

LastPass... |

Fallstudie: Litmos



„Das Schöne an LastPass ist das einfache Rollout und die einfache Verwaltung. Und dank der intuitiven Benutzeroberfläche sind die Mitarbeiter sofort an Bord.“

Dayle Alsbury, Vice President Cybersecurity





Herausforderung

Litmos entwickelt seit 2007 benutzerfreundliche Lernplattformen mit umfangreichen Inhaltsbibliotheken. Mehr als 20 Millionen Menschen in 150 Ländern nutzen seine Lösungen in 35 verschiedenen Sprachen, um Lerninhalte zu erstellen und für Mitarbeiter, Partner und Kunden zugänglich zu machen.

2022 beschloss Litmos, seine vorhandenen Firmensysteme unter die Lupe zu nehmen. Gab es irgendwelche zusätzlichen Tools, die für einen sicheren Geschäftsbetrieb erforderlich waren? Mittlerweile beschäftigte das Unternehmen 250 Angestellte, die ausschließlich im Homeoffice tätig waren. Mit über 20 Jahren Erfahrung im Bereich der Cybersicherheit war sich Dayle Alsbury, Vice President Cybersecurity bei Litmos, bewusst, welche Schäden Malware, Ransomware und Phishing-Angriffe verursachen können. Er hielt daher nach einem cloudbasierten Passwort-Manager Ausschau, der sich problemlos im ganzen Unternehmen implementieren ließ und die Passwortsicherheit und die Passwortgewohnheiten der Mitarbeiter verbessern würde.

Alsbury: *„Der Schutz unserer Mitarbeiter und Kunden war unser oberstes Ziel. Alle Daten sind sensibel und müssen geschützt werden. Aus diesem Grund entschieden wir uns für LastPass. Wir brauchten einen skalierbaren Passwort-Manager, der unserem Unternehmen alle nötigen Funktionen bietet.“*



Lösung

Mit einer mobilen Belegschaft, die mit cloudbasierten Technologien bestens vertraut ist, entschied sich Litmos für LastPass, da jedes Teammitglied einen eigenen Vault erhält. Noch dazu überzeugte der Passwort-Manager allgemein durch seine hohe Benutzerfreundlichkeit und Skalierbarkeit.

Der Passwort-Vault von LastPass ist ein zentraler Hub und Speicher für alles, was die Mitarbeiter sicher aufbewahren wollen, darunter Passwörter, sichere Notizen und Kreditkartendaten. Websites lassen sich sowohl importieren als auch manuell hinzufügen, und für eine noch einfachere Anmeldung kann die Browsererweiterung von LastPass Kontopasswörter automatisch speichern, wenn sie auf einer Website eingegeben werden. Alsbury weiter: *„Als sicherer Passwortspeicher erfüllt LastPass alle Anforderungen unserer Teams.“*

Um das Rollout zu erleichtern und die Benutzerakzeptanz zu erhöhen, war auch der Bedienkomfort ein wichtiger Faktor für Litmos. Mit der Browsererweiterung, dem Passwort-Vault, dem plattformübergreifenden Zugriff und der sicheren Freigabefunktion macht LastPass das Erstellen, Verwalten und Freigeben von Passwörtern für das gesamte Team zum Kinderspiel. Alsbury: *„Viele Enterprise-Lösungen sind mühsam und kompliziert einzurichten und zu verwalten. Bei LastPass haben wir dieses Problem nicht. Es ist ein überall verfügbares, einfach zu bedienendes und kostengünstiges Tool, das unseren Anforderungen genau entspricht.“*

Litmos entschied sich für die LastPass-Identity-Suite inklusive Single Sign-On (SSO) und Multifaktor-Authentifizierung (MFA). Das Komplettpaket bietet dem Unternehmen vollständige Transparenz und schützt jeden Benutzer und jeden Zugriffspunkt. Neben einem umfassenden Katalog mit SSO-Apps sind auch verschiedene MFA-Methoden wie die biometrische Authentifizierung, Passcodes und die Spracherkennung direkt verfügbar.



Ergebnis

Die Einführung von LastPass verlief absolut reibungslos; der Passwort-Manager wird von sehr vielen Mitarbeitern genutzt. Um sicherzugehen, dass die Angestellten die Lösung richtig verwenden, behält Alsburys Team ihre Sicherheitsbewertung genau im Blick und führt regelmäßig Gegenproben mit Phishing-Simulationsprogrammen durch. So wird das IT-Team auf weniger achtsame Mitarbeiter aufmerksam, die anfälliger für Hackerangriffe sind und schlechte Passwortgewohnheiten pflegen. Litmos kann diese Teammitglieder dann gezielt aufklären und unterstützen. Auch auf diese Weise trägt LastPass dazu bei, das Unternehmen vor künftigen Cyberbedrohungen zu schützen.

Der LMS-Anbieter forciert auch die Nutzung der Freigabefunktion in seinem Team. Mit LastPass lassen sich Passwörter schnell und einfach für andere freigeben. Änderungen werden sofort synchronisiert, sodass alle Benutzer auf dem Laufenden sind. Die einzelnen Teams nutzen die Freigabefunktion nicht nur intern, sondern auch, um Passwörter für Kollegen in anderen Abteilungen zugänglich zu machen.

Um besser zu verstehen, wie Litmos seine Cybersicherheit erhöhen und die Passwortgewohnheiten der Benutzer verbessern konnte, investierte das Unternehmen



„Bei LastPass gibt es kein Durcheinander oder Chaos. Die Benutzer finden das Gesuchte sofort.“

außerdem in professionelle Beratungs- und Schulungsleistungen durch LastPass. Das 30 Stunden umfassende Professional-Services-Paket deckt Themen wie Best Practices für die Passwortverwaltung und die Konfiguration der Verbundanmeldung ab. Litmos schätzte diese maßgeschneiderte Unterstützung sehr und gewann wertvolle Einblicke. Alsbury dazu: *„Das LastPass-Team ging immer sofort auf unsere Anliegen ein und war sehr flexibel. Insbesondere die Schulungen übertrafen all unsere Erwartungen. Aus dem gesamten Unternehmen kamen äußerst positive Rückmeldungen.“*

Finden Sie heraus, wie Litmos seine Passwortsicherheit mit LastPass verbesserte.

**LastPass
kontaktieren**