Mittelstand-Digital
Zentrum
Handwerk

Bild: TierneyMJ/Shutterstock.com

Passwort-Manager für Betriebe

Sichere Passwörter erstellen, teilen und verwalten

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

Warum lohnen sich Passwort-Manager für Betriebe?

Sichere Passwörter sind essenziell, um Onlinekonten gegen unbefugte Zugriffe abzusichern. Leider zählen unsichere Passwörter wie „123456“, „hallo“ und „Passwort“ immer noch zu den am häufigsten verwendeten Passwort-Kombinationen. Damit Passwörter sicher sind, sollten sie entweder möglichst komplex oder sehr lang sein.

Bild: stock.adobe.com 414084829

Tipps für sichere Passwörter

Immer verschiedene Zeichenarten in Kombination nutzen:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen (!”§$%&/...)

Passwortlänge:

- Mehr als 20 Zeichen, wenn nur wenige Zeichenarten genutzt werden, z. B. nur Groß- und Kleinbuchstaben
- 8-12 Zeichen, wenn alle Zeichenarten eingesetzt werden
- Kürzere Passwörter sollten nur in Kombination mit einer Mehr-Faktor-Authentifizierung (2FA) verwendet werden. 2FA ist ein Sicherheitsverfahren, bei dem zur Verifizierung der Identität neben dem Passwort eine weitere Komponente notwendig ist, z. B. ein einmaliger Code, der an ein Mobilgerät gesendet wird.

So erstellen Sie ein komplexes Passwort, das Sie sich trotzdem gut merken können:

Wählen Sie einen beliebigen Satz, z. B.

„Alle meine Entchen schwimmen auf dem See, Köpfchen unter Wasser, Schwänzchen in die Höh.”

Wählen Sie dann als Passwort die Anfangsbuchstaben der Wörter und die Satzzeichen des Satzes:

AmEsadS,KuW,SidH.

Ersetzen Sie anschließend einige der Buchstaben durch Sonderzeichen oder Zahlen:

@mE$@d$,KuW,$1d#.

Von der Strategie, ein einziges besonders komplexes Passwort für alle Accounts zu nutzen, ist jedoch dringend abzuraten. Denn sollte dieses eine Passwort durch Cyber-Kriminelle erbeutet werden, z. B. durch den Hack eines einzigen Online-Dienstes, ist ein Zugriff auf alle Ihre sensiblen Daten in allen Diensten, die dieses Passwort verwenden, möglich.

Am sichersten ist es daher, für jeden Account ein eigenes, komplexes Passwort festzulegen. Um alle Passwörter sicher und bequem verwalten zu können, bietet sich ein Passwort-Manager an.

Passwort-Manager sind Programme, die es ermöglichen, Benutzernamen und Passwörter an einem zentralen Ort sicher abzulegen, so dass sie bei Bedarf schnell zur Hand sind. Der Zugriff auf die Passwörter ist nur mit einem besonders komplexen und daher sicheren Master-Passwort möglich. Der Vorteil liegt auf der Hand: Anstelle von vielen verschiedenen Passwörtern muss man sich nur noch eines merken.

Vorteile eines Passwort-Managers

- **Sichere Verwahrung von Passwörtern** und Benutzernamen durch starke Verschlüsselung
- **Unterstützung bei der Passwortvergabe**, z. B. durch die automatische Erstellung starker Passwörter und die Kennzeichnung von bereits verwendeten oder schwachen Passwörtern
- **Warnung vor gefährlichen Websites und Phishing-Attacken**, z. B. wenn sich die URL der aufgerufenen Website von der gespeicherten URL unterscheidet
- **Synchronisierung über mehrere Geräte** wie Computer, Notebooks, Tablets und Smartphones

Nachteile eines Passwort-Managers

- Beim **Vergessen des Master-Passworts** sind oft alle Daten verloren. Das bedeutet viel Arbeit, da die Zugänge zu allen Konten individuell wiederhergestellt werden müssen. Einige Passwort-Manager bieten jedoch die Möglichkeit, das Master-Passwort zurückzusetzen und so wieder Zugriff auf die gespeicherten Passwörter zu erhalten.
- **Alle Passwörter können auf einmal gestohlen werden**, sollte ein Cyberangriff auf den Passwort-Manager erfolgreich sein.
- Bei cloudbasierten Passwort-Managern **vertrauen** Sie den Zugang zu all Ihren **sensiblen Daten in der Regel einem Unternehmen an**. Hier lohnt sich ein Blick in die AGB und Datenschutzerklärungen des jeweiligen Herstellers. Die Informationen über den Standort des Cloud-Dienste-Anbieters und der Server geben Auskunft darüber, welchem Datenschutzrecht die Daten unterworfen sind. Einige cloudbasierte Manager bieten jedoch die Möglichkeit des Self-Hostings. Das bedeutet, dass die Passwörter zwar in der Cloud gespeichert werden, aber auf keinem fremden, sondern auf einem eigenen Server oder lokalen System, das man selbst verwaltet.

Quellen:

- *Bundesamt für Sicherheit in der Informationstechnik – Passwörter verwalten mit einem Passwort-Manager*
- *Bundesamt für Sicherheit in der Informationstechnik – Sichere Passwörter erstellen*

Die Wahl des optimalen Passwort-Managers

In diesem Kapitel werden die wichtigsten Kriterien und Überlegungen vorgestellt, die bei der Auswahl eines geeigneten Passwort-Managers eine Rolle spielen. Dazu zählen Aspekte wie Speicherort, Sicherheit, Benutzerfreundlichkeit und Kompatibilität.

Datenspeicherung: lokal oder in der (eigenen) Cloud?

Bei der Auswahl eines Passwort-Managers stehen Sie als erstes vor der Wahl, ob Sie Daten ausschließlich lokal auf den verwendeten Geräten oder auch in der Cloud speichern wollen. Beide Optionen bieten spezifische Vor- und Nachteile, die je nach den persönlichen Bedürfnissen und Sicherheitsanforderungen abgewogen werden müssen.

Passwort-Manager mit ausschließlich lokal verwalteten Daten

Solche Passwort-Manager speichern die Daten auf lokalen Geräten wie z. B. Smartphones, ohne sie in eine Cloud hochzuladen. Der Zugriff auf die Passwörter ist nur über das Gerät möglich, auf dem der Passwort-Manager installiert ist.

Vorteile:

- **Datensicherheit**: Alle Daten werden nur auf lokalen Geräten gespeichert und nicht in der Cloud. Das bedeutet, dass die Daten nur dann gefährdet sind, wenn das physische Gerät kompromittiert wird. Es besteht keine Abhängigkeit von der Sicherheit der Cloud-Infrastruktur eines Drittanbieters.
- **Kontrolle**: Man besitzt die volle Kontrolle über die Speicherung und Verwaltung von Passwörtern und muss sich keine Sorgen um die Datenschutzpraktiken machen, mit denen Anbieter von Passwort-Managern ihre Cloud betreiben.
- **Keine Internetverbindung erforderlich**: Der Passwort-Manager funktioniert auch ohne Internetverbindung, was ihn ideal für Personen macht, die häufig an Orten mit unsicherer oder fehlender Internetverbindung arbeiten.
- **Einmalige Kosten**: Oft fallen nur einmalige Kosten an, im Gegensatz zu den Abonnement-Modellen vieler Cloud-Dienste.

Nachteile:

- **Eingeschränkte Synchronisation**: Die Synchronisation von Passwörtern über mehrere Geräte hinweg ist komplizierter und möglicherweise unsicherer.
- **Backup und Wiederherstellung**: Die Verantwortung für Backups liegt beim Betrieb. Bei Geräteverlust oder -schaden können Daten verloren gehen, wenn kein aktuelles Backup existiert.
- **Weniger zugänglich**: Der Zugriff auf Passwörter ist nur von dem Gerät aus möglich, auf dem der Passwort-Manager installiert ist. Das kann besonders unterwegs oder bei der Nutzung mehrerer Geräte unpraktisch sein.

Cloudbasierte Passwort-Manager

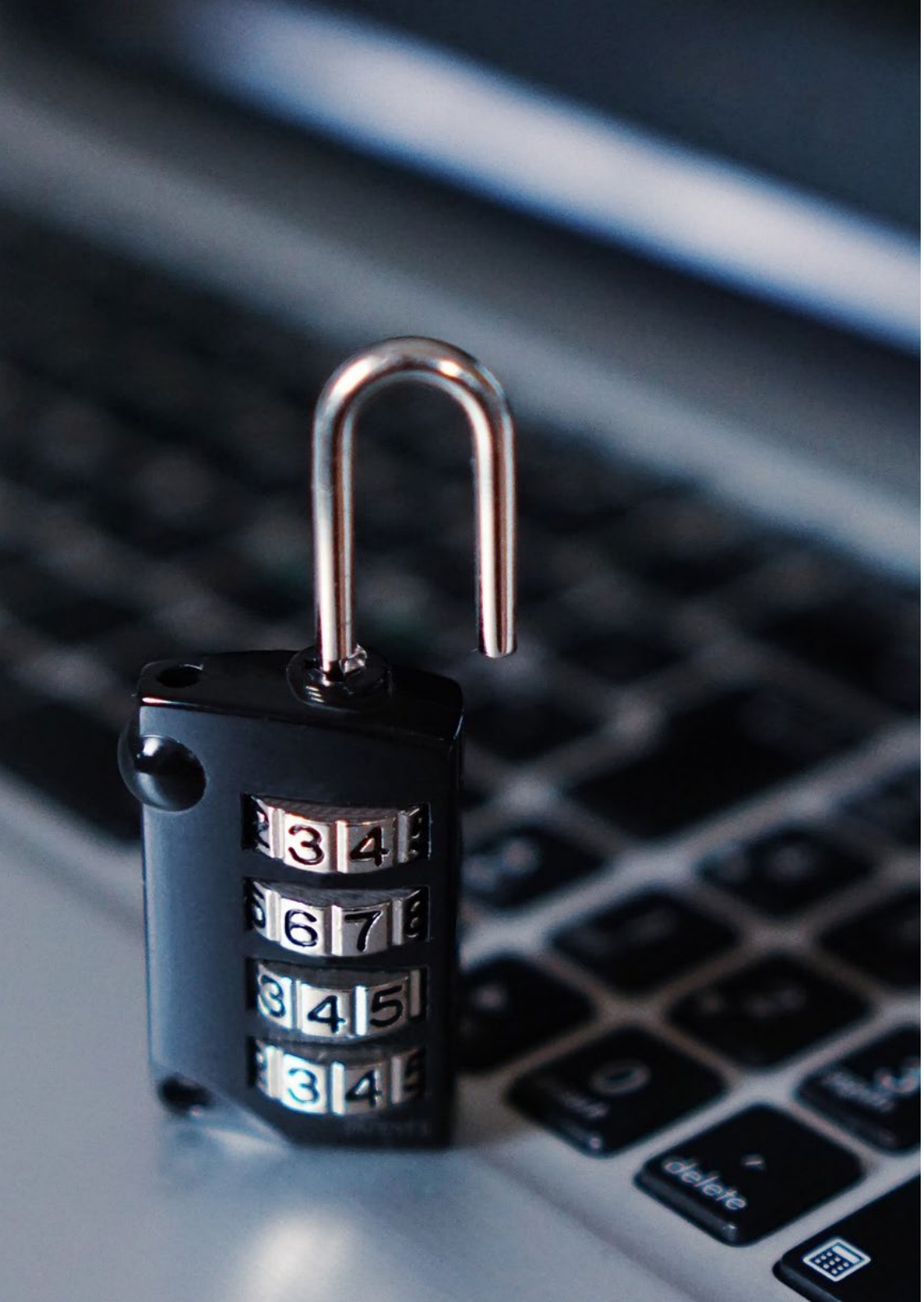
Cloudbasierte Passwort-Manager speichern Passwörter und andere Anmeldedaten auf Servern im Internet und synchronisieren sie nahtlos über alle Geräte hinweg mithilfe der Cloud-Infrastruktur des Anbieters.

Vorteile:

- **Einfache Synchronisation** über Server im Internet, wodurch der Zugriff und die Verwaltung von überall her möglich ist
- **Automatische Updates und Wartung**: Cloud-Dienste werden regelmäßig aktualisiert und gewartet, um eine hohe Sicherheit und Funktionalität zu gewährleisten. Betriebe müssen daher nicht selbst aktiv werden.
- **Professionelle Sicherheitsmaßnahmen**: Viele Cloud-Anbieter implementieren fortschrittliche Sicherheitstechnologien und -protokolle, die oft über das hinausgehen, was ein durchschnittlicher Betrieb lokal bereitstellen könnte.
- **Notzugriff**: Einige Dienste bieten Optionen für Notzugriffe, falls man die Zugangsdaten verliert oder sich in einer Notlage befindet.

Nachteile:

- **Datenschutzbedenken**: Ihre sensiblen Daten liegen in den Händen eines Drittanbieters. Die Sicherheit der Daten hängt von den Sicherheitsmaßnahmen des Anbieters ab.
- **Ohne Internetverbindung kann der Zugriff auf Passwörter eingeschränkt oder nicht möglich sein**. Viele cloudbasierte Passwort-Manager speichern die Daten aber zusätzlich lokal ab, damit im Fall einer schlechten Internetverbindung der Zugriff weiterhin gewährleistet ist.
- **Laufende Kosten**: Viele cloudbasierte Passwort-Manager nutzen ein Abonnement-Modell, was langfristig teurer sein kann als ein Einmal-Kauf.



Self-Hosting – Die eigene Passwort-Cloud

Bei cloudbasierten Passwort-Managern entscheidet der Standort der Rechenzentren des Cloud-Dienstes darüber, welchem Datenschutzrecht Ihre Daten unterliegen. Stehen die Server des Anbieters z. B. in den USA, ist eine datenschutzkonforme Nutzung des Cloud-Dienstes nach deutschem Recht praktisch unmöglich.

Einige Passwort-Manager unterstützen daher das sogenannte Self-Hosting. Dies ermöglicht es, die Passwort-Datenbank auf einem eigenen Server oder lokalen System zu hosten, anstatt den Cloud-Dienst des Passwort-Managers zu nutzen. Dabei sollten Sie jedoch folgendes beachten:

- **Technisches Know-how**: Self-Hosting erfordert technisches Verständnis für Servermanagement, Sicherheitsupdates und Fehlerbehebung.
- **Verfügbarkeit**: Die Verfügbarkeit der Daten hängt von der Stabilität des eigenen Servers und der Internetverbindung ab.
- **Sicherheitsrisiken**: Bei unsachgemäßer Konfiguration oder vernachlässigten Sicherheitsupdates können Sicherheitslücken entstehen.
- **Backups**: Es ist wichtig, regelmäßige Backups durchzuführen, um Datenverlust zu vermeiden.

Funktionsumfang: Was benötigen Sie genau?

Viele Passwort-Manager werden auch als kostenfreie Version zur Verfügung gestellt und bieten **gestaffelte Lizenz-Modelle** an, die sich in ihrem Funktionsumfang stark unterscheiden können. Achten Sie bei Ihrem Produktvergleich also nicht nur auf den Funktionsumfang, sondern auch darauf, welche Funktionen kostenpflichtig bzw. erst ab einer bestimmten Lizenzstufe nutzbar sind.

Bevor Sie damit beginnen, Passwort-Manager zu vergleichen, sollten Sie auflisten, welche **individuellen Anforderungen** Sie an die Software haben. Hier sind einige wichtige Funktionen von Passwort-Managern:

- **Sichere Verschlüsselung**: Alle Daten im Passwort-Manager sollten mit einer starken Verschlüsselung geschützt sein. Ideal ist eine Ende-zu-Ende-Verschlüsselung, bei der nur die Benutzerin oder der Benutzer den Entschlüsselungsschlüssel besitzt.

- **Zwei-Faktor-Authentifizierung (2FA)**: Ein guter Passwort-Manager sollte die Zwei-Faktor-Authentifizierung unterstützen, um die Sicherheit zu erhöhen. Mehrere der folgenden Zwei-Faktor-Authentifizierungen sollten zur Verfügung stehen: Einmal-Passwort per E-Mail, Einmal-Passwort per Authentifizierungs-App, **FIDO2 WebAuthn**, **YubiKey OTP**, **Duo**

- **Passwort-Generator**: Ein integrierter Passwort-Generator ist nützlich, um sichere Passwörter zu erstellen. Diese sollten lang, komplex und einzigartig sein.

- **Platz für Kreditkartendaten und andere sensible Informationen**: Neben Passwörtern sollte der Passwort-Manager auch die Möglichkeit bieten, andere sensible Informationen sicher zu speichern wie z. B. Notizen, Kreditkarteninformationen oder persönliche Daten.

- **Backup und Wiederherstellung**: Ein Backup-System ist wichtig, um Datenverlust zu verhindern. Der Passwort-Manager sollte regelmäßige Backups ermöglichen und eine einfache Wiederherstellungsoption bieten. Gerade bei lokal installierten Passwort-Managern sollte auf diese Funktion geachtet werden.

- **Audit-Funktion**: Eine Funktion, die die Stärke der gespeicherten Passwörter analysiert und den Benutzer auf schwache oder doppelte Passwörter hinweist, kann sehr nützlich sein.

- **Benutzerfreundlichkeit**: Der Passwort-Manager sollte einfach zu bedienen und intuitiv gestaltet sein.

- **Cross-Plattform-Kompatibilität**: Der Passwort-Manager sollte auf verschiedenen Betriebssystemen und Plattformen verfügbar sein, z. B. Windows, macOS, iOS, Android usw.

- **Browser Add-ons**: Ein Browser-Add-on für einen Passwort-Manager ermöglicht das komfortable und sichere automatische Ausfüllen von Login-Daten direkt im Browser. Es vereinfacht zudem die Passwortverwaltung und -aktualisierung, was Zeit spart und die Sicherheit erhöht.

- **Anpassbare Sicherheitseinstellungen**: Es sollte möglich sein, Sicherheitseinstellungen nach den eigenen Bedürfnissen anzupassen, z. B. Passwortlänge, Verschlüsselungsmethoden oder Authentifizierungsoptionen.

- **Teilen von Passwörtern**: Gerade im betrieblichen Einsatz kann das Teilen von Passwörtern zwischen Benutzern bzw. Benutzergruppen von großem Vorteil sein.

Im Folgenden gehen wir genauer auf einige der wichtigsten Anforderungen ein.

Sichere Verschlüsselung

Bei der Verschlüsselung der Daten sollte der Passwort-Manager immer einen 256-Bit-Verschlüsselungs-Standard verwenden, z. B. AES-256 (Advanced Encryption Standard).

Handelt es sich um einen cloudbasierten Dienst, sollte die Zero-Knowledge-Architektur zum Einsatz kommen. Das bedeutet, dass alle sensiblen Daten wie Passwörter und Schlüssel lokal auf dem Gerät des Nutzers verschlüsselt werden, bevor sie zum Speichern an den Server übermittelt werden. Diese Architektur bietet eine hohe Sicherheit, da selbst bei einem Datenleck beim Anbieter die Daten für Angreifer nutzlos sind, weil die notwendigen Schlüssel zur Entschlüsselung nicht verfügbar sind.

Teilen von Passwörtern

Vor allem bei der betrieblichen Nutzung eines Passwort-Managers kann das Teilen von Passwörtern nützlich sein, erfordert jedoch besondere Sicherheitsvorkehrungen, um die Integrität der Daten zu gewährleisten.

Vorteile:

- **Effiziente Zusammenarbeit**: Das Teilen von Passwörtern ermöglicht es Teammitgliedern oder Vertrauenspersonen, auf gemeinsame Konten oder Ressourcen zuzugreifen, ohne die Passwörter manuell weitergeben zu müssen.
- **Zentrale Verwaltung**: Ein Passwort-Manager kann als zentrale Plattform dienen, um Passwörter sicher zu teilen und zu verwalten, was den Prozess transparenter und sicherer macht.
- **Revision und Aktualisierung**: Es ist einfacher, gemeinsam genutzte Passwörter zu überprüfen und bei Bedarf zu aktualisieren.

Wichtige Funktionen:

- **Berechtigungsmanagement**: Es ist wichtig, dass die Zugriffsrechte detailliert gesteuert werden können, um sicherzustellen, dass nur autorisierte Personen Zugriff auf bestimmte Passwörter haben.
- **Audit-Funktionen**: Ein guter Passwort-Manager sollte Funktionen bieten, mit denen nachvollzogen werden kann, wer wann auf welche Passwörter zugegriffen hat.
- **Entfernen von Zugriffen**: Es sollte einfach möglich sein, den geteilten Zugriff für bestimmte Personen zu widerrufen, z. B. wenn eine Person das Unternehmen verlässt.
- **Cloud-Zugriff**: Für das Teilen von Passwörtern ist ein Cloud-Dienst nicht zwingend notwendig. In der Praxis ist es aber die praktischste und sicherste Methode, vor allem dann, wenn Passwörter mit einer Gruppe von Personen geteilt werden sollen.

Open-Source- oder proprietäre Software?

Sicherheitsrelevante Tools wie Verschlüsselungsprogramme oder -algorithmen profitieren vom Open-Source-Konzept. Dies trifft auch auf Passwort-Manager zu.

Was bedeutet Open Source?

Open-Source-Software unterscheidet sich von herstellergebundener (proprietärer) Software dadurch, dass der Quellcode frei verfügbar ist. Das bedeutet, dass Nutzerinnen und Nutzer das Programm unabhängig von dessen Urheber in der Regel beliebig verändern, weitergeben und erkannte Schwachstellen oder Fehler veröffentlichen können. Dagegen kann der Quellcode eines proprietären Programms weder geprüft noch verändert werden.

Wie sicher ist Open-Source-Software?

Die Idee, dass ein für jeden einsehbarer Quellcode für mehr Sicherheit sorgt, wirkt im ersten Moment paradox. Könnten dann nicht auch Cyber-Kriminelle den Code prüfen und gefundene Schwachstellen ausnutzen? Ja, das könnten sie und es passiert auch immer wieder. Doch eine aktive Entwicklergemeinde – Stichwort „Schwarmintelligenz“ – sorgt in der Regel dafür, dass die entsprechenden Probleme schnell behoben werden.

Natürlich gibt es auch Negativbeispiele in Bezug auf die Sicherheit von Open-Source-Software. Eines der Bekanntesten dürfte die „Heartbleed“ genannte Sicherheitslücke in der OpenSSL-Bibliothek sein, die 2014 entdeckt wurde und von der ein großer Teil der verschlüsselten Kommunikation im Internet betroffen war.

Warum ist proprietäre Software nicht automatisch sicher?

Das vielleicht beste Beispiel dafür, dass geschlossener Code nicht automatisch mehr Sicherheit bedeutet, liefert Microsoft mit seinem Betriebssystem Windows. Monat für Monat werden neue, nicht selten schwere Sicherheitslücken in Windows bekannt. Wer Windows nutzt, muss sich darauf verlassen, dass das Entwicklungsteam von Windows einen guten Job macht und die Sicherheitslücken frühzeitig entdeckt und rasch schließt. Denn anders als bei Open-Source-Betriebssystemen wie GNU/Linux hat die externe Entwickler-Community hier keine Möglichkeit, Codefehler in Windows selbst zu finden und zu beheben.

Quellen:

- *Bundesamt für Sicherheit in der Informationstechnik – Open-Source-Software und Vorabversionen von Betriebssystemen*
- *Heise Online – Ist Open-Source-Software wirklich sicherer?*

Fazit

Passwort-Manager bieten Handwerksbetrieben eine einfache und effektive Lösung, um Zugangsdaten zu Onlinediensten sowie andere wichtige Informationen sicher zu verwalten und bei Bedarf schnell zur Hand zu haben. Bei der Auswahl des Passwortmanagers sollten Betriebe neben allgemein wichtigen Kriterien wie Sicherheit, Kompatibilität und Benutzerfreundlichkeit darauf achten, dass die Software ihre individuellen Anforderungen erfüllt.

Das Mittelstand-Digital Zentrum Handwerk

Das „Mittelstand-Digital Zentrum Handwerk“ unterstützt Handwerksbetriebe und Handwerksorganisationen seit 2016 dabei, die Chancen digitaler Technologien, Prozesse und Geschäftsmodelle zu nutzen – kostenfrei, anbieterneutral und deutschlandweit.

Was macht das Mittelstand-Digital Zentrum Handwerk einzigartig?

- Nah dran am Handwerk
- Ansprechpartner für jede Digitalisierungsfrage
- Umfangreiches Material zur Unterstützung aller Digitalprojekte im Handwerk
- Einzigartiger Digitalisierungscheck für das Handwerk
- Technologie-Erlebniswelten
- Persönliche Begleitung von Betrieben bei Digitalvorhaben
- Jederzeit topinformiert mit unserem Newsletter und per Social Media
- Zahlreiche Schulungskonzepte zu Digital- und Technologiethemen für Beratende und Dozierende im Handwerk

Mehr Informationen

Folgen Sie uns auf Social Media:

X: Twitter.com/HaWe_Digital

Facebook: Facebook.com/HandwerkDigital

LinkedIn: Linkedin.com/company/mittelstand-digital-zentrum-handwerk

Instagram: Instagram.com/digitales_handwerk

YouTube: Youtube.com/@handwerkdigital

Newsletter: Handwerkdigital.de/newsletter

Das Mittelstand-Digital Zentrum Handwerk gehört zur Förderinitiative Mittelstand-Digital. Mit dem Mittelstand-Digital-Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und im Handwerk. Weitere Informationen zum Förderschwerpunkt finden Sie unter **www.mittelstand-digital.de**.

Impressum

Herausgeber	Mittelstand-Digital Zentrum Handwerk
Anschrift	Zentralverband des Deutschen Handwerks e. V., Mohrenstraße 20/21, 10117 Berlin
E-Mail	info@handwerkdigital.de
Autor	Marc Piepersjohanns | Bundestechnologiezentrum für Elektro- und Informationstechnik e. V. (BFE)
Redaktion	Andreas Hoffmann | Zentralstelle für die Weiterbildung im Handwerk (ZWH)
Gestaltung	Andrew Collar | ZWH

Stand 05/2024