

Gründe, warum Ihr Unternehmen einen Passwortmanager benötigt



Wichtige Daten sind jederzeit und überall zugänglich

Dank verschlüsselter Speicherung von Zugangsdaten, Kreditkarten, Notizen und persönlichen Daten haben Sie über einen zentralen und sicheren Ort Zugriff auf alles, was Sie brauchen.

In **64%** aller Organisationen **wird die Produktivität** täglich durch **Zugriffsprobleme beeinträchtigt**.
Quelle: StrongDM, 2022

Maßgeschneiderte Zugriffsberechtigungen für Mitarbeiter

Vertriebsmitarbeiter sollten keinen Zugang zu HR-Konten haben – und umgekehrt. Durch die Möglichkeit, volle und eingeschränkte Zugriffsrechte auf Systeme zu gewähren, können Unternehmen für bestimmte Systeme nur Lesezugriff und für andere Systeme vollen Zugriff gestatten. Gleichzeitig haben die Verantwortlichen volle Einsicht, wer wann und wo auf was zugegriffen hat.

Sichere gemeinsame Nutzung des Zugangs

Mit einem Passwortmanager ist es leicht und sicher, Zugangsdaten, Zahlungsdaten, persönliche Daten und vertrauliche Notizen zu teilen. Unternehmen und Organisationen können Gruppen und gemeinsam genutzte Ordner erstellen, um verschiedene Elemente mit Abteilungen, Teams oder einzelnen Mitarbeitern zu teilen. Das schließt die Möglichkeit ein, einen zeitlich begrenzten Zugang für zusätzliche Kontrolle festzulegen.

Effektiveres Arbeiten dank automatisierter Prozesse

Passwortmanager sparen Zeit – bei jeder Anmeldung, Zahlung und jedem Formular. Zugangsdaten, persönliche Daten und Zahlungsdaten werden mit einem Klick sicher gespeichert und können automatisch ausgefüllt werden, wann immer und wo immer sie benötigt werden.

Einfaches Onboarding und Offboarding von Mitarbeitenden

Das Onboarding mit einem Passwortmanager läuft ganz einfach: Neue Teammitglieder erhalten sofortigen Zugriff auf alle wichtigen Daten. Das Offboarding ist genauso einfach. Der Passwortmanager vermeidet das Risiko und die Ungewissheit, die damit verbunden sind, dass ehemalige Mitarbeitende weiterhin Zugang zu den Unternehmensdaten haben. Beim Verlassen des Unternehmens kann die Zugangsberechtigung aufgehoben und Daten einfach übertragen werden, sodass sie im Unternehmen bleiben.

57 % aller Organisationen benötigen mehrere **Tage, Wochen oder sogar Monate** für das **Offboarding** von technischem Personal. Quelle: StrongDM, 2022

Hackersicherere Anmeldedaten werden zum neuen Standard

Mit einem Passwortmanager kann die IT-Abteilung sicherstellen, dass sich alle Mitarbeiterinnen und Mitarbeiter an die Passwortrichtlinien des Unternehmens halten, etwa was die Mindestlänge angeht. Für einen noch besseren Schutz nutzen Sie die mehrstufige Authentifizierung, die automatische Sperre von Geräten mit öffentlichem Zugang oder das Sperren der externen Datenweitergabe.

68 % der Sicherheitsvorfälle basierten auf einem **menschlichen Fehler**, wie beispielsweise ein Hereinfallen auf einen Social Engineering-Angriff. Quelle: Verizon, 2024

Datenlecks frühzeitig erkennen, bevor sie dem Unternehmen schaden

Durchschnittlich brauchen Unternehmen 194 Tage, um ein Datenleck zu entdecken. Das verschafft Cyberkriminellen jede Menge Zeit, um Daten zu stehlen, zu verkaufen oder auszunutzen (Statista, 2024). Mit einem Passwortmanager senken Sie dieses Risiko durch frühzeitige Erkennung: Sie werden gewarnt, wenn Domains, Zugangsdaten, E-Mails oder sensible Daten Ihres Unternehmens kompromittiert wurden.

Warum ist NordPass die richtige Wahl für Ihr Unternehmen?

Kosteneffizient

Top Preis-Leistungs-Verhältnis – mit Rund-um-die-Uhr-Support, einer einfachen Benutzeroberfläche sowie einem Portfolio fortschrittlicher Sicherheitstools zu einem konkurrenzfähigen Preis. NordPass bietet große Leistung für kleines Geld, ohne versteckte Kosten.

Benutzerfreundlich

Ein Passwortmanager kann nur funktionieren, wenn er unternehmensweit eingesetzt und richtig verwendet wird. Deshalb setzt NordPass auf Benutzerfreundlichkeit mit übersichtlichen Menüs und ohne Fachjargon.

Zukunftsorientiert

NordPass nutzt modernste, sichere und schnelle Technologie und verwendet als einziger Passwortmanager den XChaCha20-Verschlüsselungsalgorithmus. Gleichzeitig wird das automatische Ausfüllen durch maschinelles Lernen stetig verbessert.

Sicher

Die Ende-zu-Ende-Verschlüsselung und Zero-Knowledge-Architektur von NordPass garantieren die höchsten Standards für, Privatsphäre und Sicherheit Ihres Unternehmens. NordPass Business ist durch ISO 27001 sowie SOC 2 Type 2 zertifiziert und erfüllt die Vorgaben von HIPAA. Darüber hinaus wird NordPass Business von Cure53 unabhängig geprüft.

Welche Vorteile bietet NordPass für jede Abteilung?

Marketing

Mit NordPass können Marketing-Teams sensitive Daten zu abteilungsübergreifenden Projekten speichern und managen. Gleichzeitig wird das Teilen von Zugangsdaten einfach und sicher, während das Team bei jeder Anmeldung, jedem auszufüllendem Formular und jeder Zahlung Zeit spart. Die Sicherheit muss nicht unter Zeitdruck leiden.

Vertrieb

NordPass ermöglicht Vertriebsmitarbeitern schnellen und sicheren Zugriff auf interne Accounts und sensitive Kundeninformation, wie persönliche Details oder Finanzdaten. Und das ortsunabhängig, im Büro genauso wie unterwegs, wenn die großen Deals verhandelt werden.

IT und Operations

NordPass ist das Tool, das Ihre Teams in IT und Operations dabei unterstützt, effizienteres Onboarding zu gewährleisten. Sensible Daten sind kategorisiert und den entsprechenden Abteilungen zugeordnet.

Finanzabteilung

NordPass bewahrt Zugangsdaten und Zahlungsinformationen geschützt in einem verschlüsselten Tresor auf. Gleichzeitig ist das Teilen von gespeicherten Elementen sicher und effizient.

Personalabteilung

NordPass ermöglicht Ihrer Personalabteilung, die hochsensiblen Daten, wie Arbeitsverträge, Gehaltsinformation oder Visumsanträge, effizient zu organisieren und zu schützen. Mit NordPass sind diese Daten keinen externen Risiken ausgesetzt.



Sie haben Fragen? Kontaktieren Sie uns!

Wir bieten rund um die Uhr Support für alle unsere Geschäftskunden.



sales@nordsecurity.com



nordpass.com/business

