LastPass •••|

Fallstudie: EpiOn

„Unsere Partnerschaft mit LastPass währt nun schon zwei Jahre, und wir fühlen uns dabei bestens aufgehoben.“

Don Viar, Managing Partner und CEO EpiOn

Herausforderung

EpiOn aus Tennessee ist ein Managed Service Provider (MSP). In dieser Funktion bietet das Unternehmen strukturierte IT-Verwaltungsdienste an, die seinen Kunden einen sicheren und produktiven Geschäftsbetrieb ermöglichen sollen. Zu den zentralen Bausteinen des EpiOn-Angebots gehört eine Lösung für die Passwortverwaltung. Don Viar, Managing Partner bei EpiOn, führt aus: *„Unser Unternehmen hält die Standards des Centre for Internet Security ein, die als ein zentrales Element Passwortverwaltung empfehlen. Browserbasierte Passwort-Manager erfüllen jedoch nicht die komplexen Anforderungen, denen Zugangsdaten bei uns unterliegen. Wir brauchten also ein Tool, das stark und zuverlässig genug war, um es Kunden anbieten zu können.“*

EpiOn sondierte den Markt und wurde dabei auf LastPass mit seinem branchenführenden Angebot aufmerksam. Don Viar: *„Wir suchten einen Partner, der uns eine stabile Multi-Tenant-Lösung bieten konnte. Diesbezüglich lag LastPass ganz klar vorne.“*

EpiOn entschloss sich zu einer exklusiven Partnerschaft mit LastPass und führte dessen Passwortverwaltungslösung auch im eigenen Unternehmen ein. Man wollte dadurch die eigene Passworthygiene weiter verbessern und der Belegschaft eine abgesicherte Umgebung für den Zugriff auf die Konten der Kunden und die sichere Freigabe von Passwörtern bieten. Bestechend fand EpiOn bei LastPass auch die Möglichkeit zum passwortlosen Login, und zwar nicht nur für das eigene Team, sondern sogar auch für die Kunden.

Lösung

Mit dem Passwortgenerator von LastPass erstellt die Belegschaft bei EpiOn nun zufällige Passwörter, die bestimmten, konfigurierbaren Parametern entsprechen. Viar dazu: *„Die Kriterien für sichere Passwörter werden immer komplexer – alle Bedingungen manuell einzuhalten, das schafft fast niemand mehr. Wir möchten, dass unsere Leute es so einfach wie möglich haben.“* Mit LastPass erstellen das EpiOn-Team und die Kunden jetzt auf Knopfdruck Passwörter, die mindestens 12 Zeichen lang sind und sich komplex aus Zeichen, Symbolen und Sonderzeichen zusammensetzen. Wenn gute Passwörter so einfach zu generieren sind, geben Benutzer die Wiederverwendung von Passwörtern nach und nach auf. Die Passworthygiene der gesamten Belegschaft verbessert sich.

Die Funktion für die Freigabe von Ordnern ermöglicht Teams ein sicheres Zusammenarbeiten. Über diese Ordner kann EpiOn genau steuern, wer mit wem die darin befindlichen Passwörter, Notizen und Dateien teilen kann. Alle Daten werden auf Endgeräten mit 256 Bit AES verschlüsselt, was ihre sichere Freigabe ermöglicht. Die Einstellungen für den Zugriff und die Freigabe sind anpassbar. So können unter anderem das Anzeigen von Passwörtern unterbunden und Ordner mit Schreibschutz versehen werden. Viar erklärt: *„Ein Benutzer hat durchschnittlich über 100 Konten. Die Ordnerfreigabe und der Passwortgenerator sind zwei Optionen von LastPass, die uns in die Lage versetzen, unsere Zugriffsvergabe abzusichern und dabei regulatorische Anforderungen einzuhalten.“*

Um den Passwortstress weiter zu eliminieren, führte EpiOn im gesamten Unternehmen Workstation MFA (WSMFA) ein. Statt der klassischen Eingabe der Zugangsdaten müssen Benutzer sich jetzt auf ihren Geräten nur noch authentifizieren, was viel komfortabler für sie ist. Das Tool von LastPass für die Multifaktor-Authentifizierung (MFA) lässt außerdem die biometrische Authentifizierung zu. Mitarbeiter können sich also anstelle der Eingabe ihrer Zugangsdaten für eine passwortlose Authentifizierung entscheiden. Dies verbessert die Resilienz des Unternehmens weiter, zumal Verfahren zum Einsatz kommen, denen die Mitarbeiter vertrauen: Biometrie oder FIDO2-zertifizierte Authentifizierung.

Ergebnis

Seit der Einführung des Passwort-Managers bei EpiOn sind zwei Jahre vergangen. Eine sorgfältig konzipierte Sicherheitsstrategie hat dafür gesorgt, dass die Nutzungsrate im eigenen Betrieb inzwischen bei 100 % liegt. Viar betont: *„MSP sind lohnende Angriffsziele für Hacker, das ist uns bewusst. Deshalb halten wir uns an die CIS-Standards. Die Zugangsdaten unserer Teams sind einfach zu kostbar.“*

Das Admin-Dashboard von LastPass liefert Einblicke in das Passwortverhalten der einzelnen Mitarbeiter und ist eine wichtige Komponente der Geschäftspraxis bei EpiOn geworden. EpiOn hat eine eigene Metrik entwickelt, mit der sich auch der Sicherheitsstatus von Kundenmitarbeitern ermitteln lässt. So kann auf etwaige Sicherheitslücken hingewiesen werden. In diese Metrik fließt der LastPass-Sicherheitswert ein; er spielt bei der Analyse des Sicherheitsverhaltens von Benutzern eine wichtige Rolle.

Bei der EpiOn-Belegschaft kam insbesondere WSMFA gut an. Viar würde die Funktion auch gerne bei allen Kunden einführen. Er führt aus: *„Unser eigenes Team nutzt tagein, tagaus diese Authentifizierungs-App. Und weil der Login damit so nahtlos funktioniert, sind alle viel entspannter. Für uns ist das die Zukunft. Manche Kunden haben uns schon darauf angesprochen. Ich schätze, dass das bald Standard sein wird.“*

„Die Integration von WSMFA und der darüber mögliche passwortlose Login werden uns über kurz oder lang eine Nutzungsrate von 100 % bescheren.“

Zur Partnerschaft zwischen EpiOn und LastPass äußert sich Viar folgendermaßen: *„Unsere Erfahrungen mit LastPass sind rundum positiv. Und mit der WSMFA-Integration ist alles noch ein Stückchen angenehmer für uns geworden. Das Projekt ist ein Erfolg auf der ganzen Linie, und die Zusammenarbeit mit LastPass ist immer eine große Freude für uns.“*

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

LastPass kontaktieren