



LastPass voor verzekeringskantoren

Verzekeringsmakelaars werken als intermediair tussen verzekeraars en klanten, met verzekeringsadvies, verkoop van assurantiën, ondersteuning bij claims, risicobeoordelingen en ondersteuning van klanten.

De zekerheid voor de verzekeringsbranche: wachtwoordbeheer met een goede dekking

Verzekeringsgegevens zijn altijd gevoelig en vertrouwelijk, en dat maakt ze een waardevol doelwit voor hackers. Cybercriminelen misbruiken zwakke of gestolen wachtwoorden via phishing, social engineering en andere aanvalstactieken. Zo krijgen ze ongeoorloofde toegang tot systemen en kunnen ze gegevens stelen of accounts overnemen. Dit soort incidenten vormt een groot risico, zowel voor het kantoor als voor de klanten. Een inbraak in het systeem schaadt het vertrouwen, en hackers kunnen gevoelige persoonlijke of financiële informatie bemachtigen.

Door de digitale transformatie staan kantoren voor grote uitdagingen rondom wachtwoord- en toegangsbeheer: er zijn simpelweg ontzettend veel verschillende systemen, accounts en wachtwoorden. Het risico op ongeoorloofde toegang groeit, en het is in de praktijk vaak lastig om goed te volgen wie er wanneer toegang heeft tot welke databases, cloudplatformen, of rekeninggegevens.

Veel kantoren werken nog met verouderde systemen en inadequaat beheer van aanmeldingsgegevens, wat de deur alleen maar verder open zet voor hackers. Compliance, bijvoorbeeld met de AVG, is essentieel om boetes en juridische consequenties te voorkomen. Sterk wachtwoordbeheer is inmiddels dan ook onmisbaar. Alleen zo kunnen kantoren hun operationele werk vertrouwelijk houden. Zonder goede oplossing loopt u het risico op gegevenslekken, ransomware, reputatieschade en ingrijpen door toezichthouders.

Ruim 88% van de grote verzekeraars gebruikt externe krachten voor een deel van hun dienstverlening, en kantoren werken steeds meer met technologie voor persoonlijke service in real-time. Door deze ontwikkeling hebben hackers veel meer aanvalsmogelijkheden.

Voorkom ongeoorloofde toegang en gegevensverlies



LastPass loopt wereldwijd voorop als vertrouwde leverancier van software voor wachtwoord- en identiteitsbeheer, en heeft unieke mogelijkheden om verzekeringskantoren te helpen met hun cyberbeveiliging. Met LastPass kunnen verzekeringsmakelaars aanmeldingsgegevens veilig aanmaken, opslaan, beheren en delen, met handige toegang zonder concessies aan de vertrouwelijkheid. Zo blijven gevoelige klantgegevens goed beschermd. LastPass is gemaakt voor de behoeften van de verzekeringsbranche, waarin alles draait om vertrouwen en vertrouwelijkheid. De software levert een centrale oplossing voor solide beheer van aanmeldingsgegevens en vermindert het risico op gegevenslekken door wachtwoorden.



Verzekeringsmakelaars moeten voldoen aan strenge compliancevereisten, maar ze moeten ook efficiënt kunnen werken. Met LastPass kunnen medewerkers zich overal veilig aanmelden en probleemloos gegevens delen met collega's en partners. Het ondersteunt een toegangsbeleid op maat en geeft real-time inzicht in het gebruik van aanmeldingsgegevens. De geavanceerde rapportagemogelijkheden maken het makkelijk om compliance te demonstreren met de AVG en andere regelgeving, en ze maken risico's zichtbaar voordat deze leiden tot een incident. Met LastPass kunnen verzekeringsmakelaars de gegevensbeveiliging voor hun bedrijf en hun klanten op orde krijgen, en zo een veilige basis leggen voor groei tijdens de digitale transformatie.

Voordelen van LastPass voor verzekeringskantoren

De makkelijkste, meest betaalbare en meest betrouwbare manier voor verzekeringskantoren om hun cyber risico 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.