

Eine klare und durchdachte Passwortstrategie reduziert das Risiko von unbefugten Zugriffen, Datenverlust und Sicherheitsvorfällen deutlich. Sichere Passwörter und zusätzliche Schutzmaßnahmen gehören deshalb zu den grundlegenden Standards eines professionellen IT-Betriebs.

Checkliste

- Für jeden Benutzerzugang wird ein individuelles Passwort verwendet
- Passwörter sind ausreichend lang komplex aufgebaut
- Es werden keine Namen, Geburtsdaten oder einfachen Begriffe verwendet
- Bekannte Muster wie 123456, Passwort123 oder Tastaturfolgen werden vermieden
- Dasselbe Passwort wird nicht mehrfach für verschiedene Dienste genutzt
- Für kritische Systeme ist Mehr-Faktor-Authentifizierung (MFA) aktiviert
- Administrator-Konten sind mit besonders starken, separaten Passwörtern geschützt
- Standardpasswörter werden bei neuen Geräten und Benutzerkonten sofort geändert
- Passwörter werden nicht offen dokumentiert oder ungeschützt weitergegeben
- Mitarbeiter sind für sichere Passwortvergabe und Phishing-Risiken sensibilisiert
- Kritische Zugänge wie E-Mail, VPN, Microsoft 365, Backup und Firewall werden regelmäßig geprüft



Weitere Passwortsicherungen

- Ein Passwort-Manager wird für die sichere Verwaltung empfohlen
- MFA für externe Zugänge verbindlich festlegen
- Admin-Konten gesondert absichern
- Prozesse für kompromittierte Passwörter definieren
- Passwortregeln in Onboarding und Offboarding integrieren

So finden Sie uns