# LastPass für Industrieunternehmen

*Der Produktionssektor umfasst so unterschiedliche Branchen wie die KfZ-Industrie, Bau, Kosmetik, Lebensmittel und Getränke, Pharma, Textilien, Verpackungen, Maschinenbau und mehr.*

## Mehr Prozesseffizienz durch Passwortverwaltung

Das produzierende Gewerbe ist ein wichtiges Standbein der globalen Wirtschaft und deshalb im Fadenkreuz von Cyberkriminellen, die Betriebsabläufe und Lieferketten sabotieren und geistiges Eigentum stehlen möchten. Kompromittierte Zugangsdaten sind für Angreifer der einfachste und wirksamste Weg in sensible Systeme, um diese auszuspionieren oder lahmzulegen, Benutzerkonten zu kapern, Betriebsprozesse zu manipulieren oder wertvolle Daten zu stehlen. Industrieunternehmen sind also enorm gefährdet. Hier steht viel auf dem Spiel; eine einzige Datenschutzverletzung kann fatale Effekte in der gesamten Lieferkette haben.

Die Auswirkungen von Cyberangriffen auf produzierende Unternehmen gehen weit über finanzielle Verluste hinaus. Betriebsstörungen können den Ausfall von Produktionsprozessen bedeuten und das Markenimage schädigen; gestohlene Daten können in die Hände von Wettbewerbern gelangen und diesen unfaire Vorteile verschaffen. Die schädlichen Effekte wirken sich auf die gesamte Lieferkette von den Zulieferern bis hin zu den Konsumenten aus.

Hinzu kommen strenge Datenschutz- und Compliance-Auflagen, die auch von der Industrie eingehalten werden müssen. Jede Datenschutzverletzung kann hier eine Katastrophe bedeuten. Auch im Produktionssektor nimmt die digitale Vernetzung zu. Um Risiken zu minimieren und die Integrität der gesamten Branche zu bewahren, ist der Schutz von Zugangsdaten also wichtig.

**71 % der Vorfälle haben mit Ransomware zu tun. Die Angriffshäufigkeit steigt jährlich um 125 %. Cyberangriffe gehören inzwischen zu den Top-drei-Risiken für Industrieunternehmen.**

## Den ganzen Betrieb sicher und effizient gestalten

In Industrieunternehmen, wo zwischen der IT-Abteilung und den Produktionsstätten oft große Distanz herrscht, ist die Einführung einer standardisierten Passwortverwaltung einer der einfachsten und wirksamsten Wege, um Risiken im Zusammenhang mit Zugangsdaten zu senken. Durch eine unternehmensweite Einführung von LastPass lässt sich sicherstellen, dass für alle Mitarbeiter von der IT-Technikerin bis hin zum Arbeiter in der Produktionshalle derselbe sichere Prozess für die Passwortverwaltung gilt. Die Nutzung schwacher oder mehrfach verwendeter Passwörter wird weniger wahrscheinlich, der Umgang mit Zugangsdaten, dem Haupteinfallstor für Kriminelle, wird weniger nachlässig.

LastPass ist Cloud-nativ. Es ist benutzerfreundlich und macht Passwortsicherheit für alle im Unternehmen einfach, auch diejenigen ohne große technische Kenntnisse. Die Lösung ermöglicht die sichere Erstellung, Speicherung und Freigabe von Zugangsdaten und eine stringente Zugriffssteuerung. Industrieunternehmen, die LastPass betriebsweit einführen, schließen die Sicherheitslücke zwischen IT und Produktion. Sie beseitigen Schwachstellen und verbessern effizient ihre Compliance. So profitieren sie in puncto Sicherheit und betrieblicher Effizienz.

# LastPass – viele Vorteile für Industrieunternehmen

Produktionsunternehmen 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 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, detail-lierte 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. |