LastPass

Fallstudie: Handshakes

Handshakes

„LastPass ist inzwischen ein selbstverständlicher Bestandteil unseres Unternehmens. Und ist sogar in unseren Wortschatz eingeflossen: In unseren Bürogesprächen fällt der Begriff LastPass recht häufig.“
Kenneth Ham

Herausforderung

Der 2011 gegründete Datentechnikanbieter Handshakes bereitet für seine Kunden Daten so auf, dass diese das Ergebnis als tragfähige Entscheidungsbasis nutzen können. Das Unternehmen hat aktuell Büros in Singapur, Australien, Taiwan und drei weiteren Standorten und pflegt Partnerschaften mit Microsoft und vergleichbaren Anbietern.

Handshakes bewegt sich in einem hochdynamischen Markt und rechnet mit einem baldigen Wachstum. Anlass genug für Kenneth Ham, Chief Technology Officer bei Handshakes, auf die Suche nach einem Tool für die Passwortverwaltung zu gehen, mit dem sein Unternehmen das eigene Passwortverhalten verbessern konnte. Angesichts ständig zunehmender Hackerangriffe über Ransomware und Phishing erkannte Ham immer klarer, wie wichtig sichere Passwörter sind und welche Rolle sie beim Schutz personenbezogener Daten spielen.

Ham erklärt: *„Nachdem uns aufgegangen war, was wir mit einem nachlässigen Passwortverhalten für unser Unternehmen riskieren, wusste ich es plötzlich: Wir brauchen einen Passwort-Manager mit einem Zero-Trust-Konzept.“*

Lösung

Kunden und Partner von Handshakes hatten bereits die Werbetrommel für LastPass gerührt, deshalb setzte sich das Tool im Unternehmen sehr bald durch. Schon bald erkannten die Mitarbeiter, welche Vorzüge LastPass für die Zusammenarbeit mit Kunden bietet, beispielsweise durch Funktionen wie die Passwortfreigabe oder freigegebene Ordner. Kenneth Ham nahm noch weitere Tools unter die Lupe, mit dem Ergebnis, dass LastPass tatsächlich die beste Lösung war, da es sämtliche Anforderungen von Handshakes erfüllte: Es bot eine breite Funktionspalette, über 100 anpassbare Richtlinien, eine Infrastruktur mit Zero-Knowledge-Verschlüsselung und die Einhaltung diverser Compliance-Standards (SOC2, SOC3, C5, ISO 27001 und DSGVO).

Nach der endgültigen Entscheidung für das Tool setzte Handshakes sofort Richtlinien in Kraft: Die Mitarbeiter sollten Passwörter nur noch mit dem Passwortgenerator erstellen. Die Freigabe von Passwörtern wurde reguliert und die Darkweb-Überwachung aktiviert. Ziel der Maßnahmen war es, das Passwortverhalten zu verbessern. Die Mitarbeiter sollten ihre Zugangsdaten nur noch über LastPass verwalten, Passwörter nicht mehr mehrfach verwenden und keine sensiblen Daten mehr per Messenger oder E-Mail weitergeben.

„Dank LastPass ist unserem Team ein sicheres Passwortverhalten zur zweiten Natur geworden.“

Ergebnis

Mit LastPass kann Handshakes Kunden und Partnern gegenüber nachweisen, dass es angemessene Maßnahmen zum Schutz personenbezogener Daten trifft. Die Infrastruktur der Lösung wird regelmäßigen Audits unterzogen und entspricht vielen externen sicherheitsrelevanten Compliance-Standards. Die Zero-Knowledge-Architektur bewirkt, dass niemand Zugriff auf die im eigenen Vault gespeicherten Passwörter oder Daten hat. Die Verschlüsselung erfolgt ausschließlich auf dem eigenen Gerät. Ham erklärt: *„Weder LastPass noch unsere Administratoren können auf die Vaults der Mitarbeiter zugreifen. Das ist ganz entscheidend. Dank der Zero-Trust-Umgebung kann jeder im Team LastPass bedenkenlos nutzen.“* Auf diesen Punkt legte das Handshakes-Entwicklungsteam großen Wert, als die Funktion zum Teilen von Passwörtern für die Zugriffsfreigabe auf Produktivsysteme aktiviert und der Zugriff überwacht werden sollte.

Nach der Einführung von LastPass schulte Handshakes sein Team zur Cybersicherheit, um Wissenslücken zu identifizieren und zu vermitteln, wie sich mit einem Passwort-Manager Risiken minimieren lassen. Die einfache und benutzerfreundliche Oberfläche kam sofort gut an; die Mitarbeiter integrierten LastPass schnell in ihr Arbeitsleben. LastPass ist inzwischen ein selbstverständlicher Bestandteil der Handshakes-Kultur – und sogar in den Wortschatz des Unternehmens eingeflossen: In den täglichen Bürogesprächen fällt der Name LastPass recht häufig.

Die Administrationskonsole gibt dem IT-Team vollen Überblick. Die Verbundanmeldung einrichten, die Darkweb-Überwachung aktivieren und Berichte zum Sicherheitsstatus erstellen, um Lücken und Nachbesserungsbedarf zu ermitteln: All das und mehr ist in der Konsole möglich. Handshakes überwacht den Sicherheitswert seiner Mitarbeiter täglich. Auf diese Weise konnte das Unternehmen Risiken durch schwache, mehrfach verwendete oder kompromittierte Passwörter eliminieren und ist nun besser gegen Hackerangriffe gewappnet. Dank der nahtlosen Integration von LastPass in Microsoft Azure konnte Handshakes auch SSO (Single Sign-On) einführen. Nun ist der Login in Systeme für die Mitarbeiter noch komfortabler.

Ham dazu: *„Unsere Mitarbeiter haben schnell gemerkt: Was auch immer sie mit LastPass tun wollen, es braucht immer nur ein paar Klicks dafür. Wir sind total glücklich mit dem Tool. Es bringt uns Sicherheit und ist dabei denkbar einfach. Jedes Unternehmen sollte sich LastPass zulegen, finden wir.“*

LastPass kontaktieren