



LastPass voor de retailsector

Retailers verkopen goederen en diensten voor persoonlijk gebruik direct aan consumenten. Dat maakt deze sector ontzettend divers, van kleine lokale winkeliers tot aan internationale ketens. Ze verkopen online, maar ook in speciaalzaken, supermarkten en bouwmarkten, kleine winkels en nog veel meer.

De beste verdediging voor de retailindustrie: wachtwoordbeheer

Retailers staan bloot aan onophoudelijke cyberbedreigingen. De retailsector is een aantrekkelijk doelwit voor hackers, met grote transactievolumes, veel medewerkers en veel personeelsverloop, en toegang tot waardevolle creditcardgegevens en gevoelige klantgegevens. Voor cybercriminelen zijn er veel toegangspunten, en er valt veel te halen. Hackers werken met zwakke, hergebruikte of gedeelde wachtwoorden om systemen te infiltreren, gegevens te stelen en operationele activiteiten te verstoren.

Een hoog personeelsverloop vergroot de risico's: gegevens raken snel verouderd en toegang wordt lang niet altijd ingetrokken. Het zorgt voor veel kwetsbaarheden, waar hackers maar al te graag misbruik van maken. Voor IT- en beveiligingsteams is het een voortdurende uitdaging om toegangsrechten te beheren voor constant veranderend personeel en talloze SaaS-toepassingen en accounts.

Deze risico's zijn niet alleen relevant voor interne operaties, maar ook voor de klantervaring. Merkentrouw is in de retailsector vaak ver te zoeken, en een cyberaanval, gegevenslek of uitval door ransomware jaagt klanten effectief weg. Eén incident kan het vertrouwen beschadigen en blijvende financiële en reputatieschade aanrichten – terwijl de concurrentie in de retail vaak sowieso al intens is, en de marges flinterdun.

MKB-retailers zijn vaker dan andere bedrijven niet bestand tegen cyberaanvallen. Ruim één derde van de kleine winkeliers in een enquête van de Amerikaanse Kamer van Koophandel gaf aan dat een grote aanval voor hen een faillissement zou betekenen.

60% van alle klanten in de retail en 74% van de klanten met een hoog inkomen zou bedrijven vermijden die onlangs te maken hebben gehad met een hack of gegevenslek. (Cyberint)

Wachtwoordbeveiliging is geen extraatje



LastPass loopt wereldwijd voorop als vertrouwde leverancier van software voor wachtwoord- en identiteitsbeheer, en heeft unieke mogelijkheden om retailers te helpen met hun cyberbeveiliging. LastPass is gemaakt voor de snelle wereld van retail, met zijn hoge transactievolumes en vele contacten. De software kan veilige aanmeldingsgegevens maken, opslaan en beheren, en een gecontroleerde toegang voor medewerkers, partners en externe partijen stroomlijnen. Door zwakke, gedeelde en verouderde wachtwoorden te vervangen, verlaagt LastPass het risico dat hackers uw aanmeldingsgegevens stelen – en daarmee blokkeert het de aanvalsmethode die hackers het meeste toepassen in de retail.



LastPass werkt in de cloud en is ontzettend gebruiksvriendelijk. Het zorgt voor een uitstekende beveiliging, maar het is ook handig voor beheerders en gebruikers, ongeacht hun technische expertise. De software maakt het handig om toegang te delen en geautomatiseerd accounts in te richten en in te trekken. Gecentraliseerd toegangsbeheer maakt het makkelijk om toegangsrechten actueel te houden als u veel personeelsverloop hebt, en voorkomt ongeoorloofde toegang tot systemen en gevoelige gegevens. Met geavanceerde rapportages kunnen IT-teams zien hoe uw medewerkers omgaan met wachtwoorden, onder andere om wachtwoordbeleid gericht af te dwingen, toegangsrechten te beoordelen en compliance aan te tonen.



Voor retailers is LastPass de perfecte oplossing om aanmeldingsgegevens veilig te houden, de klantervaring te waarborgen en hun bedrijf te wapenen tegen digitale bedreigingen.



Voordelen van LastPass voor retailers

De makkelijkste, meest betaalbare en meest betrouwbare manier voor retailers om hun cyberrisico en operationele risico terug te dringen, is door hun wachtwoordbeheer bedrijfsbreed te organiseren met LastPass.

Beveiliging	Voorkom ongeoorloofde toegang	Houd hackers en ongeoorloofde gebruikers buiten uw toepassingen, online accounts, gevoelige gegevens en systemen.
	Blokkeer overnames van uw accounts en gegevenslekken	Zorg dat online accounts en toepassingen betrouwbaar toegankelijk zijn voor geautoriseerde gebruikers en dat aanmeldingsgegevens beschermd blijven.
	Krijg schaduw-IT onder controle	Krijg zicht op toepassingen die medewerkers gebruiken zonder toestemming en beheer van de IT-afdeling. Voorkom onnodige abonnementen en volg wie er aanmeldingsgegevens deelt voor welke accounts. Beheer de toegangsrechten en herken kwetsbaarheden in het systeem
	Breid veilig toegangsbeheer uit	Integreer naadloos met identiteitsproviders als Microsoft Entra en verbeter het gebruikersbeheer van inhuur tot aan vertrek.
Naleving	Voldoe aan voorwaarden van cyberverzekeraars	Toon eenvoudig aan dat u voldoet aan de vereisten die cyberverzekeraar stellen aan wachtwoord- en toegangsbeheer.
	Ondersteun compliance	Voldoe aan de vereisten van wet- en regelgeving, onder andere voor de AVG, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA en SOX, en voor kaders voor cyberbeveiliging zoals NIST, CISA, Zero Trust, en NERC-CIP.
	Garandeer de beveiliging die partners vereisen	Voldoe aan de strenge beveiligingsvereisten van partners, met krachtige systemen voor toegangscontrole, regels voor het delen van wachtwoorden, sterke verificatiemechanismen en nuttige rapportages.
Optimalisatie	Bied iedereen een intuïtieve gebruikservaring	Profiteer van uitgebreide instelbare beleidsregels, flexibele machtigingen, gedetailleerde rapportages, en verschillende opties voor de verificatie.
	Standaardiseer de wachtwoordbeveiliging	Vereenvoudig het wachtwoordbeheer voor alle medewerkers binnen de organisatie.
	Verlaag de werkdruk voor de helpdesk	Verlos de helpdesk van problemen door aanmeldingsgegevens, zoals vergeten wachtwoorden en geblokkeerde accounts.
Samenwerking	Stroomlijn teamwerk met gedeelde toegang	Maak het makkelijk om wachtwoorden en andere informatie zowel intern als extern veilig te delen, voor meer productiviteit en efficiency voor partners, freelancers en thuiswerkers.
	Optimaliseer aanname & gebruik	Bevorder de aanname en het gebruik door medewerkers met een intuïtieve, gebruiksvriendelijke interface, die alle taken rondom wachtwoordbeheer makkelijker maakt.
	Bouw een veiligheidscultuur	Zorg ervoor dat alle medewerkers actief bijdragen aan een hoog veiligheidsbewustzijn en de organisatie beschermen tegen veel voorkomende bedreigingen rondom gestolen of gelekte aanmeldingsgegevens.