LastPass

Fallstudie: Crunchr

crunchr

„LastPass ist unsere Basishygiene – so wie täglich duschen. Es hält alles, was wir tun, tipptopp sauber und sicher.“

Jan Joris *Vereijken*, Chief Technology Officer

Herausforderung

Das Amsterdamer Unternehmen Crunchr betreibt eine Personalanalyseplattform. Es stellt Unternehmen Analysen und Prognosen zur Verfügung, die ihnen dabei helfen, ihre Arbeitsumgebung positiv und produktiv zu gestalten und ihre Personalfluktuation einzudämmen. Jan Joris *Vereijken*, Chief Technology Officer bei Crunchr, kam vor fünf Jahren in das Unternehmen, doch sein Einfluss auf das Thema Sicherheit bei Crunchr reicht weiter zurück. Als *Vereijkens* Freund, der Crunchr-Gründer Dirk Jonker, davon sprach, ein eigenes Unternehmen zu starten, riet *Vereijken* ihm, gleich einen Passwort-Manager einzuführen. Wie wichtig ein Passwort-Manager ist, hatte *Vereijken* selbst begriffen, nachdem 2012 sein eigenes Twitter-Konto gehackt worden war, weil er ein Passwort mehrfach verwendet hatte. Seitdem weiß er, dass dieser saloppe Umgang mit Zugangsdaten riskant ist und die Krux im Erstellen sicherer Passwörter liegt.

Vereijken erklärt: *„Mir wurde klar, dass ich für jedes Online-Konto ein eigenes Passwort brauche, denn dass mein Twitter gehackt worden war, lag genau daran: dass ich das nicht hatte.“* Er suchte nach einem guten Tool für sich, und ein Freund empfahl ihm LastPass.

Vereijken, der das Risiko eines nachlässigen Passwortverhaltens am eigenen Leib erfahren hatte, riet Jonker dazu, gleich Nägel mit Köpfen zu machen und mit LastPass dafür zu sorgen, dass Crunchr von Anfang an gegen Datenschutzverletzungen und Datendiebstahl geschützt war.

Lösung

2014 schaffte Crunchr LastPass an und stockte die Lizenzen mit wachsender Belegschaft sukzessive auf, um keine Sicherheitslücken in seiner Infrastruktur entstehen zu lassen.

Vom LastPass-Passwortgenerator machen die Mitarbeiter von Crunchr reichlich Gebrauch; er erleichtert ihnen das Erstellen zufälliger und sicherer Passwörter. Die Administratoren können dabei sicherstellen, dass die genutzten Passwörter mindestens zwölf Zeichen lang sind und Buchstaben, Ziffern und Sonderzeichen enthalten. *Vereijkens* Resümee: *„Ich habe verstanden, dass jedes Konto sein eigenes Passwort braucht. Dieser Richtlinie müssen jetzt alle im Unternehmen folgen.“* Mit dem Passwortgenerator von LastPass lässt sich mühelos für jedes Konto ein eigenes einmaliges Passwort erstellen. Dies entschärft das Risiko von Phishing-Angriffen und mindert das Ausmaß potenzieller Schäden.

Für *Vereijken* war die Eigenschaft von LastPass, auf vielen Geräten einsetzbar zu sein, ein weiteres ausschlaggebendes Kriterium für die Anschaffung. Die Crunchr-Belegschaft arbeitet hybrid. 60 % der Mitarbeiter sind im Homeoffice. Im Unternehmen ist außerdem unterschiedlichste Hard- und Software im Einsatz, sodass eine Lösung gewünscht war, die sowohl auf Apple iOS als auch Microsoft Windows funktioniert. „Mir war es wichtig, dass das Tool auf verschiedenen Betriebssystemen nutzbar ist“, führt *Vereijken* aus. *„Die Mitarbeiter sollten es einfach einrichten und jederzeit und überall auf ihre Passwort-Vaults zugreifen können. LastPass funktioniert auf vielen Plattformen und bietet eine konsistente Benutzererfahrung. Für uns perfekt!“*

„Wir lassen hier niemandem Entscheidungsfreiheit. Passworthygiene mit LastPass ist für alle im Unternehmen Pflicht.“

Ergebnis

LastPass ist quasi täglich Brot für die Mitarbeiter von Crunchr. Mindestanforderungen für das Master-Passwort, keine Mehrfachnutzung von Passwörtern, MFA ist obligatorisch: Insgesamt dreißig Richtlinien sorgen bei Crunchr dafür, dass die Mitarbeiter ein sicheres Passwortverhalten an den Tag legen. Aktuell gibt es nur ein einziges schwaches Master-Passwort im gesamten Unternehmen – Beweis genug dafür, dass LastPass das Passwortverhalten bei Crunchr positiv beeinflusst hat. Der Sicherheitswert liegt jetzt bei 86 %, die Passwortstärke bei 85 %. *Vereijken* dazu: *„Ich persönlich habe einen Sicherheitswert von 94 %, aber ein paar Kollegen sind inzwischen an mir vorbeigezogen!“*

Bitbucket, Google Workspace, HubSpot und so weiter: Bei Crunchr wird mit insgesamt über 60 verschiedenen Cloud-Lösungen gearbeitet. Um den Zugang zu diesen zu erleichtern und Prozesse zu straffen, denkt man im Unternehmen derzeit über Single Sign-on nach. Zur sicheren Weitergabe von Zugangsdaten an Kollegen im selben Projektteam nutzen Crunchr-Mitarbeiter im Wochenturnus die Passwortfreigabefunktion von LastPass. Über freigegebene Ordner können Administratoren in LastPass Zugangsdaten von Systemkonten aktualisieren, sodass Mitarbeiter nach ihrem Weggang vom Unternehmen keinen Zugriff mehr haben. *Vereijken* erklärt: *„Neulich hat ein Mitarbeiter das Finance-Team verlassen. Da habe ich sofort die Zugangsdaten zum System geändert. Vorausgesetzt, Mitarbeiter greifen richtlinienkonform über die freigegebenen Ordner auf unsere Systeme zu, bemerken sie diese Änderungen nicht einmal.“*

„Ich verwahre über tausend Login-Daten in meinem LastPass-Vault, und kann sagen, dass jedes Konto sein eigenes Passwort hat.“

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

LastPass kontaktieren