodex und Geschäftsethik von GoTo informiert. Diese obligatorische jährliche Schulung zu Sicherheit und Datenschutz wird für die entsprechenden Mitarbeiter durch das Talentförderungsteam und mit Unterstützung des Sicherheitsteams durchgeführt. Die Mitarbeiter und Zeitarbeiter von LastPass werden regelmäßig über die Anweisungen, Verfahren, Richtlinien und Standards zu Sicherheit und Datenschutz informiert. Dazu werden verschiedene Medien wie Einarbeitungsunterlagen für Neueingestellte, Aufklärungskampagnen, Webinare mit dem CISO, ein Sicherheits-Champion-Programm und der Aushang von Plakaten oder anderem Begleitmaterial genutzt, die mindestens halbjährlich ausgetauscht werden und Methoden zum Schutz von Daten, Geräten und Anlagen veranschaulichen.

5 Datenschutzpraktiken

LastPass nimmt den Schutz der Daten seiner Kunden, Abonnenten der LastPass-Services und Endbenutzer sehr ernst und verpflichtet sich, entsprechende Praktiken zur Verarbeitung und Verwaltung von Daten offen und transparent preiszugeben.

5.1 DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union (EU), die sich mit dem Schutz der Daten und der Privatsphäre von Einzelpersonen in der Europäischen Union befasst. Sie zielt primär darauf ab, ihren Bürgern und Bewohnern Kontrolle über ihre personenbezogenen Daten zu geben und die regulative Umgebung in der EU zu vereinfachen. LastPass erfüllt die anwendbaren DSGVO-Bestimmungen. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.2 CCPA

LastPass sichert hiermit zu, dass es mit dem California Consumer Privacy Act (CCPA) konform ist. Weitere Informationen finden Sie unter https://www.goto.com/company/trust/privacy.

5.3 Data Protection- und Datenschutzerklärung

GoTo freut sich, einen umfassenden, globalen Datenverarbeitungsnachtrag (DVN) auf Englisch und Deutsch bereitzustellen, um die Anforderungen von DSGVO, CCPA und mehr zu erfüllen und die LastPass-Verarbeitung personenbezogener Daten zu regeln.

Der DVN schließt folgende Datenschutz-Anforderungen in Bezug auf die DSGVO ein: (a) Details zur Datenverarbeitung, Offenlegung bzgl. Auftragsverarbeiter-Partnerunternehmen etc. gemäß Artikel 28 (b) EU-

Standardvertragsklauseln (auch als EU-Modellklauseln bekannt) und (c) die technischen und organisatorischen Maßnahmen von LastPass. Im Zusammenhang mit dem Inkrafttreten des CCPA haben wir zusätzlich in unserem globalen DVN Folgendes aktualisiert: (a) Definitionen im Zusammenhang mit dem CCPA, (b) Zugriffs- und Löschrechte und (c) Garantien, dass LastPass keine personenbezogenen Daten von Benutzern verkaufen wird.

Für Besucher unserer Webseiten veröffentlicht GoTo die Arten von Informationen, die es sammelt und verwendet, um seine Services bereitzustellen, aufrechtzuerhalten, zu verbessern und zu sichern, in seiner Datenschutzerklärung auf der öffentlichen Website. Das Unternehmen kann seine Datenschutzrichtlinie von Zeit zu Zeit aktualisieren, um Änderungen an seinen Informationspraktiken und/oder Änderungen geltender Gesetze zu berücksichtigen, weist aber auf seiner Website auf jegliche Materialänderungen hin, bevor diese wirksam werden.

5.4 Abkommen zur Datenübertragung

LastPass hat ein robustes globales Data Protection-Programm, das das geltende Recht berücksichtigt und rechtmäßige internationale Datenübertragungen im Rahmen der folgenden Abkommen unterstützt:

5.4.1 Standardvertragsklauseln

Die Standardvertragsklauseln („SCC“) sind standardisierte Vertragsbestandteile, die von der Europäischen Kommission anerkannt und übernommen wurden und vorrangig dem Zweck dienen, eine EU-datenschutzkonforme Übermittlung personenbezogener Daten in Regionen außerhalb des Europäischen Wirtschaftsraums („EWR“) sicherzustellen. LastPass hat ein ausgefeiltes Datenschutzprogramm eingerichtet, das die Ausführungsbestimmungen der SCC für die Übermittlung personenbezogener Daten einhält. LastPass bietet Kunden SCC (andere Bezeichnung: EU-Modellklauseln) an. Diese leisten als Bestandteil des globalen DNV spezifische Garantien betreffend die Übermittlung personenbezogener Daten für die zum Leistungsumfang gehörigen LastPass-Services. Der Abschluss der SCC hilft, die freie Übermittlung der Daten von LastPass-Kunden aus dem EWR in andere Weltregionen sicherzustellen.

Ergänzende Maßnahmen

Neben den in diesen TOMs angegebenen Maßnahmen hat GoTo die folgenden FAQ erstellt, um seine ergänzenden Maßnahmen zur Unterstützung rechtmäßiger Datenübertragungen gemäß Kapitel 5 der DSGVO zu skizzieren und alle Analysen zu adressieren und anzuleiten, die vom Europäischen Gerichtshof zusammen mit den SCCs empfohlen werden.

5.4.2 Zertifizierungen zu APEC CBPR und PRP

GoTo hat zudem die Zertifizierungen zu APEC (Asiatisch-Pazifische Wirtschaftsgemeinschaft), CBPR (Grenzüberschreitende Datenschutzregulierung) und PRP (Datenschutzanerkennung für Datenverarbeiter) erworben. Die APEC-, CBPR- und PRP-Rahmenregelungen sind die ersten Datenregelungen, die für die Übermittlung personenbezogener Daten zwischen APEC-Mitgliedsländern genehmigt wurden. Sie

wurden von TrustArc, einem von der APEC anerkannten führenden Drittanbieter für die Einhaltung von Datenschutzbestimmungen, eingeholt und unabhängig validiert.

5.5 Rückgabe und Löschung von Kundeninhalt

LastPass-Benutzer können ihre eigenen Konten und verknüpften Inhalte über die Seite „Konto löschen" auf https://lastpass.com/delete_account.php löschen. Benutzer, die keinen Zugriff auf ihren LastPass-Vault und/oder ihre E-Mail-Adresse haben, können eine Serviceanfrage an den Kundensupport senden. Das Support-Team authentifiziert den Benutzer und löscht das Konto und den Inhalt innerhalb von 30 Tagen nach der Anfrage.

Kostenlose Konten, einschließlich des darin erstellten Inhalts, werden nach zwei (2) Jahren Inaktivität (d. h. keine Anmeldung) automatisch gelöscht.

5.6 Sensible Daten

Es ist das Ziel von LastPass, den gesamten Kundeninhalt zu schützen und zu sichern. Regulatorische und vertragliche Beschränkungen verlangen jedoch, dass die Verwendung von LastPass für bestimmte Arten von Informationen eingeschränkt wird. Sofern der Kunde keine schriftliche Genehmigung von LastPass hat, dürfen die folgenden Daten nicht in LastPass hochgeladen oder dort generiert werden:

- Staatlich vergebene Identifikationsnummern und Bilder von Ausweisdokumenten.
- Informationen über die Gesundheit einer Person, einschließlich, aber nicht beschränkt auf, persönliche Gesundheitsinformationen, wie im US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) sowie anderen relevanten anwendbaren Gesetzen und Vorschriften festgelegt.
- Alle Informationen, die besonders durch geltende Gesetze und Vorschriften geschützt sind, insbesondere Informationen über die Rasse, die ethnische Zugehörigkeit, religiöse oder politische Überzeugungen, organisatorische Mitgliedschaften der Person usw.

5.7 Nachverfolgung und Analysen

LastPass verbessert kontinuierlich seine Websites und Produkte mithilfe von Webanalysetools von Drittanbietern, um Folgendes besser zu verstehen: Nutzung der Websites, Desktop-Tools und mobilen Anwendungen durch Besucher sowie Benutzerpräferenzen und Probleme. Weitere Einzelheiten finden Sie in der Datenschutzrichtlinie.

6 Drittanbieter

6.1 Nutzung von Drittanbietern

Im Rahmen der internen Bewertung und der Prozesse im Zusammenhang mit Anbietern und Dritten können Anbieterbewertungen je nach Relevanz und Anwendbarkeit von mehreren Teams vorgenommen werden. Das Sicherheitsteam nimmt Bewertungen der Hosting-Einrichtungen von Drittanbietern vor und bewertet Anbieter von Services, die auf Informationssicherheit basieren. Das Team für Recht und Beschaffung kann bei Bedarf nach internen Prozessen relevante Verträge, Leistungsbeschreibungen und Servicevereinbarungen bewerten. Angemessene Konformitätsdokumente oder -berichte können mindestens einmal jährlich eingeholt und bewertet werden, sofern dies für angemessen

erachtet wird, um sicherzustellen, dass die Kontrollumgebung ordnungsgemäß funktioniert und alle erforderlichen benutzerbezogenen Kontrollen durchgeführt werden. Zudem müssen Drittanbieter, die sensible oder vertrauliche Daten hosten oder von LastPass Zugriff darauf erhalten haben, einen schriftlichen Vertrag unterzeichnen, in dem die relevanten Anforderungen für den Zugriff auf die Informationen sowie deren Speicherung oder Verarbeitung (sofern zutreffend) festgelegt sind.

6.2 Vertragspraktiken

Um die Geschäftskontinuität zu gewährleisten und sicherzustellen, dass geeignete Maßnahmen zum Schutz der Vertraulichkeit und Integrität von Geschäftsprozessen und Datenverarbeitung durch Drittanbieter getroffen werden, überprüft LastPass die jeweiligen Nutzungsbedingungen von Drittanbietern und nutzt entweder von LastPass genehmigte Beschaffungsvorlagen oder verhandelt die Bedingungen dieser Drittanbieter, wenn dies als notwendig erachtet wird.

7 LastPass kontaktieren

Kunden können sich bei allgemeinen Anfragen unter https://support.goto.com oder bei Fragen zum Datenschutz unter privacy@goto.com an LastPass wenden.