

# LastPass... |



## Fallstudie: HealthConnections



**„Mit LastPass geht alles sehr schnell, deshalb ist es so effektiv.  
Die Bedienung ist simpel. Unsere Mitarbeiter lieben es!“**

Brad Sweet, Leiter Netzwerksysteme und Sicherheit bei HealthConnections

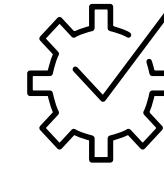


## Herausforderung

HealtheConnections ist eine Non-Profit-Organisation (NPO), die Zugang zu Gesundheitsinformationen und Ressourcen zur Verbesserung der Bevölkerungsgesundheit gibt und dafür entsprechende Lösungen bietet. Die NPO ist in 26 Verwaltungsbezirken des US-Bundesstaats New York und benachbarten Bundesstaaten aktiv. HealtheConnections verwaltet und pflegt Cloud-Portale, in denen Patientendaten verwahrt werden, und sorgt dafür, dass diese der medizinischen Fachwelt bei Bedarf zur Verfügung stehen. 11.000 Ärzte und viele Millionen Patienten nutzen die Dienste der NPO und profitieren davon.

Um die besagten Datenbestände als NPO technisch verwalten zu können, musste HealtheConnections dafür sorgen, dass sein Providerportal myConnections die Zertifizierungsanforderung HITRUST CSF v9.5 erfüllt. Wie Brad Sweet, Leiter Netzwerke und Sicherheit bei HealtheConnections, feststellte, war das nicht machbar ohne eine funktionsfähige Passwortverwaltung. Ein weiteres Problem beschrieb Christina Anastos vom IT-Support von HealtheConnections: In der gesamten Organisation herrschte ein fragwürdiges Passwortverhalten vor. Die Mitarbeiter hielten Zugangsdaten in Excel-Dateien fest oder notierten sie manchmal sogar auf Klebenotizen.

Sweet und Anastos wollten dafür sorgen, dass HealtheConnections die HITRUST-Anforderungen erfüllte und eine sichere Passwortverwaltung bekam. Sie entschieden sich für LastPass – der guten Integrationsoptionen, flexibel konfigurierbaren Richtlinien und einfach bedienbaren Oberfläche wegen.

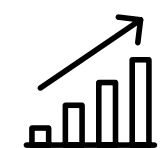


## Lösung

Die Passwörterstellung war für HealtheConnections bislang ein Problem gewesen. Die Organisation hatte zur Erstellung starker Passwörter keinen Standardprozess; oft genug wurden Zugangsdaten auf Papier notiert. Mit dem Passwortgenerator von LastPass kann HealtheConnections nun für jedes Konto ein einmaliges, aus 12 Zeichen bestehendes Passwort erstellen. Ob dieses Passwort Buchstaben, Ziffern und/oder Sonderzeichen enthalten soll, lässt sich festlegen. Anastos: *„Der Passwortgenerator gehört in LastPass zu unseren Lieblingsfunktionen. Wir müssen recht häufig Passwörter zurücksetzen, und mit dem Generator geht das jetzt für alle ganz leicht.“*

HealtheConnections hatte außerdem nach einem Weg gesucht, die Zugangsdaten des gesamten Teams sicher zu verwahren. LastPass speichert alle Passwörter und andere wichtige Informationen in einem so genannten Passwort-Vault. Ob Passwörter, vertrauliche Notizen oder Kreditkartendaten, im Vault ist all dies sicher unter Verschluss. LastPass verfügt über eine Zero-Knowledge-Architektur. Die Vault-Daten sind durch AES-256-Bit-Verschlüsselung und 600.000 Runden PBKDF2-SHA-256-Hashing mit Salting geschützt. Hashing macht Datenausgaben unleserlich, Salting wiederum macht einzelne Datenausgaben einmalig und erschwert dadurch ihren Abgleich noch einmal. Sweet erklärt: *„Unsere bisherige Methode der Passwortverwaltung war alles andere als sicher. Mit LastPass haben wir jetzt einen Ort, an dem unsere Mitarbeiter Notizen und Passwörter sicher verwahren können.“*





### Ergebnis

HealtheConnection verbesserte dank LastPass seinen Sicherheitsstatus maßgeblich und erhielt die HITRUST-Zertifizierung für sein Portal umgehend. Vier Jahre sind nun seit der Einführung von LastPass vergangen. Die Nutzungsrate für die Lösung liegt inzwischen organisationsweit bei 98%! Sweet: *„Die Einführung von LastPass funktionierte wirklich völlig reibungslos. Das LastPass-Team hat uns dabei richtig gut unterstützt“*. Damit die Nutzungsrate noch weiter steigt, steht das Sicherheitsteam der Belegschaft mit Rat und Tat zur Seite und bietet vierteljährliche Schulungen an. Um noch besser gewappnet zu sein, führte die NPO außerdem Multifaktor-Authentifizierung über Duo ein. Nun werden Anmeldungen bei Konten über Einmalcodes verifiziert. Davon profitiert nicht nur die Sicherheit, sondern auch das Sicherheitsgefühl.

Inzwischen ist LastPass ein unverzichtbares Tool im Geschäftsbetrieb der Organisation und ein zentraler Baustein im Onboarding-Programm für neue Mitarbeiter.

**„Das Zurücksetzen von Passwörtern ist mit dem LastPass-Passwortgenerator so viel einfacher geworden! Er erzeugt auf Knopfdruck lange, einmalige Zeichenkombinationen.“**

### Brad Sweet

Anastos dazu: *„Sicherheit ist nun einmal ein Muss. Die Mitarbeiter sollen LastPass möglichst umfassend nutzen; für einen risikofreien Geschäftsbetrieb ist das aus unserer Sicht ganz entscheidend.“* Bei HealtheConnections fand man außerdem die anpassbaren Richtlinien für die Automatisierung des Offboardings von Mitarbeitern praktisch. Sweet erklärt: *„LastPass hat für alles Wichtige passende Richtlinien, das gefällt uns. Wichtig für uns war beispielsweise, ausscheidenden Mitarbeitern sofort den Zugriff entziehen zu können. Mit bestimmten Parametern können wir auch die Passwortstärke und die Wiederverwendung von Passwörtern steuern und so unsere Passworthygiene nach und nach verbessern.“*

**Finden Sie heraus, wie HealtheConnections seine Passwortsicherheit mit LastPass verbesserte.**

**LastPass kontaktieren**