

## Agenturservice-Jupe

Tel.: 02325 - 558 426  
Fax : 02325 - 467 0 380

Mobil : 0174 - 29 11111

Mail : [info@agenturservice-jupe.de](mailto:info@agenturservice-jupe.de)

Web : <http://www.agenturservice-jupe.de>



## Deutsche Anwalt- und Notar-Versicherung Presseartikel

### Passwörter



Kinderleichte und supersichere Passwort-Verwaltung – dieses Versprechen macht jede Software dem Internet-Nutzer. Die Programme generieren automatisch neue, sichere Passwörter, bewahren die sensiblen Zugangsdaten sicher auf und geben den Zeichen-Kauderwelsch womöglich selbstständig in die entsprechenden Felder ein. Doch wie gut sind die Programme wirklich? Das Testmagazin „PC Professionell“ (PC pro) hat im Sommer vergangenen Jahres insgesamt acht Passwort-Manager zu Verkaufspreisen zwischen 10 und 30 EUR ausprobiert.

Das Funktionsprinzip dieser Programme ist gleich: Beim Start des Tools muss sich der Anwender als zugelassener Benutzer ausweisen. Die eingetippten Zugangsdaten speichert die Software in Form einer verschlüsselten Datenbank. Bei Bedarf stellt das Programm Benutzernamen und Kennwort bereit, sodass sich der Anwender bei Passwort-geschützten Services im Web anmelden kann.

Der Testsieger **Password Safe** and **Repository 2006 Professional (PSR)** sowie **Archicrypt Safe 3** erlauben sowohl die Anmeldung per Master-Passwort als auch durch eine Schlüsseldatei. Der Erstplatzierte lässt sich zudem durch einen USB-Dongle oder eine Smart Card schützen. Sicherer geht es nicht, urteilt PC-pro.

Die getesteten Produkte sind eine Mischung aus Password-Safe, Kennwort-Verwaltung und Login-Ausfüllhilfe. Sie besitzen einen integrierten Passwort-Generator, der knacksichere Passwörter erzeugt (beispielsweise rK\_9{Tb-ZB43JOp7}) und in der Kennwort-Datenbank ablegt, schreibt das Testmagazin. Die maximale Passwort-Länge reicht dabei von 32 (**Viskeeper Pro 3**) bis 999 Zeichen (**1 Password Pro 5.0** und **Password Manager XP 2.1**). Eine Länge von zehn Zeichen inklusive Klein- und Großbuchstaben sowie Zahlen reiche aber, um Brute-Force-Angreifer mit Top-Hardware knapp 900 Jahre lang zu beschäftigen, so PCpro.

Alle acht Tools erlauben die Nutzung von Klein-, Großbuchstaben, Zahlen und Sonderzeichen. **Archicrypt Safe 3**, **Password Depot Pro** und **PSR** informieren den Anwender auch über die Stärke des gewählten Kennworts – eine große Hilfe für Anwender, die absolut sichere Passwörter generieren wollen.

Die mit Abstand meisten Funktionen rund um die Passwort-Erzeugung finden sich in **PSR** und **Password Depot Pro**, urteilt PCpro. **Key Master** und **Viskeeper Pro** fehlen hier wichtige Funktionen wie die Anzeige der Passwort-Sicherheit und die Passwort-Erzeugung per Maus oder Tastatur.

Das Problem der Programme ist weniger die mangelnde als vielmehr die zu große Sicherheit. Bei Verlust des Master-Passworts kommt laut PCpro nämlich auch der User nicht mehr an seine Daten. Das Magazin rät, regelmäßige Backups der Datenbank anzulegen, um im Falle eines Hardware-Defekts eine Sicherheitskopie zu haben. Eine Backup-Funktion bieten alle Tools, aber nur Testsieger **PSR**, außerdem **1 Password Pro**, **Password Depot**, **Password Manager XP** und **Password Safe** legen die Sicherheitskopien auch automatisch an.

Bis auf **Key Master** und **Viskeeper Pro** sind alle Produkte mit einer Auto-Ausfüllfunktion ausgestattet. Dieses Feature nimmt dem User lästige Anmeldevorgänge ab, indem das Tool die benötigten Daten, meist Benutzernamen und Passwort, in Eigenregie in die Felder eingibt. Dabei spielt es keine Rolle, ob der Nutzer mit dem Internet Explorer oder dem Firefox im Web unterwegs ist.

Den vollständigen Testbericht gibt es online unter [www.testticker.de/pcpro/tests/security/article20060608038.aspx](http://www.testticker.de/pcpro/tests/security/article20060608038.aspx).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI; [www.bsi.de](http://www.bsi.de)) hat einige grundlegende Empfehlungen zum Umgang mit Passwörtern vorgelegt, die wir nachfolgend dokumentieren:

- **Ein gutes Passwort sieht so aus:** Es sollte mindestens acht Zeichen lang sein. Tabu sind allerdings Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars usw. Und wenn möglich sollte es nicht in Wörterbüchern vorkommen. Zusätzlich sollte es auch Sonderzeichen (?!%.....) und Ziffern enthalten. Dabei sollten allzu gängige Varianten vermieden werden, also nicht 1234abcd usw. Einfache Ziffern am Ende des Passworts anhängen oder eines der üblichen Sonderzeichen \$, !, ?, #, am Anfang oder Ende eines ansonsten simplen Passwortes, ist auch nicht empfehlenswert.  
Aber wie merkt man sich ein solches Passwort? Auch dafür gibt es Tricks. Eine beliebte Methode funktioniert so: Man denkt sich einen Satz aus und benutzt von jedem Wort nur den ersten Buchstaben (oder nur den zweiten oder letzten, etc.). Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen.  
Hier ein Beispiel: „Morgens stehe ich auf und putze meine Zähne.“ Nur die ersten Buchstaben: „MsiaupmZ“. „i“ sieht aus wie „1“, „&“ ersetzt das „und“: „Msl1a&pmZ“. Auf diese Weise hat man sich eine gute „Eselsbrücke“ gebaut. Natürlich gibt es viele andere Tricks und Methoden, die genauso gut funktionieren.
- **Passwörter regelmäßig ändern**  
Jedes Passwort sollte in regelmäßigen Zeitabständen geändert werden. Viele Programme erinnern Sie automatisch daran, wenn Sie das Passwort z. B. schon ein halbes Jahr benutzen. Diese Aufforderung nicht gleich wegklicken – sondern ihr am besten gleich nachkommen! Natürlich ist es da schwer, sich alle Passwörter zu merken. Womit wir beim nächsten Punkt sind.
- **Passwörter nicht notieren**  
Auch wenn es bei selten genutzten Zugangsdaten schwer fällt – grundsätzlich sollten Sie sich Passwörter nicht aufschreiben.
- **Keine einheitlichen Passwörter verwenden**  
Problematisch ist die Gewohnheit, einheitliche Passwörter für viele verschiedene Zwecke bzw. Zugänge (Accounts) zu verwenden. Denn gerät das Passwort einer einzelnen Anwendung in falsche Hände, so hat der Angreifer freie Bahn für Ihre übrigen Anwendungen. Das können z. B. die Mailbox oder alle Informationen auf dem PC sein.
- **Voreingestellte Passwörter ändern**  
Bei vielen Softwareprodukten werden bei der Installation (bzw. im Auslieferungszustand) in den Accounts leere Passwörter oder allgemein bekannte Passwörter verwendet. Hacker wissen das: Bei einem Angriff probieren sie zunächst aus, ob vergessen wurde, diese Accounts mit neuen Passwörtern zu versehen. Deshalb ist es ratsam, in den Handbüchern nachzulesen, ob solche Accounts vorhanden sind und wenn ja, diese unbedingt mit individuellen Passwörtern abzusichern.
- **Bildschirmschoner mit Kennwort sichern**  
Bei den gängigen Betriebssystemen haben Sie die Möglichkeit, Tastatur und Bildschirm nach einer gewissen Wartezeit zu sperren. Die Entsperrung erfolgt erst nach Eingabe eines korrekten Passwortes. Diese Möglichkeit gibt es nicht umsonst. Deshalb: Nutzen Sie sie! Ohne Passwortsicherung können unbefugte Dritte sonst bei vorübergehender Abwesenheit des rechtmäßigen Benutzers Zugang zu dessen PC erlangen. Natürlich ist es ziemlich störend, wenn die Sperre schon nach weniger Zeit erfolgt. Unsere Empfehlung: Fünf Minuten nach der letzten Benutzereingabe. Zusätzlich gibt es die Möglichkeit, die Sperre im Bedarfsfall auch sofort zu aktivieren (z. B. bei einigen Windows-Betriebssystemen: Strg+Alt+Entf drücken).

Quelle: [www.bsi-fuer-buerger.de/schuetzen/07\\_02.htm](http://www.bsi-fuer-buerger.de/schuetzen/07_02.htm)

Im IT-Grundschriftzhandbuch des BSI ([www.bsi.bund.de/gshb/index.htm](http://www.bsi.bund.de/gshb/index.htm)) gibt es darüber hinaus unter -> Maßnahmekataloge -> M4: Hardware und Software eine Vielzahl weiterführender Informationen und Empfehlungen zur Passwort-Sicherheit speziell in Unternehmen.

Redaktionsschluss: 06.02.2007  
Wir danken AOK Business

(Stand 07/2007)