LastPass für den Einzelhandel

Einzelhändler bieten Waren und Dienstleistungen für den privaten Konsum an. Von inhabergeführten Geschäften vor Ort bis hin zu den großen multinationalen Handelsketten umfasst die Branche Unternehmen jeder Größe. Fachhandel, Discounter, Drogeriemärkte, Kaufhäuser, Shops, Kiosks, Boutiquen, Supermärkte: Einzelhandel erfolgt über physische Niederlassungen und/oder E-Commerce-Plattformen.

Der beste Diebstahlschutz: Passwort-Management

Einzelhändler sind Cyberbedrohungen ausgesetzt. Ihr Geschäftsmodell ist transaktionsintensiv, und ihr Personal kommt mit Zahlungskartendaten in Kontakt. Dies macht Einzelhändler zu einem attraktiven Angriffsziel für Kriminelle, die sensible Kundendaten stehlen oder den Geschäftsbetrieb sabotieren möchten. Meist erfolgt der Zugriff über schwache, mehrfach verwendete oder sorglos weitergegebene Zugangsdaten.

Die notorisch hohe Personalfluktuation im Einzelhandel verschärft das Problem, denn häufig wird der Systemzugriff nach dem Ausscheiden von Mitarbeitern nicht sofort entzogen. Solche Lücken nutzen die Angreifer. Für die IT- und Sicherheitsteams ist die Verwaltung der Zugriffsrechte ständig wechselnder Mitarbeiter und der zahllosen SaaS-Anwendungen eine große Herausforderung.

All dies gefährdet nicht nur den Geschäftsbetrieb, sondern wirkt sich auch auf die Verbraucher mit ihrer generell schwachen Markentreue aus. Die Gefahr, dass sie nach einem bekannt gewordenen Vorfall abgeschreckt sind und woanders einkaufen, ist entsprechend groß. Ein Vorfall mit kompromittierten Zugangsdaten genügt, damit Kunden Vertrauen verlieren und Finanz- und Reputationsschäden gesetzt werden – angesichts scharfer Konkurrenz und schmalen Gewinnspannen ein hohes Risiko.

„Das Risiko, nach dem nächsten Cyberangriff den Geschäftsbetrieb einstellen zu müssen, ist für kleine Händler besonders hoch.“ – dieser Aussage stimmte in einer Umfrage der US Chamber of Commerce mehr als ein Drittel der Befragten zu.

60 % aller Verbraucher und 74 % der Verbraucher mit höherem Einkommen würden bei einem Anbieter, der Opfer eines Datendiebstahls geworden ist, nicht mehr einkaufen. (Cyberint)

Nicht nur schauen, sondern kaufen: Passwörter

Als marktführender Anbieter von Lösungen für die Passwort- und Identitätsverwaltung hilft LastPass dem Einzelhandel dabei, seine Herausforderungen rund um die Cybersicherheit zu bewältigen. LastPass erstellt, speichert und verwaltet Zugangsdaten auf sichere Weise und gibt Mitarbeitern, Geschäftspartnern und Lieferanten nahtlosen Zugriff. Es ist ideal für die dynamische und transaktionsintensive Einzelhandelsbranche. LastPass eliminiert schwache, mehrfach genutzte und veraltete Passwörter. So sinkt das Risiko des Diebstahls von Zugangsdaten – eine verbreitete Sicherheitslücke im Einzelhandel. Störungen des täglichen Geschäftsbetriebs werden vermieden.

Als Cloud-native Plattform mit einfach zu nutzenden Tools verbindet LastPass robuste Sicherheit mit einer Oberfläche, die für Administratoren wie Benutzer gleichermaßen intuitiv ist. Funktionen für eine sichere Freigabe, automatische Bereitstellung und Entziehung von Zugangsdaten und die zentrale Zugriffssteuerung vereinfachen die Verwaltung eines häufig wechselnden Personalstamms und verhindern den unbefugten Zugriff auf Systeme und sensible Daten. Erweiterte Berichtsfunktionen geben IT-Teams den nötigen Einblick, um Passwortrichtlinien durchzusetzen, Zugriffsaktivitäten zu prüfen und die Compliance des Geschäftsbetriebs nachzuweisen.

LastPass ist für Einzelhändler die ideale Lösung: Es sichert Zugangsdaten ab, sorgt für eine reibungslose Kundenerfahrung und wappnet den Betrieb gegen Cyberangriffe.

LastPass

MEHR ERFAHREN

LastPass – viele Vorteile für den Einzelhandel

Einzelhändler 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 Mitarbeiter-lebenszyklus hinweg.
Compliance	**Auflagen von Cyber-versicherungen 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 Authentifizierungs-optionen 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.