LastPass für Professional Services

Zur Branche der Professional Services (Fachdienstleistungen) gehören Anbieter im Bereich Buchhaltung und Betriebsprüfung, Consulting, Engineering, Architektur, IT, Recht, Marketing, Werbung und mehr.

Schlechte Passworthygiene – ein doppeltes Risiko für Professional Services

Fachdienstleister bieten wissensbasierte Services in ihrem jeweiligen Spezialgebiet an. Unternehmen beauftragen sie in der Regel zur Erweiterung eigener Teams. Fachdienstleister müssen also nicht nur eigene Daten, sondern auch die ihrer Auftraggeber verwalten und schützen; genau deshalb sind sie für Cyberkriminelle attraktiv.

Der einfachste Weg für Kriminelle, an wertvolle Daten zu gelangen, sind kompromittierte Zugangsdaten. Dann drohen nicht nur dem Fachanbieter Datenschutzverletzungen, die Offenlegung vertraulicher Informationen, Betrug und Reputationsverlust, sondern auch seinen Vertragspartnern. Früher oder später geraten weitere Unternehmen oder Branchen in Mitleidenschaft – ein fataler Dominoeffekt.

Eine weitere Herausforderung für Professional Services von ihrem Sicherheitsrisiko abgesehen ist die vernünftige Gestaltung von Zugriff und Zusammenarbeit. Intern wie extern tauschen sie regelmäßig Daten aus, etwa Zugangsdaten für Anwendungen, Social-Media-Konten oder interne Datenbanken. Kann der Zugriff nicht auf effektive Weise gewährleistet, verwaltet und wieder entzogen werden, kommt es zu Ineffizienzen, Produktivitätsverlusten und unbeabsichtigten Schwachstellen.

Gestohlene Zugangsdaten, Social Engineering, Nutzungsfehler: Bei **74 % aller Datenschutzverletzungen** ist der Faktor Mensch relevant.

10 % der Angriffe auf Professional Services haben Benutzerfehler zur Ursache.

Eine komfortable und sichere Zugriffsverwaltung

Als marktführender Anbieter von Lösungen für die Passwort- und Identitätsverwaltung hilft LastPass Fachdienstleistern dabei, ihre Herausforderungen in puncto sichere Zugangsdaten zu bewältigen. LastPass erfüllt die Anforderungen dieser hochkollaborativen und von Zugangsdaten abhängigen Branche und ermöglicht es Professional-Services-Anbietern, wichtige Zugangsdaten ohne Abstriche bei Sicherheit, Datenschutz oder Zugänglichkeit nahtlos zu erstellen, zu speichern, zu verwalten, freizugeben und zu schützen. Mit der zentralen und sicheren Plattform von LastPass erübrigen sich riskante Methoden der Passwortverwaltung. Sensible Geschäfts- und Kundendaten sind vor unbefugtem Zugriff stets geschützt.

LastPass vereinfacht die Zusammenarbeit: Es gibt internen Teams und externen Vertragspartnern sicheren und kontrollierten Zugriff auf gemeinsam genutzte Zugangsdaten. Dabei sieht jeder im Team nur das, was für die eigene Arbeit erforderlich ist. Wird kein Zugriff mehr benötigt, kann er automatisch wieder entzogen werden. Außerdem gibt LastPass genauen Einblick und ermöglicht die Erstellung ausgefeilter Berichte. Anbieter können so ihre Compliance nachweisen und die Nutzung von Zugangsdaten überblicken. Mit LastPass gestalten Fachdienstleister ihre Zusammenarbeit effizient und verbessern ihre Sicherheit. Sie schützen damit ihren eigenen Betrieb und den ihrer Kunden.

LastPass – viele Vorteile für Professional Services

Fachdienstleister 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 Sicherheits-anforderungen einhalten	Robuste Zugriffskontrollen, Regeln für die Freigabe von Passwörtern, starke Authentifizierungsmechanismen und aussagekräftige Berichte unterstützen die Einhaltung der Sicherheitsstandards von Geschäftspartnern.
Effizienz	**Eine intuitive Benutzer-erfahrung 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.