Passwortsicherheit & KI-basierte Passwortmanager

Ob es nun „Passwort123“ oder der Geburtstag des Kindes ist – viele Nutzerinnen und Nutzer sind sich bei der Vergabe ihrer Passwörter nicht der Tatsache bewusst, dass diese innerhalb weniger Sekunden von Kriminellen geknackt werden können.

*Das Wissensnugget **„Passwortsicherheit & KI-basierte Passwortmanager“** sensibilisiert für diese Gefahr und zeigt, wie ein KI-basierter Passwortmanager helfen kann.*

Einleitung

Passwörter sind der Schlüssel zu fast allen Anwendungen im digitalen Handel – vom Onlineshop über das Kassensystem bis hin zum E-Mail-Postfach.
Dennoch verwenden viele Menschen immer noch einfache oder wiederverwendete Passwörter wie „*Sommer2024“* oder „*123456“*.
Das Problem: Solche Passwörter lassen sich in Sekunden knacken – besonders, wenn Angreifer KI einsetzen, um Passwörter zu erraten oder Datenlecks automatisiert auszuwerten.

Starke Passwörter sind heute wichtiger denn je. Gleichzeitig kann KI auch hier **auf der Seite der Sicherheit** helfen – zum Beispiel durch intelligente Passwortmanager, die sichere Zugangsdaten erzeugen, speichern und verwalten.

Warum ist Passwortsicherheit so wichtig?

Ein einziges unsicheres Passwort kann das gesamte Unternehmen gefährden.
Gerade im Handel, wo verschiedene Mitarbeitende auf dieselben Systeme zugreifen, ist das Risiko besonders hoch.
Cyberkriminelle nutzen gestohlene oder erratene Passwörter, um:

- auf Kundendaten oder Zahlungsinformationen zuzugreifen,
- Bestellungen zu manipulieren,
- oder Schadsoftware in interne Systeme einzuschleusen.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

KI-basierte Angriffsprogramme können Milliarden von Passwortkombinationen in kürzester Zeit testen.
Je schwächer (und kürzer) das Passwort, desto kürzer die Zeit bis zum Erfolg.

Wie hilft KI bei der Passwortsicherheit?

KI wird zunehmend in **Passwortmanagern** und **Sicherheitslösungen** eingesetzt. Diese Systeme können:

- **starke, zufällige Passwörter** generieren, die kaum zu erraten sind,
- **Anmeldeinformationen automatisch speichern und verschlüsseln**,
- **auffällige Anmeldeversuche** erkennen und Nutzer:innen warnen,
- und durch **Musteranalyse** Empfehlungen geben, wann ein Passwort geändert werden sollte.

Einige moderne Lösungen nutzen KI, um aus Datenlecks zu lernen und Nutzer:innen zu informieren, wenn ihre Passwörter im Internet aufgetaucht sind.

Praxistipps – So nutzt du sichere Passwörter

1. **Lang statt komplex:** Verwende mindestens 12 Zeichen – je länger, desto besser.
2. **Kombiniere Zeichen:** Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen mischen.
3. **Keine Wiederholungen:** Für jeden Zugang ein eigenes Passwort.
4. **Passwortmanager verwenden:** Sie speichern deine Zugangsdaten sicher und erstellen bei Bedarf automatisch neue Passwörter.
5. **Zwei-Faktor-Authentifizierung (2FA):** Immer aktivieren, wo es möglich ist. Das erhöht die Sicherheit erheblich.
6. **Keine Weitergabe:** Passwörter gehören nicht auf Zettel, in E-Mails oder Chatnachrichten.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

Fazit

Passwortsicherheit ist kein Luxus, sondern die Grundlage für digitale Sicherheit im Handel.
KI kann dabei helfen, die Verwaltung von Passwörtern einfacher und sicherer zu gestalten – etwa durch intelligente Passwortmanager und automatische Sicherheitsprüfungen.

Doch egal wie fortschrittlich die Technik ist:

Nur wer bewusst mit Passwörtern umgeht, bleibt wirklich geschützt.

Regelmäßige Schulungen, klare Passwortregeln und der Einsatz moderner Tools sorgen dafür, dass der „Schlüssel zum Unternehmen“ nicht in falsche Hände gerät.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages