LastPass für Finanzdienstleister

Banken, Börsen, Broker, Kreditplattformen, Kryptoanbieter, Fintech-Plattformen, Investmentgesellschaften und Wirtschaftsprüfer sind Akteure in einer komplexen Finanzinfrastruktur, zu der auch Finanzdienstleister gehören.

Passwörter – ein Risiko für Finanzdienstleister

Finanzdienstleister betreiben in einem stark digitalisierten, dynamischen Umfeld ein transaktionsintensives Geschäftsmodell und gehen mit hochsensiblen Kundendaten und Finanzprodukten um. Deshalb sind sie großen Cyberangriffsrisiken ausgesetzt. Kriminelle nutzen Infostealer, Phishing oder KI-generiertes Social Engineering zur Kompromittierung von Passwörtern und Identitäten. Dies wiederum kann zum Diebstahl von Online-Konten oder zu Ransomeware-Angriffen führen.

Die voranschreitende Umstellung in der Finanzbranche auf einen Cloud-first- und SaaS-Betrieb macht eine sichere Verwaltung von Passwörtern und Zugriffen immer schwieriger. Teil dieser Entwicklung ist ein unkontrollierter Zuwachs an SaaS-Anwendungen und Schatten-IT. Nicht genehmigte Tools und Apps erzeugen aber neue Sicherheitslücken und Intransparenzen.

Auch das verstärkt hybride Arbeiten bringt Sicherheitslücken in die Zusammenarbeit und den Zugriff, die von Angreifern nur zu gerne genutzt werden. Fehlt der Überblick über die eingesetzten Tools, lassen sich Benutzeraktivitäten kaum verfolgen und kontrollieren. Die Zusammenarbeit über nicht genehmigte Software, etwa die private E-Mail oder Messenger-Apps, unterläuft Sicherheitsvorschriften und setzt Daten unnötigen Risiken aus. All dies ist ein Problem und eine Gefahr – für Kunden, die Opfer von Betrug und Social Engineering werden können, für Mitarbeiter, die weniger produktiv sind, und für das Unternehmen, dem Datenschutzverletzungen, Ransomware-Erpressungen, Reputationsschäden und Bußgeldverfahren drohen.

78 % der Datenschutzverletzungen in der Finanzdienstleistungsbranche haben ihre Ursache in unerlaubten Systemzugriffen, Social Engineering und Benutzerfehlern (2024 Verizon DBIR).

Moderner Passwortschutz und transparente Sicherheit

Als marktführender Anbieter von Lösungen für die Passwort- und Identitätsverwaltung hilft LastPass Finanzdienstleistern, Probleme rund um die eigene Cybersicherheit und Produktivität zu lösen. LastPass erfüllt die komplexen Anforderungen eines durchdigitalisierten, von Zugangsdaten abhängigen Geschäftsbetriebs und ermöglicht es Finanzdienstleistern, wichtige Zugangsdaten ohne Abstriche bei Sicherheit, Datenschutz oder Zugänglichkeit nahtlos zu erstellen, zu speichern, zu verwalten, freizugeben und zu schützen.

Finanzunternehmen müssen strikte Sicherheits- und Compliance-Anforderungen einhalten, möchten es Administratoren, Mitarbeitern und externen Akteuren aber auch nicht unnötig schwer machen. Mit seiner Cloud-nativen Lösung wird LastPass beidem gerecht: Sensible Zugangsdaten werden geschützt und lassen sich intern wie extern einfach und sicher freigeben. Jeder Login wird abgesichert; die Durchsetzung von Zugriffsrichtlinien garantiert Transparenz, Kontrolle und die Einhaltung von Compliance-Vorschriften.

Ausgefeilte Berichte geben den Beteiligten Überblick und erleichtern Audit-Prozesse. LastPass schafft Vertrauen, indem es unbefugte Zugriffe verhindert und das Unternehmen gegen Cyberrisiken wappnet.

LastPass

MEHR ERFAHREN

LastPass – viele Vorteile für Finanzdienstleister

Finanzdienstleister 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	**Den Passwortschutz standardisieren**	Hunderte anpassbare Richtlinien, eine flexible Rechtevergabe, detaillierte Berichterstattung und verschiedene Authentifizierungsoptionen machen LastPass zu einem unverzichtbaren Baustein im Tech-Stack.
	Zugriffsmanagement erweitern	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.