LastPass für Gesundheitsanbieter

Zum Gesundheitswesen gehören sämtliche Einrichtungen, die zur Förderung und Erhaltung der Gesundheit beitragen: private und staatliche Krankenhäuser, Rehakliniken, medizinische Dienste, Pharmaunternehmen, Medizingerätehersteller, Krankenkassen und F+E-Institutionen. Die Branche umfasst ein komplexes Netz aus Fachleuten, Einrichtungen und Technologien.

Lebenswichtig für Gesundheitsanbieter: unbefugten Zugriff vermeiden

Gesundheitsanbieter haben eine hohe Verantwortung für den Schutz sensibler Patienten- und Kundendaten – Patientenakten, identifizierbare Gesundheitsinformationen (PHI), Pflegedatenbanken oder Finanzdaten im Zusammenhang mit Patienten, Dienstleistern oder Produktanbietern. Cyberkriminelle haben zusehends den Gesundheitssektor im Blick, da dort signifikante Sicherheitslücken durch unzulängliche Passwortverwaltung und Zugriffssteuerung bestehen. Werden Zugriffsrechte unmotiviert vergeben oder nach dem Ende von Verträgen mit Personal oder Lieferanten nicht sofort wieder entzogen, erzeugt dies weitere Schwachstellen und erhöht das Risiko unbefugter Zugriffe.

Gesundheitseinrichtungen, die eine Cloud-first-Strategie haben, sind mit wachsenden Herausforderungen konfrontiert, was die sichere Passwort- und Zugriffsverwaltung über all die genutzten Tools und Plattformen hinweg angeht. Eine schlecht konfigurierte Infostruktur, veraltete Workstations und nicht abgesicherte gemeinsam genutzte Geräte sind ein Sicherheitsrisiko; das gilt auch für den häufig unkontrolliertem Zuwachs an SaaS-Anwendungen und nicht genehmigten Apps. Ohne ein zentrales Verwaltungssystem ist es noch schwieriger, die Kontrolle über den Zugriff zu behalten und ein sicheres, konsistentes Passwortverhalten durchzusetzen.

Gesundheitsanbieter müssen sich außerdem an strikte Regulierungen wie HIPAA, HITECH und ACA halten, die mit regelmäßigen Audits zum Nachweis der Compliance verbunden sind. Eine vernünftige Passwortverwaltung ist essenziell, um Bußgelder und Imageschäden zu verhindern. Lassen sich Zugangsdaten und Zugriffsrechte nicht sicher steuern, ist der Datenschutz in Gefahr. Institutionen riskieren ihre Compliance und ihren Cyberversicherungsschutz, was finanziell empfindliche Folgen haben kann.

Dem US Department of Health and Human Services (DHHS) zufolge haben Datenschutzverletzungen zwischen 2018 und 2022 um 93 % zugenommen. Ransomware-Angriffe nahmen im selben Zeitraum um 278 % zu.

Patienten brauchen Pflege – Passwörter ebenso

Als marktführender Anbieter von Lösungen für die Passwort- und Identitätsverwaltung hilft LastPass Gesundheitsanbietern dabei, ihre Herausforderungen rund um Cybersicherheit, Effizienz und Compliance zu bewältigen. LastPass erfüllt die komplexen Anforderungen einer von Zugangsdaten abhängigen Branche und ermöglicht es den Institutionen, wichtige Zugangsdaten ohne Abstriche bei Sicherheit, Datenschutz oder Zugänglichkeit nahtlos zu erstellen, zu speichern, zu verwalten und freizugeben. Die Risiken durch schwache oder unzulänglich verwaltete Passwörter sinken. Anbieter schützen ihren Betrieb und haben mehr Zeit für ihren eigentlichen Auftrag – die Gesundheitssorge.

Für Gesundheitseinrichtungen gelten strenge Sicherheitsvorschriften. Gleichzeitig möchten sie es aber IT-Administratoren, Benutzern, Lieferanten oder befristetem Personal möglichst einfach machen. Die Cloud-native Lösung von LastPass bringt beides unter einen Hut – Sicherheit und ein einfaches Zugangsdatenmanagement. Sie schützt sensible Zugangsdaten, gibt sicheren Zugriff und ermöglicht intern und extern eine sichere Freigabe von Zugangsdaten. Bei LastPass lässt sich der Zugriff über viele Richtlinien steuern. Diese verhindern den unbefugten Zugriff, vereiteln Insider-Angriffe und reduzieren Benutzerfehler.

Robuste Berichtsfunktionen geben außerdem Einblick in Benutzeraktionen und stellen so die Compliance mit Regelungen wie HIPAA, HITECH und anderen sicher. Mit LastPass sind Gesundheitsanbieter gegen Cyberbedrohungen gewappnet. Sie können effizient arbeiten und halten gesetzliche Vorgaben sicher ein.

LastPass – viele Vorteile für Gesundheitsanbieter

Gesundheitsanbieter können ihr Sicherheitsrisiko senken, indem sie ihr gesamtes Passwort-Management mit LastPass standardisieren – einfach, kostengünstig und zuverlässig.

Sicherheit	**Unbefugten Zugriff verhindern**	Anwendungen, Online-Konten, sensible Informationen und Systeme werden vor dem Zugriff Unbefugter geschützt.
	Kontendiebstahl und Datenschutzverletzungen verhindern	Online-Konten und Anwendungen sind zuverlässig verfügbar und zugänglich; Zugangsdaten bleiben stets privat.
	Kontrolle über Schatten-IT	LastPass gibt Überblick und Kontrolle über nicht genehmigte und überschüssige SaaS-Apps, die Freigabe von Zugangsdaten und Verwaltung von Zugriffsrechten. Sicherheitslücken werden aufgezeigt.
	Zugriffsmanagement erweitern	LastPass integriert sich in Identitätsanbieter wie Microsoft Entra und ermöglicht so die Benutzerverwaltung über den ganzen Mitarbeiterlebenszyklus hinweg.
Compliance	**Auflagen von Cyberversicherungen einhalten**	Cyberversicherungen stellen Anforderungen an die Passwort- und Zugriffsverwaltung – mit LastPass lassen sich diese erfüllen.
	Die Compliance fördern	LastPass ist konform mit Datenschutzgesetzen wie DSGVO, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA und SOX und Sicherheitsstandards wie NIST, CISA, Zero Trust und NERC-CIP.
	Externe Sicherheitsanforderungen einhalten	Robuste Zugriffskontrollen, Regeln für die Freigabe von Passwörtern, starke Authentifizierungsmechanismen und aussagekräftige Berichte unterstützen die Einhaltung der Sicherheitsstandards von Geschäftspartnern.
Effizienz	**Eine intuitive Benutzererfahrung bieten**	Hunderte anpassbare Richtlinien, eine flexible Rechtevergabe, detaillierte Berichterstattung und verschiedene Authentifizierungsoptionen machen LastPass zu einem unverzichtbaren Baustein im Tech-Stack.
	Den Passwortschutz standardisieren	Alle Mitarbeiter können ihre Zugangsdaten auf einfache Weise selbst verwalten.
	Helpdesk entlasten	Probleme mit Zugangsdaten wie vergessenen Passwörtern und Kontoaussperrungen gehen zurück.
Zusammenarbeit	**Teamwork durch Freigabe erleichtern**	Passwörter und Informationen lassen sich nahtlos und effizient in und außerhalb des Unternehmens freigeben – an Geschäftspartner, Homeoffice-Personal und Auftragnehmer.
	Zügige Akzeptanz und hohe Nutzungsrate	Die komfortable Oberfläche macht die Passwortverwaltung sehr einfach. LastPass wird deshalb schnell angenommen und gerne genutzt.
	Sicherheitskultur entwickeln	LastPass unterstützt Administratoren dabei, eine Sicherheitskultur im Unternehmen zu verankern und es vor Datenlecks, Kontendiebstählen und finanziellen Konsequenzen zu schützen.