

## Sichere Passwörter

### Warum sind sichere Passwörter so wichtig?

Man muss sich dessen bewusst sein: Es geht um sensible Daten, den Schutz der Privatsphäre und natürlich um Geld.

Passwörter sind in diesem Zusammenhang das wichtigste Werkzeug, um den Zugang zu einem Rechner bzw. Daten zu schützen.

Start des Rechners, E-Mail-Konto, Online-Banking: Es werden überall Passwörter benötigt. Viele wählen hier immer die gleichen und leider auch relativ einfache Passwörter, um sie sich besser merken zu können.

Angreifer, auch Hacker genannt, versuchen mit Spionageprogrammen (z. B. durch den Vergleich mit Wörterbüchern), an Benutzernamen und Passwörter zu kommen, um in entsprechende Systeme einzubrechen. Wird ein zu einfaches Passwort gewählt oder wird es leichtsinnig weiter gegeben, haben es die Kriminellen sehr leicht.

Mit den gestohlenen Daten ist es möglich, einen fremden Rechner fernzusteuern, auf Kosten des Anwenders online einzukaufen oder in dessen Namen im Netz aufzutreten.

Wir geben in diesem Flyer ein paar Tipps, wie Sie sich ein sicheres Passwort erstellen und es schützen können. Wer diese Grundregeln beachtet, kann seine Technik und Daten besser schützen als bisher.



Weitere Informationen finden Sie unter nebenstehendem QR-Code oder unter:  
[www.betrieb-machen.de](http://www.betrieb-machen.de)

## Mittelstand 4.0-Kompetenzzentrum Chemnitz

Als Mittelstand 4.0-Kompetenzzentrum Chemnitz unterstützen wir Sie als kleines und mittelständisches Unternehmen! Wir zeigen Ihnen die technologischen und wirtschaftlichen Potenziale der Digitalisierung, Vernetzung und Anwendung von Industrie 4.0 und begleiten Sie auf dem herausfordernden Weg in eine digitale Zukunft. Mit der Expertise und Erfahrung unserer Partner wollen wir das Thema Industrie 4.0 für Sie als Unternehmen greifbar machen, Ihre Führungskräfte und Mitarbeiter qualifizieren und die Umsetzung der Digitalisierung bei Ihnen vor Ort unterstützen. Unsere Angebote umfassen ein umfangreiches Leistungsportfolio – von der Sensibilisierung über den Kompetenzaufbau bis hin zur Umsetzung im Unternehmen. Die Leistungsbereiche bauen aufeinander auf und werden vor Ort in den Unternehmen, in den Testumgebungen der Partner und auf unserer Onlineplattform angeboten. Im Rahmen unserer kostenfreien und praxisnahen Angebote können Sie sich intensiv mit diesen Themen beschäftigen.

### Dabei bearbeiten wir folgende Themenfelder:

- ▶ **Menschen machen's!** – Der Mensch in der digitalen Arbeitswelt.
- ▶ **Alles Unternehmen!** – Das Unternehmen für morgen aufstellen.
- ▶ **Leistung bringen!** – Den Prozess digital verbessern.
- ▶ **Produkte gestalten!** – Das Produkt für den Nutzer machen.
- ▶ **Recht behalten!** – Recht, Sicherheit & Schutz beim digitalen Miteinander.
- ▶ **Sicher bleiben!** – Digitalisieren und vernetzen, aber sicher.

## Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weiter Informationen finden Sie unter:  
[www.mittelstand-digital.de](http://www.mittelstand-digital.de)

### Impressum

**Text und Redaktion:**  
Roland Hallau, Mittelstand 4.0-Kompetenzzentrum Chemnitz

**Herausgeber:**  
Mittelstand 4.0-Kompetenzzentrum Chemnitz  
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH  
Bruno-Wille-Straße 9, 39108 Magdeburg  
Tel.: +49 391 74435-24 • Fax: +49 391 74435-11  
E-Mail: [rhallau@tti-md.de](mailto:rhallau@tti-md.de)  
Geschäftsführer: Dr. Michael Klaeger, Marko Wunderlich  
Amtsgericht Stendal, HRB 104429  
Umsatzsteuer-Identifikationsnummer: DE 139 310 185

**Grafische Konzeption und Gestaltung:**  
toolboxx-media UG (haftungsbeschränkt)

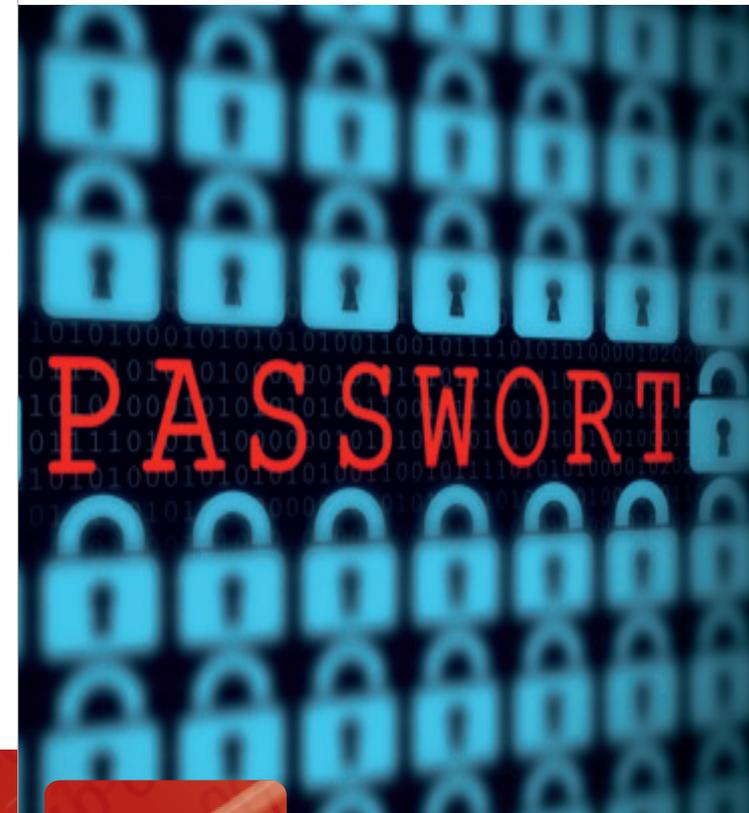
**Druckerei:** KOCH-DRUCK

**Bildnachweis:** Marco2811, Gina Sanders, alexyndr, Onidji, wavebreakpremium – Fotolia.com

Magdeburg, Dezember 2018



Betrieb 4.0  
machen!



## Sichere Passwörter

10 Goldene Regeln aus der Praxis

[www.mittelstand-digital.de](http://www.mittelstand-digital.de)

Mittelstand-  
Digital

Gefördert durch:  
  
aufgrund eines Beschlusses  
des Deutschen Bundestages

## 10 Goldene Regeln, die wirklich helfen

### Sichere Passwörter

Die 10 Goldenen Regeln sollen Ihnen helfen, die Sicherheit Ihrer Computer sowie Ihrer Daten bzw. Ihrer Werte zu schützen.

Diese Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen sowie dem Handwerk. Sie wurden auf Basis jahrelanger Beratererfahrungen und in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Anregungen rund um das Thema der Digitalisierung finden Sie unter

[www.betrieb-machen.de](http://www.betrieb-machen.de)





**+ Regel 1: Ihr Passwort ist sehr wichtig**  
Einbrecher greifen nicht nur geheime Server an, sondern jeden Rechner, den sie finden können. Mit einfachen Programmen können Angreifer komplette Netzwerke in wenigen Minuten ausspionieren. Es ist also auch Ihr Rechner gefährdet – selbst wenn Sie ihn nur für eine bessere Schreibmaschine halten. Dadurch kann Ihr Rechner die Sicherheit des gesamten Unternehmens gefährden.

**+ Regel 2: E-Mail-Postfach besonders schützen**  
Wer Zugriff auf Ihre E-Mails hat, hat auch Zugriff auf fast alle anderen Online-Dienste. Denn bei den meisten Diensten ist es möglich, mit nur einem Klick ein neues Passwort oder einen Passwort-Link per E-Mail zusenden zu lassen.



**+ Regel 3: Verwenden Sie kein Passwort, das erraten werden kann**  
Benutzen Sie nicht die Namen Ihrer Kinder, Ihres Partners, Ihrer Katze, den Geburtstag Ihrer Mutter oder das Kennzeichen Ihres Autos.

Diese Daten sind offensichtlich und leicht herauszufinden. Ein Einbrecher wird sie daher systematisch durchprobieren.

**+ Regel 4: Kein Passwort aus einem Wörterbuch**  
Passwörter werden meist verschlüsselt abgespeichert. Ein Einbrecher kann zwar die codierte Version stehlen, diese aber nicht ohne weiteres entschlüsseln.

Er kann jedoch Wörterlisten (z. B. Wörterbücher, Wikipedia, Duden) benutzen und jedes Wort darin verschlüsseln. Dann werden die verschlüsselten Wörter mit den Passwortcodes verglichen. Stimmt ein Passwortcode mit dem Wörterbucheintrag überein, hat der Einbrecher ein Passwort erraten.

Computer können tausende Wörter pro Minute verschlüsseln und vergleichen. Daher dürfen Sie kein Passwort verwenden, das in einem Wörterbuch steht.

**+ Regel 5: Lange Passwörter mit verschiedenen Zeichen**  
Passwörter zu erraten bzw. automatisch abzugleichen, kostet Zeit. Je länger das Passwort ist, desto höher ist der zeitliche Aufwand. Alle 5-stelligen Passwörter aus Kleinbuchstaben können z. B. sehr schnell durchprobiert werden, ähnlich wie bei einem Zahlenschloss von 0000 bis 9999.

Wählen Sie mindestens ein 10-stelliges Passwort aus verschiedenen Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen aus. Je länger und gemischer, desto besser. Viele ausländische Angreifer kennen keine Umlaute und ignorieren diese.



**+ Regel 6: Passwort nicht weiter geben**  
Nur Sie kennen Ihr Passwort. Schreiben Sie es nicht auf und nennen Sie es keinem Kollegen, Bekannten oder Verwandten. Nennen Sie es auch nicht Ihrem Chef oder einem Systemadministrator. Nur für Notfälle sind sinnvolle Regelungen erlaubt (Safe in der Firma o.ä.).

**+ Regel 7: Das Passwort schützen**  
Achten Sie darauf, dass Besucher, Kollegen oder Kunden nicht auf die Tastatur schauen können, wenn Sie das Passwort eingeben. Nutzen Sie Sichtschutzfolien für Laptops. Dies gilt insbesondere für öffentliche Plätze wie Bahnhöfe, Züge, Flughäfen oder auf Konferenzen. Dazu gehört auch, dass Sie Passwörter nur an Computern eingeben, denen Sie vertrauen können.

**+ Regel 8: Verschiedene Passwörter**  
Verwenden Sie auf gar keinen Fall Ihr System- oder E-Mail-Passwort an anderen Stellen. Sie wissen nie, wer z. B. hinter einem Web-Forum steht. Es kann sein, dass Ihr Passwort abgefangen oder weitergeleitet wird. Daher verwenden Sie auf jeder Webseite, in jedem Forum, für jeden E-Mail-Account, immer ein eigenes Passwort.

**+ Regel 9: Passwort regelmäßig ändern**  
Trotz aller Vorsichtsmaßnahmen kann ein Passwort geknackt werden. Daher ist es sinnvoll, in regelmäßigen und möglichst kurzen Abständen das Passwort zu wechseln. Dies erschwert einem Angreifer die Einbruchsmöglichkeiten.

Verwenden Sie dabei keine Muster (laufende Nummer, Monat, Woche o.ä.) im Passwort, sondern denken Sie sich ein neues aus. Oder nutzen Sie einen Passwortgenerator. Ändern Sie vorgegebene Passwörter gleich bei der ersten Benutzung.

**+ Regel 10: Passwörter nicht im Browser speichern**  
Die meisten Browser bieten die Möglichkeit, Benutzernamen und Passwörter für Webseiten zu speichern. Das ist zwar hilfreich, aber prinzipiell auch unsicher. Hat ein Angreifer Zugriff auf Ihren Rechner, kann er eventuell die gespeicherten Passwörter auslesen.

## Tipps

### Passwörter erstellen

- Nutzen Sie die Methode der Verwendung der Anfangsbuchstaben von Sätzen oder Sprichwörtern und kombinieren Sie das Ergebnis mit Sonderzeichen.
- Verwenden Sie einen Passwortgenerator wie z. B. PWgen

<http://pwgen-win.sourceforge.net>

### Passwörter sicher speichern

- Passwort-Tools helfen z. B.

[www.keepass.info](http://www.keepass.info)

