



LastPass voor de productie-industrie

De productie-industrie is een breed werkveld, dat uiteenlopende sectoren bedient: van auto's tot bouwmaterialen, van cosmetica tot voeding, en van medicijnen tot aan textiel, kunststof, machines en nog veel meer.

Neem wachtwoordbeveiliging op in de productielijn

De productie-industrie speelt een essentiële rol voor de wereldwijde infrastructuur. Dat maakt deze sector een interessant doelwit voor cybercriminelen die leverketens willen verstoren, intellectuele eigendommen willen stelen of operaties willen blokkeren, bijvoorbeeld met ransomware. Hackers maken hiervoor vaak misbruik van gelekte, gekraakte of gestolen aanmeldingsgegevens. Dit is de eenvoudigste en meest effectieve manier om ongeoorloofd binnen te komen in gevoelige systemen. Eenmaal binnen kunnen ze bijvoorbeeld accounts overnemen, operationele systemen manipuleren of gevoelige gegevens stelen. Dat maakt producenten kwetsbaar: de gevolgen van één lek kunnen doorwerken in de complete leverketen.

De directe financiële gevolgen zijn bij een cyberaanval nog maar het begin. Verstoringen in het werk kunnen productielijnen stilleggen, leveringen vertragen en reputaties vernietigen. En bij gestolen intellectuele eigendommen kunnen alle investeringen in R&D ten goede komen aan een concurrent. Dit soort incidenten hebben ook een uitwerking op toeleveranciers en klanten.

Bovendien zijn producenten vaak wettelijk verplicht om hun gegevensbescherming op orde te hebben. Een lek zorgt dan al snel voor veel juridische ellende en extra problemen met de compliance. Producenten zijn steeds meer afhankelijk van onderling verbonden technologie. Dat betekent dat een goede beveiliging van aanmeldingsgegevens essentieel is voor de integriteit van de volledige sector.

Ransomware was betrokken bij 71% van de incidenten. Het aantal aanvallen neemt jaarlijks met 125% toe, en cyberrisico's staan inmiddels in de top 3 van externe risico's voor de productie-industrie.

Beveilig en stroomlijn uw hele bedrijf



In de productie-industrie is er vaak veel afstand tussen IT-teams en de mensen op de werkvloer. Daardoor is de invoer van een standaard wachtwoordbeheerder voor de hele organisatie vaak één van de meest eenvoudige en effectieve manieren om risico's door aanmeldingsgegevens terug te dringen. Door LastPass organisatiebreed uit te rollen garanderen bedrijven dat alle medewerkers, van de IT-afdeling tot aan de productiemedewerkers, dezelfde veilige en gestroomlijnde processen voor veilig wachtwoordbeheer gebruiken. Dit vermindert het gebruik van zwakke of hergebruikte wachtwoorden en ondersteunt best practices, die hackers effectief buiten de deur houden.



LastPass biedt een gebruiksvriendelijke oplossing in de cloud die wachtwoordbeveiliging makkelijk maakt voor alle medewerkers – ook als ze niet handig zijn met computers. De software zorgt ervoor dat iedereen sterke wachtwoorden gebruikt, ze centraal opslaat en waar nodig veilig kan delen. Tegelijkertijd kan de IT-afdeling een strenge toegangscontrole implementeren. Met LastPass kunnen bedrijven in de productie-industrie de kloof tussen de IT-afdeling en de werkvloer overbruggen en kwetsbaarheden in hun systemen afdichten. Daarnaast ondersteunt LastPass de compliance, wat de beveiliging versterkt en de operationele efficiency bevordert.



Voordelen van LastPass voor de productie-industrie

De makkelijkste, meest betaalbare en meest betrouwbare manier voor producenten 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.
	Breid veilig toegangsbeheer uit	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.