MDSYSTEC®

PRAXIS DES PASSWORTMANAGERS

Wie Sie den passenden Passwortmanager auswählen und erfolgreich einführen

Jonas Miedl

Geschäftsführer & Chief AI Officer (CAIO)

MDSYSTEC GmbH · ISO 9001 & 27001 zertifiziert

BIHK-Reihe Cybersicherheit
IHK für München und Oberbayern
Dienstag, 14. April 2026 | 11:00 – 12:00 Uhr

JONAS MIEDL

Geschäftsführer & Chief AI Officer (CAIO)

MDSYSTEC GmbH

Full-Service IT-Provider

Managed Services · Consulting · Security

- ISO 9001 & 27001 zertifiziert
- Mitterskirchen / Niederbayern
- KMU bis Enterprise
- www.mdsystec.de

LEISTUNGSPORTFOLIO

CONSULTING	MANAGED SERVICES
Beratung & Konzeption	Cloud & Azure
Security Consulting	Modern Workplace
Cloud-Strategie	Security & Endpoint
Architektur-Design	Backup & Recovery
M365 Migration	Netzwerk & Infra
	M365 & Collaboration
	IT-Support
	Managed Firewall

AGENDA – 20 MINUTEN PRAXIS

01 **Den richtigen Passwortmanager auswählen** *~4 Min.*

Kriterien, Vergleich & Entscheidungshilfe

02 **Einrichtung: Master-Passwort & Geräte** *~4 Min.*

Sicherheit, PC, Smartphone, Browser-Plugins

03 **Passwörter erzeugen, speichern & organisieren** *~4 Min.*

Generator, Ordnerstruktur & Browser-Warnung

04 **Nutzung im Alltag – allein und im Team** *~4 Min.*

Geteilte Zugänge, Rechte & Compliance

05 **Praktische Routinen & nächste Schritte** *~4 Min.*

Onboarding, Offboarding, Sofort-Maßnahmen

1 DEN RICHTIGEN PASSWORTMANAGER AUSWÄHLEN

AUSWAHLKRITERIEN

- Unternehmensgröße & Organisation?
- IT-Verantwortlicher vorhanden?
- Compliance: DSGVO, NIS2, CRA?
- Geräte & Betriebssysteme (PC/Mac/Mobil)?
- Cloud oder lokale Speicherung?
- Budget & laufende Kosten?

EMPFEHLUNGEN

Team / Unternehmen:
1Password Business, Bitwarden Teams, Keeper

KMU / Einzelunternehmer:
Bitwarden, 1Password, Keeper

Budget-bewusst / IT-affin:
KeePass (kostenlos, Open Source, lokal)

TIPP

Cloud-basiert = einfacher Einstieg, automatische Sync über alle Geräte

2 EINRICHTUNG: DAS MASTER-PASSWORT

Ihr Master-Passwort ist der Schlüssel zu allem – behandeln Sie es entsprechend.

Lang & komplex

Mindestens 16 Zeichen
Länge schlägt Komplexität
Passphrase nutzen, z. B.:
Kaffee!Lampe7Wald-Zug

Sicher verwahren

Ausdruck im Tresor oder
Bankschließfach hinterlegen
Nur bei Verdacht auf
Kompromittierung ändern

Break-Glass-Account

Notfallkonto für den
Ernstfall (Krankheit, Unfall)
Vertrauensperson benennen
Zugang versiegelt hinterlegen

2 EINRICHTUNG: PC, SMARTPHONE & BROWSER

Desktop-App

- App herunterladen & installieren
- Mit Master-Passwort anmelden
- Bestehende Passwörter importieren
- (CSV-Export aus Chrome/Firefox)
- 2FA aktivieren (Authenticator-App)

Smartphone

- App aus App Store / Play Store
- Biometrische Entsperrung
- (Face ID / Fingerabdruck) aktivieren
- Autofill in Systemeinstellungen
- erlauben (iOS & Android)
- Synchronisation prüfen

Browser-Plugin

- Erweiterung für Chrome / Edge /
- Firefox installieren
- Automatisches Ausfüllen aktivieren
- Pop-up für neue Logins erlauben
- Tipp: Passwort-Speichern im Browser
- danach deaktivieren!

3 PASSWÖRTER ERZEUGEN, SPEICHERN & ORGANISIEREN

Passwort-Generator

Einzigartige Passwörter pro Account

Mind. 20 Zeichen, Groß-/Klein, Zahlen, Sonderz.

Nie eigene Passwörter ausdenken!

Automatisch speichern

Plugin erkennt neue Logins automatisch

Auto-Save bestätigen → im Tresor abgelegt

Notizen-Feld für Sicherheitsfragen nutzen

Struktur & Ordnung

Ordner: Finanzen, Social Media, Kunden, Intern, Privat

Tags: Priorität, Abteilung, Ablaufdatum | Favoriten für Schnellzugriff

Nicht im Browser speichern!

Browser-Passwörter sind nicht ausreichend geschützt. Nach Import: Browser-Speichern deaktivieren.

4 NUTZUNG IM ALLTAG – ALLEIN UND IM TEAM

Allein / Solo-Unternehmer

- Autofill für schnelles Einloggen
- Passwort-Audit: Schwache & doppelte finden
- Sicherheits-Dashboard regelmäßig prüfen
- Break-Glass: Notfallzugang einrichten
- Private vs. geschäftliche Tresore trennen

Im Team / Unternehmen

- Geteilte Ordner für Team-Zugänge
- Rechte pro Rolle: Lesen / Bearbeiten
- Onboarding: Neuer MA → Zugang in Minuten
- Offboarding: Rechte sofort entziehen
- Compliance: Richtlinien automatisch einhalten

MDSYSTEC®

5 PRAKTISCHE ROUTINEN FÜR DEN ALLTAG

Neue Accounts sofort im PM anlegen

Jeder neue Account wird direkt im Passwortmanager erstellt – nie im Browser speichern.

Regelmäßiger Passwort-Check

Monatlich: Sicherheits-Dashboard prüfen. Schwache & doppelte Passwörter sofort ersetzen.

MFA überall aktivieren

Zwei-Faktor-Authentifizierung für alle wichtigen Dienste. Authenticator-App statt SMS.

Onboarding-Checkliste

Neuer Mitarbeiter? PM-Zugang als fester Schritt im Onboarding-Prozess verankern.

Offboarding nicht vergessen

Mitarbeiter geht? Alle Zugriffsrechte sofort entziehen. PM macht das in Sekunden.

Ihre nächsten Schritte

MDSYSTEC®

DAS KÖNNEN SIE DIREKT NACH DEM WEBINAR UMSETZEN:

1. Passwortmanager auswählen (Tipp: Keeper als einfacher Einstieg)
2. Master-Passwort als Passphrase erstellen & sicher verwahren
3. App auf PC + Smartphone installieren, Browser-Plugin aktivieren
4. Bestehende Passwörter importieren & Browser-Speichern deaktivieren
5. Ab heute: Jeden neuen Account nur noch im Passwortmanager anlegen
6. 2FA aktivieren – für den PM selbst und alle wichtigen Dienste

Vielen Dank!

Schluss mit Passwort-Chaos –
ein Passwortmanager macht den Unterschied.

Jonas Miedl

Geschäftsführer

MDSYSTEC GmbH

jonas.miedl@mdsystec.de

+49 (0) 8725 96491 0

www.mdsystec.de

ISO 9001 | ISO 27001 zertifiziert

BIHK-Reihe
"Umsetzen statt Abwarten:
Neue Spielregeln für die
Cybersicherheit"

IHK für München und Oberbayern
Ansprechpartner: Bernhard Kux
089-5116-1705 | kux@muenchen.ihk.de